



# **Enabler Test Specification for BCAST Interoperability**

**Candidate Version 1.0 – 26 Feb 2008**

---

**Open Mobile Alliance**  
OMA-ETS-BCAST\_INT-V1\_0-20080226-D

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

# Contents

<b>1. SCOPE</b> .....	<b>6</b>
<b>2. REFERENCES</b> .....	<b>7</b>
<b>2.1 NORMATIVE REFERENCES</b> .....	<b>7</b>
<b>2.2 INFORMATIVE REFERENCES</b> .....	<b>7</b>
<b>3. TERMINOLOGY AND CONVENTIONS</b> .....	<b>8</b>
<b>3.1 CONVENTIONS</b> .....	<b>8</b>
<b>3.2 DEFINITIONS</b> .....	<b>8</b>
<b>3.3 ABBREVIATIONS</b> .....	<b>9</b>
<b>4. INTRODUCTION</b> .....	<b>12</b>
<b>5. BCAST INTEROPERABILITY TEST CASES</b> .....	<b>13</b>
<b>5.1 SERVICE PROVISIONING</b> .....	<b>13</b>
5.1.1 Service bootstrap and single content.....	13
5.1.2 Web-based Service Provisioning .....	13
<b>5.2 SERVICE GUIDE</b> .....	<b>14</b>
5.2.1 Service Guide update (same fragment id, higher version number) – Broadcast Channel .....	14
5.2.2 Service Guide update (same fragment id, higher version number) – Interaction Channel.....	15
5.2.3 Service Guide Update (new fragment id) – Broadcast Channel.....	15
5.2.4 Service Guide Update (new fragment id) – Interaction Channel .....	16
5.2.5 GZIP compression of Service Guide Delivery Unit.....	17
5.2.6 Content hierarchy.....	17
5.2.7 PreviewData and Service – Broadcast Channel .....	18
5.2.8 PreviewData and Service – Interaction Channel.....	18
5.2.9 Select language specific access parameters .....	19
5.2.10 Subscription of Service .....	19
<b>5.3 FILE AND STREAM DISTRIBUTION</b> .....	<b>20</b>
5.3.1 File Distribution.....	20
5.3.1.1 <i>Support of ALC protocol and delivery of meta-data in the Service Guide</i> .....	20
5.3.1.2 <i>Support of in-band delivery of meta-data and FLUTE</i> .....	21
5.3.1.3 <i>Support the delivery using HTTP over Interaction Channel</i> .....	21
5.3.1.4 <i>Support of FEC RAPTOR</i> .....	22
5.3.1.5 <i>Support of the post-delivery repair of files</i> .....	23
5.3.1.6 <i>Support of reception report</i> .....	23
5.3.1.7 <i>Support of Flute Session Setup and Control with RTSP</i> .....	24
5.3.2 Streaming Distribution.....	25
5.3.2.1 <i>Support of RTP for stream distribution over the broadcast channel</i> .....	25
5.3.2.2 <i>Support of RTP for stream distribution over the interactive channel using SDP</i> .....	26
5.3.2.3 <i>Support of RTP for stream distribution over the interactive channel using HTTP with out-of-band signalling</i> .....	26
5.3.2.4 <i>Support of streaming associated procedure</i> .....	27
<b>5.4 SERVICE INTERACTION</b> .....	<b>28</b>
5.4.1 XHTML MP Interactivity – Broadcast Channel .....	28
5.4.2 XHTML MP Interactivity – Interaction Channel.....	28
5.4.3 SMS interactivity – Broadcast Channel .....	29
5.4.4 SMS interactivity – Interaction Channel.....	29
5.4.5 MMS Interactivity – Broadcast Channel.....	30
5.4.6 MMS Interactivity – Interaction Channel .....	31
<b>5.5 SERVICE AND CONTENT PROTECTION</b> .....	<b>31</b>
5.5.1 DRM Profile .....	31
5.5.1.1 <i>Delivery of IPsec protected stream</i> .....	31
5.5.1.2 <i>Delivery of SRTP protected stream</i> .....	32
5.5.1.3 <i>Delivery of ISMACrypt protected stream</i> .....	33
5.5.2 Smartcard Profile .....	34
5.5.2.1 <i>Layer 1 Authentication and Service Registration</i> .....	34
5.5.2.1.1 GBA-U Bootstrapping USIM / BSM with success .....	34
5.5.2.1.2 GBA-U Bootstrapping USIM / BSM with synchronization error .....	37

