Mobile Broadcast Services

Approved Version 1.1 – 29 Oct 2013

Open Mobile Alliance

OMA-TS-BCAST_Services-V1_1-20131029-A

Contents

1. SCOPE 11

2. REFERENCES 12

2.1 NORMATIVE REFERENCES 12
2.2 INFORMATIVE REFERENCES 17

3. TERMINOLOGY AND CONVENTIONS 18

3.1 CONVENTIONS 18
3.2 DEFINITIONS 18
3.3 ABBREVIATIONS 21

4. INTRODUCTION 24

4.1 VERSION 1.0 24
4.2 VERSION 1.1 24

5. MOBILE BROADCAST SERVICES 25

5.1 SERVICE PROVISIONING 26
5.1.1 Transport Protocol for Service Provisioning Messages 28
5.1.2 HTTP Binding 29
5.1.3 Authentication 29
5.1.4 Use of Global Status Codes for Service Provisioning Messages 29
5.1.5 General Service Provisioning Messages 30
5.1.6 Smartcard Profile Service Provisioning Messages 82
5.1.7 Message Compression 97
5.1.8 Provisioning Trigger Message (DRM Profile only) 97
5.1.9 Web-based Service Provisioning 98
5.1.10 Parental Control for Service Ordering 100
5.2 TERMINAL PROVISIONING 103
5.2.1 Terminal Provisioning through Interaction Channel 103
5.2.2 Terminal Provisioning through Broadcast Channel 105
5.3 INTERACTION 106
5.3.1 Protocols and media codecs for Service Interaction Function 107
5.3.2 Interactive retrieval of Service Guide 107
5.3.3 Interactive retrieval of Service related information 107
5.3.4 Interactive service ordering 107
5.3.5 Interaction for service and content protection 107
5.3.6 Service related interaction and feedback using Interactivity Media Documents 108
5.3.7 Service related interaction and feedback using Rich Media 134
5.3.8 Service Interaction launch and feedback 135
5.4 PERSONALIZATION/SUPPORT FOR USER-BASED PROFILES AND PREFERENCES 137
5.4.1 User-based Profiles over Broadcast Channel 137
5.4.2 Communicating the End User Preferences to Network 138
5.5 CHARGING 138
5.5.1 Chargeable Events in the Scope of the BCAST Enabler 139
5.5.2 When to Trigger Calls to the Charging Enabler 140
5.5.3 BCAST-related Information in Charging Messages 140
5.5.4 Exchange of charging data among systems 144
5.6 MOBILITY 144
5.6.1 Specifying Alternative Accesses for a Service 144
5.6.2 Global Identification of Services and Content 144
5.7 BROADCAST ROAMING 144
5.7.1 Roaming messages between Terminal and BSM 146
5.7.2 Roaming messages between Home BSM and Visited BSM 150
5.7.3 Scope of identifiers and Home BSM identification while roaming 154
5.8 LOCATION FILTERING OF BROADCAST SERVICES AND CONTENT 155

5.9 XML FOR SIGNALLING 156
5.9.1 Namespace identifier 156
5.9.2 Proprietary extensions 156
5.9.3 BCAST extensions 156
5.10 SERVICE PROVISIONING OF UNICAST SERVICES 156
5.11 GLOBAL STATUS CODES 157
5.12 AUXILIARY DATA DOWNLOAD AND INSERTION, AND SUPPORT FOR ADVERTISEMENTS 161
5.12.1 Auxiliary data insertion based on notification messages 161
5.12.2 Auxiliary data insertion based on network operation 162
5.13 SUBTITLING AND CLOSED CAPTIONS 162
5.14 NOTIFICATION FUNCTION 162
5.14.1 Discovery of Availability and Access to Notifications 163
5.14.2 Declaring the usage of a Notification message 164
5.14.3 Format of Notification Message 166
5.14.4 Notification Message Delivery 181
5.14.5 Notification Interfaces 184
5.14.6 Minimal support for emergency notifications 188
5.14.7 Guidelines for MediaInformation usage 188
5.14.8 Extensibility placeholders for future usage of Notification 189
5.15 PAUSE AND RESUME OF SUBSCRIPTION 189
5.15.1 Pause of Subscription 189
5.15.2 Resume of Subscription 190
5.16 USER DEFINED BUNDLES 190
5.17 PARENTAL CONTROL OF UNICAST SERVICES 190
5.18 RICH MEDIA SOLUTIONS (INFORMATIVE) 191
5.18.1 RMS usage scenarios 191
5.18.2 Linking 194
5.18.3 W3C SVG 198
5.18.4 3GPP DIMS 198
5.18.5 OMA RME 199
5.18.6 MPEG LASeR 200
5.18.7 Other RMS 201
5.19 SMARTCARD BROADCAST PROVISIONING 202
5.19.1 Declaring Smartcard Broadcast Provisioning as a Service within the Service Guide 202
5.19.2 Declaring Smartcard Broadcast Provisioning support in the Smartcard 202
5.19.3 Filtering of Smartcard Broadcast Provisioning Services 203
5.19.4 Transmission of files to the Smartcard 205
5.19.4.1 Envelope Technology 205
5.19.4.2 SCWS Technology 206
5.20 AUDIENCE MEASUREMENT FUNCTION 206
5.20.1 Terminal-Centric Audience Measurement 206
5.20.2 Smartcard-Centric Audience Measurement 225
5.20.2.1 Process description 225
5.20.2.2 Communication protocols between BCAST AM-M and BCAST AM-C 232
5.20.2.3 Messages 236
5.21 RELATED CONTENTS INQUIRY 253
5.22 COUPON DOCUMENTS 253
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 258
A.1 APPROVED VERSION HISTORY 258
APPENDIX B. EXAMPLES ON REALIZING INTERACTIVE SERVICES (INFORMATIVE) 259
B.1 USE OF MMS TEMPLATE FOR SERVICE INTERACTION (INFORMATIVE) 259
B.1.1 Retrieving the MMS Message Template 259
B.1.2 Launching MMS Message Template Client and creating Multimedia Message 259
B.1.2.1 Use case: Voting 259
B.1.2.2 Use case: Viewer's Contribution 260
B.1.3 Sending the Interaction Message 261

APPENDIX C. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) 262
C.1 SCR FOR BCAST CLIENT 262
C.2 SCR FOR BCAST SERVICE APPLICATION (BSA) 266
C.3 SCR FOR BCAST SERVICE DISTRIBUTION/ADAPTATION (BSDA) 267
C.4 SCR FOR BCAST SUBSCRIPTION MANAGEMENT (BSM) 269
C.5 SCR FOR BCAST NOTIFICATION CLIENT (NTC) 271
C.6 SCR FOR BCAST NOTIFICATION DISTRIBUTION ADAPTATION (NTDA) 271
C.7 SCR FOR BCAST AUDIENCE MEASUREMENT CLIENT IN TERMINAL (BCAST AM-C) 272
C.8 SCR FOR BCAST AUDIENCE MEASUREMENT CLIENT IN SMARTCARD (BCAST AM-C) 275
C.9 SCR FOR BCAST AUDIENCE MEASUREMENT MANAGEMENT (AM-M) 276
APPENDIX D. <MEDIAOBJECTSET> EXAMPLES (INFORMATIVE) 280
D.1 XHTML MP BUNDLE 280
D.2 MMS MESSAGE TEMPLATE BUNDLE 280
D.3 SMIL BUNDLE 281
APPENDIX E. WALK-THROUGH OF BROADCAST ROAMING (INFORMATIVE) 283
APPENDIX F. WALK-THROUGH OF LOCATION IMPLEMENTATION (INFORMATIVE) 286
F.1 STORAGE OF LOCATION INFORMATION 286
F.2 ACQUISITION OF LOCATION INFORMATION 287
F.3 LOCATION FILTERING LIFE CYCLE 287
F.4 RESTRICTIONS ON LOCATION FILTERING 287
APPENDIX G. BCAST MANAGEMENT OBJECT 289
G.1 OMA BCAST DEVICE MANAGEMENT GENERAL 289
G.2 OMA BCAST MANAGEMENT OBJECT TREE 289
G.3 BCAST MO PARAMETERS 291
G.3.1 <X> 291
G.3.2 <X>/BCASTRelease 291
G.3.3 <X>/BCASTClientID 291
G.3.4 <X>/HomeBDSEntryPoint 291
G.3.5 <X>/ServiceProviders 291
G.3.6 <X>/ServiceProviders/<X> 291
G.3.7 <X>/ServiceProviders/<X>/ID 292
G.3.8 <X>/SGServerAddress 292
G.3.9 <X>/SGServerAddress/<X> 292
G.3.10 <X>/SGServerAddress/<X>/URL 292
G.3.11 <X>/BDSEntryPoint 292
G.3.12 <X>/BDSEntryPoint/<X> 292
G.3.13 <X>/BDSEntryPoint/<X>/IPDC 293
G.3.14 <X>/BDSEntryPoint/<X>/IPDC/<X> 293
G.3.15 <X>/BDSEntryPoint/<X>/IPDC<X>//Tuning 293
G.3.16 <X>/BDSEntryPoint/<X>/IPDC/<X>/Tuning/<X> 293
G.3.17 <X>/BDSEntryPoint/<X>/IPDC/<X>/Tuning/<X>/Frequency 293
G.3.18 <X>/BDSEntryPoint/<X>/IPDC/<X>/Tuning/<X>/UseLPChannel 294
G.3.19 <X>/BDSEntryPoint/<X>/IPDC<X>//IPPlatformID 294
G.3.20 <X>/BDSEntryPoint/<X>/IPDC/<X>/DVBNetworkID 294
G.3.21 <X>/BDSEntryPoint/<X>/IPDC/<X>/ESGProviderID 294
G.3.22 <X>/BDSEntryPoint/<X>/MBMS 295
G.3.23 <X>/BDSEntryPoint/<X>/MBMS/<X> 295
G.3.24 X>/BDSEntryPoint/<X>/MBMS/<X>/SG 295
G.3.25 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X> 295
G.3.26 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/IPSourceAddress 295
G.3.27 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/IPMulticastAddress 295
G.3.28 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/Port 295
G.3.29 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer 296
G.3.30 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer/TMGI 296
G.3.31 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer/IsCounting 296

G.3.32 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer/Version 296
G.3.33 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/URLs 297
G.3.34 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/URLs/<X> 297
G.3.35 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/URLs/<X>/URL 297
G.3.36 <X>/BDSEntryPoint/<X>/MBMS/<X>/APNs 297
G.3.37 <X>/BDSEntryPoint/<X>/MBMS/<X>/APNs/<X> 297
G.3.38 <X>/BDSEntryPoint/<X>/MBMS/<X>/APNs/<X>/APN 297
G.3.39 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer 297
G.3.40 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer/TMGI 298
G.3.41 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer/IsCounting 298
G.3.42 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer/Version 298
G.3.43 <X>/BDSEntryPoint/<X>/BCMCS 298
G.3.44 <X>/BDSEntryPoint/<X>/BCMCS/<X> 299
G.3.45 <X>/BDSEntryPoint/<X>/BCMCS/<X>/NetworkID 299
G.3.46 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ControllerIPAddress 299
G.3.47 <X>/BDSEntryPoint/<X>/BCMCS/<X>/SGMulticastAddress 299
G.3.48 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU 299
G.3.49 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/MaxCID 299
G.3.50 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/LargeCIDs 300
G.3.51 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/MaxHeaderSize 300
G.3.52 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/MRRU 300
G.3.53 <X>/BDSEntryPoint/<X>/IPDC-SH 300
G.3.54 <X>/BDSEntryPoint/<X>/IPDC-SH/<X> 300
G.3.55 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning 300
G.3.56 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Frequency 301
G.3.57 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/UseLPChannel 301
G.3.58 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Complementary 301
G.3.59 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Complementary/HybridFrequency 301
G.3.60 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/ Complementary/UseLPChannel 302
G.3.61 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/IPPlatformID 302
G.3.62 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/DVBNetworkID 302
G.3.63 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/ESGProviderID 302
G.3.64 <X>/BDSEntryPoint/<X>/FLO 302
G.3.65 <X>/BDSEntryPoint/<X>/FLO/<X> 303
G.3.66 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning 303
G.3.67 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning/Priority 303
G.3.68 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning/Frequency 303
G.3.69 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning/Bandwidth 303
G.3.70 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU 303
G.3.71 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/MaxCID 304
G.3.72 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/LargeCIDs 304
G.3.73 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/MaxHeaderSize 304
G.3.74 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/MRRU 304
G.3.75 <X>/BDSEntryPoint/<X>/FLO/<X>/SG 304
G.3.76 <X>/BDSEntryPoint/<X>/FLO/<X>/SG/IPSourceAddress 304
G.3.77 <X>/BDSEntryPoint/<X>/FLO/<X>/SG/IPMulticastAddress 305
G.3.78 <X>/BDSEntryPoint/<X>/FLO/<X>/SG/IPMulticastPort 305
G.3.79 <X>/BSMSelector 305
G.3.80 <X>/BSMSelector/<X> 305
G.3.81 <X>/BSMSelector/<X>/Name 305
G.3.82 <X>/BSMSelector/<X>/BSMFilterCode 305
G.3.83 <X>/BSMSelector/<X>/IsHomeBSM 306
G.3.84 <X>/BSMSelector/<X>/HomeServiceProvisioningRequestAddress 306
G.3.85 <X>/BSMSelector/<X>/RoamingRules 306
G.3.86 <X>/BSMSelector/<X>/RoamingRules/<X> 306
G.3.87 <X>/BSMSelector/<X>/RoamingRules/<X>/Rule 306
G.3.88 <X>/BSMSelector/<X>/RoamingPriority 307

G.3.89 <X>/Roaming 307
G.3.90 <X>/Roaming/<X> 307
G.3.91 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders 307
G.3.92 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X> 307
G.3.93 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/Priority 307
G.3.94 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/BDSEntryPoint 308
G.3.95 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/ NetworkAccessPoints/ 308
G.3.96 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/ NetworkAccessPoints/<X> 308
G.3.97 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X> /NetworkAccessPoints/<X>/NAP 308
G.3.98 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/RoamingEntryPoint/NetworkAccessPoints/<X>/Proxy 308
G.3.99 <X>/Roaming/<X>/HomeRoamingRuleRequestAddress 308
G.3.100 <X>/Roaming/<X>/ForceHomeRoamingRuleRequestAddress 309
G.3.101 <X>/Roaming/<X>/IgnoreUnIdentifiedBSM 309
G.3.102 <X>/Roaming/<X>/UseVisitedServiceProvisioningMode 309
G.3.103 <X>/SmartcardProvisioning 309
G.3.104 <X>/SmartcardProvisioning /FixedAddressingMode 310
G.3.105 <X>/ SmartcardProvisioning/FixedAddressingMode /USF 310
G.3.106 <X>/Ext 310

APPENDIX H. GUIDELINES FOR EXTENDING THE XML SCHEMAS IN FUTURE VERSIONS OF BCAST 311

APPENDIX I. MEDIA-TYPE REGISTRATIONS 312

I.1 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.SPROV+XML 312
I.2 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.DRM-TRIGGER+XML 313
I.3 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.SMARTCARD-TRIGGER+XML 313
I.4 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.IMD+XML 313
I.5 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.NOTIFICATION+XML 314
I.6 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.PROVISIONINGTRIGGER 314
I.7 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.ROAMING+XML 315
I.8 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.AM-MESSAGE+XML 316
I.9 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.AM-TRIGGER 317
I.10 MEDIA-TYPE REGISTRATION REQUEST FOR APPLICATION/VND.OMA.BCAST.COUPON+XML 318

APPENDIX J. WALK-THROUGH OF ISSUING AND REDEEMING BROADCAST COUPONS (INFORMATIVE)320

J.1 NEWSPAPER COUPON 320
J.2 SERVICE PROVIDER COUPON 320
J.3 CONTENT PROVIDER COUPON 321
J.4 PREMIUM OR FREQUENT-USER COUPONS 321
J.5 FIRST-TIME OR NEVER-SUBSCRIBED COUPONS 321

Figures

Figure 1: Notification message delivery protocol stack variant 1 183

Figure 2: Notification message delivery protocol stack variant 2 183

Figure 3: Notification component exchange protocol stack 184

Figure 4: Filtering in Smartcard Broadcast provisioning 205

Figure 5: Coupon document and its pointers to Service Guide fragments. 254

Figure 6: The screen flow of Voting Template 260

Figure 7: The screen flow of Viewer's Contribution Template 261

Figure 8: Walk-through of Broadcast Roaming. 283

Figure 9: Life Cycle for Location-Filtered Ad Download and Rendering. 287

Figure 10: OMA BCAST Management Object Structure 291

Tables

Table 1: BCAST functions, Interfaces and Specifications 26

Table 2: Summary General Service Provisioning messages 28

Table 3: Summary Smartcard Service Provisioning messages 28

Table 4: Cross Reference Table (Informative) 30

Table 5: Structure of Pricing Information Request in General Service Provisioning Message 32

Table 6: Structure of Pricing Information Response in General Service Provisioning Message 36

Table 7: Structure of Service Request in General Service Provisioning Message 41

Table 8: Structure of Service Response in General Service Provisioning Message 45

Table 9: Structure of Service Completion in General Service Provisioning Message 45

Table 10: Structure of User Defined Bundle Request in General Service Provisioning Message 47

Table 11: Structure of User Defined Bundle Response in General Service Provisioning Message 48

Table 12: Structure of Price Offering Request in General Service Provisioning Message 50

Table 13: Structure of Price Offering Response in General Service Provisioning Message 50

Table 14: Structure of LTKM renewal request in General Service Provisioning Message 52

Table 15: Structure of LTKM renewal response in General Service Provisioning Message 55

Table 16: LTKM renewal completion in General Service Provisioning Message 55

Table 17: Structure of Unsubscribe Request in General Service Provisioning Message 58

Table 18: Structure of Unsubscribe Response in General Service Provisioning Message 59

Table 19: Structure of Token Purchase Request in General Service Provisioning Message 64

Table 20: Structure of Token Purchase Response in General Service Provisioning Message 67

Table 21: Structure of Token Purchase Completion in General Service Provisioning Message 67

Table 22: Structure of Account Inquiry Request in General Service Provisioning Message 69

Table 23: Structure of Account Inquiry Response in General Service Provisioning Message 70

Table 24: Structure of Subscription Pause Request in General Service Provisioning Message 72

Table 25: Structure of Subscription Pause Response in General Service Provisioning Message 74

Table 26: Structure of Subscription Resume Request in General Service Provisioning Message 75

Table 27: Structure of Subscription Resume Response in General Service Provisioning Message 77

Table 28: Structure of Related Contents Request message in General Service Provisioning 78

Table 29: Structure of Related Contentes Response message in General Service Provisioning 82

Table 30: Structure of RegistrationRequestExtension 86

Table 31: Structure of RegistrationResponseExtension 88

Table 32: Structure of RegistrationResponseServiceExtension 90

Table 33: Structure of LTKMResponseMSKExtension 91

Table 34: Structure of DeregistrationResponseServiceExtension 92

Table 35: DRM Profile Trigger Message Structure 97

Table 36: Mnemonics used in Table 35 97

Table 37: Semantics for Table 35 98

Table 38: Service_provisioning_type Coding 103

Table 39: OMA BCAST Device Management Client Requirements 105

Table 40: Data structure of InteractivityMediaDocument 130

Table 41: elements of <InteractivityMediaDocument> used for language selection 132

Table 42: Structure of Interactivity Media Document Request 137

Table 43: Structure of Interactivity Media Document Response 137

Table 44: Structure of End User Preference Message 138

Table 45: List of chargeable events 140

Table 46: Mapping table for Subscription based Charging 141

Table 47: Mapping table for Consumption based Charging 143

Table 48: Mapping table for Service Interaction 144

Table 49: Structure of RoamingRuleRequest Message 147

Table 50: Structure of Roaming RuleResponse Message 149

Table 51: Structure of RoamingServiceRequest Message 153

Table 52: Structure of RoamingServiceResponse Message 154

Table 53: Global Status Codes 160

Table 54: Event Types of Notifications 165

Table 55: Structure of Notification Message 181

Table 56: Header for UDP Delivery of Notification Message 182

Table 57: Structure of Notification Event Request Message 186

Table 58: Structure of Notification Event Response Message 186

Table 59: Structure of Notification Delivery Request Message 187

Table 60: Structure of Notification Delivery Response Message 188

Table 61: Audience Measurement Trigger Message Structure 212

Table 62: Mnemonics used in Table 61 212

Table 63: Semantics for Table 61 213

Table 64: Metering process state 229

Table 65: Message Tag format 235

Table 66: REGISTRATION_REQUEST message 236

Table 67: Identifiers Type 236

Table 68: Identifiers 237

Table 69: REGISTRATION_ RESPONSE message 238

Table 70: AUDIT_REQUEST message 238

Table 71: AUDIT_RESPONSE message 239

Table 72: OPT_IN message 241

Table 73: OPT_IN message 241

Table 74: OPT_IN_STATE_NOTIFICATION message 241

Table 75: CONFIGURATION message 242

Table 76: ACTIVATION message 244

Table 77: REPORTING message 244

Table 78: Zapping event record format 245

Table 79: list of tags for additional metrics 246

Table 80: Location TLV definition 247

Table 81: Consumption Time TLV definition 249

Table 82: Service/Content ID TLV definition 249

Table 83: Zapping event Record Format encoding 249

Table 84: REPORTING_RESPONSE message 250

Table 85: REPORTING message sent over HTTP 251

Table 86: REPORTING_REQUEST message 251

Table 87: Clear Message Tags 252

Table 88: MMS Template Example for Voting 260

Table 89: MMS Template Example for User Feedback 261

1. Scope

This specification, together with the other specification comprising the Mobile Broadcast Services Enabler (BCAST 1.0), define a technological framework and specify globally interoperable technologies for the generation, management and distribution of mobile broadcast services over different BCAST distribution systems. The complete list of the specifications for BCAST 1.0 is defined in the Enabler Release Definition of BCAST 1.0 [BCAST11-ERELD]. This enabler suite includes specifications for the following functions: Service Guide; Service and Content protection; File and Stream distribution; Terminal Provisioning; Service Provisioning; Notifications; Service Interaction and Audience Measurement. In addition, a specification is provided for Roaming, Mobility and Charging. Adaptations to specific BCAST distribution systems (3GPP/MBMS, 3GPP2/BCMCS, "IP Datacast over DVB-H" and "IP Datacast over DVB-SH") are specified in the Adaptation Specification documents.

Overall, the scope of the BCAST 1.0 enabler is service layer technologies. Thus, all specifications address the protocol layers on top of the radio bearer level. Furthermore, a common nominator for all the BCAST 1.0 technologies is that they are based on Internet Protocol (IP) and technologies related to IP. This scoping applies to all features and functionalities specified in BCAST 1.0.

The following functions are included in this specification: Service Provisioning; Terminal Provisioning; Interaction, Personalization and Support for User-Based Profiles and Preferences; Security and Privacy; Charging; Mobility; Broadcast Roaming; Notification; Location Information; Rich Media Environment and Audience Measurement. Further, this document provides mappings between the BCAST 1.1 interfaces as defined in BCAST Architecture [BCAST11-Architecture] and the various BCAST 1.1 Technical Specifications.

2. References

2.1 Normative References

[3GPP TS 22.022] "Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification", 3rd Generation Partnership Project, Technical Specification 3GPP TS 22.022 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 23.003] "Numbering, addressing and identification", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.003 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 23.032] "Universal Geographical Area Description (GAD)", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.032 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 23.038] "Technical Specification Group Core Network and Terminals; Alphabets and language-specific information (Release 8)", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.038,
URL: http://www.3gpp.org/

[3GPP TS 23.040] "Technical realization of the Short Message Service (SMS)", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.040 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 23.060] "General Packet Radio Service (GPRS); Service description; Stage 2", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.060,
URL: http://www.3gpp.org/

[3GPP TS 24.008] "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3", 3rd Generation Partnership Project, Technical Specification 3GPP TS 24.008 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 25.413] "UTRAN Iu interface Radio Access Network Application Part (RANAP) signaling", 3rd Generation Partnership Project, Technical Specification 3GPP TS 25.413 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 26.142] "Dynamic and Interactive Multimedia Scenes (DIMS)", 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.142 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 26.245] "Transparent end-to-end Packet switched Streaming Service (PSS); Timed text format", 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.245 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 26.246] "Transparent end-to-end Packet-switched Streaming Service (PSS); 3GPP SMIL language profile", 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.246 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 26.346] "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs", 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.346 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 31.102] "Characteristics of the Universal Subscriber Identity Module (USIM) application", 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.102 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 31.111] "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) ", 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.111 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 31.115] "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications
", 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.115 Release 8,
URL: http://www.3gpp.org/

[3GPP TS 33.246] "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)", 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.246 Release 8,

URL: http://www.3gpp.org/

[3GPP2 C.S0005-E] "Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0005-E, Release E, Version 1.0, September 2009,
URL: http://www.3gpp2.org/

[3GPP2 C.S0035-A] "CDMA Card Application Toolkit (CCAT)", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0035-A, Release A, Version 2.0, August 2007,
URL: http://www.3gpp2.org/

[3GPP2 C.S0050-B] "3GPP2 File Formats for Multimedia Services", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0050, Release B, Version 1.0, May 2007,
URL: http://www.3gpp2.org/

[3GPP2 C.S0065- B] "cdma2000 Application on UICC for Spread Spectrum Systems", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0065- B, Release B, Version 1.0, January 2010,
URL: http://www.3gpp2.org/

[3GPP2 C.S0072-0] "Mobile Station Equipment Identifier (MEID) Support for cdma2000 Spread Spectrum Systems,", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0072-0, Release 0, Version 1.0, July 2005,
URL: http://www.3gpp2.org/

[3GPP2 C.S0078-0] "Secured Packet Structure for CDMA Card Application Toolkit (CCAT) Applications", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0078-0, Release 0, Version 1.0, October 2006,
URL: http://www.3gpp2.org/

[3GPP2 X.S0022-A] "Broadcast and Multicast Service in cdma2000 Wireless IP Network", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 X.S0022-A, Release A, Version 1.0, February 2007,
URL: http://www.3gpp2.org/

[BCAST11-BCMCS-Adaptation] " BCAST Distribution System Adaptation – 3GPP2/BCMCS", Open Mobile Alliance™, OMA-TS-BCAST_BCMCS_Adaptation-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-DDF-BCAST-MO] "Mobile Broadcast Services – DDF of BCAST Management Object", Open Mobile Alliance™, OMA-SUP-MO_oma_bcast-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-Distribution] "File and Stream Distribution for Mobile Broadcast Services ", Open Mobile Alliance™, OMA-TS-BCAST_Distribution-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-DVBH-IPDC-Adaptation] " BCAST Distribution System Adaptation – IPDC over DVB-H", Open Mobile Alliance™, OMA-TS-BCAST_DVB_Adaptation-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-ERELD] "Enabler Release Definition for Mobile Broadcast Services", Open Mobile Alliance™, OMA-ERELD-BCAST-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-MBMS-Adaptation] " BCAST Distribution System Adaptation – 3GPP/MBMS", Open Mobile Alliance™, OMA-TS-BCAST_MBMS_Adaptation-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-Requirements] "Mobile Broadcast Services Requirements", Open Mobile Alliance™, OMA-RD-BCAST-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-ServContProt] "Service and Content Protection for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_SvcCntProtection-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-XMLSchema-InteractivityMedia] "Mobile Broadcast Services – XML Schema for InteractivityMediaDocument", Open Mobile Alliance™, OMA-SUP-XSD_bcast_si_interactivitymedia-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-XMLSchema-orderqueries] "Mobile Broadcast Services – XML Schema for Service Provisioning Order Queries", Open Mobile Alliance™, OMA-SUP-XSD_bcast_pr_orderqueries-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-XMLSchema-Roaming-backend] "Mobile Broadcast Services – XML Schema for Roaming Messages – Backend ", Open Mobile Alliance™, OMA-SUP-XSD_bcast_roaming_backend-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-XMLSchema-Roaming-frontend] "Mobile Broadcast Services – XML Schema for Roaming Messages – Frontend", Open Mobile Alliance™, OMA-SUP-XSD_bcast_roaming_frontend-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST10-XMLSchema-Userpreference] "Mobile Broadcast Services – XML Schema for User Preferences ", Open Mobile Alliance™, OMA-SUP-XSD_bcast_pr_userpreference-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST11-DVBSH-IPDC-Adaptation] "Broadcast Distribution System Adaptation – IPDC over DVB-SH", Open Mobile Alliance™, OMA-TS-BCAST_DVB_Adaptation-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-ServContProt] "Service and Content Protection for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_SvcCntProtection-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-Services] "Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_Services-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-SG] "Service Guide for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_ServiceGuide-V1_1,
URL: http://www.openmobilealliance.org/

[CONNMO] *Standardized Connectivity Management Objects, Version 1.0,* Open Mobile Alliance™, OMA-DDS-DM_ConnMO_V1_0-D,
URL: http://www.openmobilealliance.org/

[OMA DM 1.3] "Enabler Release Definition for OMA Device Management v1.3", OMA-ERELD-DM-V1_3_0,
URL: http://www.openmobilealliance.org/

[DMBOOT] "OMA Device Management Bootstrap, Version 1.2". Open Mobile Alliance™, .
OMA-TS-DM_Bootstrap-V1_2.
URL: http://www.openmobilealliance.org/

[DMDDFDTD] "OMA DM Device Description Framework DTD, Version 1.2". Open Mobile Alliance™, .
OMA-SUP-dtd_dm_ddf-v1_2.
URL: http://www.openmobilealliance.org/

[DMNOTI] "OMA Device Management Notification Initiated Session, Version 1.2". Open Mobile Alliance™. OMA-DM_Notification-V1_2. .
URL: http://www.openmobilealliance.org/

[DMPRO] "OMA Device Management Protocol, Version 1.2". Open Mobile Alliance™, .
OMA-TS-DM_Protocol-V1_2.
URL: http://www.openmobilealliance.org/

[DMREPU] "OMA Device Management Representation Protocol, Version 1.2", .
Open Mobile Alliance™. OMA-TS-DM_RepPro-V1_2.
URL: http://www.openmobilealliance.org/

[DMSEC] "OMA Device Management Security, Version 1.2". Open Mobile Alliance™, .
OMA-TS-DM_Security-V1_2.
URL: http://www.openmobilealliance.org/

[DMSTDOBJ] "OMA Device Management Standardized Objects, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_StdObj-V1_2.
URL: http://www.openmobilealliance.org/

[DMTND] "OMA Device Management Tree and Description, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_TND-V1_2.
URL: http://www.openmobilealliance.org/

[DMTNDS] "OMA Device Management Tree and Description Serialization, Version 1.2". Open Mobile Alliance™. OMA-TS-DM_TNDS-V1_2.
URL: http://www.openmobilealliance.org/

[DRM20-Broadcast-Extensions] "OMA DRM v2.0 Extensions for Broadcast Support", Open Mobile Alliance™, OMA-TS-DRM-XBS-V1_0,
URL: http://www.openmobilealliance.org/

[DRMDRM-v2.0] "DRM Specification V2.0", Open Mobile Alliance™, OMA-DRM-DRM-V2_0,
URL: http://www.openmobilealliance.org/

[ERELDSC] "Enabler Release Definition for SyncML Common Specifications, version 1.2". Open Mobile Alliance™. OMA-ERELD-SyncML-Common-V1_2.
URL: http://www.openmobilealliance.org/

[ETSI EN 300 468] ETSI EN 300 468 v1.x.x, "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems",
URL: http://portal.etsi.org/

[ETSI EN 302 304] ETSI EN 302 304 v1.x.x, "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)",
URL:http://portal.etsi.org/

[ETSI TS 102.223] "Smart Cards; Card Application Toolkit (CAT)",
URL: http://www.etsi.org/ Release 10 or later

[ETSI TS 101.220] "Smart Cards; ETSI numbering system for telecommunication application providers"
URL: http://www.etsi.org/

[ETSI TS 102.221] "Smart Cards; UICC-Terminal interface; Physical and Logical Characteristics",
URL: http://www.etsi.org/

[ETSI TS 102.600] "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface",
URL: http://www.etsi.org/

[HTML4.01] "HTML 4.01 Specification", W3C Recommendation 24 December 1999,
URL: http://www.w3.org/TR/html401/

[IEEE 802.16-2004] IEEE 802.16-2004 October 2004, Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, August 2004
URL: http://www.ieee.org

[IEEE 802.16e-2005] IEEE 802.16-2005. Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, February 2006
URL: http://www.ieee.org

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1,
URL: http://www.openmobilealliance.org/

[ISO-639-1] "Codes for the representation of names of languages",
URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22109

[ISO/IEC 14496-20] "Information technology — Coding of audio-visual objects — Part 20: Lightweight Application Scene Representation (LASeR) and Simple Aggregation Format (SAF)", ISO/IEC 14496-20, Second edition 2008-12-01
URL: http://standards.iso.org/

[ITU-MCC] "List of Mobile Country or Geographical Area Codes", ITU-T Telecommunication Standardization Sector of ITU Complement To ITU-T Recommendation E.212 (05/2004),
URL: http://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.212A-2007-PDF-E.pdf
Note: This List will be updated regularly by numbered series of amendments published in ITU Operational Bulletin. For the latest version see:
URL: http://www.itu.int/itu-t/bulletin/annex.html

[MMSCONF] "MMS Conformance Document 1.3", Open Mobile AllianceOpen Mobile Alliance™, □. OMA-MMS-CONF-1_3.doc.
URL: http://www.openmobilealliance.org/

[MMSTEMP] "MMS Message Template Specification 1.3", Open Mobile Alliance™, Open Mobile Alliance□. OMA-MMS-TEMP-1_3.doc.
URL: http://www.openmobilealliance.org/

[OMA Charging AD] "Charging Architecture", Open Mobile Alliance™, OMA-AD-Charging-V1_1, URL: http://www.openmobilealliance.org/

[OMA Charging DDS] "Charging Data", Open Mobile Alliance™, OMA-DDS-Charging_Data-V1_0, URL: http://www.openmobilealliance.org/

[OMA DM 1.2] "Enabler Release Definition for OMA Device Management v1.2", OMA-ERELD-DM-V1_2_0, URL: http://www.openmobilealliance.org/

[OMA FUMO] "OMA Enabler Release Definition for Firmware Update Management Object v1.0", Open Mobile Alliance™, OMA-ERELD-FUMO-V1_0, URL: http://www.openmobilealliance.org/

[OMA MLP] "Mobile Location Protocol", Open Mobile AllianceOpen Mobile Alliance™TM, OMA-TS-MLP-V3_2 URL: http://www.openmobilealliance.org/

[OMA SCWS11] "Smartcard-Web-Server", Open Mobile Alliance™, OMA-TS-Smartcard_Web_Server-V1_1; URL: http://www.openmobilealliance.org/

[RFC 1951] "DEFLATE Compressed Data Format Specification version 1.3", P. Deutsch, May 1996, URL:http://www.ietf.org/rfc/rfc1951.txt

[RFC 1952] "ZIP file format specification version 4.3", P. Deutsch, May 1996, URL:http://www.ietf.org/rfc/rfc1952.txt

[RFC 2048] "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", N. Freed, J. Klensin, J. Postel, November 1996, URL: http://www.ietf.org/rfc/rfc2048.txt

[RFC 2104] "HMAC: Keyed-Hashing for Message Authentication", H. Krawczyk, M. Bellare, R. Canetti, February 1997, URL: http://www.ietf.org/rfc/rfc2104.txt

[RFC 2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL: http://www.ietf.org/rfc/rfc2119.txt

[RFC 2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997, URL: http://www.ietf.org/rfc/rfc2234.txt

[RFC 2246] "The TLS Protocol, Version 1.0", T. Dierks, C.Allen, January 1999, URL: http://www.ietf.org/rfc/rfc2246.txt

[RFC 2326] IETF RFC 2326, "Real Time Streaming Protocol (RTSP) ", URL : http://www.ietf.org/rfc/rfc2326.txt

[RFC 2616] IETF RFC 2616, "Hypertext Transfer Protocol -- HTTP/1.1", URL: http://www.ietf.org/rfc/rfc2616.txt

[RFC 2822] RFC 2822, "Internet Message Format", P. Resnick, Ed. April 2001, URL: http://www.ietf.org/rfc/rfc2822.txt.

[RFC 2865] "Remote Authentication Dial In User Service (RADIUS)", The Internet Engineering Task Force RFC 2865, URL: http:// www.ietf.org/

[RFC 3261] "SIP: Session Initiation Protocol", Rosenberg, J. et al, June 2002, URL: http://www.ietf.org/rfc/rfc3261.txt

[RFC 3830] "MIKEY: Multimedia Internet KEYing", J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman, August 2004, URL: http://www.ietf.org/rfc/rfc3830.txt

[RFC 3966] "The tel URI for Telephone Numbers", Schulzrinne, H., December 2004, URL: http://www.ietf.org/rfc/rfc3966.txt

[RFC3711] "The Secure Real-time Transport Protocol (SRTP)", M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, March 2004, URL: http://www.ietf.org/rfc/rfc3711.txt

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[RME] "Rich Media Environment Technical Specification, Version 1.0". Open Mobile Alliance™, . OMA-TS-RME-V1_0-20081014-C
URL: http://www.openmobilealliance.org/

[OMA SCOMO] "OMA Enabler Release Definition for Software Component Management Object v1.0", Open Mobile Alliance™, OMA-ERELD-SCOMO-V1_0,
URL: http://www.openmobilealliance.org/

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures,
URL: http://www.openmobilealliance.org/

[SSL30] "SSL 3.0 Specification", Netscape Communications, November 1996,
URL: http://wp.netscape.com/eng/ssl3/draft302.txt

[TIA-1099a] TIA-1099, Revision A, "Forward Link Only Air Interface Specification for Terrestrial Mobile Multimedia Multicast ", April 2009.
URL: http://global.ihs.com

[URI-Schemes] "URI Schemes for the Mobile Applications Environment", Version 1.0, Open Mobile Alliance™,
URL: http://www.openmobilealliance.org/

[W3C SVG Tiny] "Scalable Vector Graphics (SVG) Tiny 1.2 Specification", W3C Recommendation 22 December 2008
URL: http://www.w3.org/TR/SVGTiny12/

[XHTMLMP11] "XHTML Mobile Profile 1.1", Open Mobile AllianceOpen Mobile Alliance™. OMA-WAP-XHTMLMP-V1_1.
URL: http://www.openmobilealliance.org/

[XML] Extensible Markup Language (XML) 1.1, W3C Recommendation 04 February 2004, edited in place 15 April 2004.
URL: http://www.w3.org/TR/xml11

[XMLSchema] XML Schema,
URL: http://www.w3.org/XML/Schema

2.2 Informative References

[BCAST11-Architecture] "Mobile Broadcast Services Architecture", Open Mobile Alliance™, OMA-AD- BCAST-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST11-ERELD] "Enabler Release Definition for Mobile Broadcast Services", Open Mobile Alliance™, OMA-ERELD-BCAST-V1_1,
URL: http://www.openmobilealliance.org/

[DMACMO] "White Paper on Provisioning Objects". Open Mobile Alliance™. OMA-WP-AC_MO.
URL: http://www.openmobilealliance.org/

[ETSI 102 470-1] ETSI TS 102 470-1 v1.x.x,), "Digital Video Broadcasting (DVB); IP Datacast: Program Specific Information (PSI)/Service Information (SI) ; Part1: IP Datacast over DVB-H",
URL: http://portal.etsi.org

[ETSI 102 470-2] ETSI TS 102 470 v1.x.x, "Digital Video Broadcasting (DVB); IP Datacast: Program Specific Information (PSI)/Service Information (SI); IP Datacast over DVB-SH",
URL: http://portal.etsi.org

[OMADICT] "Dictionary for OMA Specifications", Version 2.7, Open Mobile Alliance™,
OMA-ORG-Dictionary-V2_7,
URL: http://www.openmobilealliance.org/

[RFC 2397] "The 'data' URL scheme", L. Masinter, August 1998,
URL: http://www.ietf.org/rfc/rfc2397.txt

[RFC 4281] "The Codecs Parameter for "Bucket" Media Types", R. Gellens, D. Singer, P. Frojdh, November 2005,
URL: http://www.ietf.org/rfc/rfc4281.txt

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

The following is the legend used in this specification:

Type: E=Element, A=Attribute, E1=sub-element, E2=sub-element’s sub-element, E[n]=sub-element of element[n-1]

Cardinality: x..y = the number of the presented instance of this element/attribute is in the range from x to y. If x=0, this specific element/attribute is OPTIONAL for network to use, otherwise it is MANDATORY for network to use.

Category: NM = Mandatory for network to support; NO = Optional for network to support; TM = Mandatory for terminal to support; TO = Optional for terminal to support. M = Mandatory to support; O = Optional to support. If an element or attribute has a cardinality greater than zero, it is always classified as M or NM to maintain consistency.

The following relationship applies between elements and their sub-elements respectively attributes:

If an implementation chooses to support an element of category, …	**… it MUST also support all its sub-elements and attributes of category**	**… it MAY also choose to support any of itssub-element or attribute of category**
O	**M**	**O**
NO	**NM**	**NO**
TO	**TM**	**TO**

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

03.40 Packet Format	SMS format as described in [3GPP TS 23.040] including the concatenation of SMS messages.
Audience Measurement	Audience Measurement is the method of measuring usage statistics in relation to consumption of BCAST Content and Service.
Audience Measurement Campaign	Audience Measurement Campaign is an Audience measurement session during a specific time period on a specific group of users
Audience Measurement Function	The global function ensuring the Audience Measurement includes the BCAST enabler entities that participate to the Audience Measurement collect/processing. The foreseen BCAST enablers related entities are the BCAST Audience Measurement function on the Client side (AM-C) and the BCAST Audience Measurement function on the Network side (AM-M).
BCAST Distribution System	A system typically but not necessarily containing the ability to transmit the same IP flow to multiple Terminal devices simultaneously. A BCAST Distribution System (BDS) typically uses techniques that achieve efficient use of radio resources. A BDS consists of Network functionality up to the IP layer and optional Service Distribution/Adaptation functionality above the IP layer. Most BDSs support broadcast/multicast distribution in the network. Some BCAST Distribution Systems have the capability to deliver the IP flows in the network via unicast.
Broadcast Roaming	Broadcast Roaming is the ability of a user to receive broadcast services from a Mobile Broadcast Service Provider different from the Home Mobile Broadcast Service Provider with which the user has a

contractual relationship.

Broadcast Service

A Broadcast Service is a "content package" suitable for simultaneous distribution to many recipients (potentially) without knowing the recipient. Either each receiver has similar receiving devices or the content package includes information, which allows the client to process the content according to his current conditions.

Examples of Broadcast Services are:

- pure Broadcast Services:
  - mobile TV
  - mobile newspaper
  - mobile file downloading (clips, games, SW upgrades, other applications, applications)
- combined broadcast/interactive Broadcast Services:
  - mobile TV for file downloading with voting
  - betting Broadcast Services
  - auction Broadcast Services
  - trading Broadcast Services

Broadcast Service Area

The geographical or logical area in which a Broadcast Service is distributed.

CSIM

Acronym for 'cdma2000 Subscriber Identify Module', corresponding to an application defined in [3GPP2 C. S0065-B] residing on the UICC to register services provided by 3GPP2 mobile networks with the appropriate security.

Home Mobile Broadcast Service Provider

The Mobile Broadcast Service Provider with which the user has a subscription. Typically a user has one Home Mobile Broadcast Service Provider. However, the user may also have no Home Mobile Broadcast Service Provider or several Home Mobile Broadcast Service Providers

IRM (International Roaming MIN)

A form of MIN defined by IFAST (International Forum on ANSI-41 Standards Technology) towards facilitating international roaming by minimizing conflicts with the North American MIN.

ISIM

An IP Multimedia Services Identity Module is an application defined in [3GPP TS 31.103 v6] and [3GPP2 C.S0069-0] residing in the memory of the UICC, providing IP service identification, authentication and ability to set up Multimedia IP Services.

Location Information

Data derived on a terminal from external hardware, such as a cellular or GPS subsystem, that tells the terminal where it is located in the physical world. The allowed types of Location Information are listed in Section 5.8.

Long-Term Key Message

Collection of keys and possibly, depending on the profile, other information like permissions and/or other attributes that are linked to items of content or services.

Measures (or metrics)

Set of parameters and procedures that quantitatively and qualitatively measure the usage of a BCAST service/content .

MIN (Mobile Identification Number)

MIN is a numeric ID that uniquely identifies a mobile defined by TIA standards for Cellular and PCS technologies. The MIN may be in the form of an IRM (International Roaming MIN). Note: the MIN may be in the form of the IRM.

Mobile Broadcast Service

Mobile Broadcast Services include a wide range of broadcast services, which jointly leverage both the unidirectional one-to-many broadcast paradigm and bi-directional unicast paradigm in a mobile environment, covering one-to-many services ranging from classical broadcast to mobile multicast. Typically, Mobile Broadcast Services deliver content suitable for simultaneous one-way distribution to a potentially large number of recipients without relying on specific addressing information of each recipient. Associated two-way interactive transactions having contextual relevance to the broadcast programs typically rely on established unicast delivery methods requiring specific recipient addressing information.

Examples of Mobile Broadcast Services include the following:

- pure Broadcast Services:
  - mobile TV
  - mobile newspaper
  - mobile file downloading
- combined broadcast/interactive Broadcast Services:
  - mobile TV for file downloading with voting

- Broadcast Services for betting
- Broadcast Services for auction
- Broadcast Services for trading

Mobile Broadcast Service Provider	Business entity that has a role of providing the Mobile Broadcast Services to the user. Mobile Broadcast Service Provider may operate any set of server side functionalities as outlined in Mobile Broadcast Services Architecture [BCAST11-Architecture]. Mobile Broadcast Service Provider may have a subscription with the user. Note: In this specification Mobile Broadcast Service Provider is not technical or architectural concept
Mobility	The ability to receive service independent of location or while moving. (from OMA Dictionary)
Opt-In	Action to agree to participate in Audience Measurement Campaigns
Opt-Out	Action to disagree to participate in Audience Measurement Campaign or to leave from Audience Measurement Campaign already Opt-in
Panel (of users)	Group of users targeted for an Audience Measurement Campaign according to some specific criteria
Purchase Item	A purchase item groups one or multiple services or pieces of content that an end-user can purchase or subscribe to as a whole [BCAST11-SG].
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices [DRMDRM-v2.0].
Rights Object	A collection of Permissions, Constraints, and other attributes which define under what circumstances access is granted to, and what usages are defined for, DRM Content. All OMA DRM Conformant Devices must adhere to the Rights Object associated with DRM Content [DRMDRM-v2.0].
R-UIM	Acronym for 'Removable User Identity Module', corresponding to a non-UICC platform based module as defined in [3GPP2 C.S0023] to register services provided by 3GPP2 mobile networks with the appropriate security.
Short-Term Key Message	Message delivered alongside a protected service, carrying key material to decrypt and optionally authenticate the service, and access rights to delivered content.
Smartcard	A non-UICC secure function platform which may contain the SIM or R-UIM module, or a UICC-based secure function platform which may contain one or more of the following applications: a 3GPP USIM 3GPP2 CSIM or 3GPP/3GPP2 ISIM. Note that the set of applications/modules residing on the Smartcard are typically governed by the affiliation of the Smartcard to 3GPP or 3GPP2 specifications, as indicated by the definition below for "Smartcard Profile".
Smartcard Profile	Alias for a set of Smartcard-based technologies and mechanisms which provide key establishment and key management, as well as permission and token handling for the Service and Content Protection solution for BCAST Terminals. In particular, subscriber key establishment and both short and long term key management may be based on GBA mechanisms and a Smartcard with (U)SIM/ISIM as defined by 3GPP, or based on a pre-provisioned shared secret key and a Smartcard with R-UIM/CSIM/ISIM or a UIM as defined by 3GPP2. The Smartcard Profile is described in [BCAST11-ServContProt] Section 6.
Smartcard-Centric Audience Measurement	The Smartcard-Centric Audience Measurement implements the Audience Measurement Client part on the Smartcard
Terminal-Centric Audience Measurement	The Terminal-Centric Audience Measurement implements the Audience Measurement Client part on the Terminal
UICC	A Universal Integrated Circuit Card is a physically removable secured device as defined in [3GPP TS 31.101] for communication purposes not restricted to mobile convenience only. It is a platform to all the resident applications (e.g., USIM, CSIM or ISIM).
User ID	A unique ID that can be used to identify the user in the BCAST service areas of both the Home Mobile Broadcast Service Provider and the Visited Mobile Broadcast Service Provider. An example is the 3GPP/3GPP2 IMSI (International Mobile Subscriber Identity) as specified in [3GPP TS 23.003] and [3GPP2 C.S0005-E] (for the case the Broadcast Service Provider is a cellular mobile operator).
Visited Mobile Broadcast Service Provider	Any other Mobile Broadcast Service Provider than the user's Home Mobile Broadcast Service Provider.

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
ADF	Application Dedicated File
ADF_BSIM	ADF for BCAST Subscriber Identity Module
AMCI	Audience Measurement Campaign Invitation
AMCP	Audience Measurement Campaign Participation
AMRD	Audience Measurement Report Delivery
AMRR	Audience Measurement Report Response
AMRT	Audience Measurement Report Trigger
APDU	Application Protocol Data Unit
BASE_ID	Base Station Identification
BASE_LAT	Base Station Latitude
BASE_LONG	Base Station Longitude
BCAST	Mobile Broadcast Services
BCMCS	Broadcast Multicast Service
BDS	BCAST Distribution System
BIP	Bearer Independent Protocol
BSA	BCAST Service Application
BSD/A	BCAST service distribution/adaptation
BSDA	BCAST Service Distribution and Adaptation
BSID	Base Station Identification
BSM	BCAST Subscription Management
BSM	BCAST Subscription Management
BSP-C	Broadcast service provisioning Client Function
BSP-M	Broadcast service provisioning Management Function
CID	Content ID
CSIM	Cdma2000 Subscriber Identity Module
DCF	DRM Content Format
DF BCAST	Dedicated File for BCAST
DIMS	Dynamic and Interactive Multimedia Scenes
DRM	Digital Rights Management
DVB	Digital Video Broadcast
DVB-H	Digital Video Broadcast – Handheld
DVB-SH	Digital Video Broadcast – Satellite to Handheld
DVB-T	Digital Video Broadcast – Terrestrial
EF	Elementary File
EN	European Norm
ESG	Electronic Service Guide
ETSI	European Telecommunications Standards Institute
FDT	File Delivery Table

FEC	Forward Error Correction
FLUTE	File Delivery over Unidirectional Transport
GAD	Geographical Area Description
GZIP	GNU zip
HSP	High Speed Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IC	Interaction Channel
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
INT	IP/MAC Notification Table
IP	Internet Protocol
IPDC	IP DataCast
IPsec	IP security
ISIM	IP Multimedia Services Identity Module
ISMACryp	Internet Streaming Media Alliance (ISMA) Encryption and Authentication
KMS	Key Management System
LAC	Location Area Code
LASeR	Lightweight Application Scene Representation
LOI	Local-Area OIS Infrastructure
LTKM	Long-Term Key Message
MBMS	Multimedia Broadcast / Multicast Service
MEID	Mobile Equipment Identifier
MF	Master File
MIKEY	Multimedia Internet KEYing
MMS	Multimedia Messaging System
MO	Management Object
MO-SMS	Mobile Originated Short Message Service
MT-SMS	Mobile Terminated Short Message Service
MPE	Multi-Protocol Encapsulation
MTD	Message Template Definition
NID	Network IDentification
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
OSF	Open Security Framework
PSI/SI	Program Specific Information/Service Information
RI	Rights Issuer
RME	Rich Media Environment
RMS	Rich Media System
RO	Rights Object

RTCP	Real Time Control Protocol
R-UIM	Removable User Identity Module
SCWS	Smart Card Web Server
SDP	Session Description Protocol
SG	Service Guide
SG-C	Service Guide-Client
SG-D	Service Guide-Distribution
SGDU	Service Guide Delivery Unit
SID	System IDentification
SIP	Session Initiation Protocol
SMIL	Synchronized Media Integration Language
SMS	Short Message Service
SMS-PP	Short Message Service Point to Point
SRTP	Secure Real-time Transport Protocol
STKM	Short Term Key Message
TAR	Toolkit Application Reference
TCP	Transmission Control Protocol
TP-C	Terminal Provisioning Client Component
TP-M	Terminal Provisioning Management Component
TR	Technical Report
TS	Technical Specification
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
USF	Unique Smartcard Filter
USIM	Universal Subscriber Identity Module
WAP	Wireless Application Protocol
WOI	Wide-Area OIS Infrastructure
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language

4. Introduction

The term "Mobile Broadcast Services" refers to a broad range of Broadcast Services, which jointly leverage the unidirectional one-to-many broadcast paradigm and the bi-directional unicast paradigm in a mobile environment, and covers one-to-many services ranging from classical broadcast to mobile multicast.

Building on mobile network systems, which provide bi-directional links, and digital broadcast systems, which provide uni-directional broadcast, Mobile Broadcast Services enable distribution of rich, interactive, and bandwidth consuming media content to large mobile audiences.

4.1 Version 1.0

In general, the availability of both broadcast channel and interaction channel are assumed for the BCAST 1.0 enabler. However, both broadcast channel and interaction channel may be temporarily unavailable, for example due to lack of radio coverage. Further, devices without access to an interaction channel are possible within the BCAST architecture and specifications. However, such devices may have limited functionality. Optimizations for devices without interaction channel are optional to implement in devices with interaction channel and are optional to use (for details see the SCR tables). Parts of the enabler are adaptation specifications for IPDC over DVB-H [BCAST10-DVBH-IPDC-Adaptation], 3GPP MBMS [BCAST10-MBMS-Adaptation], and 3GPP2 BCMCS [BCAST10-BCMCS-Adaptation].

This specification is structured as follows. Chapter 5 starts by mapping the interfaces as defined in BCAST Architecture [BCAST10-Architecture] to the various BCAST 1.0 Technical Specifications. Further, chapter 5 specifies the following BCAST 1.0 functions: Service Provisioning; Terminal Provisioning; Interaction, Personalization and Support for User-Based Profiles and Preferences; Charging; Mobility; Broadcast Roaming; Notification; and; Location Information. Appendix D provides informative examples related to service interaction and Appendix E illustrates the roaming related flows.

It is assumed that in BCAST 1.0 the network will make use of the BDS resources in accordance with the capabilities of the BDS.

4.2 Version 1.1

The Mobile Broadcast Services Enabler 1.1 aims to maintain backward compatibility while fulfilling the requirements and features stated in the BCAST requirements document [BCAST11-Requirements].

This specification is structured as follows. Chapter 5 starts by mapping the interfaces as defined in BCAST Architecture [BCAST11-Architecture] to the various BCAST 1.1 Technical Specifications. In addition to enhancement of BCAST 1.0 functionalities, chapter 5 specifies the following BCAST 1.1 functions: Pause and Resume of Subscription, User Defined Bundle, Parental Control of Unicast Services, Parental Control for Service Ordering, Rich Media Solutions, Smartcard Broadcast Provisioning, Terminal Broadcast Provisioning, Audience Measurement, Related Contents Inquiry, and Coupon Documents. Appendix F provides informative examples related to Location Services.

It is assumed that in BCAST 1.1 the network will make use of the BDS resources in accordance with the capabilities of the BDS.

5. Mobile Broadcast Services

Mobile Broadcast Services Architecture [BCAST11-Architecture] defines the Mobile Broadcast Services Enabler as a set of service-enabling functions. Within the overall architecture, each function has a set of interfaces, each of which forms the basis for interoperability. Although the architecture as such is not normatively specified, the interfaces provide a useful tool to map the various parts of BCAST specifications to the context of the overall architecture. The following table outlines how different parts of the BCAST Enabler are specified in the Technical Specifications.

Function	Interface	Normative Specification
Service Guide	SG-1	Out of scope of BCAST 1.0
	SG-2	Out of scope of BCAST 1.0
	SG-4	Refer to [BCAST11-SG], section 5.3 and 5.6
	SG-5	Refer to [BCAST11-SG], sections 5.3, 5.4.2 and 6.1.1
	SG-6	Refer to [BCAST11-SG], sections 5.3, 5.4.3, 6.1.2 and 6.2
	SG-B1	Refer to [BCAST11-SG], sections 5.3 and each BDS Adaptation Specification.
	SG-9	Refer to [BCAST11-SG], section 5.1.2.4 and to this specification section 5.19
File Distribution	FD-1	Refer to [BCAST11-Distribution], section 5.4.1
	FD-2	Refer to [BCAST11-Distribution], section 5.4.1
	FD-5	Refer to [BCAST11-Distribution], section 5.2
	FD-6	Refer to [BCAST11-Distribution], section 5.3 and 5.5
	FD-B1	Refer to [BCAST11-Distribution] section 5.4.2 and each BDS Adaptation Specification.
	FD-9	Refer to this specification, section 5.19
Stream Distribution	SD-1	Refer to [BCAST11-Distribution], section 6.4.1
	SD-2	Refer to [BCAST11-Distribution], section 6.4.1
	SD-5	Refer to [BCAST11-Distribution], section 6.2
	SD-6	Refer to [BCAST11-Distribution], section 6.3 and 6.5
	SD-B1	Refer to [BCAST11-Distribution] section 6.4.2 and each BDS Adaptation Specification.
Service Protection	SP-2	Uses SD-2 and FD-2
	SP-4	Refer to [BCAST11-ServContProt] section 13.1
	SP-5-1	Refer to [BCAST11-ServContProt] section 5.6.1.1, 5.6.2.1, 6.8.1.1, and 6.8.2.1
	SP-5-2	Refer to [BCAST11-ServContProt] section 5.3, 5.4, 5.5, 6.5, 6.6, and 6.7
	SP-7	Refer to [BCAST11-ServContProt] section 5.3, 5.4, 6.5, and 6.6
	SP-9	Refer to [BCAST10-ServContProt] section 6.12 and Appendix E
	SP-10	Out of scope (this is a terminal internal interface and is not standardized within OMA BCAST)
Content Protection	CP-2	Uses SD-2 and FD-2
	CP-4	Refer to [BCAST11-ServContProt] section 13.2
	CP-5-1	Refer to [BCAST11-ServContProt] sections 5.6.1.2, 5.6.2.2, 6.8.1.2, and 6.8.2.2
	CP-5-2	Refer to [BCAST11-ServContProt] sections 5.3, 5.4, 5.5, 6.5, 6.6, and 6.7
	CP-7	Refer to [BCAST11-ServContProt] sections 5.3, 5.4, 6.5, and 6.6
	CP-9	Refer to [BCAST10-ServContProt] sections 6.12 and Appendix E
	CP-10	Out of scope of BCAST 1.0 (this is a terminal internal interface

		and is not standardized within OMA BCAST)
Service Interaction	SI-8	Refer to this specification, section 5.3
Service Provisioning	SPR-7	Refer to this specification, section 5.1
	SPR-8	Out of scope (this interface is for out-of-band subscription)
Notification	NT-1	Refer to this specification, section 5.14
	NT-3	Refer to this specification, section 5.14
	NT-4	Refer to this specification, section 5.14
	NT-5	Refer to this specification, section 5.14
	NT-6	Refer to this specification, section 5.14
Terminal Provisioning	TP-4	Refer to this specification, section 5.2
	TP-5	Refer to this specification, section 5.2
	TP-7	Refer to this specification, section 5.2
Audience Measurement	AM-3-1	Out of scope of BCAST 1.1
	AM-3-2	Out of scope of BCAST 1.1
	AM-5	Refer to [BCAST11-SG], section 5.4.1.5.2 and to this specification, section 5.20.1and 5.20.2
	AM-7-1	Refer to [BCAST11-SG], section 5.4.1.5.2 and to this specification, sections 5.20.1 and, 5.20.2
	AM-7-2	Refer to [BCAST11-SG], section 5.4.1.5.2 and to this specification, section 5.20.1 and 5.20.2
	AM-9-1	Refer to this specification, section 5.20.2
	AM-9-2	Refer to this specification, section 5.20.2

Table 1: BCAST functions, Interfaces and Specifications

In addition to specific functions, the BCAST Enabler defines such horizontal, or universal, features as support for Mobility, Roaming and Charging. These aspects are in the scope of this specification.

5.1 Service Provisioning

BCAST Terminal SHALL support Service Provisioning messages if it supports the interaction channel and if it supports service and/or content protection as defined in [BCAST11-ServContProt]. This section specifies the messages used in Service Provisioning function over interface SPR-7, between Broadcast Service Provisioning Client (BSP-C) in the Terminal and Broadcast Service Provisioning Management (BSP-M) in the BSM. The Service Provisioning function supports the following operations:

- Requesting pricing information related to PurchaseItem declared in Service Guide
- Requesting / subscribing to service related to a PurchaseItem
- Renewing LTKMs related to already requested PurchaseItem
- Requesting /subscribing to a service that was already purchased (e.g. via out of band means)
- Cancelling a subscription related to already requested PurchaseItem
- Requesting a token or LTKM

- Inquiring the status of an account
- Subscription and unsubscription to user-specific notifications
- Pause or resume the subscription period
- Requesting to generate the User Defined Bundle
- Performing a Related Contents Request

To achieve the above operations, the Service Provisioning function works with Service Guide function, Service Protection function, and Content Protection function. The linkage to Service Guide is through the use of PurchaseItem fragment which provides the identifiers (PurchaseItemID) used in the messages of Service Provisioning function. The linkage to Service and Content Protection function is through service request and subscription management messages, which requires the functionality of Service Protection Function and Content Protection Function.

The Coupon document of the TS-Services may be delivered to everyone either by file download, or may be delivered individually after a purchase transaction, via either message-based or Web-based service provisioning. The Coupon document is intended to be used as a bonus or discount towards service or content consumption, e.g. as part of a loyalty program or to entice first-time buyers, or to attract former customers back to a product or to a sales channel.

This section has two sub-sections, one for BCAST general Service Provisioning message and one for Service Provisioning message based on Smartcard profile. BCAST General Provisioning messages supports the various kinds of Service Protection Function and Content Protection Function with the sub-elements and Smartcard service provisioning message are specified for Terminal supporting Smartcard profile.

The following two tables specify under which conditions each message is mandatory or optional to support for the general Service Provisioning message and Smartcard Service Provisioning message respectively.

Message	Section	Broadcast Service Provisioning Client (BSP-C)	Broadcast Service Provisioning Management(BSP-M)
Pricing Information Request	5.1.5.1.1	OPTIONAL	OPTIONAL
Pricing Information Response	5.1.5.1.2	MANDATORY	MANDATORY
Service Request	5.1.5.2.1	MANDATORY	MANDATORY
Service Response	5.1.5.2.2	MANDATORY	MANDATORY
Service Completion	5.1.5.2.3	OPTIONAL	MANDATORY
Related Contents Request	5.1.5.9.1	OPTIONAL	OPTIONAL
Related Contents Response	5.1.5.9.2	OPTIONAL	OPTIONAL
User Defined Bundle Request	5.1.5.2.4	OPTIONAL	OPTIONAL
User Defined Bundle Response	5.1.5.2.5	OPTIONAL	OPTIONAL
Price Offering Request	5.1.5.2.6	OPTIONAL	OPTIONAL
Price Offering Response	5.1.2.2.7	OPTIONAL	OPTIONAL
LTKM Renewal Request	5.1.5.3.1	MANDATORY	MANDATORY
LTKM Renewal Response	5.1.5.3.2	MANDATORY	MANDATORY
LTKM Renewal Completion	5.1.5.3.3	OPTIONAL	MANDATORY
Unsubscribe Request	5.1.5.4.1	MANDATORY	MANDATORY
Unsubscribe Response	5.1.5.4.2	MANDATORY	MANDATORY
Token Purchase Request	5.1.5.5.1	OPTIONAL	OPTIONAL
Token Purchase Response	5.1.5.5.2	OPTIONAL	OPTIONAL
Token Purchase Completion	5.1.5.5.3	OPTIONAL	OPTIONAL
Account Inquiry Request	5.1.5.6.1	MANDATORY	MANDATORY
Account Inquiry Response	5.1.5.6.2	MANDATORY	MANDATORY

Subscription Pause Request	5.1.5.7.1	OPTIONAL	OPTIONAL
Subscription Pause Response	5.1.5.7.2	OPTIONAL	OPTIONAL
Subscription Resume Request	5.1.5.7.3	OPTIONAL	OPTIONAL
Subscription Resume Response	5.1.5.7.4	OPTIONAL	OPTIONAL
Related Contents Request	5.1.5.8.1	OPTIONAL	OPTIONAL
Related Contents Response	5.1.5.8.2	OPTIONAL	OPTIONAL

Table 2: Summary General Service Provisioning messages

Message	Section	Broadcast Service Provisioning Client (BSP-C)	Broadcast Service Provisioning Management(BSP-M)
Pricing Information Request	5.1.6.1.1	OPTIONAL	OPTIONAL
Pricing Information Response	5.1.6.1.2	MANDATORY	MANDATORY
Service Request	5.1.6.2.1	MANDATORY	MANDATORY
Service Response	5.1.6.2.1	MANDATORY	MANDATORY
LTKM Renewal Request	5.1.6.3	MANDATORY	MANDATORY
LTKM Renewal Response	5.1.6.3	MANDATORY	MANDATORY
Unsubscribe Request	5.1.6.4.1	MANDATORY	MANDATORY
Unsubscribe Response	5.1.6.4.1	MANDATORY	MANDATORY
Token Purchase Request	5.1.6.5.1	MANDATORY	MANDATORY
Token Purchase Response	5.1.6.5.1	MANDATORY	MANDATORY
Token Purchase Completion	5.1.6.5.1	OPTIONAL	OPTIONAL
Account Inquiry Request	5.1.6.6.1	MANDATORY	MANDATORY
Account Inquiry Response	5.1.6.6.2	MANDATORY	MANDATORY
Registration Procedure	5.1.6.7	MANDATORY	MANDATORY
LTKM Request Procedure	5.1.6.8	MANDATORY	MANDATORY
Deregistration Procedure	5.1.6.9	MANDATORY	MANDATORY
Subscription Pause Request	5.1.6.10.1	OPTIONAL	OPTIONAL
Subscription Pause Response	5.1.6.10.2	OPTIONAL	OPTIONAL
Subscription Resume Request	5.1.6.10.3	OPTIONAL	OPTIONAL
Subscription Resume Response	5.1.6.10.4	OPTIONAL	OPTIONAL

Table 3: Summary Smartcard Service Provisioning messages

5.1.1 Transport Protocol for Service Provisioning Messages

Service Provisioning operations are executed by exchanging the Service Provisioning messages over interface SPR-7. All the Service Provisioning messages specified in the tables in the following sections and instantiated as XML documents.

All request and reply messages defined below contain a *requestID* field which MAY be used by a terminal to map a reply message to the corresponding request message. For this purpose, the network SHALL copy the requestID from a request message into to the corresponding reply message.

The URL towards which the service provisioning messages are directed is signaled through the PurchaseChannel fragment in SG as PurchaseURL [BCAST11-SG].

5.1.1.1 Transport Protocol for General Service Provisioning Messages

The BSP-M in the BSM SHALL support HTTP POST as a delivery method to exchange Service Provisioning messages over SPR-7.

The BSP-M in the BSM MAY support HTTPS POST as a delivery method to exchange Service Provisioning messages over SPR-7, where HTTPS SHALL be based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246].

The BSP-C in the Terminal SHALL support HTTP POST and MAY support HTTPS POST as a delivery method to exchange Service Provisioning messages over SPR-7, where HTTPS SHALL be based on .SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246].

For proper operation of Service Provisioning function, the terminal needs to know the URL for HTTP or HTTPS sessions. This is supported by 'purchaseURL' element contained in the PurchaseChannel fragment of Service Guide.

5.1.1.2 Transport Protocol for Smartcard Service Provisioning Messages

Most of the messages used for the Smartcard Profile are specified in [3GPP TS 33.246]. The remaining Service Provisioning messages are specified in the tables in the following sections and are instantiated as XML documents.

For the Smartcard Profile using (U)SIM or (R-)UIM/CSIM, the BSP-M in the BSM SHALL support HTTP POST and SHALL support HTTP digest authentication as per [3GPP TS 33.246] or [3GPP2 X.S0022-A], respectively, as a delivery method to exchange Service Provisioning messages over SPR-7.

For the Smartcard Profile using (U)SIM or (R-)UIM/CSIM, the BRP-C in the Terminal SHALL support HTTP POST and SHALL support HTTP digest authentication as per [3GPP TS 33.246] or [3GPP2 X.S0022-A], respectively.

For proper operation of Service Provisioning function, the terminal needs to know the URL for HTTP sessions. This is enabled by the 'PurchaseURL' element contained in the PurchaseChannel fragment of the Service Guide.

5.1.2 HTTP Binding

5.1.2.1 HTTP Binding for General Service Provisioning Message

Request messages are sent as HTTP content of type "application/vnd.oma.bcast.sprov+xml". Responses are always sent as part of the "200 OK" response to the original request. The content type is "application/vnd.oma.bcast.sprov+xml"

5.1.2.2 HTTP Binding for Smartcard Service Provisioning Messages

HTTP Binding rule specified in [3GPP TS 33.246] SHALL be applied. If error is occurred on the procedure, HTTP response message SHALL have the error code defined in [3GPP TS 33.246]. If General Provisioning Messages are used, the same HTTP binding rule defined in the previous section will be applied.

5.1.3 Authentication

5.1.3.1 Message Authentication for General Service Provisioning Messages

For the general Service Provisioning messages, message authentication SHALL be provided using HTTPS that SHALL be based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246].

5.1.3.2 Subscriber Authentication for Smartcard Profile Service Provisioning Messages

Subscriber authentication for the Smartcard Profile SHALL be provided using HTTP digest as explained in [3GPP TS 33.246] or [3GPP2 X.S0022-A].

5.1.4 Use of Global Status Codes for Service Provisioning Messages

Table 4 proposes example values from Table 53 for the transaction messages that require the use of Global Status Codes. The values shown below are for informative purposes and the full range of values of Table 53 are applicable to all messages if deemed required.

TS-BCAST_Services	5.1.5.1.2 Pricing Information Response	000, 001, 002, 003, 007, 008, 011, 013, 015, 016, 017, 018, 019, 020, 021, 023
	5.1.5.8.2 Related Contents Response	000, 001, 002, 005, 007, 008, 011, 013, 015, 017, 018, 019, 020, 021, 022, 023
	5.1.6.2.2 Service Response	000, 001, 002, 003, 004, 005, 006, 007, 008,

	009, 011, 013, 014, 015, 016, 017, 018, 019 020, 021, 023, 031, 032, 033, 034, 035, 037, 039, 040
5.1.5.3.2 Long-Term Key Renewal Response	000, 001, 002, 004, 005, 006, 007, 008, 010, 011, 013, 015, 016, 017, 018, 019, 020, 021, 022, 023, 024,
5.1.5.4.2 Unsubscribe Response	000, 001, 002, 007, 008, 010, 011, 013, 015, 016, 017, 018, 019, 020, 021, 022, 023
5.1.5.5.2 Token Purchase Response	000, 001, 002, 004, 005, 006, 007, 008, 009, 011, 013, 015, 016, 017, 018, 019, 020, 021, 022, 023, 024, 032, 033, 034, 035, 037, 039, 040
5.1.5.6.2 Account Inquiry Response	000, 001, 002, 004, 005, 007, 008, 011, 013, 014, 015, 017, 018, 019, 020, 021, 023
5.7.2.3. Roaming Authorization Response	000, 001, 002, 003, 004, 005, 006, 007, 008, 009, 010, 011, 013, 014, 015, 016, 017, 018, 019, 020, 021, 022, 023, 024, 025, 026
5.7.2.5 RoamingServiceResponse	000, 001, 002, 003, 004, 005, 006, 007, 008, 009, 010, 011, 013, 014, 015, 016, 017, 018, 019, 020, 021, 022, 023, 024, 025, 026

Table 4: Cross Reference Table (Informative)

5.1.5 General Service Provisioning Messages

This section specifies the General Service Provisioning Messages. As described, many of the messages in this category support the Service Provisioning function of both the Smartcard Profile and DRM Profile BCAST Terminals, whereas others specifically pertain to Service Provisioning for DRM Profile terminals. The XML schema for these messages is defined in [BCAST11-XMLSchema-orderqueries].

5.1.5.1 Pricing Information Inquiry Messages

This message is sent by the terminal to the BSM to request the pricing information of a particular purchase item or items. It is used in the following situations:

- the Service Guide announces Purchase Data elements associated with the Purchase Item, but does not announce any price for some or all of them, or
- the user wishes to discover whether a different price or additional purchase options are available for his or her subscriber ID.

The response message returns information about the price and subscription options for each purchase item, and optionally the full Service Guide fragments that describe them.

In the case of the (U)SIM Smartcard Profile, the terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

5.1.5.1.1 Pricing Information Request

Name	Type	Category	Cardinality	Description	Data Type
PricingInfo Request	E			Pricing Information Request Message. Contains the following attributes: requestID Contains the following elements:	

				UserID DeviceID PurchaseItem BroadcastRoamingSpecificPart	
requestID	A	O	0..1	Identifier for the Price Information request message.	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 of [BCAST11-ServContProt]. Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile, this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile SHALL NOT allow the user to modify the DeviceID. Contains the following attributes: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 — reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C.S0072-O] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
Purchase Item	E1	M	1..N	Identifier of the Purchase Item for which the user wants to know the price. Contains the following attribute: globalIDRef	
globalIDRef	A	M	1	The ID of the Purchase Item. A purchase item is identified by the GlobalPurchaseItemID found in the PurchaseItem fragment.	anyURI
PurchaseDataReference	E2	O	0..N	Identifier the PurchaseData fragments for which the user wishes to know the price. If this	

				element is omitted, the user is asking for the price of all the Purchase Data fragments associated with the Purchase Item, and available to the particular user.	
idRef	A	M	1	Identification of the 'PurchaseData' fragment in question.	anyURI
BroadcastRoamingSpecificPart	E1	O	0..1	This element provides information to help processing the Service Request in case of roaming. For rules on how to use this element, see section 5.7.3. If the BSM support Broadcast Roaming, it SHALL support this element. If the Terminal support Broadcast Roaming, it SHALL support this element. Contains the following elements: HomeBSM VisitedBSM	
HomeBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Visited BSM, this element indicates the Home BSM of the terminal in the context of this request.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Home BSM, this element indicates the Visited BSM from which the user wishes to purchase service.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]

Table 5: Structure of Pricing Information Request in General Service Provisioning Message

5.1.5.1.2 Pricing Information Response

If the price information request is accepted by BSM, then the message from BSM contains following data:

Name	Type	Category	Cardinality	Description	Data Type
PricingInfoResponse	E			Pricing Information Response Contains the following attributes: requestID globalStatusCode Contains the following elements: PurchaseItem	
requestID	A	O	0..1	Identifier for the corresponding Pricing Information request message or Service Request	unsignedInt

				message.	
global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in the section 5.11. ▪ If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. ▪ If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. ▪ If this attribute is not present, there was an error concerning one or more 'PurchaseItem' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'PurchaseItem'.	unsignedByte
PurchaseItem	E1	M	0..N	Describes the purchase-related information of a purchase item requested in the related PricingInfoRequest message or ServiceRequest message. It is possible to provide one or more prices of a purchase item by currency. This element SHALL not be instantiated in case the 'globalStatusCode' attribute is present and set to a value different from '0'. In any other case, it SHALL be instantiated. In case the child 'itemwiseStatusCode' indicates success, or the 'globalStatusCode' is present and set to '0', at least one of 'PurchaseDataReference' or 'PurchaseDataFragment' element SHALL be instantiated. Note that it is permitted to include instances of both 'PurchaseDataReference' and 'PurchaseDataFragment' elements into the same response. Contains the following attribute: globalIDRef itemwiseStatusCode Contains the following element: PurchaseDataReference PurchaseDataFragment	
globalIDRef	A	M	1	Identifier of the Purchase Item for which a price was requested. A purchase item is identified by the GlobalPurchaseItemID found in the PurchaseItem fragment.	anyURI
itemwise Status	A	M	0..1	Specifies a status code of each PurchaseItems using GlobalStatusCode defined in the section	unsignedByt

Code				5.11.	e
PurchaseData Reference	E2	O	0..N	Describes the purchase-related options available for this user. Contains the following attribute: idRef Contains the following elements: Price SubscriptionPeriod SubscriptionType TermsOfUse	
idRef	A	M	1	Identifier of this Purchase Data, to be used by the terminal when referencing to the purchase data in a subsequent Service Request message.	anyURI
Price	E3	M	1..N	Price information of purchase item that a user wants to know. This element takes precedence over the 'MonetaryPrice' element of the referenced PurchaseData fragment. Contains the following attributes: validTo currency	decimal
validTo	A	O	0..1	The last moment when this price information is valid. If not given, the validity is assumed to end in undefined time in the future. This field expressed as the first 32bits integer part of NTP time stamps. The validity indicated by this attribute SHALL be equal to or be within the range of the fragment validity of the associated 'PurchaseData' fragment.	unsignedInt
currency	A	M	1	Specifies the currency codes defined in ISO 4217 international currency codes.	string
SubscriptionPeriod	E3	O	0..1	Specifies the subscription period for the option represented by this PurchaseData. If the Purchase Item represents a bundle of services, the SubscriptionPeriod SHALL be returned. Otherwise it MAY be omitted. This element takes precedence over the 'SubscriptionPeriod' element of the referenced PurchaseData fragment. Contains the following attributes: startTime	duration
startTime	A	O	0..1	Attribute 'startTime' gives the point of time of the beginning of the 'SubscriptionPeriod'. This field contains the 32bits integer part of an NTP time stamp.	unsignedInt
SubscriptionType	E3	M	1	The type of subscription offered as defined in section 5.1.2.7 of [BCAST11-SG].	unsignedByte

				Allowed values are: 0 – one-time subscription 1 – open-ended subscription 2 – free trial subscription 3 – (not applicable) 4 – 127 Reserved for future use 128-255 Reserved for proprietary use The Token-based modes defined in the PurchaseData fragment SHALL NOT be signalled here.	
TermsOfUse	E3	O	0..N	Element that declares there are Terms of Use associated with the 'PurchaseData' fragment and parent 'PurchaseItem' this 'Pricing Information Response' relates to. Contains the textual presentation of Terms of Use or a reference to Terms of Use representation through 'PreviewData', and information whether user consent is required for the Terms of Use. Multiple occurrences of 'TermsOfUse' are allowed within this message, but for any two such occurrences values for elements "Country" and "Language" SHALL NOT be same at the same time. Contains the following attributes: type id userConsentRequired Contains the following sub-elements: Country Language PreviewDataIDRef TermsOfUseText	
type	A	M	1	The way the terminal SHALL interpret the Terms of Use: 0 – Display before purchasing or subscribing. If 'TermsOfUse' element of type '0' is present, terminal SHALL render the Terms of Use prior to initiating purchase or subscription request related PurchaseItem associated with this message. 1 – Not used. 2 - 127 reserved for future use 128 -255 reserved for proprietary use	unsignedByte
id	A	M	1	The URI uniquely identifying the Terms of Use.	anyURI
userConsentRequired	A	M	1	Signals whether user consent for these Terms of Use is needed.	boolean

				true: User consent is required for these Terms of Use and needs to be confirmed in the subscription / purchase request message related to the PurchaseItem associated with this message. false: User consent is not required for the Terms of Use.	
Country	E4	O	0..N	List of countries for which the Terms of Use is applicable if consuming the service in that country. Each value is a Mobile Country Code according to [ITU-MCC]. If this element is omitted, the Terms of Use are applicable to any country.	string of three digits
Language	E4	M	1	Language in which the Terms of Use is given. Value is a three character string according to ISO 639-2 alpha standard for language codes.	string
PreviewDataIDRef	E4	O	0..1	Reference to the PreviewData fragment which carries the representation of legal text. If this element is not present, the 'TermsOfUseText' element SHALL be present (Implementation in XML schema using <choice>).	anyURI
TermsOfUseText	E4	O	0..1	Terms of Use text to be rendered. If this element is not present, the 'PreviewDataIDRef' element SHALL be present (Implementation in XML schema using <choice>).	string
PurchaseDataFragment	E2	O	0..N	This element holds PurchaseData fragments in the format specified in [BCAST11-SG] This element SHALL NOT be used to provide a PurchaseData fragment that does not relate to a purchase item requested by the user	Complex Type

Table 6: Structure of Pricing Information Response in General Service Provisioning Message

5.1.5.2 Service Request Message

This message is sent by the terminal to the BSM to request the subscription to, or purchase of, the associated purchase item(s), and is applicable to both the DRM Profile and Smartcard Profile. This message is used strictly for the subscription/purchase of purchase item(s) which is(are) not associated with token-based payment. The Smartcard Profile also uses this message to submit a request for a SEK/PEK associated with a specific Key Validity period (range of STKM Time Stamp values), when the SEK/PEK required to enable play-back of protected recording is not available on the Smartcard (see Section 6.9.1 of [BCAST11-ServContProt]).

In the case of the (U)SIM Smartcard Profile, the terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

5.1.5.2.1 Service Request

This message is sent by the terminal to the BSM to request the subscription to, or purchase of, the associated purchase item.

If the price is specified in the request message and it differs from the price calculated by the BSM for one or more of the purchase items included in the request, the BSM SHALL respond with Pricing Information Response message (5.1.5.1.2).

Also, if the price is not specified for one or more of the purchase items in the request message, the BSM SHALL respond with Pricing Information Response message (5.1.5.1.2). Otherwise, the BSM SHALL respond with Service Response message (5.1.5.2.2).