5.5.2.1.3	GBA_U: Expired Bootstrapping data.....	38
5.5.2.1.4	GBA_U: Different Key K on Client and Server.....	40
5.5.2.1.5	Deregistration.....	42
5.5.2.1.6	Deregistration with Bootstrapping.....	43
5.5.2.1.7	Subscriber Key Establishment for (R-)UIM/CSIM.....	45
5.5.2.2	<i>Layer 2 LTKM</i> .....	46
5.5.2.2.1	OMA BCAST LTKM Terminal processing.....	46
5.5.2.2.1.1	LTKM without SPE, without consumption reporting, MBMS only card.....	46
5.5.2.2.1.2	LTKM without SPE, with consumption reporting, BCAST card.....	47
5.5.2.2.1.3	LTKM with SPE, MBMS only card.....	48
5.5.2.2.1.4	LTKM with SPE, BCAST card.....	49
5.5.2.2.1.5	LTKM request from the terminal, LTKM reception at the terminal / smartcard.....	49
5.5.2.2.1.6	BSM solicited pull procedure.....	50
5.5.2.2.1.7	BSM solicited pull procedure initiation over SMS Bearer.....	51
5.5.2.2.1.8	BSM solicited pull procedure to initiate the Registration Procedure.....	52
5.5.2.2.1.9	LTKM Replay Detection in secure function, failure case.....	52
5.5.2.2.2	Managing purses and counters using OMA BCAST LTKM.....	53
5.5.2.2.2.1	Set of live ppt_purse associated with a key group, SPE=0x00.....	54
5.5.2.2.2.2	Test of set mode for the live_ppt_purse associated with a key group, SPE=0x00.....	55
5.5.2.2.2.3	Test of add mode for the live_ppt_purse associated with a key group, SPE=0x00.....	56
5.5.2.2.2.4	Test of overflow for the live_ppt_purse associated with a key group, SPE=0x00.....	56
5.5.2.2.2.5	Set of playback_ppt_purse associated with a key group, SPE=0x01.....	57
5.5.2.2.2.6	Test of set mode for playback_ppt_purse associated with a key group, SPE=0x01.....	58
	Test of add mode for playback_ppt_purse associated with a key group, SPE=0x01e.....	59
5.5.2.2.2.7	.....	59
5.5.2.2.2.8	Test of overflow for playback_ppt_purse associated with a key group, SPE=0x01.....	60
5.5.2.2.2.9	Set of user_purse associated with a NAF/SMK id.....	61
5.5.2.2.2.10	Test of set mode for user_purse associated with a NAF/SMK id.....	62
5.5.2.2.2.11	Test of add mode for user_purse associated with NAF/SMK id.....	63
5.5.2.2.2.12	Test of overflow for user_purse associated with NAF/SMK id.....	64
5.5.2.2.2.13	Set of Playback counter associated with a SEK/PEK id, SPE=0x07.....	65
5.5.2.2.2.14	Test of set mode for Playback counter associated with a SEK/PEK id, SPE=0x07.....	66
5.5.2.2.2.15	Test of add mode for Playback counter associated with a SEK/PEK id, SPE=0x07.....	67
5.5.2.2.2.16	Test for overflow of Playback counter associated with a SEK/PEK id, SPE=0x07.....	68
5.5.2.2.2.17	Set of TEK counter associated with a SEK/PEK id.....	69
5.5.2.2.2.18	Test of set mode for TEK counter associated with a SEK/PEK id.....	70
5.5.2.2.2.19	Test of add mode for TEK counter associated with SEK/PEK id.....	71
5.5.2.2.2.20	Test of overflow for TEK counter associated with SEK/PEK id.....	72
5.5.2.2.3	SPE value not supported by the card.....	74
5.5.2.3	<i>Layer 3 STKM</i> .....	74
5.5.2.3.1	Correct STKM parsing by a BCAST Smartcard.....	74
5.5.2.3.2	Correct STKM parsing by Smartcard (MBMS).....	76
5.5.2.3.3	Incorrect STKM generation – inexistent SEK/PEK (wrong key domain ID).....	76
5.5.2.3.4	Incorrect STKM generation – inexistent SEK/PEK (wrong SEK ID).....	77
	STKM processing, Key Validity data check.....	78
5.5.2.3.5	.....	78
5.5.2.3.6	Key deletion from server.....	79
5.5.2.3.7	SPE deletion from the server.....	80
5.5.2.3.8	STKM processing based on the LTKM security policy extension (SPE).....	82
	STKM processing when LTKM SPE=0x00; testing live_ppt_purse.....	82
5.5.2.3.8.1	.....	82
5.5.2.3.8.2	STKM processing when LTKM SPE=0x01; testing playback_ppt_purse.....	84
5.5.2.3.8.3	STKM processing when LTKM SPE=0x02; testing user_purse.....	87
5.5.2.3.8.4	STKM processing when LTKM SPE=0x07; testing playback_counter.....	89
5.5.2.3.8.5	STKM processing when LTKM SPE=0x0C; testing TEK counter.....	93
5.5.2.3.9	STKM processing by priority order.....	96
5.5.2.3.9.1	Testing SPE priorities : live content with subscription.....	96
5.5.2.3.9.2	Testing SPE priorities : live content without subscription.....	99
5.5.2.3.9.3	Testing SPE priorities : playback modes including SPE=0x05.....	104
5.5.2.3.9.4	Testing SPE priorities : playback modes without SPE=0x05.....	109
5.5.2.3.9.5	Testing KV priorities when several LTKM available with same SPE.....	114
5.5.2.3.10	STKM processing when sent to different SPE sharing the same user purse.....	117
5.5.2.3.11	STKM reception with parental control without PIN defined in the card.....	122
5.5.2.3.12	STKM reception with parental control and with PIN defined in the card.....	123

5.5.2.3.13 Multiple streams protected with same STKM stream ..... 124

5.5.2.3.14 Multiple streams protected with different STKM streams ..... 125

5.5.2.4 *Layer 4: Traffic Encryption layer* ..... 125

5.5.2.4.1 Delivery of IPSec protected stream..... 125

5.5.2.4.2 Delivery of SRTP protected stream..... 126

5.5.2.4.3 Delivery of ISMACrypt protected stream ..... 127

**5.6 TERMINAL PROVISIONING .....128**

5.6.1 Receiving terminal provisioning messages using TP-7 ..... 128

5.6.2 Update terminal provisioning messages using TP-7 ..... 128

5.6.3 Declaring Terminal Provisioning as a Service within Service Guide ..... 128

5.6.4 Declaring Terminal Provisioning as an Access of a Service within Service Guide ..... 129

**APPENDIX A. CHANGE HISTORY (INFORMATIVE).....130**

**A.1 APPROVED VERSION HISTORY .....130**

**A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY .....130**

# 1. Scope

This document describes interoperability test cases for “Mobile Broadcast Services” according to Open Mobile Alliance™, OMA-TS-BCAST\_Services-V1\_0, <http://www.openmobilealliance.org/>.

The interoperability test cases are aimed to verify that implementations of the specifications work satisfactory.