In a similar fashion, in case the ServiceRequest message does not contain an instance of the 'UserConsentAnswer' element for a 'PurchaseItem' element, while it is expected that the user agrees to terms of use at the time of subscription for the said 'PurchaseItem', the BSM MAY respond with a PricingInformationResponse message that contains the 'TermsOfUse' element for the PurchaseItem(s) requiring it, or return the error code '31' in the itemwiseStatusCode indicating that BSM rejected the subscription because the user did not agree to the terms of use. In the latter case the terminal MAY issue a PrincingInformationRequest to obtain the terms of use.

In case the BSM answers a Service Request with a Pricing Information Response, the latter SHALL list at least all those purchase items requested in the related Service Request for which subscription-related information (e.g. pricing, terms of use, subscription type) is absent or incorrect. The terminal SHALL consider it has accurate subscription-related information for those purchase items provided in the Service Request but not present in the Princing Information Response.

Name	Type	Category	Cardinality	Description	Data Type
ServiceRequest	E			Service Request Message to subscribe or purchase PurchaseItem Contains the following attributes: requestID Contains the following elements: UserID DeviceID ServiceEncryptionProtocol PurchaseItem DrmProfileSpecificPart BroadcastRoamingSpecificPart ParentalControl The Service Request message MAY contain an instance of the DrmProfileSpecificPart element.	
requestID	A	O	0..1	Identifier for the Service request message.	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN	unsignedByte

				5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile. SHALL NOT allow the user to modify the DeviceID. Contains the following attributes: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
ServiceEncryptionProtocol	E1	O	0..N	Lists each service encryption protocol supported by the device, including the mandatory ones. Defined values: “ipsec”, “srtp”, and “ISMACryp”. The device is allowed to include more identifiers, however depending on the protocols supported by the network they may be ignored. Note: This element is only included in the message if a service is to be delivered over Interaction channel.	string
Purchase Item	E1	M	1..N	Contains the list and price of items the user wants to order and the list of services the user wants to subscribe notification. Contains the following attributes: globalIDRef Contains the following elements: PurchaseDataReference UserConsentAnswer Service CouponID Coupon	
globalIDRef	A	M	1	The identifier of the Purchase Item. The Purchase Item identifier is advertised in the PurchaseItem fragment of the Service Guide as GlobalPurchaseItemID and is inserted in this message in the same format.	anyURI
PurchaseDataReference	E2	O	0..1	Contains the price information. This specifies the PurchaseData fragment in the Service Guide which is to be used for this subscription. Contains the following attribute idRef Contains the following Element: Price	

idRef	A	M	1	References the identifiers of PurchaseData Fragment advertised in Service Guide.	anyURI
Price	E3	O	0..1	The price of the Purchase Item known to the user from Service Guide. If PurchaseData in the Service Guide contains multiple price entries by currency, this element should be specified to indicate to the BSM the entry desired by the user. Contains the following attribute: currency	decimal
currency	A	O	0..1	Specifies the currency codes defined in ISO 4217 international currency codes.	string
UserConsentAnswer	E2	O	0..1	Signals whether user agreed to the Terms of Use as represented by id of the related TermsOfUse element. true: User agrees the terms of the Terms of Use. false: User disagrees the terms of the Terms of Use. If this element is not present the interpretation is that the user has not read or understood the Terms of Use. Contains the following attribute: id	boolean
id	A	M	1	The URI uniquely identifying the Terms of Use this 'UserConsentAnswer' relates to, which is declared either in a PurchaseData fragment, or a PurchaseChannel fragment. Said otherwise, the 'UserConsentAnswer' parent element relates to Terms of Use applicable to a PurchaseData-PurchaseItem pair.	anyURI
Service	E2	O	0..N	Reference of the Service. This element is only used for subscribing service-specific Notification. As of this version of the specification, it is assumed that service-specific Notifications delivered over the Broadcast Channel do not require subscription as they are sent in the clear. Hence, this element only applies for subscription to service-specific Notification delivered over the Interaction Channel. Contains the following attributes: globalIDRef notification Note: This element is only used for the purpose of subscribing to service-specific Notification. In addition, this element should not be confused with the MBMS User Service ID (the latter is the equivalent MBMS designation for the concatenation of the attributes 'PurchaseItemID.@gobalIDRef' and 'PurchaseData.@idRef' in BCAST.	

globalIDRef	A	M	1	Unique ID of the Service, as represented by the GlobalServiceID of the 'Service' fragment. It is used to identify the Service to which the service-specific Notification relates..	anyURI
notification	A	M	1	This attribute declares whether subscription to receive service-specific Notification message over the Interaction Channel is required. If set to "true", the terminal wishes to subscribe to delivery of the service-specific Notification over the Interaction Channel. If set to "false", the terminal does not wish to subscribe to delivery of service-specific Notification over Interaction Channel.	boolean
CouponID	E2	O	0..N	Zero or more Coupon ID's referencing valid Coupon documents (see Section 5.22) to reduce the cost of the PurchaseItem.	anyURI
Coupon	E2	O	0..N	Zero or more Coupon documents (see Section 5.22) to reduce the cost of the PurchaseItem.	Coupon
DrmProfile SpecificPart	E1	O	0..1	Service & Content Protection DRM-profile specific part. This part is MANDATORY to support for the DRM Profile, and is not applicable to the Smartcard Profile. Contains the following attributes: rightsIssuerURI Contains the following element: BroadcastMode	
rightsIssuer URI	A	O	0..1	ID of the rights issuer associated with the BSM.	anyURI
Broadcast Mode	E2	O	0..1	Indicates whether or not the device supports the optional broadcast mode of operation for rights acquisition, in addition to the interactive mode of operation.	boolean
BroadcastR oamingSpec ificPart	E1	O	0..1	This element provides information to help processing the Service Request in case of roaming. For rules on how to use this element, see section 5.7.3. If the BSM support Broadcast Roaming, it SHALL support this element. If the Terminal support Broadcast Roaming, it SHALL support this element.	
HomeBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Visited BSM, this element indicates the Home BSM of the terminal in the context of this request.	complexTyp e as defined for 'BSMFilter Code' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Home BSM, this element indicates the Visited BSM from which the user	complexTyp e as defined for 'BSMFilter

				wishes to purchase service.	Code' in section 5.4.1.5.2 of [BCAST11-SG]
ParentalControl	E1	O	0..1	This element contains information used for enforcement of Parental Control for Service Ordering. Contains the following elements: ParentalControlPinCode MAC Only one of the above two elements SHALL be instantiated at the same time. Implementation in XML schema using <choice>.	
ParentalControlPinCode	E2	O	0..1	The string representation of the PINCODE used during the PINCODE verification phase in the BSM when enforcing Parental Control for Service Ordering. As an example, a parental control PINCODE equal to 020579 is encoded as "020579". The PINCODE provided in this element applies to all the purchase items included in the service request. For information on how to use this element, see section 5.1.10.	string
MAC	E2	O	0..1	Message Authentication Code computes by the Smartcard on the client side in case a parental protection is applied to the service provisioning message. This MAC is used by the BSM to verify that the service request message has been controlled by the parental control service provisioning function on the client side. This MAC is present in the service request following a service response containing a Challenge for the same RequestID.. The MAC is coded in 32 bytes. For information on how to use this element, see section 5.1.10.1.	string

Table 7: Structure of Service Request in General Service Provisioning Message

5.1.5.2.2 Service Response

This message is sent to the terminal from the BSM in response to the request for subscription to the Service Request message. This message is applicable to both the DRM Profile and Smartcard Profile.

Name	Type	Category	Cardinality	Description	Data Type
ServiceResponse	E			Service Response Message	

				Contains the following attributes: requestID globalStatusCode adaptationMode KeyMaterialAvailableFrom Contains the following elements: PurchaseItem DrmProfileSpecificPart SmartcardProfileSpecificPart BonusCoupon	
requestID	A	O	0..1	Identifier for the corresponding Service request message.	unsignedInt
global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11. This attribute also governs the way the 'itemwiseStatusCode' attribute is instantiated in this response: If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is not present, there was an error concerning one or more 'PurchaseItem' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'PurchaseItem'.	unsignedByte
adaptation Mode	A	O	0..1	Informs the terminal of the operational adaptation mode: Generic or BDS-specific adaptation false – indicates Generic adaptation mode true – indicates BDS-specific adaptation mode Note: this attribute SHALL be present only if the 'globalStatusCode' indicates "Success", and the underlying BDS is BCMCS.	boolean
KeyMaterialAvailableFrom	A	O	0..1	The first moment in time when the terminal can start to acquire key material for the purchased service. This attribute shall be instantiated if the key material is not available for the terminal immediately after service provisioning. For the smartcard profile this attribute specifies the time when the terminal can register to network according to section 5.1.6.7 to receive the key material if the network has not delivered the keys earlier. For the DRM profile this is the time when the included 'roapTrigger' element becomes valid and can be used to initiate Long-Term Key	unsignedInt

				Message acquisition. This field contains the 32bits integer part of an NTP time stamp.	
PurchaseItem	E1	M	0..N	Describes the results of the request message of subscribing to or purchasing the PurchaseItem. For the DRM Profile, if subscription or purchase is successful, rightsValidityEndTime of PurchaseItem will be present. For either the DRM Profile or Smartcard Profile, in the case of subscription/purchase failure, itemwiseStatusCode MAY be present to indicate the reason why the request is not accepted by BSM. This element SHALL NOT be instantiated in case the 'globalStatusCode' attribute is present and set to a value different from '0'. In any other condition of the 'globalStatusCode' attribute, it SHALL be instantiated. Contains the following attributes: globalDRef itemwiseStatusCode Contains the following element: SubscriptionWindow	
globalIDRef	A	M	1	The ID of the Purchase Item. A purchase item is identified by the GlobalPurchaseItemID found in the PurchaseItem fragment.	anyURI
itemwiseStatusCode	A	M	0..1	Specifies a status code of each PurchaseItems using GlobalStatusCode defined in the section 5.11.	unsignedByte
SubscriptionWindow	E2	O	0..1	The time interval during which the subscription is valid. The network SHOULD include this element for time-based subscriptions and MAY include it for pay-per-view. The terminal MAY use this information to determine the validity period of a subscription. Contains the following attributes: startTime endTime	
startTime	A	M	1	NTP timestamp expressing the start of subscription.	unsignedInt
endTime	A	O	0..1	NTP timestamp expressing the end of subscription. This attribute SHALL NOT be present for open-ended subscriptions.	unsignedInt
DrmProfileSpecificPart	E1	O	0..1	Service & Content Protection DRM-profile specific part. This part is MANDATORY to support for the DRM Profile, and is not applicable to the Smartcard Profile. This element SHALL NOT be instantiated in case the 'globalStatusCode' attribute is present	

				and set to a value different from '0'. In any other case, it MAY be instantiated. Contains the following attributes: rightsValidityEndTime Contains the following elements: roap Trigger	
rights Validity EndTime	A	O	0..1	The last time and date of validity of the Long-Term Key Message, after which it has to be renewed. This attribute will be present when BSM accept the request message. This field is expressed as the first 32bits integer part of NTP time stamps. Note: this element is validated if RO is broadcasted. Otherwise, this element is not necessary.	unsignedInt
roap Trigger	E2	O	0..1	ROAP RO Acquisition Trigger**. The device is expected to use the trigger to initiate one or more Long-Term Key Message acquisitions.	reference to "roapTrigger" element as defined in OMA DRM 2.0 XML namespace
SmartcardProfileSpecificPart	E1	O	0..1	Service & Content Protection Smartcard-profile specific part. This part is MANDATORY to support for the Smartcard Profile, and is not applicable to the DRM Profile. Contains the following elements: LTKM Challenge	
LTKM	E2	O	0..N	Smartcard profile BCAST LTKM (base64-encoded MIKEY message). This element MAY be present - if the terminal and the BSM have agreed on "HTTP" as a LTKM delivery mechanism during the registration procedure (see section 5.1.6.10), and the BSM wishes to deliver LTKM to the terminal at the moment the ServiceResponse is done.	base64Binary
Challenge	E2	O	0..1	This element corresponds to a challenge sent for the authentication of the user when the service ordering has been determined by the BSM to be protected. This challenge is sent to Smartcard supporting the Parental Control for Service Ordering protection (see [BCAST11-ServContProt]). This element in this case is present in the first service response of the transaction described in (section 5.1.10.1). The Challenge is coded in 32 bytes. This element SHALL only be used for the Smartcard Profile extension of Parental Control for Service Ordering as described in section 5.1.10.1.	String

				The challenge is any value of 32 bytes and is BSM implementation dependant.	
BonusCoupon	E1	O	0..N	Zero or more Coupon documents (see section 5.22) that represent unique (not given to other users) coupons for bonus services or content or tokens that result from this transaction.	Coupon

Table 8: Structure of Service Response in General Service Provisioning Message

** These (ROAP Messages) are DRM profile specific. They are defined in [DRMDRM-v2.0].

5.1.5.2.3 Service Completion (DRM Profile only)

This message MAY be sent by a terminal after it has received a Service Response Message and retrieved all LTKMs. The network SHALL reply with a HTTP 200 OK response message when this message is received.

Name	Type	Category	Cardinality	Description	Data Type
ServiceCompletion	E			Service Completion Message Message. Contains the following attribute: requestID Contains the following element: LTKMessageID	
requestID	A	O	0..1	Identifier for the corresponding Service request message.	unsignedInt
LTK MessageID	E1	M	1..N	A list containing the IDs of one or more LTKMs received by the device. This is the RO ID.	string

Table 9: Structure of Service Completion in General Service Provisioning Message

5.1.5.2.4 User Defined Bundle Request

This message is sent to the BSM from the Terminal to request a User Defined Bundle service.

Name	Type	Category	Cardinality	Description	Data Type
UDBRequest	E			User Defined Bundle Request Message to subscribe or purchase PurchaseItems, Contents, Schedules and Services per user selection. Contains the following attributes: requestID Contains the following elements: UserID DeviceID BroadcastRoamingSpecificPart UserDefinedBundle	
requestID	A	O	0..1	Identifier for the User Defined Bundle request	unsignedInt

				message.	
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile. SHALL NOT allow the user to modify the DeviceID. Contains the following attributes: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
BroadcastRoamingSpecificPart	E1	O	0..1	This element provides information to help processing the User Defined Bundle Request in case of roaming. For rules on how to use this element, see section 5.7.3. If the BSM support Broadcast Roaming, it SHALL support this element. If the Terminal support Broadcast Roaming, it SHALL support this element.	
HomeBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Visited BSM, this element indicates the Home BSM of the terminal in the context of this request.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]

VisitedBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Home BSM, this element indicates the Visited BSM from which the user wishes to purchase service.	complexType as defined for 'BSMFilter Code' in section 5.4.1.5.2 of [BCAST11-SG]
UserDefinedBundle	E1	O	0..1	List of purchase item, schedule, content and services requested to be bundled by the user Contains the following elements: UDBService UDBContent PurchaseItem UDBSchedule	
UDBService	E2	O	0..N	globalServiceID of Service to be added to User Defined Bundle Contains the following attribute: UDBnotification	anyURI
UDBnotification	A	M	1	To receive Notification Message related to the Service over Interaction Channel. If notification=true, it means Notification over Interaction Channel is subscribed. If notification=false, it means Notification over Interaction Channel should not be delivered	Boolean
UDBContent	E2	O	0..N	globalContentID of Content to be added to User Defined Bundle	anyURI
PurchaseItem	E2	O	0..N	globalPurchaseItemID of PurchaseItem to be added to User Defined Bundle	anyURI
UDBSchedule	E2	O	0..N	Identifier of Schedule Fragment to be added to User Defined Bundle	anyURI

Table 10: Structure of User Defined Bundle Request in General Service Provisioning Message

5.1.5.2.5 User Defined Bundle Response

This message is sent to the Terminal from the BSM to provide the results of a User Defined Bundle Request.

Name	Type	Category	Cardinality	Description	Data Type
UDBResponse	E			User Defined Bundle Response Message Contains the following attributes: requestID globalStatusCode Contains the following elements: UserDefinedBundle	
requestID	A	O	0..1	Identifier for the corresponding User Defined Bundle request message.	unsignedInt

global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11.	unsignedByte
UserDefinedBundle	E1	O	0..1	List of content and services requested to be bundled by the user Contains the following elements: PurchaseItemFragment PurchaseDataFragment	
PurchaseItemFragment	E2	O	0..N	Purchase Item Service guide fragments containing information for the User Defined Bundle. The fragment format is specified in [BCAST11-SG]	Complex Type
PurchaseDataFragment	E2	O	0..N	Purchase Data Service guide fragments containing information for the User Defined Bundle. The fragment format is specified in [BCAST11-SG]	Complex Type

Table 11: Structure of User Defined Bundle Response in General Service Provisioning Message

5.1.5.2.6 Price Offering Request

This message is sent to the terminal from the BSM to request confirmation of the price of the User Defined Bundle service and to request final confirmation of subscription to the User Defined Bundle service.

Name	Type	Category	Cardinality	Description	Data Type
PriceOfferingRequest	E			User Defined Bundle Price Offering Request Contains the following attributes: requestID Contains the following elements: UDBPrice SubscriptionPeriod TermsOfUse	
requestID	A	O	0..1	Identifier for the corresponding User Defined Bundle Request message.	unsignedInt
UDBPrice	E1	M	1..N	Price information the User Defined Bundle that a user has requested. Contains the following attribute: validTo currency	decimal
validTo	A	O	0..1	The last moment when this price information is valid. If not given, the validity is assumed to end in undefined time in the future. This field expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
currency	A	O	0..1	Specifies the currency codes defined in ISO 4217 international currency codes. If not given, value of price is amount of Tokens.	String
SubscriptionPeriod	E1	M	1	Specifies the subscription period for the UserDefinedBundle.	Duration
TermsOfUse	E1	O	0..1	Element that declares there are Terms of Use associated with the 'UserDefinedBundle' this	

				'PriceOfferingRequest' relates to. Contains the textual presentation of Terms of Use or a reference to Terms of Use representation through 'PreviewData', and information whether user consent is required for the Terms of Use. Multiple occurrences of 'TermsOfUse' are allowed within this message, but for any two such occurrences values for elements "Country" and "Language" SHALL NOT be same at the same time. Contains the following attributes: type id userConsentRequired Contains the following sub-elements: Country Language PreviewDataIDRef TermsOfUseText	
type	A	M	1	The way the terminal SHALL interpret the Terms of Use: 1 – Display before purchasing or subscribing. If 'TermsOfUse' element of type '1' is present, terminal SHALL render the Terms of Use prior to initiating purchase or subscription request related PurchaseItem associated with this message. 2 – Display before playout. If 'TermsOfUse' element of type '2' is present, terminal SHALL present the Terms of Use prior to playing out content or service associated this message.	unsignedByte
id	A	M	1	The URI uniquely identifying the Terms of Use.	anyURI
userConsentRequired	A	M	1	Signals whether user consent for these Terms of Use is needed. true: User consent is required for these Terms of Use and needs to be confirmed in the subscription / purchase request message related to the PurchaseItem associated with this message. false: User consent is not required for the Terms of Use.	Boolean
Country	E2	M	1..N	List of countries for which the Terms of Use is applicable. Each value is a three character string according to ISO 3166-1 alpha-3	String
Language	E2	M	1	Language in which the Terms of Use is given. Value is a three character string according to ISO 639-2 alpha standard for language codes.	String
PreviewDataIDRef	E2	O	0..N	Reference to the PreviewData fragment which	anyURI

				carries the representation of legal text. If this element is not present, the 'TermsOfUseText' SHALL be present.	
TermsOfUseText	E2	O	0..1	Terms of Use text to be rendered. If 'PreviewDataIDRef' element is present under the 'TermsOfUse' this element SHALL NOT be present.	String

Table 12: Structure of Price Offering Request in General Service Provisioning Message

5.1.5.2.7 Price Offering Response

This message is sent to the BSM from the terminal in response to the request for Price Offering Response message.

Name	Type	Category	Cardinality	Description	Data Type
PriceOfferingResponse	E			User Defined Bundle Price Offering Response Contains the following attributes: requestID subscribe userConsent	
requestID	A	O	0..1	Identifier for the corresponding User Defined Bundle Request message.	unsignedInt
subscribe	A	M	1	Signals whether user has agreed to the pricing of the User Defined Bundle by the BSM and agreed to subscribe to the service	Boolean
userConsent	A	O	0..1	Signals user consent if request in PriceOfferingRequest message.	Boolean

Table 13: Structure of Price Offering Response in General Service Provisioning Message

5.1.5.3 LTKM Renewal Messages

The following messages in this section are specific to the DRM Profile. For the Smartcard Profile, the equivalent messages and procedures pertaining to LTKM renewal are defined in Section 5.1.6.3.

5.1.5.3.1 LTKM Renewal Request (DRM Profile only)

The Long-term Key Message Renewal request message is sent if a terminal needs to renew the LTKM(s) associated to a certain Purchase Item or group of purchase items. It is only applicable to the DRM Profile.

This message can also be sent by the terminal to the BSM to request the subscription to any purchase items that the end user has already purchased (e.g. via out of band means), but has not yet received key material for. This could for example be used the first time the BCAST application is started in order to register the terminal to "free" or "default" channels.

Name	Type	Category	Cardinality	Description	Data Type
LTKMRenewalRequest	E			Long Term Key Message Renewal Request Message Contains the following attributes: requestID	

				Contains the following elements: UserID DeviceID PurchaseItem	
requestID	A	O	0..1	Identifier for the LTKM renewal request message.	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile, this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile SHALL NOT allow the user to modify the DeviceID Contains the following attributes: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
Purchase Item	E1	M	1..N	A list of Purchase Items that the user wants to renew. Contains the following attribute: globalIDRef If the terminal wants to request from the BSM the delivery of a list of all purchase items that the end user has already purchased, the terminal has to set the globalIDRef attribute equal to "**oma-bcast-allservices**". This could for example be used the first time the BCAST application is started in order to register the terminal to "free" or "default" channels. If the terminal wants to request from the BSM a	

				list of all those purchase items that the end user has already purchased (e.g. via out of band means), but has not yet received a ROAP trigger for, the terminal has to set the globalIDRef attribute equal to "**oma-bcast-newservices**". If either "**oma-bcast-allservices**" or "**oma-bcast-newservices**" is used, there SHALL be exactly one 'PurchaseItem element' in the request.	
globalIDRef	A	M	1	GlobalPurchaseItemID to identify this PurchaseItem, found in the PurchaseItem fragment.	anyURI

Table 14: Structure of LTKM renewal request in General Service Provisioning Message

5.1.5.3.2 LTKM Renewal Response (DRM Profile only)

Name	Type	Category	Cardinality	Description	Data Type
LTKMRenewalResponse	E			Long Term Key Message Renewal Response Message Contains the following attributes: requestID globalStatusCode Contains the following elements: PurchaseItem DrmProfileSpecificPart	
requestID	A	O	0..1	Identifier for the corresponding LTKM request message.	unsignedInt
global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11.If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is not present, the request was completed successfully but there was an error concerning one or more 'PurchaseItem' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'PurchaseItem'. In case this message is a response to an LTKMRenewalRequest with 'globalIDRef' set to "**oma-bcast-newservices**" or "**oma-bcast-allservices**", an empty result list SHALL be signalled by setting 'globalStatusCode' equal to	unsignedByte

				"010" (No Subscription) and not instantiating the 'PurchaseItem' element.	
PurchaseItem	E1	M	0..N	Describes the results of the request message of LTKM Renewal. If renewal is successful, LTKValidityEndTime of PurchaseItem will be present. If not, itemwiseStatusCode will be present to show user the reason why the request is not accepted by BSM. This element SHALL NOT be instantiated in case the 'globalStatusCode' attribute is present and set to a value different from '0'. In any other case, it SHALL be instantiated. Contains the following attributes: globalIDRef ltkValidityEndTime itemwiseStatusCode Contains the following sub-elements: SubscriptionWindow PurchaseDataReference In case the globalIDRef attribute of the PurchaseItem element has been set equal to "**oma-bcast-allservices**" in the corresponding request message, the reply message SHALL contain a list of all PurchaseItem elements which the terminal has already purchased and which it is entitled to access currently or in the future In case the globalIDRef attribute of the PurchaseItem element has been set equal to "**oma-bcast-newservices**" in the corresponding request message, the reply message SHALL contain a list of those PurchaseItem elements which the terminal has already purchased (e.g. via out of band means) and which it is entitled to access currently or in the future, but for which it has not received key material.	
globalIDRef	A	M	1	The ID of the Purchase Item to which the validity end time is related. A purchase item is identified by the GlobalPurchaseItemID found in the PurchaseItem fragment.	anyURI
ltkValidityEndTime	A	O	0..1	The last time and date of validity of the Long-Term Key Message, after which it has to be renewed again. This attribute will be present when BSM accept the request message. This field is expressed as the first 32bits integer part of NTP time stamps. Note: the information on this element can be provided in RO.	unsignedInt

itemwiseStatusCode	A	M	0..1	Specifies a status code of each PurchaseItems using GlobalStatusCode defined in the section 5.11.	unsignedByte
SubscriptionWindow	E2	O	0..1	The time interval during which the subscription is valid. The server MAY omit this element if the response is not successful. Otherwise: For time-based subscriptions, the network SHALL include this element when responding to an "**oma-bcast-allservices**" or "**oma-bcast-newservices**" request and SHOULD include it otherwise. For pay-per-view, the network MAY include this element. The terminal MAY use this information to determine the validity period of a subscription. Contains the following attributes: startTime endTime	
startTime	A	M	1	NTP timestamp expressing the start of subscription.	unsignedInt
endTime	A	O	0..1	NTP timestamp expressing the end of subscription. This attribute SHALL NOT be present for open-ended subscriptions.	unsignedInt
PurchaseDataReference	E2	O	0..1	Describes the PurchaseData associated with the subscription to the Purchase. The device MAY use this information to update its internal subscription information concerning the user. The server SHALL include this element if the response is successful, and MAY omit it if it is not. Contains the following attributes: idRef Contains the following sub-element: Price	
idRef	A	M	1	The id of the Purchase Data fragment that is being referred to.	anyURI
Price	E3	O	0..N	The price currently associated for the use to the subscription, possibly in multiple currencies. Contains the following attribute: currency	decimal
currency	A	O	0..1	Specifies the currency codes defined in ISO 4217 international currency codes. If not given, value of price is amount of Tokens.	string
DrmProfileSpecificPart	E1	O	0..1	Service & Content Protection DRM-profile specific part. This part is MANDATORY to support for the DRM Profile. Note that as this message is only applicable for the DRM profile, this element SHALL always be present for	

				successful responses (i.e. 'globalStatusCode' being equal to 0 or not instantiated). Contains the following elements: Trigger	
Trigger	E2	O	0..1	ROAP RO Acquisition Trigger**. If the LTKM renewal failed because the device was unregistered, the response MAY include a ROAP Registration Trigger**. In that case, the device is expected to use the trigger to initiate a registration and repeat the LTKM renewal once it is registered.	RoapTrigger

Table 15: Structure of LTKM renewal response in General Service Provisioning Message

** These (ROAP Messages) are DRM profile specific

5.1.5.3.3 LTKM Renewal Completion (DRM Profile Only)

This message MAY be sent by the terminal to the BSM as an acknowledgment of the terminal's receipt of the LTKM Renewal Response and subsequent retrieval of all related LTKMs. The network SHALL reply with a HTTP 200 OK response message when this message is received.

Name	Type	Category	Cardinality	Description	Data Type
LTKMRenewalCompletion	E			Long-Term Key Message Renewal Completion Message Contains the following attributes: requestID Contains the following elements: LongTermKeyID	
requestID	A	O	0..1	Identifier for the corresponding LTKM request message.	unsignedInt
LongTermKeyID	E1	M	1..N	A list containing the IDs of one or more Long-Term Key Messages received by the device.	string

Table 16: LTKM renewal completion in General Service Provisioning Message

5.1.5.4 Unsubscription Messages

These messages pertain to the request and response for cancellation of the existing subscription to the purchase item as identified by the 'globalIDRef attribute' of PurchaseItem or the notification as identified by the 'globalIDRef attribute' of Service.

Depending on the specific situation, a subscription could still be valid after this procedure has been successfully executed, for example because the user has already paid a non-refundable amount for a time span that is yet to elapse. In this case, the subscription is to be considered valid until the time indicated in the "subscribedUntil" attribute of the response.

A device supporting the DRM Profile SHALL continue to renew keys with the LTK renewal procedure while the subscription is still valid, even if the user has unsubscribed.

When the device unsubscribing supports the smartcard profile, some additional actions need to occur upon successful completion of the unsubscribe procedure. The BSM MAY also invalidate SEKs associated with the relevant purchase ID on the unsubscribing device which are not used by any other purchase items to which the device is subscribed. The BSM invalidates SEKs/PEKs by sending an LTKM with invalid Key Validity data, i.e. the lower bound is greater than the upper bound, where the bounds define the allowed range of either TEK IDs or TimeStamp values.

In the case of the (U)SIM Smartcard Profile, the terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

5.1.5.4.1 Unsubscribe Request

Name	Type	Category	Cardinality	Description	Data Type
UnsubscribeRequest	E			Unsubscribe Request Message Contains the following attributes: requestID keepSubscription Contains the following elements: UserID DeviceID PurchaseItem	
requestID	A	O	0..1	Identifier for the Unsubscribe request message.	unsignedInt
keepSubscription	A	O	0..1	This element declares whether this UnsubscribeRequest message requests un-subscription from both the PurchaseItem and related service-specific Notification delivered over the Interaction Channel, or only the latter. When the user wants to unsubscribe from service-specific Notifications delivered over the Interaction Channel but keep the subscription to PurchaseItem, this attribute SHALL be set to "true". If this attribute is not present or holds value "false", it means both PurchaseItem and its relevant notification are requested for un-subscription.	boolean
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6. Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile this element SHALL be included if the device supports IMEI	string

				or MEID. A device supporting the DRM profile SHALL NOT allow the user to modify the DeviceID. Note: If a user has multiple devices, then this element indicates a device or a group of devices that the user wants to unsubscribe. Contains the following attribute: type	
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
Purchase Item	E1	M	1..N	Specifies identifier of the Purchase Item the user wants to unsubscribe from. Also, contains ServiceID to unsubscribe service-specific notification. Contains the following attribute: globalIDRef Contains the following element: Service	
globalIDRef	A	M	1	Identifier of PurchaseItem. GlobalPurchaseItemID found in the PurchaseItem fragment will be used. In BCAST 1.1, the single parameter "oma-bcast-allservices" can be used to indicate that the user wants to unsubscribe all the purchaseitems which have been subscribed.	anyURI
Service	E2	O	0..N	This element is only used for unsubscribing service-specific Notification. See section 5.14.4.2.1. As of this version of the specification, it is assumed that service-specific Notifications delivered over the Broadcast Channel do not require un-subscription as they are sent in the clear. Hence, this element only applies for un-subscription from service-specific Notification delivered over the Interaction Channel. Contains the following attributes: globalIDRef notification	
globalIDRef	A	M	1	GlobalServiceID of the 'Service' fragment to identifying the service to which this service-specific Notification relates.	anyURI
notification	A	M	1	This attribute declares un-subscription from delivery of the service-related Notification over the Interaction Channel is required. If set to "true", the terminal wishes to unsubscribe from delivery of service specific Notification over the	boolean

				Interaction Channel. If set "false" or is absent, it means there is no change in current status of subscription for service-specific Notification delivered over the Interaction Channel.	

Table 17: Structure of Unsubscribe Request in General Service Provisioning Message

5.1.5.4.2 Unsubscribe Response

Name	Type	Category	Cardinality	Description	Data Type
UnsubscribeResponse	E			Unsubscribe Response Message Contains the following attributes: requestID globalStatusCode Contains the following elements: PurchaseItem	
requestID	A	O	0..1	Identifier for the corresponding Unsubscribe request message.	unsignedInt
global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11. ▪ If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. ▪ If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. ▪ If this attribute is not present, there was an error concerning one or more 'PurchaseItem' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'PurchaseItem'.	unsignedByte
Purchase Item	E1	M	1..N	The ID of the Purchase Item to which the message is related. This element SHALL NOT be instantiated in case the 'globalStatusCode' attribute is present and set to a value different from '0'. In any other case, it SHALL be instantiated. Contains the following attribute: globalIDRef itemwiseStatusCode In case the globalIDRef attribute of the PurchaseItem element was set to "oma-bcast-allservices" in the corresponding Unsubscribe Request, the Unsubscribe Response message	

				SHALL contain the full list of the PurchaseItems subscribed to by the terminal at the time of Unsubscribe Request.	
globalIDRef	A	M	1	Identifier of PurchaseItem. GlobalPurchaseItemID found in the PurchaseItem fragment will be used.	anyURI
itemwiseStatusCode	A	M	0..1	Indicates the results of the Unsubscribe Request message. If Value is successful, it means relevant PurchaseItem is unsubscribed. GlobalStatusCode specified in section 5.11 will be used for this code.	UnsignedByte
subscribedUntil	A	O	0..1	The date and time until which the subscription is still valid. If missing, the subscription is to be considered terminated immediately. For the DRM profile, this is the time until which the terminal SHALL continue to issue LTK renewal requests for the purchase item. For Smartcard Profile, this is the time until which the BSM SHALL continue to include the purchase item in subsequent registration responses. This field is expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
SmartcardProfileSpecificPart	E1	O	0..1	Service & Content Protection Smartcard-profile specific part. This part is MANDATORY to support for the Smartcard Profile, and is not applicable to the DRM Profile. Contains the following elements: LTKM	
LTKM	E2	O	0..N	Smartcard profile BCAST LTKM (base64-encoded MIKEY message). This element is present if the terminal and the BSM have agreed on "HTTP" as a LTKM delivery mechanism during the registration procedure (see section 5.1.6.10)	base64Binary

Table 18: Structure of Unsubscribe Response in General Service Provisioning Message

5.1.5.5 Token Purchase Request Messages

5.1.5.5.1 Token Purchase Request

This message is sent by the terminal to the BSM to request the purchase of tokens, or credits, to enable future consumption of broadcast services/content. The quantity of which is identified by the requested token amount. This message is applicable to both the DRM Profile and Smartcard Profile.

In the case of the (U)SIM Smartcard Profile, the terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

Name	Type	Category	Cardinality	Description	Data Type
TokenPurchaseRequest	E			Token Purchase Request Message Contains the following attributes:	

				requestID Contains the following elements: UserID DeviceID PermissionsIssuerURI TokensRequested BroadcastRoamingSpecificPart ParentalControl	
requestID	A	O	0..1	Identifier for the Token Purchase request message.	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attribute: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile SHALL NOT allow the user to modify the DeviceID. Contains the following attribute: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
PermissionsIssuerURI	E1	O	0..1	The identification of the Permissions Issuer depending on the Profile. For the DRM Profile, this element is MANDATORY. It identifies the Rights Issuer from which the BSM can retrieve the ROAP	anyURI

				Trigger**. For the Smartcard Profile, this element SHALL NOT be instantiated as only the BSM can grant tokens in the case of the Smartcard Profile. Contains the following attribute: type	
type	A	M	1	The type of the Permissions Issuer identified by the PermissionsIssuerURI. Allowed values are: false – DRM Profile true – Reserved for future use As of this version of the specification, this attribute SHALL be set to "false" when instantiated.	boolean
TokensRequested	E1	O	0..1	Purchase request for tokens Contains the following attributes: type amount chargingType purchaseUnitNum Contains the following elements: PurchaseItem SmartCardProfileSpecificPart	
type	A	M	1	Specifies the type of tokens requested Allowed values are: 0 - unspecified 1 – tokens for the DRM Profile 2 – service tokens for the Smartcard Profile, added to the live_ppt_purse of the specified SEK/PEK key group 3 – service tokens for the Smartcard Profile, to the playback_ppt_purse of the specified SEK/PEK key group 4 – user tokens for the Smartcard Profile added to the user purse associated to the BSM ID 5 - 127 reserved for future use 128-255 reserved for proprietary use Note: type 1 tokens are applicable only to DRM Profile, whereas types 2-4 are applicable only to Smartcard Profile For a definition of user tokens and service tokens, see Sections 6.6.4.2 and 6.6.7 of [BCAST11-ServContProt].	unsignedByte
amount	A	M	1	For types 0 and 1, this value corresponds to the number of tokens requested in this Token Purchase Request message. For types 2 and 3, this value corresponds to the number of service tokens contained in a single service token-based credit package. These tokens are valid for any LTKM using service tokens associated to the given SEK/PEK key group. For type 4, this value corresponds to the	unsignedInt

				requested number of user tokens, valid for any LTKM using user tokens associated to the ID of the BSM.	
charging Type	A	O	0..1	The type of charging (pre-paid or post-paid) the user wishes to use. The BSM will verify that the requested charging type is available for this user. The following values are defined: 0 – undefined 1 – prepaid 2 – postpaid 3-127 – reserved for future use 128-255 – reserved for proprietary use If this attribute is not present, the default value is 0.	unsignedByte
purchaseUnitNum	A	O	0..1	The number of token-based credit packages requested by the terminal, where the number of tokens in one package is indicated by 'amount' attribute above. If this field is absent, then the request is for one package only (i.e. the default value is 1.) The value of the 'amount' attribute SHALL be identical to the value of 'TotalNumberCredits' element specified in the associated 'PurchaseData' fragment in the SG. Therefore the actual number of tokens requested by the terminal is 'purchaseUnitNum' times 'amount'. Note that 'PurchaseUnitNum' SHOULD be limited in accordance to the Purchase Data fragment associated with the Purchase Item of concern in the SG. For example, in the case of play-based tokens, its maximum value SHOULD equal that of the attribute 'maxReplay' under 'TotalNumberTokenCredits', assuming the attribute 'extraTokensPurchaseable' of 'CreditPackageType' has value = 1.	unsignedShort
PurchaseItem	E2	O	0..1	Identifier of the purchase item to which the type of tokens in the token purchase request corresponds, if the information comes from the Service Guide and the request relates to a PurchaseItem. This is given by the globalPurchaseItemID as defined in [BCAST11-SG]. Contains the following attributes: globalIDRef purchaseDataIDRef Contains the following element: CouponID Coupon For Smartcard profile this field MAY be present if the request is for user tokens and	

				MAY be present if the request is for service tokens. This field MAY be absent if the request is for DRM profile tokens.	
globalIDRef	A	M	1	Identifier of PurchaseItem. GlobalPurchaseItemID found in the PurchaseItem fragment will be used.	anyURI
purchaseDataIDRef	A	O	0..1	Identifies the associated 'PurchaseData' fragment to which the requested credit package belongs.	anyURI
CouponID	E3	O	0..N	Zero or more Coupon ID's referencing valid Coupon documents (see Section 5.22) to reduce the cost of the PurchaseItem.	anyURI
Coupon	E3	O	0..N	Zero or more Coupon documents (see Section 5.22) to reduce the cost of the PurchaseItem.	Coupon
SmartcardProfileSpecificPart	E2	O	0..1	Service & Content Protection Smartcard Profile specific part. This part is MANDATORY to support for the Smartcard Profile, and is not applicable to the DRM Profile. Contains the following elements: ProtectionKeyID	
ProtectionKeyID	E3	M	0..1	The 5-byte long concatenation of the Key Domain ID with the Key group part of the SEK/PEK ID, where both values are as specified in the Smartcard Profile [BCAST11-ServContProt]. The ProtectionKeyID corresponds to the SEK/PEK ID for which service tokens are requested. The element is only present when service tokens are requested AND the PurchaseItem element is absent. When user tokens are requested, 'ProtectionKeyID' SHOULD be absent, since the received user tokens in a subsequent LTKM are deposited into the user purse.	base64Binary
BroadcastRoamingSpecificPart	E1	O	0..1	This element provides information to help processing the Service Request in case of roaming. For rules on how to use this element, see section 5.7.3. If the BSM support Broadcast Roaming, it SHALL support this element. If the Terminal supports Broadcast Roaming, it SHALL support this element.	
HomeBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Visited BSM, this element indicates the Home BSM of the terminal in the context of this request.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Home BSM, this element	complexType as defined

				indicates the Visited BSM from which the user wishes to purchase service.	for 'BSMFilter Code' in section 5.4.1.5.2 of [BCAST11-SG]
ParentalControl	E1	O	0..1	This element contains information used for enforcement of Parental Control for Service Ordering. Contains the following elements: ParentalControlPinCode MAC Only one of the above two elements SHALL be instantiated at the same time. Implementation in XML schema using <choice>.	
ParentalControlPinCode	E2	O	0..1	The string representation of the PINCODE used during the PINCODE verification phase in the BSM when enforcing Parental Control for Service Ordering. As an example, a parental control PINCODE equal to 020579 is encoded as "020579". For information on how to use this element, see section 5.1.10.	string
MAC	E2	O	0..1	Message Authentication Code computes by the Smartcard on the client side in case a parental protection is applied to the service provisioning message. This MAC is used by the BSM to verify that the token purchase request message has been controlled by the parental control service provisioning function on the client side. This MAC is present in the token purchase request following a token purchase response containing a Challenge for the same RequestID.. The MAC is coded in 32 bytes. For information on how to use this element, see section 5.1.10.1.	string

Table 19: Structure of Token Purchase Request in General Service Provisioning Message

** These (ROAP Messages) are DRM profile specific

5.1.5.5.2 Token Purchase Response

This message, sent from the BSM to the terminal, represents a successful outcome, either unconditional or conditional in nature, in response to the Token Purchase Request. This message is applicable to both the DRM Profile and Smartcard Profile.

Name	Type	Category	Cardinality	Description	Data Type
TokenPurchaseResponse	E			Token Purchase Response Contains the following attributes: requestID	

				globalStatusCode Contains the following elements: TokensGranted DrmProfileSpecificPart SmartcardProfileSpecificPart BonusCoupon Note: DrmProfileSpecificPart and SmartcardProfileSpecificPart are mutually exclusive – TokenPurchaseResponse SHALL contain either the DrmProfileSpecificPart or SmartcardProfileSpecificPart.	
requestID	A	O	0..1	Identifier for the corresponding Token Purchase request message.	unsignedInt
globalStatusCode	A	M	1	The outcome of the request, according to the return codes defined in section 5.11.	unsignedByte
TokensGranted	E1	O	0..1	Granted tokens in response to the token purchase request. It contains the following attributes: type amount chargingType Note: The element TokensGranted simply represents the information on the outcome of the token purchase request. The actual token delivery is fulfilled by a LTKM.	
type	A	M	1	Specifies the type of tokens granted in the token purchase transaction. Allowed values are: 0 – reserved 1- tokens for DRM Profile 2 – service tokens for the Smartcard Profile, added to the live_ppt_purse of the specified SEK/PEK key group 3 – service tokens for the Smartcard Profile added to the playback_ppt_purse purse of the specified SEK/PEK key group 4 – user tokens for the Smartcard Profile added to the user purse associated to the BSM ID 5-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
amount	A	M	1	Specifies the number of tokens granted in the token purchase transaction. For type 0, 1, 2, 3 and 4, the value corresponds to the number of tokens granted. Note that this value is not equal to the attribute 'amount' given in the Token Purchase Request message. In the Token Purchase Response, 'amount' represents the total number of tokens sought by the terminal in the associated token purchase request, i.e. it equals the product	unsignedInt

				(amount) x (PurchaseUnitNum) in that request.	
charging Type	A	O	0..1	The type of charging to be associated with the token purchase transaction. The following values are defined: 0 – unspecified 1 – prepaid 2 – postpaid 3-127 – reserved for future use 128-255 – reserved for proprietary use If this attribute is not present, the default value is 0.	unsignedByte
DrmProfileSpecificPart	E1	O	0..1	Service & Content Protection DRM-profile specific part. This part is MANDATORY to support for the DRM Profile, and is not applicable to the Smartcard Profile.. Contains the following elements: roap Trigger	
roap Trigger	E2	O	0..1	If the token purchase succeeded, the response SHALL include a ROAP Trigger** as an additional payload. The device is expected to use the trigger to initiate one or more token acquisitions. If the token purchase failed because the device was unregistered, the response includes a ROAP Registration Trigger** as an additional payload. The device is expected to use the trigger to initiate a registration and repeat the token purchase once it is successfully registered.	reference to "roapTrigger" element as defined in OMA DRM 2.0 XML namespace
SmartcardProfileSpecificPart	E1	O	0..1	Service & Content Protection Smartcard Profile specific part. This part is MANDATORY to support for the Smartcard Profile, and is not applicable to the DRM Profile. Contains the following element: LTKM Challenge	
LTKM	E2	O	0..N	Smartcard profile BCAST LTKM (base64-encoded MIKEY message). This element is present if the terminal and the BSM have agreed on "HTTP" as a LTKM delivery mechanism during the registration procedure (see section 5.1.6.10)	base64Binary
Challenge	E2	O	0..1	This element corresponds to a challenge sent for the authentication of the user when the service ordering has been determined by the BSM to be protected. This challenge is sent to Smartcard supporting the Parental Control for Service Ordering protection (see [BCAST11-ServContProt]). This element in this case is present in the first token purchase response of the transaction described in (section 5.1.10.1). The Challenge is coded in 32 bytes. This element SHALL only be used for the	String

				Smartcard Profile extension of Parental Control for Service Ordering as described in section 5.1.10.1. The challenge is any value of 32 bytes and is BSM implementation dependant.	
BonusCoupon	E1	O	0..N	Zero or more Coupon fragments (see section 5.22) that represent unique (not given to other users) coupons for bonus services or content or tokens that result from this transaction.	Coupon

Table 20: Structure of Token Purchase Response in General Service Provisioning Message

***These (ROAP messages) are OMA DRMv2.0 specific. They are defined in [DRMDRM-v2.0]. Implementation in XML schema will be done by referenceing the "RoapTrigger element from the OMA DRM2.0 ROAP protocol schema. Other service protection mechanisms will map their own respective messages to the corresponding fields.*

5.1.5.5.3 Token Purchase Completion

Token Purchase Completion Message MAY be sent by a terminal after it receives Token Purchase Response Message.

Name	Type	Category	Cardinality	Description	Data Type
TokenPurchaseCompletion	E			Token Purchase Completion Message for terminal to send. Contains the following attributes: requestID	
requestID	A	O	0..1	Identifier for the corresponding Token Purchase request message.	unsignedInt

Table 21: Structure of Token Purchase Completion in General Service Provisioning Message

5.1.5.6 Account Inquiry Messages

Account Inquiry allows the user to request his/her account information such as active PurchaseItem list, associated PurchaseData and Billing Information. The AccountInquiry Element in the Account Inquiry Request message (5.1.5.6.1) indicates which information the user wants to receive and the response message can include billing information or a list of purchase items, possibly complemented by purchase data and the related fragments, as requested by the value of the 'type' attribute in the request message.

In the case of the (U)SIM Smartcard Profile, the terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

5.1.5.6.1 Account Inquiry Request

Name	Type	Category	Cardinality	Description	Data Type
AccountRequest	E			Account Inquiry Request message Contains the following attributes: requestID Contains the following elements: UserID DeviceID AccountInquiry	
requestID	A	O	0..1	Identifier for this request message	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, element SHALL be	string

				included if the device supports IMEI or MEID. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attributes: type	
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile SHALL NOT allow the user to modify the DeviceID. Contains the following attribute: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
AccountInquiry	E1	M	1..N	Specifies the account information which user want to receive from the BSM. Possible values are: 0 – undefined 1 – PurchaseItem list 2 – PurchaseItem list with a copy of the applicable PurchaseItem fragments 3 – Billing Information 4 – PurchaseItem and PurchaseData list 5– PurchaseItem and PurchaseData list with a copy of the applicable fragments 6 ~ 127 – Reserved for future use 128 ~ 255 – Reserved for proprietary use If value is 0, BSM SHOULD deliver the response message as either one of the message types defined above, or as defined by the BSM operator.	unsignedByte

				If value is '1', the BSM SHOULD respond with one or more instances of the 'PurchaseItem' element. There MAY be no instance of this element in the response in case there is no applicable purchase item. The 'BillingInformation', 'PurchaseItemFragment' and 'PurchaseData' elements SHALL NOT be instantiated. If value is '2', the BSM SHOULD respond as for value '1' and MAY additionally provide an instance of the 'PurchaseItemFragment' element under the 'PurchaseItem' element. The 'BillingInformation' and 'PurchaseData' elements SHALL NOT be instantiated. If value is '3', the BSM SHOULD instantiate the 'BillingInformation' element in the response. There MAY be no instance of this element in the response in case there is no applicable billing information. The 'PurchaseItem' element SHALL NOT be instantiated. If value is '4', the BSM SHOULD respond as for value '1' and additionally instantiate the 'PurchaseData' element with an 'idRef' attribute in the response. There MAY be no instance of the 'PurchaseData' element in the response in case there is no applicable purchase information. The 'BillingInformation' , 'PurchaseItemFragment' and 'PurchaseDataFragment' elements SHALL NOT be instantiated. If value is '5', the BSM SHOULD respond as for value '4' and in addition MAY provide an instance of the 'PurchaseItemFragment' element under the 'PurchaseItem' element and MAY provide an instance of the 'PurchaseDataFragment' element under the 'PurchaseData' element. The 'BillingInformation' element SHALL NOT be instantiated.	

Table 22: Structure of Account Inquiry Request in General Service Provisioning Message

5.1.5.6.2 Account Inquiry Response

Name	Type	Category	Cardinality	Description	Data Type
AccountResponse	E			Account Inquiry Response Message Contains the following attributes:	

				requestID globalStatusCode Contains the following elements: BillingInformation PurchaseItem	
requestID	A	O	0..1	Identifier for the corresponding Account Inquiry message	unsignedInt
global Status Code	A	M	1	The overall outcome of the request, according to the return codes defined in section 5.11.	unsignedByte
BillingInformation	E1	O	0..N	Describes the total billing information, possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this element.	string
PurchaseItem	E1	O	0..N	Specifies a PurchaseItem to which the user subscribed or purchased. Contains the following attributes: globalIDRef Contains the following elements: Description PurchaseItemFragment PurchaseData	
globalIDRef	A	M	1	GlobalPurchaseItemID of Purchase Item which the End user subscribed or purchased.	anyURI
Description	E2	O	0..N	Describes the subscription information such as price, period, etc., possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this element.	string
PurchaseItemFragment	E2	O	0..1	Contains the PurchaseItem Fragment related to the PurchaseItem to which the End user subscribed or purchased.	complexType as defined for 'PurchaseItem' in section 5.1.2.6 of [BCAST11-SG]
PurchaseData	E2	O	0..1	Specifies the PurchaseData fragment applicable to the PurchaseItem to which the user subscribed or purchased.	
idRef	A	M	1	Identifier of the PurchaseData fragment	anyURI
PurchaseDataFragment	E3	O	0..1	Contains a copy of the PurchaseData fragment declared by the parent 'PurchaseData' fragment.	complexType as defined for 'PurchaseData' in section 5.1.2.7 of [BCAST 10-SG]

Table 23: Structure of Account Inquiry Response in General Service Provisioning Message

5.1.5.7 Pause and Resume of Subscription Period

Pause and Resume of subscription period allows the end user to change his or her subscription period on PurchaseItems already purchased. The Request message specified in 5.1.5.7.1 and the Response message specified in 5.1.5.7.2 will be used for user to request temporary pause of subscription status. After receiving a successful response, terminal will proceed to LTK retrieval to expire LTKs so that user cannot consume any services related to paused PurchaseItems. The Request message specified in 5.1.5.7.3 and the Response message specified in 5.1.5.7.4 will be used by the user to resume subscription status and terminal will retrieve the relevant LTKs after receiving a successful response.

5.1.5.7.1 Subscription Pause Request

Name	Type	Category	Cardinality	Description	Data Type
SubscriptionPause	E			Request to pause the subscription period of user account Contains the following attributes: requestID Contains the following elements: UserID DeviceID PurchaseItem	
requestID	A	O	0..1	Identifier for this request message	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For DRM profile, in case of roaming this element SHALL be included, otherwise it MAY be included. If it is missing, the network SHALL be able to identify the user with other means. For Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. contains the following attribute: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003]	unsignedByte

				2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	
PurchaseItem	E1	M	1..N	Purchase Items the end user wants to pause his or her subscription period. If user wants to pause the subscription period on every purchased items, then 'globalIDRef' SHOULD have the value "oma-bcast-allservices". Contains the following attributes: globalIDRef Contains the following elements: PausePeriod	
globalIDRef	A	M	1	Identifier of PurcahseItem. GlobalPurchaseItemID found in the PurchaseItem fragment will be used.	anyURI
PausePeriod	E2	M	0..1	Describes the period user wants to pause his/her subscription period from startDate to endDate. Contains the following attributes: startDate endDate	
startDate	A	M	0..1	Indicates start date. If not present, startDate assumes the day this request message sent and accepted	dateTime
endDate	A	M	0..1	Indicates end date. After this date, subscription period is resumed by the terminal using the Subscription Resume Request. If not present, endDate assumes no specific day to resume.	dateTime

Table 24: Structure of Subscription Pause Request in General Service Provisioning Message

5.1.5.7.2 Subscription Pause Response

Name	Type	Category	Cardinality	Description	Data Type
SubscriptionPauseResponse	E			Response Message for SubscriptionPause Request Contains the following attributes: requestID globalStatusCode Contains the following elements: PurchaseItem	
requestID	A	O	0..1	Identifier for the corresponding SubscriptionPause request message	unsignedInt
global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11. If this attribute is present and set to value "0", the request was completed successfully.	unsignedByte

				In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is not present, there was an error concerning one or more 'PurchaseItem' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'PurchaseItem'.	
PurchaseItem	E1	M	1..N	The ID of the Purchase Item to which the message is related. Contains the following attributes: globalIDRef itemWiseStatusCode Contains the following elements: Trigger LTKM PossiblePeriod	
globalIDRef	A	M	1	Identifier of PurchaseItem. GlobalPurchaseItemID found in the PurchaseItem fragment will be used.	anyURI
itemwiseStatusCode	A	M	0..1	Specifies a status code of each PurchaseItems using GlobalStatusCode defined in the section 5.11.	unsignedByte
Trigger	E2	O	0..N	Indicates information terminal can trigger for DRM Profile update of Long term key. Note that this is the placeholder to define any information necessary for terminal to trigger.	anyType
LTKM	E2	O	0..N	LTKM to be used for disabling the keys for the paused PurchaseItem.. To be used with SmartCard Profile.	base64Binary
PossiblePeriod	E2	M	0..1	Describes the possible period user is able to pause his/her subscription period from startDate to endDate Contains the following attributes: startDate endDate	
startDate	A	M	0..1	Indicates start date. If not present, startDate assumes the day this request message sent and accepted	dateTime
endDate	A	M	0..1	Indicates end date. After this date, subscription period is resumed. If not present, endDate assumes no specific day to	dateTime

				resume.	

Table 25: Structure of Subscription Pause Response in General Service Provisioning Message

5.1.5.7.3 Subscription Resume Request

Name	Type	Category	Cardinality	Description	Data Type
SubscriptionResume	E			Request to pause the subscription period of user account Contains the following attributes: requestID Contains the following elements: UserID DeviceID PurchaseItem	
requestID	A	O	0..1	Identifier for this request message	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For DRM profile, in case of roaming this element SHALL be included, otherwise it MAY be included. If it is missing, the network SHALL be able to identify the user with other means. For Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the BSM. contains the following attribute: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
PurchaseIt	E1	M	1..N	Purchase Items the end user wants to resume his	

em				or her subscription period. If user wants to resume the subscription period on every purchased items, then 'globalIDRef' SHOULD have the value "oma-bcast-allservices". Contains the following attributes: globalIDRef	
globalIDRef	A	M	1	Identifier of PurchaseItem. GlobalPurchaseItemID found in the PurchaseItem fragment will be used.	anyURI

Table 26: Structure of Subscription Resume Request in General Service Provisioning Message

5.1.5.7.4 Subscription Resume Response

Name	Type	Category	Cardinality	Description	Data Type
SubscriptionResumeResponse	E			Response Message for SubscriptionResume Request Contains the following attributes: requestID globalStatusCode Contains the following elements: PurchaseItem	
requestID	A	O	0..1	Identifier for the corresponding SubscriptionResume request message	unsignedInt
global Status Code	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11. If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'PurchaseItem'. If this attribute is not present, there was an error concerning one or more 'PurchaseItem' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'PurchaseItem'.	unsignedByte
PurchaseItem	E1	M	1..N	Describes the results of the request message of Subscription Resume. If resume is successful, LTKValidityEndTime of PurchaseItem will be present. If not, ItemWiseStatusCode will be present to show user the reason why the request is not accepted by BSM.	

				Contains the following attributes: globalIDRef ltkValidityEndTime itemwiseStatusCode Contains the following sub-element: PurchaseDataReference Trigger LTKM	
globalIDRef	A	M	1	The ID of the Purchase Item to which the validity end time is related. A purchase item is identified by the GlobalPurchaseItemID found in the PurchaseItem fragment.	anyURI
LTKValidityEndTime	A	O	0..1	The last time and date of validity of the Long-Term Key Message, after which it has to be renewed again. This attribute will be present when BSM accept the request message. This field is expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
itemwiseStatusCode	A	O	0..1	Specifies a status code of each PurchaseItems using GlobalStatusCode defined in the section 5.11.	unsignedByte
PurchaseDataReference	E2	M	1	Describes period user can consume this PurchaseItem with the remaining money in user's account. Contains the following sub-element: Price PossiblePeriod	
Price	E3	O	0..N	The remaining money currently, possibly in multiple currencies. Contains the following attribute: currency	decimal
currency	A	O	0..1	Specifies the currency codes defined in ISO 4217 international currency codes. If not given, value of price is amount of Tokens.	string
PossiblePeriod	E2	M	0..1	Describes the remaining period user can consume after resuming subscription period Contains the following attributes: startDate endDate	
startDate	A	M	0..1	Indicates start date. If not present, startDate assumes the day this request message sent and accepted	dateTime
endDate	A	M	0..1	Indicates end date. After this date, subscription period is ended. If not present, endDate assumes no specific day to end the subscription period.	dateTime
Trigger	E2	O	0..N	Indicates information terminal can trigger for DRM Profile update of Long term key. Note	anyType

				that this is the placeholder to define any information necessary for terminal to trigger.	
LTKM	E2	O	0..N	LTKM to be used for enabling the keys for the paused PurchaseItem. To be used with SmartCard Profile	base64Binary

Table 27: Structure of Subscription Resume Response in General Service Provisioning Message

5.1.5.8 Related Contents Request Messages

Related Contents Request messages allows service provider to recommend user with contents which is related to what user is interested in. The Request message specified in 5.1.5.8.1 and the Response message specified in 5.1.5.8.2 will be used for user to request provisional Service Guide fragments for related contents.

5.1.5.8.1 Related Contents Request

This message is sent to the BSM from the Terminal to request a Related Contents service.

Name	Type	Category	Cardinality	Description	Data Type
RelatedContentsRequest	E			Related Contents Request Message to obtain Service Guide information of Contents contents related to the content the user is interested in Contains the following attributes: requestID Contains the following elements: UserID DeviceID BroadcastRoamingSpecificPart GlobalContentID	
requestID	A	O	0..1	Identifier for the Related Contents request message.	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. For the DRM profile, this element SHALL be included. For the Smartcard profile, this element SHALL be omitted, and the user identity SHALL be provided by the network with HTTP DIGEST authentication procedure defined in section 6.6 Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte

DeviceID	E1	O	0..N	A unique device identification known to the BSM. For the DRM profile this element SHALL be included if the device supports IMEI or MEID. A device supporting the DRM profile. SHALL NOT allow the user to modify the DeviceID. Contains the following attributes: type	string
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
BroadcastRoamingSpecificPart	E1	O	0..1	This element provides information to help processing the RelatedContentsRequest in case of roaming. For rules on how to use this element, see section 5.7.3. If the BSM supports Broadcast Roaming, it SHALL support this element. If the Terminal supports Broadcast Roaming, it SHALL support this element.	
HomeBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Visited BSM, this element indicates the Home BSM of the terminal in the context of this request.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSM	E2	M	0..1	In case the Service Provisioning request is issued against the Home BSM, this element indicates the Visited BSM from which the user wishes to purchase service.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
GlobalContentID	E1	M	1	Globally unique identifier of the content of interest. Terminal transmits this value to receive information regarding related contents.	anyURI

Table 28: Structure of Related Contents Request message in General Service Provisioning

5.1.5.8.2 Related Contents Response

This message is sent to the Terminal from the BSM to provide the result of Related Contents Request.

Name	Type	Category	Cardinality	Description	Data Type

RelatedContentsResponse	E			Related Contents Response Message Contains the following attributes: requestID globalStatusCode expirationTime Contains the following elements: PurchaseItem	
requestID	A	O	0..1	Identifier for the corresponding Related Contents request message.	unsignedInt
global Status Code	A	M	1	The outcome of the request, according to the return codes defined in section 5.11.	unsignedByte
expirationTime	A	M	1	Its purpose is to indicate to the terminals that this received purchaseItem fragments provided in this response is scheduled to be at least up-to-date from the current response time up to the expirationTime'value. If "expirationTime" is present, a terminal that wants to track updates of this received purchaseItem, SHOULD not renew the request before the expirationTime is reached, without further instruction. This field is expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
PurchaseItem	E1	M	0..N	Describes the purchase-related information of a purchase item related to the content requested in the RelatedContentsRequest message. It is possible to provide one or more prices of a purchase item by currency. This element SHALL not be instantiated in case the 'globalStatusCode' attribute is present and set to a value different from '0'. In any other case, it SHALL be instantiated. Note that it is permitted to include instances of both 'PurchaseDataReference' and 'PurchaseDataFragment' elements into the same response. Contains the following element: PurchaseItemFragment PurchaseDataReference PurchaseDataFragment PurchaseChannelFragment	
PurchaseItemFragment	E2	M	1	Describes the purchase-related information including reference to Service or Content fragments. This element holds a PurchaseItem fragment in the format specified in [BCAST11-SG]	Complex Type as defined in section 5.1.2.6 of

					[BCAST11-SG]
PurchaseDataReference	E2	O	0..N	Describes the purchase-related options available for this user. Contains the following attribute: idRef Contains the following elements: Price SubscriptionPeriod SubscriptionType TermsOfUse	
idRef	A	M	1	Identifier of this Purchase Data, to be used by the terminal when referencing to the purchase data in a subsequent Service Request message.	anyURI
Price	E3	M	1..N	Price information of purchase item that a user wants to know. This element takes precedence over the 'MonetaryPrice' element of the referenced PurchaseData fragment. Contains the following attributes: validTo currency	decimal
validTo	A	O	0..1	The last moment when this price information is valid. If not given, the validity is assumed to end in undefined time in the future. This field expressed as the first 32bits integer part of NTP time stamps. The validity indicated by this attribute SHALL be equal to or be within the range of the fragment validity of the associated 'PurchaseData' fragment.	unsignedInt
currency	A	M	1	Specifies the currency codes defined in ISO 4217 international currency codes.	string
SubscriptionPeriod	E3	O	0..1	Specifies the subscription period for the option represented by this PurchaseData. If the Purchase Item represents a bundle of services, the SubscriptionPeriod SHALL be returned. Otherwise it MAY be omitted. This element takes precedence over the 'SubscriptionPeriod' element of the referenced PurchaseData fragment.	duration
startTime	A	O	0..1	Attribute 'startTime' gives the point of time of the beginning of the 'SubscriptionPeriod'. This field contains the 32bits integer part of an NTP time stamp.	unsignedInt
SubscriptionType	E3	M	1	The type of subscription offered as defined in section 5.1.2.7 of [BCAST11-SG]. Allowed values are:	unsignedByte

				0 – one-time subscription 1 – open-ended subscription 2 – free trial subscription 3 – (not applicable) 4 – 127 Reserved for future use 128-255 Reserved for proprietary use The Token-based modes defined in the PurchaseData fragment SHALL NOT be signalled here.	
TermsOfUse	E3	O	0..N	Element that declares there are Terms of Use associated with the 'PurchaseData' fragment and parent 'PurchaseItem' this 'Related Contents Response' relates to. Contains the textual presentation of Terms of Use or a reference to Terms of Use representation through 'PreviewData', and information whether user consent is required for the Terms of Use. Multiple occurrences of 'TermsOfUse' are allowed within this message, but for any two such occurrences values for elements "Country" and "Language" SHALL NOT be same at the same time. Contains the following attributes: type id userConsentRequired Contains the following sub-elements: Country Language PreviewDataIDRef TermsOfUseText	
type	A	M	1	The way the terminal SHALL interpret the Terms of Use: 0 – Display before purchasing or subscribing. If 'TermsOfUse' element of type '0' is present, terminal SHALL render the Terms of Use prior to initiating purchase or subscription request related PurchaseItem associated with this message. 1 – Not used. 2 - 127 reserved for future use 128 -255 reserved for proprietary use	unsignedByte
id	A	M	1	The URI uniquely identifying the Terms of Use.	anyURI
userConsentRequired	A	M	1	Signals whether user consent for these Terms of Use is needed. true: User consent is required for these Terms of Use	boolean

				and needs to be confirmed in the subscription / purchase request message related to the PurchaseItem associated with this message. false: User consent is not required for the Terms of Use.	
Country	E4	O	0..N	List of countries for which the Terms of Use is applicable if consuming the service in that country. Each value is a Mobile Country Code according to [ITU-MCC]. If this element is omitted, the Terms of Use are applicable to any country.	string of three digits
Language	E4	M	1	Language in which the Terms of Use is given. Value is a three character string according to ISO 639-2 alpha standard for language codes.	string
PreviewDataIDRef	E4	O	0..1	Reference to the PreviewData fragment which carries the representation of legal text. If this element is not present, the 'TermsOfUseText' element SHALL be present (Implementation in XML schema using <choice>).	anyURI
TermsOfUseText	E4	O	0..1	Terms of Use text to be rendered. If this element is not present, the 'PreviewDataIDRef' element SHALL be present (Implementation in XML schema using <choice>).	string
PurchaseDataFragment	E2	O	0..N	Describes the purchase-related information including pricing information and terms of use. This element holds PurchaseData fragments in the format specified in [BCAST11-SG]	Complex Type as defined in section 5.1.2.7 of [BCAST11-SG]
PuchaseChannelFragment	E2	O	0..N	Describes the purchase-related information including purchase URI from which the Terminal can purchase content rights. This element holds PurchaseChannel fragments in the format specified in [BCAST11-SG]	Complex Type as defined in section 5.1.2.7 of [BCAST11-SG]

Table 29: Structure of Related Contentes Response message in General Service Provisioning

5.1.6 Smartcard Profile Service Provisioning Messages

This section specifies the Smartcard Service Provisioning Messages. These messages support the Service Provisioning function of BCAST Terminals with Smartcard Profile capability. The messages in Sections 5.1.6.1, 5.1.6.2 and 5.1.6.4 through 5.1.6.6 below are identical to General Service Provisioning Messages. The messages in Section 5.1.6.3 are somewhat unique as described in the corresponding section below. The messages in Sections 5.1.6.7 through 5.1.6.9 are unique to the Smartcard Profile (i.e. no counterparts for these exist in the General Service Provisioning Messages).

The XML schema for these messages is defined in [BCAST11-XMLSchema-orderqueries].

5.1.6.1 Pricing Information Inquiry Messages

5.1.6.1.1 Pricing Information Request

This message is the same as the general service provisioning message. See section 5.1.5.1.1.

5.1.6.1.2 Pricing Information Response

This message is the same as the general service provisioning message. See section 5.1.5.1.2.

5.1.6.2 Service Request Messages

Service Request and Service Response messages are the same as those specified in Section 5.1.5.2.

Although there is no Service Completion message for the Smartcard profile, the BSM can determine if the terminal has successfully received the Service Response by requesting an LTKM verification message (specified in section 6.6.6.1 of [BCAST11-ServContProt]) in at least one of the LTKMs subsequently transmitted to the terminal in the context of this Service Request procedure. The LTKM verification message(s) sent by BCAST terminal to BSM will confirm to BSM the successful reception of this Service Response.

5.1.6.3 LKTM Renewal, Response and Completion Messages

LTKMs can be explicitly renewed with a Registration Procedure (Section 5.1.6.7), the LTKM Request Procedure (Section 5.1.6.8) or implicitly renewed via MSK delivery procedure as described in [3GPP TS 33.246].

Although there is no LTKM Renewal Completion message for the Smartcard profile, the BSM can determine if the terminal has successfully received the LTKM(s) by requesting an LTKM verification message (specified in section 6.6.6.1 of [BCAST11-ServContProt]) in the LTKM(s) transmitted to the terminal in the context of this LTKM Renewal procedure. The LTKM verification message(s) sent by BCAST terminal to BSM will confirm to BSM the successful reception of the LTKM(s).

5.1.6.4 Unsubscription Messages

5.1.6.4.1 Unsubscribe Request and Response

These messages are the same as those specified in Section 5.1.5.4.

5.1.6.5 Token Messages

These messages are the same as those specified in Section 5.1.5.5.

5.1.6.6 Account Inquiry Messages

These messages are the same as the General Service Provisioning Account Inquiry messages as specified in Section 5.1.5.6.

This message is the same as the general service provisioning message. See section 5.1.5.6.2

5.1.6.7 Registration Procedure

The Registration procedure is invoked by the terminal when the BCAST Client is started or re-activated and upon re-establishing connectivity to the interactivity network after having lost coverage or in response to a BSM Solicited Pull Procedure where BM-SC Solicited Pull message is formatted according to Section 6.6.2 of [BCAST11-ServContProt].

In order to ensure proper LTKM delivery mechanism negotiation prior to LTKM delivery, the terminal SHALL besides perform a Registration procedure:

- before a terminal-initiated LTKM Request procedure, if terminal has not yet registered to the PermissionsIssuerURI of the Access fragment describing service access.

- before a Service Provisioning procedure subject to LTKM delivery (Service Request, Token Purchase, Unsubscription), if terminal has not yet registered to the PermissionsIssuerURI of the Access fragment (indirectly) associated with the purchase item.

The Registration procedure is used by the terminal to notify the BSM that it is available to receive LTKMs or parental control messages. The Registration procedure is not used in OMA BCAST to request any change in the subscription/ purchase status of the terminal. This functionality is provided by the Service Provisioning messages, e.g. Service Request.

For the (U)SIM Smartcard Profile terminal, this procedure is the MBMS User Service Registration procedure as defined by [3GPP TS 33.246], in which one single MBMS User Service ID is indicated in the Registration Request: the value is "oma-bcast-allservices". The Registration Response returned by the BSM SHALL indicate the total list of (PurchaseItem, PurchaseData) for which the terminal is authorized to receive the related LTKMs (including LTKMs to invalidate SEKs/PEKs). More specifically, the response SHALL contain one Response element per MBMS User Service ID. Each MBMS User Service ID identifies a (PurchaseItem, PurchaseData) pair, encoded as the concatenation of GlobalPurchaseItemID and PurchaseDataReference values. Items that are unsubscribed but still valid due to the presence of the "subscribedUntil" attribute in the "Unsubscribe Response" message SHALL be also included in the Registration Response. In case there are no such items available to return, there SHALL be exactly one "Response" element with "serviceID" set to the reserved identifier "oma-bcast-noservices" and "ResponseCode" set to "200 OK". In this particular registered state, the BSM SHALL NOT send LTKMs, BSM solicited pull procedure initiation messages and Parental Control messages to the terminal, but MAY send BSM solicited pull messages to trigger re-registrations.

The above procedure is not applicable in the case of the (R-)UIM/CSIM Smartcard Profile, i.e., when BCMCS is the underlying BDS.

The terminal SHALL handle the PDP context used for this procedure as specified in section 5.1.6.12.

The terminal MAY include in the registration request one RegistrationRequestExtension in order to:

- indicate the LTKM delivery mechanisms it supports starting from the time of this request. This mechanism is defined in sections 5.1.6.7.1 and 5.1.6.10.1 and 5.1.6.12.1.

- indicate the minimal intended lifetime of terminal PDP context after the completion of MBMS-based and Service Provisioning HTTP procedures. This mechanism is defined in sections 5.1.6.7.1 and 5.1.6.12.

The BSM MAY include in the registration response one RegistrationResponseExtension in order to:

- indicate the LTKM delivery mechanisms it plans to use for further messages deliveries to the terminal. This mechanism is defined in sections 5.1.6.7.2, 5.1.6.10.1 and 5.1.6.12.1.

- specify the minimal lifetime of terminal PDP context after the completion of MBMS-based and Service Provisioning HTTP procedures. This mechanism is defined in sections 5.1.6.7.2 and 5.1.6.12.

The BSM can also include in the registration response one or several RegistrationResponseServiceExtensions in order to:

- deliver the LTKMs the terminal is authorized to receive and any parental control messages. This information MAY be included. The underlying mechanism is defined in sections 5.1.6.7.2, 5.1.6.10.3 and 5.1.6.11.2.

- indicate the subscription start and end times of the PurchaseItem/PurchaseData pairs for which the terminal is authorized to receive the related LTKMs. For time-based subscriptions, this information SHALL be. For pay-per-view, this information MAY be included.

The following is an informative example illustrating the BCAST extensions (printed in boldface) possibly present in a Registration Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<mbmsSecurityRegisterResponse
    xmlns="urn:3GPP:metadata:2005:MBMS:securityRegistrationResponse"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:bcast="urn:oma:xml:bcast:pr:orderqueries:1.0">
    <Response>
        <serviceID>urn:3gpp:mbms:example:service:identification:123456789abcdef</serviceID>
```

```
        <ResponseCode>200 OK</ResponseCode>
        <bcast:RegistrationResponseServiceExtension>
            <LTKM>...</LTKM>
            <SubscriptionWindow startTime="3408134400" endTime=”3410812800”/>
        </bcast:RegistrationResponseServiceExtension version="0">
    </Response>
    <Response>
        <serviceID>urn:3gpp:mbms:example:service:identification:fedcba987654321</serviceID>
        <ResponseCode>200 OK</ResponseCode>
        <bcast:RegistrationResponseServiceExtension>
            <LTKM>...</LTKM>
            <LTKM>...</LTKM>
            <SubscriptionWindow startTime="3408134400" endTime=”3410812800”/>
        </bcast:RegistrationResponseServiceExtension>
    </Response>
   <bcast:RegistrationResponseExtension version="0">
       <LTKMDelivery>
           <Trigger>1</Trigger> <!-- indicates ‘SMS’ -->
           <Type>1</Type>      <!-- indicates ‘HTTP’ -->
       <LTKMDelivery>
       <PDPContextLifetime>0</PDPContextLifetime>
   </bcast:RegistrationResponseExtension>
</mbmsSecurityRegisterResponse>
```

5.1.6.7.1 Registration Request Extension

The Registration Request payload is an “mbmsSecurityRegister” message defined according to XML schema “urn:3GPP: metadata:2005:MBMS:securityRegistrationRequest” specified in section 11.4.1 of [3GPP TS 26.346].

To allow the inclusion of BCAST-specific information at <mbmsSecurityRegister> level of Registration Request payload, a *RegistrationRequestExtension* element is defined in the namespace “urn:oma:xml:bcast:pr:orderqueries:1.0” [BCAST11-XMLSchema-orderqueries]. When included, this element SHALL be present exactly once, as a child of <mbmsSecurityRegister> element matching the <xs:any> wildcard defined there.

The *RegistrationRequestExtension* element is structured as follows:

Name	Type	Category	Cardinality	Description	Data Type
RegistrationRequestExtension	E		0..1	Defines a container for the inclusion of BCAST-specific information at the <mbmsSecurityRegister> level of Registration Request payload defined in section 11.4.1 of [3GPP TS 26.346]. Contains the following attributes: version Contains the following elements: LTKMDelivery PDPContextLifetime	
version	A	NM/ TM	1	Version of this extension element. 0x00 identifies BCAST 1.0	unsignedByte
LTKMDelivery	E1	NO/ TO	0..1	This element lists all the LTKM and parental control message delivery mechanisms the terminal will support from this registration request till next registration request. Detailed use of this element is further specified in section 5.1.6.10.1and 5.1.6.11.1.	

				Contains the following elements: Trigger Type	
Trigger	E2	NM/TM	1..N	Specifies the trigger delivery mechanisms supported by the terminal at the time of registration request (triggers designating: messages to initiate BSM solicited pull procedure, and BSM solicited pull messages to initiate registration). Allowed values are: 0 – UDP 1 – SMS as per section 5.1.6.10.2 2 – 127 reserved for future use 128 – 255 reserved for proprietary use	unsignedByte
Type	E2	NM/ TM	1..N	Specifies the LTKM and parental control message delivery mechanisms supported by the terminal at the time of registration request. Allowed values are: 0 – UDP 1 – HTTP as per section 5.1.6.10.3 and 5.1.6.11.2 2-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
PDPContext Lifetime	E1	NO/ TO	0..1	Approximate minimal lifetime in seconds during which terminal intends to maintain its PDP context alive, after the completion of each MBMS-based procedure (registration, deregistration, LTKM request) and Service Provisioning procedure (Service Request, Token Purchase, Unsubscription), whether these procedures are initiated by terminal or triggered by BSM. Note: how the terminal can determine an appropriate PDP context lifetime value for the interaction network in use is out of the scope of this specification This number of seconds SHALL be counted starting from the approximate time of sending/reception of the last message of the HTTP procedure (Registration Response, Service Response, etc). The terminal SHOULD NOT set this number of seconds to zero, as the BSM may not support other means than UDP for the delivery of LTKMs, triggers and Parental Control messages. When the element is absent, the lifetime spans till the completion of next De-registration procedure wih this BSM. The use of this element is further specified in section 5.1.6.12.	unsignedInt

Table 30: Structure of RegistrationRequestExtension

5.1.6.7.2 Registration Response Extension

The Registration Response payload is an "mbmsSecurityRegisterResponse" message defined according to XML schema "urn:3GPP: metadata:2005:MBMS:securityRegistrationResponse" specified in section 11.7.1 of [3GPP TS 26.346].

To allow the inclusion of BCAST-specific information at <mbmsSecurityRegisterResponse> level of Registration Response payload, a *RegistrationResponseExtension* element is defined in the namespace "urn:oma:xml:bcast:pr:orderqueries:1.0" [BCAST11-XMLSchema-orderqueries]. When included, this element SHALL be present once as a child of <mbmsSecurityRegisterResponse> element matching the <xs:any> wildcard defined there.

This *RegistrationResponseExtension* element is structured as follows:

Name	Type	Category	Cardinality	Description	Data Type
RegistrationResponseExtension	E		0..1	Defines a container for the inclusion of BCAST-specific information at the <mbmsSecurityRegisterResponse> level of Registration Response payload defined in section 11.7.1 of [3GPP TS 26.346]. Contains the following attributes: version Contains the following sub-elements: LTKMDelivery ParentalControlMessage PDPContextLifetime	
version	A	NM/ TM	1	Version of this extension element. 0x00 identifies BCAST 1.0	unsignedByte
LTKMDelivery	E1	NO/ TO	0..1	This element lists all the LTKM and parental control message delivery mechanisms the BSM plans to use from this registration response (included) till next terminal registration request occurs. Detailed use of this element is further specified in section 5.1.6.10.1 and 5.1.6.12.1. Contains the following elements: Trigger Type	
Trigger	E2	NM/TM	1..N	Specifies the delivery mechanisms which the BSM intends to use to deliver triggers to the terminal till next registration request (triggers designating: messages to initiate BSM solicited pull procedure, and BSM solicited pull messages to initiate registration). Allowed values are: 0 – UDP 1 – SMS as per section 5.1.6.10.2 2 – 127 reserved for future use 128 – 255 reserved for proprietary use	unsignedByte
Type	E2	NM/ TM	1..N	Specifies the delivery mechanisms which the BSM intends to use to deliver LTKMs and parental control messages to the terminal, till next registration request. Allowed values are: 0 – UDP	unsignedByte

				1 – HTTP as per section 5.1.6.10.3 and 5.1.6.12.2 2-127 reserved for future use 128-255 reserved for proprietary use	
ParentalControlMessage	E1	NO/TO	0..1	Smartcard profile BCAST Parental control message (base64-encoded MIKEY message) as defined in section 6.6.5 of [BCAST11-ServContProt]. This element is used to deliver parental control messages via HTTP, in case the terminal and the BSM have agreed on "HTTP" as a delivery mechanism for LTKM during this registration procedure (see section 5.1.6.10) This element SHALL be supported in case HTTP delivery of LTKMs and Parental control messages is supported.	base64Binary
PDPContext Lifetime	E1	NO/ TO	0..1	Approximate minimal lifetime in seconds during which terminal SHALL maintain its PDP context alive, after the completion of each MBMS-based procedure (registration, deregistration, LTKM request) and Service Provisioning procedure (Service Request, Token Purchase, Unsubscription), whether these procedures are initiated by terminal or triggered by BSM. This number of seconds SHALL be counted starting from the approximate time of sending/reception of the last message of the HTTP procedure (Registration Response, Service Response, etc). The BSM MAY set this number of seconds to zero, when UDP bearer is not a negotiated mechanism for the delivery of LTKMs, triggers and Parental Control messages When the terminal indicates in Registration Request a PDP context lifetime in seconds greater than zero, the BSM SHOULD replicate this number of seconds in the returned <PDPContextLifetime> element. When the element is not included by the BSM, the lifetime spans till completion of De-registration with this BSM. The use of this element is further specified in section 5.1.6.12.	unsignedInt

Table 31: Structure of RegistrationResponseExtension

5.1.6.7.3 Registration Response Service Extension

The Registration Response payload is an "mbmsSecurityRegisterResponse" message defined according to XML schema "urn:3GPP: metadata:2005:MBMS:securityRegistrationResponse" specified in section 11.7.1 of [3GPP TS 26.346].

To allow the inclusion of BCAST-specific information at <Response> level of Registration Response payload (i.e. at the level corresponding to one registered PurchaseItem/PurchaseData pair), a *RegistrationResponseServiceExtension* element is defined in the namespace "urn:oma:xml:bcast:pr:orderqueries:1.0" [BCAST11-XMLSchema-orderqueries]. This element

MAY be included in each/any <Response> element in the Registration Response. When included in a <Response> element, it SHALL be present once as a child of <Response> element matching the <xs:any> wildcard defined there.

This *RegistrationResponseServiceExtension* element is defined below:

Name	Type	Category	Cardinality	Description	Data Type
RegistrationResponseServiceExtension	E		0..1	Defines a container for the inclusion of BCAST-specific information at the <Response> level of Registration Response payload defined in section 11.7.1 of [3GPP TS 26.346]. Contains the following attributes: version Contains the following elements: LTKM	
version	A	NM/ TM	1	Version of this extension element. 0x00 identifies BCAST 1.0	unsignedByte
LTKM	E1	NO/ TO	0..N	Smartcard profile BCAST LTKM (base64-encoded MIKEY message) associated with the successfully registered PurchaseItem/PurchaseData pair identified by <serviceID> element sibling of <RegistrationResponseServiceExtension> element. This element SHALL NOT be included if <ResponseCode> element sibling of <RegistrationResponseServiceExtension> does not indicate status code “200 OK”. More details on this element are further specified in section 5.1.6.10.3.	base64Binary
Subscription Window	E1	NO/TM	0..1	The time interval during which the subscription is valid, where the subscription is associated with the successfully registered PurchaseItem/PurchaseData pair identified by the <serviceID> sibling element of the <RegistrationResponseServiceExtension> element. For time-based subscriptions, the network SHALL include this element. For pay-per-view, the network MAY include this element.The terminal MAY use this information to determine the validity period of a subscription. Contains the following attributes: startTime endTime	
startTime	A	NM/TM	1	NTP timestamp expressing the start of subscription.	unsignedInt

endTime	A	NO/TM	0..1	NTP timestamp expressing the end of subscription. This attribute SHALL NOT be present for open-ended subscriptions.	unsignedInt

Table 32: Structure of RegistrationResponseServiceExtension

5.1.6.8 LTKM Request Procedure

Upon the completion of the subscription/purchase transaction (as defined by the Service Request messages in Section 5.1.5.2), or once the lifetime of the current SEK/PEK in the Smartcard has expired, the required new SEK/PEK can be obtained via the LTKM Request procedure. This can occur:

- When the BCAST Terminal has missed a SEK/PEK key update procedure, due to, for example, being out of coverage;
- In response to a BM-SC solicited pull procedure.

For the Smartcard Profile, this procedure is the MBMS MSK request procedure as defined by [3GPP TS 33.246], in which the key identification information comprises a list of one or more Key Domain ID – SEK/PEK ID pairs, subject to the following clarification. For the (U)SIM Smartcard Profile terminal, the SRK used in the HTTP digest authentication of the subscriber corresponds to the MBMS Request Key (MRK); for the (R-)UIM/CSIM Smartcard Profile terminal, the SRK is the BCMCS Authentication Key (Auth-Key).

The terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

The BSM MAY include in the LTKM response one or several LTKM ResponseMSKExtensions in order to:

- include the LTKM(s) carrying the SEK(s)/PEK(s) requested in the LTKM request. This mechanism is defined in sections 5.1.6.8.1 and 5.1.6.10.3.

5.1.6.8.1 LTKM Response MSK Extension

The LTKM Response payload is an “mbmsMSKResponse” message defined according to XML schema “urn:3GPP:metadata:2005:MBMS:mskResponse” specified in section 11.8.1 of [3GPP TS 26.346].

To allow the inclusion of BCAST-specific information at <Response> level of LTKM Response payload (i.e. at the level corresponding to one requested SEK/PEK), an *LTKMResponseMSKExtension* element is defined in the namespace “urn:oma:xml:bcast:pr:orderqueries:1.0” [BCAST11-XMLSchema-orderqueries]. This element MAY be included in each/any <Response> element in the response. When included in a <Response> element, it SHALL be present once as a child of <Response> element matching the <xs:any> wildcard defined there.

This *LTKMResponseMSKExtension* element is structured as follows:

Name	Type	Category	Cardinality	Description	Data Type
LTKMResponseMSKExtension	E		0..1	Defines a container for the inclusion of BCAST-specific information at the <mbmsMSKResponse> level of LTKM Response payload defined in section 11.8.1 of [3GPP TS 26.346]. Contains the following attributes: version Contains the following sub-elements: LTKM	
version	A	NM/	1	Version of this extension element.	unsignedByt

		TM		0x00 identifies BCAST 1.0	e
LTKM	E1	NO/ TO	0..N	Smartcard profile BCAST LTKM (base64-encoded MIKEY message) carrying the SEK/PEK identified by the <MSK> element sibling of <LTKMResponseMSKExtension> element. This element SHALL NOT be included if <ResponseCode> element sibling of <LTKMResponseMSKExtension> does not indicate status code "200 OK". More details on this element are further specified in section 5.1.6.10.3.	base64Binary

Table 33: Structure of LTKMResponseMSKExtension

5.1.6.9 Deregistration Procedure

The Deregistration procedure is invoked by the terminal upon termination or suspension of the BCAST Client, or whenever the terminal wishes to indicate that it is not anymore available to receive LTKMs.

It may happen that the terminal is unable to perform a Deregistration procedure upon termination of the BCAST Client, due to uncontrolled power down or loss of coverage of interaction channel network. In this case, the terminal SHOULD perform a Deregistration procedure on the first occasion, i.e. upon next availability of interaction channel network while BCAST Client is besides not running (since otherwise the terminal would perform a Registration procedure).

For the Smartcard Profile, this procedure is the MBMS User Service Deregistration procedure as defined by [3GPP TS 33.246], in which one single MBMS User Service ID is indicated in the Deregistration Request: the value is "oma-bcast-allservices". This procedure is not applicable in the case of the (R-)UIM/CSIM Smartcard Profile, i.e., when BCMCS is the underlying BDS.The terminal SHALL send the Deregistration request to the PermissionsIssuerURI used by the terminal to send latest Registration request with this BSM, with "requesttype" parameter set to "deregister" instead of "register". This implies in particular that a BSM SHOULD accept De-Registration requests against a particular PermissionsIssuerURI as long as there are terminals considered in registered state against that URI. It is thus possible that the terminal might not receive any response to a De-Registration request after the BSM has invalidated the PermissionsIssuerURI.

The BSM SHALL interpret the Deregistration Request as a deregistration to the total list of (Purchase Items, PurchaseData) pairs for which the terminal is authorized to receive the related LTKMs.

The BSM SHALL include in the Deregistration Response:

- Either one "Response" element, in which the MBMS User Service ID value is "oma-bcast-noservices", in the case where the terminal is not subscribed to any purchase items
- Or one "Response" element, in which the MBMS User Service ID value is "oma-bcast-allservices".
- Or one or more"Response" elements in which each MBMS User Service ID SHALL be identified by the concatenation of GlobalPurchaseItemID and PurchaseDataReference values. These response elements SHALL contain the total list of MBMS User Service IDs for which the terminal is authorized to receive the related LTKMs.

The terminal SHALL handle the PDP context used by this procedure as specified in section 5.1.6.12.

In the latter case, the BSM MAY include in the deregistration response one or several DeregistrationResponseServiceExtensions, in order to:

- deliver LTKMs corresponding to the services that the terminal has deregistered to. This mechanism is defined in sections 5.1.6.9.1 and 5.1.6.10.3. The LTKMs contained in the deregistration response MAY be used to invalidate SEKs/PEKs, e.g. by carrying invalid Key Validity Data.

5.1.6.9.1 Deregistration Response Service Extension

The Deregistration Response payload follows the format of Registration Response payload: it is an "mbmsSecurityRegisterResponse" message defined according to XML schema "urn:3GPP: metadata:2005:MBMS:securityRegistrationResponse" specified in section 11.7.1 of [3GPP TS 26.346].

To allow the inclusion of BCAST-specific information at the <Response> level of Deregistration Response payload (i.e. at the level corresponding to one deregistered service), a *DeregistrationResponseServiceExtension* element is defined in the namespace "urn:oma:xml:bcast:pr:orderqueries:1.0" [BCAST11-XMLSchema-orderqueries]. This element MAY be included in each/any <Response> element in the response. When included in a <Response> element, it SHALL be present once as a child of <Response> element matching the <xs:any> wildcard defined there.

This *DeregistrationResponseServiceExtension* element is structured as follows:

Name	Type	Category	Cardinality	Description	Data Type
DeregistrationResponseServiceExtension	E		0..1	Defines a container for the inclusion of BCAST-specific information at the <Response> level of Deregistration Response payload defined in section 11.7.1 of [3GPP TS 26.346]. Contains the following attributes: version Contains the following sub-elements: LTKM	
version	A	NM/ TM	1	Version of this extension element. 0x00 identifies BCAST 1.0	unsignedByte
LTKM	E1	NO/ TO	0..N	Smartcard profile BCAST LTKM (base64-encoded MIKEY message) associated to the service successfully deregistered to identified by <serviceID> element sibling of <DeregistrationResponseServiceExtension> element. This element SHALL NOT be included if <ResponseCode> element sibling of <DeregistrationResponseServiceExtension> does not indicate status code "200 OK". More details on this element are further specified in section 5.1.6.10.3.	base64Binary

Table 34: Structure of DeregistrationResponseServiceExtension

5.1.6.10 LTKM delivery mechanisms

The BSM can send LTKMs over UDP to the terminal following BCAST-specific service provisioning messages (Service Response, Subscription Long-Term Key Renewal Response, Token Purchase Response, Unsubscribe Response) or MBMS-based provisioning messages (Registration response, Deregistration response, LTKM response). The BSM can also push to the terminal unsolicited LTKMs over UDP, to update SEKs/PEKs. Finally, the BSM can push messages over UDP (called triggers in this section) to trigger the terminal to initiate a LTKM request procedure or a registration procedure.

The terminal as well as the BSM MUST support LTKM delivery over UDP.

There are however situations where the terminal is temporarily or permanently not reachable by UDP:

- temporarily if for instance the terminal is configured to release its PDP context shortly after an HTTP-based procedure with the BSM, including the registration procedure.

Note: this configuration must be avoided if the number of maintained PDP contexts is not an issue for the network.

- permanently if for instance the terminal is attached to a private IP network behind a NAT , or if the terminal sends the registration request via an HTTP Proxy which modifies sender's IP address.

To cope with these situations, other LTKM delivery mechanisms than UDP MAY be used, such as the inclusion of LTKMs in the HTTP response to a service provisioning request, as well as trigger delivery over SMS bearer.

Note: this version of the specification defines no tools enabling terminal or BSM to detect network configurations problematic for the reliability of trigger/LTKM delivery over UDP (e.g. NAT equipments, HTTP Proxy modifying sender's IP address, short-term PDP contexts, etc). For these problematic network configurations the following is advised:

- If UDP delivery issues are of permanent nature (e.g. NAT equipments), SMS bearer can be used for trigger delivery, and HTTP bearer for LTKM and Parental Control Message delivery.

If UDP delivery issues are only about short lifetime of PDP contexts, UDP bearer can still be used for trigger, LTKM and Parental Control Message delivery, provided that terminal and BSM are able to negotiate PDP context lifetime during Registration procedure.

5.1.6.10.1 Signaling of supported delivery mechanisms for triggers and LTKMs

The terminal SHALL indicate in the registration request the complete list of LTKM delivery mechanisms it will support starting from the time of this registration request till next registration request. This indication applies to all the LTKMs the BSM will deliver to the terminal during this period, whether these LTKMs actually carry a SEK/PEK or not (i.e. with KEMAC Encr Data Len = 0).

The terminal SHALL indicate in the registration request the complete list of trigger delivery mechanisms it will support starting from the time of this registration request till next registration request. Triggers in scope are messages initiating a BSM solicited pull procedure, and BSM solicited pull messages initiating a registration procedure.

The terminal SHALL indicate these supported delivery mechanisms by including in the registration request one <RegistrationRequestExtension> element containing one <LTKMDelivery> element, itself containing zero or more <Trigger> sub-elements to denote trigger delivery mechanisms, and one or more <Type> sub-elements to denote LTKM delivery mechanisms.

The terminal MAY however omit in the request the indication of supported delivery mechanisms, if it supports no more and no less than UDP and SMS bearers for trigger delivery, and UDP bearer for LTKM delivery.

The BSM SHALL handle this terminal indication as follows:

- For each successfully authenticated registration request it receives, the BSM SHALL determine which trigger and LTKM delivery mechanisms the terminal will support from this registration request till next registration request:
  - If <RegistrationRequestExtension> element is present and includes an <LTKMDelivery> sub-element, the BSM SHALL read terminal-supported trigger and LTKM delivery mechanisms from respectively <Trigger> and <Type> sub-elements.
  - Otherwise the BSM SHALL conclude that the terminal supports UDP and SMS bearers for trigger delivery, and UDP bearer for LTKM delivery.
- If the BSM supports one or more of the terminal-supported LTKM delivery mechanisms, the BSM SHALL include in the registration response a <RegistrationResponseExtension> element, and this element SHALL include an <LTKMDelivery> sub-element listing all the terminal-supported mechanisms which the BSM plans to use for further trigger and LTKM deliveries to this terminal, starting from this registration response.
  - The BSM MAY choose to not return an <LTKMDelivery> sub-element to implicitly signal to the terminal it only plans to use UDP bearer for trigger and LTKM delivery.
  - For this terminal, the BSM SHALL NOT later on use trigger and LTKM delivery mechanisms other than those implicitly or explicitly signaled to the terminal in the registration response.

- If the BSM supports none of the terminal-supported LTKM delivery mechanisms (regardless of supported trigger delivery mechanisms), the BSM SHALL signal this to the terminal by a "403 Forbidden" in the HTTP status line of the response.
- The BSM SHALL NOT attempt to deliver triggers or LTKMs to this terminal, from this registration response included, till next registration request.

<RegistrationRequestExtension> element and related <LTKMDelivery> sub-element are defined in section 5.1.6.7.1.

<RegistrationResponseExtension> element and related <LTKMDelivery> sub-element are defined in section 5.1.6.7.2.

5.1.6.10.2 LTKM delivery over SMS

In this version of specification, LTKM delivery over SMS designates the delivery of an LTKM initiating a BSM solicited pull procedure (specified in section 6.6.1 of [BCAST11-ServContProt]) or BSM initiated registration procedure (specified in section 6.6.2 of [BCAST11-ServContProt].

5.1.6.10.3 LTKM delivery over HTTP

The terminal MAY support LTKM delivery over HTTP as defined in this section.

In this version of specification, LTKM delivery over HTTP designates the delivery of LTKMs:

- in the Registration Response payload, by the inclusion of RegistrationResponseServiceExtension(s) and related <LTKM> sub-element(s), as defined in section 5.1.6.7.3.
- in the LTKM Response payload, by the inclusion of LTKMResponseMSKExtension(s) and related <LTKM> sub-element(s), as defined in section 5.1.6.8.1.
- in the Deregistration Response payload, by the inclusion of DeregistrationResponseServiceExtension(s) and related <LTKM> sub-element(s), as defined in section 5.1.6.9.1.
- in the Service Response payload, by the inclusion of <LTKM> elements in the Smartcard Profile specific part of the message, as defined in section 5.1.5.2.2.
- in the Unsubscribe Response payload, by the inclusion of <LTKM> elements in the Smartcard Profile specific part of the message, as defined in section 5.1.5.4.2.
- in the Token Purchase Response payload, by the inclusion of <LTKM> elements in the Smartcard Profile specific part of the message, as defined in section 5.1.5.5.2

The following applies for the delivery of LTKMs in any of these HTTP responses:

- The BSM SHALL NOT include LTKMs in unsuccessful HTTP responses.
- The BSM SHALL NOT include LTKMs initiating a BSM solicited pull procedure or BSM solicited pull messages initiating a registration procedure
- In case multiple LTKMs are carried in the same HTTP payload, the BSM SHALL insert them in order of increasing TS.

5.1.6.10.4 LTKM general processing

Unless otherwise stated, the terminal SHALL process all the LTKMs delivered by the BSM using any of the delivery mechanisms signaled by the BSM in the registration response, or using UDP if the BSM omitted this signaling in the registration response. The terminal MAY ignore LTKMs delivered by the BSM using other delivery mechanisms. Note that as the terminal signals the LTKM delivery mechanisms that it supports in the registration request, the BSM SHOULD NOT deliver LTKMs using a mechanism that is not supported by the terminal.

In case multiple LTKMs are carried in the same payload, the terminal SHALL process them one by one in order of inclusion in the payload.

For each processed LTKM respectively with V flag in HDR set or leading to the return of LTKM reporting message(s), the terminal SHALL send respectively one verification message or LTKM reporting message(s) over UDP to the BSM IP address resolved from NAF FQDN encoded in IDi payload, regardless of the method used by the BSM to deliver the LTKM.

Determination of the destination port to use is defined as follow:

- In case the LTKM is delivered over UDP, the terminal SHALL send the message to the same destination port as the destination port that was used by the BSM to deliver the LTKM.
- In case the LTKM is delivered via HTTP in the context of BCAST delivery mechanisms as specified in section 5.1.6.10.3the terminal SHALL send the message to destination port 4359

In case multiple LTKMs are carried in the same payload, the verification messages SHALL be sent one by one in order of LTKM processing.

5.1.6.11 Pause and Resume of Subscription Period

5.1.6.11.1 Subscription Pause Request

These messages are the same as those specified in Section 5.1.5.7.1.

5.1.6.11.2 Subscription Pause Response

These messages are the same as those specified in Section 5.1.5.7.2.

5.1.6.11.3 Subscription Resume Request

These messages are the same as those specified in Section 5.1.5.7.3.

5.1.6.11.4 Subscription Resume Response

These messages are the same as those specified in Section 5.1.5.7.4.

5.1.6.12 Parental control messages delivery mechanisms

Potential problems for the delivery over UDP of parental control as described in Section 5.1.6.10 are also possible; therefore, the mechanisms for the delivery of the parental control messages are identical to those defined for the delivery of LTKMs in Section 5.1.6.10.

The terminal as well as the BSM MUST support parental control message delivery over UDP. To cope with situations where the terminal is not reachable, other delivery mechanisms than UDP MAY be used, such as the inclusion of parental control message in the HTTP response.

5.1.6.12.1 Signaling of supported Parental Control Message delivery mechanisms

Signaling of supported parental control messages delivery mechanisms SHALL be done as defined for the LTKM delivery mechanisms in section 5.1.6.10.1. The signaled mechanisms for LTKM delivery according to that section SHALL also be used for the delivery of Parental control messages.

5.1.6.12.2 Parental Control Message delivery over HTTP

The terminal MAY support delivery over HTTP as defined in this section.

In this version of specification, delivery over HTTP designates the delivery of parental control messages:

- in the Registration Response payload, by the inclusion of base64-encoded Parental control messages into the RegistrationResponseExtension as defined in section 5.1.6.7.2.

The following applies for the delivery of parental control messages in any of these HTTP responses:

- The BSM SHALL NOT include parental control messages in unsuccessful HTTP responses.

5.1.6.12.3 Parental Control Message general processing

The terminal SHALL process the parental control message delivered by the BSM following processing methods defined for LTKMs in section 5.1.6.10.4

5.1.6.13 PDP context handling

The terminal needs to create or reuse a Packet Data Protocol (PDP) context [3GPP TS 23.060] to perform unicast IP communications with the BSM.

For the (U)SIM Smarcard profile, the BSM can besides make use of this PDP context to deliver messages over UDP to the terminal, such as: LTKMs, BSM solicited pull procedure initiation messages, BSM solicited pull messages and Parental Control messages. The BSM can send these messages to the terminal over UDP subsequently to an HTTP procedure, or at the initiative of the BSM (unsolicited push). This implies that the BSM must know terminal IP address, as well as validity of this IP address in the time, which can be achieved using the following rules:

- Rules on PDP context below apply to the HTTP Digest authenticated procedures performed between terminal and BSM (Registration, Deregistration, LTKM Request, Service Request, Token Purchase, Unsubscription, Pricing Information and Account Inquiry).
- When performing one of these procedures with the BSM, the terminal SHALL reuse any existing active PDP context which it has previously used to communicate with this BSM. This rule is to ensure that the BSM sees at most one valid IP address for a given registered terminal (B-TID).
- The BSM SHALL infer terminal IP address from the latest of these procedures successfully performed by the terminal with this BSM.

  Note: although Pricing Information and Account Inquiry procedures are not subject to subsequent LTKM delivery, this rule applies also to these procedures, as updating terminal IP address whenever possible reduces the likelihood for the BSM to send messages over UDP to an IP address reallocated to another terminal (case of terminal not being able to deregister before the release of its PDP context).

- The minimal lifetime of PDP context used by these procedures SHALL be negotiated at the time of each terminal registration and re-registration with the BSM (either explicitly via the inclusion of <PDPContextLifetime> element, or implicitly via the omission of this element, in Registration Request and/or Registration Response) and SHALL apply from this (Re-)registration procedure (included) till the Deregistration procedure with this BSM (included).
- For Registration, LTKM Request, Service Request, Token Purchase and Unsubscription procedures:
  - If <PDPContextLifetime> element was absent in Registration Response, the terminal SHALL NOT release the PDP context used by this procedure until completion of next Deregistration procedure or until a PDP context deactivation procedure has been initiated by the network as defined in [3GPP TS 23.060].
  - If <PDPContextLifetime> element was present in Registration Response and set to zero, the terminal MAY release the PDP context used by this procedure immediately after completion of the HTTP message flow and the delivery of any requested Parental Control verification, LTKM verification and LTKM reporting messages.
  - If <PDPContextLifetime> element was present in Registration Response and set to a number of seconds greater than zero, the terminal SHALL NOT release the PDP context used by this procedure until this number of seconds has elapsed (starting from completion of the HTTP message flow) or until completion of next Deregistration procedure, or until a PDP context deactivation procedure has been initiated by the network as defined in [3GPP TS 23.060].
- For the Deregistration procedure:
  - The terminal MAY release the PDP context used by this procedure immediately after completion of the HTTP message flow and the delivery of any requested LTKM verification and LTKM reporting messages.
- For Pricing Information or Account Inquiry procedure:

- If the PDP context used by this procedure was constrained to a specific lifetime by a previous HTTP procedure, the terminal SHALL NOT release the PDP context used by this procedure until this lifetime has expired or a PDP context deactivation procedure has been initiated by the network as defined in [3GPP TS 23.060].
- Otherwise the terminal MAY release the PDP context used by this procedure immediately after completion of the HTTP message flow.

5.1.7 Message Compression

The Service Provisioning messages MAY be compressed during the transport of the messages. In that case, the compression applies to entire Service Provisioning message which is the payload of HTTP message. If the compression is used, in the HTTP message delivering the Service Provisioning message the "Content-Encoding" attribute SHALL be present in the HTTP header and set to MIME value representing the compression scheme.

The BSP-M in the BSM SHALL support the GZIP algorithm for the delivery of Service Provisioning messages. The BSP-C in the Terminal SHALL support the GZIP algorithm for the delivery of Service Provisioning messages. In case GZIP compression is used for the delivery of Service Provisioning messages, the "Content-Encoding" attribute SHALL be set to "gzip".

5.1.8 Provisioning Trigger Message (DRM Profile only)

The message below is defined to trigger the terminal to send a provisioning message to the BSM. A Terminal and a BSM supporting the DRM profile and the Web-based Service Provisioning feature SHALL support the Provisioning Trigger Message.

The BSM SHALL use SMS to send this message to the Terminal. The SMS SHALL satisfy the following conditions:

- The SMS carries a WAP connectionless push (WDP/WSP encoding) as defined in [OMA Push].
- The WSP content type header contains the Content Type code registered by OMNA for 'application/vnd.oma.bcast.provisioningtrigger' (see Appendix I.6,) i.e. the binary value 0x031B.
- The WSP X-Wap-Application-Id header contains the binary code registered by OMNA for the PUSH Application ID identifying the BCAST Push client, as specified in section 9 of [BCAST11-Distribution].

The message SHALL be structured as follows. Note that the 'type' parameter signals the type of the message and as such determines its structure (i.e. number, semantics and size of the parameters contained).

Data Field Name	Data Type
Provisioning_Trigger_Message {	
type	uimsbf8
if(type==0) {	
LTKMRenewalRequestTrigger.idCode	uimsbf8
LTKMRenewalRequestTrigger.url	bytestring
}	
}	

Table 35: DRM Profile Trigger Message Structure

uimsbfN	Unsigned Nbit Integer, most significant bit first
bytestring	Array of bytes

Table 36: Mnemonics used in Table 35

type	Signals the type of the message. 0 – BCAST 1.0 LTKMRenewalRequest Trigger Message 1-255 – reserved for future use Terminals MAY discard messages with an unknown value in the 'type' field.
LTKMRenewalRequestTrigger.idCode	Code signalling the string to put into the 'globalIDRef' attribute 0 – "oma-bcast-allservices" 1 – "oma-bcast-newservices" 2-255 – reserved for future use
LTKMRenewalRequestTrigger.url	Signals the URL to which to send the LTKMRenewalRequest message as a null-terminated string

Table 37: Semantics for Table 35

If the terminal receives a message with the 'type' parameter equals to 0, it SHALL send an LTKMRenewalRequest to the BSM addressed by the URL signalled in the parameter 'LTKMRenewalRequestTrigger.url', containing one instance of 'PurchaseItem' with the 'globalIDRef' attribute set to the value signalled by the parameter 'LTKMRenewalRequestTrigger.idCode'. This message SHALL NOT be sent if the URL is not available to the terminal as 'purchaseURL' in any 'PurchaseChannel' fragment in the Service Guide, and is also not trusted by the terminal based on some other mechanism outside the scope of this specification.

5.1.9 Web-based Service Provisioning

A Terminal and server MAY support Service Provisioning via a web-portal. The description of web portal provisioning is based on the following assumptions:

- The web portal is a completely separate entity from the BSM (NAF), BSF, etc. and has no knowledge of key management.
- No HTTP digest authentication as per [3GPP TS 33.246] or [3GPP2 X.S0022-A](used in the Smartcard profile service provisioning messages) is required by the portal.

The Terminal MAY receive additional information related to the PurchaseItem, PurchaseData, and PurchaseChannel fragments using the '*url*' attribute of the '*extension*' element in each fragment. The Terminal SHALL use the '*PortalURL'* element of the PurchaseChannel fragment, defined in the Service Guide, as the entry point for Service Provisioning via a web portal. The *PortalURL* can be used to support three purposes:

1. The *PortalURL* provides additional information on services available over this PurchaseChannel. This method SHALL be signalled by setting the attribute *supportedService* under *PortalURL* to "0". In this case the Terminal MAY access the *PortalURL* to retrieve information on supported services but SHALL NOT purchase or (un)subscribe to the services by accessing the URL. In this case, the service provisioning functions SHALL be achieved by addressing Service Provisioning messages to the *PurchaseURL* as defined in section 5.1.5.

2. The *PortalURL* supports the full set of service provisioning functionality via the web-portal in addition to providing service related information. This method SHALL be signalled by setting the attribute *supportedService* under *PortalURL* to "1". The Terminal SHALL access the *PortalURL* where the Terminal SHALL expect that the facilities for service provisioning are provided by the web-portal. When the *supportedService* attribute under *PortalURL* is set to "1", the Service Provisioning messages sent to the *PurchaseURL* as defined in section 5.1.5 SHALL NOT be used.

3. The *PortalURL* provides additional information on services available over this PurchaseChannel. The Terminal MAY achieve the service provisioning either via web-portal or by addressing Service Provisioning messages to the *PurchaseURL* as defined in section 5.1.5. This method SHALL be signalled by setting the attribute *supportedService* under *PortalURL* to "2".

Note: care must be taken when value "2" of 'supportedService' is used that the web-portal and the BSM are correctly synchronized, as synchronization delays can result in the user being subscribed twice to the same service.

In the context of the above three methods, there are three ways the request to *PortalURL* can be formed.

1. Request without reference to a specific PurchaseItem.

   When Terminal accesses the *PortalURL* without any specific reference to any PurchaseItem, the Terminal SHALL issue an HTTP POST request to the *PortalURL*. This request SHALL be made over SSL/TLS when "https:" scheme is present in PortalURL. This request SHALL besides follow the conventions defined in section 17.13 of [HTML4.01] for submitting HTML form data by the "post" method using the "application/x-www-form-urlencoded" encoding type. For example, if *PortalURL* is http://server.example.org/webshop". The HTTP POST request sent to the web portal would be "http://server.example.org/webshop", not containing any associated data block.

2. Request with reference to a specific PurchaseItem.

   When the Terminal accesses the *PortalURL* with specific reference to a PurchaseItem or a set of PurchaseItems, the Terminal knows the relevant globalPurchaseItem IDs from the Service Guide.

3. Request with reference to a specific PurchaseItem and associated PurchaseData. In similar fashion than method 2, the terminal knows the identifier of the relevant PurchaseData fragments from the Service Guide.

   For methods 2 and 3 defined above, the Terminal SHALL issue an HTTP POST request to the *PortalURL*. This request SHALL be made over SSL/TLS when "https:" scheme is present in PortalURL.This request SHALL besides follow the conventions defined in section 17.13 of [HTML4.01] for submitting HTML form data by the "post" method using the "application/x-www-form-urlencoded" encoding type. The PurchaseItem(s) are identified using the globalPurchaseItem_ID(s). Each globalPurchaseItem_ID SHALL be signalled in a separate name-value pair, using "globalPurchaseItemID" as the name. The PurchaseData fragments are identified using their 'id' attribute, each PurchaseData fragment id SHALL be signalled in a separate name-value pair, using "purchaseDataID" as the name. For example, if *PortalURL* is "http://server.example.org/webshop" and the globalPurchaseItemIDs are "aau17135@bsda.example.org" and "fhh7982@bsda.example.org" and "jke132486@bsda.example.org", and there is also a related PurchaseData fragment id "bbu17135@bsda.example.org", the HTTP POST request sent to the web portral would be "http://server.example.org/webshop", containing a data block of the following structure:

   "globalPurchaseItemID=aau17135@bsda.example.org&
   globalPurchaseItemID=fhh7982@bsda.example.org&
   globalPurchaseItemID =jke132486@bsda.example.org&
   purchaseDataID= bbu17135@bsda.example.org"

NOTE 1: it is reminded that, according to [BCAST11-SG], the PurchaseData fragment points to one, and only one, PurchaseItem fragment. This allows mapping the purchaseDataID with the correct globalPurchaseItemID upon processing the request.

NOTE 2: "globalPurchaseItemID" name is intentionally reused for each name-value pair. This reuse is conformant with [HTML4.01] and the web-based system is assumed to support it.

The Terminal MAY receive an HTTP response message that contains a list of PurchaseItems, each of which is associated with either price information or price information and purchase options. Price information for each listed PurchaseItem SHOULD be consistent with that in the relevant PurchaseData fragment announced in the Service Guide. However, user specific purchase options such as promotions could be included in the response. The implementation and display of user specific purchase options is out of scope for BCAST 1.0.

After a successful subscription or purchase event, the BSM SHALL send a Trigger message to the terminal. The Trigger message and its further processing differs in the DRM and Smartcard profiles

For the DRM Profile:

1. Once the web-based subscription/purchase transaction is completed, the web-based system informs the BSM of the completed transaction via means that are outside the scope of this specification.

2. The BSM SHALL send a Provisioning Trigger message (see section 5.1.8) the Terminal, providing a URL to which the terminal can send the subsequent provisioning message, setting 'type'=0 and 'LTKMRenewalRequestTrigger.idCode'=1, i.e. 'oma-bcast-newservices'.

3. . The Terminal SHALL process this message as specified in section 5.1.8) and send an LTKMRenewalRequest to the BSM.

4. The BSM SHALL respond with an LTKMRenewalResponse that contains all those PurchaseItem/PurchaseData combinations for which the Terminal has not yet received a ROAP trigger, plus a ROAP trigger that allows the terminal to acquire those keys.

The BSM MAY re-send the trigger message if the terminal does not react to it within an assumed time interval. The terminal MAY send the LTKMRenewalRequest with 'globalIDRef' set to "oma-bcast-newservices" without having received a trigger message. The Terminal MAY ignore a trigger message if another trigger message with identical parameters has been previously received within a short time frame and successfully processed.

For the Smartcard Profile:

1. Once the web-based subscription/purchase transaction is completed, the web-based system informs the BSM of the completed transaction via means that are outside the scope of this specification.

2. If the terminal is in a registered state in BSM, and if at least one LTKM trigger bearer (e.g. UDP or SMS) has been successfully negotiated between BSM and terminal, the BSM SHALL send a BSM solicited pull message to the terminal to trigger registration procedure and subsequent delivery of LTKMs, including at a minimum the LTKMs associated to the items just purchased on the web-based system.

3. Otherwise, the BSM SHALL wait for another opportunity to deliver these LTKMs, such as the registration procedure initiated by terminal on BCAST application start.

In case of the other subsequent operations such as LTKM renewal, Token Purchase, Account Inquiry, the Terminal SHOULD use either the general service provisioning procedures or Smartcard Profile Service Provisioning procedures, defined in Sections 5.1.5 and 5.1.6 respectively, according to the security profile. The Terminal MAY unsubscribe using the web portal or using the General Service Provisioning procedure defined in section 5.1.5.

5.1.10 Parental Control for Service Ordering

The BSP-M in the BSM MAY enforce Parental Control for Service Ordering, i.e., parental control for service subscription, service purchase, and token purchase. The parental rating for service ordering is signalled in the 'ParentalRating' element of the 'PurchaseItem' fragment as described in [BCAST11-SG]. This element is merely an indication to the user which restriction the BSM enforces with regards to parental control and the Parental Control for Service Ordering is enforced within the BSM. The Smartcard Profile Extension, see section 5.1.10.1, also adds the possibility to enforce Parental Control for Service Ordering locally on the Smartcard.

If the BSM receives a Service Request message used for the subscription/purchase of one or more purchase items which are subject to parental rating restrictions, the BSM enforces parental control on each of these purchase items one by one according to the following bullets. Correspondingly, the same bullets apply also for any purchase item specified in a Token Purchase Request message.

1. If the purchase item is associated with a less restrictive parental rating than the level granted for the Terminal, the purchase item passes the parental control enforced by the BSM and the BSM responds to the request by specifying status code 000 "Success".
2. If the purchase item is associated with a more restrictive parental rating than the level granted for the Terminal and it is not possible to pass parental control by providing PINCODE, the BSM responds by specifying status code 032 "Parental Control Restriction- Request Disallowed" (see section 5.11) for the purchase item in the Service Response/Token Purchase Response.

3. If the purchase item is associated with a more restrictive parental rating than the level granted for the Terminal and no parental control PINCODE is provided in the Service Request/Token Purchase Request, the BSM requests the Terminal to provide the parental control PINCODE by specifying status code 033 “Parental Control Authentication Requested” (see section 5.11) for the purchase item in the Service Response/Token Purchase Response.
4. If the purchase item is associated with a more restrictive parental rating than the level granted for the Terminal and a parental control PINCODE specified in the Service Request/Token Purchase Request, the BSM verifies the specified PINCODE against the PINCODE associated with the Terminal.
    - If the verification fails, status code 034 “Parental Control Verification Failed” (see section 5.11) is specified for the purchase item in the returned Service Response/Token Purchase Response. Alternatively, status code 035 “Parental Control PINCODE Blocked” is specified as explained in the subsequent bullet.
    - If the PINCODE associated with the Terminal has been blocked by the BSM, e.g., the amount of incorrect PINCODEs submitted exceeds the limit set by the BSM, status code 035 “Parental Control PINCODE Blocked” (see section 5.11) is specified for the purchase item in the returned Service Response/Token Purchase Response.
    - If the verification succeeds, the purchase item passes the parental control enforced by the BSM.

Note: For each Terminal the BSM stores the level granted associated with the Terminal (this level is possibly mapped onto several rating systems) along with one Parental Control for Service Ordering PINCODE. How the BSM retrieves and stores the level granted associated with a Terminal and the PINCODE associated with a Terminal is out-of-scope of this specification.

The Terminal MAY support Parental Control for Service Ordering. A Terminal supporting Parental Control for Service Ordering MAY ask the user to input the parental control PINCODE for service ordering in case the BSM sends a Service Response/Token Purchase Response containing status code 033 “Parental Control Authentication Requested” or status code 034 “Parental Control Verification Failed”. After the user has inputted the PINCODE, it can be provided in the ‘ParentalControlPinCode’ element of a Service Request/Token Purchase Request along with the purchase items for which the BSM requested a PINCODE to be provided.

Note: How the user acquires the parental control PINCODE value for service ordering is out of scope of this specification. Examples of mechanisms that can be used include post and calling to operator’s customer service centre.

In order to authenticate the Terminal, the BSM and Terminal MAY support HTTPS POST or HTTP digest authentication as described in section 5.1.3 . In addition, the BSM and Terminal MAY support HTTPS POST for General Service Provisioning Messages to provide confidentiality protection of a PINCODE submitted in Service Request as described in section 5.1.1.1.

A Terminal supporting Parental Control for Service Ordering SHALL support detection of the ‘Challenge’ element in service provisioning messages. A Terminal is thereby able to differentiate between generic solution for parental control of service ordering described in this section compared to the Smartcard Profile extension described in section 5.1.10.1.

5.1.10.1 Smartcard Profile Extension

Independently from supported Service Protection profile(s), BSM MAY support and use the generic solution specified in section 5.1.10 or the Smartcard Profile extension of Parental Control for Service Ordering described in this section. For the Smartcard Profile extension, the Parental Control for Service Ordering is enforced within the BSM or locally in the Smartcard and verification of the PINCODE is enforced by the Smartcard in the Terminal at the BSM request.

If Parental Control for Service Ordering is enforced by the BSM, the BSM operates as described for the generic solution in step 1 and 2 in section 5.1.10 . In order to signal to the Terminal that the Smartcard Profile extension is used, the BSM SHALL in step 3 instantiate the ‘Challenge’ element of the service provisioning response.

The BSM MAY also, at the reception of a service request/token purchase request, systematically request Parental PINCODE verification allowing a local enforcement of the Parental Control for Service Ordering in the Smartcard. In this case the BSM specifies the status code 033 “Parental Control Authentication Requested” (see section 5.11) and instantiates the ‘Challenge’ element in the Service Response/Token Purchase Response.

Note: The ‘ParentalControlPinCode’ element of the service provisioning request is not used by the Smartcard Profile extension.

Independently from supported Service Protection profile(s), Terminal MAY support and use the generic solution specified in section 5.1.10 or the Smartcard Profile extension of Parental Control for Service Ordering described in this section. The Terminal operates according to the following bullets at the reception of the service provisioning response with a status code 033 “Parental Control Authentication Requested” and ‘Challenge’ element instantiated:

- If the Terminal doesn’t support the Parental Control for Service Ordering for Smartcard Profile, the Terminal informs the user that the request is disallowed.
- If the Terminal supports the Parental Control for Service Ordering for Smartcard Profile, the Terminal checks that the Smartcard implements the Service Provisioning Message Protection reading the EF_{BST} in the Smartcard under the ADF BSIM if the Smartcard Profile is implemented in ADF BSIM or under the DF BCAST if the Smartcard Profile is implemented under the USIM (see [BCAST11-ServContProt])
    - If the Smartcard doesn’t support the Service Provisioning Message Protection, the Terminal informs the user that the request is disallowed.
    - If the Smartcard supports the Service Provisioning Message Protection, the Terminal sends to the Smartcard using the AUTHENTICATE command in MBMS Security Context for OMA BCAST operation defined for Parental Control Service Provisioning Mode, the service provisioning type information, the requestID of the request and the Challenge included in the service provisioning response by the BSM .(see [BCAST11-ServContProt])

- If the Terminal receives in the response of the AUTHENTICATE command an operation status code indicating that a PINCODE is required (i.e. “PINCODE required”) with the Key reference of the PIN defined for the Parental Control for Service Ordering, the Terminal SHALL then prompt the user for verification of the Parental Control for Service Ordering PINCODE using the VERIFY PIN command and the Key Reference transmitted by the Smartcard in the response of the AUTHENTICATE Command. After a successful verification of the PINCODE the Terminal re-sends the AUTHENTICATE Command to obtain the Message Authentication Code of the Challenge transmitted in the command. After reception of this Message Authentication Code in the response of the AUTHENTICATE command, the Terminal sends to the BSM a new service provisioning message similar to the first one but including this MAC received from the Smartcard .
- If the Terminal receives in the response of the AUTHENTICATE command an operation status code indicating that the PINCODE is blocked (i.e. “PINCODE blocked”), the Terminal SHOULD signal to the user that the service request is not allowed and that the Parental PINCODE is blocked.
- If the Terminal receives in the response of the AUTHENTICATE command an operation status code indicating that the service provisioning requests are locally disallowed (i.e. “Service provisioning requests locally disallowed”), the Terminal SHOULD signal to the user that the service request is not allowed.

At the reception of the service provisioning message including a MAC, the BSM verifies the MAC received to authenticate the issuer of the MAC and verify that the sending of the service provisioning message has been controlled by the parent. This replaces the step 4 of the generic solution.

The verification of the MAC is done in the following way:

- the BSM derives an Authentication Key (Serv_Prov_Auth_Key (SPAK)) from the SMK associated to the client using the service provisioning type of the message and the request ID received in the service provisioning message. The SPAK shall be derived from the key SMK using the GBA key derivation function (see Annex B of [3GPP TS 33.220]) as follows (see notation style is explained in Annex B of [3GPPTS 33.220]):
    - FC = 0x01,
    - P0 = "bcast-serv-prov" (i.e. 0x62 0x63 0x61 0x73 0x74 0x2d 0x73 0x65 0x72 0x76 0x2d 0x70 0x72 0x6f 0x76), and
    - L0 = length of P0 is 15 octets (i.e. 0x00 0x0f).
    - P1 = Service Provisioning Type

- L1 = Length of P1 is 1 octet (i.e 0x00 0x01)
- P2 = requestID
- L2 = Length of P2 is 4 octets (i.e. 0x00 0x04)

Where Service Provisioning Type is coded as follows:

Table 38: Service_provisioning_type Coding

Value	Description
0x00	Service request
0x01	Token purchase request
0x02 to 0xFF	Reserved for future use

The Key to be used in key derivation shall be the SMK

In summary, the SPAK shall be derived from the SMK as follows:

SPAK = KDF (SMK, "bcast-serv-prov", Service Provisioning Type, requestID)

- The BSM then computes the MAC code of the Challenge sent previously in the response of the corresponding first service provisioning request

MAC' = HMAC-SHA-256(SPAK, Challenge)

- The BSM then compares the MAC' obtained to the MAC received in the service provisioning message.
  - If the MAC'=MAC then the service provisioning message is correct and has been protected by the parental control function in the Smartcard. Then the BSM responds to the service request by specifying status code 000 "Success"
  - If the MAC' ≠ MAC then the service provisioning message is not correct and has been modified or has not been controlled by the Smartcard. Then the BSM responds to the service request by specifying status code 034 "Parental Control Verification Failed"

5.2 Terminal Provisioning

5.2.1 Terminal Provisioning through Interaction Channel

The Terminal Provisioning function SHALL support OMA Device Management [OMA DM 1.2], as specified in this section. To allow firmware upgrades using DM over the interaction channel, the Terminal Provisioning function SHOULD support OMA FUMO 1.0 [OMA FUMO].

Terminal Provisioning function provides data structures to provision and manage the terminal through the interaction channel using OMA DM [OMA DM 1.2].

The interfaces related to Terminal Provisioning function, as outlined in BCAST Architecture [BCAST11-Architecture] are normatively specified as follows:

- Over interface TP-7-1 and TP-7-2, both the network and the terminal SHALL support exchange of terminal provisioning and management messages as specified in [OMA DM 1.2]

5.2.1.1 Terminal Provisioning of BCAST Client

The Terminal Provisioning Client Component (TP-C) SHALL receive the parameters needed for OMA BCAST service (see [BCAST11-Services] Appendix G) by the Terminal Provisioning function which manage the terminal configuration parameters, e.g. data, parameters and applications with the help of OMA DM [OMA DM 1.2]. This information would be delivered through TP-7-1 as specified in OMA DM [OMA DM 1.2].

The Terminal Provisioning Client Component (TP-C) SHALL be able to:

- receive the parameters needed for BCAST service included in the terminal provisioning messages sent over TP-7-1.
- update the parameters needed for BCAST service included in the terminal provisioning messages sent over TP-7-1.
- perform firmware upgrades of the BCAST client using the interaction channel over TP-7-1.

Further, the existence and access description to Terminal Provisioning function MAY be declared through the Service Guide using the Service, Access and Content fragments of Service Guide or through the process as specified in OMA DM. Both of the following cases are specified in section 5.2.2:

- Declaration of the existence and access to the OMA DM based exchange over TP-7-1.

5.2.1.2 Declaring the existence of and access to Terminal Provisioning

There are two ways to declare the existence of and the access to Terminal Provisioning with Service Guide: Terminal Provisioning declared as a Service; and; Terminal Provisioning declared as a means for accessing of a Service. The terminal SHALL support both methods of declaring the Terminal Provisioning within the Service Guide. The following sections specify both of these ways.

The TP-C MAY also be bootstrapped with the Terminal Provisioning server information to access the Terminal Provisioning by TP-7-1.

5.2.1.2.1 Declaring Terminal Provisioning as a Service within Service Guide

When the Terminal Provisioning is declared as a service, the following applies:

- There SHALL be at least one Service fragment with the value of attribute “ServiceType” equals “9 - Terminal Provisioning service”.
- There SHALL be at least one Access fragment that specifies the access to the above-mentioned Service:
  - In case Terminal Provisioning over TP-7-1 is declared, the AccessType SHALL contain “UnicastServiceDelivery” element, which defines the access to the respective provisoning server.
- There MAY be one or more Content fragments that specify the Terminal Provisioning messages as files, as defined in section 5.2.1.

5.2.1.2.2 Declaring Terminal Provisioning as an Access of a Service within Service Guide

When the Terminal Provisioning is declared as an access of a service, the following applies:

- There SHALL be at least one Service fragment that defines a service of arbitrary type.
- There SHALL be at least one Access fragment associated with the above-mentioned Service. The Access fragment SHALL have “ServiceClass” element present with value “urn:oma:bcast:oma_bsc:tp:1.0”. Further:
  - In case Terminal Provisioning over TP-7-1 is declared, the AccessType SHALL contain “UnicastServiceDelivery” element, which defines the access to the respective OMA DM server.

5.2.1.2.3 Declaring Terminal Provisioning through Bootstrap

5.2.1.2.3.1. Initiation of Terminal Provisioning by DM server

Terminal Provisioning through bootstrap (e.g. server information or account for such as the Session Description, Authentication, and/or Connectivity) MAY be supported as specified in [OMA DM 1.2]. Bootstrap information comprising

DM server's Connectivity information, would be delivered to the terminal. Then, the DM server would deliver to the terminal information for the Terminal Provisioning server such as Session Description, Authentication Information (certificate, OCSP Response) for secure delivery and/or Connectivity as specified in [OMA DM 1.2].

5.2.1.2.3.2. Initiation of Terminal Provisioning by Smartcard

Terminals with cellular interface and (U)SIM/R-UIM/CSIM that support BCAST and OMA DM [OMA DM 1.2] SHALL support bootstrap from the smartcard as specified in [DMBOOT]. In these terminals DM TND Serialization [DMTNDS] SHALL also be supported otherwise

The following table shows the DM Client Requirements. The table is based on section 8 of [ERELDSC].

Feature / Application	Status	References
DM Client	MANDATORY	[DMPRO] [DMREPU] [DMSEC] [DMTND] [DMSTDOBJ] [DMDDFDTD]
DM Client Bootstrap	MANDATORY if Terminal with cellular radio interface and (U)SIM/(R-)UIM/CSIM	[DMBOOT]
DM TND Serialization	MANDATORY if Terminal with cellular radio interface and (U)SIM/(R-)UIM/CSIM	[DMTNDS]

Table 39: OMA BCAST Device Management Client Requirements

5.2.1.3 Carrying OMA DM messages through Interaction Channel

Over interface TP-7-1, DM provisioning messages SHALL be delivered using DM mechanism. The details follow the OMA DM procedure.

5.2.2 Terminal Provisioning through Broadcast Channel

The Terminal Provisioning function SHALL support OMA Device Management [OMA DM 1.3], as specified in this section. The use of Terminal Provisioning through the Broadcast Channel is intended to provide a broadcast delivery mechanism. OMA DM commands and related files, if required, are packaged as a Terminal Provisioning Package and distributed through the broadcast channel of BCAST. Currently, firmware update [OMA FUMO], software update [OMA SCOMO], network measurement and device capability control are to be delivered as Terminal Provisioning Packages through the Broadcast Channel.

The interfaces to be used are defined in the BCAST Architecture [BCAST11-Architecture].

5.2.2.1 Terminal Provisioning of BCAST Client

The Terminal Provisioning Client Component (TP-C) SHALL receive the parameters needed for Terminal Provisioning through the Service Guide or Notification functions.

The Terminal Provisioning Client Component (TP-C) SHALL be able to:

- Identify whether there is a Terminal Provisioning Package applicable for the terminal via checking the Terminal Provisioning service parameters delivered through the BCAST Service Guide sent over TP-5.
- Retrieve the Terminal Provisioning Package from the file carousel sent over TP-5
- Perform Terminal Provisioning of the BCAST client based on the Terminal Provisioning Package.

5.2.2.2 Declaring the existence of and access to Terminal Provisioning

The existence and access description to Terminal Provisioning function is declared either through the Service Guide using the Service, Access and Content fragments or through the Notification function.

5.2.2.2.1 Declaring Terminal Provisioning through Service Guide

Terminal Provisioning SHALL be declared as a service and the following applies:

- There SHALL be at least one Service fragment with the value of attribute "ServiceType" equals "9 - Terminal Provisioning service".
- There SHALL be at least one PurchaseItem fragment with autosubscription enabled (DependencyReference pointing to the PurchaseItem it belongs to) which is linked to the above-mentioned Service fragment.
- There SHALL be at least one Content fragment that has the TerminalProvisioning element instantiated to specify the type of Terminal Provisioning and targeted terminal set. The Content fragment SHALL be created by the TP-M and sent over the TP-4 interface to the TP-DA with the Terminal Provisioning Package.
- There SHALL be at least one Access fragment that specifies the access to the above-mentioned Content

5.2.2.2.2 Declaring Terminal Provisioning through Notification

Terminal Provisioning MAY be declared as a Notification service and the following applies:

- There SHALL be at least one Service fragment with the value of attribute "ServiceType" equals "9 - Terminal Provisioning service".
- There MAY be at least one PurchaseItem fragment with autosubscription enabled (DependencyReference pointing to the PurchaseItem it belongs to) which is linked to the above-mentioned Service fragment.
- There SHALL be at least one Content fragment that identifies a Terminal Provisioning Package.
- There SHALL be at least one Access fragment that specifies the access to the above-mentioned Content
- Notifications SHALL be created at the TP-M with the "eventType" equals "8 – Terminal Provisioning Trigger" and with the TerminalProvisioning element instantiated to specify the type of Terminal Provisioning and targeted terminal set. SessionInformation SHALL be set to indicate the delivery session related to the Terminal Provisioning Package. Notifications and Terminal Provisioning Packages SHALL be sent over the TP-4 interface from the TP-M to the TP-DA.
- Notifications SHALL be sent either as a Service Specific Notification or a Service Provider Specific Notification.

5.2.2.3 Carrying OMA DM message through Broadcast Channel

Over interface TP-5, OMA DM messages and if required related files (e.g. firmware) SHALL be delivered as a file (Terminal Provisioning Package) using the BCAST File Delivery methods as defined in BCAST Distribution [BCAST11-Distribution].

5.3 Interaction

The BCAST enabler specifies different types of interactions between the end user and their terminal, and the service provider.

These are the following:

1. Interactive retrieval of the Service Guide (SG). The terminal requests, and receives, the service guide or changed parts of the service guide for a service. This type of interaction is described in the [BCAST11-SG], section 5.4.3.
2. Interactive retrieval of additional information related to Service Guide fragments, for example in form of a webpage presenting additional information. This is enabled using the ExtensionURL which can optionally be included into some SG fragments for retrieving further information about the fragment by accessing the URL. For details see in the [BCAST11-SG].
3. Service interaction, i.e. interaction as part of the service (in contrast to the previous two types of interaction, which are used to receive information about a service). Examples for such interactions within a service are voting about the service or actor, or the offer to the user to order a ring-tone matching the music that is just played in a show. This is enabled using interactivity information in the SG as an entry point and interactivity media that are distributed in a channel associated with the service itself. This is described in more detail in this document in section 5.3.6.

4. Interactive delivery of BCAST services, i.e. delivery over the interaction channel. This is enabled using the UnicastServiceDelivery in the SG.

In general, the availability of the interaction channel is assumed. However, the interaction channel may be temporarily unavailable, for example due to lack of radio coverage. Further, devices without access to an interaction channel are possible; however, such devices may have limited functionality.

5.3.1 Protocols and media codecs for Service Interaction Function

This section describes the protocols which are provided by the Service Interaction Function of the BCAST enabler at the interface between BSI-G and BSI-C through SI-8 and the media codecs the BCAST application supports.

With respect to the protocols, please note that this section only specifies the protocols to be used for the Service Interaction Function. The use of the interaction channel by other functions (e.g. Service Guide Function) is defined in the respective other parts of the BCAST specifications and is not part of this section.

The available interaction protocols for a service are signalled in the Service Guide according to section 5.1.2.4 in the BCAST Service Guide specification. If a terminal does not support any of the interaction protocols specified here, it SHALL not offer the interactive parts of the service to the user.

A service making use of the interaction function MAY use any of the following protocols.

Regarding support of the protocols in the terminal for use by the Service Interaction Function, the following rules apply:

- The terminal SHALL support the following protocols: IP, TCP, HTTP.
- The terminal MAY support the following protocols: SMS, IPSEC, UDP, MMS, WAP, HTTPS based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246], SIP/IMS.
- If a terminal supports SMS, it SHALL support SMS as an interaction protocol for BCAST services.
- If a terminal supports MMS, it SHALL support MMS as an interaction protocol for BCAST services.
- Furthermore, the terminal MAY offer the user an option to initiate a voice call from the service application of an interactive broadcast service. In this case, the terminal SHALL prompt the user before actually making the call.

5.3.2 Interactive retrieval of Service Guide

If the Terminal has a capability for interaction, it SHALL support interactive retrieval of Service Guide fragments as specified in [BCAST11-SG].

5.3.3 Interactive retrieval of Service related information

Within any Service, Content, PurchaseItem, PurchaseData, PurchaseChannel, or InteractivityData fragment, the network MAY include an “Extension” element. The semantics of this element is to provide a pointer to a web resource providing further information related to the fragment (For example, a www page related to the certain content can be reached by following an extension URL in Content fragment). If the Terminal has a capability for interaction, it SHALL support this element and SHALL be capable of accessing such additional information by using HTTP.

5.3.4 Interactive service ordering

After receiving Service Guide, Terminal can subscribe or purchase PurchaseItem via Interaction Network. Interactive service ordering includes service request for subscription or purchase, Subscription LTK Renewal request, Token purchase request and also unsubscription request specified in the section 5.1.6 of this specification.

5.3.5 Interaction for service and content protection

Service and Content Protection have four layers. Those four layers are the registration layer, the LTKM delivery layer, the STKM delivery layer and the traffic encryption layer. Terminal executes registration procedure with BSM to acquire

Registration Data. After that Terminal acquires SEK and/or PEK from LTKM delivered from BSM or BSD/A. Terminal can perform traffic decryption using TEK after receiving STKM from BSD/A.

5.3.6 Service related interaction and feedback using Interactivity Media Documents

The mechanism described in this section allows the user to interact with the service, for example for voting applications. The main entry point for interactivity services is the InteractivityData fragment in the SG (see section 5.1.2.10). This InteractivityData fragment points to one or more interactivity media documents, which contain the actual interactivity media objects.

5.3.6.1 Interactivity Media Document

An instance of 'InteractivityMediaDocument' represents details of an interactive component of a service. This component is thought as interactive means for a user to consume the service. The interactive component can consist of multiple instances of 'InteractivityMediaDocument' and can be associated to both services and individual pieces of services through the 'InteractivityData' fragment of the Service Guide. In practice, the contents of an 'InteractivityMediaDocument' triggers the Terminals to render the details of the interaction(s) "interactivity media objects" message onto the GUI which in turn is thought to prompt the user of the terminal to react on it..

5.3.6.1.1 Media Object Group and Media Object Set

Each instance of 'InteractivityMediaDocument' can consist of multiple media object groups, and each media group can consist of one or more media object sets. A media object set is a bundle of related media objects to be rendered as a unit (e.g. XHTML pages + external stylesheet + pictures) and clearly identified as pertaining to a specific interactivity technology (SMS, MMS template, XHTML, Rich Media…). From each media object group only one media object set is rendered at the same time by the terminal. This is indicated by the media object set with the highest relative priority, expressed by the element 'RelativePreference', and that is besides supported by the terminal. If a media object set is not supported by the terminal it is discarded. If none of the media object sets are supported by the terminal the terminal SHALL display the alternative text.

The media objects of a media object set are packed into one file bundle transported separately from the instances of 'InteractivityMediaDocument' (except for email and SMS). The element 'MediaObjectGroup' of InteractivityMediaDocument only describes each media set the involved interactivity technology, the type of included media objects, and the file delivery information needed to retrieve the set of media objects. This decoupled structure allows the terminal to discard the unsupported media object sets at the very beginning of file bundle reception, and more importantly to avoid storing them. Content promotion can be enabled by one media object group in the InteractivityMediaDocument . By referring to this same media object group through the attributeOnActionPointer of the element 'ActionDescriptor' the terminal will always return to the same media object set when the end-user triggered the terminal to send out a message over the interaction channel. Referring to information on an external web-site can be enabled by declaring one media object group with an XHTML MP media object set or a Rich Media media object set in the InteractivityMediaDocument . By omitting the attribute OnActionPointer of the element 'ActionDescriptor', hyperlinks in XHTML pages or Rich Media scenes can refer the user to external web-sites. Further, SMS-URIs according to [URI-Schemes] can also be embedded in XHTML or Rich Media scenes. If the Terminal supports XHTML or a Rich Media Solution allowing hyperlinks, it SHALL support SMS URIs [URI-Schemes].

Time-dependent behaviour of the interaction can be enabled by defining 3 media object groups in the InteractivityMediaDocument . The first media group defines the media to start with, e.g. a list of possible answers of a voting. When the user answers in time (as defined by the attribute InputAllowedTime of the element 'ActionDescriptor'), the user is presented the media object set from the second media group (as defined by the OnActionPointer). If the user waits too long or does not provide any input the media object set from the third media group is presented (as defined by the attribute OnTimeOutPointer of the element 'ActionDescriptor'). Setting the Update Flag in turn in an instance of 'InteractivityMediaDocument' having group position zero to "true" enables the rendering of the media object set for the next question. When the amount of time represented by the attribute InputAllowedtime is passed the terminal will start listening to the file delivery channel for an instance of InteractivityMediaDocument with a higher value of GroupPosition.

Interactivity Media Document can specify that interaction sent back from device to service provider shall be distributed over time, e.g. to avoid overload in network nodes or links caused by too many simultaneous interactivity messages sent back. The

explicit signaling of the required parameters in Interactivity Media Document prevails, for that interaction, over default values possibly signaled in the corresponding 'Interactivity Data' fragment.

Instances of 'InteractivityMediaDocument' and the files declared in the element 'MediaObjectSet' are delivered using BCAST File Distribution Function. The system MAY deliver instances of 'InteractivityMediaDocuments' and associated files over broadcast file distribution or serve those over interactive channel. Terminals supporting the interactive channel SHALL support reception of the instances of 'InteractivityMediaDocuments' and the associated files over broadcast file distribution.

5.3.6.1.2 Format of Interactivity Media Document

The following table defines the message format of Interactivity Media Documents. . The XML schema for this message format is defined in [BCAST11-XMLSchema-InteractivityMedia].

Name	Type	Category	Cardinality	Description	Data Type
InteractivityMediaDocument	E	NO/TM		The InteractivityMediaDocument defines the actual InteractivityMedia objects Contains the following attributes: groupID groupPosition id version validFrom validTo Contains the following sub-elements: MediaObjectGroup PrivateExt	
groupID	A	NM/TM	1	ID of the group of Interactivity Media document, globally unique	anyURI
groupPosition	A	NM/TM	1	Relative position of this document in the group. The greater value has higher priority to handle (i.e 2 has higher priority than 1).	unsignedShort
id	A	NM/TM	1	ID of the InteractivityMediaDocument , globally unique.	anyURI
version	A	NM/TM	1	Version of this InteractivityMediaDocument. The newer version overrides the older one with the same id as soon as it has been received.	unsignedInt
validFrom	A	NM/TM	0..1	The first moment when the media object sets in this document is valid to be rendered. If not given, the media object sets SHALL be rendered as soon as they are available. This field expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
validTo	A	NM/TM	0..1	The last moment when the media object set is valid to be rendered. If not given the rendering is assumed to end in undefined time in the future. This field expressed as the first 32bits integer part of NTP time stamps. Whenever there is an InteractivityMediaDocument available with the same GroupID but with a higher GroupPosition and the 'validFrom' time of that InteractivityMediaDocument arrives, the terminal SHALL stop rendering the current document and render the new InteractivityMediaDocument.	unsignedInt

MediaObject Group	E1	NM/TM	1..N	Grouping of the media object sets, which serve the same purpose during interactivity, e.g. as a starting media object set, as a media object set to be shown after action was taken or to be shown after time-out was reached. Has the following attributes: id startMediaFlag Has the following sub-elements: ActionDescriptor BackOffTiming MediaObjectSet SMSTemplate EmailTemplate VoiceCall WebLink AlternativeText RichMedia StreamingLink	
id	A	NM/TM	1	The ID of the media group	anyURI
startMediaFlag	A	NM/TM	1	The flag indicates, whether the media object sets in this MediaObject-Group should be started with. There SHALL only be one MediaObjectGroup with this flag set to "true" in an InteractivityMediaDocument	boolean
Action Descriptor	E2	NM/TM	0..1	The action descriptor describes the behaviour of the terminal when the media objects enable end-user input. Has the following attributes inputAllowedTime onTimeOutPointer updateFlag onActionPointer	
inputAllowedTime	A	NM/TM	0..1	The last moment the terminal allows the end-user to provide end-user input for the active media object set in this media object group. This field is expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
onTimeOutPointer	A	NM/TM	0..1	This pointer refers to the ID of a media object group in this InteractivityMediaDocument. When the InputAllowedTime is passed the terminal SHALL present the appropriate media object set of the MediaObjectGroup indicated by the OnActionPointer. The terminal SHALL NOT present this media object set if the terminal has already presented the media object set indicated by the OnActionPointer.	anyURI
updateFlag	A	NM/TM	0..1	Whenever this flag is "true" the terminal shall listen to and fetch the following interactivity media document and the associated media objects from the file delivery stream when the	boolean

				Inputallowedtime is passed. The following inter-activity media document is identified by the document with the same group ID and a higher GroupPosition number.	
onActionPointer	A	NM/TM	0..1	This pointer refers to the ID of a media object group in this interactivity media document. When the end-user undertakes action before the InputAllowedTime, which triggers the terminal to send out a message over the interaction channel (e.g. MMS, SMS or HTTP request), the terminal SHALL present the appropriate media object set of the media object group indicated by this pointer. If this pointer refers to the same ID as the current media object group, the terminal SHALL return to the same media object set after completing the action. In this case InputallowedTime and OnTimeOutPointer SHALL NOT be declared.	anyURI
BackOffTiming	E2	NM/TM	0..1	This element specifies timing behaviour of interaction sent back from the device to the service provider. Its purpose is to provide a mechanisms that ensures distribution over time of feedback sent from receivers, e.g. in order to avoid overload in nodes or links. If present, the interaction, if any, SHALL be sent back in the time interval [OffsetTime, OffsetTime+RandomTime] after the event that triggered the interactivity (e.g. user feedback). The exact time within the allowed time window shall be random with uniform probability. Explicit timing behaviour expressed in Interactivity Media Document prevails over possible default timing behaviour expressed in InteractivityData.	
offsetTime	A	NM/TM	1	The OffsetTime specifies the minimum time that a device SHALL wait after an event that triggers interaction (e.g. user input), before sending the interaction. The unit is seconds (fractions can be expressed using data type Decimal). OffsetTime shall be a non-negative number.	decimal
randomTime	A	NM/TM	1	The RandomTime refers to the time window length over which a device SHALL calculate a random time for the transmission of interaction. The method provides for statistically uniform distribution over a relevant period of time. The device SHALL calculate a uniformly distributed random time out of the interval between 0 and RandomTime. The unit is seconds (fractions can be expressed using data type Decimal). RandomTime shall be a non-negative number.	decimal
MediaObjectSet	E2	NM/TM	0..N	A media object set defines the media objects attached to one interactivity technology proposed in the MediaObjectGroup. These media objects	

				are related to each other, and form an interactivity unit to be rendered upon MediaObjectGroup activation (provided this interactivity technology is the one selected for rendering). The set of media objects is not stored in the MediaObjectGroup itself (i.e. in the InteractivityMediaDocument) but as another external file, where this external file is : either one uncompressed media file (like a .3GP video, a .JPEG picture), or one GZIP archive file containing one or several compressed media objects (a .GZ file e.g. containing a compressed SMIL + 3GP video + text) The GZIP archive format is the one defined in [RFC 1951] and [RFC 1952]. In case the archive contains multiple media objects, it consists of the plain concatenation of each compressed media object (i.e. each GZIP member), as specified in section 2.2 of [RFC 1952]. The optional FNAME field SHOULD be set by the sender in each GZIP member header, with an FNAME value in accordance with the 'Object' Content-Location one (see below Content-Location description). The 'MediaObjectSet' element contains the following attributes: relativePreference Content-Type Content-Location The language of a MediaObjectSet element is expressed by using the built-in XML attribute xml:lang with this element. In case this attribute is not instantiated, the terminal SHALL interpret the MediaObjectSet element to be applicable for any language. The 'MediaObjectSet' element contains the following elements: Description Object File	
relativePreference	A	NM/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media object sets elements are instantiated in this 'MediaObjectGroup' then all the media object sets SHALL have mutually exclusive values of 'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these	unsignedInt (32 bits)

				elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	
Content-Type	A	NM/TM	1	Gives the media type of the ‘MediaObjectSet’’s external file : If this media type is ‘application/x-gzip’, the external file is a GZIP archive file containing one or several media objects. Otherwise (in this version of the specification) the external file is one uncompressed media file (e.g. ‘video/3gpp’ for a 3GP video file containing a SMIL presentation). In case the external file is transported by FLUTE, this attribute MUST match the ‘File’ Content-Type value provided in the FDT instance(s) describing this file.	string
Content-Location	A	NM/TM	1	Uniquely identifies the ‘MediaObjectSet’’s external file within the file delivery session. In case this external file is transported by FLUTE, this attribute MUST match the ‘File’ Content-Location value provided by the FDT instance(s) describing this file, but if the file is transported by ALC/LCT, this field is NOT used but SHALL nevertheless match the Content-Location in the ‘’File’’ element below. The session used for file retrieval is the same session that carries this InteractivityMediaDocument. Using this attribute, multiple ‘MediaObjectSet’ instances belonging to the same or different ‘MediaObjectGroup’ instances of the same or different instance of ‘InteractivityMediaDocument’ MAY point to the same external file.	anyURI
Description	E3	NM/TM	0..1	Description of the Media Object Set, expressed in the same language as the parent ‘MediaObjectSet’ element. This is used to provide the end-user extra information regarding the Media Object Set content.	string
Object	E3	NM/TM	0..N	Describe each media object contained in the media object set. Depending on ‘MediaObjectSet’’s external file nature: if a single uncompressed file, this element is not needed unless it can provide supplemental information not given by parent ‘MediaObjectSet’ (such as ‘PartType’, etc.). if a GZIP archive, the sequence order of ‘Object’s in ‘MediaObjectSet’ MUST be the same as the sequence of members in the GZIP archive (side-by-side relationship between ‘Object’ sequence and GZIP members).	

				Contains the following attributes: …….Content-Location Content-Type ……..start Contains the following elements: PartType	
Content-Location	A	NM/TM	0..1	*If 'MediaObjectSet''s external file is an uncompressed file:* useless. *If 'MediaObjectSet''s external file is a GZIP archive:* The external file can be found by decompressing the n'-th member of the GZIP archive, given n is the position of the 'Object' in the 'MediaObjectSet'. The Content-Location value SHALL be a Relative-Path Reference as defined in [RFC 3986] and SHALL represent the sub-folder(s) + the filename of the deflated GZIP member to be used on storage. This relative storage content location is intended to be directly pointed by common markup language references (typically via src="" and href""). If present, the FNAME field of the GZIP member MAY be verified against the filename part of Content-Location, ignoring case differences. In case these two values differ, the terminal MAY choose to discard the Media Object Set. When storing the deflated media object, the terminal MUST create any indicated sub-folder(s) specified in the Content-Location, and store the media object in the leaf sub-folder, using the file name indicated in the Content-Location. The terminal SHOULD preserve the letter case specified in the Content-Location value when deflating the subfolders and the media file locally. The dot-segment "." MUST be supported. Content-Location value SHALL be unique within the sequence of 'Object' elements belonging to the same 'MediaObjectSet' in the following respect: A folder (including root folder) SHALL NOT contain two different subfolders or files for which the names only differ by the letter case. For security reasons, the terminal SHOULD discard the Media Object Set in case a naming conflict is detected. For security reasons, the terminal SHOULD discard the Media Object Set if one or several dot-segments ".." are present in the Content-Location.	anyURI
Content-Type	A	NM/TM	1	*If 'MediaObjectSet''s external file is an uncompressed file:* useless (information already given in 'MediaObjectSet').	string

				If 'MediaObjectSet''s external file is a GZIP archive: Gives the media type of the GZIP archive member mapped to the 'Object'.	
start	A	NM/TM	0..1	*If 'MediaObjectSet''s external file is an uncompressed file, or else a GZIP archive containing one media object:* useless (implicitly "true"). *If 'MediaObjectSet''s external file is a GZIP archive containing multiple media objects :* This attribute must be set to "true" for exactly one 'Object' and one only in the 'Object' sequence, the "start media object" on which the interactivity client must be launched. Default value, and applicable value for the other 'Object' elements : false	boolean
PartType	E4	NM/TM	0..N	Indicates the media types that should be supported also in order to correctly render an 'Object' consisting of several sub-media objects. E.g. a 3GP "Extended-presentation profile" would be one 'Object' with one "application/smil" 'PartType' advertising the presence of a SMIL presentation in the file.	string
File	E3	NO/TM	0..1	Present in case ALC/LCT without FLUTE is used for the delivery of 'MediaObjectSet''s external file. Structure identical to the 'File' child element of 'FileDescription' in the Access fragment. [BCAST11-SG].	
Content-Location	A	NM/ TM	1	See RFC 3926, section 3.4.2	anyURI
TOI	A	NM/ TM	1	See RFC 3926, section 3.4.2	positiveInteger
Content-Length	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	unsignedLong
Transfer-Length	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	unsignedLong
Content-Type	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	string
Content-Encoding	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	string
Content-MD5	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	base64Binary
FEC-OTI-FEC-Encoding-ID	A	NO/TM	0..1	See RFC 3926, section 3.4.2	unsignedByte
FEC-OTI-FEC-Instance-ID	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	unsignedLong
FEC-OTI-Maximum-Source-Block-Length	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	unsignedLong
FEC-OTI-	A	NO/	0..1	See RFC 3926, section 3.4.2	unsignedLon

Encoding-Symbol-Length		TM			g
FEC-OTI-Max-Number-of-Encoding-Symbols	A	NO/ TM	0..1	See RFC 3926, section 3.4.2	unsignedLong
FEC-OTI-Scheme-Specific-Info	A	NO/TM	0..1	This attribute MAY be used to communicate FEC information which is not adequately represented by the other attributes related to FEC.	base64Binary
SMSTemplate	E2	NM/TM	0..1	Contains the following attributes: relativePreference Contains the following elements: Description SelectChoice Picture Note: the SMSTemplate is a media object set, although not encoded using the 'MediaObjectSet' generic structure. Note: The SMSTemplate provides information about the option(s) in an interaction and some basic rendering tools through the possibility to insert static pictures. If improved rendering is to be specified by the service provider, the interaction can alternatively be described in an XHTML document with in-lined SMS URIs.	
relativePreference	A	NM/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e., 2 has higher priority than 1). If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all the media object sets SHALL have mutually exclusive values of 'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	unsignedInt
Description	E3	NM/TM	0..N	Text describing the interaction to the end user, possibly in multiple languages. The language is expressed using the built-in XML attribute xml:lang with this element. This text can e.g. describe the overall scope of the interaction, valid for all interaction options described below. It might e.g. also contain information about the prize of the SMS interaction.	string

				For an interaction with only one choice (e.g. an offer to purchase merchandise like a ringtone), the 'Description' element SHOULD be used to provide information regarding the interaction and the 'ChoiceText' element MAY be discarded by the terminal.	
text	A	NO/TM	0..1	This attribute can contain a string that can be inserted into SMS messages specified by SMS-URI attributes below. Note: this attribute enables message size savings for the case where the same text appears in the SMS bodies of several choices, i.e. if multiple SelectChoice elements are present	string
SelectChoice	E3	NM/TM	1..N	Contains the following attributes: smsURI Contains the following elements: ChoiceText Picture Note: For an interaction with multiple choices (like a voting between several options), the SelectChoice elements describe the different options to the user, and declare the SMS interaction to be executed when the user selects this option. For an interaction with one choice (e.g. an offer to purchase merchandise like a ringtone), there is only one SelectChoice element. The SMS template provides basic rendering tools through the possibility to insert static pictures. Other rendering indications to display the choice(s) to the user are out of scope of this specification.	
smsURI	A	NM/TM	1	SMS receiver address and payload encoded as “sms:” URI scheme. Value of this attribute SHALL comply with “sms:” URI scheme [URI-Schemes], with the following exceptions: If the sms-body [URI-Schemes] of the sms URI scheme contains the string “$userid$”, it shall be replaced by the user ID. If the sms-body [URI-Schemes] of the sms URI scheme contains the string “$deviceid$”, it shall be replaced by the device ID. If the sms-body [URI-Schemes] of the sms URI scheme contains the string “$userinput$”, it should be replaced by a string that the user can enter. This may be an empty string. If $userinput$ is present in the SMS-URI, the terminal SHALL open the SMS template in SMS editor (or similar) to allow user input before sending the SMS. If, however, the $userinput$ string is not present in the sms-body, the terminal SHALL not provide the SMS for the end user to modify. The terminal SHOULD prompt the end user before sending the	anyURI

				SMS out. If the sms-body [URI-Schemes] of the sms URI scheme contains the string “$text$”, it SHALL be replaced by the string signalled in the attribute “Text” (if this attribute is present).	
ChoiceText	E4	NM/TM	0..N	Description of the interaction option, possibly in multiple languages. This is used to provide the end-user information on this interaction choice.. The language is expressed using the built-in XML attribute xml:lang with this element. For an interaction with one choice (e.g. an offer to purchase merchandise like a ringtone), the 'Description' element SHOULD be used to provide information regarding the interaction and the 'ChoiceText' element MAY be discarded by the terminal and the ChoiceText element MAY be omitted. For interactivity with multiple choices, the ´ChoiceText´ element SHALL be instantiated for each ´SelectChoice´.	string
Picture	E4	NM/TM	0..1	In order to give to the end-user basic rendering on this interaction option, a picture MAY be provided. This element defines the way to access the picture to display and further information on how the terminal is expected to handle this picture For an interaction with one choice (e.g. an offer to purchase merchandise like a ringtone), the 'Picture' element under the SMSTemplate SHOULD be used to provide basic rendering of the interaction message and the 'Picture' element under the 'SelectChoice' element MAY be omitted and MAY be discarded by the terminal. Contains the following attributes: mimeType activateByClick override pictureURI Contains the following element: AlternativeURL	
mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that upon a user's click on this picture, the SMS interaction signaled in the "smsURI" attribute of the SelectChoice element SHALL be executed. In the case this attribute is omitted or set to "false", the execution of the sms interaction is launched by terminal UI specific means.	boolean
override	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that the 'ChoiceText' SHALL be ignored by terminals that are capable to display the related	boolean

				picture. Terminals that can't display the related picture SHALL ignore this attribute. It SHALL be omitted or set to "false" otherwise	
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	anyURI
Alternative URL	E5	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If terminal cannot access the indicated delivery session, the terminal can receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	anyURI
Picture	E3	NM/TM	0..1	Possibly in addition to the "Description" element a picture MAY be delivered to provide basic rendering of the interaction message. This element defines the way to access the picture to display Contains the following attributes: mimeType activateByClick pictureURI Contains the following element: AlternativeURL	
mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	The instantiation of this attribute is only allowed in the case the interaction provides only one choice. This attribute SHALL be set to "true" to signal that upon a user's click on this picture, the SMS interaction signaled in the 'smsURI' attribute of the 'SelectChoice' element SHALL be executed. It SHALL be omitted or set to "false" when no "Click" action on this picture is expected to launch the SMS interaction.	boolean
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When	anyURI

				ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	
Alternative URL	E4	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If a terminal cannot access the indicated delivery session, the terminal can receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	anyURI
EmailTemplate	E2	NO/TM	0..1	Contains attributes: relativePreference toHeader ccHeader bccHeader subjectHeader Contains the following elements: Description MessageBody Picture Note: the EmailTemplate is a media object set, although not encoded using the 'MediaObjectSet' generic structure.	
relativePreference	A	NO/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all the media object sets SHALL have mutually exclusive values of 'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	unsignedInt
toHeader	A	NM/TM	1	The e-mail recipient(s) as defined in [RFC 2822]	string
ccHeader	A	NO/TM	0..1	The e-mail cc-recipient(s) as defined in [RFC 2822]	string
bccHeader	A	NO/TM	0..1	The e-mail bcc-recipient(s) as defined in [RFC 2822]	string
subjectHeader	A	NO/TM	0..1	The e-mail subject header as defined in [RFC 2822]	string
Description	E3	NO/TM	0..N	Description of the Email Template, possibly in multiple languages. This is used to provide the	string

				end-user extra information regarding the Email message. The language is expressed using the built-in XML attribute xml:lang with this element.	
MessageBody	E3	NO/TM	0..1	The e-mail message body (text format defined in [RFC 2822] The value of this element SHALL be base64-encoded. Note: At least one of Subjectheader and MessageBody in an EmailTemplate SHOULD be present	base64Binary
Picture	E3	NM/TM	0..1	Possibly in addition to the "Description" element a picture MAY be delivered to provide basic rendering of the interaction message. This element defines the way to access the picture to display and further information on how the terminal is expected to handle this picture Contains the following attributes: mimeType activateByClick pictureURI Contains the following element: AlternativeURL	
mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that upon a user's click on this picture, the email interaction SHALL be executed. In the case this attribute is omitted or set to "false", the execution of the email interaction is launched by terminal UI specific means.	boolean
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	anyURI
AlternativeURL	E4	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If a terminal cannot access the indicated delivery session, the terminal can receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	anyURI

VoiceCall	E2	NO/TM	0..1	Contains the following attributes: relativePreference Contains the following elements: Description PhoneNumber PhoneNumberExtension Picture Note: the VoiceCallInteraction is a media object set, although not encoded using the 'MediaObjectSet' generic structure. It allows for voice call based interaction, by giving a description and/or a picture to the user and one or more telephone numbers that the user can call.	
relativePreference	A	NO/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all the media object sets SHALL have mutually exclusive values of 'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	unsignedInt
Description	E3	NM/TM	0..N	Text describing the interaction to the end user, possibly in multiple languages. The language is expressed using the built-in XML attribute xml:lang with this element. This text can e.g. describe the overall scope of the interaction, valid for all interaction options described below. It might e.g. also contain information about the prize of the voice call interaction. For an interaction with only one choice, the 'Description' element SHOULD be used to provide information regarding the interaction and the 'OptionText' element under the 'PhoneNumberExtension' element MAY be discarded by the terminal.	string
PhoneNumber	E3	NM/TM	1..N	Phone number to which the terminal initiates a voice call when the interactivity related to this InteractivityMediaDocument is triggered. The terminal SHALL prompt the user before actually making the call. If several phone numbers are present, the user SHALL be able to select the one to be used. A terminal with voice call capabilities MUST	anyURI

				support telephone URI [RFC 3966]. Further, a terminal with SIP capabilities MUST support SIP URI [RFC 3261].	
PhoneNumberExtension	E3	NM/TM	0..N	The 'PhoneNumberExtension' gives the possibility to associate to each declared phone number, that relate to the voice interaction, a picture and a textual description. If several phone numbers are proposed by the voice interaction, at least one ´OptionText´ element or one 'Picture' element SHALL be instantiated for each declared phone number, and the user SHALL be able to select the phone number to be used. If this element is instantiated, terminals SHALL ignore the 'PhoneNumber' element under the 'VoiceCall' element. For an interaction with one unique choice (i.e. a unique phone number), the 'PhoneNumberExtension' SHOULD NOT be instantiated and terminals MAY ignore the 'OptionText' and 'Picture' subelements. It contains the following attribute: phoneNumber It contains the following elements: OptionText Picture	
phoneNumber	A	NM/TM	1	Phone number to which the terminal initiates a voice call when the interactivity related to this InteractivityMediaDocument is triggered. The terminal SHALL prompt the user before actually making the call. A terminal with voice call capabilities MUST support telephone URI [RFC 3966]. Further, a terminal with SIP capabilities MUST support SIP URI [RFC 3261].	anyURI
OptionText	E4	NM/TM	0..N	Description of the interaction option, possibly in multiple languages. This is used to provide the end-user information on this interaction choice. The language is expressed using the built-in XML attribute xml:lang with this element. For an interaction with one unique choice, the 'Description' element SHOULD be used to provide information regarding the interaction and the ' OptionText' element MAY be omitted and it MAY be discarded by the terminal, if present.	string
Picture	E4	NM/TM	0..1	Possibly associated to each phone number a picture MAY be provided, in order to give to the end-user basic rendering on this interaction option, This element defines the way to access the picture to display and further information on how the terminal is expected to handle this picture Contains the following attributes: mimeType activateByClick	

				override pictureURI Contains the following element: AlternativeURL	
mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that upon a user's click on this picture, the voice call SHALL be executed, after the terminal has prompted the user to obtain his consent. In the case this attribute is omitted or set to "false", the execution of the voice call interaction is launched by terminal UI specific means.	boolean
override	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that the 'OptionText' SHALL be ignored by terminals that are capable to display the related picture. Terminals that can't display the related picture SHALL ignore this attribute. It SHALL be omitted or set to "false" otherwise	boolean
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	anyURI
AlternativeURL	E5	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If a terminal cannot access the indicated delivery session, the terminal can receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	anyURI
Picture	E3	NM/TM	0..1	Possibly in addition to the "Description" element a picture MAY be delivered to provide basic rendering of the interaction message.. This element defines the way to access the picture to display Contains the following attributes: mimeType activateByClick pictureURI Contains the following elements: AlternativeURL	

mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	The instantiation of this attribute is only allowed in the case the interaction provides only one choice. This attribute SHALL be set to "true" to signal that upon a user's click on this picture, the voice call interaction SHALL be executed, after the terminal has prompted the user to obtain his consent. In the case the interaction provides only one choice and this attribute is omitted or set to "false", the execution of the voice call interaction is launched by terminal UI specific means	boolean
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	anyURI
AlternativeURL	E4	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If a terminal cannot access the indicated delivery session, the terminal can receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	anyURI
WebLink	E2	NM/TM	0..1	This provides a reference to an external website. Contains attributes: - relativePreference - webURL Contains the following elements: - Description - Picture Note: the WebLink is a media object set, although not encoded using the 'MediaObjectSet' generic structure.	
relativePreference	A	NM/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all the media object sets SHALL have mutually exclusive values of	unsignedInt

				'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	
webURL	A	NM/TM	1	URL to an external website.	anyURI
Description	E3	NM/TM	0..N	Description of the WebLink, possibly in multiple languages. This is used to provide the end-user extra information regarding the WebLink. The language is expressed using the built-in XML attribute xml:lang with this element.	string
Picture	E3	NM/TM	0..1	Possibly in addition to the "Description" element, a picture MAY be delivered to provide basic rendering of the interaction message. This "Picture" element defines the way to access the picture to display and further information on how the terminal is expected to handle the picture Contains attributes: mimeType activateByClick pictureURI Contains the following element: AlternativeURL	
mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that the Web site signaled by the webURL attribute of the WebLink element SHALL be accessed upon user's click on the picture. In the case this attribute is omitted or set to "false", the execution of the Web interaction is launched by terminal UI specific means.	boolean
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	anyURI
AlternativeURL	E4	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If a terminal cannot access the indicated delivery session, the terminal can	anyURI

				receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	
AlternativeText	E2	NM/TM	0..N	Alternative Text to be displayed if none of the other media object sets is supported by the terminal , possibly in multiple languages. The language is expressed using the built-in XML attribute xml:lang with this element.	string
StreamingLink	E2	NM/TM	0..1	This provides a reference to an external unicast streaming server. Contains the following attributes: - relativePreference - streamingType - streamingURL Contains the following element: - Description - Picture Note: the StreamingLink is a media object set, although not encoded using the 'MediaObjectSet' generic structure.	
relativePreference	A	NM/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all the media object sets SHALL have mutually exclusive values of 'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	unsignedInt
streamingType	A	NM/TM	0..1	1- Generic RTSP to initialize RTP delivery 2- RTSP to initialize RTP delivery as per 3GPP-PSS (3GPP packet-switched streaming service) 3- RTSP to initialize RTP delivery as per 3GPP2-MSS (3GPP2 multimedia streaming services) 4-127 Reserved for future use 128-255 Reserved for proprietary use Note that in the case the 'streamingType' attribute has one of the values "1", "2" or "3", the "streamingURL" value MAY declare a resource that provides the Session Description information of the target RTSP session (including RTSP Control URL). In this latter case, the	unsignedByte

				"streamingURL" is an HTTP URL	
streamingURL	A	NM/TM	1	URL to an external unicast streaming server.	anyURI
Description	E3	NM/TM	0..N	Description of the StreamingLink, possibly in multiple languages. This is used to provide the end-user extra information regarding the StreamingLink. The language is expressed using the built-in XML attribute xml:lang with this element.	string
Picture	E3	NM/TM	0..1	Possibly in addition to the "Description" element, a picture MAY be delivered to provide basic rendering of the interaction message. This "Picture" element defines the way to access the picture to display and further information on how the terminal is expected to handle the picture Contains attributes: mimeType activateByClick pictureURI Contains the following element: AlternativeURL	
mimeType	A	NM/TM	0..1	MIME type of the Picture.	string
activateByClick	A	NM/TM	0..1	This attribute SHALL be set to "true" to signal that the streamingURL SHALL be accessed upon user's click on the picture. In the case this attribute is omitted or set to "false", the execution of the streaming interaction is launched by terminal UI specific means.	boolean
pictureURI	A	NM/TM	0..1	This is the location of the Picture to be retrieved in the file delivery session over the broadcast channel that is used also to convey the given Interactivity Media Document. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the Picture. When ALC/LCT is used for file delivery, this corresponds to the 'Content-Location' attribute in the 'File' element in the 'Access ' fragment that declares the Interactivity Media Documents file delivery session. As a result, the session used for file retrieval is the same session that carries this InteractivityMediaDocument.	anyURI
AlternativeURL	E4	NM/ TM	0..N	Alternative URI for receiving the picture via the interaction channel. If a terminal cannot access the indicated delivery session, the terminal can receive the picture by AlternativeURL. Multiple instances of the AlternativeURL MAY be instantiated for the purpose of server load distribution. In that case, the terminal SHALL randomly select one of them.	anyURI
RichMedia	E2	NO/TO	0..N	Each Rich Media element is a media object set describing rich media content either embedded in InteractivityMediaDocument or distributed as a	

				separate file in the FLUTE or ALC/LCT session. Contains the following attributes: relativePreference Contains the following elements: Description Capabilities RichMediaData RichMediaURI File When a RichMedia Solution is intended to be used for a media object set of a MediaObjectGroup, the Rich Media content file SHALL be signalled via a <RichMedia> element. In addition, in case backward compatibility with BCAST 1.0 terminals is sought, the Rich Media content file MAY be signalled also via a generic <MediaObjectSet> element, with a RelativePreference lower than <RichMedia> element, and with Content-Location or File equal to RichMediaURI or File (i.e. both <RichMedia> and <MediaObjectSet> are pointing to the same FLUTE orALC/LCT object). The session used for Rich Media retrieval is the same session that carries this InteractivityMediaDocument. Note: RichMedia is a media object set, although not encoded using the 'MediaObjectSet' generic structure.	
relativePreference	A	NM/TM	0..1	This attribute gives the relative preference of this media object set. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all the media object sets SHALL have mutually exclusive values of 'relativePreference'. If multiple media object sets are instantiated in this 'MediaObjectGroup ' then all of these elements SHALL have the 'relativePreference' attribute instantiated. If only a single media object set is instantiated in 'MediaObjectGroup' then the 'relativePreference' attribute MAY be instantiated for that element.	unsignedInt
Description	E3	NM/TM	0..N	Description of the Rich Media content, possibly in multiple languages. This is used to provide the end-user extra information regarding the Rich Media content. The language is expressed using the built-in XML attribute xml:lang with this element.	string
Capabilities	E3	NM/TM	1	Describes the type and complexity of Rich Media content the Rich Media Client has to deal with.	complexType as defined in [BCAST11-SG] section 5.1.2.4

					for Capabilities element child of RichMedia element in Access fragment
RichMediaData	E3	NM/TM	0..1	Inlined Rich Media content which SHALL be embedded either in a CDATA section or as a base64-encoded string. Contains the following attribute: encoding Either RichMediaURI or RichMediaData SHALL be instantiated.	string
encoding	A	NM/TM	0..1	This attribute signals the way rich media content is embedded: • It SHALL NOT be present when rich media content is embedded into a CDATA section. Note: binary data inside CDATA shall always be encoded in base64 • It SHALL be present and set to "base64" in case the whole rich media content is base64-encoded	string
RichMediaURI	E3	NM/TM	0..1	Uniquely identifies the Rich Media content file within the file delivery session. In case this external file is transported by FLUTE, this attribute MUST match the 'File' Content-Location value provided by the FDT instance(s) describing this file.	anyURI
File	E3	NM/TM	0..1	Present if RichMediaURI is instantiated and if ALC without FLUTE is besides used for the delivery of Rich Media content file.	complexType as defined in [BCAST11-SG] section 5.1.2.4 for the File element child of FileDescription in Access fragment.
PrivateExt	E1	NO/TO	0..1	An element serving as a container for proprietary or application-specific extensions.	
<proprietary elements>	E2	NO/TO	0..N	Any number of proprietary or application-specific elements that are not defined in this specification. These elements may further contain sub-elements or attributes.	

Table 40: Data structure of InteractivityMediaDocument

5.3.6.1.3 On the rendering

The terminal SHALL render the information contained in the instances of 'InteractivityMediaDocument' when these are completely and successfully retrieved from the file delivery stream and when the interactivity is scheduled to take place, i.e.

one or more InteractivityMediaDocuments are valid and are associated with the service or content that is being rendered at that moment. When instances of 'InteractivityMediaDocuments' with the same GroupID are valid at the same time, the terminal SHALL render those media objects in the document with the highest GroupPosition.

Upon parsing, or activation of, a received 'InteractivityMediaDocument' instance, the BCAST application SHALL identify the supported 'MediaObjectSet' instances according to:

- the interactivity technology(ies) supported, see section 5.3.6.1.4 below

AND

- supported language options for rendering the described interactivity, see section 5.3.6.1.6 below

and discard those instances that are not supported according to the two criteria above.

After having done this filtering step, the terminal obtains a list of languages supported for the interactive technologies it supports. From this list of languages, the terminal request the user to select one language, or perform this step automatically

Note: it is the responsibility of the network to ensure an instance of 'InteractivityMediaDocument' describes the interactivity in a given language for the given interactivity technology.

Furthermore the following applies:

- If multiple media object sets are instantiated in a 'MediaObjectGroup' the BCAST application SHALL render the media object set with the highest value of the 'relativePreference' attribute among the media object sets it supports.
- If only a single media object sets is instantiated in a 'MediaObjectGroup' the BCAST application SHALL render that media object if that media object set is supported.
- In the two previous cases, the BCAST application SHALL only select media object sets that correspond to the selected language or, alternatively, that apply to any language.
- If multiple 'MediaObjectGroups' are defined in the selected instance of 'InteractivityMediaDocument' the BCAST application SHALL go through all of them and render all the media object sets that are supported according to the three previous rules.
- The terminal SHALL support keeping track and rendering of several 'InteractivityMediaDocument' instances belonging to multiple groups (i.e. with different values of 'groupID') at the same time.

The InteractivityMediaDocument defines the actual details, which enable e.g. voting or ringtone ordering. The terminal SHALL be able to acquire and render the media objects attached to the 'InteractivityMediaDocument' without interrupting the acquisition and rendering of the 'regular' broadcast media stream.

5.3.6.1.4 MediaObjectSet parsing for interactivity technology selection

Information provided in the <MediaObjectSet> element is sufficient to determine whether the media object set is supported or not by the terminal. There is no need to open and parse the external file bundle. The terminal MAY take guidance of the following rules to determine this support :

- if <MediaObjectSet>'s external file is a single uncompressed file, the media object set SHOULD be seen as "supported" if :
  - the "Content-Type" attribute value of the <MediaObjectSet> is supported, and
  - if present, the 'PartType' s values of the 'Object' are all supported.
- if <MediaObjectSet>'s external file is an archive file, the media object set SHOULD be seen as "supported" if :
  - the "Content-Type" attribute value of each <Object> is supported, and
  - if present, the <PartType>s values in each <Object> are all supported.

5.3.6.1.5 InteractivityMediaDocument generation and parsing for language selection

The following table provides the list of elements that the terminal can use for language selection when parsing an instance of the <InteractivityMediaDocument>:

Element name	Language selection	Parent element
Description	Through the <xml:lang> attribute of this element	<SMSTemplate>, <EmailTemplate>, <VoiceCall>, <WebLink> and <RichMedia> elements
ChoiceText	Through the <xml:lang> attribute of this element	<SelectChoice> element of the <SMSTemplate> element.
MediaObjectSet	Through the <xml:lang> attribute of this element	<MediaObjectGroup> element.

Table 41: elements of <InteractivityMediaDocument> used for language selection

In order for the terminal to provide a single language choice to the user (or perform an automatic selection), the language(s) available for a given interactivity have to be declared in a consistent manner across all the <MediaObjectGroup> instances in an <InteractivityMediaDocument> instance that describes such interactivity. In order to enable this, the server SHALL comply with the following rule:

- The instance of the <MediaObjectGroup> that has its <startMediaFlag> set to true SHALL explicitly declare all available languages for the interactivity scenario represented by the <InteractivityMediaDocument> instance, that is to say
    - If the said <MediaObjectGroup> provides any instance of <SMSTemplate>, <EmailTemplate>, <VoiceCall>, <WebLink> or <RichMedia>, then the corresponding <Description> element SHALL be instantiated for each language
    - If the said <MediaObjectGroup> provides one or more instances of <MediaObjectSet>, there SHALL be at least one such instance per language option
- For each language declared as specified above
    - Each <Description> element as pointed by Table 41 that is to be used within its parent instance SHALL be instantiated for the said language
    - Each <ChoiceText> element as pointed the Table 41 that is to be used within its parent instance SHALL also be instantiated for the said language
    - For each instance of the <MediaObjectGroup> there SHALL be at least one instance of <MediaObjectSet> for the said language or, alternatively, an instance of <MediaObjectSet> configured for any language.
    - For any of the element pointed by Table 41 there SHALL NOT be any instance for a language that is not part of the available language options

Upon parsing the <InteractivitityMediaDocument> instance, the BCAST application identifies the available languages from the <MediaObjectGroup> instance that has the <startMediaFlag> set to true. The BCAST application MAY discard the languages that it does not support.

Upon activation of the <InteractivityMediaDocument>, the BCAST application SHALL select the media object sets for rendering that:

- are defined for the selected language or,
- are defined as applicable to any language

5.3.6.1.6 MediaObjectSet definition for some interactivity technologies

A media object set conveying an **MMS Message Template** conforming to [MMSTEMP] SHALL consist of the following:

- one GZIP archive file containing all the media objects (Message Template Definition, MMS presentation part, fixed/replaceable media objects).
- one <MediaObjectSet>, with Content-Type attribute set to “application/x-gzip”, and containing :
  - one “MTD” <Object>, with Content-Type attribute set to “application/vnd.omammsg-mtd+xml", and Start attribute set to “true”.
  - zero or one “MMS presentation part” <Object>, with Content-Type attribute set to “application/smil". If <MediaObjectSet> contains MMS presentation part, the sub-folder(s) SHALL NOT be used in <Content-Location> since MMS-SMIL cannot support sub-folder(s).
  - one <Object> per other bundled file, if any (fixed/replaceable media objects).

Note: If the end user decides to interact as triggered by Media Object Set of type **MMS Message Template**, it implies that the Terminal SHALL be able to execute any interaction over the Interaction channel by sending the MMS (the filled-in MMS Template).

A media object set conveying an **XHTML MP bundle** conforming to [XHTMLMP11] SHALL consist of the following:

- one GZIP archive file containing all the media objects (e.g. XHTML MP page(s), external ECMAScript MP files, external WAP CSS stylesheets, audio/visual media objects…).
- one <MediaObjectSet>, with Content-Type attribute set to “application/x-gzip”, and containing :
  - one “XHTML MP” <Object>, with Content-Type attribute set to “application/vnd.wap.xhtml+xml" and Start attribute set to “true”.
  - one <Object> per other bundled file, if any (that may be additional XHTML MP pages).

Note**:** If the end user decides to interact as triggered by Media Object Set of type **XHTML MP bundle**, it implies that the Terminal SHALL be able to execute any interaction over the Interaction channel by executing HTTP requests (following the hyperlinks present in XHTML). Further, if the Terminal supports SMS-based messaging, the Terminal SHALL be able to support “sms:”-URI scheme as defined in section 5.3.6.1 and consequently be able to perform SMS-based interaction over the Interaction channel.

A media object set conveying a **3GPP PSS SMIL bundle** conforming for the presentation part to [3GPP TS 26.246]) SHALL consist of the following:

- one GZIP archive file containing all the media objects (SMIL presentation, audio/visual media objects…).
- one <MediaObjectSet>, with Content-Type attribute set to “application/x-gzip”, and containing :
  - one “3GPP PSS SMIL” <Object>, with Content-Type attribute set to “application/smil" and Start attribute set to “true”.
  - one <Object> per other bundled file, if any.

Note: If the end user decides to interact as triggered by Media Object Set of type **3GPP PSS SMIL bundle**, it implies that Terminal SHALL be able to execute any interaction over the Interaction channel by executing HTTP requests (following the hyperlinks present in SMIL). Further, if the Terminal supports SMS-based messaging, the Terminal SHALL be able to support “sms:”-URI scheme as defined in section 5.3.6.1 and consequently be able to perform SMS-based interaction over the Interaction channel.

A media object set conveying a **3GPP2 MSS SMIL bundle** conforming for the presentation part to [3GPP2 C. S0050-B]) SHALL consist of the following:

- one GZIP archive file containing all the media objects (SMIL presentation, audio/visual media objects…).
- one <MediaObjectSet>, with Content-Type attribute set to “application/x-gzip”, and containing :
  - one “3GPP2 MSS SMIL” <Object>, with Content-Type attribute set to “application/smil" and Start attribute set to “true”.
  - one <Object> per other bundled file, if any.

Note: If the end user decides to interact as triggered by Media Object Set of type 3GPP2 MSS SMIL bundle, it implies that Terminal SHALL be able to execute any interaction over the Interactive Channel by executing HTTP requests (following the hyperlinks present in SMIL). Further, if the Terminal supports SMS-based messaging, the Terminal SHALL be able to support “sms:”-URI scheme as defined in section 5.3.6.1 and consequently be able to perform SMS-based interaction over the Interactive Channel.

See Appendix C for some informative examples of <MediaObjectSet> elements.

5.3.6.1.7 Using URI scheme “sms:”

Terminals that support SMS-based messaging and/or that support XHTML-based Media Object Sets or Rich Media Solutions allowing hyperlinks SHALL support the “sms:” URI scheme as specified in [URI-Schemes] as a valid scheme for hyperlinks.

5.3.6.1.8 Service Interaction using MMS Message Template

This section describes how to retrieve and use MMS Message Template for Service Interaction.

The terminal SHALL retrieve MMS Message Template from InteractivityMediaDocument (refer to 5.3.6.1). The terminal MAY retrieve MMS Message Template from MMS.

The terminal SHOULD store MMS Message Templates in its storage area after retrieval.

The terminal MAY use Application ID described in [MMSCONF] to launch client software, which handles MMS Message Template (MMS Message Template Client), in the case that the Template is retrieved from MMS.

5.3.7 Service related interaction and feedback using Rich Media

To support full layout and timing model including the scripting support for Service Interactivity, Rich Media Solutions are applied.

When Rich Media Solution provides the service related interaction, it is provided so that the main components of service are amended with a RMS data that is delivered before or along with the main component. This allows those terminals not supporting the RMS to receive and render the basic service without the added RMS data.

5.3.7.1 Signaling of RMS component being a part of service

The RMS component is delivered via a stream delivery session along with the main service. This is signalled in BCAST Service Guide via the ‘Access’ fragment so that the Session Description associated with ‘Access’ fragment signals also the presence of RME stream. In case OMA RME [RME] and 3GPP DIMS [3GPP TS 26.142] the details of Session Description signalling are defined in section 7.3.3 or [3GPP TS 26.142].

5.3.7.2 Broadcast delivery of RMS component

In case OMA RME [RME] or 3GPP DIMS [3GPP TS 26.142] the stream delivery of RMS component over broadcast access SHALL be using RTP encapsulated DIMS Units according to section 7.3 [3GPP TS 26.142].

5.3.7.3 Interactive delivery of RMS component

In case OMA RME [RME] or 3GPP DIMS [3GPP TS 26.142] the stream delivery of RMS component over interactive access SHALL be using RTP encapsulated DIMS Units according to section 7.3 [3GPP TS 26.142].

5.3.8 Service Interaction launch and feedback

The terminal SHALL launch MMS Message Template Client according to the timing described in InteractivityMediaDocument , in a similar way to the other Service Interaction methods.

MMS Message Template Client SHALL create Multimedia Message (MM) according to the process defined in MMS Message Template Definition (MTD) [MMSTEMP].

After creating the resulting MM, MMS Message Template SHOULD send the Message to Service Application address defined in MTD.

5.3.8.1 Broadcast delivery of InteractivityMediaDocuments

The broadcast delivery of the instances 'InteractivityMediaDocument' and any associate files has the following characteristics and constraints. For the delivery the network SHALL

- use FLUTE file delivery session containing at least one FDT Instance,
- list all the delivered files in every instance of FDT,
- use the string "application/vnd.oma.bcast.imd+xml" as the value of 'Content-Type' for every instance of 'InteractivityMediaDocument' in every FDT Instance and
- use the following convention for allocating the 'Content-Location' values for the instances of the 'InteractivityMediaDocument': <GroupID>:<GroupPosition> where the
- <GroupID> stands for the group identifier and <GroupPosition> for the group position represented by the instance of 'InteractivityMediaDocument'.

Furthermore in the case of broadcast delivery the network SHALL use the string "oma:bcast1.0:imd:" as the prefix of the interactivity media group identifier (GroupID).