## 2. References

### 2.1 Normative References

- [IOPPROC] “OMA Interoperability Policy and Process”, Version 1.4, Open Mobile Alliance™, OMA-ORG-IOP\_Process-V1\_4, URL:<http://www.openmobilealliance.org/>
- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, URL:<http://www.ietf.org/rfc/rfc2119.txt>
- [BCAST10-ETR] “Enabler Test Requirements for Mobile Broadcast Services” Open Mobile Alliance™, OMA-ETR-BCAST-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10-ERELED] “Enabler Release Definition for Mobile Broadcast Services”, Open Mobile Alliance™, OMA-ERELED-BCAST-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10 –Services] “Mobile Broadcast Services”, Open Mobile Alliance™, OMA-TS-BCAST\_Services-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10 – Distribution] “File and Stream Distribution for Mobile Broadcast Services “, Open Mobile Alliance™, OMA-TS-BCAST\_Distribution-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10 –ESG] “Service and Content Protection for Mobile Broadcast Services”, Open Mobile Alliance™, OMA-TS-BCAST\_SvcCntProtection-V1\_0, [http://www.openmobilealliance.org](http://www.openmobilealliance.org/)
- [BCAST10– ServContProt] “Service and Content Protection for Mobile Broadcast Services”, Open Mobile Alliance™, OMA-TS-BCAST\_SvcCntProtection-V1\_0, <http://www.openmobilealliance.org/>
- [DRM20-Broadcast-Extensions] “OMA DRM v2.0 Extensions for Broadcast Support”, Open Mobile Alliance™, OMA-TS-DRM-XBS-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10 –MBMS Adaptation] “Broadcast Distribution System Adaptation – 3GPP/MBMS”, Open Mobile Alliance™, OMA-TS-BCAST\_MBMS\_Adaptation-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10–BCMCS Adaptation] “Broadcast Distribution System Adaptation – 3GPP2/BCMCS”, Open Mobile Alliance™, OMA-TS-BCAST\_BCMCS\_Adaptation-V1\_0, <http://www.openmobilealliance.org/>
- [BCAST10–DVB-H-IPDC–Adaptation] “Broadcast Distribution System Adaptation – IPDC over DVB-H”, Open Mobile Alliance™, OMA-TS-BCAST\_DVB\_Adaptation-V1\_0, <http://www.openmobilealliance.org/>
- [OMA DM] “Enabler Release Definition for OMA Device Management v1.2”, Open Mobile Alliance™, OMA-ERELED-DM-V1\_2\_0, <http://www.openmobilealliance.org/>
- [DRM-v2.0] “DRM Specification V2.0”, Open Mobile Alliance™, OMA-DRM-DRM-V2\_0, <http://www.openmobilealliance.org/>
- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, URL:<http://www.ietf.org/rfc/rfc2119.txt>

### 2.2 Informative References

- [OMADICT] “Dictionary for OMA Specifications”, Open Mobile Alliance™, OMA-Dictionary, URL:<http://www.openmobilealliance.org/>
- [BCAST10-Architecture] “Mobile Broadcast Services Architecture”, Open Mobile Alliance™, OMA-AD-BCAST-V1\_0, <http://www.openmobilealliance.org/>

## 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”, are normative, unless they are explicitly indicated to be informative.

The following numbering scheme is used:

**xxx-y.z-con-number** where:

xxx	Name of enabler, e.g. MMS or Browsing
y.z	Version of enabler release, e.g. 1.2 or 1.2.1
'con'	Indicating this test is a conformance test case
number	Leap number for the test case

Or

**xxx-y.z-int-number** where:

xxx	Name of enabler, e.g. MMS or Browsing
y.z	Version of enabler release, e.g. 1.2 or 1.2.1
'int'	Indicating this test is a interoperability test case
number	Leap number for the test case

### 3.2 Definitions

**Test-Fest** Multi-lateral interoperability testing event

**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 filedownloading 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.



<b>Purchase Item</b>	A purchase item groups one or multiple services or pieces of content that an end-user can purchase or subscribe to as a whole. [BCAST10-ESG].
<b>Rights Object</b>	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]
<b>Rights Issuer</b>	An entity that issues Rights Objects to OMA DRM Conformant Devices. [DRMDRM-v2.0]
<b>User ID</b>	A unique ID that can be used to identify the user in both the Home Service Provider and Visited Service Provider BCAST service area. An example is the 3GPP/3GPP2 IMSI (International Mobile Subscriber Identity) as specified in 3GPP TS 23.003 and 3GPP2 C.S0005 (for the case the Broadcast Service Provider is a cellular mobile operator).

### 3.3 Abbreviations

<b>ATSC</b>	Advanced Television Systems Committee
<b>BCMCS</b>	Broadcast/Multicast Services
<b>BDS</b>	Broadcast Distribution System
<b>BDS-SD</b>	BDS Service Distribution
<b>BSA</b>	BCAST Service Application
<b>BSM</b>	BCAST Subscription Management
<b>BSD/A</b>	BCAST Service Distribution and Adaptation
<b>BSI-C</b>	BCAST Service Interaction – Client Component
<b>BSI-G</b>	BCAST Service Interaction – Generic Component
<b>BSP</b>	Broadcast Service Provisioning
<b>BSP-C</b>	BCAST Service Provisioning – Client Component
<b>BSP-M</b>	BCAST Service Provisioning – Management Component
<b>CC</b>	Content Creation
<b>Cell ID</b>	Mobile network cell identification
<b>CID</b>	Content Identification
<b>CODEC</b>	Compressor/Decompressor
<b>CP</b>	Content Protection
<b>DRM RO</b>	Digital Rights Management Rights Object
<b>DT</b>	Date Time
<b>DVB-H</b>	Digital Video Broadcasting – Handhelds
<b>DVB-T</b>	Digital Video Broadcasting – Terrestrial
<b>FA</b>	File Application Component
<b>FD</b>	File Delivery Component
<b>FD-C</b>	File Delivery – Client Component
<b>FLUTE</b>	File Delivery over Unidirectional Transport

<b>IMS</b>	IP Multimedia Subsystem
<b>IN</b>	Interaction Network
<b>IP</b>	Internet Protocol
<b>IPSec</b>	IP Security
<b>ISMACryp</b>	ISMA Encryption and Authentication specification
<b>MBMS</b>	Multimedia Broadcast/Multicast Service
<b>MMS</b>	Multi-media Messaging
<b>MPEG2-TS</b>	Motion Pictures Expert Group 2 – Transport Stream
<b>MPEG-4</b>	Motion Pictures Expert Group 4
<b>MSISDN</b>	Mobile Subscriber ISDN number
<b>NT</b>	Notification Function
<b>NTC</b>	Notification Client Component
<b>NTDA</b>	Notification Distribution
<b>NTE</b>	Notification Event Component
<b>NTG</b>	Notification Generation Component
<b>OCSP</b>	Online Certificate Status Protocol
<b>OMA</b>	Open Mobile Alliance
<b>OMA BCAST</b>	OMA Digital Mobile Broadcast enabler
<b>OMA DM</b>	OMA Device Management enabler
<b>OMA DRM</b>	OMA Digital Rights Management enabler
<b>OMA LOC</b>	OMA Location enabler
<b>PEAK</b>	Program Encryption/Authentication Key
<b>RI</b>	Rights Issuer
<b>RO</b>	Rights Object
<b>ROAP</b>	Rights Object Acquisition Protocol
<b>RTCP</b>	RTP Control Protocol
<b>RTP</b>	Real-time Transport Protocol
<b>SA</b>	Stream Application Component
<b>SD</b>	Stream Delivery Component
<b>SD-C</b>	Stream Delivery Client Component
<b>SDP</b>	Session Description Protocol
<b>SEAK</b>	Subscription Encryption/Authentication Key
<b>SG</b>	Service Guide
<b>SGA</b>	Service Guide Adaptation

---

<b>SGAS</b>	Service Guide Application Source
<b>SG-C</b>	Service Guide Client Component
<b>SGCCS</b>	Service Guide Content Creation Source
<b>SGD</b>	Service Guide Distribution
<b>SG-G</b>	Service Guide Generation
<b>SG-G/D/A</b>	The entity of Service Guide Generation, Distribution and Adaptation components
<b>SGSS</b>	Service Guide Subscription Source
<b>SI</b>	Service Interaction
<b>SMS</b>	Short Message Service
<b>SP</b>	Service Protection
<b>SRTP</b>	Secure Real-time Transport Protocol
<b>TP-C</b>	Terminal Provisioning Client component
<b>TP-M</b>	Terminal Provisioning Management component
<b>UDP</b>	User Datagram Protocol
<b>URI</b>	Universal Resource Identified
<b>VLR</b>	Visitor Location Register
<b>XML</b>	Extensible Markup Language

## 4. Introduction

The purpose of this document is to provide interoperability test cases for “Mobile Broadcast Services version 1.0”.

## 5. BCAST Interoperability Test Cases

### 5.1 Service Provisioning

#### 5.1.1 Service bootstrap and single content

<b>Test Case Id</b>	BCAST-1.0-DIST-int-101
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Bootstrapping a service with content. Associating content with service. This test case also tests that the reception of the SG is performed correctly.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.1, 5.4.2, 6.1.
<b>SCR Reference</b>	BCAST-SG-C-002, BCAST-SG-C-004, BCAST-SG-C-008, BCAST-SG-C-010, BCAST-SG-C-011.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime of the content to match the test time.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>Start the BCAST application in the terminal and update the SG (if not done automatically).</li> <li>Browse the SG in the terminal</li> </ul>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>The SG is correctly received by the terminal.</li> </ul>

#### 5.1.2 Web-based Service Provisioning

<b>Test Case Id</b>	BCAST-1.0-DIST-int-102
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Use Web portal URL in Purchase fragment of Service Guide to provide entry point for web based provisioning.
<b>Specification Reference</b>	
<b>SCR Reference</b>	
<b>Tool</b>	
<b>Test code</b>	

<b>Preconditions</b>	<p>Set up a web portal that provides additional information and ability to handle provisioning requests from a terminal for a particular PurchaseChannel.</p> <p>Setup a Service Guide with a PurchaseChannel fragment identifying a PortalURL pointing to the entry point of a related web-based system.</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Start the BCAST application in the terminal and update the SG (if not done automatically).</li> <li>• Browse the SG in the terminal.</li> <li>• Select the service to subscribe.</li> <li>• Access portal related to the service.</li> </ul>
<b>Pass-Criteria</b>	<p>The following actions should be possible to perform</p> <ul style="list-style-type: none"> <li>• Browse service information presented by the portal.</li> <li>• The user is able to order the service through the portal.</li> <li>• The user is able to access the service.</li> </ul>

## 5.2 Service Guide

### 5.2.1 Service Guide update (same fragment id, higher version number) – Broadcast Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-103
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Updating description of content. This test case also tests that the update of the SG is performed correctly.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.4.2.1.2.
<b>SCR Reference</b>	BCAST-SG-C-013
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime of the content to match the test time.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal.</li> <li>• Browse the SG on the terminal</li> <li>• Update the SG in the server to contain a newer version of the content (Content Fragment has a higher version number)</li> <li>• Update the SG in the terminal.</li> <li>• Browse the SG in the terminal</li> <li>• View the updated programme.</li> </ul>

<b>Pass-Criteria</b>	<p>The following things should be visible to the end user after the first update of the SG</p> <ul style="list-style-type: none"> <li>• The SG is visible and contains a programme.</li> </ul> <p>The following things should be visible to the end user after the second update of the SG</p> <ul style="list-style-type: none"> <li>• The SG is visible and contains an updated version of the programme.</li> <li>• The updated programme can be received by the terminal.</li> </ul>
----------------------	--

### 5.2.2 Service Guide update (same fragment id, higher version number) – Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-104
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Updating description of content. This test case also tests that the update of the SG is performed correctly.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.4.2.1.2.
<b>SCR Reference</b>	BCAST-SG-C-014
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime of the content to match the test time.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal.</li> <li>• Browse the SG on the terminal</li> <li>• Update the SG in the server to contain a newer version of the content (Content Fragment has a higher version number)</li> <li>• Update the SG in the terminal.</li> <li>• Browse the SG in the terminal</li> <li>• View the updated programme.</li> </ul>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user after the first update of the SG</p> <ul style="list-style-type: none"> <li>• The SG is visible and contains a programme.</li> </ul> <p>The following things should be visible to the end user after the second update of the SG</p> <ul style="list-style-type: none"> <li>• The SG is visible and contains an updated version of the programme.</li> <li>• The updated programme can be received by the terminal.</li> </ul>

### 5.2.3 Service Guide Update (new fragment id) – Broadcast Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-105
<b>Test Object</b>	BCAST Terminal and Server

<b>Test Case Description</b>	Applying the associated access and session description parameters with content.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.4.2.1.1.
<b>SCR Reference</b>	BCAST-SG-C-013
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime of the content to match the test time.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal.</li> <li>• Browse the SG in the terminal</li> <li>• Update the SG in the server to contain a new programme.</li> <li>• Update the SG in the terminal.</li> <li>• Browse the SG in the terminal</li> <li>• Select the new programme and start viewing it.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• After the first update the SG is available and contains all the available programs.</li> <li>• After the second update the SG, all the previous programmes and the new programme are available and can be viewed by the terminal.</li> </ul>

## 5.2.4 Service Guide Update (new fragment id) – Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-106
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Applying the associated access and session description parameters with content.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.4.2.1.1.
<b>SCR Reference</b>	BCAST-SG-C-014
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime of the content to match the test time.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal.</li> <li>• Browse the SG in the terminal</li> <li>• Update the SG in the server to contain a new programme.</li> <li>• Update the SG in the terminal.</li> <li>• Browse the SG in the terminal</li> <li>• Select the new programme and start viewing it.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• After the first update the SG is available and contains all the available programs.</li> <li>• After the second update the SG, all the previous programmes and the new programme are available and can be viewed by the terminal.</li> </ul>