5.3.8.2 Interactive delivery of InteractivityMediaDocuments

5.3.8.2.1 Transport protocols

There are the two following mechanisms for delivering InteractivityMediaDocuments to the terminal using the interactive channel:

- using HTTP as the transport the terminal specifically requesting the InteractivityMediaDocuments from the network and
- using OMA PUSH the network pushing the InteractivityMediaObjects to the terminals.

If the terminal supports the interaction channel, the terminal SHALL support the former and additionally if the terminal supports OMA PUSH, the terminal SHALL also support the latter.

When the InteractivityMediaDocuments are delivered using OMA PUSH the content type SHALL be set to "application/vnd.oma.bcast.imd+xml".

5.3.8.2.2 InteractivityMediaDocument request messages

When the terminal requests InteractivityMediaDocuments from the network, the terminal SHALL use HTTP POST

with the following syntax : "POST <interactivityMediaURL> HTTP/1.1\r\n<InteractivityMediaDocumentRequest>" where <interactivityMediaURL> denotes the destination for the HTTP requests as signaled in the 'interactivityMediaURL' attribute of the 'InteractivityData' fragment representing the interactivity in question, see section 5.1.2.10 of [BCAST11-SG].. Both the HTTP POST request and the corresponding HTTP response SHALL also contain the following HTTP header fields:

- 'Content-Length',
- for request message: 'Content-Type' which SHALL be set to "text/xml".

- for response message: 'Content-Type' which SHALL be set to "multipart/mixed" and
- 'Host' in case the 'Request-URI' is not in the absolute form specified in [RFC 2616].

The XML structure in Table 42 defines the syntax for the 'InteractivityMediaDocumentRequest' placed into the payload of the HTTP POST request.

The HTTP response of the HTTP POST request response message SHALL be of type "multipart/mixed".

The first body part of the multipart in the response:

- SHALL contain one 'InteractivityMediaDocumentResponse' XML document as defined in Table 43.
- SHALL include Content-Type header set to 'text/xml'

Other body parts may follow the first body part in the response. In that case each body part:

- SHALL contain one file representing the full set of media objects associated to exactly one <MediaObjectSet> of a MediaObjectGroup of the returned InteractivityMediaDocument. This file SHALL be either one uncompressed media file (e.g. 3GP file) being the media object itself, or one GZIP archive file containing the compressed media objects, as described in section 5.3.6.1.2.
- SHALL include Content-Location header set to Content-Location attribute value of <MediaObjectSet> element.
- SHALL include Content-Type header, set to actual MIME type of uncompressed media file (e.g. 'video/3gpp') or to 'application/x-gzip'if the media objects are carried in a GZIP archive.

In case the response message does not contain all the files associated with the 'InteractivityMediaDocuments' contained in the response message, the terminal MAY use HTTP GET to retrieve these missing files.

Name	Type	Category	Cardinality	Description	Data Type
InteractivityMediaDocumentRequest	E			The request to be used by the terminal to request InteractivityMediaDocuments. Contains the following attributes: requestID Contains the following elements: UserID DeviceID GroupID	
requestID	A	O	0..1	Identifier for the InteractivityMediaDocument request message.	unsignedInt
UserID	E1	O	0..N	The user identity known to the BSM. Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	O	0..N	A unique device identification known to the	string

				BSM. Contains the following attributes: type	
type	A	M	1	Specifies the type of Device ID. Allowed values are 0 – reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
GroupID	E1	M	1	ID of the requested group of InteractivityMediaDocument, globally unique The GroupID is carried in BCAST SG fragment called InteractivityData	anyURI

Table 42: Structure of Interactivity Media Document Request

Name	Type	Category	Cardinality	Description	Data Type
InteractivityMediaDocumentResponse	E			The response to the 'InteractivityMediaDocumentRequest' message. Contains the following attributes: requestID statusCode Contains the following elements: InteractivityMediaDocument	
requestID	A	O	0..1	Identifier for the corresponding InteractivityMediaDocument request message.	unsignedInt
status Code	A	M	1	The overall outcome of the request, according to the return codes defined in section 5.11.	unsignedByte
InteractivityMediaDocument	E1	M	0..1	The InteractivityMediaDocument as specified in 5.2.6.1. This element SHALL NOT be instantiated in case the statusCode attribute is present and set to a value different from '0'. In any other case, it SHALL be instantiated."	complexType

Table 43: Structure of Interactivity Media Document Response

5.4 Personalization/Support for User-based Profiles and Preferences

5.4.1 User-based Profiles over Broadcast Channel

The BCAST Enabler enables targeted reception through delivery of user-based profiles over the broadcast channel using the Service Guide. The "TargetUserProfile" element of Service Guide SHALL be used for that purpose.

Exact terminal behavior for interpreting the "TargetUserProfile" is not specified. However, the terminal MAY be able to filter the Service Guide based on the "TargetUserProfile".

5.4.2 Communicating the End User Preferences to Network

The terminal MAY communicate the End User preferences to the network using the scheme defined in this section. Both the Terminal and the network MAY support the scheme. The behavior of the network and any subsequent actions beyond providing the End User preferences are not specified in BCAST Enabler.

The data structure for communicating the End User preferences from terminal to network is as follows:

Name	Type	Category	Cardinality	Description	Data Type
EndUserPreferences	E	O		The end user preferences signalled to the Service Provider Contains the following elements: UserID Preference	
UserID	E1	M	1	User Identity known to the BSM. It describes The identification of the end user whose preferences are described here. Contains the following attribute: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
Preference	E1	M	1..N	The attribute-value pair describing an individual preference. NOTE: the exact attribute for preference shall be defined by service or content provider. Contains the following attributes: attribute value	
attribute	A	M	1	Attribute being described	string
value	A	M	1	Value of the attribute	string

Table 44: Structure of End User Preference Message

The above data structure SHALL be instantiated as XML instance according to XML Schema [BCAST10-XMLSchema-Userpreference].. The XML instance in turn SHALL be communicated from terminal to network by HTTP POST. For confidentiality, HTTPS based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246] MAY be used.

5.5 Charging

This section specifies the use of OMA Charging Enabler to realize the charging of OMA Mobile Broadcast Services. OMA Charging Enabler defines a set of interfaces to allow other Enablers to access the charging functionality. The interfaces are

specified in [OMA Charging AD]. This section defines how, when and by whom the charging is triggered and which functional entity invokes the charging using the interface of OMA Charging Enabler. This section also defines the data that will be exchanged within the charging event and maps them to OMA Charging Data Elements defined in [OMA Charging DDS].

5.5.1 Chargeable Events in the Scope of the BCAST Enabler

Chargeable event is a service related event that has taken place, and can be specified and recorded. This section identifies chargeable events in the scope of the OMA Mobile Broadcast Services technical specification. It should be noted that chargeable events can also occur for example in a BCAST Distribution System or in other entities of the OMA BCAST Architecture to record the usage of the mechanisms that they provide (e.g. distribution and protection mechanisms) but these chargeable events are not specified in this document.

Not all chargeable events lead necessarily to a *charging event*, i.e. the sending of charging information to the Charging Enabler for further processing. The events that are actually charged for can depend on the implementation. Therefore, the list in this section should be regarded as a list of events that potentially trigger charging events.

Chargeable Event	Section where defined	Source of the event
Subscription-Based Charging		
Subscribe/Purchase Request End-user subscribes or purchases a certain service based on information received through the Service Guide.	5.1.5, 5.1.6 [BCAST11-Architecture] 5.4.6.1	BSM
Subscription Update In case of open-ended subscriptions, the BSM may need to generate charging information from time to time until the subscription is cancelled.	5.1.5, 5.1.6 [BCAST11-Architecture] 5.4.6.7	BSM
Unsubscribe Request Open-ended subscriptions, and possibly other subscriptions, are valid until they are cancelled by the end-user. Depending on the contract, they may also have to be cancelled (and renewed by issuing a new order request) when the price per subscription period changes.	5.1.6.7 [BCAST11-Architecture] 5.4.6.8	BSM
Consumption-Based Charging		
Token Purchase Request Token Purchase Request can be used to order tokens that can be used in consumption-based charging models. As to calls to the Charging Enabler, tokens can be used in two ways: • Pre-paid tokens: When the BCAST client orders tokens, BSM calls the Charging Enabler and tokens are charged as they are ordered before the actual service delivery • Post-paid tokens: When the BCAST client orders tokens, if the subscriber uses online charging, a respective credit reservation is made. In the offline case, a positive credit response is assumed implicitly. Used service units are reported to the Charging Enabler only when the BCAST client reports used tokens to the BSM. **NOTE!** It is important to note here that the prepaid/postpaid distinction is independent of the type of the subscriber's account in the Charging Infrastructure (i.e. pre-paid or post-paid subscription).	5.1.5, 5.1.6 [BCAST11-Architecture] 5.4.6.9	BSM
Service Interaction		
Interactive Service Ordering The end-user reacts to an interaction pointer and requests for an additional service, such as voting or related value-added content. Charging for interactive service ordering is in the BCAST Enabler's scope only in simple cases where the additional service can be identified with a simple combination of a purchase item ID and purchase option or	[BCAST11-Architecture] 5.4.5	BSI-G

equivalent. In more complex cases, it is likely that service interaction is redirected to a separate application the charging of which is outside the scope the BCAST Enabler.

Table 45: List of chargeable events

5.5.2 When to Trigger Calls to the Charging Enabler

This section identifies when charging information needs to be sent to the Charging Enabler in relation to the different chargeable events.

In the case of Subscription/Purchase Request, Subscription Update, Unsubscribe, Token Purchase Request, or Interactive Service Ordering, the high-level charging flow is the following:

- When the request arrives, before service delivery
  - The BCAST Enabler implementation may know based on pre-configured information or through a query to an external system whether online or offline charging interface should be used towards the Charging Enabler. It this information is not available, the BCAST Enabler may assume online and make the first request to the online (CH-2) interface, which may return an error code indicating that offline should be used.
  - If online charging is to be used, send an Initial Request using CH-2 to make a credit reservation
- During service delivery
  - In the online case, Interim Requests to CH-2 may be needed if the quota granted in the previous step(s) is depleted
- After service delivery
  - If the online-offline determination outcome was offline, report service usage using CH-1
  - If the online-offline determination outcome was online, report the final service usage step using Termination Request of CH-2

5.5.3 BCAST-related Information in Charging Messages

This section specifies how charging information for BCAST services is mapped to OMA Charging Data Elements of the Charging Enabler as specified in [OMA Charging DDS].

5.5.3.1 Subscription-Based Charging: Subscribe/Purchase, Subscription Update, Unsubscribe Request

BCAST field name or value constants	Type	OMA Data Elements in Charging interface	Description
Value: BCAST@openmobilealliance.org	String	Service Context Id	Fixed value to identify the service specification in the context of which the charging events must be interpreted.
Values: SUBSCRIBE, SUBSCRPITION_UPDATE, UNSUBSCRIBE (for Subscription-Based Charging)	String	Service Identifier	Identifies more precisely the type of service within the context defined by the Service Context Id. NOTE: Different from Service ID.
Field: UserID	String	Subscription Id Data	The globally unique identity of the subscriber
Field: type attribute under UserID	unsignedByte	Subscription Id Type	Type of the subscriber identity (e.g. MSISDN, IMSI, SIP_URI)
Field: PurchaseItemID	anyURI	Service Key	The globally unique ID of the Service Guide fragment that describes what the end-user has

			ordered or cancelled. It should be noted that a particular Service Item may be available through several Purchase Items (e.g. because of bundling and several order options or purchase channels).
Values: depending on context	String	Correlation Id	Depending on the deployment, different identifiers can be used here to enable correlation between the charging events generated by BCAST service entities and charging events generated by other entities (such as distribution entities or content protection mechanisms).
Field: Price	decimal	Unit Value, Value Digits, Exponent	Amount to be reserved/debited from the end-user's account. In case of reservation, the listed data elements must be included in the requested service units data element. In case of reporting units to be debited, the used service units data element must be used in the charging interface.
Field: currency	String	Currency Code	Numeric representation of Currency Code as specified in ISO4217
Field: DeviceID	String	User Equipment Info Value	A unique device identification known to the BSM
Field: type attribute under DeviceID element	unsignedByte	User Equipment Info Type	The type of the unique device identification (e.g. IMEI, MEID).

Table 46: Mapping table for Subscription based Charging

5.5.3.2 Consumption-Based Charging: Token Purchase Request

BCAST field name or value constants	Type	OMA Data Elements in Charging interface	Description
Value: BCAST@openmobilealliance.org	String	Service Context Id	Fixed value to identify the service specification in the context of which the charging events must be interpreted.
Values:TOKEN_PURCHASE (for Consumption-based charging)	String	Service Identifier	Identifies more precisely the type of service within the context defined by the Service Context Id. NOTE: Different from Service ID.
Field: UserID	String	Subscription Id Data	The globally unique identity of the subscriber
Field: type attribute under UserID	unsignedByte	Subscription Id Type	Type of the subscriber identity (e.g. MSISDN)
Field: PurchaseItemID	anyURI	Service Key	The globally unique ID of the Service Guide fragment that represents the token product.
Values: depending on context	String	Correlation Id	Depending on the deployment, different identifiers can be used here to enable correlation between

			the charging events generated by BCAST service entities and charging events generated by other entities (such as distribution entities or content protection mechanisms).
Field: currency	String	Currency Code	Numeric representation of Currency Code as specified in ISO4217. If the Currency Code element is present, the Unit Value, Value Digits and Exponent elements below will be used. If the CurrencyCode element is not given, the Service Specific Units element below will be used.
Field: Price	decimal	Unit Value, Value Digits, Exponent	Amount to be reserved/debited from the end-user's account. These sub-elements of the Money data element are used in the charging interface if the BCAST Enabler is able to determine the price of the request (either in monetary or non-monetary terms). In case of reservation for post-paid tokens, the listed data elements must be included in the requested service units data element. In case of reporting used post-paid tokens or ordering pre-paid tokens, the used service units data element must be used in the charging interface.
Field: Price	decimal	Service Specific Units	Amount of tokens to be reserved/debited from the end-user's account. The Service specific units data element is used in the charging interface if price determination is left to the Charging Enabler. In case of reservation for post-paid tokens, the listed data elements must be included in the requested service units data element. In case of reporting used post-paid tokens or ordering pre-paid tokens, the used service units data element must be used in the charging interface.
Field: DeviceID	String	User Equipment Info Value	A unique device identification known to the BSM
Field: type attribute under DeviceID element	unsignedByte	User Equipment Info Type	The type of the unique device identification (e.g. IMEI, MEID)

Table 47: Mapping table for Consumption based Charging

5.5.3.3 Service Interaction

Service interaction pointers may lead the end-user to a completely different service from BCAST (e.g. to MMS sending), and these external services usually have their own charging which is not in the scope of this specification. This specification, however, caters for cases where the additional interactive service does not have charging specified separately and the price of the interaction transaction is available to the BCAST Enabler or some part of the BCAST Enabler implementation can determine the price. Also cases where price determination is delegated to the Charging Enabler but price can be calculated simply based on the InteractivityDataId accessed can be supported.

BCAST field name or value constants	Type	OMA Data Elements in Charging interface	Description
Value: BCAST@openmobilealliance.org	string	Service Context Id	Fixed value to identify the service specification in the context of which the charging events must be interpreted.
Value:SERVICE_INTERACTION (for Service Interaction)	string	Service Identifier	Identifies more precisely the type of service within the context defined by the Service Context Id. NOTE: Different from Service ID.
Field: UserID	string	Subscription Id Data	The globally unique identity of the subscriber
Field: type attribute under UserID	unsignedByte	Subscription Id Type	Type of the subscriber identity (e.g. MSISDN)
Field: InteractivityDataID	anyURI	Service Key	The globally unique ID of the Service Guide fragment that describes what the end-user has accessed.
Values: depending on context	string	Correlation Id	Depending on the deployment, different identifiers can be used here to enable correlation between the charging events generated by BCAST service entities and charging events generated by other entities (such as distribution entities or content protection mechanisms).
Field: Price	decimal	Unit Value, Value Digits, Exponent	Amount to be reserved/debited from the end-user's account. In case of reservation, the listed data elements must be included in the requested service units data element. In case of reporting units to be debited, the used service units data element must be used in the charging interface.
Field: currency	string	Currency Code	Numeric representation of Currency Code as specified in ISO4217
Field: DeviceID	String	User Equipment Info Value	A unique device identification known to the BSM
Field: type attribute under DeviceID element	unsignedByte	User Equipment Info Type	The type of the unique device identification (e.g. IMEI, MEID)

Table 48: Mapping table for Service Interaction

5.5.4 Exchange of charging data among systems

It can be assumed that entities that are reflected in the BCAST architecture may need to exchange business related data.

However, the BCAST enabler does not specify a defined format for the exchange of charging data between Broadcast Service Providers, or between a Broadcast Service Provider and a Content Provider.

5.6 Mobility

The location of the Terminal may change over time. Different usage scenarios typically involve different rates of change in the location of the Terminal. However, what is significant in the change is not the speed of the change but the fact that the change in the location of Terminal may involve a change in the set of available Mobile Broadcast Services. Along with the change in the location of Terminal the currently available transmission may become unavailable due to changing radio reception conditions. Alternatively, the change in Terminal's location may move the Terminal away from its currently available Broadcast Service Area. In both cases the current set of available Mobile Broadcast Services may change.

There are two cases to consider in the context of mobility and Mobile Broadcast Services. Firstly, the terminal may be currently receiving a Mobile Broadcast Service which is affected by the change. Secondly, the terminal may only be receiving and updating the Service Guide that is related to the Service, affected by the change. Both cases are exceptions in a normal service consumption process and require handling. In the former case, the change affects the current access to the Service while in the latter case the change affect to the possible ways of accessing the Service Guide.

This section provides normative specification for the network side (Service Guide function) to support the mitigation of mobility effects. On the network side the support for broadcast mobility is centralized in the Service Guide function. The methods outlined in the following sections are supported by the SG-D and MAY be used in the transmitted Service Guide.

5.6.1 Specifying Alternative Accesses for a Service

Service Guide allows describing several Accesses for a particular Service. The Service Guide can declare a Service in the Service Guide that MAY have several Accesses associated with it. In case the selected Access becomes unavailable due to mobility (or some other reason), the Terminal MAY continue accessing the Service via another Access given that the other Access semantically represents same or similar component of the Service.

5.6.2 Global Identification of Services and Content

The Service Guide MAY declare global identification for both Service (attribute GlobalServiceID in Service Fragment) and Content (attribute GlobalContentID in Content Fragment). Two fragments with the same global identifiers describe the same asset. How the terminal uses the global service identifier or the global content identifier is out of scope of this specification.

5.7 Broadcast Roaming

Broadcast Roaming allows a user to receive Broadcast Services from a Mobile Broadcast Service Provider different from his Home Mobile Broadcast Service Provider. This can happen, for example, when the user is not able to access the services provided by Home Mobile Broadcast Service Provider. In that case the Broadcast Roaming enables the user to receive Broadcast Services from another Mobile Broadcast Service Provider independent on the underlying BCAST Distribution System.

The Mobile Broadcast Services (BCAST) 1.0 Enabler enables the Broadcast Roaming through the use of various functions of the enabler: through the Service Guide, through roaming signaling between Terminal and Visited Mobile Broadcast Service Provider, through roaming signaling between Visited Mobile Broadcast Service Provider and Home Mobile Broadcast Service Provider and through the Terminal Provisioning function. The following gives the overview on how these functions relate in the context of Broadcast Roaming:

- Service Guide Delivery Descriptors (SGDD) within the Service Guide declare the existence and the availability of Service Guide fragments. The SGDD allows the Terminal to deduce which fragments are associated with

which Mobile Broadcast Service Provider (through use of BSMFilterCodes). Related to this signaling, there are visibility rules that the terminals are expected to comply with. Further, SGDD enables a method to convey points of contact which the visiting terminals can contact in case Broadcast Roaming is needed. This aspect of Broadcast Roaming is normatively specified within the specification of SGDD, in section 5.4.1.5 of [BCAST11-SG].

- Terminal Provisioning enables the Home Broadcast Service Provider to maintain terminal-resident elements used by the roaming function. These elements include the list of Service Providers (their BSMFilterCodes) affiliated with the terminal and the entry details of preferred roaming contact points. The entry details of the preffered roaming contact points consists of the following:
  - a list of preferred Visited Mobile Broadcast Service Provider for the BCAST service. This indicates to the terminal to which of the BDSes the terminals has to attach in order of priority.
  - the address of the server that the terminal can send roaming requests in the case terminal does not find any other entry points within the Service Guide signaling.
  - elements that include parameters that determines whether the terminal initiates the service provisioning requests to Visited BSM or to Home BSM.
  - elements that include parameters that can be used to control terminal behaviour in the context of Broadcast Roaming: an element that controls whether roaming requests should always be sent to Home BSM
  - an element that determines terminal behavior for fragments that are not associated with any BSMSelector.

  These aspects of Broadcast Roaming are normatively specified within this document, Appendix G (Management Object).

  In addition to using Terminal Provisioning, the management information in Appendix G can be pre-configured in the Terminal, or can be conveyed to the terminal by some other means which are out of scope of this specification.

- Roaming Rule request and response messages between Terminal and BSM associated with Home and/or Visited Mobile Broadcast Service Provider allow Terminals to request and Mobile Broadcast Service Providers to provide the visibility constraints defined by Roaming Rules. This aspect of Broadcast Roaming is normatively specified within this document (section 5.7.1). The contact points for the request messages are signaled within the SGDDs – that aspect of Broadcast Roaming is normatively specified within the specification of SGDD, in section 5.4.1.5 of [BCAST11-SG].
- Specific Service Provisioning messages that enable Terminal to request for service, request for Tokens and request for renewal of subscriptions. In the context of Broadcast Roaming, the Service Provisioning messages sent by the Terminal trigger roaming message exchange between Home and Visited Mobile Broadcast Service Provider. This aspect is normatively specified within this document (section 5.1). Subsequent of successful Roaming Service Response, LTKMs can be delivered to the terminal (via Push LTKM with Smartcard profile or Trigger with DRM profile). The LTKM acquisition is not covered in this document as it is a Service and Content protection procedure.
- The roaming messages between Home and Visited Mobile Broadcast Service Providers allow the either the Home or Visited Mobile Broadcast Service Provider to initiate the roaming as a reaction to initial user roaming request. This aspect of Broadcast Roaming is normatively specified within this document (section 5.7.2).
- The informative walk-through of Broadcast Roaming is given in this document (Appendix E).

Broadcast Roaming in BCAST 1.0 allows a Terminal to be associated with multiple Home BSMs (and hence multiple BSMFilterCodes). While this allows a model wherein the Terminal is associated with different service providers, the primary use of this functionality will be of specifying different subscription types per a single provider.

Roaming agreements between Home Mobile Broadcast Service Provider and Visited Mobile Broadcast Service Provider and the related trust relationship are out of BCAST scope.

Both the Network and the Terminal MAY support Broadcast Roaming. If the Network supports Broadcast Roaming, backend interfaces for roaming SHALL also be supported.

Note: playback of protected content recorded while roaming may have limitations due to the inability of the terminal to retrieve rights once back in its home network. Such use case may not be supported until a later release of the present specification.

5.7.1 Roaming messages between Terminal and BSM

Terminal uses the RoamingRuleRequest to request the RoamingRules associated with BSMSelector (identified by the id of the selector). As a response, the Terminal receives RoamingRuleResponse that carry the RoamingRules.

The XML schema for these messages is defined in [BCAST11-XMLSchema-Roaming-frontend].

5.7.1.1 RoamingRuleRequest

Name	Type	Category	Cardinality	Description	Data Type
RoamingRuleRequest	E			Request message of Roaming Rules. Contains the following elements: UserID RequestEntry	
UserID	E1	M	1	A unique ID that SHALL be used to identify the terminal in BCAST service area of both the Home Mobile Broadcast Service Provider and Visited Mobile Broadcast Service Provider. Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
RequestEntry	E1	M	1..N	This element represents a request for roaming rules associated with the given 'HomeBSMFilterCode' and 'VisitedBSMFilterCode' instances. It is expected that the terminal will request rules separately (i.e. with different 'RequestEntry' instances) for each Visited BSM of interest. However, in case the terminal provides more than one instance of 'VisitedBSMFilterCode' in a	

				'RequestEntry' instance, the server SHALL assume that the 'HomeBSMFilterCode' instance applies for all the given 'VisitedBSMFilterCode' of the same 'RequestEntry' instance. As of BCAST 1.0, the terminal SHALL provide one and only one instance of the 'RequestEntry' element in a given 'RoamingRuleRequest' message. That instance MAY include an instance of the child 'HomeBSMFilterCode' element that, when instantiated, SHALL represent the Home BSM the terminal is affiliated with. Contains the following elements: HomeBSMFilterCode VisitedBSMFilterCode	
HomeBSMFilterCode	E2	M	0..1	The code that specifies the Home BSM the terminal is affiliated with. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSMFilterCode	E2	M	1..N	The code that specifies the Visited BSM. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]

Table 49: Structure of RoamingRuleRequest Message

5.7.1.2 RoamingRuleResponse

Name	Type	Category	Cardinality	Description	Data Type
RoamingRuleResponse	E			Response message of Roaming Rules Contains the following attribute: globalStatusCode Contains the following element: ResponseEntry	
globalStatusCode	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11. This attribute also governs the way the 'itemwiseStatusCode' attribute is instantiated in this response: If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each 'ResponseEntry'	unsignedByte

				If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'ResponseEntry' If this attribute is not present, there was an error concerning one or more 'RequestEntry' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each 'ResponseEntry'.	
ResponseEntry	E1	M	0..N	Entry containing response to each requested Visited BSM. This element SHALL be instantiated in case of successful completion of the related request. Contains the following attribute: itemwiseStatusCode exclusive Contains the following element: VisitedBSMFilterCode HomeBSMFilterCode RoamingRule	
itemwiseStatusCode	A	M	0..1	Specifies a status code of each PurchaseItems using GlobalStatusCode defined in the section 5.11.	unsignedByte
exclusive	A	O	0..1	Indicates whether the rules delivered in this response are exclusive when executed. If "true", the rules are exclusive and terminal that accesses fragments covered by these rules (i.e. associated with the BSMFilterCode declared in the 'VisitedBSMFilterCode' instance) SHALL NOT access fragments associated with any other BSM. This means that – if the terminal selects a Visited BSM for which the rule are marked with the value "true" of this attribute the Terminal SHALL only use the SG fragments of the selected BSM and not mix SG fragments from other BSM even if the Terminal already got access to those. If "false", the rules are not exclusive and, upon selection of the related Visited BSM, the terminal can access fragments associated with any other BSM. Default value of this attribute is "false".	boolean
VisitedBSMFilterCode	E2	M	1	The code that specifies the Visited BSM for which this ResponseEntry applies. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
HomeBSMFil	E2	M	0..N	The code that specifies the Home BSM for which	complexTyp

terCode				this ResponseEntry applies. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'. Note that a RoamingRule can apply to several Home BSM for a given Visited BSM. In case no HomeBSMFilterCode instance is given, the terminal SHALL interpret the associated RoamingRule as applicable to any Home BSM. In case the BSM instantiates this element, it SHALL provide one instance corresponding to the 'HomeBSMFilterCode' provided by the terminal in the related 'RoamingRuleRequest' message.	e as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
RoamingRule	E2	M	1..N	Entry specifying the RoamingRule between the Visited BSM and Home BSM declared in the parent 'ResponseEntry' instance. This element has the same structure as the 'RoamingRule' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'RoamingRule' in section 5.4.1.5.2 of [BCAST11-SG]

Table 50: Structure of Roaming RuleResponse Message

In case a roaming rule is not specific to any given Home BSM, it is RECOMMENDED that:

- in case the roaming rule is not subject to frequent changes, the Network delivers it following a RoamingRuleRequest from the terminal in a RoamingRuleResponse.
- and, in case the roaming rule is subject to frequent changes, the Network delivers it through the 'RoamingRule' element in the SGDD.

Note: delivery of roaming rules through SGDD over the interaction channel is not subject to either any recommendations or limitations with regard to the considerations defined above.

However, in case a roaming rule is specific to a given Home BSM, it SHOULD NOT be delivered via the 'RoamingRule' element of the SGDD.

5.7.1.3 Transport protocol

The BSM and Terminal SHALL support HTTP 1.1 [RFC 2616] as a delivery method to exchange roaming messages. The BSM and Terminal MAY also support HTTPS for this purpose, where HTTPS SHALL be based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246]. Furthermore, the following rules apply:

- The Terminal SHALL issue HTTP/1.1 POST request carrying one 'RoamingRuleRequest' element in the 'message-body' part.
- The BSM SHALL answer with an HTTP/1.1 200 (OK) response carrying one, and only one, 'RoamingRuleResponse' element in the 'message-body' part
- In both request and responses, the Content-Type entity-header field SHALL be set to 'application/vnd.oma.bcast.roaming+xml'
- The BSM MAY compress the response using GNU zip [GZIP], in which case the Content-Encoding entity-header field SHALL be set to 'gzip'.

5.7.2 Roaming messages between Home BSM and Visited BSM

Roaming messages between Home BSM and Visited BSM are used to carry out the roaming negotiation between the two BSMs. The exchange of these messages is triggered by the Terminal sending the Service Provisioning message. Four cases exist as follows.

If the value of Management Object "<X>/Roaming/UseVisitedServiceProvisioningMode" is assigned with value "false" the following SHALL apply:

- Terminal sends Home BSM the Service Request message involving service provided by the Visited BSM. If the Home BSM deduces from the message that it needs to contact Visited BSM to get clearance for the request, the Home BSM SHALL send the 'RoamingServiceRequest' (section 5.7.2.2) to the Visited BSM. Visited BSM SHALL respond to the request by sending 'RoamingServiceResponse' (section 5.7.2.3).). In case the response allows roaming, then the Home BSM sends a successful 'ServiceResponse' to the terminal. This leads to a subsequent LTKM delivery (push LTKM with Smartcard Profile or Trigger with DRM Profile).

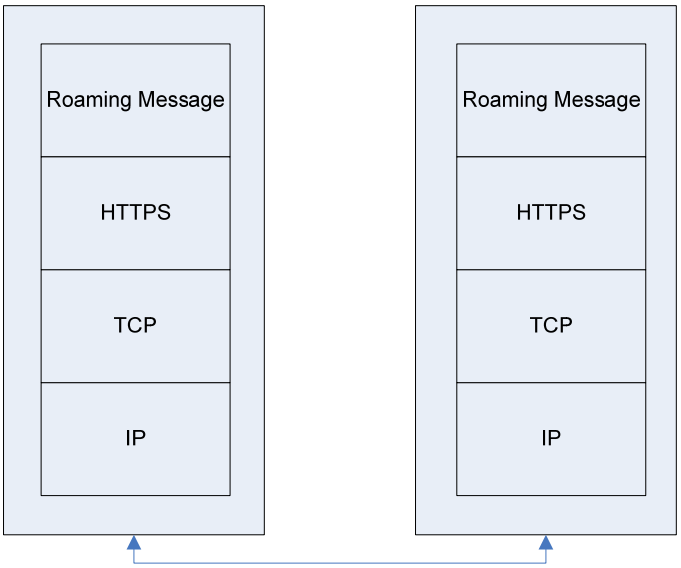
If the value of Management Object "<X>/Roaming/UseVisitedServiceProvisioningMode" is assigned with value "true" the following SHALL apply:

- Terminal sends Visited BSM the Service Request message involving service provided by the Visited BSM. If the Visited BSM deduces from the message that it needs to contact Home BSM to get clearance for the request, the Visited BSM SHALL send the 'RoamingServiceRequest' (section 5.7.2.2) to the Home BSM. Home BSM SHALL respond to the request by sending 'RoamingServiceResponse' (section 5.7.2.3). In case the response allows roaming, then the Visited BSM sends a successful 'ServiceResponse' to the terminal. This leads to a subsequent LTKM delivery (push LTKM with Smartcard Profile or Trigger with DRM Profile).

The XML schema for these messages is defined in [BCAST11-XMLSchema-Roaming-backend].

5.7.2.1 Protocol stack for message exchanges between BSMs

The following protocol stack SHALL be used for message exchange between BSMs. HTTP over TCP/IP SHOULD be used for the delivery of the roaming procedure authorisation messages. HTTPS based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246] SHALL be used in conjunction with TCP/IP to provide secure delivery of the authorisation messages.



HTTP 1.1 over TCP/IP SHALL be used for file delivery via the interfaces, subject to the following conditions:

- The interfaces using HTTP 1.1 [RFC 2616] SHALL support gzip, compress, deflate and identity content codings. Other content codings MAY be supported.
- The interfaces using HTTP 1.1 [RFC 2616] MAY use persistent connections, pipelining and chunked transfer coding.

5.7.2.2 Back-end Interface Messages

Messages between the Visited and Home BSMs are transported using HTTP as the transport by placing both the requests and the responses addressed to either BSM into the payload of the HTTP messages. The requests SHOULD be transported using HTTP POST and the responses SHOULD be transported using the HTTP responses corresponding to the HTTP POST requests. The syntax for the requests SHOULD be as follows:

- POST <host>/oma/bcast1.0/roaming HTTP/1.1\r\n<*requests*>

where the <host> denotes the part of the URI representing the address of the host.

Both the HTTP POST message and the corresponding HTTP response MAY also contain the following HTTP header fields:

- 'Content-Length',
- 'Content-Type' which if used SHALL be set to "text/xml" and
- 'Host' in case the 'Request-URI' is not in the absolute form specified in [RFC 2616].

5.7.2.3 Processing and Responding

The processing of the messages between the Visited BSM and Home BSM involves first the HTTP transport level to deliver the messages between the Visited BSM and Home BSM. This is followed by the HTTP level passing the embedded XML message to the BSMs. While the status and error codes corresponding to the processing in the HTTP level are signaled using the HTTP headers, the result of the BSMs processing the XML request in the HTTP payload is signaled using XML messages placed into the payloads of the HTTP responses corresponding to the HTTP requests carrying the XML requests. Whenever an HTTP response contains an XML response from the BSM, the HTTP status code SHALL be set to 200 OK regardless of the contents of the XML response.RoamingServiceRequest

Name	Type	Category	Cardinality	Description	Data Type
RoamingServiceRequest	E			Request message for Roaming Service between Home BSM and Visited BSM. Contains the following attributes: requestID Contains the following elements: HomeBSMFilterCode VisitedBSMFilterCode TerminalSubscriptionType UserID GlobalPurchaseItemID	
requestID	A	M	1	An ID that is unique in the scope of this exchange that SHALL be used throughout the roaming service procedure. It SHALL be generated by the party that initiates the message exchange when it first requests roaming service.	unsignedInt
HomeBSMFilterCode	E1	M	1	The code that specifies the Home BSM. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSMFilterCode	E1	M	1	The code that specifies the Visited BSM. - This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
Terminal Subscription Type	E1	M	1	A field that SHALL indicate the subscription scope of the terminal in terms of roaming. The Home Service Provider and the Visited Service Provider have a common understanding of the field according to roaming agreements between them. This element is not further specified in this specification.	anyURI
UserID	E1	M	1..N	A unique ID that SHALL be used to identify the terminal in both the Home Service Provider and Visited Service Provider BCAST service area. Contains the following attributes: type	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
GlobalPurch	E1	M	1..N	Set of PurchaseItems (represented by	anyURI

aseItemID				GlobalPurchaseItemIDs) which are associated with the VisitedBSM and which the terminal wants to subscribe /to purchase.	

Table 51: Structure of RoamingServiceRequest Message

5.7.2.4 RoamingServiceResponse

Name	Type	Category	Cardinality	Description	Data Type
RoamingServiceResponse	E			Response message for Roaming Service between Home BSM and Visited BSM. Contains the following attribute: requestID roamingServiceStatus globalStatusCode Contains the following elements: UserID HomeBSMFilterCode VisitedBSMFilterCode GlobalPurchaseItemID	
requestID	A	M	1	An ID that is unique in the scope of this exchange SHALL be used throughout the roaming service procedure. It SHALL be generated by the party that initiates the message exchange when it first requests roaming service.	unsignedInt
roamingServiceStatus	A	M	1	A field that SHALL indicate whether the terminal has been authorized for roaming services or not. . The return codes are defined in section 5.11.	unsignedByte
globalStatusCode	A	M	0..1	The overall outcome of the request, according to the return codes defined in section 5.11. ▪ If this attribute is present and set to value "0", the request was completed successfully. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'GlobalPurchaseItemID'. ▪ If this attribute is present and set to some other value than "0", there was a generic error concerning the entire request. In this case the 'itemwiseStatusCode' SHALL NOT be given per each requested 'GlobalPurchaseItemID'. If this attribute is not present, there was an error concerning one or more 'GlobalPurchaseItemID' elements associated with the request. Further, the 'itemwiseStatusCode' SHALL be given per each requested 'GlobalPurchaseItemID'.	unsignedByte
UserID	E1	M	1	A unique ID that SHALL be used to identify the terminal in both the Home Service Provider and Visited Service Provider BCAST service area. Contains the following attribute: type	string

type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
HomeBSMFilterCode	E1	M	1	The code that specifies the Home BSM. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'BSMFilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
VisitedBSMFilterCode	E1	M	1	The code that specifies the Visited BSM. This element has the same structure as the 'BSMFilterCode' element in the 'ServiceGuideDeliveryDescriptor'.	complexType as defined for 'FilterCode' in section 5.4.1.5.2 of [BCAST11-SG]
GlobalPurchaseItemID	E1	M	0..N	Set of PurchaseItems (represented by GlobalPurchaseItemIDs) which are associated with the Visited BSM and which the terminal is authorized to subscribe /to purchase. This element SHALL NOT be instantiated in case the 'globalStatusCode' attribute is present and set to a value different from '0'. In any other case, it SHALL be instantiated. Contains the following attribute: itemwiseStatusCode	anyURI
itemwiseStatusCode	A	M	0..1	Specifies a status code of each GlobalPurchaseItemID using GlobalStatusCode defined in the section 5.11.	unsignedByte

Table 52: Structure of RoamingServiceResponse Message

5.7.3 Scope of identifiers and Home BSM identification while roaming

This section defines tools and normative requirements in order to address two potential scoping problems for identifiers while roaming:

1. When the terminal is in a roaming situation and issues service provisioning requests against the Home BSM, the latter may not be able to identify the services of the Visited BSM the user wishes to subscribe to. This is due to potential limitations in the scope of identifiers in the Service Guide, as such identifiers may not be globally defined.

Said otherwise, the Home BSM may not be able to map fragment identifiers and global identifiers (such as the 'globalPurchaseItemId' attribute) back to the Visited BSM.

2. When the terminal is in a roaming situation and issues service provisioning requests against the Visited BSM, the latter may not be able to identify the Home BSM terminal despite the information provided by the terminal (such as device and user identifiers).

In order to address these potential problems, a 'BroadcastRoamingSpecificPart' element has been defined in the Service Provisioning messages, sections 5.1.5 and 5.1.6.

When in a roaming situation, the terminal issuing a Service Provisioning request against its Home BSM SHALL instantiate the 'VisitedBSM' element under the 'BroadcastRoamingSpecificPart' element for the said request.

When in a roaming situation, the terminal issuing a Service Provisioning request against the Visited BSM SHALL instantiate the 'HomeBSM' element under the 'BroadcastRoamingSpecificPart' element for the said request.

5.8 Location Filtering of Broadcast Services and Content

The BCAST client MAY implement the optional Location Filtering of Broadcast Services and Content. The BCAST Enabler MAY use Location Information for various purposes in conjunction with other functions of BCAST, such as File and Stream Distribution and Service Guide. Location Information MAY be used to enable location based filtering of services; location based targeting of services; service blackout regions; and so on.

Location Filtering is performed on the terminal using Location Information in the service guide. A terminal SHOULD NOT display (to the end-user or in the service guide) the Services or Content that have been filtered out by processing the BroadcastArea attributes of the service guide. A sporting-event blackout filter (i.e. no transmission near a stadium) can be enabled by setting the polarity attribute to FALSE in the BroadcastArea element. A local-emergency blackout filter (i.e. transmission only in a localized area) can be enabled by setting the polarity attribute to TRUE in the BroadcastArea element. The following rules define the availability of Location Information to the BCAST Enabler and the dependencies the BCAST Enabler has with respect to Location Information:

- The BCAST system MAY utilize Location Information in OMA MLP format [OMA MLP].
- The BCAST system MAY utilize Location Information in BDS-specific cell target area (for example the cell identifier of 3GPP, 3GPP2, DVB-H, DVB-SH, FLO, WiMAX, etc. system) format.
- The BCAST system MAY utilize Location Information in other formats, such as country-code, zip code, name-area, etc. A terminal MAY calculate its Location Information by measuring its cell ID or by using GPS and may employ a lookup table stored on the terminal in order to convert between different representations (e.g. to convert a cell ID into a zip code). Location Information MAY be derived by querying an MLP server or a SUPL server to determine location in one of these formats.
- The BCAST system SHALL NOT expect all the BCAST terminals to have capability to utilize Location Information in any particular allowed format.

Note that the solution to restrict access to content through the SG by using the polarity attribute of Location Information is not secure and if security is needed then the location-based restriction solution described in the SPCP specification should be used instead.

To implement the enhanced Location Filtering functionality of BCAST 1.1, the terminal MUST store a log of location data. If the terminal stores this log, the following guidelines SHALL apply.

- A location history log SHALL be an "opt-in" function, i.e. the user must give permission for the terminal to store a location history log.
- The terminal SHALL store the location history log in a secure location. If the log is encrypted, the terminal SHALL use a secure encryption protocol such as AES-CBC to store the location history log, the encryption keys SHALL be at least 128 bits in length, and the keys to encrypt the location history log SHALL also be stored in a secure location, i.e. together with other security keys held on the terminal.

- Access to the location history log SHALL only be provided to authorized applications on the terminal.
- Reports of viewing history for Location Filtered Content and Services (including e.g. audience measurement reports or diagnostic reports) SHALL NOT contain the user identity, to protect the location privacy of the user.

Appendix F describes a recommended implementation of location-based broadcast filtering for handsets wanting to implement minimal location function capabilities.

5.9 XML for Signalling

The BCAST enabler uses XML as a format for many signalling messages (e.g. Service Guide Fragments, Provisioning Messages, Interactivity). This section describes how to facilitate a maximum degree of backward and forward compatibility between the current and future versions of BCAST. Furthermore, it ensures that vendor- and operator-specific extensions will not lead to inconsistent states when interpreting an XML instance. Related to this, design rules for extending XML schemas are given in Appendix H.

5.9.1 Namespace identifier

Each XML schema targets one XML namespace. The namespace identifiers of the BCAST XML schemas are structured as follows: <prefix>:<version>, where <prefix> is a colon-separated list of strings like “urn:oma:xml:bcast:sg:fragments” and <version> is the representation of the version of the BCAST enabler, structured as <major>.<minor>.<service_indicator>. While the <major> and <minor> parts of <version> SHALL be provided, the <service_indicator> part and its leading dot are OPTIONAL. A decoder SHOULD use <prefix> to determine that a particular piece of XML information is compliant with OMA BCAST, and SHOULD use <version> to determine its version.

5.9.2 Proprietary extensions

XML schemas defined in BCAST MAY be extended by proprietary elements. Such extensions SHALL be located inside a container called <PrivateExt> as defined in the XML schemas, and SHALL be defined in a non-BCAST namespace. Decoders MAY discard proprietary extensions. In any case, they SHALL NOT get into an error state when they encounter such extensions.

5.9.3 BCAST extensions

Decoders being able to interpret XML instances compliant to an earlier version of the OMA BCAST XML schemas but not able to interpret possible extensions MAY discard those extensions. In any case, they SHALL NOT get into an error state when they encounter unknown extensions.

5.10 Service Provisioning of Unicast Services

BCAST 1.0 enables a provider to offer services by both unicast and broadcast access methods. Service Provisioning for services that can be accessed via a Broadcast Channel typically involves Service and Content Protection [BCAST11-ServContProt]. Additionally, Service and Content Protection can be applied to services that can be accessed via the Interactive Channel. Alternatively, the access to those services can also be controlled by the BSM. In the latter case the BSM only allows access to the resource over the Interactive Channel after the user has purchased or subscribed to the associated purchase item of the service. So Service and Content Protection might not always be required for services that can be accessed via the Interactive Channel.

In such a case the terminal performs the regular Service Request and Service Response message sequence as defined in section 5.1.5.2. Upon successful purchase or subscription the ‘Service Response’ message from the BSM contains the ‘itemwiseStatusCode’ attribute set related to respective ‘PurchaseItemID’ set to ‘029’ (now subscribed). Further, in this case, the ‘DRMProfileSpecificPart’ element MAY be omitted. Upon reception of the request message the BSM MAY possibly proceed with the required charging event. Upon reception of the response message the terminal SHALL assume the network resource is accessible, i.e. the service can be consumed via the announced Access fragment in the Service Guide [BCAST11-SG].

5.11 Global Status Codes

The following table lists all the possible status codes for success or error case, and their applicability to each transaction. The table is to be used for GlobalStatusCode and roamingAuthorizationStatus in Provisioning and Roaming response messages. The codes may also be used in other response messages in other BCAST technical specifications.

Code	Status
000	**Success** The request was processed successfully.
001	**Device Authentication Failed** This code indicates that the BSM was unable to authenticate the device, which may be due to the fact that the device is not registered with the BSM, or that inappropriate security credentials were submitted by the device. In this case, the user may contact the BSM, and establish a contract, or get the credentials in place that are used for authentication.
002	**User Authentication Failed** This code indicates that the BSM was unable to authenticate the user, which may be due to the fact that the user is not registered with the BSM, or that inappropriate security credentials were submitted by the user. In this case, the user may contact the BSM, and establish a contract, or get the credentials in place that are used for authentication. Alternatively, if offered another opportunity, the user may re-enter the security credentials required for user authentication.
003	**Purchase Item Unknown** This code indicates that the requested purchase item is unknown. This can happen e.g. if the device has a cached service guide with old information. In this case, the user may re-acquire the service guide.
004	**Device Authorization Failed** This code indicates that the device is not authorized to get Long-Term Key Messages from the RI. For example, the device certificate was revoked in the case of the DRM Profile, or because trust relationship could not be established between the terminal and the BSM, in the case of the Smartcard Profile.
005	**User Authorization Failed** This code indicates that the user has not subscribed to the requested broadcast service, in the case of either the DRM Profile or the Smartcard Profile. In this case, the user may be given an opportunity to contact the BSM operator for service subscription.”.
006	**Device Not Registered** This code indicates that the device is not registered with the RI that is used for the transaction in the case of the DRM Profile, or that the device is not registered with the BDS-SD or the BSM, in the case of the Smartcard Profile. In this case, the device may automatically perform the registration, and, if the registration is successful, re-initiate the original transaction.
007	**Server Error** This code indicates that there was a server error, such as a problem connecting to a remote back-end system.
008	**Mal-formed Message Error** This code indicates that there has been a device malfunction, such as a mal-formed XML request. In such a case, the transaction may or may not (e.g. if there is an interoperability problem) succeed if it is re-initiated later. Note: This code can also be used between network entities

009	**Charging Error** This code indicates that the charging step failed (e.g. agreed credit limit reached, account blocked). The user may in such a case contact the BSM operator. Note: This code can also be used between network entities.
010	**No Subscription** This code indicates that there has never been a subscription for this service item, or that the subscription for this item has terminated. The user may in such a case issue a service request for a new subscription.
011	**Operation not Permitted** This code indicates that the operation that the device attempted to perform is not permitted under the contract between BSM and user. The user may in this case contact BSM operator and change the contract. Note: This code can also be used between network entities.
012	**Unsupported version** This code indicates that the version number specified in the request message is not supported by the network. In case the terminal cannot fall back to another version, the user may contact the BSM operator. Note: This code can also be used between network entities.
013	**Illegal Device** This code indicates that the device requesting services is not acceptable to the BSM. E.g. Blacklisted. In this case, the user may contact the BSM operator.
014	**Service Area not Allowed** This code indicates that the device is not allowed in the requested area due to subscription limits In this case, the user may contact the BSM operator or subscribe to the applicable service.
015	**Requested Service Unavailable** This code indicates that the requested service is unavailable due to transmission problems. In this case, the request may be re-initiated at a later time. Note: This code can also be used between network entities.
016	**Request already Processed** This code indicates that an identical request has been previously processed. In this case, the user or the entity may check to see if the request had already been processed (i.e. received an LTK), if not retry the request.
017	**Information Element Non-existent** This code indicates that the message includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the entity receiving the message. In this case related entities should contact each other.
018	**Unspecified** This code indicates that an error has occurred which cannot be identified. In this case related entities should contact each other.

019	**Process Delayed** Due to heavy load, request is in the queue, waiting to be processed. In this case the user or entity should wait for the transaction to complete. Note: If this error occurs between network entities, the system should wait for the transaction to complete.
020	**Generation Failure** This code indicates that the request information (message) could not be generated. In this case the user or entity should retry later.
021	**Information Invalid** This code indicates that the information given is invalid and cannot be used by the system. In this case the request should be rechecked and sent again.
022	**Invalid Request** This code indicates that the requesting key materials and messages (e.g., LTKM) are not valid and can not be fulfilled. In this case the request should be rechecked and sent again.
023	**Wrong Destination** This code indicates that the destination of the message is not the intended one. In this case the request should be rechecked and sent again.
024	**Delivery of Wrong Key Information** This code indicates that the delivered key information and messages (e.g., LTKM) are invalid. In this case the request should be rechecked and sent again.
025	**Service Provider ID Unknown** This code indicates a confliction when the Visited or Home Service Provider requests a message to the Home or Visited Service Provider.
026	**Service Provider BSM_ID Unknown** This code indicates a confliction when the Visited or Home Service Provider BSM requests a message to the Home or Visited Service Provider BSM.
027	**Already in Use** This indicates requested setup value is already used in the Network Entity. Response message may contain the recommended value to use.
028	**No Matching Fragment** No fragment or SGDD matches the given request criteria.
029	**Now Subscribed** Specifies whether the subscription did succeed. Upon reception of this status code the terminal SHALL assume the service associated with the associated purchase item can be consumed via the associated 'Access' fragment of the service as defined in the Service Guide [BCAST11-SG]. This status code SHALL NOT be returned if the Purchase Item in question is associated with a service that is protected by Service or Content Protection.
030	**User already subscribed with different purchase options** Indicates that the user tries to repurchase an already subscribed item, but with different options. This can happen when terminal loses subscription information. In this case, the terminal MAY issue an AccountInquiry request to restore the subscription information.
031	**User must agree to the terms of use** Indicates that the BSM rejected the subscription because the user did not agree to the terms of use.

032	**Parental Control Restriction- Request Disallowed** This code indicates that the purchase item is associated with a more restrictive parental rating than the level granted for the Terminal, and that it is not possible to pass parental control enforced by the BSM by submitting a PINCODE. It is not possible for the Terminal to purchase/subscribe to the purchase item or buy tokens for the purchase item.
033	**Parental Control Authentication Requested** This code indicates that the ordered item (e.g., purchase item) is associated with a more restrictive parental rating than the level granted for the Terminal, and that the BSM requests a parental control PINCODE or MAC (in case of Smartcard Profile Extension) to be submitted in order for the service ordering to pass the parental control enforced by the BSM. In this case, a new Service Request/Token Purchase Request should be sent which includes the concerned purchase item and the parental control PINCODE or MAC used for service ordering.
034	**Parental Control Verification Failed** This code indicates that the BSM failed to verify the submitted PINCODE or MAC (in case of Smartcard Profile Extension) used for Parental Control for Service Ordering. The provided PINCODE did not match the PINCODE associated with the Terminal, or the provided MAC did not match the MAC computed by the BSM. In case the generic solution is used, the user can be asked to input a new PINCODE to be provided in a new Service Request/Token Purchase Request which includes the concerned purchase item.
035	**Parental Control PINCODE Blocked** This code indicates that the PINCODE associated with the Terminal is blocked. Reasons for a PINCODE to be blocked include, e.g., that a certain amount of incorrect PINCODEs, which exceeds the limit set by the BSM, have been submitted. This status code SHALL NOT be used for the Smartcard Profile Extension of Parental Control for Service Ordering, see section 5.1.10.1.
036	**Campaign participation rejected** Indicates that the Terminal has been rejected a request to participate in an Audience Measurement campaign.
037	**Coupon Expired** This code indicates that the terminal submitted a Coupon or CouponID with a purchase transaction, but the coupon has an expiry date and is expired.
038	**Coupon Unknown** A CouponID was given in a purchase transaction but the BSM was unable to identify the coupon in its records. The transaction may succeed if the terminal retries it with the full Coupon object in the purchase transaction.
039	**Coupon Already Used** This code indicates that the user employed a valid Coupon or CouponID to purchase an available PurchaseData, but the coupon had already been used in a previous transaction and is therefore no longer valid.
040	**Coupon Conditions not Met** This code indicates that special conditions (such as being a first-time buyer) associated with a Coupon or CouponID were not met, and so the purchase transaction has been rejected.
041 ~ 127	**Reserved for future use**
128 ~ 255	**Reserved for proprietary use**

Table 53: Global Status Codes

5.12 Auxiliary data download and insertion, and support for advertisements

The BCAST enabler supports the insertion of auxiliary data within the service in two ways. The first method is based on triggers that are delivered within notification messages. The second method is based on network operation for content delivery. Both methods are detailed below.

5.12.1 Auxiliary data insertion based on notification messages

This method is based on triggers that are delivered within notification messages. Such triggers can be used to trigger presentation of terminal-resident data or to initiate downloading of data to be presented later (in response to the trigger for auxiliary data insertion). These triggers are expected to produce terminal-specific behavior by specifying filtering data which may contain location context, target profiles, or which may reference terminal-resident rule sets. This results in selective downloading and insertion of auxiliary data, and can serve a variety of purposes, including personalization of the selection of terminal-resident advertisements for rendering. Triggers for auxiliary data downloading and insertion, and related signallingand message formats are normatively specified in chapter 5.14. The overall process normally consists of three steps.

1. An initial download notification trigger identifies an auxiliary data content item and an associated download opportunity.
2. At some future time, the terminal can download and store the corresponding auxiliary data content item (e.g. an advertisement) and store it locally. Such download SHALL be based on the delivery session information contained either in the initial trigger, or the Service Guide [BCAST11-ServiceGuide], and the decision whether or not to store the content is governed by filtering data contained in the download trigger.
3. Subsequently, an insertion notification trigger is sent, causing a suitable auxiliary content item (e.g. targeted advertisement) stored in the terminal to be played back during program viewing.

As indicated previously, the delivery session information for auxiliary data is conveyed in one of two ways:

a) For normal auxiliary data content, the Access/Session Description and Schedule fragments of the Service Guide MAY provide the associated delivery session information. In this mode, the File Delivery Client of the BCAST Terminal is responsible for downloading the associated file content.

b) Download session information MAY alternately be carried in the Notification message as described in Section 5.14. This represents a means to inform the terminal of dynamic updates to nominal auxiliary data content (e.g., delivery of last-minute changes to previously transmitted advertisements). In this mode, the Notification Client of the BCAST Terminal is responsible for downloading the associated file content.

The terminal determines the download method by examining the presence or absence of the element ‘SessionInformation’ in the Notification message. Presence of ‘SessionInformation’ indicates the use of delivery session information contained in the Notification message, whereas absence of this element indicates that the delivery session information is provided by the Service Guide.

For download session information specified in the Service Guide, the value of ‘ServiceType’ element in the Service Guide SHALL be “10” (i.e. correspond to “Auxiliary Data”). The existence of an ‘Auxiliary Data’ service SHOULD be hidden from user awareness in the Service Guide. The ‘Auxiliary Data’ service SHOULD be monitored by terminals which support auxiliary data download/caching for subsequent insertion display to users. Transport related information for downloading the associated auxiliary data files is provided either by the Access fragment that references the ‘Auxiliary Data’ service, or by the SessionDescription fragment identified by the Access fragment. Each content item comprising the Auxiliary Data service is scheduled for broadcast file delivery according to the Schedule fragment, and linked to the Notification message by the ‘GlobalContentID’ sub-element of the download ‘AuxDataTrigger’.

Once a notification carrying a ‘SessionInformation’ element is received, the associated auxiliary data download SHALL replace any auxiliary data download implied by session information in the Service Guide, or in earlier notification messages with a ‘SessionInformation’ element. Further updates to the same auxiliary data will therefore require further notifications with a ‘SessionInformation’ element.

5.12.2 Auxiliary data insertion based on network operation

This method is entirely based on network operation for content delivery. The network elements that schedule and transmit the service can perform the insertion of auxiliary data as normal content, multiplexed with the service. This method of auxiliary data insertion does not support rendering of terminal-resident auxiliary data nor does it allow personalization. The Service Guide data model inherently supports this method of auxiliary data insertion: auxiliary data can be added to an existing content or a new 'Content' fragment can be instantiated for auxiliary data.

5.13 Subtitling and Closed Captions

The Network MAY provide the subtitling or closed captions for a service using 3GPP Timed Text format. The Terminal SHOULD support 3GPP Timed Text as a format for subtitling and closed captions. The 3GPP Timed Text format is defined in [3GPP TS 26.245]. The signalling for subtitling is defined in section 5.1.2.5.2 of [BCAST11-SG].

5.14 Notification Function

Notification function can be used to provide information about forthcoming, imminent or immediate events, messages and notifications related to the BCAST system, to all broadcast services, or to a specific broadcast service. The notifications may be targeted to all reachable terminals or users, or specific terminals or users. Notifications are delivered as Notification Messages, which can be delivered over Broadcast Channel or over Interaction Channel, and stored in the terminal. Notification Messages fall into at least two categories, one category is user-oriented Notification Messages which are to be displayed to terminal users, the other category is terminal-oriented Notification Messages which are to be used for terminal operation and should not be displayed to users. The users are able to subscribe to user-oriented service-specific notifications using Service Provisioning Function specified in Section 5. Advertisement may be directly sent as Notification Messages, or triggered for local insertion by notification. The following outlines the purpose of Notification function in terms of types of Notification Messages that are specified:

- Emergency messages
- General announcements (informing about BCAST system problems, operator announcements, etc.)
- Broadcast main service or content associated notifications
  - Information regarding the availability of a specific service such as service breaks, abrupt change in the schedule (start time / end time) or access entry point of the service
  - Service-specific information that is a part of service experience (such as news, sports scores, etc.)
  - Information about services available in neighbouring systems, messages providing roaming support
  - Download or update announcement on SGDD or SG fragments
  - Download or update announcement on normal files such as movie, music, software, etc.
  - Auxiliary data downloading or insertion trigger (which are related to the main service or contents)
  - Other information related to the main service or content
- Notification-based information that the user has subscribed (i.e. asked to get delivered as soon the information is available).

Specification of Notification function consists of following parts:

- Discovery of availability and access to notifications
- Specification of event types of notifications (eventType)
- Format of Notification Message (syntax as defined by XML Schema in [BCAST11-XMLSchema-Notification])
- Notification Message delivery
  - Delivery over Broadcast Channel
  - Push delivery over Interaction Channel (including subscribing to notifications over Interaction Channel)
  - Polling notifications over Interaction Channel
- Notification interfaces(syntax as defined by XML Schema in [BCAST11-XMLSchema-Notification]).

Both the Network and Terminal MAY support the Notification function.

5.14.1 Discovery of Availability and Access to Notifications

5.14.1.1 Discovery of availability and access to general notifications

General notifications are not bound to any specific service nor Service Provider. Usually they are meant to be received by either all or majority of terminals, regardless of their Service Provider they are affiliated with. Examples of general notifications are emergency messages and announcements related to the operational aspects of BCAST system.

General notifications can be delivered either over Broadcast Channel or over Interaction Channel. The availability and access to general notifications can be discovered through SGDD.

5.14.1.1.1 General notifications: discovery through SGDD

The availability and access to general notifications can be signalled using the Service Guide Delivery Descriptor by instantiating the 'NotificationReception' element under the 'ServiceGuideDeliveryDescriptor' root element in the SGDD as defined in section 5.4.1.5.2 of [BCAST11-SG]. In case the Notification function is supported:

- NTC in the Terminal SHALL support the signalling of the availability and access to general notifications through the SGDD.
- NTDA in the Network SHALL support the signalling of the availability and access to general notifications through the SGDD.

5.14.1.2 Discovery of availability and access to notifications specific to a Service Provider

These notifications relate to a specific Service Provider. Usually they are meant to be received by either all or majority of terminals affiliated to the said Service Provider. Examples of such notifications are announcements related to operational aspects of a service.

Notifications specific to a Service Provider can be delivered either over Broadcast Channel or over Interaction Channel. The availability of and access to notifications specific to a Service Provider can be discovered through SGDD.

5.14.1.2.1 Notifications specific to a Service Provider: discovery through SGDD

The availability and access to notifications specific to a Service Provider can be signalled using the Service Guide Delivery Descriptor by instantiating the 'NotificationReception' element under the 'BSMSelector' element in the SGDD as defined in section 5.4.1.5.2 of [BCAST11-SG].

- NTC in the Terminal SHALL support the signalling of the availability and access to notifications specific to a Service Provider through the SGDD.
- NTDA in the Network MAY support the signalling of the availability and access to notifications a Service Provider through the SGDD.

5.14.1.3 Discovery of availability and access to service-specific notifications

Service-specific notifications are notifications that are associated with a specific service of a specific Service Provider. Usually they are meant to be received by the terminals that are accessing the service in question. Examples of service-specific notifications are sports goals, news and operational announcements related to a specific service.

Service-specific notifications can be delivered either over Broadcast Channel or over Interaction Channel. The availability and access to service-specific notifications can be discovered through 'Access' fragment.

5.14.1.3.1 Service-specific notifications: discovery through 'Access' fragment

The availability and access to service-specific notifications can be signalled by including the 'NotificationReception' element in any of the 'Access' fragments associated with a Service as defined in section 5.1.2.4 of [BCAST11-SG]. In case the Notification function is supported:

- NTC in the Terminal SHALL support the signalling of the availability and access to service-specific notifications through 'Access' fragment.
- NTDA in the Network SHALL support the signalling of the availability and access to service-specific notifications through the 'Access' fragment.

5.14.1.4 Discovery of availability and access to notifications as an independent service

Notification messages can also be delivered as part of a Notification service that can be discovered through the Service Guide. Usually they are meant to be received by the terminals as an independent service. Examples of such services are news tickers or traffic updates for navigation systems.

Independent Notification services can be delivered either over Broadcast Channel or over Interaction Channel. The availability and access to such Notification services can be discovered through the 'Service' and 'Access' fragments.

5.14.1.4.1 Notifications as an independent service: discovery through 'Access' fragment

The availability and access to independent Notification services is signalled by:

- providing a 'Service' fragment with the 'ServiceType' element set to '7' (Notification), and
- providing an 'Access' fragment pointing to the previous 'Service' fragment. The sessions or URLs used to deliver the Notification Messages SHALL be signalled by the "AccessType" element, by providing a session description of a file delivery session using the 'SessionDescription' element, or by providing a list of URLs to be polled for notification messages using the 'AccessServerURL' element. The 'NotificationReception' element MAY be instantiated (in order to declare the polling period over HTTP), but the IPBroadcastDelivery and PollURL SHALL not be given as this information is provided by the "AccessType" element.

In order to enable discovery of Notifications as independent services:

- NTC in the Terminal SHALL support the signalling of the availability and access to notification services through 'Service' and 'Access' fragment.
- NTDA in the Network SHALL support the signalling of the availability and access to notification services through the 'Service' and 'Access' fragment.

5.14.2 Declaring the usage of a Notification message

Besides the various elements and attributes of the Notification message schema, two attributes are used to specifically announce the intended usage of the message:

- the 'eventType' attibute describes the type of notification, it allows the Terminal to identify the nature of the received notification, and
- the 'notificationType' attribute, which is used to signal the primary target of the Notification message. As of this version 1.0 of the specification, either the notification message is primarily intended for the user (value '0') or the terminal (value '1'). A terminal-oriented notification usually implies preliminary processing of the notification message by the terminal prior to rendering, if any.

The table below defines the possible values of the 'eventType' attribute.

EventType	Name	Description
0	-	Reserved for future use.
1	Emergency notification	To announce emergency messages to users.

2	SG download or update notification	To announce download or update of SGDD or SG fragments
3	File download or update notification	To announce download or update of normal files such as movie, music, software, etc.
4	Service availability notification	To announce the errors, problems or interruption of broadcast main services or contents. To announce the abrupt schedule changes of broadcast main service or content To announce the abrupt changes on access entry point of broadcast main service or content.
5	Supplemental service notification	To announce service supplemental information that is a part of service experience (such as news, sports scores, promotional events etc.)
6	Auxiliary Data Trigger for Real-time main contents	To trigger either the auxiliary data downloading and storage, or the auxiliary data insertion, associated with the real-time main service or content. This notification may be associated with filtering related data to support customization of the auxiliary data storage or insertion.
7	Auxiliary Data Trigger for Non-Real-time main contents	To trigger either the auxiliary data downloading and storage, or the auxiliary data insertion, associated with the non-real-time main service content. This notification may be associated with filtering related data to support customization of the auxiliary data storage or insertion.
8	Terminal Provisioning Trigger	To trigger the retrieval of Terminal Provisioning Packages for targeted terminals. The Terminal Provisioning Package is delivered through file distribution.
9 -127	Reserved for future use	
128 -255	Reserved for proprietary use	

Table 54: Event Types of Notifications

The various combination of ‘eventType’ and ‘notificationType’ are defined below. The reader is reminded that User-oriented notifications are signalled with value ‘0’ of the ‘notificationType’ attribute, while terminal-oriented notifications are signalled with value ‘1’.

Emergency notification (‘eventType’ value ‘1’)

User-oriented: the user is presented with the emergency notification. Other parameters of the notification message can impact the rendering of the notification, such as the ‘presentationType’ attribute.

Terminal-oriented: not applicable.

As of this version of the specification, the ‘notificationType’ attribute SHALL be set to ‘0’ if the ‘eventType’ attribute is set to ‘1’. In case the ‘notificationType’ attribute is not set to ‘0’ but the eventType attribute is set to ‘1’, the 1.0 terminal SHALL assume the notification message is a User-oriented emergency message and SHALL proceed as per the rules defined in section 5.14.6.

Service availability notification (‘eventType’ value ‘4’)

User-oriented: the user is presented with the payload of the notification.

Terminal-oriented: not applicable.

As of this version of the specification, the 'notificationType' attribute SHALL be set to '0' if the 'eventType' attribute is set to '4'. In case the 'notificationType' attribute is not set to '0' but the eventType attribute is set to '4', the 1.0 terminal MAY discard the message.

Supplemental service notification ('eventType' value '5')

User-oriented: the user is presented with the payload of the notification.

Terminal-oriented: not applicable.

As of this version of the specification, the 'notificationType' attribute SHALL be set to '0' if the 'eventType' attribute is set to '5'. In case the 'notificationType' attribute is not set to '0' but the eventType attribute is set to '5', the 1.0 terminal MAY discard the message.

Auxiliary Data Trigger for Real-time main content ('eventType' value '6')

User-oriented: not applicable.

Terminal-oriented: the terminal silently processes the payload of the notification.

As of this version of the specification, the 'notificationType' attribute SHALL be set to '1' if the 'eventType' attribute is set to '6'. In case the 'notificationType' attribute is not set to '1' but the eventType attribute is set to '7', the 1.0 terminal MAY discard the message.

Auxiliary Data Trigger for Non-Real-Time man content ('eventType' value '7')

User-oriented: not applicable.

Terminal-oriented: the terminal silently processes the payload of the notification.

As of this version of the specification, the 'notificationType' attribute SHALL be set to '1' if the 'eventType' attribute is set to '7'. In case the 'notificationType' attribute is not set to '1' but the eventType attribute is set to '8', the 1.0 terminal MAY discard the message.

Terminal Provisioning Trigger ('eventType' value '8')

User-oriented: not applicable.

Terminal-oriented: the terminal silently processes the payload of the notification.

5.14.3 Format of Notification Message

Notification Message structure consists of:

- **Generic fields:** id, version, notificationType, eventType, IDRef, validTo, Title, Description, PresentationType and Extension
- **Notification content:** SessionInformation, MediaInformation, SGDD, SGDDReference, FragmentReference and AuxDataTrigger

While the generic fields can be used with all types of notifications, the notification content varies according to the notification type and event type. For example: emergency notification could contain generic fields + MediaInformation; SG download or update notification could contain SGDD, SGDDReference, or FragmentReference, etc.

A Notification Message carrying Service Guide update (eventType with value 2) SHALL only notify updates that relate to the currently bootstrapped Service Guide.

Name	Type	Category	Cardinality	Description	Data Type

Notification Message	E			Notification Message Contains the following attributes: id version notificationType eventType validTo Contains the following elements: IDRef Title Description PresentationType Extension SessionInformation MediaInformation ServiceGuide AuxDataTrigger TerminalProvisioning PrivateExt	
id	A	NM/ TM	1	Identifier of Notification Message	anyURI
version	A	NM/ TM	1	Notification Message version information. It is to be used to check for Notification Message Redundancy and new Notification Messages. This field can be expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
notificationType	A	NM/ TM	1	This attribute indicates whether the message is primarily targeted at the user or the terminal. Allowed values are: 0 – indicates that this message is user-oriented 1– indicates this message is terminal-oriented 2 - 127: For future use 128 - 255: For proprietary use Possible combinations of the 'notificationType' attribute and the 'eventType' attribute are detailled in section 5.14.2.	unsignedByte
eventType	A	NM/TM	1	This attribute indicates the nature of the notification conveyed by the message. For a detailed list of values of the 'eventType' attribute and its possible combinations with 'notificationType', see section 5.14.2.	unsignedByte
validTo	A	NM/ TM	0..1	Valid time of Notification Message. This field expressed as the first 32bits integer part of NTP time stamps. If 'validTo' is specified, the Notification Message SHOULD be expired at the specified time.	unsignedInt
IDRef	E1	NM/ TM	0..N	Fragment ID references of the main services or contents which the Notification Message is related to. This SHALL only be used for Service	anyURI

				specific or AuxData Notifications. The terminal SHALL consider the fragment reference to be scoped under the BSMSelector the Notification message applies to.	
Title	E1	NM/ TM	0..N	Title of Notification Message, possibly in multiple languages. The language is expressed using built-in XML attribute 'xml:lang' with this element.	string
Description	E1	NM/ TM	0..N	Description or Messages of Notification, possibly in multiple languages The language is expressed using built-in XML attribute 'xml:lang' with this element Only one instance of this element is allowed per language.	string
Presentation Type	E1	NM/ TM	0..1	Recommends the type of presentation for the received Notification Messages based on the priority of the Notification Message. Allowed values are: 0 – For high priority Notification Messages, Terminal MAY immediately render the message after interrupting all the applications. 1 – For medium priority Notification Messages, Terminal MAY immediately render the message, overlaying the present playing services. 2 – For low priority Notification Messages, Terminal MAY NOT immediately render the message, the user can see the stored message whenever he or she wants. 3-127: For future use 128-255: For proprietary use	unsignedByte
Extension	E1	NM/ TM	0..N	Additional information related to this Notification Message. Contains following attribute: url Contains following sub-element: Description	
url	A	NM/ TM	1	URL containing additional information related to this notification.	anyURI
Description	E2	NM/ TM	0..N	Description regarding the additional information which can be retrieved from a web page. The language is expressed using built-in XML attribute 'xml:lang' with this element	string
SessionInformation	E1	NM/ TM	0..N	This element SHALL be present when the Notification Message carries pointer to another delivery session, for example for file download or update, SG download or update, or auxiliary data download. SessionInformation defines the delivery session information, including the schedule, of the objects delivered over the broadcast channel, and URI as alternative method for delivery over interaction	

				channel. After receiving Notification Message with SessionInformation, Terminal would access the relevant session specified by SessionInformation and take a proper action like receiving contents. Contains the following attributes: validFrom validTo usageType Contains the following elements: DeliverySession AlternativeURI Nominally, access and schedule related delivery session information for relatively long-lived auxiliary data contents SHOULD be specified by the Access and Schedule fragments, respectively, of the Service Guide [BCAST11-ServiceGuide]. Other updates of auxiliary data MAY be delivered on the delivery session referenced by this SessionInformation, specifically, over the duration spanned by the ('validFrom', 'validTo') attributes of this element. If 'AuxDataTrigger' is instantiated and corresponds to the download trigger, and 'SessionInformation' is also instantiated, then the latter element SHALL be used to convey the delivery session information for the auxiliary data content. If 'AuxDataTrigger' is instantiated and corresponds to the download trigger, and 'SessionInformation' is not instantiated, then the <GlobalContentID> sub-element of 'AuxDataTrigger' SHALL be instantiated to provide the linkage to the Service Guide, which in turn conveys the delivery session information for the auxiliary data content. Note: For AuxData Download and Insert triggers, more than one 'SessionInformation' element may be instantiated.	
validFrom	A	NM/ TM	0..1	The first moment when the session for terminal to receive data is valid. This field expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
validTo	A	NM/ TM	0..1	The last moment when the session for terminal to receive data is valid. This field expressed as the first 32bits integer part of NTP time stamps.	unsignedInt
usageType	A	NM/ TM	0..1	Defines the type of the object transmitted through the indicated delivery session. Allowed values are: 0 – unspecified	unsignedByte

				1 - files 2- streams 3 – SGDD only 4 – mixed SGDD and SGDU 5 – notification 6 – Terminal Provisioning Package 7-127 reserved for future use 128-255 reserved for proprietary use Note: the delivery session only carrying SGDUs is declared through 'SGDD' element or "SGDDReference" element in this Notification Message. Default: 0	
Delivery Session	E2	NM/ TM	0..1	Target delivery session information indicated by the Notification Message. Contains the following attributes: ipAddress port sourceIP transmissionSessionID Contains the following element: ContentLocation	
ipAddress	A	NM TM	1	Destination IP address of the target delivery session	string
port	A	NM/ TM	1	Destination port of target delivery session	unsignedShort
sourceIP	A	NM/ TM	0..1	Source IP address of the delivery session	string
transmissionSessionID	A	NM/ TM	1	This is the Transmission Session Identifier (TSI) of the session at ALC/LCT level.	unsignedShort
ContentLocation	E3	NM/TM	0..N	This is the location of the Content to be retrieved. It corresponds to the 'Content-Location' attribute in the FDT. Note: If both 'ContentLocation' and 'AlternativeURI' elements are present, there is a 1:1 correspondence between these elements.	anyURI
AlternativeURI	E2	NM/ TM	0..N	Alternative URI for receiving the object via the interaction channel. If terminal cannot access the indicated delivery session, the terminal can receive the objects associated with the Notification Message by AlternativeURI. Note: If both 'ContentLocation' and 'AlternativeURI' elements are present, there is a 1:1 correspondence between these elements.	anyURI

Media Information	E1	NO/ TM	0..1	This element SHALL be present when the Notification Message carries information for rendering support of the notification. Media Information is used to construct and render Notification Messages. The notification media objects declared below can be delivered over a file delivery session specified by 'DeliverySession' element, or be retrieved via interaction channel via AlternativeURI of the media object as defined below. Contains the following elements: DeliverySession Picture Video Audio RichMedia In the description below, " Picture ", "Video", "Audio", and "RichMedia" E2elements are referred to as the "media elements" of the Notification Message	
DeliverySession	E2	NM/ TM	0..1	Session information to retrieve contents to be used for MediaInformation. Contains the following elements: ipAddress port sourceIP transmissionSessionID	
ipAddress	A	NM/ TM	1	Destination IP address of the target delivery session	string
port	A	NM/ TM	1	Destination port of target delivery session	unsignedShort
sourceIP	A	NM/ TM	0..1	Source IP address of the delivery session	string
transmissionSessionID	A	NM/ TM	1	This is the Transmission Session Identifier (TSI) of the session at ALC/LCT level.	unsignedShort
Picture	E2	NO/ TM	0..1	Defines how to obtain a picture and MIME type. Contains the following attributes: relativePreference mimeType pictureURI Contains the following element: AlternativeURI Note: For BCAST 1.0 the cardinality is set to 0..1 however in future releases the cardinality may change to 0..N in this case for backward compatibility the 1.0 terminal SHOULD only utilize the first Picture element.	
relativePrefe	**A**	**NM/TM**	**0..1**	This attribute gives the relative preference of this	unsignedInt

rence				element. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media elements are instantiated in this Notification Message, then all the elements SHALL have the 'relativePreference' attribute instantiated and SHALL have mutually exclusive values of this attribute. If only a single element is instantiated in this Notification Message then the 'relativePreference' attribute MAY be instantiated for that element.	
mimeType	A	NO/ TM	0..1	MIME type of Picture	string
pictureURI	A	NO/ TM	0..1	This is the location of the Content to be retrieved. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the pictureURI. This attribute is to be used in conjunction with the DeliverySession element defined above.	anyURI
AlternativeURI	E3	NO/ TM	0..N	Alternative URI for receiving the object via the interaction channel. If terminal cannot access the indicated delivery session, the terminal can receive the objects associated with the Notification Message by AlternativeURI. Multiple instances of the AlternativeURI MAY be instantiated for the purpose of server load distribution.	anyURI
Video	E2	NO/ TO	0..1	Defines how to obtain a video and MIME type. Contains the following attributes: relativePreference mimeType codec videoURI Contains the following element: AlternativeURI Note: For BCAST 1.0 the cardinality is set to 0..1 however in future releases the cardinality may change to 0..N in this case for backward compatibility the 1.0 terminal SHOULD only utilize the first Video element.	
relativePreference	**A**	**NM/TM**	**0..1**	This attribute gives the relative preference of this element. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media elements are instantiated in this Notification Message, then all the elements SHALL have the 'relativePreference' attribute instantiated and SHALL have mutually exclusive values of this attribute.	unsignedInt

				If only a single element is instantiated in this Notification Message then the 'relativePreference' attribute MAY be instantiated for that element.	
mimeType	A	NO/ TO	0..1	MIME type of Video	string
codec	A	NO/ TO	0..1	The codec parameters for the associated MIME Media type. If the file's MIME type definition specifies mandatory parameters, these MUST be included in this string. Optional parameters containing information that can be used to determine as to whether the terminal can make use of the file SHOULD be included in the string. One example of the parameters defined for video/3GPP, video/3GPP2 is specified in [RFC 4281].	string
videoURI	A	NO/ TO	0..1	This is the location of the Content to be retrieved. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the videoURI. This attribute is to be used in conjunction with the DeliverySession element defined above.	anyURI
AlternativeURI	E3	NO/ TM	0..N	Alternative URI for receiving the object via the interaction channel. If terminal cannot access the indicated delivery session, the terminal can receive the objects associated with the Notification Message by AlternativeURI. Multiple instances of the AlternativeURI MAY be instantiated for the purpose of server load distribution.	anyURI
Audio	E2	NO/ TM	0..1	Defines how to obtain a audio and MIME type. Contains the following attributes: relativePreference mimeType codec AudioURI Contains the following element: AlternativeURI Note: For BCAST 1.0 the cardinality is set to 0..1 however in future releases the cardinality may change to 0..N in this case for backward compatibility the 1.0 terminal SHOULD only utilize the first audio element.	
relativePreference	**A**	**NM/TM**	**0..1**	This attribute gives the relative preference of this element. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media elements are instantiated in this Notification Message, then all the elements SHALL have the 'relativePreference' attribute	unsignedInt

				instantiated and SHALL have mutually exclusive values of this attribute. If only a single element is instantiated in this Notification Message then the 'relativePreference' attribute MAY be instantiated for that element.	
mimeType	A	NO/ TM	0..1	MIME type of Audio	string
codec	A	NO/ TM	0..1	The codec parameters for the associated MIME Media type. If the file's MIME type definition specifies mandatory parameters, these MUST be included in this string. Optional parameters containing information that can be used to determine as to whether the terminal can make use of the file SHOULD be included in the string. One example of the parameters defined for audio/3GPP, audio/3GPP2 is specified in [RFC 4281].	string
audioURI	A	NO/ TM	0..1	This is the location of the Content to be retrieved. It corresponds to the 'Content-Location' attribute in the FDT, if FLUTE is used to deliver the audioURI. This attribute is to be used in conjunction with the DeliverySession element defined above.	anyURI
AlternativeURI	E3	NO/ TM	0..N	Alternative URI for receiving the object via the interaction channel. If terminal cannot access the indicated delivery session, the terminal can receive the objects associated with the Notification Message by AlternativeURI. Multiple instances of the AlternativeURI MAY be instantiated for the purpose of server load distribution.	anyURI
RichMedia	E2	NO/TO	0..N	Defines how to obtain a rich media content and MIME Type for the presentation of Notification. If the RichMedia element is present and the terminal supports the corresponding rich media solution, then the terminal will render the Notification according to the information in this element. It contains the following attributes: relativePreference It contains the following elements: Capabilities RichMediaData RichMediaURI AlternativeText AlternativePicture	
relativePreference	A	NM/TM	0..1	This attribute gives the relative preference of this element. The greater value has higher priority to handle (i.e 2 has higher priority than 1). If multiple media elements are instantiated in this	unsignedInt

				Notification Message, then all the elements SHALL have the 'relativePreference' attribute instantiated and SHALL have mutually exclusive values of this attribute. If only a single element is instantiated in this Notification Message then the 'relativePreference' attribute MAY be instantiated for that element.	
Capabilities	E3	NM/TM	1	Describes the type and complexity of Rich Media Solution the rich media engine has to deal with.	complexType as defined in section 5.1.2.4 for Capabilities element child of RichMedia element in Access fragment
RichMediaData	E3	NM/TM	0..1	An inlined Rich Media content that SHALL either be embedded in a CDATA section or base64-encoded. Contains the following attribute: encoding Either RichMediaURI or RichMediaData MUST be used if RichMedia element is present.	
encoding	A	NM/TM	0..1	This attribute signals the way the rich media data have been embedded: • It SHALL NOT be present when the rich media data are embedded into a CDATA section. Note: binary data inside CDATA shall always be encoded in base64 • It SHALL be present and set to "base64" in case the rich media data are base64-encoded	String
RichMediaURI	E3	NM/ TM	0..1	The URI referencing the rich media content. When ALC is used for delivery of the rich media content, this corresponds to the 'Content-Location' attribute' in the File element in the 'Access' fragment. When FLUTE is used for delivery of the rich media content, this corresponds to the 'Content-Location' attribute in the FDT of the FLUTE session. When HTTP is used for delivery of the rich-media content, the rules defined for usage of HTTP with the 'contentLocation' attribute of the 'Schedule' fragment apply (see section 5.1.2.2 of [BCAST 1.1-SG]). When RTSP is used for negotiation of the rich media	anyURI

				content delivery, this corresponds to the 'Request-URI' to be used in the request line of RTSP request.	
AlternativeText	E3	NM/ TM	0..N	Alternative Text to be displayed if the rich media content is not available. Possibly in multiple languages. The language is expressed using built-in XML attribute 'xml:lang' with this element. Text format attributes (e.g. font, size and colour) are defined by HTML version 4.01. The content of the 'AlternativeText' element SHALL either be embedded in a CDATA section or base64-encoded. Contains the following attribute: encoding	string
encoding	A	NM/TM	0..1	This attribute signals the way the HTML data have been embedded: It SHALL NOT be present when the HTML data are embedded into a CDATA section. It SHALL be present and set to "base64" in case the HTML data are base64-encoded.	string
AlternativePicture	E3	NO/ TM	0..1	Alternative Picture to be displayed if the rich media content is not available. AlternativePicture can be PictureData or URI reference of the Picture. The same schema of element 'Picture' is used for 'AlternativePicture'	
ServiceGuide	E1	NO/ TO	0..N	This element acts as a placeholder for future extensions of the Notification message in order to allow notifications related to the Service Guide (e.g. Service Guide update). BCAST 1.0 Terminals MAY decide to perform a complete Service Guide update in case they receive a Notification message with value '2' of the 'eventType' attribute and an instance of the 'ServiceGuide' element.	ServiceGuideType as defined in section 5.14.8
AuxDataTrigger	E1	NO/ TO	0..N	This Element contains information to trigger the auxiliary data downloading and storage, or the auxiliary data insertion associated with main service or content. 'globalContentID' and/or 'FilteringData' can be used to identify and/or fetch the auxiliary data content, and/or FilteringData associated with the auxiliary data content. Note: The auxiliary data downloading trigger indicates that auxiliary data should be downloaded and stored when the filtering criteria are met. Absence of FilteringData in the downloading trigger implies that the auxiliary data should be stored. Persistence of storage is terminal implementation dependent.	

				Contains the following attributes: type Contains the following Elements: GlobalContentID FilteringData PresentationRule	
type	A	NM/TM	1	0-The auxiliary data trigger is a download trigger; 1- The auxiliary data trigger is an insertion trigger. 2-127: Reserved for future use. 128-255: Reserved for proprietary use When AuxDataTrigger is present in the Notification Message, and the 'type' attribute is set to '0', the IDRef element SHALL NOT be present; When the 'type' attribute is set to '1', the IDRef element SHALL be present to indicate to terminal which main service should this auxiliary data be inserted to.	unsignedByte
GlobalContentID	E2	NO/ TM	1..N	Globally Unique Identifier of the auxiliary data content. If this identifier is absent and a renderingTime is specified, the Terminal may pull a random piece of content from its cache. If 'AuxDataTrigger' is of <type> = 0 (download trigger), and if 'SessionInformation' is absent, then this element's value SHALL match that of the <globalContentID> attribute of a Service Guide Content fragment which describes a content item belonging to the 'Auxiliary Data' service type (see [BCAST11-ServiceGuide]). 'GlobalContentID' then identifies the auxiliary data content item to which the 'FilteringData' sub-element of 'AuxDataTrigger' is applicable in controlling the subsequent download and caching operation. if 'SessionInformation' is present, then 'GlobalContentID' is used to identify the Auxiliary Data content downloadable via the 'SessionInformation', for the purposes of replacing Auxiliar Data content already on the terminal, or cancelling a later scheduled download of that Auxiliary Data content using the Service Guide. 'GlobalContentID' is not intended to be used to point at the service guide for providing download session information. Note: for every 'GlobalContentID', there MUST either be a matching 'SessionInformation' element by order (see above), or there MUST be zero 'SessionInformation' elements in this 'NotificationMessage'. If 'AuxDataTrigger' is of <type> = 1 (insertion trigger), then this element SHALL be omitted.	anyURI

				Such insertion trigger and its associated filtering data leads to the insertion of terminal-resident auxiliary data for rendering (which is independent of the identification of an auxiliary data content item for downloading and caching purposes).	
FilteringData	E2	NO/ TO	0..N	Reference to the location of the filtering related information associated with the AuxDataTrigger Notification Message, or the filtering–related information embedded within this Notification Message. Note: filtering related information can include attributes, values, rules, filter IDs, etc. Contains the following sub-elements: Location TargetProfile FilterIDs Either Location, TargetProfile, or FilterIDs, but not more than one of these sub-elements, MAY be present in FilteringData.	
Location	E3	NO/ TM	0..1	Reference to the location of the filtering related information associated with the AuxDataTrigger, from which that data can be retrieved.	anyURI
TargetProfile	E3	NO /TM	0..N	Filter rules and/or attributes to be used in the selection of auxiliary data for downloading and storage, or insertion. The extensible list of TargetProfile for a particular AuxDataTrigger notification enables the filtering/customization of the auxiliary data triggered by the notification, according to any specified filtering characteristic, e.g. user preference, user age, user location, service provider, etc. If the AuxDataTrigger is used to trigger the terminal to download and cache auxiliary data, in which case the 'type' attribute under AuxDataTrigger is set to '0', the number of TargetProfile entries SHALL be the same as the number of SessionInformation entries, and specifically, TargetProfile 1 maps to SessionInformation 1, TargetProfile 2 maps to SessionInformation 2, and so on. Attribute: filterID Sub-elements: Attribute FilterRules Note: TargetProfile is intended to be used to identify the type of auxiliary data file associated with the AuxDataTrigger notification. As an example, for an ad insertion event, 'attributeName' = "URI" and 'attributeValue' = "advertisement" can be used to match against the URI identifiers of auxiliary data files stored on the terminal for the keyword "advertisement".	

				Such mechanism would identify all the advertisements stored on the terminal, for subsequent insertion selection based on filter rules/attributes.	
filterID	A	NO /TM	0..1	Identity of the TargetProfile to be stored on the terminal for subsequent reference as a Filter ID sent as part of the FilterIDs (E3).	anyURI
Attribute	E4	NO/ TM	0..N	Profile attribute. Contains the following attributes: name value	
name	A	NM/TM	1	Profile attribute name	string
value	A	NM/ TM	1	Profile attribute value.	string
FilterRules	E4	NM/ TM	0..1	Filter rules that are used in the selection of auxiliary data for downloading and storage, or insertion.	string
FilterID	E3	NO /TM	0..N	Zero or more filter IDs used in the selection of auxiliary data for downloading and storage, or insertion. Each ad filter ID is an alias for a corresponding set of filter rules stored in the terminal. The rule set(s) in the FilterID list is(are) applied to the selection of the auxiliary data for downloading and storage, or insertion. The FilterID refers to the TargetProfile previously stored on the terminal.	anyURI
Presentation Rule	E2	NO/ TM	0..1	Specifies the presentation rules when the cached content should be rendered with this Notification Message. Contains the following attributes: renderingTime duration Contains the following elements: IDRef	
renderingTime	A	NO/ TM	0..1	Specifies the timing to start the presentation of the auxiliary data. In case eventType = 6 this element represent the time instant as the first 32bits integer part of NTP time for which the Notification Message is displayed or the auxiliary data insertion event occurs. In case eventType = 7, this element represent the offset in segments for which the auxiliary data insertion event occurs, relative to the start of the presentation of the associated main content.	unsignedInt
duration	A	NO/ TM	0..1	Time length of presentation of the auxiliary data in seconds.	unsignedShort
IDRef	E3	NO/	0..1	Service ID that specifies the AuxData service	anyURI

		TO		cache which contains the presentation to be played back.	
TerminalProvisioning	E1	NO/TO	0..1	Broadcast Terminal Provisioning specific information. This element is used to provide filtering information so that only the targeted terminals retrieve the Terminal Provisioning Package. The SessonInformation element SHALL be instantiated with this element to provide the delivery session information for the Terminal Provisioning Package. This feature is based upon OMA-DM [OMA DM 1.3]. For details on using Broadcast Terminal Provisioning refer to section 5.2 This feature is not related to smartcard provisioning and only related to the Terminal Consists of the following attribute: type Consists of the following element: Target Note: The detailed scope of Broadcast Terminal Provisioning is to be defined by DM WG.	
type	A	NM/TM	1	The type of Terminal Provisioning. Allowed values are: 0 - Firmware update [OMA FUMO] 1 - Software update [OMA SCOMO] 2 - Device Capability Control 3 - 127 reserved for future use 128 -255 reserved for proprietary use	unsignedByte
Target	E2	NM/TM	1..N	Filtering information for targeted terminals. Contains the following attributes: version manufacturer model hardware dm Contains the following elements: Extensions TargetArea	
version	A	NM/TM	0..1	Version of the announced update. MAY be used for filtering in Firmware.	unsignedInt
manufacturer	A	NM/TM	0..1	Targeted manufacturer name of the terminal. MAY be usedfor filtering in Firmware, Software and Device Capability Control.	string
model	A	NM/TM	0..1	Targeted model name/number of the terminal. MAY be usedfor filtering in Firmware, Software and Device Capability Control.	String
hardware	A	NM/TM	0..1	Version of the hardware of the targeted device.	string

				May be used for filtering in Firmware	
dm	A	NM/TM	0..1	Version of the OMA DM enabler required for the Terminal Provisioning service. Allowed values are: 0 – DM 1.3 1 – DM 2.0 2 – FUMO 1.0 3 – SCoMO 1.0 4 – DiagMon 1.0 5 - 127 reserved for future use 128 -255 reserved for proprietary use	unsignedByte
Extensions	E3	NM/TM	0..N	Supplementary extensions filters Consists of the following attributes: attributeName attributeValue	
attributeName	A	NM/ NM	1	Extension filter attribute name	string
attributeValue	A	NM/ TM	1	Extension filter attribute value	string
TargetArea	E3	NM/TM	0..1	Targeted area information. MAY be used for filtering in Firmware, Software, Audience Measurement, Network Measurement and Device Capability Control. Structure is as defined in E2 TargetArea in 5.1.2.1 Service Fragment [BCAST11-ESG]. Note: This element takes precedence over the target area in the content fragment	complexType
PrivateExt	E1	NO/ TO	0..1	An element serving as a container for proprietary or application-specific extensions.	
<proprietary elements>	E2	NO/TO	0..N	Proprietary or application-specific elements that are not defined in this specification. These elements may further contain sub-elements or attributes.	

Table 55: Structure of Notification Message

5.14.4 Notification Message Delivery

Notification Messages are created by the NTG (Notification Generation Function) according to the structure in 7.3 and are prepared for delivery by the NTDA (Notification Distribution/Adaptation Function). Notification Messages MAY be delivered in a number of ways:

- Notification Message delivery over Broadcast Channel (see section 5.14.4.1)
- Notification Message push-delivery over Interaction Channel (see section 5.14.4.2)
    - Related to push-delivery over Interaction, subscribing to Notification Messages (see section 5.14.4.2.1)
- Polling Notification Messages over Interaction Channel (see section 5.14.4.3)

5.14.4.1 Notification Message Delivery over Broadcast Channel

Over Broadcast Channel, the Notification Messages SHALL be delivered to terminals using one of the following methods:

1) UDP delivery: The Notification Message is delivered in a UDP packet.

The UDP packet SHALL be sent over the Broadcast Channel using the UDP destination port defined in the NotificationReception in the SGDD or the 'Access' fragment and the IP address of the ongoing session that the Notification Message is targeted for. If a separate IP address is defined in the NotificationReception in the SGDD or 'Access' fragment for the Notification Message then it SHALL be used. It is RECOMMENDED that to avoid IP level segmentation, Notification Message sizes should be less than 1500 bytes, the average network MTU (Maximum Transfer Unit) size.

To decrease the message size, GZIP MAY be used to compress the Notification Message.

The payload of the UDP file SHALL start with a header as specified below, followed by the uncompressed or compressed Notification Message. The format of the header is defined as follows:

Field	Type	Definition
Payload_type	uimsbf4	Signals the type of the payload Values: 0 – Notification according to MIME type vnd.oma.bcast.notification+xml 1-7 – reserved for future BCAST extensions 8-15 – reserved for proprietary extensions
Encoding_type	uimsbf4	Signals the encoding of the payload Values: 0 – unencoded 1 – GZIP encoded 2-7 – reserved for future BCAST extensions 8-15 – reserved for proprietary extensions

Table 56: Header for UDP Delivery of Notification Message

Mnemonics: uimsbf4 = Unsigned 4 bit Integer, most significant bit first

2) File delivery: The Notification Message is delivered in a separate file delivery session. There are two options for announcing such a file delivery session.

(a) the session parameters are announced in a separate Notification Message using the 'DeliverySession' element. This approach is RECOMMENDED for service-specific notifications, general notifications, and notifications specific to a Service Provider in case the Notification Message size exceeds the MTU size.

(b) the session parameters are announced in the Service Guide. This method SHALL be used for independent Notification services as specified in section 5.14.1.4.

To decrease the message size, GZIP MAY be used to compress the Notification Message. The fact that a message is compressed SHALL be signalled in the FDT. The Content-Type of a Notification Message in the FDT SHALL be signalled as "application/vnd.oma.bcast.notification+xml".

The terminal SHALL support GZIP decompression of Notification Messages.

The Notification Messages MAY be repeatedly transmitted by the Service Provider or Network Provider to increase the probability of all intended terminals receive the Notification Messages.

The following figures illustrate the protocol stacks of the two Notification Message delivery methods over the Broadcast Channel:

Notification Message

ALC/LCT/FLUTE

UDP

IP

Figure 1: Notification message delivery protocol stack variant 1

Notification Message

UDP

IP

Figure 2: Notification message delivery protocol stack variant 2

5.14.4.2 Notification Message push-delivery over Interaction Channel

The NDTA MAY deliver a Notification Message to the NTC using OMA Push as defined in [BCAST11-Distribution]. The terminal MAY support reception of Notification Messages delivered with OMA Push as defined in [BCAST11-Distribution].

5.14.4.2.1 Subscribing and Unsubscribing to User-oriented Notification Messages

Service Provisioning Function SHOULD be used for subscribing or unsubscribing Notification Message over Interaction channel. If the terminal has interaction capability, the terminal SHOULD support subscription and unsubscription of Notification Messages.

- When Terminal subscribes service-specific notification or notification service, Service Request message (See section 5.1.5) SHALL include 'ServiceID' element and 'notification' attribute under 'ServiceID' element
- When Terminal unsubscribes service-specific notification or notification service, Unsubscription message (See section 5.1.5) SHALL include 'keepSubscription' attribute, 'ServiceID' element and 'notification' attribute under 'ServiceID' element.

5.14.4.3 Polling notifications over Interaction Channel

In case the Terminal supports the Notification function, the NTC in Terminal with Interaction Channel capability SHALL support polling to notifications over Interaction Channel as follows:

- NTC sends an HTTP1.1 GET Request to the NTDA that is signalled in SGDD or 'Access' fragment.
- Response to the HTTP Request sent to the NTDA SHALL embed a set of zero or one or more Notification Messages encapsulated in a Notification MessageContainer delivered over anHTTP1.1 message. The NotificationMessageContainer embeds the exhaustive list of valid Notification Messages (i.e. that have not expired at the time of the response). The following table specifies the format of the NotificationMessageContainer.

Name	Type	Category	Cardinality	Description	Data Type
Notification MessageContainer	E			Notification MessageContainer Contains the following element: NotificationMessage	
Notification Message	E1	NM/ TM	0..N	Notification Message as specified in section 5.14.3	Notification MessageType as specified in section 5.14.3

- The Content-Type of the HTTP Response message containing a NotificationMessageContainer SHALL be set to "application/vnd.oma.bcast.notification+xml".
- In order to reduce the information that are present in the NTDA response when no update occurred between two subsequent requests from the same terminal, it is recommended that the NTDA sends an entity tag and/or a Last-Modified value in each HTTP 1.1 [RFC 2616] response header. It is expected that the NTC uses these information for subsequent cache-conditional requests as specified in HTTP 1.1 [RFC 2616].
- As specified in HTTP 1.1 [RFC 2616], if the NTC has performed a conditional GET request and access is allowed, but the document has not been modified, the NTDA SHOULD respond with the 304 status code. The 304 response SHALL NOT contain a message-body, and thus is always terminated by the first empty line after the header fields.
- As specified in [BCAST11-SG], when the "PollPeriod" element is instantiated in the "NotificationReception" element of an Access fragment or an SGDD, no caching mechanisms of HTTP 1.1 [RFC 2616] SHOULD conflict with the fact that the NTC is expected to request for a fresh NotificationMessageContainer every "PollPeriod" value.
- The NTDA MAY compress the HTTP response body with the GZIP algorithm. In this case the Content-Encoding attribute in the corresponding description of the HTTP response SHALL be set to "gzip". Terminals SHALL support this content encoding.

5.14.5 Notification Interfaces

The following sections specify the Notification interfaces between logical BCAST "backend" entities for message exchanges. The specification is applicable if the interfaces are exposed in a BCAST implementation. If a BCAST implementation does not expose the interfaces, i,e, they are implementation internal, they can be realized using protocols and methods not specified here. If a BCAST implementation does expose the interfaces, the network SHALL support the Notification Backend Interfaces syntax as defined by XML Schema in [BCAST11-XMLSchema-Notification].

5.14.5.1 Protocol Stacks

The following protocol stack SHALL be used for exchanging messages between Notification Components such as CC, NTE, NTG, and NTDA. HTTP or HTTPS that SHALL be based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246] over TCP/IP SHALL be used for the delivery of messages.

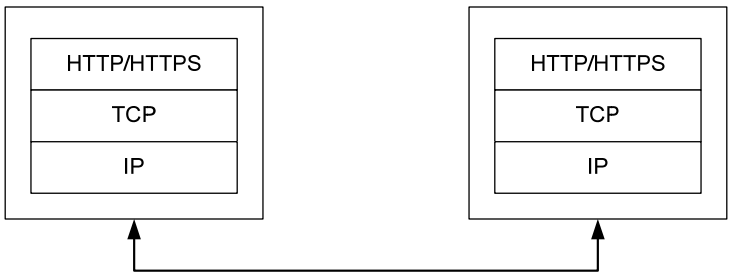


Figure 3: Notification component exchange protocol stack

Messages to and from CC, NTE, NTG or NTDA are transported using HTTP by placing both the requests and the responses addressed to CC, NTE, NTG or NTDA into the payload of the HTTP messages. The requests SHOULD be transported using HTTP POST and the responses SHOULD be transported using the HTTP responses corresponding to the HTTP POST requests. The syntax for the requests SHOULD be as follows:

- POST <host>/oma/bcast1.0/nt HTTP/1.1\r\n<NTEReq>
- POST <host>/oma/bcast1.0/nt HTTP/1.1\r\n<NTDReq>

where the <host> denotes the part of the URI representing the address of the host.

Both the HTTP POST message and the corresponding HTTP response MAY also contain the following HTTP header fields:

- 'Content-Length',
- 'Content-Type' which if used SHALL be set to "text/xml" and
- 'Host' in case the 'Request-URI' is not in the absolute form specified in [RFC 2616].

5.14.5.2 Notification Event Delivery

Notification Event can be generated in CC, BSA, BSM, or BSD/A. Each Entity delivers Notification Event via Backend Interface such as NT-1, NT-3, and NT-4. CC can deliver Notification Event to NTE via NT-1, NTE will deliver Notification Event generated in either CC or BSA to NTG via NT-3, and NTDA will deliver Notification Event generated in BSD/A to NTG via NT-4.

5.14.5.2.1 Request Message

The following is the delivery message of Notification Event, which is sent from the CC (Content Creation) to the NTE over interface NT-1, from NTE to NTG over interface NT-3 or NTDA to NTG over interface NT-4.

Name	Type	Category	Cardinality	Description	Data Type
NTEReq	E			Specifies the delivery message of Notification Event for generating Notification Message. Contains the following attributes: nteID entityAddress deliveryPriority Contains the following elements: NotificationEvent	
nteID	A	M	1	Identifier of Notification Event	unsignedInt
entityAddress	A	M	1	Network Entity Address to receive the response of this message.	anyURI
deliveryPriority	A	O	0..1	Defines the priority of this notification event. This information is applied to generate Notification Message in NTG. NTG may be ignored this field.	boolean
NotificationEvent	E1	M	1..N	Specifies the Notification Event, containing information to be included into the Notification Message. It is RECOMMENDED that the information is delivered in the form of BCAST Notification Message format (as specified in section 5.14.3). Other formats MAY be used only for NT-1. Contains the following sub-element: NotificationMessage	
Notification Message	E2	O	0..1	BCAST NotificationMessage format as specified in section 5.14.3. The following rule applies to child elements or attributes of NotificationMessage which are not relevant: If the element/attribute has a minimum cardinality of 0, it SHALL NOT be instantiated. Otherwise, it SHALL be delivered as empty field.	complexType as specified in section 5.14.3
Private	E2	O	0..1	This container allows to use data formats not	

				specified in BCAST.	

Table 57: Structure of Notification Event Request Message

5.14.5.2.2 Response Message

The following is the response message of NotificationEvent Delivery and which is sent from the NTE to CC over interface NT-1, from NTG to NTE over interface NT-3 or form NTG to NTDA over interface NT-4.

Name	Type	Category	Cardinality	Description	Data Type
NTERes	E			Specifies the Response message for NTEReq. Contains the following elements: Result	
Result	E1	M	1..N	The list of results, each entry consisting of a pair of ID and statusCode Contains the following attributes: nteID statusCode	
nteID	A	M	1	Identifier of NTEReq Message	unsignedInt
statusCode	A	M	1	Indicates the overall outcome how NTEReq is processed, according to the global status code (as specified in Section 5.11).	unsignedByte

Table 58: Structure of Notification Event Response Message

5.14.5.3 Notification Message Delivery

Notification Message is generated by NTG in BSM. NTG will request to deliver Notification Message to NTDA via NT-4.

5.14.5.3.1 Request Message

The following is the delivery message of Notification Message which is sent from the NTG to NTDA over interface NT-4.

Name	Type	Category	Cardinality	Description	Data Type
NTDReq	E			Specifies the Request message of Notification Message Delivery from NTG to NTDA. Contains the following attributes: ntdReqID entityAddress deliveryPriority Contains the following elements: TargetAddress NotificationMessage	
ntdReqID	A	M	1	Identifier of NTDReq	unsignedInt
entityAddress	A	M	1	Network Entity Address to receive the response of this message.	anyURI
deliveryPriority	A	O	0..1	Defines the delivery priority of this Notification Message. NTG can request NTDA to deliver this notifcaiton message as high priority. If priority=true, it means high priority. If priority=false, it means general message.	boolean
TargetAddress	E1	O	0..N	Specifies TargetAddress to deliver Notification Message.	string

				For service-specific notification, AccessReference or address under NotificationReception in 'Access' fragment can be possible value. If Notification message is delivered over interaction channel, the value can be e-mail address, IMSI, etc. If not given, Notification message SHALL be delivered to all users of the service provider using address defined in SGDD. Contains the following attributes: deliveryChannel AddressType	
deliveryChannel	A	M	1	Specifies the delivery channel If deliveryChannel = false, Notificaiton Message SHALL be delivered over Broadcast Channel. If deliveryChannel = true, Notification Message SHALL be delivered over Interaction Channel.	boolean
addressType	A	M	1	Specifies the type of TargetAddress Value 0 - IPAddress 1 - anyURI 2 - IMSI 3 -127: For Future Use 128 - 255: For Proprietary Use	unsignedByte
Notification Message	E1	O	0..1	BCAST NotificationMessage format as specified in section 5.14.3. The following rule applies to child elements or attributes of NotificationMessage which are not relevant: If the element/attribute has a minimum cardinality of 0, it SHALL NOT be instantiated. Otherwise, it SHALL be delivered as empty field.	complexType as specified in section 5.14.3

Table 59: Structure of Notification Delivery Request Message

5.14.5.3.2 Response Message

The following is the response message of Notification Message Delivery which is sent from NTDA to NTG over interface NT-4.

Name	Type	Category	Cardinality	Description	Data Type
NTDRes				Specifies the Response message for NTDReq. Contains the following elements: Result	
Result	E1	M	1..N	The list of results, each entry consisting of a pair of request ID and statusCode Contains the following attributes: ntdReqID statusCode	
ntdReqID	A	M	1	Identifier of NTDReq Message	unsignedInt
statusCode	A	M	1	Indicates the overall outcome how NTDReq is processed, according to the global status code (as	unsignedByte

				specified in Section 5.11).	

Table 60: Structure of Notification Delivery Response Message

5.14.6 Minimal support for emergency notifications

If the terminal supports emergency notifications, then the terminal SHALL support the use of Notification Function for those notifications as follows:

- The terminal SHALL be able to discover of the entry point to notification delivery channel as specified in section 5.14.1.1.1 through the use of element 'NotificationReception'. Further, the terminal SHALL assume that 'NotificationReception' element describes the entry point to general notification delivery channel within which the notification messages are delivered using "UDP Delivery" as specified in section 5.14.4.1.
- The terminal SHALL support the "UDP delivery" over Broadcast Channel as specified in section 5.14.4.1 as follows:
  - The terminal SHALL support 'Payload_type' having value '0'
  - The terminal SHALL support 'Encoding_type' having value '0'
- The terminal SHALL support the Notification Message format for emergency notifications as follows:
  - The terminal SHALL assume that attribute 'notificationType' is assigned with value '0' (user oriented notification message)
  - The terminal SHALL assume that attribute 'eventType' is assigned with value '1' (emergency notification)
  - The terminal SHALL assume that element 'Title' is present and expressed possibly in multiple languages.
  - The terminal SHALL assume that element 'Description' is present and expressed possibly in multiple languages.
  - The terminal SHALL assume that element 'PresentationType' is assigned with value '0' (high-priority notification messages)
  - The terminal MAY skip all the other elements and attributes in the Notification Message.

5.14.7 Guidelines for MediaInformation usage

As rich media presentation technologies are not specified in BCAST 1.0, the rendering of the Notification message is implementation specific. However the following section provides basic guidelines on the use of MediaInformation elements provide a consistent layout for the Notification messages. If required by service providers the guidelines below can be replaced with proprietary mechanisms.

- If multiple instances of Description element are present then the terminal SHOULD select and display the text of the Description based on the Terminal language setting.
- The Description element SHOULD always be set when using MediaInformation.
- Either the DeliverySession element or the AlternativeURI element SHOULD be set to indicate the delivery session providing the content to be used for MediaInformation.
- If RichMedia element is present and terminal supports the corresponding rich media solution, then terminal will use this element for the presentation of Notification message itself. This element SHOULD NOT be instantiated without at least one of Picture/Audio/Video elements, in this way, if terminal doesn't support the rich media solution, it can ignore the 'RichMedia' element and render other media objects contained in Picture/Audio/Video elements.
- If the Picture element is set in the MediaInformation, the Picture element SHOULD be displayed first with the text contained in the Description element being displayed under the Picture element.
- If the Audio element is set in the MediaInformation, the Audio element SHOULD be played in conjunction with the text contained in the Description element being displayed.

- If both the Picture and the Audio elements are set in the MediaInformation then two guidelines above SHOULD be met.
- Video element in the MediaInformation MAY be supported by the terminal and if the Video element is supported by the terminal, the following guidelines apply:
  - If the Video element is set in the MediaInformation, the Video element SHOULD be displayed first with the text contained in the Description element being displayed under the Video element.
  - If both the Video and the Picture elements are set in the MediaInformation then only the Video element SHOULD be displayed.
  - If both the Video and the Audio elements are set in the MediaInformation then only the Video element SHOULD be displayed.

To support the possibility of multiple cardinalities of Picture and Audio elements in future release of BCAST 1.1 the Terminals supporting BCAST 1.0 SHOULD be able to parse and only select the first Picture or Audio element even if there are multiple instances of Picture and Audio elements in future BCAST 1.1 Notifications.

5.14.8 Extensibility placeholders for future usage of Notification

For the purpose of extending the usage of the Notification message in releases following the BCAST 1.0 specification while maximizing backward compatibility with 1.0 terminals, extensibility placeholders have been defined. These contains a wildcard schema component in which new attributes and elements can be inserted. Currently defined placeholders are:

- the ‘ServiceGuide’ element in the Notification message (see section 5.14.3)

Extensions targeting the extensibility placeholders SHALL NOT be defined within the XML namespaces applicable to BCAST 1.0.

The Terminal SHALL ignore Notification messages with values of the ‘eventType’ or ‘notificationType’ attributes that it does not support.

5.14.8.1 The ServiceGuide placeholder

The ‘ServiceGuide’ element in the Notification message is the placeholder for future extensions related to the Service Guide. It is of type ‘ServiceGuideType’, that is defined as an element containing the following wildcard:

```
<xs:any namespace="##other" processContents="skip" minOccurs="0" maxOccurs="unbounded"/>
```

5.15 Pause and Resume of Subscription

Pause and resume of subscription allows the user to pause and resume periodical subscriptions. Subscriptions based on Tokens are not applicable.

5.15.1 Pause of Subscription

When using the Pause of Subscription as specified in this section, the Terminal SHALL send a Subscription Pause Request to temporarily pause the subscription of a periodical subscription. Token based subscription pause SHALL NOT be allowed. After receiving a Subscription Pause Request message the BSM SHALL send a Subscription Pause Response message to the Terminal with the results of the request. If the BSM does not allow the pause of the subscription it SHALL respond with the Global Status Code “011 Operation Not Permitted”. If the user requested pause period exceeds the BSM permitted pause period the Global Status Code “011 Operation Not Permitted” is sent in the response message with the allowed maximum pause period. If the BSM receives a pause request which exceeds the maximum pause period allowed by the BSM the BSM SHALL NOT allow the pause period to exceed the BSM defined pause period. If the pause is allowed the BSM SHALL respond with Global Status Code “001 Success” and MAY also provide the allowed period of pause. After the Terminal

receives permission to pause the subscription sections 5.4.4 of [SPCP11] and 6.6 of [SPCP11] apply for DRM Profile and Smartcard Profile respectively.

5.15.2 Resume of Subscription

When using the Resume of Subscription as specified in this section, the Terminal SHALL send a Subscription Resume Request to resume a temporarily paused subscription. After receiving a Subscription Resume Request message the BSM SHALL send a Subscription Resume Response message to the Terminal with the results of the request. If the BSM does not allow the resume of the subscription it SHALL respond with the Global Status Code "011 Operation Not Permitted". If the resume is allowed the BSM SHALL respond with Global Status Code "001 Success" and MAY also provide the remaining allowed period of the subscription. After the Terminal receives permission to resume the subscription sections 5.4.4 of [SPCP11] and 6.6 of [SPCP11] apply for DRM Profile and Smartcard Profile respectively. If the terminal does not resume the service automatically by the indicated time in the pause response message then the BSM MAY resume the service and charge the user for the resumption for the service.

5.16 User Defined Bundles

BCAST services are bundled together by the Service Provider and signalled to the user through the Service Guide. Bundles are usually grouped together based upon the Service Provider's provisioning strategies. However the Service Provider can provide a premium 'a la carte' bundling service to allow the user to create User Defined Bundles. The availability of User Defined Bundles SHALL be signalled through the Service Guide allowing the user to subscribe to User Defined Bundles. Service and contents which are allowed to be part of the User Defined Bundle SHALL be marked using UDBAllowed attribute in the Schedule, Service or Content Fragment of the Service Guide. Services and content which have dependencies to each other SHOULD not be offered for User Defined Bundles as dependency problems MAY occur for User Defined Bundle creations. After the user creates a selection of Services and Contents to be part of the User Defined Bundle, the terminal SHALL send a UDBRequest to the BSM where it is assessed and based on the internal policy of the Service Provider, a pricing is made and the BSM SHALL send a PriceOfferingRequest message to the terminal. If the user agrees to the pricing, the terminal SHALL send a PriceOfferingResponse back to the BSM with the userContent set to TRUE. After receiving a positive PriceOfferingResponse the BSM SHALL create PurchaseData and PurchaseItem fragments and SHALL send them to the terminal through the UDBResponse message. After receiving the UDBResponse message the terminal SHALL initiate the Service Request procedure using the information in the received Purchase Fragments. If the user disagrees to the pricing the terminal SHALL send a PriceOfferingResponse message back to the BSM with the userContent set to FALSE. After receiving a negative PriceOfferingResponse the BSM shall send a UDBReponse message with Global Status Code 031 "User must agree to terms of use". If the Service Provider wishes to deny a User Defined Bundle, then the BSM SHALL respond with a UDBReponse message with Global Status Code 011 "Operation Not Permitted".

5.17 Parental Control of Unicast Services

BCAST enables a provider to enforce parental control for services delivered over both unicast and broadcast access methods. Services that can be accessed via a Broadcast Channel typically involve Service and Content Protection which inherently makes it possible to enforce parental control. Additionally, Service and Content Protection can be applied to services that can be accessed via the Interactive Channel and thereby in the same way enforce parental control. Alternatively, Service and Content Protection is not applied to the unicast service and parental control is enforced using basic authentication or digest authentication as described in [RFC 2326] and [RFC 2616] for RTSP services and HTTP services, respectively.

The BCAST server MAY enforce parental control of service consumption for unicast services using the authentication mechanism specified in [RFC 2326] and [RFC 2616] for RTSP services and HTTP services, respectively, with the following input parameters:

- Realm: "parental_control@" concatenated with the service provider domain name (e.g., "parental_control@provider.com")
- Username: The string representation of the MSISDN (e.g., "79261234567")
- Password: The string representation of the parental control PINCODE (e.g., "020579")

When a terminal attempts to access a unicast service, the terminal can be authenticated by the BSM and access to the resource might only be allowed after the user has purchased or subscribed to an associated purchase item as described in

section 5.11. Correspondingly, the BSM MAY determine if parental control verification is needed or not. If the service is subject to parental rating restrictions and is associated with a more restrictive parental rating than the level granted for the terminal, the BCAST server responds with status code 401 (Unauthorized) as described in [RFC 2326] and [RFC 2616] thereby initiating basic authentication or digest authentication with the input parameters listed above.

Note: For each terminal the BSM stores the level granted associated with the terminal (this level is possibly mapped onto several rating systems) along with one parental control PINCODE. How the BSM retrieves and stores the level granted associated with a terminal and the PINCODE associated with a terminal is out-of-scope of this specification.

The terminal MAY support parental control of service consumption for unicast services. A terminal supporting parental control for unicast services MAY ask the user to input the parental control PINCODE in case the BCAST server responds with status code 401 (Unauthorized) as described in [RFC 2326] or [RFC 2616] and the realm begins with "parental_control@". After the user has inputted the PINCODE, it is provided in the password parameter along with the username in the "Authorization" header field. The BCAST server responds with status code 200 (OK) for successful parental control verification and with status code 401 (Unauthorized) for unsuccessful parental control verification.

Note: How the user acquires the parental control PINCODE value is out of scope of this specification. Examples of mechanisms that can be used include post and calling to operator's customer service centre.

5.18 Rich Media Solutions (informative)

This version of the specification describes the support of four Rich Media Solutions (RMS) in BCAST enabler: W3C SVG, 3GPP DIMS, OMA RME and MPEG LASeR.

RMS signaling is besides generic, which allows the support of other RMSs in BCAST (support out of the scope of this specification).

5.18.1 RMS usage scenarios

5.18.1.1 Supported RMS usage scenarios

The following Rich Media Solutions usage scenarios are supported in BCAST:

- **Service Guide presentation**: Service Guide presentation layer instantiated in rich media format, from RMS templates and Service Guide metadata.

  This usage scenario is based on Service Guide function and is signaled in SGDD as per section 5.4.1.5.2 of [BCAST11-SG].

- **Streaming**: one rich media primary stream, eventually associated with other media streams (audio, video, text…), delivered in the context of a BCAST stream delivery service. Rich media content delivered in this context is usable not only for enhanced presentation but for service interactivity as well.

  This usage scenario is based on Stream Distribution function and is signaled in Access fragment as per section 5.1.2.4 of [BCAST11-SG].

  Example: rich media content enriching a TV channel presentation layout and enabling service-related interactivity.

- **File Delivery**: one rich media file delivered in the context of a BCAST file delivery service (e.g. hourly weather forecast clips delivered in a FLUTE session).

  This usage scenario is based on File Distribution function and is signaled in Access fragment as per section 5.1.2.4 of [BCAST11-SG].

  Example: hourly stock market indices delivered as rich media file in a FLUTE session.

- **Notification**: one rich media discrete payload used as the presentation payload of a Notification Message

This usage scenario is based on Notification function and is signaled in Notification message as per section 5.14.3 of this specification.

- **IMD Interactivity**: one rich media file/discrete payload used as a MediaObjectSet of an InteractivityMediaDocument.

  This usage scenario is based on Service Interaction function and is signaled in InteractivityMediaDocument as per section 5.3.6.1.2 of this specification.

- **Preview Data**: one rich media file/ discrete payload used as the presentation of a Preview Data.

  This usage scenario is based on Service Guide function and is signaled in Preview Data fragment as per section 5.1.2.9 of [BCAST11-SG].

These RMS usage scenarios are categorized according to the primary delivery channel of the very first initial scene (see next section), and not according to further operations possibly taking place after the loading of initial scene. In particular:

- Rich-media based interactivity can also take place for scenarios other than "IMD interactivity" scenario.
- Linking to rich media secondary streams can also take place for scenarios other than "Streaming" scenario.
- Linking to media streams (video, audio…) can also take place for scenarios other than "Streaming" scenario.

Other RMS usage scenarios - out of the scope of this specification - can also be supported by the terminal.

5.18.1.2 Scenario instantiations

Instantiations of RMS usage scenarios start by the loading of a rich media initial scene in the rich media client.

From this point, instantiations of RMS usage scenarios have each their own rich media scene data space, even if they are instantiated from the same RMS usage scenario. For instance:

- two Notification messages embedding each a RichMedia element are two distinct instantiations of Notification usage scenario.
- two rich media content files delivered in same file delivery session are two distinct instantiations of File Delivery usage scenario.

5.18.1.3 Collaborating RMS usage scenarios

This section applies to the RMSs supporting scene updates (in this specification: 3GPP DIMS, OMA RME and MPEG LASeR).

Instantiations of RMS usage scenarios cannot collaborate with each other from a rich media scene data standpoint.

More specifically, it is not possible for some rich media content of a scenario instantiation to replace or update the rich media scene of another scenario instantiation. Examples of non-possible cases:

- Rich media content in Notification, updating/replacing the rich media scene of a running Streaming scenario instantiation.
- Rich media content in InteractivityMediaDocument, updating/replacing the rich media scene of a running Streaming scenario instantiation.
- Rich media content in a File Delivery session, updating/replacing a rich media scene of any running scenario instantiation.

This restriction is due to the unidirectional linking structure of the RMSs described in this specification (from scene to update, but not from update to scene):

- a scene can link to sources of scene commands (e.g. update sources, remote interaction points)
- a scene can be delivered in a rich media stream, along with in-stream scene commands
- but a standalone scene command delivered in some other delivery context has no means to reference the scene which it applies to.

This restriction only applies to rich media scene data: nothing prevents two scenes of two different scenario instantiations to reference the same media components (image, video stream…).

5.18.1.4 Concurrent RMS usage scenarios

The terminal can face situations where, while an instantiation of a RMS usage scenario is running, an event triggers the instantiation of a second RMS usage scenario, thus resulting in two rich media scenes running concurrently. Some examples of concurrent instantiations:

- Streaming + Notification scenario instantiations: the BCAST terminal is viewing a TV channel composed of audio, video and rich media streams. And then a Notification Message is received with presentation part encoded in rich media format.
- Streaming + Interactivity scenario instantiations: the BCAST terminal is viewing a TV channel made of audio, video and rich media stream. And then a IMD interactivity session is started (as per Service Guide signaling) with a MediaObjectGroup instantiated by a rich media MediaObjectSet.
- IMD Interactivity + Notification scenario instantiations: a IMD interactivity is started (as per Service Guide signaling) with the active MediaObjectGroup instantiated by a rich media MediaObjectSet. And then a Notification Message is received with presentation part encoded in rich media format.

To cope with these situations, the terminal can follow various strategies:

- Priority can be given to second instantiation, and scene of first instantiation is either aborted or paused or switched to background processing.
- Priority can be given to first running instantiation, and second instantiation is either cancelled or else deferred or else rendered using a non-rich media alternative format (alternative picture, alternative text, other MediaObjectSet, etc.).

These strategies inherently depend on the capabilities of the terminal, and are out of the scope of this specification. Service providers have to be aware anyhow that concurrent instantiations of RMS usage scenarios can degrade rich media experience in some terminals, and thus are to be avoided whenever this can be anticipated.

5.18.1.5 Service switching in Streaming scenario

This section applies to the RMSs supporting the Streaming usage scenario (in this specification: 3GPP DIMS, OMA RME and MPEG LASeR).

When the terminal switches from a BCAST Service 1 to a BCAST Service 2, and if Service 1 comprises a rich media primary stream at least, the following switching transitions are possible depending on Service 2 stream composition:

a. Service 2 comprises no rich media stream, or a rich media stream of a different RMS;

b. Service 2 comprises a different rich media primary stream of same RMS;

c. Service 2 comprises the same rich media primary stream, with same or different secondary streams if any.

In transition (c) in particular, and if the rich media scene is the master of all the media components of the service, service-by-service switching could be done within the rich media client, without invoking BCAST client.

However this behavior does not allow the other transitions (a) and (b). Also it bypasses BCAST information, such as presentation of Preview Data associated to service-by-service switching, or weighted order of the list of services.

Service-by-service switching is therefore assumed to be always controlled by the BCAST client. Rich media content generation needs to be authored accordingly.

Service-by-service switching controlled by BCAST client could appear inefficient however, in the case of transition (c). But implementation-dependent optimizations can be used to achieve some rich media state continuity in rich media client during such service switching transition.

5.18.2 Linking

5.18.2.1 Overview

Binding the many RMS linking mechanisms to the many BCAST delivery methods enables refined but at the same time complex rich media content distribution scenarios. To cope with this potential complexity, this section structures RMS linking methods in three categories: links to scene components, links to update sources and links to remote interaction points.

Scene components:

- A scene component designates any element part of the rich media composition, and referred to by the scene description.
- When external to the scene, the scene component is typically automatically fetched by the rich media client.
- When active in the scene, a component has to be available to the rich media client, otherwise the scene is incomplete and could enter a state error.
- Depending on the RMS, the scene component can be: image, video, audio, text, animation, script, font, foreign object…
- The scene component can be: discrete (e.g. video clip) or continuous (e.g. video stream).
- The scene component can be embedded (e.g. base64-encapsulated video clip, video track) or external (video clip, video stream)
- The scene component can be available over broadcast channel or interaction channel.
- Example of link to scene component: <video xlink:href=” “/>.

Update sources:

- An update source designates a source of unsolicited scene commands referred to by the scene description.
- The update source is typically automatically tuned to by the rich media client.
- The update source can be: discrete (e.g. scene command group, file-embedded secondary scene track) or continuous (e.g. rich media secondary update stream over RTP).
- The update source can be available over broadcast channel or interaction channel.
- Example of link to update source: <updates xlink:href=” “/>

Remote interaction points:

- A remote interaction point is a remote resource accessed upon some user interaction, and which might involve the sending of data.

- The remote interaction point is generally represented as a hyperlink, using various possible URI schemes (“http:”, “sms:”, “mailto:”, “mmsto:” , “tel:”, “sip:”, “rstp:”…)
- The remote interaction point can only be available over interaction channel.
- Accessing the remote interaction point can trigger many kinds of subsequent actions, resulting in scene changes or not: reception of an SMS, return of a scene command group in HTTP response, etc.
- Example of link to remote interaction point: <a xlink:href=” “/>

This specification especially focuses on the scene links which might raise integration concerns with BCAST enabler, i.e. which demand the rich media client to open new delivery contexts:

- Linking to *external* scene components (not including scene-embedded and file-embedded components, and not including external components delivered in-stream for the Streaming usage scenario).
- Linking to update sources.
- Linking to remote interaction points.

5.18.2.2 Primary and secondary delivery channels

In the context of BCAST RMS usage:

- The **primary delivery channel** designates the channel delivering the very first rich media initial scene (or RAP or DRAP) to the rich media client, initial scene which actually starts the RMS usage scenario instantiation.

  In this version of the specification, the primary delivery channel can be either the interaction channel or a specific broadcast channel of a specific BDS.

- A **secondary delivery channel** designates a channel delivering any rich media content associated to the scene of the RMS usage scenario instantiation.

  In this version of the specification, a secondary delivery channel can only be the interaction channel.

At the time of RMS scenario instantiation, the terminal needs to memorize which channel is the primary delivery channel so to resolve some linking issues described in next sections.

The primary delivery channel is defined once and for all at the very start of scenario instantiation. In particular, if over a secondary delivery channel is delivered a “replacing” rich media scene (e.g. LASeR NewScene command), the secondary delivery channel does not become the primary delivery channel.

5.18.2.3 Embedded links encoding a session description

A link value typically contains a reference to a resource. A link value can alternatively contain the resource data itself encoded in base64 , using the “data” URL scheme (defined in [RFC2397]), and provided the resource is a discrete payload and has a well-known media type.

In W3C SVG (and thus in 3GPP DIMS and OMA RME), the “data” URL scheme is the standard way to embed media objects in the scene itself.

Example: <video xlink:href= 'data:video/3gpp;base64,/9j…' />

This specification extends the support of “data” URL scheme in rich media scenes, to encode a SDP as the link value, where the SDP is identified by “application/sdp” media type.

Example: <video xlink:href= 'data:application/sdp;base64,/9j…' />

This mechanism is used in BCAST in particular to declare a reference to a broadcast stream from the scene description. It is an extension to the RMS standards described in this specification.

5.18.2.4 Linking to broadcast streams

This section applies to the RMSs which represent links as URIs in scene descriptions (in this specification: SVG, DIMS, RME and LASeR ML).

A link to a stream distributed over broadcast channel is represented by a SDP encoded in the link value itself, as specified in section 5.18.4.1:

Example1 (media stream) : <video xlink:href= 'data:application/sdp;base64,/9j…' />

Example 2 (updates stream) : <updates xlink:href= 'data:application/sdp;base64,/8i…' />

However, when the primary delivery channel is the interaction channel, the rich media client cannot determine in what type of channel (broadcast channel or unicast channel) the link has to be resolved. This ambiguity is resolved as follows:

- Embedded links to broadcast streams always use the “data” URL scheme encoding a SDP
- Embedded links to unicast streams never use this “data” URL scheme and use instead any other appropriate URI scheme like RTSP:

  Example: <video xlink:href=”rtsp://…” />

Even though, when the primary delivery channel is the interaction channel, the rich media client can still not determine in what broadcast channel (in terms of tuning parameters) of what BDS the broadcast link has to be resolved. This second ambiguity is resolved as follows:

- A rich media scene can only link to broadcast streams if the primary delivery channel is a broadcast channel. In this case, links to broadcast streams are to be resolved in this broadcast channel.

  This rule applies to the link in the scene, and does not prejudge which delivery channel transports the rich media content which creates the ‘broadcast link’ in the scene. It can be the broadcast channel, but it could be the interaction channel as well, if for instance the scene links to a unicast update source delivering a scene command creating the ‘broadcast link’ in the scene. This latter configuration is consistent as long as the originator of unicast update source has enough information to generate the SDP of the broadcast stream distributed in the primary delivery channel.

5.18.2.5 Linking to file delivery sessions

This section applies to the RMSs which define a discrete payload (identified by a MIME type) to carry scene commands (in this specification: OMA RME and 3GPP DIMS).

Using the “data” URL scheme encoding a SDP, an <updates> element could theoretically point to a broadcast FLUTE session carrying scene commands (e.g. RME scene command groups).

This configuration is not supported (and is discouraged), because objects in FLUTE are not delivered in a sequential and fixed order, which is required to deliver scene commands.

5.18.2.6 Linking from ISO base media file format file

The packaging of rich media content in ISO base media file format file is specified in the following RMS specifications: 3GPP DIMS (3GPP file format, other ISO base media file format), OMA RME (which references 3GPP DIMS specification in this regard) and MPEG LASeR (MP4 file format).

Starting from the rich media initial scene embedded in the file (either in a box or in a scene track), linking to other embedded resources is specified in these specifications, but linking to resources external to the file itself is under-specified and subject to interpretation, whether it can be:

- Linking to external discrete or continuous components.
- Linking to external discrete or continuous update sources.
- Linking to remote interaction points (HTTP, SMS, MMS, Email…)

This specification brings no clarification on this matter: BCAST terminals might ignore or might support linking to external resources from rich media scenes initialized by ISO base media file format files.

5.18.2.7 Linking to remote interaction points

Links to remote interaction points are represented as hyperlinks which can contain a variety of URI schemes: “http:”, “sms:”, “mailto:”, “mmsto:” , “tel:”, “sip:”, “rstp:”…

RMS specifications usually leave open the question of support (supported or not, mandatory or not) of URI schemes in scene-embedded hyperlinks.

In this specification:

- for all RMS usage scenarios, support of “http:” is mandated and support of “sms:” is recommended.
- for IMD Interactivity usage scenario, support of “sms:” is mandated.

5.18.2.8 Hybrid broadcast/unicast delivery

The same BCAST service can combine streaming and file delivery sessions over broadcast and/or unicast channels. This benefits to the wide variety of RMS linking mechanisms (for composition, update and remote interaction), and a RMS usage scenario instantiation can potentially involve many channels and sessions in its lifetime.

When the primary delivery channel is the interaction channel, a broadcast channel of a BDS cannot be identified, so all linking from rich media scene can only be in the interaction channel.

- For external scene components, update sources, remote interaction points: in primary delivery channel (i.e. interaction channel).

When the primary delivery channel is a broadcast channel of a BDS, linking from rich media scene has to be resolved as follows:

- For external scene components:
  - Continuous: in primary delivery channel, or in interaction channel “with reservation”
  - Discrete: in interaction channel “with reservation”

  “with reservation” means that the scene has to be composed in such a way that unavailability of interaction channel does not cause a scene rendering failure.

- For update sources:
  - Continuous: in primary delivery channel or interaction channel “with reservation”
  - Discrete: in interaction channel “with reservation”

  “with reservation” means that the scene has to be composed in such a way that unavailability of interaction channel does not cause a scene inconsistency from a user’s perspective. A problematic configuration would be a scene containing no other data than a link to a unicast update source which role would be to deliver scene commands populating the presentation data of the scene.

- For remote interaction points:
  - In interaction channel

5.18.3 W3C SVG

5.18.3.1 Scope

This specification defines the support of W3C SVG Tiny 1.2 Rich Media Solution specified in [W3C SVG Tiny].

This RMS is identified in RichMedia Capabilities element by type="1", version="1.2" and profile="tiny".

The signaling allows other versions and profiles of W3C SVG to be potentially used as BCAST RMSs, if appropriate.

W3C SVG is a usable RMS for all the RMS usage scenarios listed in section 5.18.1.1, except Streaming usage scenario.

5.18.3.2 Signaling

For W3C SVG Tiny, the RichMedia element included in Access fragment, PreviewData fragment, Notification message and InteractivityMediaDocument is populated as follows:

- In Capabilities element, "type" attribute is set to "1" (W3C SVG)
- In Capabilities element, "version" attribute is set to the "version" attribute value of <svg> element (e.g. "1.2").
- In Capabilities element, applicable "MIME type" element values for SVG discrete payloads are summarized below:
  - "image/svg+xml": SVG document.
- In MIMEType sub-element of Capabilities element, "codec" is unspecified in this version of the specification.
- In Complexity element, "profile" attribute is set to the "baseProfile" attribute value of the SVG document (e.g. "none", "tiny", "basic", "full").
- In Scripting element, the list of "MIMEType" corresponds to the MIME types found in "contentScriptType" attribute of <svg> element, and in "type" attribute of <script> and <handler> elements.

In File Delivery usage scenario, where RichMedia signaling in Access fragment applies to multiple SVG documents, elements and attributes instantiated once apply to all SVG documents delivered in the session, whereas elements instantiated more than once (like MIMEType) apply to some SVG documents delivered in the session.

5.18.4 3GPP DIMS

5.18.4.1 Scope

This specification defines the support of 3GPP DIMS Rel8 Rich Media Solution specified in [3GPP TS 26.142].

This RMS is identified in RichMedia Capabilities element by type="4" and version="Rel8".

The signaling allows other versions of 3GPP DIMS to be potentially used as BCAST RMSs, if appropriate.

3GPP DIMS is a usable RMS for all the RMS usage scenarios listed in section 5.18.1.1, with one reservation: 3GPP DIMS would not be suitable for BCAST Interactivity scenario if linking to external resources in 3GP file-embedded scenes is not supported by the terminal.

5.18.4.2 Signaling

For 3GPP DIMS, the RichMedia element included in Access fragment, PreviewData fragment, Notification message and InteractivityMediaDocument is populated as follows:

- In Capabilities element, “type” attribute is set to “4” (3GPP DIMS)
- In Capabilities element, “version” attribute is set to “Rel” followed by the release number (e.g. “Rel7”, “Rel8”).
- In Capabilities element, applicable “MIME type” element values for a DIMS file or discrete payload are summarized below:
  - “video/3gpp”: 3GP file embedding DIMS content (box-embedded DIMS scene and/or DIMS scene track), and either one video track at least or no audio track.
  - “audio/3gpp”: 3GP file embedding DIMS content (box-embedded DIMS scene and/or DIMS scene track), and no video track and at least one audio track.
  - “video/mp4”: MP4 file embedding DIMS content (DIMS scene track), and at least one video track.
  - “audio/mp4”: MP4 file embedding DIMS content (DIMS scene track), and no video track and at least one audio track.
  - “application/mp4”: MP4 file embedding DIMS content (DIMS scene track), and no video track and no audio track.
  - Any other MIME type of other ISO Base Media file format embedding DIMS content
- In Capabilities element, applicable “MIME type” values for a DIMS stream is summarized below:
  - “video/richmedia+xml”: DIMS data stream over RTP
- In MIMEType sub-element of Capabilities element, “codec” attribute value contains the semi-colon separated list of DIMS stream parameters specified in section 11.1 of [3GPP TS 26.142] (e.g.”Version-profile=10; Level=20;”).

  Note: this list of DIMS stream parameters, although a subset only of the parameters contained in DIMS file boxes, is sufficient to describe also File Delivery usage scenario.
- In Complexity element, “profile” attribute value can be omitted since “Version-profile” and “Level” parameters are already provided in “codec” value.
- In Scripting element, the list of “MIMEType” values corresponds to the MIME types found in “content_script_types” parameter of DIMS file boxes, or found in DIMS units (in “contentScriptType” attribute of <svg> element or , and in “type” attribute of <script> and <handler> elements).

In Streaming and File Delivery usage scenario, where RichMedia signaling in Access fragment applies to multiple DIMS units or files, elements and attributes instantiated once apply to all DIMS units delivered in the session, whereas elements instantiated more than once (like MIMEType) apply to some DIMS units or files delivered in the session.

5.18.5 OMA RME

5.18.5.1 Scope

This specification defines the support of OMA RME 1.0 Rich Media Solution specified in [RME].

This RMS is identified in RichMedia Capabilities element by type=”2” and version=”1.0”.

The signaling allows other versions of OMA RME to be potentially used as BCAST RMSs, if appropriate.

OMA RME is a usable RMS for all the RMS usage scenarios listed in section 5.18.1.1.

5.18.5.2 Signaling

For OMA RME, the RichMedia element included in Access fragment, PreviewData fragment, Notification message and InteractivityMediaDocument is populated as follows:

- In Capabilities element, "type" attribute is set to "2" (OMA RME)
- In Capabilities element, "version" attribute is set to "1.0" text string or other version
- In Capabilities element, applicable "MIME type" element values for a RME file are summarized below:
  - "application/richmedia+xml": RME initial scene
  - "application/richmediacommands+xml": RME scene command group
  - "multipart/related": RME MIME multipart
  - "video/3gpp": 3GP file embedding RME content (box-embedded RME scene and/or RME scene track), and either one video track at least or no audio track.
  - "audio/3gpp": 3GP file embedding RME content (box-embedded RME scene and/or RME scene track), and no video track and at least one audio track.
  - "video/mp4": MP4 file embedding RME content (RME scene track), and at least one video track.
  - "audio/mp4": MP4 file embedding RME content (RME scene track), and no video track and at least one audio track.
  - "application/mp4": MP4 file embedding RME content (RME scene track), and no video track and no audio track.
  - Any other MIME type of other ISO base media file format file embedding RME content.
- In Capabilities element, applicable "MIME type" values for a RME stream is summarized below:
  - "video/richmedia+xml": RME data stream over RTP.
- In MIMEType sub-element of Capabilities element, "codec" attribute value contains the semi-colon separated list of RME stream parameters specified in section 11.1 of [3GPP TS 26.142] (e.g."Version-profile=10; Level=20;").

  Note: this list of RME stream parameters, although a subset only of the parameters contained in RME (DIMS) file boxes, is sufficient to describe also File Delivery usage scenario.
- In Complexity element, "profile" attribute value can be omitted since "Version-profile" and "Level" parameters are already provided in "codec" value.
- In Scripting element, the list of "MIMEType" values corresponds to the MIME types found in "content_script_types" parameter of RME file boxes, or found in RME units (in "contentScriptType" attribute of <svg> element or , and in "type" attribute of <script> and <handler> elements).

In Streaming and File Delivery cases, where RichMedia signaling in Access fragment applies to multiple RME units or files, signaling elements and attributes instantiated once apply to all RME units/files delivered in the session, whereas signaling elements instantiated more than once (like MIMEType) apply to some RME units/ files delivered in the session.

5.18.6 MPEG LASeR

5.18.6.1 Scope

This specification defines the support of MPEG LASeR 2nd Edition Rich Media Solution specified in [ISO/IEC 14496-20].

This RMS is identified in RichMedia Capabilities element by type="3" and version="2008".

The signaling allows other versions of MPEG LASeR to be potentially used as BCAST RMSs, if appropriate.

MPEG LASeR is a usable RMS for all the RMS usage scenarios listed in section 5.18.1.1.

5.18.6.2 Signaling

For MPEG LASeR, the RichMedia element included in Access fragment, PreviewData fragment, Notification message and InteractivityMediaDocument is populated as follows:

- In Capabilities element, "type" attribute is set to "3".
- In Capabilities element, "version" attribute is set to a space-separated string list of the year of specification edition followed if applicable by amendments – using "Amd#" pattern - and corrigenda – using "Cor#" pattern.

  Examples: "2006 Cor1 Cor2 Amd1", "2008", "2008 Amd2 Amd3"

- In Capabilities element, applicable "MIME type" element values for a LASeR discrete payload/file are summarized below:
  - "application/laser+xml": file embedding a LASeR ML unit.
  - "application/laser+saf": file embedding a sequence of SAF packets carrying (at least) LASeR units in binary syntax.
  - "video/mp4": MP4 file embedding LASeR content (box-embedded LASeR unit and/or LASeR scene track), and at least one video track.
  - "audio/mp4": MP4 file embedding LASeR content (box-embedded LASeR unit and/or LASeR scene track), and no video track and at least one audio track.
  - "application/mp4": MP4 file embedding LASeR content (box-embedded LASeR unit and/or LASeR scene track), and no video track and no audio track.
  - Any other MIME type of other ISO base media file format file embedding LASeR content.
- In Capabilities element, applicable "MIME type" values for a LASeR-enabled stream is summarized below:
  - "application/laser+saf": SAF stream over RTP carrying at least a LASeR stream in binary syntax.
  - "application/laser": LASeR ML stream over RTP.
- In MIMEType sub-element of Capabilities element, "codec" attribute is unspecified in this version of specification.
- In Complexity element, "profile" attribute is either omitted, or set to "full" or "core" or "mini".
- In Scripting element, the list of "MIMEType" corresponds to the MIME types found in "contentScriptType" attribute of the scene, and in "type" attribute of "script" and "handler" elements.

In Streaming and File Delivery usage scenarios, where RichMedia signaling in Access fragment applies to multiple LASeR units or files, signaling elements and attributes instantiated once apply to all LASeR units/files delivered in the session, whereas signaling elements instantiated more than once (like MIMEType) apply to some LASeR units/ files delivered in the session.

5.18.7 Other RMS

The RMS generic signaling allows other Rich Media Solutions to be potentially used as BCAST RMSs, if appropriate.

These RMSs can support any of the RMS usage scenarios listed in section 5.18.1.1.

5.18.7.1 Signaling

For other RMSs, the RichMedia element included in Access fragment, PreviewData fragment, Notification message and InteractivityMediaDocument is populated as follows:

- In Capabilities element, "type" attribute is set to "0" (any other MIME type).
- Version, profile, MIMEtype value(s) and associated codec parameter(s) need to be explicit enough so to allow the terminal to clearly identify the RMS in use and the complexity of associated rich media content.

5.19 Smartcard Broadcast Provisioning

The Smartcard Broadcast Provisioning function provides a way to send files to a Smartcard using the Broadcast bearer.

The Smartcard Broadcast Provisioning function uses FLUTE protocol to convey the files to the terminal.

The Smartcard Broadcast Provisioning is OPTIONAL for Network, Terminal and Smartcard.

5.19.1 Declaring Smartcard Broadcast Provisioning as a Service within the Service Guide

The Smartcard Broadcast Provisioning function SHALL be declared as a service in the service guide:

- There SHALL be at least one Service fragment with the attribute "ServiceType" equals to "13 –Smartcard Provisioning services"
- There SHALL be at least one Access fragment that specifies the access to the above-mentioned service:
    - The AccessType SHALL contain
        - "BroadcastServiceDelivery" element, which defines the BDSType used for the delivery of files and the Session Description information used by the terminal to access to the service.
        - The ServiceClass used for the Smartcard Broadcast Provisioning function is "urn:oma:bcast:oma_bsc:sp:1.1" as defined in OMNA registry.
        - SmartcardProvisioningReception element, which specifies which devices are concerned by the Smartcard Broadcast Provisioning files through the SubscriberGroupIdentifier and the access technology used to send the files to the Smartcard.
- If multiple small payloads are sent to the Smartcard in period of time, one content fragment MAY be defined for these multiple payloads and a schedule fragment defines the DistributionWindow in which the referenced content is available for delivery. In this case, the schedule fragment SHALL not contain content location and the terminal will retrieve all payloads described in the FDT.
- If large content is sent to the Smartcard intermittently, then a content fragment for each large payload MAY be defined and a schedule fragment defines the distribution time in which the content is available for delivery.

5.19.2 Declaring Smartcard Broadcast Provisioning support in the Smartcard

If the Smartcard supports the ADF_BSIM (as defined in [BCAST11-ServContProt], the support of the Smartcard Broadcast Provisioning function by the Smartcard SHALL be signalled in the EF_{BST} under the ADF_BSIM as defined in [BCAST11-ServContProt].

If the Smartcard doesn't support the ADF_BSIM, the support of the Smartcard Broadcast Provisioning function by the Smartcard SHALL be signalled in the EF_{BST} under the DF BCAST under the USIM, CSIM or R-UIM as defined in [BCAST11-ServContProt].

The terminal SHALL discover the support of Smartcard Broadcast Provisioning in the Smartcard reading EF_{BST} under the ADF BSIM if this ADF is present or under the DF BCAST under the USIM, CSIM or R-UIM otherwise.

If ADF_BSIM is not present and EF_{BST} under DF BCAST is not present or DF BCAST is not present,

Smartcard Broadcast provisioning is not supported by the Smartcard.

The Terminal SHALL ignore the announcement of Smartcard broadcast provisioning services, if the Smartcard doesn't support the Smartcard Broadcast Provisioning function.

5.19.3 Filtering of Smartcard Broadcast Provisioning Services

The terminal SHALL filter the Smartcard Provisioning services according to Subscriber Group Identifier defined in the SubscriberGroupIdentifier element in the Addressing element of the Access fragment of the service guide if present. If the Terminal is not able to retrieve in the Smartcard or in the BCAST MO the information necessary for the filtering announced in the service guide and described below, the Terminal SHALL ignore the announcement for such services in the service guide.

If the Addressing element is absent, all Smartcards supporting the Smartcard Broadcast Provisioning function are targeted and the Terminal SHALL NOT perform address filtering as specified in [BCAST11-SG] The Terminal SHALL transmit the related content to the Smartcard if the Smartcard supports the Smartcard Broadcast Provisioning function.

The SubscriberGroupIdentifier element is of SubscriberGroupIdentifier type, defined below in "urn:oma:xml:bcast:sg:fragments:1.1" namespace:

```
<complexType name="SubscriberGroupIdentifier">
  <sequence>
    <choice>
      <element name="subscriberGroupBase" type="base64Binary"/>
      <sequence>
        <element name="flexibleGroupAddress" type="base64Binary"/>
        <element name="uniqueSmartcardFilter" type="base64Binary" minOccurs="0"/>
      </sequence>
    </choice>
    <choice minOccurs="0">
      <element name="subscriberAccessMask" type="base64Binary"/>
      <element name="subscriberPosition" type="base64Binary"/>
    </choice>
  </sequence>
</complexType>
```

The SubscriberGroupIdentifier MUST contain *either* a <**subscriberGroupBase**> element *or* a <**flexibleGroupAddress**> element. If a Device in a Fixed Subscriber Group is addressed, the <**subscriberGroupBase**> element MUST be present. If a Device in a Flexible Subscriber Group is addressed, the <**flexibleGroupAddress**> element MUST be present and the <uniqueDeviceFilter> element MAY be present.

In the scope of BCAST1.1, only the Fixed Subscriber Group addressing is defined with a group size of 2^n Smartcards, group size defined in the SmartcardProvisioningReception element as defined in [BCAST11-SG]. In this case the <**subscriberGroupBase**> MUST be present and depending of the addressing mode (whole subscriber group, subset of the subscriber group, or a unique Smartcard in the subscriber group), <**subscriberAccessMask**> or <**subscriberPosition**> MAY be present:

- If the whole subscriber group is addressed, then only <**subscriberGroupBase**> element is present
- If unique Smartcard in the subscriber group is addressed, then the <**subscriberGroupBase**> element is present and the <**subscriberPosition**> element is present
- If a subset of the subscriber group is addressed, then the <**subscriberGroupBase**> element is present and the <**subscriberAccessMask**> element is present

<**subscriberGroupBase**> element contains the base64 representation of the fixed group address. The size depends on the group size. For a group size of 2^n Smartcards, this size is 40 – n bits. When this size is not a multiple of 8 bits, the fixed group address value SHALL be zero-bit left-padded before base64 encoding.

<subscriberPosition> element contains the base64 coding of the fixed position in the group of the Smartcard addressed. The size depends on the group size. For a group size of 2^n Smartcards, this size is n bits. When this size is not a multiple of 8 bits, the fixed position value SHALL be zero-bit left-padded before base64 encoding.

<subscriberAccessMask> element is used to define which Smartcards in the group are addressed. It is a Eurocrypt style bit access mask added to the group address. Each device in the subscriber group has a unique position in that group. The bit in the bit access mask at this position determines whether the Smartcard is addressed or not.

In case of Fixed Subscriber Group addressing, the Unique Smartcard Filter (USF) is used and compared with SubscriberGroupBase and SubscriberPosition to determine if the Smartcard is concerned by the file as follows:

- In the case of a group size of 256 devices, the first 32 bits of the USF contain the fixed_group_address field, whilst the last 8 bits contain the fixed_position_in_group field. If the whole Fixed Subscriber Group is addressed, the first 32 bits of the USF are compared to the SubscriberGroupBase in the SubscriberGroupIdentifier element. If a unique Smartcard in the Fixed Subscriber Group is addressed, the last 8 bits (fixed_position_in_group field) are additionally compared to the subscriberPosition in the SubscriberGroupIdentifier element. When a subset of a fixed group is addressed, the subscriberAccessMask can be used to define to which Smartcards in the group the file is addressed to. Terminals connected to Smartcard not listed in the subscriberAccessMask will ignore the file.
- In the case of a group size of 512 devices, the first 31 bits of USF contain the fixed_group_address field whilst the last 9 bits contain the fixed_position_in_group field. If the whole Fixed Subscriber Group is addressed, the first 31 bits of the USF are compared to the SubscriberGroupBase in the SubscriberGroupIdentifier element. If a unique Smartcard in the Fixed Subscriber Group is addressed, the last 9 bits (fixed_position_in_group field) are additionally compared to the 8bits of subscriberPosition and the most significant bit (padding bit) of the subscriberGroupBase in the SubscriberGroupIdentifier element. When a subset of a fixed group is addressed, the subscriberAccessMask can be used to define to which Smartcards in the group the file is addressed to. Terminals connected to Smartcard not listed in the subscriberAccessMask will ignore the file.
- In case of a group size of 2^n devices, The first (40-n) bits of USF contain the fixed_group_address field whilst the last n bits contain the fixed_position_in_group field. If the whole Fixed Subscriber Group is addressed, the first (40-n) bits of the USF are compared to the SubscriberGroupBase in the SubscriberGroupIdentifier element. If a unique Smartcard in the Fixed Subscriber Group is addressed, the last n bits (fixed_position_in_group field) are additionally compared to the subscriberPosition of the subscrinberGroupBase in the SubscriberGroupIdentifier element. When a subset of a fixed group is addressed, the subscriberAccessMask can be used to define to which Smartcards in the group the file is addressed to. Terminals connected to Smartcard not listed in the subscriberAccessMask will ignore the file.

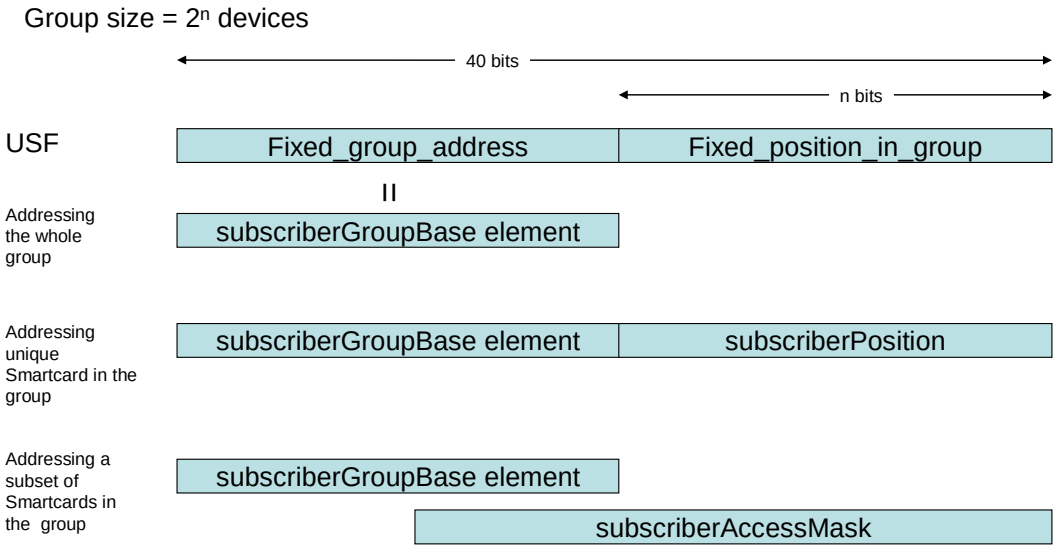


Figure 4: Filtering in Smartcard Broadcast provisioning

The USF is stored either in the EF_{USF} under the ADF_BSIM in the Smartcard or in EF_{USF} under the DF BCAST defined under the USIM, CSIM or R-UIM of the Smartcard (as defined in [BCAST11-ServContProt]), or retrieved from the BCAST MO. The EF_{USF} under the ADF_BSIM takes precedence to the others and EF_{USF} under the DF BCAST takes precedence to the BCAST MO.

5.19.4 Transmission of files to the Smartcard

Two types of technology are defined in this version of specification to transmit the files from the terminal to the Smartcard. The type of Smartcard Access is signalled in the SmartcardAccess element in the Access fragment.

- When the Technology attribute of the SmartcardAccess element is "0 – Envelope", the file SHALL contain command in the format of SMS. The class of this SMS message SHALL be class 2 indicating that the destination of the SMS is the Smartcard (as defined in [3GPP TS 23.040])
- When the Technology attribute of the SmartcardAccess element is "1 – SCWS", the file SHALL contain HTTP commands.

5.19.4.1 Envelope Technology

In this mode, a Command Packet is encapsulated in a secured packet (as defined in [3GPP TS 31.115] for 3GPP or [3GPP2 C.S0078-0] for 3GPP2) which is generally secured to provide either or both of source authentication, data protection and data integrity. The definition of the key used for this security process is out of scope of this specification.

A Command Packet can be longer than what can be carried into a single SMS. In this case it is split into several pieces concatenated together using the 03.40 Packet Format (as defined in [3GPP TS 23.040]). The resulting pieces are called Envelopes. They are all the same size, the maximum size of an SMS, except the last one.

In this mode, the terminal SHALL use the ENVELOPE COMMAND defined in [ETSI TS 102.221] to transmit the file to the Smartcard.

5.19.4.2 SCWS Technology

In this mode, the terminal will transfer the file to SCWS as defined in [OMA SCWS11]. The local transport protocol between terminal and SCWS can be Bearer Independent Protocol (BIP) in case the Smartcard uses ISO APDU defined in [ETSI TS 102.221] or TCP/IP in case the Smartcard uses High Speed Protocol (HSP) defined in [ETSI TS 102.600].

When the terminal receives a file targeting a Smartcard and the Technology for the Smartcard Broadcast Provisioning service signalled in the Access fragment of the service guide is SCWS,

- if the terminal does not support SCWS, the terminal SHALL discard message
- if the terminal supports SCWS, but Smartcard does not support SCWS, the terminal SHALL discard the message
- if the terminal supports SCWS, and Smartcard supports SCWS, the terminal SHALL transfer the message to Smart Card Web Server (SCWS).

Terminal will choose to send message to localhost (loopback address 127.0.0.1), or localuicc (TCP/IP), depending on the underlying transport protocol that is implemented in the terminal.

HTTP request type specified in the service guide in the SmartcardAccess element of the Access fragment SHALL be used to transfer the file to SCWS.

URL of the application SHALL be the URL defined in the URL element of the SmartcardAccess Element in Access fragment.

Data body contains the file transported on FLUTE.

5.20 Audience Measurement Function

The Audience Measurement Function provides to the service provider measures on the user consumption of BCAST contents and services. The measures are processed on the client side and collected by a collection function on the server side. The measures are then analyzed to produce statistics on them.

The Audience Measurement Function allows a remote configuration of the Audience measurement parts on the client side to activate/deactivate the metering and the reporting, to setup the parameters used for the audience measurement process (e.g. the list of metrics, the report delivery frequency,..).

The Audience Measurement Function provides also means for the user to opt-in to the measuring and be included in a panel of users for a given Audience Measurement Campaign.

The Client Audience Measurement Function could be implemented in the Terminal in case of Terminal-Centric Audience Measurement implementation or in the Smartcard in case of Smartcard-Centric Audience Measurement implementation.

An architectural overview of the Audience Measurement function appears in [BCAST11-Architecture]

This specification proposes two profiles for the Audience Measurement system:

- A Terminal-centric solution where the Audience Measurement of the client side (BCAST AM-C) as defined in [BCAST11-Architecture] is implemented on the Terminal and,
- A Smartcard-centric solution where the Audience Measurement of the client side (BCAST AM-C) as defined in [BCAST11-Architecture] is implemented on the Smartcard.

5.20.1 Terminal-Centric Audience Measurement

The Terminal-Centric Audience Measurement provides a solution of audience monitoring, by introducing the Audience Measurement in the Terminal on the client side. The Terminal-Centric solution offers secure processing for the Audience Measurement process controlled by the agreement (Opt-In) of the user, and a secure storage of measures on the client side.

The Terminal-Centric Audience Measurement function allows a remote configuration of the function on the client side.

Note: Secure processing and secure storage of measurement data are implementation specific and out of scope of this specification.

5.20.1.1 Process description

The following sections detail each step involved in the Terminal-Centric Audience Measurement function.

5.20.1.1.1 Registration Process

The Registration process is used to populate a BCAST AM-M clients database. BCAST AM-M MAY use the database to facilitate the selection of the panel of users for an Audience Measurement campaign.

Registration is OPTIONAL. How the Registration is performed, is out of the scope for this version of the specification.

5.20.1.1.2 Opt-In Process

The Opt-In process is used to call a user to participate a specific Audience Measurement campaign. BCAST AM-M provides an invitation to BCAST AM-C, asking it participate a specific Audience Measurement campaign. After consulting the user (directly or indirectly), BCAST AM-C responses whether it will or will not participate in the campaign. In case Terminal will participate the campaign, the BCAST AM-M provides the configuration data for the campaign.

Opt-In process starts by BCAST AM-M sending an Audience Measurement Trigger (**AM Trigger**) message (see section 5.20.1.2.1). The AM Trigger message MAY be sent over Broadcast Channel or Interaction Channel.

- The AM Trigger message MAY be sent over Broadcast Channel in Service Guide. In this case, the message is targeted to all Terminals receiving the SG.
- The AM Trigger message MAY be sent over Interaction Channel in Service Guide. In this case, the message is targeted to the Terminal receiving the AM Trigger message.
- The AM Trigger message MAY be sent over SMS bearer, over Interaction Channel. In this case, the message is targeted to the Terminal receiving the AM Trigger message. This SMS message MAY either include the full AM Trigger message, or just serve as a trigger to download that message. See section5.20.1.1.7 for details on SMS delivery.

To prevent unauthorized parties opening campaigns and possibly collecting measurement data from the users, Terminal SHALL verify ServerAddressURL in AM Trigger message in the following ways:

- Terminal MAY map the ServerAddressURL in the AM Trigger message with the ServerAddressURL of AudienceMeasurement element received in SGDD (see [BCAST11-SG]). If the address in AM Trigger message is not found in the AudienceMeasurement element in SGDD, verification fails.
- Other methods not specified in this specification, for example authentication provided by a trusted party, MAY be used.

If the verification fails, Terminal SHALL ignore the AM Trigger message. Otherwise, Terminal SHALL continue the Opt-In process as described further below in this section.

If the AM Trigger message attribute consentRequired is false, Terminal MAY perform a silent Opt-In, which MAY result "Refuse" (opted-out) or "Accept" (opted-in).

If the AM Trigger message attribute consentRequired is true, Terminal MAY perform a silent Opt-In, which MAY result "Refuse" (opted-out), but SHALL NOT result "Accept" (opted-in).

The BCAST AM-M may wish to have a random panel of users participating in the Audience Measurement campaign. In such case, the BCAST AM-M MAY select to deliver the AM Trigger message over Broadcast Channel, and provide the randomSelector to indicate the percentage of user wished to participate in the campaign.

If the AM Trigger message was received over Broadcast Channel in SGDD, Terminal SHALL generate a random decimal value between 0 (exclusive) and 100 (inclusive). If the generated value is less than or equal to the value of the randomSelector in the AM Trigger message, the Terminal SHALL continue the Opt-In process as described further below in this section. Otherwise, the Terminal SHALL silently ignore the AM Trigger message.

If the AM Trigger message attribute consentRequired is false, the Terminal MAY use silent Opt-In, in which case the user is not consulted directly, but a pre-set answer is used instead.

For example, if the received AM Trigger message contains a campaignID in which the current user has already accepted to participate, the Terminal MAY silently assume user acceptance. Note that the AM Trigger message can be used to trigger the process of providing new configuration data for the existing campaign, for which a user of the Terminal has already accepted to participate.

A pre-set answer MAY be acquired from the user and stored into the Terminal by some other means, which are out of scope of this specification. For example, user's acceptance for some or all Audience Measurement campaigns could be part of the contract between the operator and the user.

If the AM Trigger message contains the campaignStartTime, and if the current time has passed the campaignStartTime, and the current user of the Terminal has not opted-in to the campaign referred in the AM Trigger message attribute campaignID, Terminal SHOULD silently result "Refuse" (silent opt-out).

It is OPTIONAL for a Terminal to support more than one simultaneous Audience Measurement campaigns. If a Terminal has an active Audience Measurement campaign when receiving an AM Trigger message for a different campaign, the Terminal MAY silently result "Refuse".

If the AM Trigger message attribute consentRequired is true, and the Terminal did not silently refuse the invitation, the Terminal SHALL consult the user for the participation in the campaign. In such case, the result of the Opt-In process is according to the user choice.

Note that within a Terminal the Opt-In process is user specific. The Terminal SHALL not assume "Accept" for other users of the Terminal, only if some users have accepted an invitation to participate an Audience Measurement campaign.

When the answer ("Accept" or "Refuse") to the campaign invitation is known, Terminal SHOULD respond to the AM Trigger message by sending an Audience Measurement Request (**AM Request**) message (see section 5.20.1.2.2). If sent, the AM Request SHALL be sent over the Interaction Channel, to the URL provided in the AM Trigger message. In case the Opt-In process answer to the campaign invitation was "Accept", the AM Request message SHALL contain the userConsent attribute set to true. (Note that omitting the userConsent attribute from the AM Request implies that the output was "Refuse".)

If the Terminal sends an AM Request message indicating a "Refuse" (opted-out), against the campaign invitation the BCAST AM-M SHALL remove the Terminal/user combination from the panel of users of the campaign, and respond with AM Response message, with campaignEndTime set to past (indicates that the campaign has closed for the user identified in userID of the AM Request message).

If the AM Request message indicates an "Accept" (opted-in), the BCAST AM-M SHALL respond with an Audience Measurement Response (**AM Response**) message (see section 5.20.1.2.3). This message SHALL contain the configuration data for the campaign (see section 5.20.1.1.3). If the globalStatusCode anything else than by 000 ("Success"). Terminal SHALL consider the campaign closed for the associated user (identified by the userID in the corresponding AM Request message). In particular, the global status code value 036 can be returned to reject a Terminal to participate in a campaign.

The protocol used for AM Request and AM Response messages is HTTP(S), according to the URL provided in the AM Trigger message attribute ServerAddressURL, with the MIME type set to application/vnd.oma.bcast.am-message+xml (see appendix I.8).

5.20.1.1.3 Configuration Process

Each campaign has its own configuration data, including such information as what to measure, when to report, and where to report, etc.

Configuration data is provided to a Terminal at the end of the Opt-In process (see section5.20.1.1.2), using the Audience Measurement Response (**AM Response**) message (see section 5.20.1.2.3).

Configuration data of a Terminal that has accepted to be part of a campaign MAY be changed during the campaign. In such case, BCAST AM-M sends an Audience Measurement Trigger (**AM Trigger**) message over Interaction Channel to the Terminals being part of the campaign. When sending AM Trigger message to change the configuration data of an existing campaign, the AM Trigger message SHALL be sent over Interaction Channel. For the process triggered by an incoming AM Trigger message, see section5.20.1.1.2. The configuration of a Terminal MAY also be changed by AM-M in the response (AMRR) to a measurement report (AMRD).

Terminal MAY support pushed AM Response message, allowing BCAST AM-M to push updated configuration data to the Terminal. Such pushed AM Response message can be used e.g. to activate or de-activate a previously opted-in campaign. When pushed AM Response message is supported, BCAST AM-M MAY send an AM Response message to an opted in Terminal.

On receiving Configuration data during a campaign, the AM-C SHALL check if the version of the received Configuration data is having higher value than the stored Configuration data version. If the version is less or equal, the AM-C ignores the received Configuration data

Configuration data is campaign and user specific. Each user of a Terminal has its own configuration data for each campaign the user has opted-in.

5.20.1.1.4 Measurement Process

The Measurement process is for collecting data as configured in the configuration data of the Audience Measurement campaign.

During a campaign, Terminal SHALL NOT delete any Audience Measurement data of the campaign before the data has been reported to the AM-M (see section 5.20.1.1.5). When the campaign ends, Terminal SHOULD report all the measured data, and MAY delete all the Audience Measurement data for that campaign.

The end time of the Measurement process of a given campaign is configured in the configuration data of the campaign. Note that the configuration data MAY be changed during the campaign. This can be used e.g. to deactivate an active campaign.

How the Measurement process in further detail is performed, is out of the scope for this version of the specification.

The monitored events are defined in the configuration data of the campaign. Events and the associated parameters can include the followings:

- Service Consumption
    - Service ID
    - Start time of consumption
    - End time of consumption
- Recording Consumption
    - Service ID
    - Start time of recording
    - End time of recording
    - Start time of consumption of recorded content
    - End time of consumption of recorded content

It is OPTIONAL for a Terminal to support more than one simultaneous Audience Measurement campaigns. How terminal would manage simultaneous campaigns is out of scope for this version of the specification.

Audience Measurements of selected services or contents might be disallowed due to specific regulatory requirements.

Attribute ‘amAllowed’ that is specified in ‘Service’ and ‘Content’ fragments of the BCAST Service Guide [BCAST11-SG] provides the necessary signalling to disallow measurement of a service or a content consumption even if the user has accepted Opt-in for an audience measurement campaign.

Terminal-Centric Audience Measurement SHALL obey the limitations for audience measurement signalled by the ‘amAllowed’ attribute in the BCAST Service Guide [BCAST11-SG].

5.20.1.1.5 Reporting Process

In the Reporting process, Terminal that has accepted to participate in an Audience Measurement campaign sends measured data of the campaign to the BCAST AM-M, as defined in the configuration data of the campaign.

Note that this section applies only on Terminals and users that have accepted to participate in the associated Audience Measurement campaign.

The BCAST AM-C SHALL send the report to the BCAST AM-M depending on the report delivery parameters which have been set during the configuration process, or upon specific request from the BCAST AM-M. The BCAST AM-M can store the measurement results in a database. Note that it is expected the service provider takes necessary precautionary measures to store the measurement data in a secure manner in order to prevent non-authorised use. How this is achieved is out of scope of this specification.

The Terminal SHALL NOT perform the reporting if the opted-in user is not present. For example, if the user is identified by the SIM (IMSI), reporting is performed only when the relevant SIM is present in the Terminal.

BCAST AM-C SHOULD be able to send a report to BCAST AM-M based on an internal event of the Terminal. BCAST AM-C SHOULD send a un-scheduled report to the BCAST AM-M in case of danger of loss of measurement data, e.g., due to insufficient storage capacity. BCAST AM-M SHOULD be prepared to receive un-scheduled (‘ad hoc’) reports from the BCAST AM-C.

The BCAST AM-C SHALL send the Audience Measurement data to the BCAST AM-M in an Audience Measurement Report Delivery (**AMRD**) message (see section 5.20.1.2.4). The AMRD message SHALL be transported over HTTP(S), as configured with the configuration data of the campaign (see section 5.20.1.1.3), with the MIME type set to application/vnd.oma.bcast.am-message+xml (see appendix I.8).

While sending the AMRD message, the BCAST AM-C SHALL continue Measurement process (see section 5.20.1.1.4), according to the configuration data.

The BCAST AM-M SHOULD respond to an incoming AMRD message with an Audience Measurement Report Response (**AMRR**) message (see section 5.20.1.2.5), using the same protocol for message delivery as used for AMRD message. When BCAST AM-C receives the AMRR message with globalStatusCode 000 (“Success”), BCAST AM-C SHOULD delete the reported Audience Measurement data.

When BCAST AM-M explicitly wants to request a reporting from a specific BCAST AM-C, it SHALL send an Audience Measurement Report Trigger (**AMRT**) message (see section5.20.1.2.6) to the BCAST AM-C This message is sent over SMS (see section 5.20.1.1.7). It either carries the actual AMRT data, or a link from which the AM-C can download the AMRT data via HTTP(S). For pull delivery over HTTP(S) following an SMS Trigger, the structure is specified in section 5.20.1.2.6. When receiving AMRT message to an open campaign, Terminal SHALL enter the Reporting process and send an AMRD message to the BCAST AM-M.

If the BCAST AM-M intends to reconfigure a Terminal, it MAY include an AudienceMeasurementConfigurationData element into the response (AMRR) to the measurement report (AMRD).

5.20.1.1.6 Opt-Out process

The Opt-Out process is for stopping a user from participating in Audience Measurement Campaign(s) in which the user is currently participating. Many ways are supported for the Opt-Out process. Below are described some of the options.

The User MAY contact the BCAST AM-M (off-line), and request to be opted out. In such case, the BCAST AM-M sends to the Terminal an Audience Measurement Trigger (**AM Trigger**) message, with consentRequired set to true. User would be consulted, and the user would respond "Refuse". Terminal then sends Audience Measurement Request (**AM Request**) message, and server responds with Audience Measurement Response (**AM Response**) message with campaignEndTime set to past.

The BCAST AM-M MAY initiate opt-out by sending an **AM Trigger** message with consentRequired set to false. Terminal would response with**AM Request** message, and server then responds with**AM Response** message with campaignEndTime set to past.

The Terminal MAY initiate opt-out by sending the AM Request message to the BCAST AM-M (to the same address as it was sent when opted-in). In the AM Request message, Terminal sets the userConsent to "Refuse". Server then responds with anAM Response, with campaignEndTime set to past.

On receiving AM Response message, the AM-C SHALL compare the campaignEndTime with its current time. In case the campaignEndTime is past, the AM-C SHOULD report all the remaining measured data, SHALL close the campaign for the user and MAY delete all the Audience Measurement data for the campaign indicated by the AM Response message.

5.20.1.1.7 Audience Measurement SMS Trigger

When SMS bearer is used for delivering an Audience Measurement message to a Terminal, the SMS SHALL satisfy the following conditions:

- The SMS carries a WAP connectionless push (WDP/WSP encoding) as defined in [OMA Push] ;
- The WSP content type header contains the Content Type code registered by OMNA for 'application/vnd.oma.bcast.am-trigger' (see AppendixI.9), i.e. the binary value 0x36;
- The WSP X-Wap-Application-Id header contains the binary code registered by OMNA for the PUSH Application ID identifying the BCAST Push client, as specified in [BCAST11-Distribution].

The actual trigger message SHALL be structured as follows. Note that the 'type' parameter signals the type of the message and as such determines its structure (i.e. number, semantics and size of the parameters contained).

Data Field Name	Data Type
Audience_Measurement_Trigger_Message {	
type	uimsbf8
if(type==0 or type==2) {	
Download.validFrom	uimsbf32
Download.validTo	uimsbf32
Download.url	bytestring
}	
else if(type==1) {	
AMTrigger.flags	uimsbf8
AMTrigger.campaignID	uimsbf32
AMTrigger.campaignStartTime	uimsbf32
if(AMTrigger.flags[7]==1) {	
AMTrigger.campaignEndTime	uimsbf32
}	
AMTrigger.campaignName	bytestring
AMTrigger.campaignDescription	bytestring
AMTrigger.serverAddressURL	bytestring
if(AMTrigger.flags[6]==1) {	
AMTrigger.additionalInfoURL	bytestring

}	
}	
else if(type==3) {	
AMRT.bsmID	bytestring
AMRT.numDeviceIDs	uimsbf8
for(j=0; j<AMRT.numDeviceIDs; j++) {	
AMRT.deviceIDType	uimsbf8
AMRT.deviceID	bytestring
}	
AMRT.numCampaignIDs	uimsbf8
for(k=0; k<AMRT.numCampaignIDs; k++) {	
AMRT.campaignID	bytestring
}	
}	

Table 61: Audience Measurement Trigger Message Structure

uimsbfN	Unsigned Nbit Integer, most significant bit first
bytestring	Array of bytes

Table 62: Mnemonics used in Table 61

Type	Signals the type of the message. 0 – Trigger to download a BCAST 1.1 AM Trigger message 1 – Binary structure for pushing a BCAST 1.1 AM Trigger message 2 – Trigger to download a BCAST 1.1 AMRT message 3 – Binary structure for pushing a BCAST 1.1 AMRT message 4-255 – reserved for future use Terminals MAY discard messages with an unknown value in the 'type' field.
Download.validFrom	Point in time from which the AM Trigger or AMRT message can be downloaded from Download.url, represented as 32bit integer part of NTP time stamp
Download.validTo	Point in time until which the AM Trigger or AMRT message can be downloaded from Download.url, represented as 32bit integer part of NTP time stamp
Download.url	URL from which the Terminal can download the AM Trigger or AMRT message, encoded as null-terminated string
AMTrigger.flags	Flags bit 7: presence of 'campaignEndTime' field (1 = present; 0 = absent) bit 6: presence of 'additionalInfoURL' field (1 = present; 0 = absent) bit 5: value of field 'consentRequired' as defined in section 5.20.1.2.1 bit 4 … bit 0: reserved, set to 0
AMTrigger.campaignID	Campaign ID as defined in section 5.20.1.2.1
AMTrigger.campaignStartTime	Campaign start time as defined in section 5.20.1.2.1
AMTrigger.campaignEndTime	Campaign end time as defined in section 5.20.1.2.1
AMTrigger.campaignName	CampaignName as defined in section 5.20.1.2.1 encoded as null-terminated

	string
AMTrigger.campaignDescription	Description as defined in section5.20.1.2.1 encoded as null-terminated string
AMTrigger.serveraddressURL	ServerAddressURL as defined in section 5.20.1.2.1 encoded as null-terminated string
AMTrigger.additionalInfoURL	AdditionalInfoURL as defined in section 5.20.1.2.1 encoded as null-terminated string
AMRT.bsmID	BSMID as defined in section 5.20.1.2.6 encoded as null-terminated string
AMRT.numDeviceIDs	Number of device IDs
AMRT.deviceIDType	type attribute of element DeviceID as defined in section 5.20.1.2.6
AMRT.deviceID	DeviceID as defined in section 5.20.1.2.6 encoded as null-terminated string
AMRT.numCampaignIDs	Number of campaign IDs
AMRT.campaignID	CampaignID as defined in section 5.20.1.2.6 encoded as null-terminated string

Table 63: Semantics for Table 61

If the Terminal receives a message with the 'type' parameter equals to 0 or 2, it SHALL send an HTTP(S) request to the URL indicated in the field Download.url, if the current time is in the interval signalled by Download.validFrom and Download.validTo, and the URL is authenticated (see section 5.20.1.1.2). In case the 'type' equals to 0, the BCAST AM-M SHALL respond with an AM Trigger message as specified in section5.20.1.2.1, and the Terminal SHALL then proceed as defined in section 5.20.1.1.2. In case the 'type' equals to 2, the BCAST AM-M SHALL respond with an AMRT message as specified in section 5.20.1.2.6, and the Terminal SHALL then proceed as defined in section 5.20.1.1.5.

If the Terminal receives a message with the 'type' parameter equals to 1, it SHALL populate the fields of an AM Trigger as delivered in the SMS message, and proceed as defined in section 5.20.1.1.2, if the URL content in the 'AMTrigger.serveraddressURL' field is authenticated (see section 5.20.1.1.2).

If the Terminal receives a message with the 'type' parameter equals to 3, it SHALL populate the fields of an AMRT as delivered in the SMS message, and proceed as defined in section 5.20.1.1.5Note that due to the size of the structure, the resulting message will be fragmented over multiple SMSs.

5.20.1.2 Message Description

5.20.1.2.1 Audience Measurement Trigger (AM Trigger) message

The Audience Measurement Trigger (AM Trigger) message SHALL be used to invite the Terminal to an Audience Measurement campaign. It MAY also be used to trigger the process to reconfigure the existing campaign. AM Trigger message is sent by BSM to the Terminal over SMS (see section5.20.1.1.7), in the Service Guide or via HTTP after an SMS Trigger. For Service Guide delivery of theAM Trigger, the structure is specified in the [BCAST11-SG]. For SMS initiated pull delivery over HTTP(S), the structure is specified below. This message MAY be compressed with GZIP [RFC 1952].

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementTrigger	E			Audience Measurement Trigger message. Contains the following attributes: campaignID campaignStartTime campaignEndTime Contains the following elements: UserConsentInformation	

				ServerAddressURL AdditionalInfoAddressURL	
campaignID	A	M	1	Identifier of the Audience Measurement Campaign.	unsignedInt
campaignStartTime	A	M	1	Time when the measurement is planned to start. This parameter is directed to the Terminal for pre-filtering purposes, e.g. to filter overlapping campaigns if the Terminal is not capable of handling multiple campaigns simultaneously. This information SHALL NOT be used to configure the Audience Measurement function on the Terminal. This information SHOULD NOT be presented to the user. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
campaignEndTime	A	O	0..1	Time when the measurement is planned to end. This parameter is directed to the Terminal for pre-filtering purposes, e.g. to filter overlapping campaigns if the Terminal is not capable of handling multiple campaigns simultaneously. This information SHALL NOT be used to configure the Audience Measurement function on the Terminal. This information SHOULD NOT be presented to the user. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
UserConsentInformation	E1	M	1	User consent information needed to perform opt-in for Campaign participation. Contains the following attributes: consentRequired Contains the following elements: CampaignName CampaignDescription	
consentRequired	A	NM/TM	1	User consent required for Campaign participation. If this attribute is FALSE the Terminal MAY perform silent Opt-In (“Refuse” or “Accept”). If this attribute is TRUE, the Terminal MAY perform a silent Opt-In, which MAY result “Refuse” (opted-out), but SHALL NOT result “Accept” (opted-in). If the Terminal did not silently refuse the invitation (“Refuse”), the Terminal SHALL consult the user for the participation in the campaign, and the result of the Opt-In process is according to the user choice (“Refuse” or “Accept”).	boolean
CampaignName	E2	M	1…N	Name of the campaign. This field SHALL be presented to user only if user consent is asked.	string

				The language MAY be expressed using built-in XML attribute 'xml:lang' with this element.	
CampaignDescription	E2	M	1..N	Description of the campaign. • This information is intended to be displayed to the user.In a case of campaign reconfiguration this attribute gives reasoning for the change. • In case the campaign requires user consent (i.e. 'consentRequired' is set to TRUE), and the Terminal did not silently refuse the invitation ("Refuse"), this information SHALL be shown to the user, and MAY include the Terms of Use of the campaign. The language MAY be expressed using built-in XML attribute 'xml:lang' with this element.	string
ServerAddressURL	E1	M	1	This element signals a URL of the Audience Measurement server to which the Audience Measurement Request message is sent. The Terminal SHALL verify the URL as described in section 5.20.1.1.2. If the verification fails, the Terminal SHALL ignore this message.	anyURI
AdditionalInfoAddressURL	E1	O	0..1	URL for additional information related to this Campaign. This link SHOULD be shown to the user, when user consent is asked.	anyURI

5.20.1.2.2 Audience Measurement Request (AM Request) message

This message is sent by the Terminal (AM-C) to the BSM (AM-M). This message MAY be compressed with GZIP [RFC 1952].

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementRequest	E			Audience Measurement Request message. Contains the following attributes: campaignID requestID userConsent Contains the following element: UserID DeviceID	
campaignID	A	M	1	Identifier for the Audience Measurement Campaign. Maps with the campaignID delivered overAudience Measurement Trigger.	unsignedInt
requestID	A	M	1	Identifier for this particular Audience Measurement Request Message	unsignedInt
userConsent	A	O	0..1	This attribute is set to True, if the user accepts	boolean

				to participate in the campaign. If the attribute is missing from the request or set to False, the user has refused the attendance to the campaign.	
UserID	E1	M	1..N	The user identity known to the BSM. Contains the following attributes: type For AM Request message, each instantiated UserID SHALL have different type.	string
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	M	1..N	A unique device identification known to the BSM. Contains the following attributes: type For AM Request message, each instantiated DeviceID SHALL have different type.	string
type	A	M	1	Specifies the type of Device ID. Allowed values are: 0 — reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte

5.20.1.2.3 Audience Measurement Response (AM Response) message

This message is sent by the BSM (AM-M) to the Terminal (AM-C). This message MAY be compressed with GZIP [RFC 1952].

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementResponse	E			Audience Measurement Response message. Contains the following attributes: requestID globalStatusCode Contains the following elements:	

				ConfigurationData	
requestID	A	M	1	Identifier for the corresponding Audience Measurement Request message. This SHALL be instantiated if the corresponding request message includes it. In case instantiated, it SHALL contain the same value as the requested in the corresponding AM Request message.	unsignedInt
globalStatusCode	A	M	1	The overall outcome of the request, according to the return codes defined in the section 5.11. If this value is anything else by 000 ("Success"), the Terminal SHALL consider the campaign with the associated userID closed. See in particular the global status code value 032 that can be returned to reject a Terminal participating in a campaign.	unsignedByte
AudienceMeasurementConfigurationData	E1	O	0..1	Set of parameters to configure the client for the campaign in question. This element MUST be instantiated, if the globalStatusCode is "success".	complexType as defined in section 5.20.1.2.7

5.20.1.2.4 Audience Measurement Report Delivery (AMRD) message

This message is sent by the Terminal (AM-C) to the BSM (AM-M). This message MAY be compressed with GZIP [RFC 1952].

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementReportDelivery	E			Audience Measurement Report Delivery message. Contains the following attributes: campaignID requestID version Contains the following elements: UserID DeviceID ServiceConsumptionMeasurementEvent RecordingConsumptionMeasurementEvent ProprietaryMeasurementEvent	
campaignID	A	M	1	Identifier for the Audience Measurement Campaign the measurement results relate to.	unsignedInt
requestID	A	O	0…1	Identifier for the Audience Measurement Report delivery message.	unsignedInt
version	A	M	1	The value of the version attribute in the current configuration data (see 5.20.1.2.7) in the Terminal.	unsignedInt
UserID	E1	M	1..N	The user identity known to the BSM.	string

				Contains the following attributes: type For AMRD message, each instantiated UserID SHALL have different type.	
type	A	M	1	Specifies the type of User ID. Allowed values are: 0 –username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
DeviceID	E1	M	1..N	A unique device identification known to the BSM. Contains the following attributes: type For AMRD message, each instantiated DeviceID SHALL have different type.	string
type	A	M	1	Specifies the type of Device ID. Allowed values are: 0 — reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
ServiceConsumptionMeasurementEvent	E1	O	0..N	Single Service Consumption Measurement event. Contains the following attributes: globalServiceIDRef Contains the following elements: GlobalContentIDRef Start End	
globalServiceIDRef	A	M	1	Reference to global Service ID of the service consumed.	anyURI
GlobalContentIDRef	E2	O	0..N	References to global Content ID(s) of the content consumed.	anyURI
Start	E2	M	1	Information about start of the consumption. Contains the following attributes: time Contains the following elements: Location	

time	A	M	1	Point of time when consumption started. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
Location	E3	O	0..1	Location where consumption started. Contains the following elements: Point Cell At most one of Cell and Point SHALL be instantiated (implementation in XML schema using <choice>)	
Point	E4	O	0..1	Coordinates of the point where consumption started	See [OMA MLP]
Cell	E4	O	0..1	The target area to distribute content specified by the BDS specific service coverage area or minimum transmit area.	complexType as defined by E3 element "CellTargetArea" in section 5.1.2.1 of [BCAST11-SG]
End	E2	M	1	Information about end of the consumption. Contains the following attributes: time Contains the following elements: Location	
time	A	M	1	Point of time when consumption ended This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
Location	E3	O	0..1	Location where consumption ended. Contains the following attributes: sameAsStart Contains the following elements: Point Cell At most one of Cell and Point SHALL be instantiated (implementation in XML schema using <choice>). In case this location is the same as under 'Start', the attribute 'sameAsStart' MAY be instantiated.	
sameAsStart	A	O	0..1	Indicates that the consumption ended at the same location where it started. In case this attribute is instantiated and set to 'true', the parent element 'Location' SHALL contain no	boolean

				child elements. Default: false.	
Point	E4	O	0..1	Coordinates of the point where consumption started	See [OMA MLP]
Cell	E4	O	0..1	The target area to distribute content specified by the BDS specific service coverage area or minimum transmit area.	complexType as defined by E3 element "CellTargetArea" in section 5.1.2.1 of [BCAST11-SG]
RecordingConsumptionMeasurementEvent	E1	O	0..N	Single Service Recording Consumption Measurement event Contains the following attributes: globalServiceIDRef Contains the following elements: GlobalContentIDRef Recording Consumption	
globalServiceIDRef	A	M	1	Reference to global Service ID of the service consumed.	anyURI
GlobalContentIDRef	E2	O	0...N	References to global Content ID(s) of the content consumed.	anyURI
Recording	E2	O	0..1	Information about the recording. Contains the following elements: Start End	
Start	E3	M	1	Information about start of the recording. Contains the following attribute: time Contains the following elements: Location	
time	A	M	1	Point of time when recording started. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
Location	E4	O	0..1	Location where consumption started. Contains the following elements: Point Cell At most one of Cell and Point SHALL be instantiated (implementation in XML schema using <choice>)	
Point	E5	O	0..1	Coordinates of the point where consumption started	See [OMA MLP]
Cell	E5	O	0..1	The target area to distribute content specified by	complexType

				the BDS specific service coverage area or minimum transmit area.	as defined by E3 element "CellTargetArea" in section 5.1.2.1 of [BCAST11-SG]
End	E3	M	1	Information about end of the recording. Contains the following attributes: time Contains the following elements: Location	
time	A	M	1	Point of time when recording ended This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
Location	E4	O	0..1	Location where consumption ended. Contains the following attributes: sameAsStart Contains the following elements: Point Cell At most one of Cell and Point SHALL be instantiated (implementation in XML schema using <choice>). In case this location is the same as under 'Start', the attribute 'sameAsStart' MAY be instantiated.	
sameAsStart	A	O	0..1	Indicates that the recording ended at the same location where it started. In case this attribute is instantiated and set to 'true', the parent element 'Location' SHALL contain no child elements. Default: false.	boolean
Point	E5	O	0..1	Coordinates of the point where consumption started	See [OMA MLP]
Cell	E5	O	0..1	The target area to distribute content specified by the BDS specific service coverage area or minimum transmit area.	complexType as defined by E3 element "CellTargetArea" in section 5.1.2.1 of [BCAST11-SG]
Consumption	E2	O	0..N	Information about the consumption. Contains the following elements: Start End	
Start	E3	M	1	Information about the start of the consumption.	

				Contains the following attribute: time	
time	A	M	1	Point of time when recorded content consumption was started. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
End	E3	M	1	Information about the end of the consumption. Contains the following attribute: time	
time	A	M	1	Point of time when recorded content consumption ended. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
ProprietaryMeasurementEvent	E1	O	0..N	An element serving as a container for proprietary or application-specific measurements that are not defined in this specification. Terminal MAY report these measurements.	
<proprietary elements>	E2	O	0..N	Proprietary or application-specific elements which may further contain sub-elements or attributes.	

5.20.1.2.5 Audience Measurement Report Response (AMRR) message

This message is sent by the BSM (AM-M) to the Terminal (AM-C). This message MAY be compressed with GZIP [RFC 1952].

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementReportResponse	E	O		Audience Measurement Reporting Response message. Contains the following attributes: campaignID requestID globalStatusCode Contains the following elements: AudienceMeasurementConfigurationData	
campaignID	A	M	1	Identifier for the Audience Measurement Campaign the measurement results relate to.	unsignedInt
requestID	A	O	0..1	Identifier for the corresponding Audience Measurement Report delivery message. This SHALL be instantiated if the corresponding Report Delivery message includes it. In case instantiated, it SHALL contain the same value as the requested in the corresponding Report Delivery message.	unsignedInt
global Status Code	A	M	1	The overall outcome of the request, according to the return codes defined in the section 5.11.	unsignedByte

AudienceMeasurementConfigurationData	E1	O	0..1	Set of parameters to re-configure the client for the campaign in question after delivering the measurement results.	complexType as defined in section 5.20.1.2.7

5.20.1.2.6 Audience Measurement Report Trigger (AMRT)

This message is sent by the BSM (BCAST AM-M) to the Terminal (BCAST AM-C) (see section 5.20.1.1.7). It either carries the actual AMRT data, or a link from which the AM-C can download the AMRT data via HTTP.. For pull delivery over HTTP(S) following an SMS Trigger, the structure is specified below. This message MAY be compressed with GZIP [RFC 1952].

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementReportTrigger	E			Audience Measurement Report Trigger Contains the following elements: BSMID DeviceID CampaignID	
BSMID	E1	M	1	Identifier of the BCAST AM-M known to the BCAST AM-C	string
DeviceID	E1	M	1…N	A unique device identification known to the BSM. Contains the following attributes: type For AMRD message, each instantiated DeviceID SHALL have different type.	string
type	A	M	1	Specifies the type of Device ID. Allowed values are: 0 — reserved for future use 1 – IMEI [3GPP TS 23.003] 2 – MEID [3GPP2 C. S0072-0] 3-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
CampaignID	E1	M	0..N	Identifier of Audience Measurement Campaign that the BCAST AM-C is participate in.	unsignedInt

5.20.1.2.7 Audience Measurement Configuration Data

This data structure contains the configuration data of an Audience Measurement campaign.. It is sent by the BSM (BCAST AM-M) to the Terminal (BCAST AM-C), in AM Response message (see section 5.20.1.2.3) and AMRR message (see section 5.20.1.2.5)

Name	Type	Category	Cardinality	Description	Data Type
AudienceMeasurementConfiguration	E			Audience Measurement Configuration Data.	

Data				Contains the following attributes: campaignID campaignStartTime campaignEndTime version Contains the following elements: ReportInfo RequestedMeasurementEvent ProprietaryMeasurementEvent	
campaignID	A	M	1	Identifier for the Audience Measurement Campaign. Maps with the campaignID delivered overAudience Measurement Trigger.	unsignedInt
campaignStartTime	A	M	1	Time when the measurement is activated in the Terminal. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
campaignEndTime	A	M	1	Time when the measurement is de-activated in the Terminal. This field contains the 32-bits integer part of an NTP time stamp.	unsignedInt
version	A	M	1	Version of this configuration data.	unsignedInt
ReportInfo	E1	M	1	Report policy to be used for AM-C to deliver reports to AM-M Contains the following attributes: serverURL. Contains the following elements: PeriodicReporting. DataThresholdReporting. TriggeredReporting. Exactly one of the elements MUST be instantiated.	
serverURL	A	M	1	URL through which the Terminal delivers the Audience Measurement reports.	anyURI
PeriodicReporting	E2	O	0…1	Reporting is performed periodically. Contains the following attributes: randomOffset reportingPeriod	
randomOffset	A	M	1	Random offset for reporting time in minutes.	unsignedShort
reportingPeriod	A	M	1	Reporting period representing the number of hours between reporting sessions. `Reporting time (N) = campaignStartTime + N x reportingPeriod + random,` where ‘N’ represents the number of the report, and ‘random’ represents a real number between 0 and ‘randomOffset’	unsignedByte
DataThresholdRep	E2	O	0…1	Reporting is performed based on the amount of	

orting				data to report. Contains the following attributes: nbrOfEvents	
nbrOfEvents	A	M	1	Number of events measured, before AM-C sends a report.	unsignedInt
TriggeredReporting	E2	O	0…1	The presence of this element signals that reporting is performed when AM-C receives the AMRT message (see 5.20.1.2.6) This is an empty element which has neither child elements nor attributes.	
RequestedMeasurementEvent	E1	O	0…N	Request to the Terminal to measure and report certain events. If this element is not instantiated, the Terminal SHALL measure all the event types according to its capabilities Contains the following attributes: eventType	
eventType	A	M	1	Types of events that the Terminal will observe and report. 0 – Service Consumption 1 – Recording Consumption 2-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
ProprietaryMeasurementEvent	E1	O	0..N	An element serving as a container for proprietary or application-specific measurements that are not defined in this specification. Terminal MAY report these measurements.	
<proprietary elements>	E2	O	0..N	Proprietary or application-specific elements which may further contain sub-elements or attributes.	

5.20.2 Smartcard-Centric Audience Measurement

The Smartcard-Centric Audience Measurement provides a solution of audience monitoring based on the Smartcard on the client side. The Smartcard-Centric solution offers a secure processing for the metering process controlled by the agreement (Opt-In) of the user, and a secure storage of measures on the client side.

The Audience Measurement function allows a remote configuration of the function on the client side.

The metering process for the Smartcard-Centric Audience measurement is linked to the Service and Content Protection Smartcard Profile described in [BCAST11-SrvCntProtection].

5.20.2.1 Process description

The Audience measurement function provides means to track user consumption of services and to report this consumption on the network side for analysis and statistics. The Audience measurement function contains the following steps:

- **Registration process**: The Registration process is used to know which clients support the AM function and identify them. This is used to build the pool of users from which the panel will be set-up. During this registration process, an authentication process is performed and credentials are exchanged for further communication between the Client and the server.
- **Panel Management and campaign definition**: During this process a selection of a group of users to make a panel for a specific Audience Measurement Campaign is performed.
- **Opt-In process**: The Opt-In phase is used to obtain a contractual binding between the Audience Measurement function on the server side (BCAST AM-M) and the Audience Measurement function on the client side (BCAST AM-C) to ensure that the user agrees to participate in Audience Measurement.
- **Configuration and activation process**: The BCAST AM-M configures the BCAST AM-C with the parameters specific to the campaign (e.g. the list of metrics, the report delivery frequency,…). Then the BCAST AM-M activates the AM function on the client side to start the metering process.
- **Metering process**: upon activation and depending on the Opt-In state, the BCAST AM-C launches the metering process on the client side. The Metering process consists in tracking user consumption of services and storing these events along with other corresponding data, in accordance with the list of metrics.
- **Reporting process**: The BCAST AM-C aggregates the measures in the appropriate report. The BCAST AM-C sends the report to the BCAST AM-M on a periodic basis depending of the report delivery frequency that has been configured during configuration process or on specific request from the BCAST AM-M. The BCAST AM-M stores the measures in a data base.
- **Analysis process**: The Audience Measurement Application function (BCAST AM-A) on the server side retrieves the group of users for the specific campaign from the Audience Measurement Management function (BCAST AM-M) on the server side to setup the analysis. The BCAST AM-A retrieves, from the BCAST AM-M, the measures related to a panel of users for analysis and produces statistics on them. The result of the analysis may be used for example to setup the timetable of services or for other purposes.

5.20.2.1.1 Registration Process

The registration process is used to populate the BCAST AM-M client's database. After the registration, a panel may be activated to allow the audience measurement by BCAST AM-C.

After the first handset power on, the BCAST AM-C sends a REGISTRATION_REQUEST message defined in section 5.20.2.3.1.1 to the BCAST AM-M. Using this message, the BCAST AM-M can retrieve the client's information using the IMSI, the card profile using the ICCID and the handset features using the IMEI or MEID value. To finish the registration process the BCAST AM-M sends a REGISTRATION_ RESPONSE message defined in section 5.20.2.3.1.2 to BCAST AM-C.

The registration acknowledgement sets the User ID value, launches the key derivation mechanism (Key Kamue and Kamus as defined below) and sets the BCAST AM-C state to registered. The REGISTRATION_REQUEST message SHALL be sent by the Smartcard in a MO-SMS every time the handset is powered-on until the registration acknowledgement response (REGISTRATION_RESPONSE message) is received from the BCAST AM-M within a MT-SMS. When the registration acknowledgement is received, the Smartcard is in a registered state and stops sending REGISTRATION REQUEST.

For the user authentication and collected data protection, two keys (Kamue and Kamus) are derived using exchanged credentials and user ID. The derivation algorithm is the pseudo-random function (PRF) as described in [RFC 3830], PRF(key, label, message), where:

- Key: Km key is a pre-shared key
- Label: character string encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629, concatenated to User ID value
- Message: card random concatenated with server random

Kamue = PRF(Km , LabelEncryption || UserID , CardRandom || ServerRandom)

Kamus = PRF(Km , LabelSignature || UserID , CardRandom || ServerRandom)

The LabelEncryption and LabelSignature parameters SHALL be the following:

LabelEncryption = “BCAST-AM-e” (i.e. 0x42 0x43 0x41 0x53 0x54 0x2D 0x41 0x4D 0x2D 0x65)

LabelSignature = “BCAST-AM-s” (i.e. 0x42 0x43 0x41 0x53 0x54 0x2D 0x41 0x4D 0x2D 0x73)

The Registration process is OPTIONAL. The Registration process MAY be NOT performed in case Kamue, Kamus and UserID have been set in the Smartcard at the personalization stage of the card or using remote provisioning of the Smartcard.

In order to know the list of optional features that the BCAST AM-C in the Smartcard supports, the current state of the BCAST AM-C and some internal parameters, the BCAST AM-M MAY send an AUDIT_REQUEST command to the BCAST AM-C in the Smartcard through the SMS bearer. This command is described in the section 5.20.2.3.1.3.

At the reception of the AUDIT_REQUEST command, the BCAST AM-C in the Smartcard sends an AUDIT_RESPONSE command to BCAST AM-M through the SMS bearer. This command is described in section 5.20.2.3.1.4.

The BCAST AM-C, through this AUDIT_RESPONSE, informs the BCAST AM-M

- On its support of the following features:
  - Bearers supported (SMS, HTTP, HTTPS,..)
  - Location type supported
  - Security type supported
  - …
- And on its current state and configuration:
  - Buffer size, Buffer filling level, reporting trigger
  - Last status error
  - …

5.20.2.1.2 Opt-In Process

The Opt-In phase is used to obtain a contractual binding between the Audience Measurement function on the server side (BCAST AM-M) and the Audience Measurement function on the client side (BCAST AM-C) to ensure that the user agrees to participate in Audience Measurement.

There are many different ways the service provider can solicit the user to opt-in, e.g.:

- when the user subscribes to the Mobile TV service, she can, at the same time, agree to participate in Audience Measurement campaigns;
- the service provider can send surface mails to its subscribers to request them to opt-in;
- the service provider can send an SMS or email inviting its subscribers to opt-in;
- the service provider can call its subscribers to propose them to opt-in;
- The service provider can send a OPT_IN_INVITATION_TRIGGER defined in section 5.20.2.3.2.1
- …

Similarly, the user can actually opt-in using different channels, either in-band or out-of-band, such as:

- Signing a paper contract;

- Using the service provider web portal;
- Using an application on the user's client;
- …

A service provider can even combine several solicitation forms and opt-in channels to provide more flexibility to its users. For these reasons, the Opt-in process is out of scope of OMA BCAST 1.1 and rather left open to implementers to cope with different market requirements.

However the service provider MAY also use the OPT_IN_INVITATION_TRIGGER message to trigger an application in the Smartcard that will request the consent of the user. The content of this message is specified in section 5.20.2.3.2.1. The way the consent is actually requested to the user is left open to implementation and is out of scope of this specification. If several prompt messages are sent in the OPT_IN_INVITATION_TRIGGER message for different languages, the prompt message used for the display to the user SHOULD be the one with the language code corresponding to the preferred language indicated in EF_{LI} (Language Indication) under the USIM/CSIM or in the EF_{PL} (Preferred Languages) under the MF of the smartcard as defined in [3GPP TS 31.102 v8] for 3GPP or [3GPP2 C.S0065- B] for 3GPP2.

The result of the Opt-in process SHALL be sent by the BCAST AM-C to the BCAST AM-M using the OPT_IN_STATE_NOTIFICATION message as specified in section 5.20.2.3.2.3, as an acknowledgement. This message contains the Opt-In state in the BCAST AM-C in the Smartcard, resulting from the Opt-In process that has been triggered by the OPT_IN_INVITATION_TRIGGER message, or any other solicitation form.

The result of the Opt-in process SHALL be materialized by a binary state that is maintained in the Smartcard and controls the metering process: opted-in/opted-out. For all channels that are not directly involving the Smartcard in the user's opt-in, the user's opt-in state SHALL be reflected in the Smartcard by any appropriate means identified by the service provider. In this case, an OPT_IN message SHALL be sent by the BCAST AM-M to the BCAST AM-C to set the current user's state according to her request. This message is further specified in section 5.20.2.3.2.2. The OPT_IN message MAY be sent over a secure channel using the credentials exchanged during the registration process. However, as there is no guarantee that the opt-in actually occurs after registration, sending the OPT_IN message SHALL be delayed until the BCAST AM-C is registered at the BCAST AM-M.

When the Smartcard is directly involved in the user's opt-in, e.g., at the reception of an OPT_IN_INVITATION_TRIGGER message, a user's Audience Measurement PIN (AM PIN) code MUST be entered to sign the opt-in and provide non-repudiation to the service provider. The BCAST AM-C in the Smartcard SHALL prompt the user to enter this AM PIN code. When the service provider is the network operator, the AM PIN MAY be mapped to the GLOBAL PIN of the USIM, ISIM or R-UIM application, or to the Parental Control PIN when regulatory reasons impose that only a parent is entitled to opt-in. The proactive commands such as DISPLAY TEXT or GET INPUT as described in [ETSI TS 102.223] MAY be used for such process. The Terminal SHALL support the proactive commands DISPLAY TEXT and GET INPUT as described in [ETSI TS 102.223] .

It is not strictly mandatory that the BCAST AM-M maintains the users' opt-in state. If business needs justify that the BCAST AM-M stays up-to-date with users' opt-in state, then the BCAST AM-C MAY send to the BCAST AM-M an OPT_IN_STATE_NOTIFICATION message indicating the current user's state after each successful modification. This is done at the initiative of the BCAST AM_C in the Smartcard and depends on operator's requirements. For instance, depending on regulation, an opt-out could be made by the user at any time locally in the Smartcard using, e.g., a SIMToolkit application. The Smartcard MAY then send an OPT_IN_STATE_NOTIFICATION message to the server indicating that the user has opted-out. The OPT_IN_STATE_NOTIFICATION message is further specified in section 5.20.2.3.2.3. When the opt-in state is changed after reception of an OPT_IN message, the OPT_IN_STATE_NOTIFICATION message MAY NOT be sent. If it is, it will be used by the BCAST AM-M as a confirmation of the reception of the OPT_IN message in the BCAST AM-C.

5.20.2.1.3 Configuration Process

The BCAST AM-M configures the BCAST AM-C with the parameters specific to the campaign (e.g. the list of metrics, the report delivery frequency,…).

Configuration consists in setting the following parameters:

- Reporting parameters
- Address of BCAST AM-M
- Bearer parameters
- Additional metrics

The list of metrics that SHALL be recorded are signalled in the configuration message during the configuration stage. This message MAY contains some additional metrics as the Location when the user starts the consumption of a content, the location when the user ends the consumption of the content, the consumption time and Content ID provided by the Terminal.

Anytime the BCAST AM-M needs to set or modify the BCAST AM-C configuration parameters, it SHALL send a CONFIGURATION message. Any bearer described in 5.3 is suitable to transport this message. It CAN be sent at any time after Registration has occurred.

The CONFIGURATION message is further specified in section 5.20.2.3.3.

5.20.2.1.4 Activation Process

Then the BCAST AM-M activates the Audience Measurement Metering process on the client side by sending an ACTIVATION message to BCAST AM-C. This message can be sent at any time after Registration has occurred. Whether or not Metering process will be activated on the BCAST AM-C depends on both the Activation and Opt-in states as described in section 5.20.2.1.5.

The ACTIVATION message is further specified in section 5.20.2.3.4.

5.20.2.1.5 Metering Process

Depending on the activation and opt-in states, the BCAST AM-C SHALL run, stop or pause the metering process on the client side as specified in Table 64. The activation state is controlled by the Activation process as described in 5.20.2.1.4. The Opt-in state is controlled by the Opt-in process as described in 5.20.2.1.2. The Metering process contains features that allow to meet regulatory requirements

Metering process state		Opt-in state	
		Opted-in	Opted-out
Activation state	Activated	RUNNING	PAUSED
	Deactivated	STOPPED	STOPPED

Table 64: Metering process state

The Metering process consists in tracking user consumption of services, materialized by zapping events, and storing these events along with other corresponding data, in accordance with the list of metrics. Zapping events together with the other corresponding data constitute the Audience data. The Metering process for encrypted services and contents SHALL be based on information, exchanged between the Terminal and the Smartcard during consumption of services, that cannot be forged by a malicious third-party, i.e., signed at the head-end: STKMs, LTKMs, Parental Control Messages, and any other message presenting such characteristic. Depending of the configuration the service provider has chosen during the Configuration process, the Metering process for unencrypted (clear-to-air) services and contents MAY be based on the STKMs received by the Smartcard, or the information received from the Terminal using Event Signalling Mode of BCAST Command (see section 6.14 of [BCAST11-ServContProt]). As the process is controlled by the user's opt-in state, Audience data SHALL not be recorded in the Smartcard when the user decides to opt-out. Recording of Audience data SHALL resume as soon as the user decides to opt-in again.

During metering, the Audience data SHALL be stored in the Smartcard and SHALL be protected from unauthorized access. The Audience data SHALL not be erased after a power-off of the terminal or a battery shortage. The size of the buffer is defined by a configuration parameter (see section 5.20.2.3.3). When the buffer fills up, a Reporting process SHALL be automatically launched by the Smartcard as specified in section 5.20.2.1.6 to prevent any loss of data.

The Metering process contains features that allow meeting regulatory requirements. In some countries, there could be regulations concerning personal data processing.

Opt-in process is one of these features.

Additionally, regulations could prohibit the processing of personal data that could provide information on a person's religious or philosophical beliefs, political opinions, sex life... Audience Measurements of selected services or contents might be disallowed due to these specific regulatory requirements. For these countries there is then a need to control the AM process for specific contents.

For encrypted services

Audience_measurement_disallowed flag in the access criteria Smartcard-Centric_Audience_measurement_control descriptor SHALL be used in the STKM message (as described in [BCAST11-ServContProt] to signal to the Audience Measurement Client that the corresponding content is a critical content in term of audience measurement and that the Audience measurement of such content is prohibited.

The following process SHALL apply:

- If the Smartcard supports Smartcard-centric Audience Measurement function and if the Audience_measurement_disallowed flag in the STKM is set to TKM_FLAG_TRUE, then the Audience Measurement metering process SHALL be put in PAUSED state and Audience measurement data relative to this content SHALL NOT be stored on the client side.
- If the Smartcard supports Smartcard-centric Audience Measurement function and if the Audience_measurement_disallowed flag in the STKM is set to TKM_FLAG_FALSE or no Audience_measurement_control descriptor is present in the STKM, then the Audience Measurement process is authorized and measurement MAY be stored on the client side.

For clear to air services (non encrypted)

If Audience_measurement_disallowed flag in the access criteria Smartcard-Centric_Audience_measurement_control descriptor is used in the STKM message (as described in [BCAST11-ServContProt] to signal that the Audience measurement of a critical content is prohibited, then the following process SHALL apply:

- If the Smartcard supports Smartcard-centric Audience Measurement function and if the Audience_measurement_disallowed flag in the STKM is set to TKM_FLAG_TRUE, then the Audience Measurement metering process SHALL be put in PAUSED state and Audience measurement data relative to this content SHALL NOT be stored on the client side.
- If the Smartcard supports Smartcard-centric Audience Measurement function and if the Audience_measurement_disallowed flag in the STKM is set to TKM_FLAG_FALSE or no Audience_measurement_control descriptor is present in the STKM, then the Audience Measurement process is authorized and measurement MAY be stored on the client side.

The traffic_protection_protocol value in the STKM is the one for NULL encryption as defined in [BCAST11-ServContProt].

If the Terminal receive audience measurement control in the Service Guide, then the terminal SHALL signal to the Smartcard that the AM is disallowed or allowed for a content using the “AM Disallowed Service/Content” or “AM Allowed Service/Content” event of the Event Signalling Mode of BCAST Command as described in [BCAST11-ServContProt] according to Attribute amAllowed that is specified in Service and Content fragments of BCAST Service Guide [BCAST11-SG]

- In case the AM is allowed and the AM control Type for clear to air has been set during the configuration phase to the value 1 indicating Event Signalling is used, the Audience Measurement metering process is authorized and measurement MAY be stored on the client side..
- In case the AM is disallowed and the AM control Type for clear to air has been set during the configuration phase to the value 1 indicating Event Signalling is used, the Audience Measurement metering process SHALL be put in PAUSED state and Audience measurement data relative to this content SHALL NOT be stored on the client side.

This process is described in more details in section 6.14 of [BCAST11-ServContProt].

5.20.2.1.6 Reporting Process

The BCAST AM-C aggregates the measures in the appropriate report. The BCAST AM-C sends the report to the BCAST AM-M on a periodic basis, depending of the report delivery frequency that has been configured during the configuration process, or upon specific request from the BCAST AM-M. The BCAST AM-M stores the measures in a data base.

BCAST AM-C SHALL be able to send the report to BCAST AM-M based on an internal event of the card (the buffer size for storing the measures) For example, if the buffer used to store the measures is almost full (with Trigger Low and Trigger High value), BCAST AM-C SHALL send the report to the BCAST AM-M to prevent any loss of data.

The BCAST AM-C SHALL send a REPORTING message containing the audience data recorded to the BCAST AM-M on a specific request from BCAST AM-M or on a timely basis or an event basis. The REPORTING message CAN be transported via SMS or over HTTP as described in section 5.20.2.3.5. The description of the REPORTING message via SMS is described in section 5.20.2.3.5.1 and the REPORTING message sent over HTTP is described in section 5.20.2.3.5.3 The bearer used MUST be configured accordingly during the Configuration process as described in 5.20.2.1.3.

The address of the BCAST AM-M to send the reporting message SHALL be configured during the Configuration process via the CONFIGURATION message described in section 5.20.2.3.3

While sending the reporting message to the BCAST AM-M, the BCAST AM-C SHALL continue to record the audience data and wait for an acknowledgement from BCAST AM-M for the reception of the reporting message before flushing the recorded audience data to prevent any loss of data.

When BCAST AM-C receives an acknowledgment of the reception of the reporting message from BCAST AM-M, BCAST AM-C SHALL flush the recorded audience data sent to BCAST AM-M and continue its Metering process according to its state.

If no Acknowledgement of the reporting message is received by the BCAST AM-C, the BCAST AM-C SHALL not delete the measurement data, and SHALL send them at the next opportunity (either upon specific request from the server or at the next reporting time or upon other relevant event).

When BCAST AM-M explicitly wants to request a reporting from a specific user, it SHALL send a REPORTING_REQUEST message to the BCAST AM-C. The REPORTING_REQUEST message is further specified in section 5.20.2.3.5.5.

5.20.2.1.7 Analysis process

The Audience Measurement Application function (BCAST AM-A) on the server side retrieves the group of users for the specific campaign from the Audience Measurement Management function (BCAST AM-M) on the server side to setup the analysis. The BCAST AM-A retrieves, from the BCAST AM-M, the measures related to a panel of users for analysis and produces statistics on them. The result of the analysis may be used for example to setup the timetable of services or for other purposes.

This process is out of scope of OMA BCAST 1.1 and is server implementation specific.

5.20.2.1.8 Audience measurement for clear to air services

Audience measurement for clear to air services SHALL be implemented in two ways: STKM-Based solution and Event-signalling-based solution. Terminal and Smartcard supporting Smartcard Centric Audience Measurement SHALL support both solutions.

The STKM-Based solution audience measurement of clear-to-air services uses the STKM messages and signalling as described below:

- A STKM stream is sent along with the clear-to-air service, with a traffic_protection_protocol value set to TKM_ALGO_NULL (as defined in section 7.3 of [BCAST11-ServContProt]). The Terminal SHALL support the STKM stream processing with NULL encryption as defined in section 6.7.4 of [BCAST11-ServContProt]. The KEMAC field of the STKM in this case SHOULD contain no TEK and no SALT. The SEK/PEK ID, in the EXT_MBMS field refers to a dedicated SEK/PEK for this service which acquisition could be pre-provisioned or acquired through LTKM as for encrypted services.
- The Terminal SHALL support the signalling of such service in the service guide described below:
    - In the Access fragment of the Clear-to-air service, the KmsType in the KeyManagementSystem element indicates that the protection is the Smartcard profile using the GBA-U oma-bcast-gba_u-mbms = "1" or using bcmcs oma-bcast-prov-bcmcs = "3"
    - In the Access fragment of the Clear-to-air service, the EncryptionType element is absent.
    - The STKM stream is signalled in the SDP as for encrypted services.

The Event Signalling-Based solution audience measurement of clear-to-air services uses consumption time and Service and Content Identifiers provided by the terminal in the Event Signalling Mode of BCAST Command (see section 6.14 of [BCAST11-ServContProt]).

5.20.2.1.9 Signalling the Terminal and Smartcard Smartcard-centric AM capability

If the Terminal supports the Smartcard-centric Audience Measurement, it SHALL read, after power-on, the EFBST file in the Smartcard (as defined in [BCAST11-ServContProt]) to discover the Smartcard-centric AM capability of the Smartcard.

- If the Smartcard doesn't support the Smartcard-Centric Audience Measurement, the Terminal SHALL NOT send Event signalling Mode of the OMA BCAST Command with AM related events to the Smartcard.
- If the Smartcard supports the Smartcard-Centric Audience Measurement, theTerminal SHALL send a OMA BCAST Command in the Event Signalling Mode with the event 'Smartcard-Centric AM support' to indicate to the Smartcard that the Terminal supports the Smartcard-centric Audience Measurement.

After the reception of this command from the Terminal, the Smartcard MAY send the Smartcard-centric AM capability of the Terminal to the server in the AUDIT_RESPONSE message.

5.20.2.2 Communication protocols between BCAST AM-M and BCAST AM-C

The Audience Measurement Management module (BCAST AM-M) and the Audience Measurement Client (BCAST AM-C) exchanges data through AM-7-1, AM-7-2 and AM-5 interfaces.

At least one of the following communication protocols SHALL be supported for AM-7-1 interface:

- Short Message Service Point to Point (SMS-PP) as defined in [3GPP TS 31.115] for 3GPP or [3GPP2 C.S0078-0] for 3GPP2,

- Hyper Text Transfer Protocol (HTTP) as defined in [RFC 2616],

Smartcard Broadcast Provisioning as defined in [BCAST11-Services] SHALL be supported when the optional AM-5 is used.

At least one of the following communication protocols SHALL be supported for AM-7-2 interface:

- Short Message Service Point to Point (SMS-PP) as defined in [3GPP TS 31.115] for 3GPP or [3GPP2 C.S0078-0] for 3GPP2
- Hyper Text Transfer Protocol (HTTP) as defined in RFC 2616.

5.20.2.2.1 Security

Security of the communication between the BCAST AM-M and BCAST AM-C in the Smartcard, i.e., confidentiality, integrity and authentication, MAY be provided at different levels:

- at transport level: using the mechanisms provided by the transport protocol used, e.g., secured SMS-PP as defined in [3GPP TS 31.115] (see section 5.20.2.2.2) or HTTPs see section 5.20.2.2.3);
- at application level: using the mechanisms defined in the present specification in section 5.20.2.2.5.1,this can be particularly interesting when the transport protocol used does not provide any security mechanism, like Smartcard Broadcast Provisioning;
- at both levels: combining the security mechanisms available at the transport level with those available at the application level, provided that credentials are never used at both levels. For instance, it is possible to use HTTPs as a transport providing confidentiality using Kamue, and to use the application-level security for data integrity and authentication based on Kamus. And it is also possible to use transport-level security with SMS-PP using pre-provisioned credentials, together with application-level security using the credentials resulting from the Registration process.

5.20.2.2.2 SMS-PP

The SMS provides a means to transfer short messages between a GSM Mobile Station and a Short Message Entity via a Service Centre.

5.20.2.2.2.1. Structure of data

The TLV (Tag Length Value) format is used to carry data in the SMS payload.

Data	Value	Length
Tag	A predefined Byte that defines the kind of data. Tags shall be well-defined and unambiguous in a recognized context.	1 Byte
Length	Number of bytes composing the data	1 Byte
Value	The sequence of bytes composing the data	Up to 256 Bytes

Messages sent from BCAST AM-M to BCAST AM-C are MT-SMS. . The class of this SMS message SHALL be class 2 indicating that the destination of the SMS is the Smartcard (as defined in [3GPP TS 23.040]). Messages and messages sent from BCAST AM-C to BCAST AM-M are MO-SMS messages.

The TAR value used to transfer the SMS is as defined in [ETSI TS 101.220] in section “Toolkit Application Reference (TAR)” for OMA BCAST Smartcard-Centric Audience Measurement.

For the MO-SMStwo addresses are used:

- The address of the SMSC of the service provider

- The TPDA (Transport Protocol Destination Address) address, which is the address of the final destination of the SMS. For the Audience measurement function the TPDA is the address of the BCAST AM-M

These addresses are set in the Smartcard at the personalization stage of the Smartcard or using remote provisioning of the Smartcard. These addresses MAY be updated by the configuration message as described in 5.20.2.3.3.

The Terminal is involved only to forward the messages from the Smartcard to the BCAST AM-M for MO-SMS and from BCAST AM-M to the Smartcard for MT-SMS using standard proactive commands as described in [3GPP TS 31.115] for 3GPP or [3GPP2 C.S0078-0] for 3GPP2. The fact that the SMS received or to be sent is for Audience Measurement function is transparent for the Terminal.

5.20.2.2.2. Security

Secured packets as defined in [3GPP TS 31.115] for 3GPP and [3GPP2 C.S0078-0] for 3GPP2 SHALL be supported when a secure transmission of data is required. The Kamue and Kamus established during the Registration process MAY be used.

5.20.2.2.3 HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems defined in RFC 2616.

Bearer Independent Protocol (BIP) MAY be used between the Smartcard and the Mobile Equipment as defined in [3GPP TS 31.111] for 3GPP or [3GPP2 C.S0035-A] for 3GPP2.

The Terminal is involved only to forward the messages from the Smartcard to the BCAST AM-M or from BCAST AM-M to the Smartcard as described in [3GPP TS 31.111] for 3GPP or [3GPP2 C.S0035-A] for 3GPP2. The fact that the HTTP channel is for Audience Measurement function is transparent for the terminal.

HTTP sessions are exclusively initiated by the application on the Smartcard. When a communication is requested by the BCAST AM-M, a push mechanism has to be sent to the card by the server in order to tell the application on the card to open a communication channel.

5.20.2.2.3.1. Structure of Data

Data are formatted in HTTP Post message and acknowledgements are sent back as HTTP Response message as described in RFC 2616.

5.20.2.2.3.2. Security

When required, TLS can be used to secure HTTP connections as defined in RFC 2818 and RFC 2246. HTTP over TLS provides privacy and integrity of data. Symmetric cryptographic materials (Kamue) exchanged at registration phase MAY be used.

5.20.2.2.4 Broadcast Provisioning

Broadcast Provisioning is the ability to deliver data through the broadcast channel to the Smartcard in the terminal. This is inherently a one way communication and thus can only apply for communication in AM-5 interface that does not require interaction. This functionality is described in section 5.19.

5.20.2.2.5 Generic Payload

Whatever the bearer used, the payload of messages is defined as a recursive BER TLV structure formatted as specified in [ETSI TS 101.220]:

```
<Message Tag (1 byte)> || <Message Length> || <Message Payload>
```

where the Message Value can be itself another BER TLVas defined in the various subsections in 5.20.2.3.

Several messages can also be concatenated in one single payload and MUST be treated like independent messages.

In addition, the message payload MAY be signed and/or encrypted as explained in section 5.20.2.2.5.1

Proprietary messages and fields can be defined for a specific usage on the field. BCAST AM-M and BCAST AM-C SHALL ignore messages and fields that they don't know.

5.20.2.2.5.1. Security

In the Smartcard, several key sets MAY be used for authentication, encryption and data integrity applied on generic payload:

User Keys: associated to a specific User.

Broadcast Keys: associated to a group of users or all users and used for Smartcard Broadcast Provisioning protocol

Credentials established during the Registration process (Kamue, Kamus) are User keys and are used to secure messages sent for a specific user

Broadcast Keys (Kambe, Kambs) are pre-provisioned in the Smartcard at the personalization stage of the card or set remotely using protocols that are out of scope of the present specification (e.g., OTA protocols). These keys are used for messages sent using Smartcard Broadcast Provisioning protocol.

The security level of a message SHALL be indicated in the Message Tag itself using the two most significant bits as specified below.

Message Tag format	Length (in bits)
`Message Tag () {`	**8**
`Signed message flag`	**1**
`Encrypted message flag`	**1**
`Clear Message Tag`	**6**
`}`	

Table 65: Message Tag format

For example, for a message which Clear Message Tag would be 0x01:

- its Message Tag would be 0x81 if it is sent signed;
- its Message Tag would be 0x41 if it is sent encrypted but not signed;
- and its Message Tag would be 0xC1 if it is sent signed and encrypted.

When a message is secured, it SHALL be formatted as:

```
<Secured Message Tag (1 byte)>|| <Message Length> || <Security information> ||
    <Secured Message Payload>
```

The Security information is used to retrieve the keys associated to a user, and also contains an optional signature. It SHALL be formatted as specified below.

Description	Value	M/O	Length (in bytes)
Security Tag	**0x10**	M	1
Length	L1+1+20	M	1
UserID (mandatory only for messages from BCAST AM-C to BCAST AM-M)	Binary	M/O	L1
Key set (mandatory only for messages from BCAST AM-M to BCAST AM-C, Absent for messages from BCAST AM-C to BCAST AM-M)	Binary	M/O	1
Signature	Binary	C	20

UserID: Indicates the UserID that has been assigned to the Smartcard either during registration process or during personalization stage of the Smartcard.

Key set: Indicates the key set to be used for decryption and for the verification of the signature.

0x00: User keys are used (Kamue and Kamus).

0x01: Broadcast Keys (Kambe and Kambs).

0x02 to 0x0F: reserved for future use

0x10 to 0xFF: reserved for proprietary use

Signature: The optional signature SHALL be computed on the entire clear Message Payload (i.e., excluding the Security information) using a keyed hash function:

For Key set= 0x00: Signature = HMAC SHA-1 (Message Payload, Kamus)

For Key set= 0x01: Signature = HMAC SHA-1 (Message Payload, Kambs)

For an encrypted message, the encryption SHALL be done on entire clear Message Payload (i.e., excluding the Security information) using the encryption algorithm:

For Key set= 0x00: Secured Message Payload = AES-CTR (Message Payload, Kamue)

For Key set= 0x01: Secured Message Payload = AES-CTR (Message Payload, Kambe)

When the message is not encrypted, the Secured Message Payload is identical to the clear Message Payload.

HMAC SHA-1 is defined in [RFC2104]. AES-CTR (counter mode) is defined in [RFC3711].

5.20.2.3 Messages

5.20.2.3.1 Registration

5.20.2.3.1.1. REGISTRATION_REQUEST message (BCAST AM-C to BCAST AM-M)

The REGISTRATION_REQUEST message tag is 0x01 The Registration Request TLV is sent in an MO-SMS that triggers a server registration request

Description	Value	M/O	Length (in bytes)
Client Identifiers Tag	**0x11**	M	1
Length	1+L1	M	1
Identifiers Type	Binary	M	1
Identifiers	Binary	M	L1
Card Random Tag	**0x12**	M	1
Length	16	M	1
Random	Binary	M	16

Table 66: REGISTRATION_REQUEST message

Identifiers Type: This field gives the type of the following Identifiers field

Value	Definition
0	3GPP type
1	3GPP2 type
2-127	for future use
128-255	for private use

Table 67: Identifiers Type

Identifiers: This field defines identifiers of Smartcard and Terminal, in the format specified through IdentifierType.

Identifiers Type	Identifiers	Definition	coding	Length (in bytes)	Length of Identifiers field (L1)
0	IMSI	International Mobile Subscriber Identity	as described in [3GPP TS 23 003]	9	27
	ICCID	Integrated Circuit Card Identification. This parameter provides a unique identification number for the UICC	as described in [ETSI TS 102221]	10	
	IMEI	International Mobile Equipment Identity	as defined in [3GPP TS 23.003]	8	
1	IMSI	International Mobile Subscriber Identity	as described in [3GPP TS 23 003]	9	26
	ICCID	Integrated Circuit Card Identification. This parameter provides a unique identification number for the UICC	as described in [ETSI TS 102221]	10	
	MEID	Mobile Equipment Identifier	As defined in [3GPP2 C.S0072-0]	7	
2-127		For future use			
128-255		For private use			

Table 68: **Identifiers**

Identifiers that occupy less space than the length in bytes specified for them in the table are padded with leading zeros to fill all the bytes after padding.

Random: Random value of 16 bytes used, together with the server random, for user keys generation (signature and cipher keys) as described in 5.20.2.1.1.

5.20.2.3.1.2. REGISTRATION_RESPONSE message (BCAST AM-M to BCAST AM-C)

The REGISTRATION_RESPONSE message tag is 0x02. The Registration Acknowledgement Response TLV is sent in an MT-SMS to set the user value.

Description	Value	M/O	Length (in bytes)
User ID Tag	**0x13**	M	1
Length	L1	M	1
User ID	Binary	M	L1
Server Random Tag	**0x14**	M	1
Length	16	M	1
Random	Binary	M	16

Table 69: REGISTRATION_ RESPONSE message

User ID: unique identifier assigned by BCAST AM-M to each BCAST AM-C. It can be the IMSI or any other service provider specific identifier, such as, e.g., a registration serial number.

Random: Random value of 16 bytes used, together with the card random, for user keys generation (signature and cipher keys) as described in 5.20.2.1.1.

5.20.2.3.1.3. AUDIT_REQUEST message (BCAST AM-M to BCAST AM-C)

The AUDIT_REQUEST message tag is 0x0B. The TLV (Tag Length Value) format is used to request the list of features the BCAST AM-C supports, the current state, configuration of the BCAST AM-C and the last status error.

Description	Value	M/O	Length (in bytes)
Audit_request Tag	**0xXX**	M	1
Length	L1	M	1
Tags list	Binary	M	L1

Table 70: AUDIT_REQUEST message

Tags list : This field contains the list of parameters, the AUDIT_RESPONSE SHALL contain. This list of parameters is in the form of list of tags of the corresponding parameters. The accepted values of tags are those listed in the AUDIT_RESPONSE message table.

5.20.2.3.1.4. AUDIT_RESPONSE message (BCAST AM-C to BCAST AM-M)

The AUDIT_RESPONSE message tag is 0x0C. The TLV (Tag Length Value) format is used to carry the list of features supported by BCAST AM-C and the current state and configuration of BCAST AM-C. The AUDIT_RESPONSE contains all the parameters that were requested in the AUDIT_REQUEST command in the Tags list.

Description	Value	M/O	Length (in bytes)
Client Identifiers Tag	**0x11**	O	1
Length	1+L1	O	1
Identifiers Type	Binary	O	1
Identifiers	Binary	O	L1
User ID Tag	**0x13**	O	1
Length	L2	O	1
User ID	Binary	O	L2
Opt-in state Tag	**0x21**	O	1
Length	1	O	1
Opt-in state	Boolean value	O	1
AM-C state Tag	**0xE0**	O	1
Length	L3	O	C
AM-C state	Binary	O	L3
BCAST AM-M address Tag	**0xA2**	O	1
Length	L4	O	A
BCAST AM-M address	URL	O	L4
SMSC address Tag	**0xA3**	O	1

Length	L5	O	B
SMSC address	Binary	O	L5
TPDA address Tag	**0xA4**	O	1
Length	L6	O	C
TPDA address	Binary	O	L6
Supported bearers Tag	**0xE1**	O	1
Length	L7	O	C
Supported bearers	Binary	O	L7
Security type supported Tag	**0xE2**	O	1
Length	L8	O	C
Security type supported	Binary	O	L8
Location type supported Tag	**0xE3**	O	1
Length	L9	O	C
Location type supported	Binary	O	L9
Buffer size Tag	**0xE4**	O	1
Length	L10	O	C
Buffer size	Binary	O	L10
Buffer filling level Tag	**0xE5**	O	1
Length	L11	O	C
Buffer filling level	Binary	O	L11
Reporting trigger Tag	**OxA8**	O	1
Length	L12	O	D
Reporting trigger	Unsigned short	O	L12
Last status error Tag	**0xE6**	O	1
Length	1	O	1
Last status error	Binary	O	1
Terminal Smartcard-Centric AM Capability Tag	0xE7	O	1
Length	1	O	1
Terminal Smartcard-Centric AM Capability	Binary	O	1

Table 71: AUDIT_RESPONSE message

Identifiers Type: same as Table 66: REGISTRATION_REQUEST message

Identifiers: same as Table 66: REGISTRATION_REQUEST message

User ID: same as Table 69: REGISTRATION_RESPONSE message

Opt-in state: same as Table 73: OPT_IN message

AM-C state: this field gives the state of the AM-C:

0x00: Stopped

0x01: Running

0x02: Pause

Other values: reserved for future use

BCAST AM-M address: same as Table 75: CONFIGURATION message

SMSC address: same as Table 75: CONFIGURATION message

TPDA address: same as Table 75: CONFIGURATION message

Supported bearers: this field gives the list of supported bearers

0x00: BIP

0x01: SMS only

0x02: BIP and SMS

0x80: BIP only (but Terminal does not support TCP)

0x81: SMS only (but Terminal does not support TCP)

0x82: BIP and SMS (but Terminal does not support TCP)

Other values: reserved for future use

Security type supported: This field gives the type of security the BCAST AM-C supports.

0x01: At transport level (e.g. SMS-PP or HTTPs)

0x02: At application level

0x03 At both levels (transport level and application level)

Other values: reserved for future use

Location type supported: This field gives the type of location tracking supported by the BCAST AM-C. If several types are supported a list of location types is present in the location type supported TLV.

The MSB of the location type supported indicates the tracking state of this location system (0XXXXXXX: Deactivated; 1XXXXXXX: Activated)

The other bits indicate the type of location:

0x00: Geographical location (as defined for GAD shapes in [3GPP TS 31.111])

0x01: 3GPP Location (as defined for Location Information in [3GPP TS 31.111])

0x02: 3GPP2 location (as defined for Location Information in [3GPP2 C.S0035-A])

0x03: DVB-H location (as defined for Broadcast Network Information in [3GPP TS 102.223])

0x04: DVB-SH location (as defined for Broadcast Network Information in [3GPP TS 102.223])

0x05: WiMAX location

0x06: Forward Link Only location

Buffer size: This field indicates the size of the buffer for the reporting, in bytes

Buffer filling level: This filed indicates the used size of the buffer, in bytes

Reporting trigger: same as Table 75: CONFIGURATION message

Last status error: This field gives the last status error

0x0000: NO_ERROR

0x00XX: XX is the tag value of the TLV in error or the tag value of the command in error.

(e.g. 0x0011 ERROR_TAG_CLIENT_IDENTIFIERS)

Terminal Smartcard-Centric AM Capability: This field indicates if the Terminal supports the Smartcard-Centric Audience Measurement

0x00: Indicates that the Terminal doesn't support the Smartcard-Centric AM

0x01: Indicates that the Terminal supports the Smartcard-Centric AM

5.20.2.3.2 Opt-in

5.20.2.3.2.1. OPT_IN_INVITATION_TRIGGER message (BCAST AM-M to BCAST AM-C)

The OPT_IN_INVITATION_TRIGGER message tag is 0x03. The format of its payload is detailed in Table 73 below.

Description	Value	M/O	Length (in bytes)
Prompt message Tag	**0x22**	O	1
Length	L1	O	C
Language code	As defined below	O	2
Prompt message	String	O	L1-2

Table 72: OPT_IN message

Note: there MAY be more than one Prompt message tag in the OPT_IN_INVITATION_TRIGGER message, each for different languages.

Language code – the language code is a pair of alpha numeric characters, defined in [ISO-639-1]. the alpha-numeric character shall be coded on one byte using SMS default 7-bit coded alphabet as defined in [3GPP TS 23.038] with bit 8 set to 0.

Prompt message - this is a text that is displayed on the Terminal. The way the Smartcard will use for this display on Terminal is out of scope of this specification but e.g. DISPLAY TEXT SIMToolkit command defined in [ETSI TS 102.223] MAY be used.

5.20.2.3.2.2. OPT_IN message (BCAST AM-M to BCAST AM-C)

The OPT_IN message tag is 0x04. The format of its payload is detailed in Table 73 below.

Description	Value	M/O	Length (in bytes)
Opt-in state Tag	**0x21**	M	1
Length	1	M	1
Opt-in state	Boolean value	M	1

Table 73: OPT_IN message

Opt-in state - this is a flag indicating whether the user is currently opted-in (value 0x01) or opted-out (value 0x00).

5.20.2.3.2.3. OPT_IN_STATE_NOTIFICATION message (BCAST AM-C to BCAST AM-M)

OPT_IN_STATE_NOTIFICATION message tag is 0x05. The format of its payload is detailed in Table 74 below.

Description	Value	M/O	Length (in bytes)
User ID Tag	**0x13**	M	1
Length	L1	M	1
User ID	Binary	M	L1
Opt-in state Tag	**0x21**	M	1
Length	1	M	1
Opt-in state	Boolean value	M	1

Table 74: OPT_IN_STATE_NOTIFICATION message

User ID: same as Table 69: REGISTRATION_ RESPONSE message

Opt-in state: same as Table 73: OPT_IN message

5.20.2.3.3 CONFIGURATION message (BCAST AM-M to BCAST AM-C)

The CONFIGURATION message tag is 0x06. The TLV (Tag Length Value) format is used to carry configuration parameters to the BCAST AM-C.

Description	Value	M/O	Length (in bytes)
Reporting bearer Tag	**0xA1**	O	1
Length	1	O	1
Reporting bearer	Binary	O	1
BCAST AM-M address Tag	**0xA2**	O	1
Length	L1	O	A
BCAST AM-M address	URL	O	L1
SMSC address Tag	**0xA3**	O	1
Length	L2	O	B
SMSC address	Binary	O	L2
TPDA address Tag	**0xA4**	O	1
Length	L3	O	C
TPDA address	Binary	O	L3
Reporting mode Tag	**0xA6**	O	1
Length	1	O	1
Reporting mode	Binary	O	1
Reporting frequency Tag	**0xA7**	O	1
Length	1	O	1
Reporting frequency	Unsigned short	O	1
Reporting trigger Tag	**OxA8**	O	1
Length	L5	O	D
Reporting trigger	Unsigned short	O	L5
Location Type Tag	**0xA9**	O	1
Length	1	O	1
Location Type	Binary	O	1
AM Control Type for Clear to Air Tag	**0xAB**	O	1
Length	1	O	1
AM Control Type for Clear to Air	Binary	O	1
Additional metrics Tag	**0xAA**	O	1
Length	4	O	1
Additional metrics	Binary	O	4

Table 75: CONFIGURATION message

Reporting bearer: bearer used for reporting messages (SMS or HTTP)

0x00 = Hyper Text Transfer Protocol (HTTP)

0x01 = Short Message Service Point to Point (SMS-PP)

BCAST AM-M address: BCAST AM-M URL coded in UTF-8. This address is used to send the REPORTING message over HTTP.

SMSC address: address of SMS centre. This is the TS-Service Centre Address as defined in [3GPP TS 31.102]. Coded as defined for EF_{SMSP} [3GPP TS 31.102] for TS-Service Centre Address

TPDA address: address of BCAST AM-M when using SMS bearer, This is the TP-Destination Address as defined in [3GPP TS 31.102]. Coded as defined for EF_{SMSP} in [3GPP TS 31.102] for TP-Destination Address

Reporting mode: Mode of reporting:

0x00 = Push (from BCAST AM-C to BCAST AM-M)

0x01 = Pull (Reporting triggered by BCAST AM-M)

Reporting frequency: period in hours between two data reporting in Push mode

Reporting trigger: data size which triggers an automatic reporting from BCAST AM-C

Location Type: This field gives the type of location the BCAST AM_C should return in the report. This tag is present only if the location information is required by BCAST AM_M as indicated in additional metrics. If several location types are needed a list of location types is present in the location type TLV. The following values are defined:

0x00: Geographical location (as defined for GAD shapes in [3GPP TS 31.111])

0x01: 3GPP Location (as defined for Location Information in [3GPP TS 31.111])

0x02: 3GPP2 location (as defined for Location Information in [3GPP2 C.S0035-A])

0x03: DVB-H location (as defined for Broadcast Network Information in [3GPP TS 102.223])

0x04: DVB-SH location (as defined for Broadcast Network Information in [3GPP TS 102.223])

0x05: WiMAX location

0x06: Forward Link Only location

0xFF to 0x07: reserved for future use.

AM Control Type for Clear to Air: Indicates if the AM control for clear to air services is used using "AM Control for Clear to Air contents" event of the Event Signalling Mode of BCAST command as defined in [BCAST11-ServContProt].

- If set to 0 or the TLV is absent**,** indicates that the AM control signalled in the Event Signalling Mode of the BCAST command is not used. If the AM control is needed, it is done using the access criteria Audience_measurement_control descriptor in the STKM .
- If set to 1 indicates that the AM control for Clear to air services signalled in the Event Signalling Mode of the BCAST command is used.

Additional metrics: this is a bit mask indicating the additional metrics required by the BCAST AM-M, in addition to zapping information.

Bit 0: indicates the location_In information shall be provided (1) or not (0). Location_In is the Location where the user is when she starts watching a particular service.

Bit 1: indicates the location_Out information shall be provided (1) or not (0). Location_Out is the Location where the user is when she stops watching a particular service

Bits 2 : Indicates that the consumption time provided by the Terminal in the Event Signalling Mode of the BCAST command SHALL be provided (1) or SHALL NOT (0)

Bit 3: Indicates that the Content ID provided by the Terminal in the Event Signalling Mode of the BCAST Command SHALL be provided (1) or SHALL NOT (0)

Bit 4 to 15 are reserved for future use.

Bits 16 to 31 are reserved for proprietary extensions.

5.20.2.3.4 ACTIVATION message (BCAST AM-M to BCAST AM-C)

The ACTIVATION message tag is 0x07. The TLV (Tag Length Value) format is used to carry activation parameters to the BCAST AM-C.

Description	Value	M/O	Length (in bytes)
Activate state Tag	**0xB0**	M	1
Length	1	M	1
Activation state	Boolean value	M	1

Table 76: ACTIVATION message

Activation state: Activation state sent by BCAST AM-M to activate (value 0x01) or deactivate (value 0x00) the Audience Measurement application in the BCAST AM-C

5.20.2.3.5 Reporting

The REPORTING message MAY be transported via SMS or over HTTP. The description of the REPORTING message via SMS is described in section 5.20.2.3.5.1 and the REPORTING message sent over HTTP is described in section 5.20.2.3.5.3

5.20.2.3.5.1. REPORTING message via SMS (BCAST AM-C to BCAST AM-M)

The REPORTING message tag is 0x08. The format of its payload is detailed in the table below.

Description	Value	M/O	Length (in bytes)
User ID Tag	**0x13**	M	1
Length	L1	M	A
User ID	Binary	M	L1
Reporting data Tag	**0xC0**	M	1
Length	3+L1+…+Ln	M	1
Reporting mode	Binary	M	1
Report ID	Binary Unsigned short	M	2
Zapping event [1]	Zapping event record	M	L1
….			
Zapping event [n]	Zapping event record	O	Ln

Table 77: REPORTING message

User ID: same as Table 69: REGISTRATION_ RESPONSE message

Reporting mode: indicates the mode of the report:

0x00: Push (reporting triggered by BCAST AM-C when data size reaches the reporting trigger value),

0x01: pull (reporting triggered by BCAST AM-M request)

0x02: cyclic (automatic periodic reporting)

Report ID: reporting identifier, this information is repeated in the REPORTING_RESPONSE message for BCAST AM-M acknowledgement

Zapping event: audience data representing a service consumption session, sent from BCAST AM-C to BCAST AM-M

The BCAST AM-C SHALL format Zapping event records as follows:

Description	Value	M/O	Length (in bytes)
Record Format	Binary	M	2
Key Domain ID	Binary	O	3
Key group part	Binary	O	2
Time stamp	Binary	O	1,2,3,4
Duration	Binary	O	1,2,3,4
Additional_metrics TLV	See values below	O	1
””	L1	O	1
””	Binary	O	L1

Table 78: Zapping event record format

Note 1: The first Zapping event of Audience data SHALL contain Key Domain ID, Key group part and Time stamp.

Note 2: A Zapping event MAY contain Key Domain ID, Key group part and Time stamp even if it is not the first event.

Record Format: detailed below in Table 78: Zapping event record format

Key Domain ID: key domain ID value retrieved from STKM message

Key group part: key group part value retrieved from STKM message

Time stamp: if it is the first Zapping event of the Audience data, this is the value of the Time stamp extracted from the STKM and coded on 4 bytes. Otherwise, it is the difference between the Time stamp of the current Zapping event and the Time stamp in the previous Zapping event. The format of the Time stamp is then defined in the Record Format (see Table 78: Zapping event record format)

Duration: equal to the last time stamp minus the first time stamp of a service consumption sequence**Additional_metrics TLV:** These TLVs allow the coding of additional metrics. The MSB of the tag value signals if there is additional TLV after the current TLV. If the MSB is set to 1, this indicates that there is another TLV (another metric) after this current TLV. If the MSB is set to 0, this indicates that this is the last metric of this zapping event.

The list of tags for additional metrics defined for this version of the specification is given in the table below

Tag name	Value	Description
Location_In	0x01	This TLV gives the Location where the user is when she starts watching a particular service
Location_Out	0x02	This TLV gives the Location where the user is when she stops watching a particular service
Consumption Time	0x03	This TLV gives the Consumption Time provided by the Terminal, consumption time by a user of the content concerned by the zapping event..

Service/Content ID	0x04	This TLV gives the Identifier of the content concerned by the zapping event. This Identifier is provided by the Terminal

Table 79: **list of** tags for **additional metrics**

Description	Value	M/O	Length (in bytes)
Location Tag	0x01 or 0x02	M	1
Length	L0	M	1
Location_Type	See below	M	1
If (Location_type ==0x00) {			
Length of GAD shape	L1	O	1
GAD shape	See below	O	L1
}			
If (Location_type ==0x01) {			
3gpp_LAC	Binary	O	2
3gpp_Cell ID	Binary	O	2
}			
If (Location_type == 0x02) {			
3gpp2_SID	Binary	O	2
3gpp2_NID	Binary	O	2
3gpp2_BASE_ID	Binary	O	2
3gpp2_BASE_LAT	Binary	O	3
3gpp2_BASE_LONG	Binary	O	3
}			
If (Location_type == 0x03 or 0x04) {			
dvb_Network_ID	See below	O	2
dvb_Cell ID	See below	O	2
number_of_dvb_subcell_ID	Binary	O	1
for (j=0; j< number_of_dvb_subcell_ID; j++) {			
dvb_Subcell_ID	See below	O	1
}			
}			
If (Location_type == 0x05) {			
number_of_wimax_bsids	Binary	O	2
for (j=0; j< number_of_wimax_bsids; j++) {			
wimax_BSID	See below	O	6
}			
}			
If (Location_type == 0x06) {			
flo_network_ID	See below	O	2
flo_presence_flags	See below	O	1
If (flo_presence_flags = 0xXXXXXXX1) {			
flo_WOI_ID }	See below	O	2
If (flo_presence_flags = 0xXXXXXX1X) {			
flo_LOI_ID	See below	O	2

}			
}			

Table 80: **Location TLV definition**

Note: several Location tags MAY be present with a location_type different for each.

Location_Type: This field gives the type of location. The following values are defined:

0x00: Geographical location (as defined for GAD shapes in [3GPP TS 31.111])

0x01: 3GPP Location (as defined for Location Information in [3GPP TS 31.111])

0x02: 3GPP2 location (as defined for Location Information in [3GPP2 C.S0035-A])

0x03: DVB-H location (as defined for Broadcast Network Information in [3GPP TS 102.223])

0x04: DVB-SH location (as defined for Broadcast Network Information in [3GPP TS 102.223])

0x05: WiMAX location

0x06: Forward Link Only location

Length of GAD shape: the length of the Universal Geographical Area Description (GAD) shape in Binary coding

GAD shape: Universal geographical area description shape. Shape data is encoded as described in [3GPP TS 23.032] with the first byte of the shape containing the shape type. The GAD shape is retrieved from the terminal using the ENVELOPE (Geographical Location Reporting) Command (as defined in[3GPP TS 31.111 v8]. This is the value of GAD shape when the user starts watching a particular service in the Location_In TLV and is the value of GAD shape when the user stops watching the current service in the Location_Out TLV.

3gpp_LAC: This is the value of LAC (Location Area Code) when the user starts watching a particular service in the Location_In TLV and is the value of LAC (Location Area Code) when the user stops watching the current service in the Location_Out TLV. LAC is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP TS 31.111] for 3GPP at the beginning of a service consumption sequence or at the end of a service consumption sequence.

3gpp_Cell ID: This is the identifier of the cell where the user is when she starts watching a particular service in the Location_In TLV and this is the identifier of the cell where the user is when she stops watching the current service in the Location_Out TLV. The cell identifier is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP TS 31.111] for 3GPP) at the beginning of a service consumption sequence or at the end of a service consumption sequence.

3gpp2_SID: 3GPP2 System Identification as defined in [3GPP2 C.S0005-E]. SID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP2 C.S0035-A] for 3GPP2)

3gpp2_NID: 3GPP2 Network Identification as defined in [3GPP2 C.S0005-E]. NID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP2 C.S0035-A] for 3GPP2)

3gpp2_BASE_ID: 3GPP2 Base Station Identification of the current base station as defined in [3GPP2 C.S0005-E]. BASE_ID is retrieved from terminal using proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP2 C.S0035-A] for 3GPP2

3gpp2_BASE_LAT: 3GPP2 Base Station Latitude of the current base station as defined in [3GPP2 C.S0005-E]. BASE_LAT is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP2 C.S0035-A] for 3GPP2)

3gpp2_BASE_LONG: 3GPP2 Base Station Longitude of the current base station as defined in [3GPP2 C.S0005-E]. BASE_LONG is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION (as defined in [ETSI TS 102.223] and [3GPP2 C.S0035-A] for 3GPP2)

dvb_Network_ID: is defined in [ETSI EN 300 468] and is transmitted in the Network Information Table (NIT) according to [ETSI EN 300 468]. The dvb_Network_ID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION(Broadcast Network Information) (as defined in [ETSI TS 102.223]) at the beginning of a service consumption sequence in the Location_In TLV or at the end of a service consumption sequence in the Location_Out TLV.

number_of_dvb_subcell_ID: specifies the number of dvb subcell_ID fields included in the following loop.

dvb_Subcell_ID: corresponds to cell_id_extension defined in [ETSI EN 300 468] and is transmitted as "cell_id_extension" in the Network Information Table (NIT) according to [ETSI EN 300 468]. The dvb_Subcell_ID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION(Broadcast Network Information) (as defined in [ETSI TS 102.223]) at the beginning of a service consumption sequence in the Location_In TLV or at the end of a service consumption sequence in the Location_Out TLV.

number_of_wimax_bsids: specifies the number of WiMAX BSID fields included in the following loop.

wimax_BSID: WiMAX Base Station Identifier as specified in [IEEE 802.16-2004] and [IEEE 802.16e-2005]

flo_network_ID: Identifier of the particular network defining the WOI_ID and LOI_ID, according to [TIA-1099a], Section 1.11. The flo_network_ID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION(Broadcast Network Information) (as defined in [ETSI TS 102.223]) at the beginning of a service consumption sequence in the Location_In TLV or at the end of a service consumption sequence in the Location_Out TLV.

flo_presence_flags: - indicates whether the Infrastructure Identifiers are present in the forward link only cell identification structure.

Bit 0:

If set to 1, Wide-Area Infrastructure Identifier is present in the forward link only cell identification structure.

If set to 0: Wide-Area Infrastructure Identifier is absent in the forward link only cell identification structure.

Bit 1:

If set to 1, Local-Area Infrastructure Identifier is present in the forward link only cell identification structure.

If set to 0: Local-Area Infrastructure Identifier is absent in the forward link only cell identification structure.

Bit 2 to 7: reserved for future use

flo_WOI_ID: Wide-Area Infrastructure ID, transmitted in Wide-Area OIS Channel, according to [TIA-1099a], Section 1.11. The flo_WOI_ID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION(Broadcast Network Information) (as defined in [ETSI TS 102.223]) at the beginning of a service consumption sequence in the Location_In TLV or at the end of a service consumption sequence in the Location_Out TLV.

flo_LOI_ID: Local-Area Infrastructure ID, transmitted in Wide-Area OIS Channel or RF Channel Description Message, according to [TIA-1099a], Section 1.11. The flo_LOI_ID is retrieved from the terminal using the proactive command PROVIDE LOCAL INFORMATION(Broadcast Network Information) (as defined in [ETSI TS 102.223]) at the beginning of a service consumption sequence in the Location_In TLV or at the end of a service consumption sequence in the Location_Out TLV.

Description	Value	M/O	Length (in bytes)
Consumption Time Tag	0x03	M	1
Length	4	M	1
Consumption Time	Binary	M	4

Table 81: Consumption Time TLV definition

Consumption Time: integer value of the accumulated service consumption time encoded on 4 bytes. Service/Content consumption time is calculated from the information sent in "Event Signalling Mode" command defined in [BCAST11-ServContProt]. Actual service consumption time is $2^{\text{Consumption Time}}$ seconds. For reliability,time reference for this Consumption Time SHOULD NOT be a time that may be modified by the user.

Description	Value	M/O	Length (in bytes)
Service/Content IDTag	0x04	M	1
Length	L0	M	7
Service/content ID	String	M	L0

Table 82: Service/Content ID TLV definition

Service/Content ID: anyURI value (GlobalServiceID and GlobalContentID) retrieved from "Event Signalling Mode" command defined in [BCAST11-ServContProt]. This Identifier is retrieved by the Terminal in the Service Guide.

In case of clear to air services and contents, this value is present and is coded as follows:

"GlobalServiceID"||"/"||"GlobalContentID"

For encrypted services, The GlobalServiceID is not necessary as the Key domain ID and Key group part are introduced in the Zapping event record as described in table78. The Service/content ID is then coded as follow

"/"||"GlobalContentID"

The Record Format field is encoded as follows:

Record_Format field description	Length (in bits)	Type
Record_Format() {	16	
key_domain_id_presence_flag	1	bslbf
key_group_part_index	6	uimsbf
ts_sign	1	bslbf
ts_format	3	uimsbf
duration_format	3	uimsbf
additional_metrics_presence_flag	1	bslbf
reserved_for_future_use	1	bslbf
}		

Table 83: Zapping event Record Format encoding

key_domain_id_presence_flag - key_domain_id is present (1) or absent (0) in this Zapping event. When it is absent, the last key_domain_id present in the Audience data is used.

key_group_part_index – 0 indicates that the key_group_part is not present; any other value indicates the index of the first occurrence of key_group_part coded on 6 bits.

ts_sign – used when ts_format=1,2,3, or 4.0 indicates that Time stamp is greater than or equal to zero, 1 indicates that Time stamp is strictly lower than 0.

ts_format – coding of Time stamp in absolute or relative value: the value 0 indicates that Time stamp is not present; values 1, 2, 3 and 4 indicate the number of bytes used to code the Time stamp relative value; 8 indicates that the absolute Time stamp value is present.

duration_format – 0 indicates that Duration is not present, 1, 2, 3 and 4 indicate the number of bytes used to code the Duration.

additional_metrics_presence_flag –This bit indicates whether additional metrics are present in the zapping event record. 0: there no additional metrics; 1: Additional metrics are appended in the zapping event record in the form of TLV.

5.20.2.3.5.2. REPORTING_RESPONSE via SMS (BCAST AM-M to BCAST AM-C)

The REPORTING_RESPONSE message tag is 0x09. The format of its payload is detailed in the table below.

Description	Value	M/O	Length (in bytes)
User ID Tag	**0x13**	M	1
Length	L1	M	1
User ID	Binary	M	L1
Reporting message state Tag	**0xC1**	M	1
Length	L2+1	M	1
Report ID	Binary Unsigned short	M	L2
Reporting message state	Boolean value	M	1

Table 84: REPORTING_RESPONSE message

Report ID: same as Table 77: REPORTING message

Reporting message state - Boolean value indicating the user's reporting message state: 0x00 = Successful (BCAST AM-M has received the REPORTING message), 0x01 = Failed (BCAST AM-M has failed to handle the REPORTING message received)

5.20.2.3.5.3. REPORTING message over HTTP (BCAST AM-C to BCAST AM-M)

When the REPORTING message is sent over HTTP, the data is formatted in a POST message and the acknowledgement is received via an HTTP response..

Data	Description	M/O
POST [BCAST AM-M reporting URI] HTTP/1.1 Content-Type: application/x-www-form-urlencoded(CRLF) Accept-Encoding: deflate(CRLF) User-Agent: BCAST AM-C/1.0(CRLF) Host: [BCAST AM-M address](CRLF) From: [User ID](CRLF) Content-Length: [XXX] (CRLF) (CRLF)	Header	M
data=[REPORTING message]	Base 64 encoding of the REPORTING message	M

	defined in section 5.20.2.3.5.1	

Table 85: REPORTING message sent over HTTP

5.20.2.3.5.4. REPORTING_RESPONSE over HTTP (BCAST AM-M to BCAST AM-C)

HTTP response returned after receiving a reporting message:

Data	Description	M/O
HTTP/1.[X] 200 OK Host: [XXX] Content-Length: [XXX]	Header	M
REPORTING_RESPONSE message: [XX]	Base 64 encoding of the REPORTING_RESPONSE message defined in section 5.20.2.3.5.2	M

5.20.2.3.5.5. REPORTING_REQUEST message (BCAST AM-M to BCAST AM-C)

The REPORTING_REQUEST message tag is 0x0A. The format of its payload is detailed in Table 86.

Description	Value	M/O	Length (in bytes)
Reporting request Tag	**0xD0**	M	1
Length	0	M	1

Table 86: REPORTING_REQUEST message

5.20.2.3.6 Defined Message Tags

The following table lists all the Clear Message Tags defined in the previous sections.

Message Name	Clear Message Tag	Defined in Section
REGISTRATION_REQUEST	0x01	5.20.2.3.1.1
REGISTRATION_RESPONSE	0x02	5.20.2.3.1.2
OPT_IN_INVITATION_TRIGGER	0x03	5.20.2.3.2.1
OPT_IN	0x04	5.20.2.3.2.2
OPT_IN_STATE_NOTIFICATION	0x05	5.20.2.3.2.3
CONFIGURATION	0x06	5.20.2.3.3
ACTIVATION	0x07	5.20.2.3.4
REPORTING	0x08	5.20.2.3.5.3

REPORTING_RESPONSE	0x09	5.20.2.3.5.4
REPORTING_REQUEST	0x0A	5.20.2.3.5.5
AUDIT_REQUEST	0x0B	5.20.2.3.1.3
AUDIT_RESPONSE	0x0C	5.20.2.3.1.4

Table 87: Clear Message Tags

5.20.2.3.7 Defined Field Tags

The following table lists all the Tags defined in the previous sections for message fields.

Tag Name	Value	Defined in Section
Security	0x10	5.20.2.2.5.1
Client Identifiers	0x11	5.20.2.3.1.1
Card Random	0x12	5.20.2.3.1.1
User ID	0x13	5.20.2.3.1.2, 5.20.2.3.2.3
Server Random	0x14	5.20.2.3.1.2
Opt-in state	0x21	5.20.2.3.2.2, 5.20.2.3.2.3
Prompt message	0x22	5.20.2.3.2.1
Reporting bearer	0xA1	5.20.2.3.3
BCAST AM-M address	0xA2	5.20.2.3.3
SMSC address	0xA3	5.20.2.3.3
TPDA address	0xA4	5.20.2.3.3
Reporting mode	0xA6	5.20.2.3.3
Reporting frequency	0xA7	5.20.2.3.3
Reporting trigger	0xA8	5.20.2.3.3
Location Type	0xA9	5.20.2.3.3
Additional metrics	0xAA	5.20.2.3.3
AM Control Type for Clear to Air	0xAB	5.20.2.3.3
Activation state	0xB0	5.20.2.3.4
Reporting data	0xC0	5.20.2.3.5.1
Reporting message state	0xC1	5.20.2.3.5.2
Reporting request	0xD0	5.20.2.3.5.5
AM-C state	0xE0	5.20.2.3.1.4
Supported bearers	0xE1	5.20.2.3.1.4
Security type supported	0xE2	5.20.2.3.1.4
Location type supported	0xE3	5.20.2.3.1.4
Buffer size	0xE4	5.20.2.3.1.4
Buffer filling level	0xE5	5.20.2.3.1.4
Last status error	0xE6	5.20.2.3.1.4
Terminal Smartcard-Centric AM Capability	0xE7	5.20.2.3.1.4

5.21 Related Contents Inquiry

Related Contents Inquiry allows service provider to recommend user according to user's interest. The phrase 'one content is related to another content', in this section, refers to the case where two contents are similar in terms of context or of theme. The relationships between different contents are determined by the service provider.

Overall procedure of Related Contents Inquiry is as follows:

1. On user's command, the terminal SHALL send RelatedContentsRequest message including GlobalContentID of Content of interest to the BSM in order to obtain complete set of Service Guide fragments which describes contents related to the content of interest.

2. On receiving the RelatedContentsRequest message, the BSM SHALL check if there exist contents related to the one contained in the request and the related contents are provided with on-Demand services, then BSM SHALL respond with RelatedContentsResponse message containing provisioning Service Guide fragments and with success code of '000' in globalStatusCode. The Service Guide fragments may offer both on-Demand services of individual content and on-Demand service of bundled contents. If globalStatusCode contains '000' for its value, the Service Guide fragments SHALL include one or more PurchaseItem fragments, PurchaseChannel fragments, and PurchaseData fragments.

    A. In this step, the BSM SHALL inform BSD/A to prepare for the Service Guide fragments, so that the BSD/A can respond to request of the Service Guide fragments from the Terminal.

3. For several reasons such as network failure, missed SG reception, or memory shortage, the Terminal may not have entire set of Service Guide fragments indicated in the RelatedContentsResponse message. Thus, for each idRef of ServiceReference, and ContentReference in the PurchaseItem fragment, the Terminal SHALL search for matching Service or Content fragments in the stored Service Guide which has been obtained via process specified in the section 5.4 of BCAST11-SG. If the Terminal failed to find any Service or Content fragments referenced by PurchaseItem fragments, the Terminal SHALL acquire the missing fragments via procedure specified in section 5.5.2 of BCAST 1.1 SG.

4. After obtaining required Service Guide fragments the terminal SHALL initiate the Service Request procedure using the information in the received Purchase Fragments.

If either the service provider cannot find any related contents or cannot provide on-Demand services for the found related contents, BSM SHALL respond with Related Contents Response message with error code of '22' in globalStatusCode indicating BSM cannot provide user with on-Demand service of the related contents.

5.22 Coupon Documents

The Coupon document is used to express a relative discount to some PurchaseData fragment. Thus, the Coupon document meets a number of contrasting goals in BCAST. Examples of these goals are:

- A Coupon document can be awarded as a result of a purchase transaction (as a premium, bonus, or 'frequent user' reward). As such, it can be awarded as a result of BCAST service provisioning.
- A Coupon can be broadcast to the terminal to attract new customers, i.e. delivered via BCAST broadcast file delivery in an electronic newspaper, or unicast via email or mms, or downloaded from a web page. All the non-BCAST delivery methods require integrity protection (digital signatures) to prevent coupon forgery.
- A Coupon can be specific to a particular user, or can be usable by any user. A coupon can be single-use, or can allow multiple uses by the same user.
- A Coupon can be issued by a service provider, or by a content producer. In the latter case, a service provider needs a method to securely verify the authenticity of a coupon via digital signing, so that the service provider can be assured of being compensated for the coupon.
- A Coupon can be used to produce a discount on a Service subscription. However, a service subscription can be available in several different lengths (a day, a week, a month, a year.) Thus, the coupon can be specific to a certain length of subscription (e.g. half-off for a monthly or yearly subscription only. To meet this goal, a coupon must be

able to identify not only a PurchaseItem, but also a specific PurchaseData associated with the PurchaseItem, because the PurchaseData contains the subscription term.

- A Coupon can be issued by one of many purchase channels. In that case, the coupon's scope can be narrowed to refer to a specific PurchaseChannel associated with the PurchaseData.

There are many similarities between a coupon document and a PurchaseData fragment in the service guide [BCAST11-SG]. However, most fragments in the service guide change often, whereas coupon documents are long-lived, and so coupons are managed outside of the service guide. Nevertheless, the last three use cases require coupons to point to fragments in the service guide. This is done using globally unique pointers (globalPurchaseItemID, globalPurchaseDataID, and globalPurchaseChannelID), which do not change as the service guide is refreshed. Figure 5shows the relationship between Coupon documents and service guide fragments.

This specification makes use of digital signatures and message authentication codes (MACs) to ensure integrity and authenticity of coupon documents. Coupon document generators MUST generate the coupon in "pre-canonicalized" form and MUST NOT rewrite coupons when transmitting or copying coupons. This means that coupons MUST NOT use namespace prefixes and MUST use Exclusive Canonicalization without comments, as specified in [XC14N]. The *InclusiveNamespaces PrefixList* of a coupon MUST be empty.

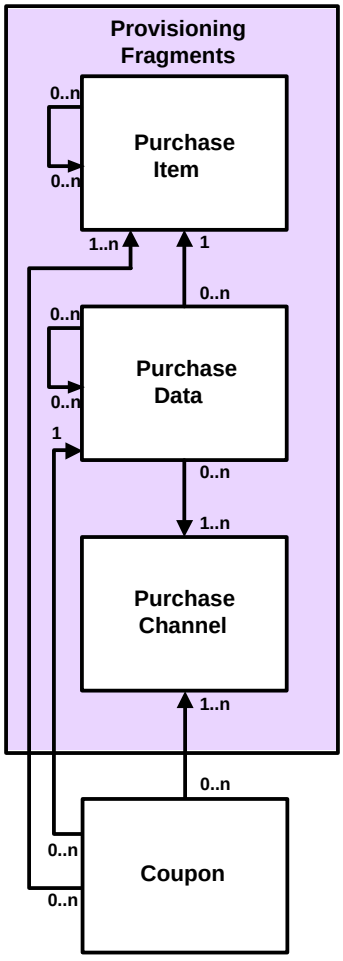


Figure 5: Coupon document and its pointers to Service Guide fragments.

Coupon documents are XML documents with a top-level Coupon element defined in "urn:oma:xml:bcast:pr:orderqueries:1.1" namespace [BCAST11-XMLSchema-orderqueries], with the following structure:

Name	Type	Category	Cardinality	Description	Data Type
Coupon	E	O		'Coupon' fragment	

				Contains the following attributes: id version validFrom validTo mustVerify Contains the following elements: GlobalPurchaseItemID GlobalPurchaseDataID GlobalPurchaseChannelID Description Provider MultiUserWeight ReuseDelay PriceInfo CouponImage AuthorityURI UserID AuthoritySignature	
id	A	NM/ TM	1	ID of the 'Coupon' fragment. The value of this attribute SHALL be globally unique.	anyURI
version	A	NM/ TM	1	Version of this fragment. The newer version overrides the older one starting from the time specified by the 'validFrom' attribute, or as soon as it has been received if no 'validFrom' attribute is given.	unsignedInt
validFrom	A	NM/ TM	0..1	The first moment when this fragment is valid. If not given, the validity is assumed to have started at some time in the past. This field contains the 32bits integer part of an NTP time stamp.	unsignedInt
validTo	A	NM/ TM	0..1	The last moment when this fragment is valid. If not given, the validity is assumed to end in undefined time in the future. This field contains the 32bits integer part of an NTP time stamp.	unsignedInt
mustVerify	A	NM/ TM	0..1	Set to true if the coupon must be verified with the Authority listed in the AuthorityURI.	boolean
GlobalPurchaseItemID	E1	NM/ TM	0..N	The globalPurchaseItemID to which this coupon applies.	anyURI
GlobalPurchaseDataID	E1	NM/ TM	0..N	The globalPurchaseDataID to which this coupon applies. This element is included when there are several PurchaseDatas pointing to a PurchaseItem, e.g. to indicate a minimum subscription time period for this coupon to apply.	anyURI
GlobalPurchaseChannelID	E1	NM/ TM	0..N	The globalPurchaseChannelID of the PurchaseChannel fragment which this coupon document is associated with. This field is used to narrow the scope of this coupon to only those Purchase Channels that are specified here.	anyURI
Description	E1	NM/ TM	0..N	Description of the coupon, possibly in multiple languages. The language is expressed using built-	string

				in XML attribute 'xml:lang' with this element. The information is expected to indicate the valid start and end times of a given purchase offer (during which the user could make the corresponding purchase). This time interval is expected to be bounded within the period spanned by the attributes 'validFrom' and 'validTo'.	
Provider	E1	NM/ TM	1	Indicates the coupon provider type. Numeric values are: 0 - coupon is from a content originator (i.e. manufacturer or rights owner.) 1 - coupon is from the service provider (i.e. retailer or system operator.) 2-127 – reserved 128-255 – reserved for proprietary use	unsignedByte
MultiUseWeight	E1	NM/ TM	0..1	A weight (a number between 0.0 and 1.0) which indicates whether the coupon can be used together with another coupon. Two coupons from the same type of Provider cannot be combined. Two coupons whose weight sums to a value larger than 1.0 cannot be combined. If this field is absent it is presumed to be 1.0.	decimal
ReuseDelay	E1	NM/ TM	0..1	If the coupon is reusable, then this field contains the minimum delay (in seconds) before the coupon can be reused. If this field is absent the system remembers the couponID and authorityURI until the 'validTo' time and does not allow reuse.	unsignedInt
PriceInfo	E1	NM/ TM	1	Specifies the relative price information of the Coupon, typically as a negative number. Contains the following elements: SubscriptionType MonetaryPrice	
Subscription Type	E2	NM/ TM	1..N	The intended type of PurchaseItem referenced by this coupon. One subscriptionType in the Coupon must match the subscriptionType in the PurchaseData for the coupon to be used. See the subscriptionType attribute of the PurchaseItem fragment for numeric definitions. When multiple subscriptTypes are provided, the type in the PurchaseItem must match ONE type in subscriptType field.	unsignedByte
MonetaryPrice	E2	NM/ TM	0..N	Specifies the monetary discount of the price for the associated purchase, typically as a negative number. If the MonetaryPrice is zero then the item is free. Only one 'MonetaryPrice' per currency SHALL be defined. Contains the following attribute: currency	decimal

currency	A	NM/ TM	1	Specifies the monetary currency codes defined in ISO 4217 international currency codes.	string
CouponImage	E1	NM/ TM	1	URL that will display a printable image of this coupon.	anyURI
AuthorityURI	E1	NM/ TM	1	A URI describing the Authority that signed this coupon and that will redeem this coupon. The coupon redeemer SHALL issue an HTTP GET to this URI with the argument "&getCertficiate" to retrieve the X.509 certificate for coupon signing. Once retrieved, the X.509 certificate MAY be cached according to HTTP caching rules. The coupon redeemer SHALL HTTP POST to this URI with the argument "&getConsent" and place the contents of the coupon in the body of the message if consent is required before redeeming a coupon.	anyURI
UserID	E1	NM/ TM	0..1	If present, contains the user identity type and value known to the BSM for a user-specific coupon. This element is ONLY included for a user-specific (vs. general-use) coupon. Contains the following attributes: type	string
type	A	NM/ TM	1	Specifies the type of User ID. Allowed values are: 0 – username defined in [RFC 2865] 1 – IMSI 2 – URI 3 – IMPI 4 – MSISDN 5 – MIN 6-127 reserved for future use 128-255 reserved for proprietary use	unsignedByte
AuthoritySignature	E1	NM/ TM	1	An XML digital signature from the issuing authority which is presented to the issuing authority to authenticate the coupon. The signature is calculated according to the XML Signature methods as described in section 5.3.3. of [DRMDRM-v2.0]. The MAC is defined by the coupon issuing authority, over all of the previous attributes and elements. The signature algorithm is specified in the X.509 certificate.	base64binary

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-BCAST_Services-V1_1-20131029-A	29 Oct 2013	Status changed to Approved by TP TP Ref # OMA-TP-2013-0332-INP_BCAST_V1_1_ERP_for_final_Approval

Appendix B. Examples on Realizing Interactive Services (Informative)

Editor's note: this section may contain a walk-through for selected services that clarifies how the service can be generated, managed, and delivered, end-to-end.

B.1 Use of MMS Template for Service Interaction (Informative)

This section describes an example on how to use MMS Message Template for Service Interaction.

B.1.1 Retrieving the MMS Message Template

MMS Message Template can be broadcasted, as similar as other Service Interaction methods such as SMIL, XHTML MP etc.. In this case the files constructing MMS Message Template are concatenated in one GZIP and broadcasted within the file broadcast. The name and the MIME-type of each file are given in InteractivityMediaDocument (See Appendix.C for example).

MMS Message Template can also be retrieved from MMS. In this case the service provider or directly the operator author the MMS Template containing the MTD (MMS Message Template Definition), i.e. the template wizard toward the service. The template and some contents are embedded within a MMS Message with Multipart/Related or Multipart/Mixed format. The name and the MIME-type of each file are given in a header of the each part in Multipart Message. This MMS Message is send to the terminal whose users are registered to use Service Interaction.

The terminal will extract the files before the time when MMS Message Template is used in Service Interaction.

B.1.2 Launching MMS Message Template Client and creating Multimedia Message

After MMS Message Template retrieval, the terminal launches MMS Message Template Client with MMS Message Template. This section describes two cases for MMS Message Template use.

B.1.2.1 Use case: Voting

The first use case is Voting, for example, to vote 'who will win the game of the TV program'. In this case, MMS Message Template will have the following files:

- Message Template Definition (MTD) : using text-editor to input the name of the winner (shown below)

- MMS Presentation Part (SMIL)

- Media Objects (Text, Image)

Voting-sample.mtd

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE mmstemplate PUBLIC "-//OMA//DTD MTD 1.3//EN"
"http://www.openmobilealliance.org/MMS/MTD/1.3/DTD/mtd13.dtd">
<mmstemplate xmlns="http://www.openmobilealliance.org/2004/mtd">
   <head>
     <title>Vote the winner</title>
     <description>MTD sample code for BCAST Service Interaction</description>
     <date>2005-10-10</date>
     <version>1.00</version>
     <author>John Doe</author>
   </head>
   <body>
     <message>
        <to-header editable="false">1677721664</to-header>
        <subject-header>Vote the winner</subject-header>
     </message>
```

```
     <wizard>
        <step guide="Please input the name of the winner " app="text-input" target-name="name.txt"
target-type="text/plain" required="true"/>
     </wizard>
   </body>
</mmstemplate>
```

Table 88: MMS Template Example for Voting

MMS Message Template Client could display the following text input screen.

Note: MMS Message Template only specifies the input method. It does not specify the screen flow and how to construct text input screen. The appearance of the input screen will depend on the implementation of the client.

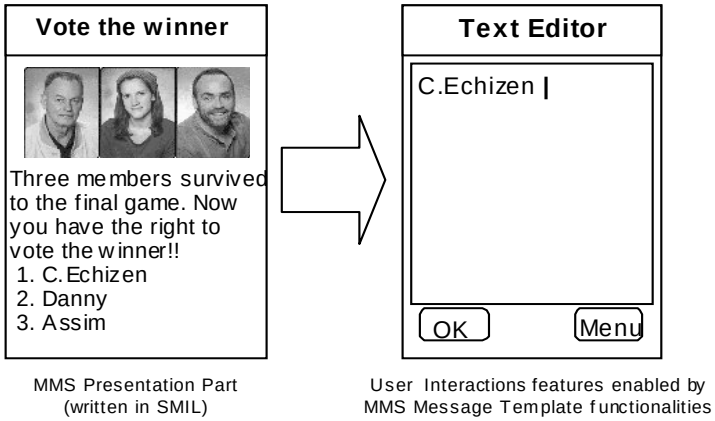


Figure 6: The screen flow of Voting Template

B.1.2.2 Use case: Viewer's Contribution

The second use case is Viewer's Contribution, for example, to send the viewer's pet boast to the TV program.

In this case, MMS Message Template will have the following files:

- Message Template Definition (MTD) :

  description that uses still camera to take a photo of the pet, and text editor to input the comment (shown below).

- MMS Presentation Part (SMIL)

- Media Objects (Text, Image)

Contribution-sample.mtd

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE mmstemplate PUBLIC "-//OMA//DTD MTD 1.3//EN"
"http://www.openmobilealliance.org/MMS/MTD/1.3/DTD/mtd13.dtd">
<mmstemplate xmlns="http://www.openmobilealliance.org/2004/mtd">
   <head>
     <title>Boast of my pet</title>
     <description>MTD sample code for BCAST Service Interaction</description>
     <date>2005-10-10</date>
     <version>1.00</version>
     <author>John Doe</author>
   </head>
   <body>
     <message>
```

```
        <to-header editable="false">1677721664</to-header>
        <subject-header>Show your pet off</subject-header>
     </message>
     <wizard>
        <step guide="Please take the picture of your pet" app="still-camera" target-name="photo.jpg"
target-type="image/jpg" required="true"/>
        <step guide="Please input your comment" app="text-input" target-name="comment.txt" target-
type="text/plain" required="true"/>
     </wizard>
   </body>
</mmstemplate>
```

Table 89: MMS Template Example for User Feedback

MMS Message Template Client will show the multiple input screens. The first screen will be the camera application and next one will be text editor. The example of input screens could be figured as follows:

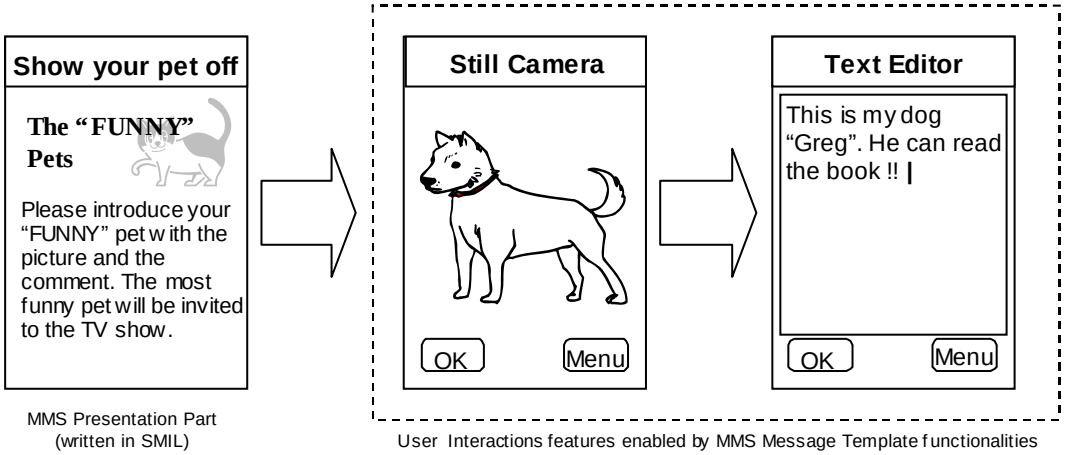


Figure 7: The screen flow of Viewer's Contribution Template

B.1.3 Sending the Interaction Message

The Resulting MM created by MMS Message Template Client will be sent to BCAST Service Application via MMS through SI-8.

Appendix C. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

Note 1: References refer to this specification unless otherwise noted.

Note 2: BCAST adaptation specifications, in which it is specified how the BCAST 1.0 enabler is implemented over a specific BDS (BCAST Distribution System), may overrule or adapt requirements from this SCR or provide additional requirements

C.1 SCR for BCAST Client

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-C-001	Terminal with access to interaction channel	general	O	BCAST-SERVICES-C-011 AND BCAST-SERVICES-C-012 AND BCAST-SERVICES-C-013 AND BCAST-SERVICES-C-017 AND BCAST-SERVICES-C-018 AND BCAST-SERVICES-C-019 AND BCAST-SERVICES-C-020 AND BCAST-SERVICES-C-025 AND BCAST-NT-C-003 AND BCAST-NT-C-005
BCAST-SERVICES-C-002	Terminal with access to interaction channel and support for Service and/or Content Protection	general, [BCAST11-ServContProt]	O	BCAST-SERVICES-C-006 AND BCAST-SERVICES-C-007 AND BCAST-SERVICES-C-008
BCAST-SERVICES-C-003	Terminal supporting SMS	general	O	BCAST-SERVICES-C-014
BCAST-SERVICES-C-004	Terminal supporting MMS	general	O	BCAST-SERVICES-C-015
BCAST-SERVICES-C-005	Terminal supporting Voice call	general	O	BCAST-SERVICES-C-016
BCAST-SERVICES-C-006	Service Provisioning	Section 5.1	O	
BCAST-SERVICES-C-007	HTTP POST for service provisioning	Section 5.1.1	O	
BCAST-SERVICES-C-008	Provisioning Messages	Section 5.1	O	BCAST-SERVICES-C-009
BCAST-SERVICES-C-009	GZIP compression of Provisioning Messages	Section 5.1.7	O	
BCAST-SERVICES-C-010	Web-based Service Provisioning	Section 5.1.8	O	
BCAST-SERVICES-C-011	Terminal Provisioning using OMA DM	Sections 5.2, 5.2.2	O	
BCAST-SERVICES-C-012	Reception of terminal provisioning messages and update of the parameters included in the terminal provisioning messages	Section 5.2	O	

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-C-013	Service interaction using IP, TCP, HTTP	Section 5.3.1	O	
BCAST-SERVICES-C-014	Service interaction using SMS	Sections 5.3.1, 5.3.6.1.2., 5.3.6.1.3	O	
BCAST-SERVICES-C-015	Service interaction using MMS	Sections 5.3.1., 5.3.6.1.2	O	
BCAST-SERVICES-C-016	Service interaction using Voice Call	Section 5.3.6.1.2	O	
BCAST-SERVICES-C-017	Interactive retrieval of SG	Section 5.3.2	O	
BCAST-SERVICES-C-018	Interactive retrieval of Service Guide related information	Section 5.3.3	O	
BCAST-SERVICES-C-019	Reception of InteractivityMedia documents over broadcast file distribution	Section 5.3.6.1, 5.3.6.2	O	
BCAST-SERVICES-C-020	Retrieval of InteractivityMedia documents and associated files over interaction channel	Section 5.3.6.1, 5.3.6.3	O	
BCAST-SERVICES-C-021	Rendering of InteractivityMedia objects	Section 5.3.6.1	M	
BCAST-SERVICES-C-022	Acquisition and rendering of the media objects attached to the InteractivityMedia document without interrupting the acquisition and rendering of the 'regular' broadcast media stream	Section 5.3.6.1.3	M	
BCAST-SERVICES-C-023	Description and evaluation of end user preferences	Section 5.4	O	BCAST-SERVICES-C-024
BCAST-SERVICES-C-024	Format of end user preference description	Section 5.4.2	O	
BCAST-SERVICES-C-025	Broadcast Roaming	Section 5.7	O	BCAST-SERVICES-C-026
BCAST-SERVICES-C-026	Format of roaming messages	Sections 5.7.1	O	
BCAST-SERVICES-C-027	Support of Location Information	Section 5.8	O	(BCAST-SERVICES-C-028 OR BCAST-SERVICES-C-029 OR BCAST-SERVICES-C-030) AND (BCAST-SERVICES-C-033 OR BCAST-SERVICES-C-034)
BCAST-SERVICES-C-028	Support of Location Information in OMA	Section 5.8	O	

Item	Function	Reference	Status	Requirement
	MLP format			
BCAST-SERVICES-C-029	Support of Location Information in zip code format	Section 5.8	O	
BCAST-SERVICES-C-030	Support of Location Information in BDS-specific cell_id format	Section 5.8	O	
BCAST-SERVICES-C-031	XML formatting rules for signalling	Section 5.9	M	
BCAST-SERVICES-C-032	3GPP Timed Text for Subtitling and Closed Captions	Section 5.13	O	
BCAST-SERVICES-C-033	Support of Parental Control for Service Ordering	Section 5.1.10	O	BCAST-SERVICES-C-006 AND (BCAST-SERVICES-C-055 OR BCAST-SERVICES-C-056)
BCAST-SERVICES-C-034	Support of Rich Media	Section 5.18	O	(BCAST-SERVICES-C-035 OR BCAST-SERVICES-C-036 OR BCAST-SERVICES-C-037 OR BCAST-SERVICES-C-038 OR BCAST-SERVICES-C-039) AND (BCAST-SERVICES-C-040 OR BCAST-SERVICES-C-041 OR BCAST-SERVICES-C-042 OR BCAST-SERVICES-C-043 OR BCAST-SERVICES-C-044 OR BCAST-SERVICES-C-045)
BCAST-SERVICES-C-035	Support of W3C SVG for BCAST Rich Media Solution	Section 5.18.3	O	
BCAST-SERVICES-C-036	Support of 3GPP DIMS for BCAST Rich Media Solution	Section 5.18.4	O	
BCAST-SERVICES-C-037	Support of OMA RME for BCAST Rich Media Solution	Section 5.18.5	O	
BCAST-SERVICES-C-038	Support of MPEG LASeR for BCAST Rich Media Solution	Section 5.18.6	O	
BCAST-SERVICES-C-039	Support of other BCAST Rich Media Solution identified by MIME Type	Section 5.18.7	O	
BCAST-SERVICES-C-040	Support of Rich Media "Service Guide presentation" usage	Section 5.18.1.1	O	BCAST-SG-C-020

Item	Function	Reference	Status	Requirement
	scenario			
BCAST-SERVICES-C-041	Support of Rich Media "Streaming" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-C-042	Support of Rich Media "File Delivery" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-C-043	Support of Rich Media "Notification" usage scenario	Section 5.18.1.1	O	BCAST-NT-C-006
BCAST-SERVICES-C-044	Support of Rich Media "IMD Interactivity" usage scenario	Section 5.18.1.1	O	BCAST-SERVICES-C-046
BCAST-SERVICES-C-045	Support of Rich Media "Preview Data" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-C-046	Service Interaction using InteractivityMediaDocuments	Section 5.3.6	O	BCAST-SERVICES-C-014 OR BCAST-SERVICES-C-015 OR BCAST-SERVICES-C-016 OR BCAST-SERVICES-C-019 OR BCAST-SERVICES-C-020 OR BCAST-SERVICES-C-021 OR BCAST-SERVICES-C-022
BCAST-SERVICES-C-047	Support of Smartcard Broadcast Provisioning	Section 5.19	O	BCAST-SERVICES-C-048 AND BCAST-SERVICES-C-049 AND BCAST-SERVICES-C-050
BCAST-SERVICES-C-048	Support the discovery of Smartcard Broadcast Provisioning support in the Smartcard	Section 5.19.2	O	
BCAST-SERVICES-C-049	Support the Smartcard Broadcast Provisioning services filtering	Section 5.19.3	O	
BCAST-SERVICES-C-050	Support ENVELOPE Command defined in [ETSI TS 102.221]	Section 5.19.3	O	
BCAST-SERVICES-C-051	Support [OMA SCWS11]	Section 5.19.3	O	
BCAST-SERVICES-C-052	Support for Related Contents Inquiry	Section 5.21	O	BCAST-SERVICES-C-053 AND BCAST-SERVICES-C-054 AND BCAST-SG-C-014
BCAST-SERVICES-C-053	Support for Related Contents Request messages via HTTP(S)	Section 5.1.5.8	O	
BCAST-SERVICES-C-054	Format of Related Contents Request	Section 5.1.5.8	O	

Item	Function	Reference	Status	Requirement
	messages			
BCAST-SERVICES-C-055	Support of generic solution for Parental Control for Service Ordering	Section 5.1.10	O	
BCAST-SERVICES-C-056	Support of Smartcard Profile extension for Parental Control for Service Ordering	Section 5.1.10.1	O	BCAST-SERVICES-C-057
BCAST-SERVICES-C-057	Support of AUTHENTICATE Command for OMA BCAST operation: Parental Control Service Provisioning Mode	Section 5.1.10.1	O	
BCAST-SERVICES-C-058	Support of Parental Control of Unicast Services	Section 5.17	O	BCAST-SERVICES-C-001
BCAST-SERVICES-C-059	Support of Broadcast Terminal Provisioning signalling	Section 5.2	O	
BCAST-SERVICES-C-060	Support of Pause & Resume of Subscription Period messages	Section 5.1.5.7	O	
BCAST-SERVICES-C-061	Support of User Defined Bundle related provisioning messages	Section 5.1.5.2.4 5.1.5.2.6	O	
BCAST-SERVICES-C-062	Reception of Coupon documents as a result of Service Provisioning Transaction.	Section 5.1.5.2, Sectio n5.1.5.5	O	
BCAST-SERVICES-C-063	Redemption of Coupon documents via Service Provisioning	Section 5.1.5.2, Section 5.1.5.5	O	
BCAST-SERVICES-C-064	Reception of Coupon documents over broadcast file distribution	Section 5.22	O	
BCAST-SERVICES-C-065	Retrieval of Coupon documents over interaction channel	Section 5.22	O	
BCAST-SERVICES-C-066	Support for simple TargetArea location filters	Section 5.8,	O	BCAST-SG-C-023
BCAST-SERVICES-C-067	Support for history-based LocationFilter location filters	Section 5.8	O	BCAST-SG-C-023

C.2 SCR for BCAST Service Application (BSA)

The BSA is an entity in the OMA BCAST Architecture, see [BCAST11-Architecture] Fig. 3.

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-BSA-001	Service interaction using one or several of: IP, TCP, HTTP, SMS, IPSEC, UDP, MMS, WAP, HTTPS based on SSL 3.0 [SSL30] and TLS 1.0 [RFC 2246], SIP/IMS	Section 5.3.1	O	
BCAST-SERVICES-BSA-002	Support for Interactivity MediaDocument format and delivery	Section 5.3.6.1.2	O	
BCAST-SERVICES-BSA-003	Support for Smartcard Broadcast provisioning messages format and delivery	Section 5.19	O	
BCAST-SERVICES-BSA-004	Support for Coupon Document format and delivery	Section 5.22	O	

C.3 SCR for BCAST Service Distribution/Adaptation (BSDA)

The BSDA is an entity in the OMA BCAST Architecture, see [BCAST11-Architecture] Fig. 3.

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-BSDA-001	Description and evaluation of end user preferences	Section 5.4	O	BCAST-SERVICES-BSDA-002
BCAST-SERVICES-BSDA-002	Format of end user preference description	Section 5.4.1	O	
BCAST-SERVICES-BSDA-003	Use of Location Information	Section 5.8	O	BCAST-SERVICES-BSDA-004 OR BCAST-SERVICES-BSDA-005 OR BCAST-SERVICES-BSDA-006
BCAST-SERVICES-BSDA-004	Use of Location Information in OMA MLP format	Section 5.8	O	
BCAST-SERVICES-BSDA-005	Use of Location Information in zip code format	Section 5.8	O	
BCAST-SERVICES-BSDA-006	Use of Location Information in BDS-specific cell_id format	Section 5.8	O	
BCAST-SERVICES-BSDA-007	XML formatting rules for signalling	Section 5.9	M	
BCAST-SERVICES-BSDA-008	Subtitling and Closed Captions	Section 5.13	O	
BCAST-SERVICES-BSDA-009	Support of Rich Media	Section 5.18	O	(BCAST-SERVICES-BSDA-010 OR BCAST-SERVICES-BSDA-011 OR BCAST-SERVICES-BSDA-012 OR BCAST-SERVICES-BSDA-013 OR BCAST-SERVICES-BSDA-014) AND (BCAST-SERVICES-BSDA-015

Item	Function	Reference	Status	Requirement
				OR BCAST-SERVICES-BSDA-016 OR BCAST-SERVICES-BSDA-017 OR BCAST-SERVICES-BSDA-018 OR BCAST-SERVICES-BSDA-019 OR BCAST-SERVICES-BSDA-020)
BCAST-SERVICES-BSDA-010	Support of W3C SVG for BCAST Rich Media Solution	Section 5.18.3	O	
BCAST-SERVICES-BSDA-011	Support of 3GPP DIMS for BCAST Rich Media Solution	Section 5.18.4	O	
BCAST-SERVICES-BSDA-012	Support of OMA RME for BCAST Rich Media Solution	Section 5.18.5	O	
BCAST-SERVICES-BSDA-013	Support of MPEG LASeR for BCAST Rich Media Solution	Section 5.18.6	O	
BCAST-SERVICES-BSDA-014	Support of other BCAST Rich Media Solution identified by MIME Type	Section 5.18.7	O	
BCAST-SERVICES-BSDA-015	Support of Rich Media "Service Guide presentation" usage scenario	Section 5.18.1.1	O	BCAST-SGGAD-S-027
BCAST-SERVICES-BSDA-016	Support of Rich Media "Streaming" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSDA-017	Support of Rich Media "File Delivery" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSDA-018	Support of Rich Media "Notification" usage scenario	Section 5.18.1.1	O	BCAST-NT-DA-014
BCAST-SERVICES-BSDA-019	Support of Rich Media "IMD Interactivity" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSDA-020	Support of Rich Media "Preview Data" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSDA-021	Support of Broadcast Terminal Provisioning signalling	Section 5.2	O	
BCAST-SERVICES-BSDA-022	Support of Parental Control of Unicast Services	Section 5.17	O	
BCAST-SERVICES-BSM-023	Support for Provisioning using Coupon documents	Section 5.22	O	
BCAST-SERVICES-BSDA-024	Generation of simple TargetArea location filters	Section 5.8	O	

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-BSDA-025	Generation of history-based LocationFilter location filters	Section 5.8	O	

C.4 SCR for BCAST Subscription Management (BSM)

The BSM is an entity in the OMA BCAST Architecture, see [BCAST11-Architecture] Fig. 3.

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-BSM-001	Service Provisioning	Section 5.1	M	
BCAST-SERVICES-BSM-002	HTTP POST for service provisioning	Section 5.1.1	M	
BCAST-SERVICES-BSM-003	GZIP compression of Provisioning Messages	Section 5.1.7	M	
BCAST-SERVICES-BSM-004	Web-based Service Provisioning	Section 5.1.8	O	
BCAST-SERVICES-BSM-005	Terminal Provisioning using OMA DM	Section 5.2	M	
BCAST-SERVICES-BSM-006	Delivery of OMA DM messages through Interaction Channel using DM mechanism	Section 5.2.4	M	
BCAST-SERVICES-BSM-007	Broadcast Roaming	Section 5.7	O	BCAST-SERVICES-BSM-008
BCAST-SERVICES-BSM-008	Format of roaming messages	Sections 5.7.1, 5.7.2	O	
BCAST-SERVICES-BSM-009	XML formatting rules for signalling	Section 5.9	M	
BCAST-SERVICES-BSM-010	Protocol stack for message exchanges between BSMs	Section 7.2.1	M	
BCAST-SERVICES-BSM-011	Support of Parental Control for Service Ordering	Section 5.1.10	O	BCAST-SERVICES-BSM-001 AND (BCAST-SERVICES-BSM-028 OR BCAST-SERVICES-BSM-029)
BCAST-SERVICES-BSM-012	Support of Rich Media	Section 5.18	O	BCAST-SERVICES-BSM-013 OR BCAST-SERVICES-BSM-014 OR BCAST-SERVICES-BSM-015 OR BCAST-SERVICES-BSM-016 OR BCAST-SERVICES-BSM-017) AND (BCAST-SERVICES-BSM-018 OR BCAST-SERVICES-BSM-019 OR BCAST-SERVICES-BSM-020 OR BCAST-SERVICES-BSM-021 OR BCAST-SERVICES-BSM-022 OR BCAST-SERVICES-BSM-023)
BCAST-SERVICES-BSM-013	Support of W3C SVG for BCAST Rich Media Solution	Section 5.18.3	O	
BCAST-SERVICES-BSM-014	Support of 3GPP DIMS for BCAST Rich Media Solution	Section 5.18.4	O	

Item	Function	Reference	Status	Requirement
BCAST-SERVICES-BSM-015	Support of OMA RME for BCAST Rich Media Solution	Section 5.18.5	O	
BCAST-SERVICES-BSM-016	Support of MPEG LASeR for BCAST Rich Media Solution	Section 5.18.6	O	
BCAST-SERVICES-BSM-017	Support of other BCAST Rich Media Solution identified by MIME Type	Section 5.18.7	O	
BCAST-SERVICES-BSM-018	Support of Rich Media "Service Guide presentation" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSM-019	Support of Rich Media "Streaming" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSM-020	Support of Rich Media "File Delivery" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSM-021	Support of Rich Media "Notification" usage scenario	Section 5.18.1.1	O	BCAST-SERVICES-BSM-024
BCAST-SERVICES-BSM-022	Support of Rich Media "IMD Interactivity" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSM-023	Support of Rich Media "Preview Data" usage scenario	Section 5.18.1.1	O	
BCAST-SERVICES-BSM-024	Notification Generation (NTG)	Section 5.14	O	
BCAST-SERVICES-BSM-025	Support of Smartcard Broadcast Provisioning service	Section 5.19	O	
BCAST-SERVICES-BSM-026	Support of Related Contents Inquiry	Section 5.21	O	BCAST-SERVICES-BSM-027
BCAST-SERVICES-BSM-027	Format of Related Contents Request messages	Section 5.1.5.8	O	
BCAST-SERVICES-BSM-028	Support of generic solution for Parental Control for Service Ordering	Section 5.1.10	O	
BCAST-SERVICES-BSM-029	Support of Smartcard Profile extension for Parental Control for Service Ordering	Section 5.1.10.1	O	
BCAST-SERVICES-BSM-030	Support of Parental Control of Unicast Services	Section 5.17	O	
BCAST-SERVICES-BSM-031	Support of Broadcast Terminal Provisioning	Section 5.2	O	

Item	Function	Reference	Status	Requirement
	signalling			
BCAST-SERVICES-BSM-032	Support of Pause & Resume of Subscription Period messages	Section 5.1.5.7	O	
BCAST-SERVICES-BSM-033	Support of User Defined Bundle related provisioning messages	Section 5.1.5.2.5 5.1.5.2.7	O	

C.5 SCR for BCAST Notification Client (NTC)

Item	Function	Reference	Status	Requirement
BCAST-NT-C-001	Support for the signalling of the availability and access to generic notifications through the SGDD.	Sections 5.14.1.1.1, [BCAST11-SG] 5.4.2.5	O	
BCAST-NT-C-002	Support for the signalling of the availability and access to service-specific notifications through 'Access' fragment.	Sections 5.14.1.2.1, [BCAST11-SG] 5.1.2.4	O	
BCAST-NT-C-003	Support for subscribing to notifications by sending a Notification Request to NTG	Section 5.14.4.2.1	O	
BCAST-NT-C-004	Support for user-oriented notification request message format	Section 5.14.4.2.1	O	BCAST-NT-C-003
BCAST-NT-C-005	Support for polling to notifications over Interaction Channel	Section 5.14.4.3	O	
BCAST-NT-C-006	BCAST Notification Client (NTC)	Section 5.14	O	BCAST-NT-C-001 OR BCAST-NT-C-002 OR BCAST-NT-C-004 OR BCAST-NT-C-005
BCAST-NT-C-007	Support of Broadcast Terminal Provisioning signalling	Section 5.2, 5.14	O	

C.6 SCR for BCAST Notification Distribution Adaptation (NTDA)

Item	Function	Reference	Status	Requirement
BCAST-NT-DA-001	Support for the signalling of the availability and access to generic notifications through the SGDD.	Sections 5.14.1.1.1, [BCAST11-SG] 5.4.2.5	O	
BCAST-NT-DA-002	Support for the signalling of the availability and access to service-specific notifications through the	Sections 5.14.1.2.1, [BCAST11-SG] 5.1.2.4	O	

Item	Function	Reference	Status	Requirement
	'Access' fragment.			
BCAST-NT-DA-003	Notification back-end interface exposed	Section 5.14.5.1	O	BCAST-NT-DA-004 AND BCAST-NT-DA-005
BCAST-NT-DA-004	Support back-end interface for notification function	Section 5.14.5.1	O	
BCAST-NT-DA-005	Support the back-end message for notification	Section 5.14.5.2	O	
BCAST-NT-DA-006	Backend interface SG-4 exposed in implementation	Section 5.14.5.1	O	BCAST-NT-DA-007
BCAST-NT-DA-007	Support backend interface SG-4 for SG function	Section 5.14.5.1	O	(BCAST-NT-DA-008 OR BCAST-NT-DA-009) AND BCAST-NT-DA-010 AND (BCAST-NT-DA-011 OR BCAST-NT-DA-012) AND BCAST-NT-DA-013 AND BCAST-NT-DA-005
BCAST-NT-DA-008	Support IPv4	Section 5.14.5.1	O	
BCAST-NT-DA-009	Support IPv6	Section 5.14.5.1	O	
BCAST-NT-DA-010	Support TCP	Section 5.14.5.1	O	
BCAST-NT-DA-011	Support HTTP1.1	Section 5.14.5.1	O	
BCAST-NT-DA-012	Support HTTPS	Section 5.14.5.1	O	
BCAST-NT-DA-013	SG backend messages for content delivery	Section 5.14.5.1	O	
BCAST-NT-DA-014	BCAST Notification Distribution Adaptation	Section 5.14	O	BCAST-NT-DA-001 OR BCAST-NT-DA-002 OR BCAST-NT-DA-003 OR BCAST-NT-DA-006
BCAST-NT-DA-0015	Support of Broadcast Terminal Provisioning signalling	Section 5.2, 5.14	O	

C.7 SCR for BCAST Audience Measurement Client in Terminal (BCAST AM-C)

Item	Function	Reference	Status	Requirement
BCAST-AM-C-001	Support for Terminal-Centric Audience Measurement	Section 5.20.1	O	[BCAST-AM-C-002 OR (BCAST-AM-C-002 AND BCAST-AM-C-003) OR (BCAST-AM-C-005 AND BCAST-AM-C-002 AND BCAST-AM-C-003) OR (BCAST-AM-C-005 AND BCAST-AM-C-002)] AND BCAST-AM-C-034

BCAST-AM-C-002	Support for Terminal-Centric Audience Measurement via HTTP(S)	Section 5.20.1	O	BCAST-AM-C-007 AND BCAST-AM-C-013 AND BCAST-AM-C-015 AND BCAST-AM-C-021 AND BCAST-AM-C-023 AND BCAST-AM-C-025
BCAST-AM-C-003	Support for Terminal-Centric Audience Measurement via SMS	Section 5.20.1	O	BCAST-AM-C-004
BCAST-AM-C-004	Audience Measurement SMS Trigger	Section 5.20.1.1.7	O	BCAST-AM-C-008 AND BCAST-AM-C-026 AND BCAST-AM-C-033
BCAST-AM-C-005	Support signalling of Audience Measurement function in SG	Section 5.4.1.5.2 in [BCAST11-SG]	O	BCAST-AM-C-006
BCAST-AM-C-006	Audience Measurement Trigger (AM Trigger) message over SG	Section 5.20.1.1.2, 5.20.1.2.1, [BCAST11-SG]	O	BCAST-AM-C-010 AND BCAST-AM-C-012
BCAST-AM-C-007	AM Trigger message over HTTP(S)	Section 5.20.1.1.2, 5.20.1.2.1	O	BCAST-AM-C-009
BCAST-AM-C-008	AM Trigger message over SMS	Section 5.20.1.1.7	O	BCAST-AM-C-009
BCAST-AM-C-009	AM Trigger message format	Section 5.20.1.2.1	O	BCAST-AM-C-010 AND BCAST-AM-C-012
BCAST-AM-C-010	ServerAddressURL authentication	Section 5.20.1.1.2, 5.20.1.2.1	O	
BCAST-AM-C-011	Silent Opt-In	Section 5.20.1.1.2, 5.20.1.2.1	O	
BCAST-AM-C-012	Non-silent Opt-In, user consent asked explicitly	Section 5.20.1.1.2, 5.20.1.2.1	O	
BCAST-AM-C-013	Audience Measurement Request (AM Request) message over HTTP(S)	Section 5.20.1.1.2	O	BCAST-AM-C-014
BCAST-AM-C-014	AM Request message format	Section 5.20.1.2.2	O	BCAST-AM-C-016
BCAST-AM-C-015	Audience Measurement Response (AM Response) message over HTTP(S)	Section 5.20.1.1.2, 5.20.1.1.3, 5.20.1.2.3	O	BCAST-AM-C-018
BCAST-AM-C-016	AM Response message responding the AM Request	Section 5.20.1.1.2, 5.20.1.1.3, 5.20.1.2.3	O	BCAST-AM-C-018
BCAST-AM-C-017	AM Response message	Section	O	BCAST-AM-C-018

	pushed (not responding to an AM Request message)	5.20.1.1.3, 5.20.1.2.3		
BCAST-AM-C-018	AM Response message format	Section 5.20.1.2.3	O	BCAST-AM-C-019
BCAST-AM-C-019	Audience Measurement Configuration Data	Section 5.20.1.2.7, 5.20.1.2.3	O	BCAST-AM-C-020
BCAST-AM-C-020	Event measurement	Section 5.20.1.1.4	O	
BCAST-AM-C-021	Audience Measurement Report Delivery (AMRD) message over HTTP(S)	Section 5.20.1.1.5, 5.20.1.2.4	O	BCAST-AM-C-022 AND BCAST-AM-C-023
BCAST-AM-C-022	AMRD message format	Section 5.20.1.2.4	O	
BCAST-AM-C-023	Audience Measurement Report Response (AMRR) message over HTTP(S)	Section 5.20.1.1.5, 5.20.1.2.5	O	BCAST-AM-C-024
BCAST-AM-C-024	AMRR message format	Section 5.20.1.2.5	O	
BCAST-AM-C-025	Audience Measurement Report Trigger (AMRT) message over HTTP(S)	Section 5.20.1.1.5, 5.20.1.2.6	O	BCAST-AM-C-027
BCAST-AM-C-026	AMRT message over SMS	Section 5.20.1.1.5, 5.20.1.1.7, 5.20.1.2.6	O	BCAST-AM-C-027
BCAST-AM-C-027	AMRT message format	Section 5.20.1.2.6	O	
BCAST-AM-C-028	Support for Smartcard-centric Audience measurement	Sections 5.20.2	O	BCAST-AM-C-029 AND (BCAST-AM-C-030 OR BCAST-AM-C-031) AND BCAST-AM-C-035 AND BCAST-AM-C-036
BCAST-AM-C-029	Support of DISPLAY TEXT and GET INPUT SIMtookit commands	Sections 5.20.2.1.2	O	
BCAST-AM-C-030	Support of SMS-PP protocol	Sections 5.20.2.2.2	O	
BCAST-AM-C-031	Support of BIP protocol	Sections 5.20.2.2.3	O	
BCAST-AM-C-032	Support of Smartcard Broadcast provisioning protocol	Sections 5.20.2.2.4	O	
BCAST-AM-C-033	Support CampaignInfo in SG	Section 5.4.1.5.2 in [BCAST11-SG]	O	
BCAST-AM-C-034	Allowing/Disallowing measurements of	Section 5.20.1	O	

	particular service or content items			
BCAST-AM-C-035	Support of Event Signalling Modes of the BCAST command (Time Consumption and AMallowed/AMDisallowed	Section of [BCAST11-ServContProt]	O	
BCAST-AM-C-036	Support of STKM for Clear to air Services with NULL encryption	Section 5.20.2.1.8	O	

C.8 SCR for BCAST Audience Measurement Client in Smartcard (BCAST AM-C)

Item	Function	Reference	Status	Requirement
BCAST-AM-SC-001	Support of Audience measurement in Smartcard	Sections 5.20.2	O	(BCAST-SCSPCP-C-005 OR BCAST-SCSPCP-C-007) AND BCAST-AM-SC-005 AND BCAST-AM-SC-008 AND BCAST-AM-SC-009 AND BCAST-AM-SC-0010 AND BCAST-AM-SC-011 AND BCAST-AM-SC-023 AND BCAST-AM-SC-024 AND BCAST-AM-SC-025
BCAST-AM-SC-002	Support of Registration Process for AM	Sections 5.20.2.1.1	O	BCAST-AM-SC-001 AND BCAST-AM-SC-003 AND BCAST-AM-SC-004
BCAST-AM-SC-003	Support of REGISTRATION-REQUEST	Sections 5.20.2.1.1	O	BCAST-AM-SC-018
BCAST-AM-SC-004	Support of REGISTRATION-RESPONSE Message	Sections 5.20.2.1.1	O	BCAST-AM-SC-018
BCAST-AM-SC-005	Support of OPT_IN message	Sections 5.20.2.1.2	O	
BCAST-AM-SC-006	Support of OPT_IN_INVITATION_TRIGGER message	Sections 5.20.2.1.2	O	BCAST-AM-SC-007
BCAST-AM-SC-007	Support of OPT_IN_STATE_NOTIFICATION message	Sections 5.20.2.1.2	O	
BCAST-AM-SC-008	Support of Configuration process	Sections 5.20.2.1.3	O	BCAST-AM-SC-012
BCAST-AM-SC-009	Support of Activation process	Sections 5.20.2.1.4	O	BCAST-AM-SC-013
BCAST-AM-SC-0010	Support of Metering Process	Sections 5.20.2.1.5	O	
BCAST-AM-SC-011	Support of Reporting Process	Sections 5.20.2.1.6	O	BCAST-AM-SC-014 AND BCAST-AM-SC-015 AND BCAST-AM-SC-016 AND BCAST-AM-SC-017
BCAST-AM-SC-012	Support of CONFIGURATION	Sections 5.20.2.1.3	O	BCAST-AM-SC-018 OR BCAST-AM-SC-019 OR BCAST-AM-SC-

Item	Function	Reference	Status	Requirement
	message			020
BCAST-AM-SC-013	Support of ACTIVATION message	Sections 5.20.2.1.4	O	BCAST-AM-SC-018 OR BCAST-AM-SC-019 OR BCAST-AM-SC-020
BCAST-AM-SC-014	Support of REPORTING message	Sections 5.20.2.1.6	O	BCAST-AM-SC-018 OR BCAST-AM-SC-019
BCAST-AM-SC-015	Support of REPORTING_RESPONSE message	Sections 5.20.2.1.6	O	BCAST-AM-SC-018 OR BCAST-AM-SC-019
BCAST-AM-SC-016	Support of REPORTING_REQUEST message	Sections 5.20.2.1.6	O	BCAST-AM-SC-018 OR BCAST-AM-SC-019 OR BCAST-AM-SC-020
BCAST-AM-SC-017	Reporting based on internal event	Sections 5.20.2.1.6	O	BCAST-AM-SC-014
BCAST-AM-SC-018	Support of SMS-PP protocol	Sections 5.20.2.2.2	O	
BCAST-AM-SC-019	Support of HTTP protocol	Sections 5.20.2.2.3	O	
BCAST-AM-SC-020	Support of Smartcard Broadcast provisioning protocol	Sections 5.20.2.2.4	O	
BCAST-AM-SC-021	Support of Security at transport level	Sections 5.20.2.2.1	O	
BCAST-AM-SC-022	Support of Security at application level	Sections 5.20.2.2.1	O	
BCAST-AM-SC-023	Support of AM Control using Access criteria in STKM	Section 5.20.2	O	
BCAST-AM-SC-024	Support of AM Control using Event Signalling command for clear to air services	Section 5.20.2	O	
BCAST-AM-SC-025	Support of Event Signalling command for Time consumption	Section 5.20.2	O	

C.9 SCR for BCAST Audience Measurement Management (AM-M)

Item	Function	Reference	Status	Requirement
BCAST-AM-M-001	Support for Terminal-Centric Audience Measurement	Section 5.20.1	O	[(BCAST-AM-M-002 OR (BCAST-AM-M-002 AND BCAST-AM-M-003)) OR (BCAST-AM-M-002 AND BCAST-AM-M-003 AND BCAST-AM-M-005) OR (BCAST-AM-M-002 AND BCAST-AM-M-005)] AND BCAST-AM-M-042
BCAST-AM-M-002	Support for Terminal-Centric Audience Measurement via	Section 5.20.1	O	BCAST-AM-M-007 AND BCAST-AM-M-010 AND BCAST-AM-M-012 AND

Item	Function	Reference	Status	Requirement
	HTTP(S)			BCAST-AM-M-017 AND BCAST-AM-M-019 AND BCAST-AM-M-021
BCAST-AM-M-003	Support for Terminal-Centric Audience Measurement via SMS	Section 5.20.1	O	BCAST-AM-M-004
BCAST-AM-M-004	Audience Measurement SMS Trigger	Section 5.20.1.1.7	O	BCAST-AM-M-008 AND BCAST-AM-M-022 AND BCAST-AM-M-039
BCAST-AM-M-005	Support signalling of Audience Measurement function in SG	Section 5.4.1.5.2 in [BCAST11-SG]	O	BCAST-AM-M-006
BCAST-AM-M-006	Audience Measurement Trigger (AM Trigger) message over SG	Section 5.20.1.1.2, 5.20.1.2.1, [BCAST11-SG]	O	
BCAST-AM-M-007	AM Trigger message over HTTP(S)	Section 5.20.1.1.2, 5.20.1.2.1	O	BCAST-AM-M-009
BCAST-AM-M-008	AM Trigger message over SMS	Section 5.20.1.1.7	O	BCAST-AM-M-009
BCAST-AM-M-009	AM Trigger message format	Section 5.20.1.2.1	O	
BCAST-AM-M-010	Audience Measurement Request (AM Request) message over HTTP(S)	Section 5.20.1.1.2 5.20.1.2.2	O	BCAST-AM-M-011
BCAST-AM-M-011	AM Request message format	Section 5.20.1.1.2 5.20.1.2.2	O	BCAST-AM-M-013
BCAST-AM-M-012	Audience Measurement Response (AM Response) message over HTTP(S)	Section 5.20.1.1.2 5.20.1.1.3 5.20.1.2.3	O	BCAST-AM-M-015
BCAST-AM-M-013	AM Response message responding the AM Request	Section 5.20.1.1.2 5.20.1.1.3 5.20.1.2.3	O	BCAST-AM-M-015
BCAST-AM-M-014	AM Response message pushed (not responding to an AM Request message)	Section 5.20.1.1.3 5.20.1.2.3	O	BCAST-AM-M-015
BCAST-AM-M-015	AM Response message format	Section 5.20.1.2.3	O	BCAST-AM-M-016
BCAST-AM-M-016	Audience Measurement Configuration Data	Section 5.20.1.2.7, 5.20.1.2.3	O	
BCAST-AM-M-017	Audience Measurement Report Delivery	Section 5.20.1.1.5	O	BCAST-AM-M-018 AND BCAST-AM-M-019

Item	Function	Reference	Status	Requirement
	(AMRD) message over HTTP(S)	5.20.1.2.4		
BCAST-AM-M-018	AMRD message format	Section 5.20.1.2.4	O	BCAST-AM-M-020
BCAST-AM-M-019	Audience Measurement Report Response (AMRR) message over HTTP(S)	Section 5.20.1.1.5 5.20.1.2.5	O	BCAST-AM-M-020
BCAST-AM-M-020	AMRR message format	Section 5.20.1.2.5	O	
BCAST-AM-M-021	Audience Measurement Report Trigger (AMRT) message over HTTP(S)	Section 5.20.1.1.5 5.20.1.2.6	O	BCAST-AM-M-023
BCAST-AM-M-022	AMRT message over SMS	Section 5.20.1.1.5 5.20.1.1.7 5.20.1.2.6	O	BCAST-AM-M-023
BCAST-AM-M-023	AMRT message format	Section 5.20.1.2.6	O	
BCAST-AM-M-024	Support of Audience measurement in Smartcard	Sections 5.20.2	O	BCAST-AM-M-028 AND BCAST-AM-M-031 AND BCAST-AM-M-032 AND BCAST-AM-M-033 AND BCAST-AM-M-034 AND BCAST-AM-M-035 AND (BCAST-AM-M-043 OR BCAST-AM-M-044) AND BCAST-AM-M-045
BCAST-AM-M-025	Support of Registration Process for AM	Sections 5.20.2.1.1	O	BCAST-AM-M-024 AND BCAST-AM-M-026 AND BCAST-AM-M-027
BCAST-AM-M-026	Support of REGISTRATION-REQUEST	Sections 5.20.2.1.1	O	BCAST-AM-M-036
BCAST-AM-M-027	Support of REGISTRATION-RESPONSE Message	Sections 5.20.2.1.1	O	BCAST-AM-M-036
BCAST-AM-M-028	Support of OPT_IN message	Sections 5.20.2.1.2	O	
BCAST-AM-M-029	Support of OPT_IN_INVITATION _TRIGGER message	Sections 5.20.2.1.2	O	BCAST-AM-M-030
BCAST-AM-M-030	Support of OPT_IN_STATE_NOTIFICATION message	Sections 5.20.2.1.2	O	
BCAST-AM-M-031	Support of CONFIGURATION message	Sections 5.20.2.1.3	O	BCAST-AM-M-036 OR BCAST-AM-M-037 OR BCAST-AM-M-038
BCAST-AM-M-032	Support of ACTIVATION message	Sections 5.20.2.1.4	O	BCAST-AM-M-036 OR BCAST-AM-M-037 OR BCAST-AM-M-038
BCAST-AM-M-033	Support of REPORTING message	Sections 5.20.2.1.6	O	BCAST-AM-M-036 OR BCAST-AM-M-037

Item	Function	Reference	Status	Requirement
BCAST-AM-M-034	Support of REPORTING_RESPONSE message	Sections 5.20.2.1.6	O	BCAST-AM-M-036 OR BCAST-AM-M-037
BCAST-AM-M-035	Support of REPORTING_REQUEST message	Sections 5.20.2.1.6	O	BCAST-AM-M-036 OR BCAST-AM-M-037 OR BCAST-AM-M-038
BCAST-AM-M-036	Support of SMS-PP protocol	Sections 5.20.2.2	O	
BCAST-AM-M-037	Support of HTTP protocol	Sections 5.20.2.2	O	
BCAST-AM-M-038	Support of Smartcard Broadcast provisioning protocol	Sections 5.20.2.2	O	
BCAST-AM-M-039	Support CampaignInfo in SG	Section 5.4.1.5.2 in [BCAST11-SG]	O	
BCAST-AM-M-040	Support of Smartcard-centric Security at transport level	Sections 5.20.2.2	O	
BCAST-AM-M-041	Support of Smartcard-centric Security at application level	Sections 5.20.2.2	O	
BCAST-AM-M-042	Allowing/Disallowing measurements of particular service or content items	Section 5.20.1	O	
BCAST-AM-M-043	Support of AM Control using signalling in Service Guide (clear to air services).	Section 5.20.2	O	
BCAST-AM-M-044	Support of AM Control using Access criteria in STKM (clear-to-air services)	Section 5.20.2	O	BCAST-AM-M-046
BCAST-AM-M-045	Support of AM Control using Access criteria in STKM (encrypted services)	Section 5.20.2	O	
BCAST-AM-M-046	Support of Smartcard Centric AM for clear to air services using STKM with NULL encryption.	Section 5.20.2	O	

Appendix D. <MediaObjectSet> examples (Informative)

This appendix provides illustrative examples of <MediaObjectSet> elements present in InteractivityMedia documents. The external file (GZIP archive or single media file part) is not given.

D.1 XHTML MP bundle

Example of an XHTML MP bundle containing two XHTML pages, one picture and one external WAP CSS stylesheet:

```
<MediaObjectSet
     RelativePreference="5"
     Content-Type="application/x-gzip"
     Content-Location="http://www.bcast.com/purchaseme.gz"
     xml:lang="en-GB"
 >
     <Object
         Content-Type="application/vnd.wap.xhtml+xml"
         Content-Location="index.html"
         Start="true" />
     <Object
         Content-Type="application/vnd.wap.xhtml+xml"
         Content-Location="other.html" />
     <Object
         Content-Type="text/css"
         Content-Location="./style/style.css" />
     <Object
         Content-Type="image/gif"
         Content-Location="./images/background.gif" />
     <Description>Purchase me</Description>
</MediaObjectSet>
```

File structure after deflation would be :

index.html

other.html

/style/style.css

/images/background.gif

with ‘index.html’ typically containing the following links :

<link rel= "stylesheet" href= "./style/style.css" />

 Click to see next page

D.2 MMS Message Template bundle

Example of an MMS Message Template bundle containing one MMS Template Definition, one SMIL and one text part and one picture:

```
<MediaObjectSet
     RelativePreference="10"
     Content-Type="application/x-gzip"
```

```
    Content-Location="http://www.bcast.com/votenow.gz"
>
    <Object
        Content-Type="application/vnd.omammsg-mtd+xml"
        Content-Location="votenow.mtd" />
        Start="true" />
    <Object
        Content-Type="application/smil"
        Content-Location="presentation.smil" />
    <Object
        Content-Type="image/png"
        Content-Location="title.png" />
    <Object
        Content-Type="text/plain"
        Content-Location="vote.txt" />
</MediaObjectSet>
```

File structure after deflation would be :

votenow.mtd

presentation.smil

title.png

vote.txt

with ‘presentation.smil’ typically containing the following links :

<text src = "vote.txt" />

D.3 SMIL bundle

Example of a SMIL bundle containing one XHTML MP Rich Text and one Audio file :

```
<MediaObjectSet
    RelativePreference="8"
    Content-Type="application/x-gzip"
    Content-Location="http://www.bcast.com/inputtimeout.gz"
>
    <Object
        Content-Type="application/smil"
        Content-Location="presentation.smil"
        Start="true" />
    <Object
        Content-Type="application/vnd.wap.xhtml+xml"
        Content-Location="farewell.html" />
    <Object
        Content-Type="audio/3gpp"
        Content-Location="./audio/symphony.3gp" />
</MediaObjectSet>
```

File structure after deflation would be :

presentation.smil

farewell.html

/audio/symphony.3gp

with ‘presentation.smil’ typically containing the following links :

<text src= "farewell.html" type="application/vnd.wap.xhtml+xml" />

<audio src= "./audio/symphony.3gp" type="audio/3gpp" />

Appendix E. Walk-through of Broadcast Roaming (Informative)

This appendix illustrates how the Broadcast Roaming is achieved through the use of core functionalities of BCAST 1.0. This informative explanation of Broadcast Roaming is presented as a walk-through mainly from the terminal point of view.

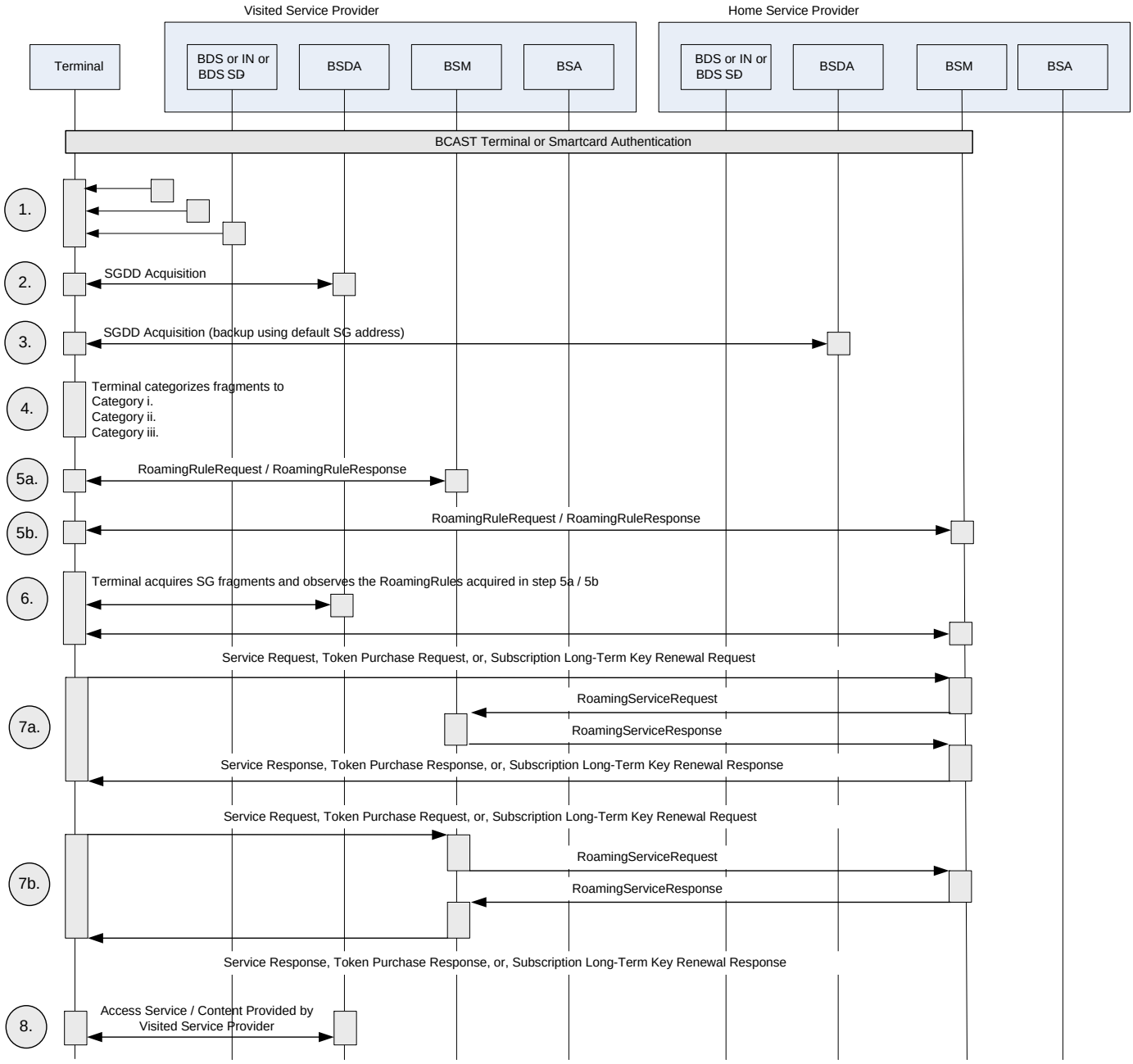


Figure 8: Walk-through of Broadcast Roaming.

The walk-through below is illustrated as flow chart in Figure 6.

1. Terminal scans or otherwise detects available BCAST Distribution Systems (BDS). If the terminal has a list of Management Objects that determine the preferred Visited Mobile Broadcast Service Provider it will attempt to attach to the network(s) of the Visited Mobile Broadcast Service Provider with the highest priority.

2. Terminal attempts to perform Service Guide discovery bootstrap to locate entry point to BCAST Service Guide on all or any of the detected BDSes. Upon successful completion of bootstrap procedure, the Terminal acquires the entry point to BCAST Service Guide over the respective bearer. Consequently, the Terminal acquires SGDDs either by receiving or by retrieving those.
3. In case Terminal fails to perform bootstrap and to locate the entry point to BCAST Service Guide over all the detected BDSes, the Terminal attempts to retrieve SGDDs using the entry point as provisioned in the Terminal (defined by Management Object "<X>/SGServerAddress").
4. Once the Terminal acquires SGDDs, the Terminal looks for BSMSelector elements and BSMFilterCodes within those elements in the SGDD. Together with that information and the terminal's affiliated BSM(s) which are represented within the Terminal as Management Objects with identifier '<X>/BSMFilterCode', the Terminal categorizes all the fragments declared in the SGDD into three categories:
    i. Fragments that are associated with a BSMFilterCode (within BSMSelector), which matches at least one of the BSMFilterCodes associated with Home Mobile Broadcast Service Provider the terminal (<X>/ BSMFilterCode/IsHomeBSM == true). Terminal can use, interpret and render the information contained in these fragments without restrictions.
    ii. Fragments that are associated with a BSMFilterCode (within BSMSelector), which does not match with any of the BSMFilterCodes associated with the terminal or match BSMFilterCodes associated with Visited Mobile Broadcast Service Provider (<X>/ BSMFilterCode/IsHomeBSM == false). The terminal selects the BSMSelector with the highest RoamingPriority that is available on the BDS. Terminal can render, interpret and handle the fragments according to RoamingRules associated with this BSMSelector. BSMSelector and the associated RoamingRules are identified by the attribute "Id" present within the BSMSelector as well as in RoamingRules. If the RoamingRules have been provisioned using BCAST Terminal Provisioning, the rules are associated with each BSMFilterCode, under <X>/ BSMFilterCode/RoamingRule.
    iii. Fragments that are not associated with any BSMFilterCode (no BSMSelector).
        - In case Terminal has no Management Objects with identifier '<X>/ BSMFilterCode' present, the Terminal can use, interpret and render the information contained in these fragments without restrictions.
        - In case Terminal has at least one Management Object with identifier '<X>/ BSMFilterCode' present, the Terminal will determine behaviour according to Management Objects with identifier '<X>/IgnoreUnIdentifiedBSMIf the Management Objects with identifier '<X>/ IgnoreUnIdentifiedBSM' is set with value "true" the Terminal cannot use, interpret and render the information contained in these fragments at all.
            - If the Management Objects with identifier '<X>/ IgnoreUnIdentifiedBSM' is set with value "false" the Terminal can use, interpret and render the information contained in these fragments without restrictions.
            - If the Management Objects with identifier '<X>/ IgnoreUnIdentifiedBSM' is not present, the Terminal assumes that the value of such Management Object is "true".
5. If the terminal wants to render, interpret and handle the fragments in category (ii.) above, it needs to acquire the RoamingRules related to the BSMSelector in question. There are three ways to achieve this.
    a. The Terminal fetches the RoamingRules from Visited BSM. For that, the BSMSelector contains attribute "RoamingRuleRequestAddress" to which the Terminal can address the RoamingRuleRequest. As a response of to the RoamingRuleRequest the Terminal will receive RoamingRuleResponse which contains the RoamingRules associated with the BSMSelector.
    b. The Terminal fetches the RoamingRules from Home BSM. This happens if the BSMSelector does not have "RoamingRuleRequestAddress" present, OR, if the Terminal has Management Object "<X>/ForceHomeRoamingRuleRequestAddress" present and set to "true". In these cases the Terminal sends the RoamingRuleRequest to "<X>/HomeRoamingRuleRequestAddress". As a response of to the

RoamingRuleRequest the Terminal will receive RoamingRuleResponse which contains the RoamingRules associated with the BSMSelector.

c. The RoamingRules were originally provided as a part of BSMSelector (not illustrated in figure D.1)

6. The Terminal acquires Service Guide fragments. It interprets handles and renders the fragments according to RoamingRules. Consequently the Terminal uses the Service Guide fragments to perform subscriptions to services and content, and to access services and content described by the Service Guide.

7. Depending on the value of Management Object "<X>/Roaming/UseVisitedServiceProvisioningMode" the terminal determines whether to initiate the service provisioning request to Visited BSM or to Home BSM. Then the terminal sends the message to either Visited BSM or Home BSM. The receiving system determines from the requested GlobalPurchaseItemId and included UserID whether the request is about roaming. Two cases for this exist: either the Terminal sends the Service Request message to its Home BSM or to the Visited BSM.

   a. In the former case Home BSM detects that one of its terminal is requesting PurchaseItem served by another BSM. If the Home BSM wants to allow terminal to access the PurchaseItem, the Home BSM goes ahead and sends RoamingServiceRequest to the Visited BSM. Visited BSM answers with RoamingServiceResponse. In case the response allows roaming, then the Home BSM sends a successful ServiceResponse to the terminal. This leads to a subsequent LTKM delivery (push LTKM with Smartcard Profile or Trigger with DRM Profile). The LTKM acquisition is not shown in the diagram as it is a Service & Content Protection procedure.

   b. In the latter case Visited BSM detects that a terminal that is not one of the terminals affiliated with this BSM is requesting PurchaseItem served by this BSM. The Visited BSM consequently sends RoamingServiceRequest to the Home BSM of the terminal. Home BSM answers with RoamingServiceResponse. In case the response allows roaming, then the Visited BSM sends a successful ServiceResponse to the terminal. This leads to a subsequent LTKM delivery (push LTKM with Smartcard Profile or Trigger with DRM Profile). The LTKM acquisition is not shown in the diagram as it is a Service & Content Protection procedure.

   Upon successful RoamingProvisioning, the Terminal is granted right to purchase and/or subscribe to the PurchaseItem it requested.

8. In case the Terminal decides to request Long Term Key or to renew Long Term Key associated with a subscription, the Terminal sends either 'LTKM Request' or 'Subscription LTKM Renewal Request'. Two cases for this exist: either the Terminal sends the message to its Home BSM or to the Visited BSM.

   a. In the former case Home BSM detects that one of its terminal is requesting LTKM or renewal of LTKM associated with PurchaseItem served by another BSM. If the Home BSM wants to allow terminal to access the LTKM, the Home BSM goes ahead and sends RoamingAuthorizationRequest to the Visited BSM.

   b. In the latter case Visited BSM detects that a terminal that is not one of the terminals affiliated with this BSM is requesting LTKM or renewal of LTKM associated with PurchaseItem served by this BSM. The Visited BSM consequently sends RoamingAuthorizationRequest to the Home BSM of the terminal.

      Note: If step 8a or 8b follow 7a or 7b within a certain time frame, the authorization between home and visited BSM is not necessary.

The Terminal accesses service and//or content related to PurchaseItem, provided by Visited Service Provider.

Appendix F. Walk-through of Location Implementation (Informative)

This section describes an example of how a BCAST terminals might implement location-specific unicast/broadcast and blackout. Sections F.1-F.4 outline a simple way to implement location filtering of broadcast services and content. The simple functionality is a minimal subset of location functionality. The terminal may implement location functionality in BCAST 1.0 and BCAST 1.1. A terminal supporting BCAST 1.1 should implement at least the functionality of this appendix if the location functionality is supported.

In modern cellular systems most antennas support 3 or more sectors. Normally, each sector has a unique ID, however in some cases the cell is not divided into 3 sectors. The BCAST Location Filters only talk about cell ID. Therefore, in this appendix only the term cell ID will be used, meaning the identifier that is being broadcast by the present sector or cell where the handset is located.

F.1 Storage of Location Information

The targeted location function of the Service Guide Content and Service fragments allows expressions to be evaluated using a location history log. A BCAST 1.0 compatible terminal may be able to filter content based on its location at the time of content download, according to a simple rule defined in the content or service fragments. A BCAST 1.1 compatible terminal may further be able to filter content based on its location history, via an extended rule defined in content or service fragments. To support the BCAST 1.1 feature the terminal should implement a location history log. A location history log SHALL be an "opt-in" function, i.e. the user must give permission for the terminal to store a history log.

The support of a location history log is implementation dependent but should fulfill the following minimum requirements.

- Store location history for the last 6 months in the normal case
- Record location at intervals of 15 minutes, preferably synchronized to quarter hour boundaries
- Record location in the form of cell ID (and optionally other forms)
- Record time with an accuracy and granularity of 1 minute or less in a form suitable for time zone conversion (e.g. UTC)
- Store the log in encrypted form and/or in protected memory.
- Access to the location history log SHALL only be provided to authorized applications on the terminal.

If a location history log is supported, the terminal SHALL store the log in a secure location. If the log is encrypted, the terminal SHALL use a secure encryption protocol such as AES-CBC to store the location history log, the encryption keys SHALL be at least 128 bits in length, and the keys to encrypt the location history log SHALL also be stored in a secure location, i.e. together with other security keys held on the terminal. Reports of viewing history for Location Filtered Content and Services (including e.g. audience measurement reports or diagnostic reports) SHALL NOT contain the user identity, to protect the location privacy of the user.

The log could be composed of tuples, consisting of (cell ID, cell arrival time) at least. Note that the cell ID is at most 7 bytes in the BCAST specification, and a timestamp with "seconds granularity" is at most 4 bytes, so log entries need not be larger than 11 bytes per entry.

If the terminal stores the history log in encrypted blocks, then to save power, the terminal could store the most recent (partial) block as cleartext. When a full block of cleartext is available, the terminal could encrypt and store the block as ciphertext. The recursive location expressions in the LocationFilter element typically require the terminal to inspect a range of entries in the location history log. If the speed of this inspection process is an issue, then the following optimization could be adopted. After a new copy of the service guide arrives, the first operation to search the history log may cause the entire log to be decrypted (if it were stored encrypted) into RAM protected by the operating system kernel. Subsequent history operations would not require decryption, and the RAM log version could be discarded after all location expressions in the service guide had been processed.

F.2 Acquisition of Location Information

Cellular terminals periodically measure the cell ID of their serving cells as part of normal operation. Typically, every five seconds the terminal wakes up, turns on the receiver, and looks at the received ID for the current cell. If the cell ID changes, then the terminal may register its new location to receive paging messages. Paging regions may cover several sectors or cells and so not every change of cell ID results in a new paging registration. All of this functionality is present in cellular terminals.

The BCAST location logging function might wake up every fifteen minutes (i.e. once every 180 cell-sector wakeups) and measure the cell ID, and record a log entry if the cell ID has changed. The location logging function would not log changes every five seconds, as this would produce excessive flash-memory writes and increase battery consumption.

F.3 Location Filtering Life Cycle

The life cycle for a location-filtered advertisement download and rendering is depicted in Figure 7. Note that this example is specific to delivery and presentation of advertising content. There are 3 major events. First, the terminal receives an Auxiliary Data Download Notification Message, pointing to a particular piece of content, which contains a location filter, or inherits the location filter from the associated service. The terminal looks at the filteringTime attribute to decide when to evaluate the location filter expression. If the filteringTime attribute is "as soon as the fragment is received", then the location expression is evaluated, and a content download decision is made, and this decision is associated with the content in the service guide. If the filteringTime attribute is "some time in the future" (i.e. at the distribution window, or during the presentation window), then the location expression is presumed to be "indeterminate" (i.e. meaning the content should be downloaded), until the filteringTime has arrived.

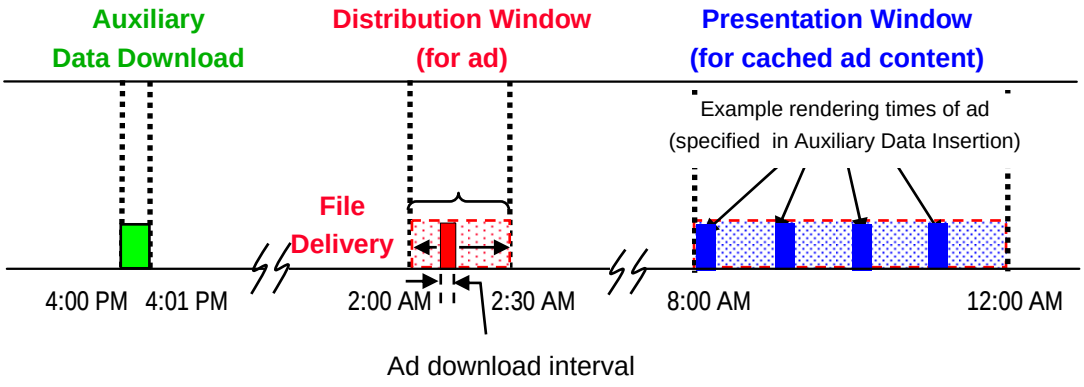


Figure 9: Life Cycle for Location-Filtered Ad Download and Rendering.

During the distribution window, if the location expression has not yet been evaluated, a similar check ("can this expression be evaluated now?") is made. If the filteringTime is "during the distribution window", the location expression is evaluated and a download decision is made, otherwise, the result is "indeterminate" and the default behaviour is to download the content. Later, an Auxiliary Data Insertion Message is received by the terminal during the Presentation Window, and this message selects a particular piece of cached content. After retrieving the content from the cache, if the filteringTime expression has not yet been evaluated, the location expression is evaluated at this time. If the content passes the filters, it is played back, otherwise the content is left in the cache, pending further Auxiliary Data Insertion Notification Messages (or expiry from the cache, presumably after the end of the PresentationWindow)

F.4 Restrictions on Location Filtering

The service guide should not contain location expressions containing time periods in the future, i.e. the StartTime of the LocationRequirement1 element should not be greater than the time for evaluation, specified by the filteringTime attribute of

the BroadcastArea element. The behaviour of the terminal that receives expressions with later StartTime values is undefined. We note that in many cases, the service provider may be able to convert queries about the future (e.g. "In the shopping mall with some lev_conf next weekend") into queries about the past (e.g. "In the shopping mall with high lev_conf in past weekends.")

An implementation may choose not to process a LocationFilter element that recurses to a depth of more than 8 elements of the LocationFilter type. This allows at most 255 LocationFilter elements to be sent in any single location constraint, which limits the resources needed on the terminal to process these constraints.

While the results of a location filter are "indeterminate", the terminal should not display the associated content in the service guide.

Appendix G. BCAST Management Object

G.1 OMA BCAST Device Management general

BCAST MOs allow a device to present the configuration of the device in a standardized way, allowing a server to be able to bootstrap, retrieve and manage the configuration of a device (the parameters included in the MO).

The BCAST MO structure is formally defined in [BCAST11-DDF-BCAST-MO].

Note: for the semantics of 'Status' of each of the MO parameters see [DMACMO]. This information is repeated here for convenience.

- Definition:
  - The Status definition in the node definitions indicates if the Client must support that node or not.
  - If the Status is "Required" even though the node may not be present at that time, the Server can expect the Client to be able to support it.
  - If the Status is "Required" then the Client must support that node in the case the Client supports the parent node. If the status is "Optional" then this should be reflected in DDF file to show whether the node is supported.
  - When creating the status of an MO, the child may be Required, while the parent node may be Optional. This would mean that all those elements would be Optional, but in case the parent node is present, then those child nodes would be Required.
- Possible Values: The value of this parameter can be "Required" or "Optional".

G.2 OMA BCAST Management Object Tree

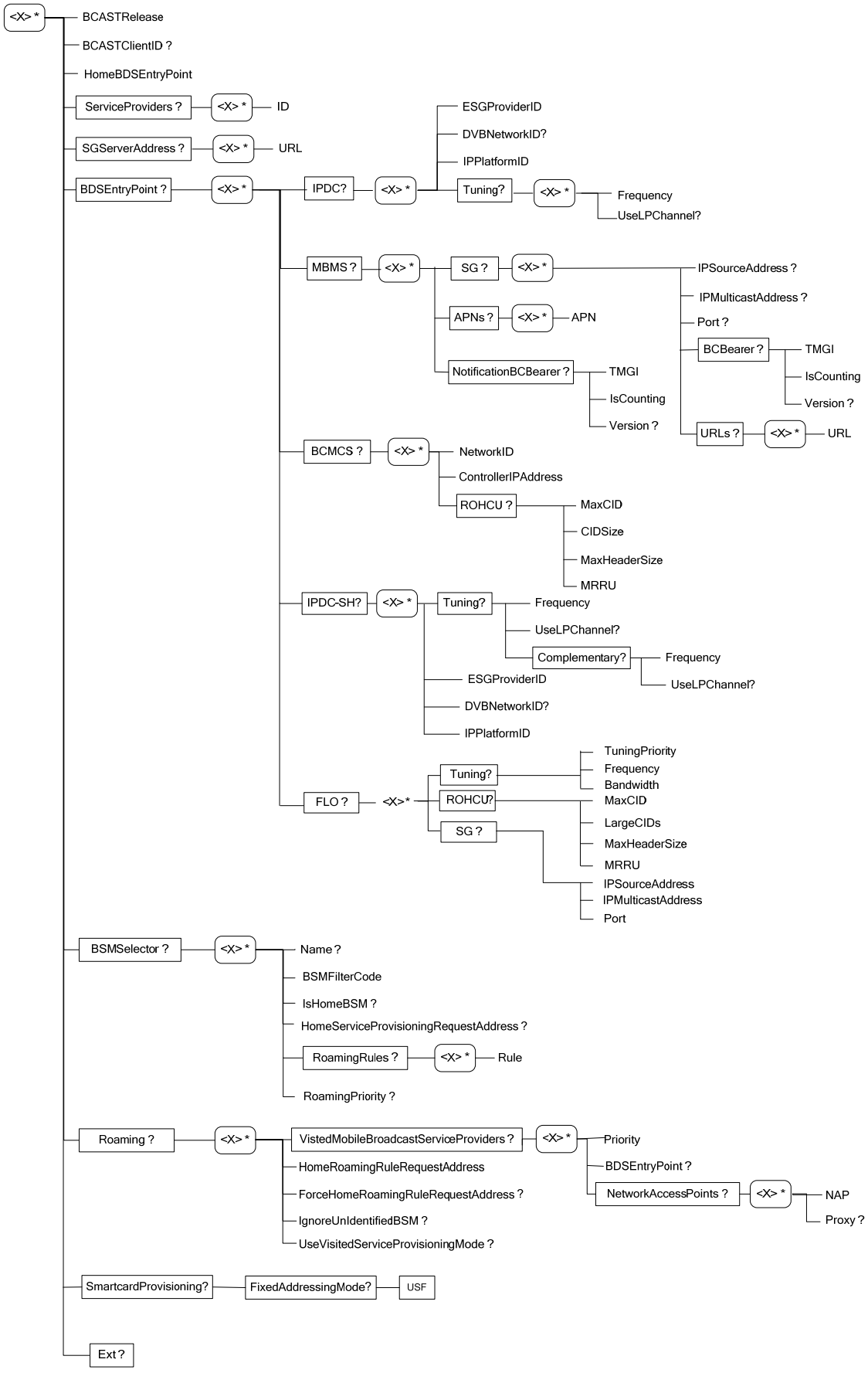


Figure 10: OMA BCAST Management Object Structure

Note: "?" means zero or one occurrences, "*" means zero or more occurrences. No symbol means one occurrence.

G.3 BCAST MO parameters

This section provides a description of the elements of the BCAST MO. Unless otherwise stated, BCAST terminals SHALL s upport the nodes defined below.

G.3.1 <X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for one or more BCAST Management Object root nodes. It is MANDATORY if the UE supports OMA BCAST.

G.3.2 <X>/BCASTRelease

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node specifies the BCAST release of the client. It is MANDATORY and MUST have the value "1.0" for this release.

G.3.3 <X>/BCASTClientID

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node contains the BCAST_Client_ID used by the Smartcard Profile as per [BCAST11-ServContProt].

G.3.4 <X>/HomeBDSEntryPoint

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the URL referencing the BDSEntryPoint/<X> node that is associated to the Home Mobile Broadcast Service Provider. The value of this node MUST be in the form of a URI.

G.3.5 <X>/ServiceProviders

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node acts as a container for a list of Service Provider identifiers.

G.3.6 <X>/ServiceProviders/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for a list of Service Provider identifiers.

G.3.7 <X>/ServiceProviders/<X>/ID

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node specifies the Service Provider identifier for the BCAST Service. It is e.g. used in the 'serviceproviders' field for protection signalling in SDP as per section 10.1.1 of [BCAST11-SrvContProt]. The value of this node MUST be in the form of a URI.

G.3.8 <X>/SGServerAddress

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains information about BCAST Service Guide Servers for the interactive mode. In case there are multiple servers present, the terminal MAY use any of them.

G.3.9 <X>/SGServerAddress/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node serves as a placeholder for a list of addresses of BCAST Service Guide Servers for the interactive mode.

G.3.10 <X>/SGServerAddress/<X>/URL

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node specifies the BCAST Service Guide server URL for the interactive mode.

G.3.11 <X>/BDSEntryPoint

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node contains information about the service entry points in the different BDSs. Possible children: IPDC, MBMS, BCMCS, IPDC-SH..

It is RECOMMENDED to also include Add, Delete and Replace access types on the implementations, in order to support write access on the sub-nodes to provision the necessary sets of information.

G.3.12 <X>/BDSEntryPoint/<X>

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node acts as a placeholder for sets of BDS-specific information. associated to a Mobile Broadcast Service Provider.

Typically one instance of this node is associated to the Home Mobile Broadcast Service Provider and the remaining nodes are associated with the Visited Mobile Broadcast Service Provider.

G.3.13 <X>/BDSEntryPoint/<X>/IPDC

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

For a terminal using DVB-H IPDC as the BDS, it is necessary to provision some information how to tune the device to the DVB-H broadcast network and to discover the IP flows in it.

If this interior node is present, a terminal using the DVB-H IPDC BDS SHOULD use this information to tune its receiver, to discover the IP flows which carry the service, and to resolve the actual Service Guide to use in a multi provider scenario.

This node acts as a container for all the BDS-specific information regarding IPDC over DVB-H. BCAST Terminals MAY support this node and its sub-nodes.

G.3.14 <X>/BDSEntryPoint/<X>/IPDC/<X>

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node serves as a placeholder for a list of IPDC network tuning parameters. If more than one instance of this node are present, the terminal MAY use suitable means (like the reception quality or user selection) to choose the most appropriate one.

G.3.15 <X>/BDSEntryPoint/<X>/IPDC<X>//Tuning

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node contains tuning parameters for the DVB-H receiver.

G.3.16 <X>/BDSEntryPoint/<X>/IPDC/<X>/Tuning/<X>

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node serves as a placeholder for a list of tuning frequencies for the IPDC network.

G.3.17 <X>/BDSEntryPoint/<X>/IPDC/<X>/Tuning/<X>/Frequency

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node carries the center frequency of the DVB-H channel to tune to.

The value representsthe frequency in kHz. This MUST be a decimal number and MUST fit within the range of a 32 bit unsigned integer.

G.3.18 <X>/BDSEntryPoint/<X>/IPDC/<X>/Tuning/<X>/UseLPChannel

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

DVB-H may use an optional hierarchical modulation mode in which case the receiver needs to make a selection between a "high priority" (HP) channel and a "low priority" (LP) channel.

This leaf node provides the information which is needed to tune to a hierarchically modulated DVB-H channel.

If present and **true**, the terminal SHALL use the LP channel in DVB-H hierarchical modulation. If not present or **false**, the terminal SHALL use the HP channel in DVB-H hierarchical modulation or assume that no hierarchical modulation is used.

G.3.19 <X>/BDSEntryPoint/<X>/IPDC<X>//IPPlatformID

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

DVB uses the concept of IP platforms to disambiguate the IP address ranges of several sources of IP traffic sharing a DVB channel. For a DVB-H terminal, the IP platform ID is required as side information to discover the IP flows.

According to [ETSI 102 470-1], section 4.2, an IP platform ID value is either registered with DVB in which case it is globally unique, or it is scoped to the network ID (see next section).

This leaf node provides

> the IP Platform ID. This node MUST contain a decimal number and MUST fit within the range of a 24 bit unsigned integer.

G.3.20 <X>/BDSEntryPoint/<X>/IPDC/<X>/DVBNetworkID

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	int	Get

There are cases where the IP platform ID is not globally unique but scoped to a DVB network ID which is registered with DVB.

This leaf node provides the network ID. It SHALL be present only if the IP platform ID is not globally unique according to [ETSI 102 470-1], section 4.2.

This node MUST contain a decimal number and MUST fit within the range of a 16 bit unsigned integer.

G.3.21 <X>/BDSEntryPoint/<X>/IPDC/<X>/ESGProviderID

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

In a DVB-H IPDC deployment, multiple service providers can share a DVB-H channel. The Service Guide bootstrap session can therefore contain multiple Service Guides (one per service provider and IP platform). To select and receive a service guide via the DVB-H IPDC BDS, the terminal needs to know the ID of the service guide provider to be used.

This leaf node provides

Service Guide Provider ID for SG bootstrapping. This node MUST contain a decimal number and MUST fit within the range of a 16 bit unsigned integer.

G.3.22 <X>/BDSEntryPoint/<X>/MBMS

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior acts as a container for all the BDS-specific information regarding MBMS. BCAST Terminals MAY support this node and its sub-nodes.

G.3.23 <X>/BDSEntryPoint/<X>/MBMS/<X>

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node serves as a placeholder for a list of MBMS Bearer Services. If more than one instance of this node are present, the terminal MAY use suitable means (like the reception quality or user selection) to choose the most appropriate one.

G.3.24 X>/BDSEntryPoint/<X>/MBMS/<X>/SG

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains bootstrap parameters for SG reception over MBMS broadcast bearer or SG retrieval over MBMS unicast bearer.

G.3.25 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for sets of bootstrap parameters for SG reception over MBMS broadcast bearer or SG retrieval over MBMS unicast bearer.

G.3.26 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/IPSourceAddress

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

This leaf node contains the IP Source Address of the SG delivery session for a broadcasted SG.

G.3.27 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/IPMulticastAddress

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

This leaf node contains the IP Multicast Address of the SG Announcement Channelfor a broadcasted SG.

G.3.28 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/Port

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	int	Get

This leaf node contains the port number for a broadcasted SG. The value MUST be a decimal number and MUST fit within the range of a 16 bit unsigned integer.

G.3.29 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node acts as a placeholder for sets of MBMS bearer parameter used for reception of a broadcasted SG (both SG Announcement Channel and SG Delivery Channel). This node SHALL be present in case the mode of the MBMS bearer is Broadcast Mode, and SHALL be absent otherwise.

G.3.30 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer/TMGI

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the Temporary Mobile Group Identity (TMGI) for a broadcasted SG as defined in [3GPP TS 23.003]. An MBMS Bearer service is uniquely identified by the TMGI. The value is encoded as a decimal number which in hexadecimal form represent octets 3 to 8 of the TMGI information element structure defined in [3GPP TS 24.008]. Octet 3 is the most significant octet.

G.3.31 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer/IsCounting

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get

This leaf node contains the information element MBMS Counting Information as defined in [3GPP TS 25.413]. It indicates whether the RAN level counting procedures is applicable or not for the MBMS broadcast mode.

The value **true** corresponds to the information element value of “counting” and the value **false** corresponds to the information element value “not counting”.

It is OPTIONAL for the terminal to act on to the information provided in this leaf node, e.g., if it has received the counting information out-of-band of the BCAST MO.

G.3.32 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/BCBearer/Version

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

This leaf node describes the version of the MBMS bearer. Possible values SHALL be constructed as the values of <Version> sub-element of <BDSType> element in SG Access fragment, when <Type> of <BDSType> is set to "1 – 3GPP MBMS" (see [BCAST11-SG] section 5.1.2.4). Accordingly, examples of valid values are: “3GPP.R6.UTRAN”, “3GPP.R8.MBSFN-IMB”. When this node is absent, the terminal SHALL assume "3GPP.R8.UTRAN" value for the MBMS bearer version of BCBearer node.

G.3.33 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/URLs

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains a list of URLs where an SDP describing the delivery session of a broadcasted SG can be fetched.

G.3.34 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/URLs/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for a list of URLs where an SDP describing the Announcement Channel of a broadcasted SG can be fetched.

G.3.35 <X>/BDSEntryPoint/<X>/MBMS/<X>/SG/<X>/URLs/<X>/URL

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the URL where an SDP describing the Announcement Channel of a broadcasted SG can be fetched.

G.3.36 <X>/BDSEntryPoint/<X>/MBMS/<X>/APNs

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains a list of URIs of usable Access Point Names (APN).

G.3.37 <X>/BDSEntryPoint/<X>/MBMS/<X>/APNs/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for a list of URIs of usable Access Point Names (APN).

G.3.38 <X>/BDSEntryPoint/<X>/MBMS/<X>/APNs/<X>/APN

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the URI of a usable Access Point Name (APN). An MBMS bearer is identified by IP multicast address and APN.

G.3.39 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer

Status	Occurrence	Format	Min. Access Types

Required	ZeroOrOne	node	Get

This interior node acts as a placeholder for sets of MBMS bearer parameter used for the Notification Function. This node SHALL be present in case the mode of the MBMS bearer is Broadcast Mode, and SHALL be absent otherwise.

G.3.40 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer/TMGI

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the Temporary Mobile Group Identity (TMGI) for a broadcasted SG as defined in [3GPP TS 23.003]. An MBMS Bearer service is uniquely identified by the TMGI. The value is encoded as a decimal number which in hexadecimal form represent octets 3 to 8 of the TMGI information element structure defined in [3GPP TS 24.008]. Octet 3 is the most significant octet.

G.3.41 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer/IsCounting

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get

This leaf node contains the information element MBMS Counting Information as defined in [3GPP TS 25.413]. It indicates whether the RAN level counting procedures is applicable or not for the MBMS broadcast mode.

The value **true** corresponds to the information element value of “counting” and the value **false** corresponds to the information element value “not counting”.

It is OPTIONAL for the terminal to act on to the information provided in this leaf node, e.g., if it has received the counting information out-of-band of the BCAST MO.

G.3.42 <X>/BDSEntryPoint/<X>/MBMS/<X>/NotificationBCBearer/Version

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

This leaf node describes the version of the MBMS bearer used for the Notification Function. Possible values SHALL be constructed as the values of <Version> sub-element of <BDSType> element in SG Access fragment, when <Type> of <BDSType> is set to "1 – 3GPP MBMS" (see [BCAST11-SG] section 5.1.2.4). Accordingly, examples of valid values are: “3GPP.R6.UTRAN”, “3GPP.R8.MBSFN-IMB”. When this node is absent, the terminal SHALL assume "3GPP.R8.UTRAN" value for the MBMS bearer version of NotificationBCBearer node.

G.3.43 <X>/BDSEntryPoint/<X>/BCMCS

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node acts as a placeholder for all the BDS-specific information regarding BCMCS. BCAST Terminals MAY support this node and its sub-nodes.

G.3.44 <X>/BDSEntryPoint/<X>/BCMCS/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for a list of Networks recognized by the terminal. If more than one instance of this node are present, the terminal MAY use suitable means (like the reception quality or user selection) to choose the most appropriate one.

G.3.45 <X>/BDSEntryPoint/<X>/BCMCS/<X>/NetworkID

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains network region identification information for BCMCS. The Value of this node is a string comprising the concatenation of 1 (in the case of subnet) or 1, 2, or 3 (in the case of SID/NID/PZID) hexdecimal numbers, each number prefixed by characters ‘s’ (subnet), ‘S’ (SID), ‘N’ (NID), or ‘P’ (PZID), used by the terminal to determine when overhead channels indicate that the terminal is in a particular network region.

G.3.46 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ControllerIPAddress

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the IP address of the BCMCS Controller, saving DHCP bootstrap time.

G.3.47 <X>/BDSEntryPoint/<X>/BCMCS/<X>/SGMulticastAddress

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains a string in the form of “<Hostname/Address>:<Port>”, much like an URL without a scheme prefix. For example, the contents might be “BCMCS.example.com:83” or “129.63.44.2:8000”.

G.3.48 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains ROHC Unidirectional (ROHC-U) parameters for BCMCS IP multicast communication. If the node is not present, compression is not enabled.

G.3.49 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/MaxCID

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node indicates the maximum number of CIDs used by ROHC-U.

G.3.50 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/LargeCIDs

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get

This leaf node is true when large CIDs (1 or 2 bytes) are used, otherwise it is false and small CIDs (0 or 1) are used.

G.3.51 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/MaxHeaderSize

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node contains the maximum header size, in octets, that can be compressed.

G.3.52 <X>/BDSEntryPoint/<X>/BCMCS/<X>/ROHCU/MRRU

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node contains the size of the Maximum Reconstructed Reception Unit, in octets, that the decompressor is expected to reassemble from segments. Value 0 means that no segment headers are allowed on the channel.

G.3.53 <X>/BDSEntryPoint/<X>/IPDC-SH

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

For a terminal using DVB-SH IPDC as the BDS, it is necessary to provision some information how to tune the device to the DVB-SH broadcast network and to discover the IP flows in it.

If this interior node is present, a terminal using the DVB-SH IPDC BDS SHOULD use this information to tune its receiver, to discover the IP flows which carry the service, and to resolve the actual Service Guide to use in a multi provider scenario.

This node acts as a container for all the BDS-specific information regarding IPDC over DVB-SH. BCAST Terminals MAY support this node and its sub-nodes.

G.3.54 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node serves as a placeholder for a list of DVB-SH IPDC network tuning parameters. If more than one instance of this node are present, the terminal MAY use suitable means (like the reception quality or user selection) to choose the most appropriate one.

G.3.55 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node contains tuning parameters for the DVB-SH receiver.

G.3.56 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Frequency

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node carries the center frequency of the primary DVB-SH signal to tune to.

When this frequency is part of the S band, it corresponds to the satellite signal.

The value represents the frequency in kHz. This MUST be a decimal number and MUST fit within the range of a 32 bit unsigned integer.

G.3.57 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/UseLPChannel

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

DVB-SH in OFDM mode may use an optional hierarchical modulation mode in which case the receiver needs to make a selection between a “high priority” (HP) channel and a “low priority” (LP) channel.

This leaf node provides the information which is needed to tune to a hierarchically modulated DVB-SH primary channel.

If present and **true**, the terminal SHALL use the LP channel in DVB-SH hierarchical modulation. If not present or **false**, the terminal SHALL use the HP channel in DVB-SH hierarchical modulation or assume that no hierarchical modulation is used.

G.3.58 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Complementary

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains parameters for the DVB-SH receiver to tune to the complementary terrestrial DVB-SH signal.

This node MUST be present:

- if frequency value given in /Tuning/Frequency node is in the S band (satellite signal)
- if moreover the Complementary Ground Component does not use this satellite frequency to repeat the satellite signal (non SFN case).

This node MUST be omitted otherwise.

G.3.59 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Complementary/HybridFrequency

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node carries the center frequency of the complementary terrestrial DVB-SH signal to tune to (hybrid frequency).

The value represents the frequency in kHz. This MUST be a decimal number and MUST fit within the range of a 32 bit unsigned integer.

G.3.60 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/Tuning/Complementary/UseLPChannel

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

DVB-SH in OFDM mode may use an optional hierarchical modulation mode in which case the receiver needs to make a selection between a “high priority” (HP) channel and a “low priority” (LP) channel.

This leaf node provides the information which is needed to tune to a hierarchically modulated DVB-SH channel.

If present and **true**, the terminal SHALL use the LP channel in DVB-SH hierarchical modulation. If not present or **false**, the terminal SHALL use the HP channel in DVB-SH hierarchical modulation or assume that no hierarchical modulation is used.

G.3.61 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/IPPlatformID

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

DVB uses the concept of IP platforms to disambiguate the IP address ranges of several sources of IP traffic sharing a DVB channel. For a DVB-SH terminal, the IP platform ID is required as side information to discover the IP flows.

According to [ETSI 102 470-2], section 4.1.2, an IP platform ID value is either registered with DVB in which case it is globally unique, or it is scoped to the network ID (see next section).

This leaf node provides the IP Platform ID. This node MUST contain a decimal number and MUST fit within the range of a 24 bit unsigned integer.

G.3.62 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/DVBNetworkID

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	int	Get

There are cases where the IP platform ID is not globally unique but scoped to a DVB network ID which is registered with DVB.

This leaf node provides the network ID. It SHALL be present only if the IP platform ID is not globally unique according to [ETSI 102 470-2], section 4.1.2.

This node MUST contain a decimal number and MUST fit within the range of a 16 bit unsigned integer.

G.3.63 <X>/BDSEntryPoint/<X>/IPDC-SH/<X>/ESGProviderID

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

In a DVB-SH IPDC deployment, multiple service providers can share a DVB-SH channel. The Service Guide bootstrap session can therefore contain multiple Service Guides (one per service provider and IP platform). To select and receive a service guide via the DVB-SH IPDC BDS, the terminal needs to know the ID of the service guide provider to be used.

This leaf node provides Service Guide Provider ID for SG bootstrapping. This node MUST contain a decimal number and MUST fit within the range of a 16 bit unsigned integer.

G.3.64 <X>/BDSEntryPoint/<X>/FLO

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node acts as a placeholder for all the BDS-specific information regarding Forward Link Only. BCAST Terminals MAY support this node and its sub-nodes.

G.3.65 <X>/BDSEntryPoint/<X>/FLO/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for a list of Networks recognized by the terminal.

G.3.66 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node contains information needed to tune the Forward Link Only receiver to the right frequency to receive Forward Link Only broadcasts.

G.3.67 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning/Priority

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node contains a priority (lower values signal higher priority) that is used to select the proper frequency for tuning, when two or more frequencies are available.

G.3.68 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning/Frequency

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node carries the center frequency of the Forward Link Only channel to tune to. The value represents the frequency in units of 50 Hz. This MUST be a decimal number and MUST fit within the range of a 32 bit unsigned integer.

G.3.69 <X>/BDSEntryPoint/<X>/FLO/<X>/Tuning/Bandwidth

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node carries the bandwidth of the Forward Link Only transmission system (e.g. 5000, 6000, 7000 or 8000 kHz.) The value represents the bandwidth in units of 50 Hz, and MUST be a decimal number and MUST fit within the range of a 32 bit unsigned integer.

G.3.70 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU

Status	Occurrence	Format	Min. Access Types

Required	ZeroOrOne	node	Get

This interior node contains ROHC Unidirectional (ROHC-U) parameters for Forward Link Only IP multicast communication. If the node is absent, compression is disabled.

G.3.71 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/MaxCID

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node indicates the maximum number of CIDs used by ROHC-U.

G.3.72 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/LargeCIDs

Status	Occurrence	Format	Min. Access Types
Required	One	bool	Get

This leaf node is true when large CIDs (1 or 2 bytes) are used, otherwise it is false and small CIDs (0 or 1) are used.

G.3.73 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/MaxHeaderSize

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node contains the maximum header size, in octets, that can be compressed.

G.3.74 <X>/BDSEntryPoint/<X>/FLO/<X>/ROHCU/MRRU

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node contains the size of the Maximum Reconstructed Reception Unit, in octets, that the decompressor is expected to reassemble from segments. Value 0 means that no segment headers are allowed on the channel.

G.3.75 <X>/BDSEntryPoint/<X>/FLO/<X>/SG

Status	Occurrence	Format	Min. Access Types
Required	One	node	Get

This interior node contains information that allows the Terminal to tune to the proper IP address and port to receive the broadcasted service guide.

G.3.76 <X>/BDSEntryPoint/<X>/FLO/<X>/SG/IPSourceAddress

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the IP address of the BSD/A that broadcasts the service guide.

G.3.77 <X>/BDSEntryPoint/<X>/FLO/<X>/SG/IPMulticastAddress

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node contains the IP address used for multicast delivery of the service guide.

G.3.78 <X>/BDSEntryPoint/<X>/FLO/<X>/SG/IPMulticastPort

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node contains the IP port used for multicast delivery of the service guide. The value MUST be a decimal number and MUST fit within the range of a 16 bit unsigned integer.

G.3.79 <X>/BSMSelector

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains information about the BSMSelector structures associated with the BSM of the Home or Roaming Broadcast Service Provider.

G.3.80 <X>/BSMSelector/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for sets of BSMSelector information.

G.3.81 <X>/BSMSelector/<X>/Name

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node specifies a user readable name of BSMFilterCode associated with the BSM of the Home or Roaming Broadcast Service Provider of the user.

G.3.82 <X>/BSMSelector/<X>/BSMFilterCode

Status	Occurrence	Format	Min. Access Types
Required	One	xml	Get

This leaf node specifies the value of the

BSMFilterCode associated with the BSM. This value is used in comparisons against the BSMFilterCode values in BSMSelectors in Service Guide Delivery Descriptors and RoamingRules. The value is a BSMFilterCode XML structure as defined in [BCAST11-SG] section 5.4.1.5.2.

G.3.83 <X>/BSMSelector/<X>/IsHomeBSM

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

This leaf node specifies whether the BSM that is associated with the BSMSelector belongs to the Home Broadcast Service Provider of the user. Absence means “false”.

G.3.84 <X>/BSMSelector/<X>/HomeServiceProvisioningRequestAddress

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	chr	Get

This leaf node specifies the address (URL) of the BSM the terminal can use to issue Service Provisioning requests, as defined in section 5.1 of the present document. This address is used when the leaf node “<X>/Roaming/<X>/UseVisitedServiceProvisioningMode” is set to “false”. This leaf node SHALL be present in case the leaf node <X>/BSMSelector/<X>/IsHomeBSM is set to “true”.

G.3.85 <X>/BSMSelector/<X>/RoamingRules

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node contains a list of RoamingRule structures associated with the BSMSelector.

G.3.86 <X>/BSMSelector/<X>/RoamingRules/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node acts as a placeholder for a list of RoamingRule structures associated with the BSMSelector,

G.3.87 <X>/BSMSelector/<X>/RoamingRules/<X>/Rule

Status	Occurrence	Format	Min. Access Types
Required	One	xml	Get

This leaf node that contains a RoamingRule

,given as a RoamingRule XML structure as defined in section 5.4.1.5.2 of [BCAST11-SG]. This element enables the use of OMA DM as a method to manage and update roaming rules at the terminal. This leaf node SHALL apply for <X>/BSMSelector elements which have <X>/BSMSelector/IsHomeBSM set to “false”.

G.3.88 <X>/BSMSelector/<X>/RoamingPriority

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	int	Get

This leaf node specifies the priority of the BSM in case of roaming the BCAST service. The terminal SHALL select the BSM with the highest priority among the available BSMs on the network of the Visited Mobile Broadcast Service Provider in a roaming scenario. Values: "1", "2", "3" etc, representing the numerical value of the priority. Value "1" represents the highest priority.

This leaf node is absent for <X>/BSMSelector elements which have <X>/BSMSelector/IsHomeBSM set to “true”.

G.3.89 <X>/Roaming

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node is a container for Roaming structures.

G.3.90 <X>/Roaming/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node is a placeholder for a list of Roaming structures.

G.3.91 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node is a container for providing information about the preferred Visited Mobile Broadcast Service Provider for the BCAST service in a roaming scenario.

G.3.92 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrMore	node	Get

This interior node is a placeholder for a list of Visited Mobile Broadcast Service Providers.

This interior node contains the references to the network entry points of the Visited Mobile Broadcast Service Provider and the priority of this Visited Mobile Broadcast Service Provider. The referenced entry points provides all the relevant information to tune into the various network of the Visited Mobile Broadcast Service Provider. More specifically, the referenced entry points are the BDSEntryPoint as defined in the BCAST MO structure and the Network Access Points as defined in [CONNMO].

G.3.93 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/Priority

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get

This leaf node specifies the priority of this Visited Mobile Broadcast Service Provider for consuming the BCAST service in a roaming situation. The terminal SHALL select the Visited Mobile Broadcast Service Provider with the highest priority

among the available network operators in a roaming scenario. Values: "1", "2", "3" etc, representing the numerical value of the priority. Value "1" represents the highest priority.

G.3.94 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/BDSEntryPoint

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node contains the reference to the BDSEntryPoint/<X> node under the BCAST MO of the Visited Mobile Broadcast Service Provider. The referenced BDS Entry Points provides all the relevant information to tune into the BDS of the Visited Mobile Broadcast Service Provider. The value of this node MUST be in the form of a URI.

G.3.95 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/NetworkAccessPoints/

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

. This interior node is a container for the unicast Network Access Points for roaming the BCAST service.

G.3.96 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/NetworkAccessPoints/<X>

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrMore	node	Get

This interior node is a placeholder for a list of references to unicast Network Access Points and Proxies for roaming the BCAST service.

Please note that when roaming unicast networks (in contrast to the networks defined under BDSEntryPoint) , the terminal can either access services through the Home Mobile Broadcast Service Provider or through the Visited Mobile Broadcast Service Provider. In the former case the child node NAP will refer to network access point in the home network and in the latter case to network access point in the visited network.

G.3.97 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/NetworkAccessPoints/<X>/NAP

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node references the id of a Network Access Points MO as defined in [CONNMO]. The value of this node MUST be in the form of a URI.

G.3.98 <X>/Roaming/<X>/VisitedMobileBroadcastServiceProviders/<X>/RoamingEntryPoint/NetworkAccessPoints/<X>/Proxy

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	chr	Get

This leaf node references the id of a Proxy MO as defined in [CONNMO]. The value of this node MUST be in the form of a URI.

G.3.99 <X>/Roaming/<X>/HomeRoamingRuleRequestAddress

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get

This leaf node specifies the URL of the default Server to which the terminal can send RoamingRule Requests related to the BSMSelector in case no other contact points are signalled in the Service Guide Delivery Descriptors associated with BSMSelector, or, in case the <X>/Roaming/<X>/ForceHomeRoamingRuleRequestAddress is set to "true".

G.3.100 <X>/Roaming/<X>/ForceHomeRoamingRuleRequestAddress

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

This leaf node specifies whether the Terminal SHALL override any other RoamingRuleRequestAddresses and always contact the address represented by <X>/Roaming/<X>/HomeRoamingRuleRequestAddress for Roaming Requests.

In case its value is "true", theTerminal SHALL always use <X>/Roaming/<X>HomeRoamingRuleRequestAddress when sending a RoamingRule Request message. In case its value is "false", the Terminal uses <X>/Roaming/<X>/HomeRoaming-RuleRequestAddress as the backup address in case the BSMSelector in SGDD does provide any other addresses for RoamingRule Requests. In the absence of this node, default value "true" is assumed.

G.3.101 <X>/Roaming/<X>/IgnoreUnIdentifiedBSM

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

This leaf node specifies whether Terminal SHALL ignore fragments that are not associated with BSMSelector(s).

If its value is "true", the Terminal SHALL ignore fragments that are not associated with any BSMSelector. If its value is "false", the Terminal MAY interpret, handle, access and render fragments that are not associated with any BSMSelector without any restrictions. In the absence of this, default value "true" is assumed if the terminal has any nodes of "<X>/ BSMFilterCode" present. Otherwise default value "false" is assumed.

G.3.102 <X>/Roaming/<X>/UseVisitedServiceProvisioningMode

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	bool	Get

This leaf node specifies whether Terminal SHALL initiate the service provisioning requests through Visited BSM or Home BSM.

In case its value is "true", the Terminal SHALL initiate the service provisioning requests through the Visited BSM. If its value is"false", the Terminal SHALL initiate the service provisioning requests through the Home BSM. Default value "true" is assumed.

G.3.103 <X>/SmartcardProvisioning

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node contains information about the SmartcardProvisioningReception structures.

G.3.104 <X>/SmartcardProvisioning /FixedAddressingMode

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node acts as a placeholder for sets of FixedAdressingMode information.

G.3.105 <X>/ SmartcardProvisioning/FixedAddressingMode /USF

Status	Occurrence	Format	Min. Access Types
Required	One	b64	Get

This leaf node specifies the base64-encoded value of the 40-bit USF (Unique Smartcard Filter) associated to the device. This value is used in comparisons against the USF values in section 5.19.2.

G.3.106 <X>/Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

Inside this interior node, vendor specific information related to BCAST can be placed (vendor meaning application vendor, device vendor, OS vendor etc.). Usually the vendor extension is identified by vendor specific name under the 'Ext' node. The tree structure under the vendor extension is not defined and can therefore include a non-standard sub-tree.

Appendix H. Guidelines for extending the XML schemas in future versions of BCAST

This appendix describes the extension rules which MUST be obeyed to ensure that the XML schemas defined in future versions of BCAST keep backward compatibility.

Future versions of BCAST SHALL make sure that extensions are defined in a backward compatible way such that decoders which are not aware of these extensions can safely ignore them but still are provided all expected information. To ensure this, the following rules SHALL be obeyed when extending a BCAST XML schema in future versions of BCAST:

1) Derivation-by-extension MAY be used to derive new types from existing ones, in accordance with the rules set out in [XMLSchema].
2) Wherever possible, an extended schema SHALL only add functionality and not replace existing functionality. This will allow a decoder which is only aware of a previous version to maximally understand an instance of the extended version.
3) Existing element names SHALL never be re-used for new elements. New element names SHALL be defined under their own XML namespace.
4) Extended versions of a BCAST XML schema SHALL use a namespace identifier with a different <version> indicator but with the same <prefix>.

If a desired extension can not be done in accordance with the above rules, it is REQUIRED not to extend existing elements or types but to define new ones or to specify new signalling such that decoders which do not support the extension are able to ignore them.

Appendix I. Media-Type Registrations

I.1 Media-Type Registration Request for application/vnd.oma.bcast.sprov+xml

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name: application
Subtype name: vnd.oma.bcast.sprov+xml
Required parameters: none
Optional parameters: none
Encoding considerations: binary

Security considerations:
Service Provisioning messages are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. As Service Provisioning messages convey information which services a user accesses, there is some risk that unintentional information may be exposed. The information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.
Interoperability considerations:
This content type carries Service Provisioning information within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:
OMA BCAST 1.0 Enabler Specification – Mobile Broadcast Services, especially section 5.1. Available from http://www.openmobilealliance.org

Applications, which use this media type:
OMA BCAST Services

Additional information:
Magic number(s): none
File extension(s): none
Macintosh File Type Code(s): none

Person & email address to contact for further information:
Uwe Rauschenbach
Uwe.Rauschenbach@nsn.com

Intended usage: Limited use.
Only for usage with Service Provisioning for Mobile Broadcast Services, which meet the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

Intended usage: Limited use.
Only for usage with Service Provisioning for Mobile Broadcast Services, which meet the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.2 Media-Type Registration Request for application/vnd.oma.bcast.drm-trigger+xml

This MIME type registration is obsolete as the DRM Trigger definition has been removed from BCAST 1.0 specifications.

I.3 Media-Type Registration Request for application/vnd.oma.bcast.smartcard-trigger+xml

This MIME type registration is obsolete as the Smartcard Trigger definition has been removed from BCAST 1.0 specifications.

I.4 Media-Type Registration Request for application/vnd.oma.bcast.imd+xml

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name: application
Subtype name: vnd.oma.bcast.imd+xml
Required parameters: none
Optional parameters: none
Encoding considerations: binary

Security considerations:
InteractivityMediaDocument data are active, meaning that upon the reception of the InteractivityMediaDocument, the terminal will interpret it and act based on the commands and structures in the document. There is a possibility that a maliciously formed InteractivityMediaDocument will cause unwanted operations. To protect the user and terminal against these operations, the terminal should notify or prompt the user in case the interpretation of InteractivityMediaDocument will cause a critical operation at the terminal (sending outbound data, accessing system areas, etc.). InteractivityMediaDocument data do not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.

Interoperability considerations:
This content type carries service interactivity information within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:
OMA BCAST 1.0 Enabler Specification – Mobile Broadcast Services, especially section 5.3.6.1. Available from http://www.openmobilealliance.org

Applications, which use this media type:
OMA BCAST Services

Additional information:
Magic number(s): none
File extension(s): none
Macintosh File Type Code(s): none

Person & email address to contact for further information:
Uwe Rauschenbach
Uwe.Rauschenbach@nsn.com

Intended usage: Limited use.
Only for usage with Service Interactivity for Mobile Broadcast Services, which meet the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.5 Media-Type Registration Request for application/vnd.oma.bcast.notification+xml

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name:	application
Subtype name:	vnd.oma.bcast.notification+xml
Required parameters:	none
Optional parameters:	none
Encoding considerations:	binary

Security considerations:
BCAST Notification message data are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.
Interoperability considerations:
This content type carries notification information within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:
OMA BCAST 1.0 Enabler Specification – Mobile Broadcast Services, especially section 5.14. Available from http://www.openmobilealliance.org

Applications, which use this media type:
OMA BCAST Notification client

Additional information:

Magic number(s):	none
File extension(s):	none
Macintosh File Type Code(s):	none

Person & email address to contact for further information:
Uwe Rauschenbach
Uwe.Rauschenbach@nsn.com

Intended usage: Limited use.
Only for usage with the BCAST Notification message, which meet the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.6 Media-Type Registration Request for application/vnd.oma.bcast.provisioningtrigger

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name:	application
Subtype name:	vnd.oma.bcast.provisioningtrigger

Required parameters: none
Optional parameters: none
Encoding considerations: binary

Security considerations:

BCAST Provisioning Trigger message data are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.

Interoperability considerations:

This content type carries trigger messages within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:

OMA BCAST 1.0 Enabler Specification – Mobile Broadcast Services, especially section 5.1.8. Available from http://www.openmobilealliance.org

Applications, which use this media type:

OMA BCAST Service Provisioning Client

Additional information:

Magic number(s): none
File extension(s): none
Macintosh File Type Code(s): none

Person & email address to contact for further information:

Uwe Rauschenbach

Uwe.Rauschenbach@nsn.com

Intended usage: Limited use.

Only for usage with the BCAST Provisioning Trigger message, which meets the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.7 Media-Type Registration Request for application/vnd.oma.bcast.roaming+xml

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name: application
Subtype name: vnd.oma.bcast.roaming+xml
Required parameters: none
Optional parameters: none
Encoding considerations: binary

Security considerations:

BCAST Roaming message data are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.

Interoperability considerations:

This content type carries roaming information within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements for this content.

Published specification:

OMA BCAST 1.0 Enabler Specification – Mobile Broadcast Services, especially section 5.7.1. Available from http://www.openmobilealliance.org

Applications, which use this media type:

OMA BCAST Roaming client

Additional information:

Magic number(s):	none
File extension(s):	none
Macintosh File Type Code(s):	none

Person & email address to contact for further information:

Uwe Rauschenbach

Uwe.Rauschenbach@nsn.com

Intended usage: Limited use.

Only for usage with the BCAST Roaming message, which meet the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.8 Media-Type Registration Request for application/vnd.oma.bcast.am-message+xml

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name:	application
Subtype name:	vnd.oma.bcast.am-message+xml
Required parameters:	none
Optional parameters:	none
Encoding considerations:	binary

Security considerations:

BCAST Audience Measurement Message data are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.

Interoperability considerations:

This content type carries audience measurement messages within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:

OMA BCAST 1.1 Enabler Specification – Mobile Broadcast Services, especially section <insert number of section defining Terminal-based AM>. Available from http://www.openmobilealliance.org

Applications, which use this media type:

OMA BCAST Audience Measurement Client

Additional information:

Magic number(s):	none
File extension(s):	none
Macintosh File Type Code(s):	none

Person & email address to contact for further information:

Name tbd

Email tbd

Intended usage: Limited use.

Only for usage with the BCAST Audience Measurement XML messages, which meets the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.9 Media-Type Registration Request for application/vnd.oma.bcast.am-trigger

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name:	application
Subtype name:	vnd.oma.bcast.am-trigger
Required parameters:	none
Optional parameters:	none
Encoding considerations:	binary

Security considerations:

BCAST Audience Measurement Trigger message data are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.

Interoperability considerations:

This content type carries trigger messages within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:

OMA BCAST 1.1 Enabler Specification – Mobile Broadcast Services, especially section <insert number of section defining AM Trigger>. Available from http://www.openmobilealliance.org

Applications, which use this media type:

OMA BCAST Audience Measurement Client

Additional information:

Magic number(s):	none
File extension(s):	none
Macintosh File Type Code(s):	none

Person & email address to contact for further information:

Name tbd

Email tbd

Intended usage: Limited use.

Only for usage with the BCAST Audience Measurement Trigger message, which meets the semantics given in the mentioned specification.

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

I.10 Media-Type Registration Request for application/vnd.oma.bcast.coupon+xml

This section provides the registration request, as per [RFC 2048], to be submitted to IANA.

Type name:	application
Subtype name:	vnd.oma.bcast.coupon+xml
Required parameters:	none
Optional parameters:	none
Encoding considerations:	binary

Security considerations:

BCAST coupon documents are passive, meaning they do not contain executable or active content which may represent a security threat. The format does not include confidential fields. However, the information present in this media format is used to configure the receiving application. Thus, the usage of the format may be vulnerable to attacks modifying or spoofing the content of this format. Depending on the system architecture, it is recommended to use source authentication and integrity protection.

Interoperability considerations:

This content type carries coupon information within the scope of the OMA BCAST enabler. The OMA BCAST enabler specification includes static conformance requirements and interoperability test cases for this content.

Published specification:

OMA BCAST 1.1 Enabler Specification – Mobile Broadcast Services, especially section 5.22. Available from http://www.openmobilealliance.org

Applications, which use this media type:

OMA BCAST Services

Additional information:

Magic number(s): none

File extension(s): none

Macintosh File Type Code(s): none

Person & email address to contact for further information:

Donald Gillies

dgillies@qualcomm.com

Intended usage: Unlimited use.

For usage with the BCAST Service provisioning messages, which meet the semantics given in the mentioned specification. Coupon documents are also for delivery via BCAST broadcast file delivery. Coupon documents are also for delivery via SMTP email, HTTP, SMS, and other message transports,

Author/Change controller: OMNA – Open Mobile Naming Authority, OMA-OMNA@mail.openmobilealliance.org

Appendix J. Walk-Through of issuing and redeeming broadcast coupons (Informative)

The BCAST system defines a Coupon document that can be broadcast in the service guide or delivered via means other than FLUTE/ALC. In the subsequent section, we describe how BCAST can meet the need to issue many different types of coupons with the Coupon document of the service guide.

J.1 Newspaper Coupon

To create a newspaper coupon, the issuer (typically a retailer) creates a coupon document and fills in the validFrom and validTo fields, the Description, and PriceInfo. If the coupon is a physical (store) coupon, the CouponImage field is filled with an URL that displays a viewable (and possibly scannable) version of the coupon. It is recommended that the scannable image contain a bar code or matrix code holding the contents of the coupon document. The 'Provider' is set to '1' (Retailer) and the 'MultiUseWeight' is set to '0.5' (allowing the coupon to be combined with a manufacturer coupon.)

The AuthorityURI is filled in for the coupon. The AuthorityURI names the public-key of the issuer. The issuer must have an X.509 that points (perhaps through a chain of X.509 certificates) to a certificate authority that the BCAST system recognizes. The coupon issuer signs the coupon using its private key. The signature protects the entire body of the XML coupon document.

When the coupon is presented to an electronic system for redemption, the system inspects the AuthorityURI and finds the appropriate certificate for the authorityURI. If the certificate is not already cached for the AuthorityURI, the system shall issue an HTTP GET to the AuthorityURI with the argument “getCertificate”, and the X.509 certificate will be returned in the body of the HTTP response. If necessary, the electronic system uses a protocol such as SCVP to trace the path from the issuer's certificate to a trusted root authority. Alternately, the electronic system may have a set of static, cached certificates that it accepts.

All certificates along the certificate path are cached so that the path is only retraced when one certificate expires or is revoked. Once the certificate for authorityURI and a path to a trusted root authority is established, then the coupon signature is verified by decrypting the coupon authoritySignature using the public key. If the signature is correct, the coupon is accepted.

J.2 Service Provider Coupon

To create a typical coupon for BCAST content, the BCAST system creates a coupon document and fills in the validFrom and validTo fields, the Description, and PriceInfo. The MultiUseWeight is set to 0.5, and the Provider is set to '1' (system operator).

In addition, the PurchaseItem field is filled in with the globalPurchaseItemID for the associated PurchaseItem. This is a long-lived identifier that will not change when new versions of the service guide are downloaded. If the coupon is specific to one or more PurchaseDatas, the associated (long-lived) GlobalPurchaseDataIDs are filled in for the coupon. This allows a coupon to e.g. be used to purchase 1-month or 1-year of a service (which may be represented by a single PurchaseItem), however, the discount might not apply to 1-week of the same service.

The coupon authority is filled in the the BSM's AuthorityURI and the coupon is signed. It may now be broadcast to all users, or sent via any unicast transport to an individual user. Because there is a mimeType for the coupon, the coupon may be received via email, and stored in a file. The user may then cut and paste the coupon into BCAST, or open the file via BCAST, so that BCAST may process the coupon.

The aforementioned coupon is transferrable. To make a non-transferrable coupon, the UserID is filled in with the Identity type and IdentityValue, causing the AuthoritySignature to be calculated over both the Coupon contents AND the Identity type, appended to the coupon in memory. Thus, the coupon will not validate with another user.

J.3 Content Provider Coupon

To create a typical coupon for BCAST content, the BCAST system creates a coupon document and fills in the validFrom and validTo fields, the Description, and PriceInfo. The MultiUseWeight is set to 0.5, and the Provider is set to '0' (content provider).

The rest of the steps are as described for the Service Provider Coupon.

J.4 Premium or Frequent-User Coupons

To make a frequent-user coupon or a premium-coupon, the steps of section J.2 are followed and a non-transferrable coupon is made. At the Service Provider's option, the coupon may be made transferrable. The MultiUseWeight is set to '1.0' and the ReuseDelay is omitted, which creates a non-combinable, single-use coupon.

The result coupon can be transported to the terminal by any mechanism, including broadcast, unicast, as the result of a service purchase or webshop purchase transaction, or via email, SMS, MMS, or HTTP transport.

J.5 First-time or never-Subscribed Coupons

To make a frequent-user coupon or a premium-coupon, the steps of section J.2 are followed. The 'mustVerify' attribute is set to '1', which causes the BCAST system (or coupon redeemer) to contact the coupon issuer (via the authorityURI) to get consent to redeem the coupon. The contact transaction is an HTTP POST message with an argument "&getConsent", and the coupon contents in the body of the message. A 200 OK response implies that consent has been granted. This allows e.g. a movie studio (content producer) to issue a coupon for customers watching a movie from the studio for the first time. The protocol for this consent transaction is outside the scope of BCAST. The coupon issuer can tell from the user identity and/or BCAST-provided information whether the user is a first-time user or has never purchased the item before. The result of thie consent transaction is a 'yes' or 'no' approval for BCAST to accept the coupon, and the BCAST purchase transaction relays this information to the user making the purchase.