## 5.2.5 GZIP compression of Service Guide Delivery Unit

<b>Test Case Id</b>	BCAST-1.0-DIST-int-107
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Testing the case where the SGDU is GZIP compressed.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.4.1.4.
<b>SCR Reference</b>	BCAST-SG-C-009
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. All fragments are packaged in SGDUs, which are GZIP compressed.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• View the programme.</li> </ul>
<b>Pass-Criteria</b>	The following things should be visible to the end user <ul style="list-style-type: none"> <li>• The SG and the programme can be received by the terminal.</li> </ul>

## 5.2.6 Content hierarchy

<b>Test Case Id</b>	BCAST-1.0-DIST-int-108
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating content with service.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.1.
<b>SCR Reference</b>	BCAST-SG-C-002, BCAST-SG-C-004
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	There are two consecutive programmes in the SG. The StartTime and EndTime of these match the test time (e.g. first programme 2:00-2:05 PM and second programme 2:05-2:15 PM).
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• View the programmes.</li> </ul>

<b>Pass-Criteria</b>	The following things should be visible to the end user <ul style="list-style-type: none"> <li>• There are two consecutive programmes in the SG.</li> <li>• Both programmes can be seen, one after the other at the right time.</li> </ul>
----------------------	---

## 5.2.7 PreviewData and Service – Broadcast Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-109
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating preview data with service.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.1.2.9
<b>SCR Reference</b>	BCAST-SG-C-005
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a preview icon associated with the SG
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> </ul>
<b>Pass-Criteria</b>	In case the terminal displays icons associated with service, the service should be coupled with an icon.

## 5.2.8 PreviewData and Service – Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-110
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating preview data with service.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.1.2.9
<b>SCR Reference</b>	BCAST-SG-C-006
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a preview icon associated with the SG
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> </ul>

<b>Pass-Criteria</b>	In case the terminal displays icons associated with service, the service should be coupled with an icon.
----------------------	--

## 5.2.9 Select language specific access parameters

<b>Test Case Id</b>	BCAST-1.0-DIST-int-111
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Applying the associated access and session description parameters with content choose the correct parameters for a specific choice of language.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 7.2.
<b>SCR Reference</b>	BCAST-SG-C-002, BCAST-SG-C-004 Appendix C.3 (informative)
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There are several audio languages for a programme.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that has several audio languages.</li> <li>• Change the audio language of the programme.</li> </ul>
<b>Pass-Criteria</b>	The SG is visible and the video and audio streams in the selected programme can be rendered correctly by the terminal. The audio language of the programme can be changed, depending on the selection.

## 5.2.10 Subscription of Service

<b>Test Case Id</b>	BCAST-1.0-DIST-int-112
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating Service with provisioning information and applying the latter for subscription.
<b>Specification Reference</b>	[BCAST10 –ESG] Section 5.1.2.6.
<b>SCR Reference</b>	BCAST-SG-C-002, BCAST-SG-C-004
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime of the content to match the test time. subscriptionType is open-ended.

<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a service.</li> <li>• Try to subscribe to the same service again.</li> <li>• Try to stream the programme in the selected service.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service. The terminal registers the service as subscribed.</li> <li>• The user is not able to subscribe to the same service again.</li> <li>• The user can stream the programme within the subscribed service.</li> </ul>

## 5.3 File and Stream Distribution

### 5.3.1 File Distribution

#### 5.3.1.1 Support of ALC protocol and delivery of meta-data in the Service Guide

<b>Test Case Id</b>	BCAST-1.0-DIST-int-201
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	To test the support of ALC and the interpretation of the file description information on the Service Guide
<b>Specification Reference</b>	[BCAST10-Distribution] Section 5.2
<b>SCR Reference</b>	BCAST-FD-C-001, BCAST-FD-C-002, BCAST-FD-C-003, BCAST-FD-C-005, BCAST-FD-C-007, BCAST-FD-C-008, BCAST-FD-C-011, BCAST-FD-C-012, BCAST-FD-S-001, BCAST-FD-S-002, BCAST-FD-S-003, BCAST-FD-S-004, BCAST-FD-S-005, BCAST-FD-S-006, BCAST-FD-S-008, BCAST-FD-S-009, BCAST-FD-S-012, BCAST-FD-S-013
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	<p>Set up the Service Guide delivery to use</p> <ul style="list-style-type: none"> <li>• Broadcast channel</li> </ul> <p>The file 1 is available on the broadcast channel</p> <p style="padding-left: 40px;">The Access fragment describes the file delivery session, to be done through the broadcast channel</p> <p style="padding-left: 40px;">File is GZIP encoded</p> <p style="padding-left: 40px;">Compact No-Code FEC is used</p> <p style="padding-left: 40px;">Ipv4 is used</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file 1 to download</li> <li>• Wait for the file download</li> </ul> <p>Note: file1 can be a jpg picture</p>

<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service “FILE1” that contains a file “File1”</li> <li>• The file is successfully downloaded to the terminal</li> </ul> <p>Note: To verify the file was correctly downloaded the picture should be correctly displayed</p>
----------------------	---

### 5.3.1.2 Support of in-band delivery of meta-data and FLUTE

<b>Test Case Id</b>	BCAST-1.0-DIST-int-202
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	To test the support of the in-band delivery of the metadata associated with file distributed using FLUTE
<b>Specification Reference</b>	[BCAST10-Distribution] Section 5.2
<b>SCR Reference</b>	BCAST-FD-C-006, BCAST-FD-C-010, BCAST-FD-S-007, BCAST-FD-S-011
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	<p>Set up the Service Guide delivery to use</p> <ul style="list-style-type: none"> <li>• Broadcast channel <ul style="list-style-type: none"> <li>The access fragment refers a valid Flute Session Descriptor</li> <li>File is GZIP encoded</li> </ul> </li> </ul>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file 2 to download</li> <li>• Wait for the file download</li> </ul> <p>Note: file2 can be a jpg picture</p>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service “FILE2” that contains a file “File2”</li> <li>• The file is successfully downloaded to the terminal</li> </ul> <p>Note: To verify the file was correctly downloaded the picture should be correctly displayed</p>

### 5.3.1.3 Support the delivery using HTTP over Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-203
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	To test the support of the delivery of a file using http over the interaction channel
<b>Specification Reference</b>	[BCAST10-Distribution] Section 5.2
<b>SCR Reference</b>	BCAST-FD-C-016, BCAST-FD-C-017, BCAST-FD-C-020, BCAST-FD-C-021, BCAST-FD-C-023, BCAST-FD-C-023, BCAST-FD-S-026, BCAST-FD-S-028, BCAST-FD-S-029, BCAST-FD-S-030, BCAST-FD-S-031, BCAST-FD-S-032

<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	Set up the Service Guide The access fragment refers a valid URI and correctly states that the transport type is http File is GZIP encoded
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file 3 to download</li> <li>• Wait for the file download</li> </ul> Note: file3 can be a jpg picture
<b>Pass-Criteria</b>	The following things should be visible to the end user <ul style="list-style-type: none"> <li>• There is a service “FILE3” that contains a file “File3”</li> <li>• The file is successfully downloaded to the terminal</li> </ul> Note: To verify the file was correctly downloaded the picture should be correctly displayed

#### 5.3.1.4 Support of FEC RAPTOR

<b>Test Case Id</b>	BCAST-1.0-DIST-int-204
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test the support of the FEC encoding ID 1 scheme
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 5.2.2
<b>SCR Reference</b>	BCAST-FD-C-007, BCAST-FD-C-009, BCAST-FD-S-008, BCAST-FD-S-010
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	Set up the Service Guide The access fragment refers a valid Flute Session Descriptor File is GZIP encoded The Forward Correction Error used is the FEC RAPTOR scheme The file is downloaded over the broadcast channel
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file4 to download</li> <li>• Wait for the file download</li> </ul> Note: file 4 can be a jpg picture
<b>Pass-Criteria</b>	The following things should be visible to the end user <ul style="list-style-type: none"> <li>• There is a service “FILE4” that contains a file “File4”</li> <li>• The file is successfully downloaded to the terminal</li> </ul> Note: To verify the file was correctly downloaded the picture should be correctly displayed

### 5.3.1.5 Support of the post-delivery repair of files

<b>Test Case Id</b>	BCAST-1.0-DIST-int-205
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test if the file repair is correctly performed
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 5.3.3
<b>SCR Reference</b>	BCAST-FD-C-014, BCAST-FD-C-015, BCAST-FD-S-015, BCAST-FD-S-016
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	Set up the Service Guide <p style="text-align: center;">The access fragment refers a valid Flute File Descriptor and a valid Associated Delivery Procedure with the relevant file repair information</p> <p style="text-align: center;">A repair server is available</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file 2 to download</li> <li>• The file is downloaded but some file fragments are not send on purpose</li> <li>• Wait for the file repair procedure</li> </ul> <p>Note: file 2 can be a jpg picture</p>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service “FILE2” that contains a file “File2”</li> <li>• The file is incompletely downloaded to the terminal</li> <li>• The terminal enters the repair procedure and the file is successfully downloaded for the second time</li> </ul> <p>Note: To verify the file was correctly downloaded the picture should be correctly displayed</p>

### 5.3.1.6 Support of reception report

<b>Test Case Id</b>	BCAST-1.0-DIST-int-206
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test the report of the reception of a successful download
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 5.3.2
<b>SCR Reference</b>	BCAST-FD-C-013, BCAST-FD-C-015, BCAST-FD-S-014, BCAST-FD-S-016
<b>Tool</b>	
<b>Test code</b>	

<b>Preconditions</b>	<p>Set up the Service Guide</p> <p>The access fragment refers a valid Flute File Descriptor and a valid Associated Delivery Procedure with the postReceptionReport element and the report type to StaR and the samplePercentage to 100</p> <p>There is a reception report server available</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file 2 to download</li> <li>• The file is downloaded successfully</li> </ul> <p>Note: file 2 can be a jpg picture</p>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service “FILE2” that contains a file “File2”</li> <li>• The file is successfully downloaded</li> <li>• The terminal reports the successful download of the file</li> </ul> <p>Note: To verify the file was correctly downloaded the picture should be correctly displayed</p>

### 5.3.1.7 Support of Flute Session Setup and Control with RTSP

<b>Test Case Id</b>	BCAST-1.0-DIST-int-207
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test the report of the SDP handling and control with RTSP
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 5.5.1.1
<b>SCR Reference</b>	N/A
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	<p>Set up the Service Guide</p> <p>Note: All the fragments are associated with the same Service fragment.</p> <p>The access fragment refers a valid Flute File Descriptor with a valid control URI</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the file 5 to download</li> <li>• The user request the file to play</li> <li>• The user request the playing of the file to pause after the rendering has started</li> <li>• The user resumes the rendering of the file by requesting the file to play</li> <li>• The user give up on rendering the file</li> </ul> <p>Note: file 5 must be a video or music file, 3gpp and mp3 file types are recommended</p>



<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service “FILE5” that contains a file “File5”</li> <li>• When the user request to play the file, the transmission starts followed by a rendering of the file</li> <li>• The rendering of the file is correctly paused on request</li> <li>• The rendering of the file is correctly resumed on user request</li> <li>• The rendering of the file is correctly stopped on user request and the transmission ceased.</li> </ul>
----------------------	---

## 5.3.2 Streaming Distribution

### 5.3.2.1 Support of RTP for stream distribution over the broadcast channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-208
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test the supports of RTP as a transport protocol for streaming distribution over the broadcast channel
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 6.2
<b>SCR Reference</b>	BCAST-SD-C-001, BCAST-SD-C-002, BCAST-SD-C-003, BCAST-SD-C-004, BCAST-SD-C-006, BCAST-SD-C-007, BCAST-SD-C-008, BCAST-SD-C-009, BCAST-SD-S-001, BCAST-SD-S-001, BCAST-SD-S-002, BCAST-SD-S-003, BCAST-SD-S-004, BCAST-SD-S-005, BCAST-SD-S-007, BCAST-SD-S-008, BCAST-SD-S-009, BCAST-SD-S-010
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	<p>Set up the Service Guide</p> <p style="padding-left: 40px;">The access fragment refers a valid SDP Session Descriptor</p> <p style="padding-left: 40px;">The SDP points a stream available on broadcast channel</p> <p style="padding-left: 40px;">The SDP has the RTCP receiver reports turned off</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the stream 1 to render</li> <li>• The stream starts to be correctly rendered</li> <li>• The server sends the RTCP packets (sender reports)</li> </ul> <p>Note: stream 1 must be a video or music file, 3gpp and mp3 file types are recommended</p>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service “STREAM1” that contains a service “Stream1”</li> <li>• The rendering of the stream starts correctly</li> </ul>

### 5.3.2.2 Support of RTP for stream distribution over the interactive channel using SDP

<b>Test Case Id</b>	BCAST-1.0-DIST-int-209
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test the support of RTP as a transport protocol for streaming distribution on the interactive channel using SDP
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 6.2
<b>SCR Reference</b>	BCAST-SD-C-016, BCAST-SD-C-017, BCAST-SD-C-018, BCAST-SD-S-026, BCAST-SD-S-027, BCAST-SD-S-028
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	Set up the Service Guide <ul style="list-style-type: none"> <li>The access fragment refers a valid SDP Session Descriptor</li> <li>The SDP points a stream available on interactive channel</li> <li>The SDP has the RTCP receiver reports turned off</li> </ul>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the stream 2 to render</li> <li>• The stream starts to be correctly rendered</li> <li>• The server sends the RTCP packets (sender reports)</li> </ul> <p>Note: stream 2 must be a video or music stream, 3gpp and mp3 file types are recommended</p>
<b>Pass-Criteria</b>	The following things should be visible to the end user <ul style="list-style-type: none"> <li>• There is a service “STREAM2” that contains a service “Stream2”</li> <li>• The rendering of the stream starts correctly</li> <li>• The terminal does not send RTCP packets (receiver reports)</li> </ul>

### 5.3.2.3 Support of RTP for stream distribution over the interactive channel using HTTP with out-of-band signalling

<b>Test Case Id</b>	BCAST-1.0-DIST-int-210
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test the support of RTP as a transport protocol for streaming distribution over the interactive channel using HTTP and out-of-band signalling
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 6.7
<b>SCR Reference</b>	BCAST-SD-C-017, BCAST-SD-C-014, BCAST-SD-S-015
<b>Tool</b>	
<b>Test code</b>	

<b>Preconditions</b>	<p>Set up the Service Guide</p> <p>The access fragment has all the description information for the streaming session</p> <p>The media type of stream 3 doesn't have a corresponding RTP definition</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the stream 3 to render</li> <li>• The stream starts to be correctly rendered</li> </ul> <p>Note: stream 3 must be a video or music file, 3gpp and mp3 file types are recommended</p>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service "STREAM3" that contains a service "Stream3"</li> <li>• The rendering of the stream starts correctly</li> </ul>

#### 5.3.2.4 Support of streaming associated procedure

<b>Test Case Id</b>	BCAST-1.0-DIST-int-211
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to test the support of the streaming associated procedure
<b>Specification Reference</b>	[BCAST10-Distribution] – Section 6.8.1
<b>SCR Reference</b>	BCAST-SD-C-013, BCAST-SD-S-014
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	<p>Set up the Service Guide</p> <p>The access fragment refers a valid SDP Session Descriptor and a URI for an streaming associated procedure description</p> <p>The streaming associated procedure description is valid and requests a fixed duration based measurements</p>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal and select the stream 4 to render</li> <li>• The stream starts to be correctly rendered</li> <li>• The server receives the correct streaming reception reports at the requested time</li> </ul> <p>Note: stream 4 must be a video or music file, 3gpp and mp3 file types are recommended</p>
<b>Pass-Criteria</b>	<p>The following things should be visible to the end user</p> <ul style="list-style-type: none"> <li>• There is a service "STREAM2" that contains a service "Stream2"</li> <li>• The rendering of the stream starts correctly</li> <li>• The terminal does not send RTCP packets (receiver reports)</li> </ul>

## 5.4 Service Interaction

### 5.4.1 XHTML MP Interactivity – Broadcast Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-301
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating content with interactivity. Reception of InteractivityMediaDocuments over broadcast file distribution. XHTML MP as an interaction method.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.3.6, 5.3.6.1.5.
<b>SCR Reference</b>	BCAST-SG-C-003, BCAST-SERVICES-C-013, BCAST-SERVICES-C-019, BCAST-SERVICES-C-022
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. The terminal supports XHTML MP as an interaction method.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that contains XHTML MP interactivity.</li> <li>• Use the XHTML MP interactivity.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• User is able to use the XHTML MP interactivity.</li> <li>• The user input is correctly received by the recipient.</li> <li>• The XHTML MP interactivity can be used without interrupting the “regular” broadcast stream.</li> </ul>

### 5.4.2 XHTML MP Interactivity – Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-302
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating content with interactivity. Retrieval of InteractivityMediaDocuments over interaction channel. XHTML MP as an interaction method.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.3.6, 5.3.6.1.5.
<b>SCR Reference</b>	BCAST-SG-C-003, BCAST-SERVICES-C-013, BCAST-SERVICES-C-020, BCAST-SERVICES-C-022
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. The terminal supports XHTML MP as an interaction method.

<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that contains XHTML MP interactivity.</li> <li>• Use the XHTML MP interactivity.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• User is able to use the XHTML MP interactivity.</li> <li>• The user input is correctly received by the recipient.</li> <li>• The XHTML MP interactivity can be used without interrupting the “regular” broadcast stream.</li> </ul>

### 5.4.3 SMS interactivity – Broadcast Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-303
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating content with interactivity. Reception of InteractivityMediaDocuments over broadcast file distribution. SMS as an interaction method.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.3.6, 5.3.6.1.6.
<b>SCR Reference</b>	BCAST-SG-C-003, BCAST-SERVICES-C-014, BCAST-SERVICES-C-019, BCAST-SERVICES-C-022
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. The terminal supports SMS.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that contains SMS interactivity.</li> <li>• Use the SMS interactivity.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• User is able to use the SMS interactivity.</li> <li>• The recipient receives an SMS from the terminal formatted correctly according to the SMS template and it contains the user input.</li> <li>• The SMS interactivity can be used without interrupting the “regular” broadcast stream.</li> </ul>

### 5.4.4 SMS interactivity – Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-304
<b>Test Object</b>	BCAST Terminal and Server

<b>Test Case Description</b>	Associating content with interactivity. Retrieval of InteractivityMediaDocuments over interaction channel. SMS as an interaction method.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.3.6, 5.3.6.1.6.
<b>SCR Reference</b>	BCAST-SG-C-003, BCAST-SERVICES-C-014, BCAST-SERVICES-C-020, BCAST-SERVICES-C-022
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. The terminal supports SMS.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that contains SMS interactivity.</li> <li>• Use the SMS interactivity.</li> </ul>

#### 5.4.5 MMS Interactivity – Broadcast Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-305
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating content with interactivity. Reception of InteractivityMediaDocuments over broadcast file distribution. MMS as an interaction method.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.3.6, 5.3.6.1.7.
<b>SCR Reference</b>	BCAST-SG-C-003, BCAST-SERVICES-C-015, BCAST-SERVICES-C-019, BCAST-SERVICES-C-022 Adaptation requirements:
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. The terminal supports MMS Template.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that contains MMS interactivity.</li> <li>• Use the MMS interactivity.</li> </ul>

<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• User is able to use the MMS interactivity.</li> <li>• The recipient receives an MMS from the terminal formatted correctly according to the MMS Template and it contains the the user input.</li> <li>• The MMS interactivity can be used without interrupting the “regular” broadcast stream.</li> </ul>
----------------------	---

## 5.4.6 MMS Interactivity – Interaction Channel

<b>Test Case Id</b>	BCAST-1.0-DIST-int-306
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Associating content with interactivity. Retrieval of InteractivityMediaDocuments over interaction channel. MMS as an interaction method.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.3.6, 5.3.6.1.7.
<b>SCR Reference</b>	BCAST-SG-C-003, BCAST-SERVICES-C-015, BCAST-SERVICES-C-020, BCAST-SERVICES-C-022 Adaptation requirements:
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. The terminal supports MMS Template.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal</li> <li>• Browse the SG in the terminal</li> <li>• Select a programme that contains MMS interactivity.</li> <li>• Use the MMS interactivity.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• User is able to use the MMS interactivity.</li> <li>• The recipient receives an MMS from the terminal formatted correctly according to the MMS Template and it contains the the user input.</li> <li>• The MMS interactivity can be used without interrupting the “regular” broadcast stream.</li> </ul>

## 5.5 Service and Content Protection

### 5.5.1 DRM Profile

#### 5.5.1.1 Delivery of IPsec protected stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-401
<b>Test Object</b>	BCAST Terminal and Server

<b>Test Case Description</b>	Opening an Ipv4 encrypted stream with key material associated to the subscription.
<b>Specification Reference</b>	[BCAST10–ServContProt] Section 9.1. [BCAST10–ServContProt] Section 5.6.1
<b>SCR Reference</b>	BCAST-SPCP-C-002, BCAST-ContentLayer-C-008, BCAST-SDP-C-014. BCAST-TerminalCapability-C-004, BCAST-SPCP-C-006, BCAST-STKM –C-011, BCAST-LTKM_DRM-C-013, BCAST-CP_RTP_DRM-C-019.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a service which is IPsec encrypted. subscriptionType is open-ended.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a IPsec protected service</li> <li>• View an IPsec encrypted programme.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service.</li> <li>• The terminal registers the service to be subscribed and disallows the end user to subscribe again.</li> <li>• The terminal is able to decrypt and render the IPsec encrypted audio and video streams belonging to the programme.</li> </ul>

### 5.5.1.2 Delivery of SRTP protected stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-402
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Opening an SRTP encrypted stream with key material associated to the subscription.
<b>Specification Reference</b>	[BCAST10–ServContProt] Section 9.2. [BCAST10–ServContProt] Section 5.6.1
<b>SCR Reference</b>	BCAST-SPCP-C-002, BCAST-ContentLayer-C-007, BCAST-SDP-C-014, BCAST-SRTPsignal-C-030. BCAST-TerminalCapability-C-004, BCAST-SPCP-C-006, BCAST-STKM –C-011, BCAST-LTKM_DRM-C-013, BCAST-CP_RTP_DRM-C-019.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a service which is SRTP encrypted. subscriptionType is open-ended.



<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a SRTP protected service</li> <li>• View an SRTP encrypted programme.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service.</li> <li>• The terminal registers the service to be subscribed and disallows the end user to subscribe again.</li> <li>• The terminal is able to decrypt and render the SRTP encrypted audio and video streams belonging to the programme.</li> </ul>

### 5.5.1.3 Delivery of ISMACrypt protected stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-403
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Opening an ISMACrypt encrypted stream with key material associated to the subscription.
<b>Specification Reference</b>	[BCAST10–ServContProt] Section 9.3. [BCAST10–ServContProt] Section 5.6.1.
<b>SCR Reference</b>	BCAST-SPCP-C-002, BCAST-ContentLayer-C-009, BCAST-SDP-C-014, BCAST-CP_Form-C-023. BCAST-TerminalCapability-C-004, BCAST-SPCP-C-006, BCAST-STKM –C-011, BCAST-LTKM_DRM-C-013, BCAST-CP_RTP_DRM-C-019.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a service which is ISMACrypt encrypted. subscriptionType is open-ended.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a ISMACrypt protected service</li> <li>• View an ISMACrypt encrypted programme.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service.</li> <li>• The terminal registers the service to be subscribed and disallows the end user to subscribe again.</li> <li>• The terminal is able to decrypt and render the Ipsec encrypted audio and video streams belonging to the programme.</li> </ul>

## 5.5.2 Smartcard Profile

### 5.5.2.1 Layer 1 Authentication and Service Registration

3G Authentication used in bootstrapping procedures:

Authentication between the UE and the BSF needs a valid cellular subscription. Authentication is based on the 3GPP AKA protocol.

The use of a well specified algorithm for the 3GPP Authentication and Key Agreement (AKA) could be used to avoid the use of operator specific cards. This well specified algorithm is described in the TS 35 206 specification and is called MILENAGE. This algorithm will be implemented in the USIM card. If operator cellular network is used then the algorithm needs to be known and implemented in the smartcard.

The USIM contains also a permanent user identifier: IMSI and a secret key K shared with the Authentication Center (AuC).

The use of test data proposed by the TS 35 207-700 (Implementor's Test Data) and TS 35 208-700 (Design Conformance Test Data) could facilitate the computing of valid Authentication Vectors for the HSS in case the HSS is simulated and to verify the return values.

In case a (R-)UIM/CSIM is used, the pre-provisioned key based mechanism using Registration Key (RK), as specified in 3GPP2 for BCMCS, SHALL be implemented. Authentication between the BCAST Terminal and the BSM presumes a valid cellular subscription. In case the BSM wishes to authenticate the terminal, it uses the Auth-Key computed from RK. On the terminal side, Auth-Key is computed in the (R-)UIM/CSIM. Such computation is specified in [3GPP2 S.S0083-A]. Furthermore, this authentication is performed using a challenge-response protocol, also specified in [3GPP2 S.S0083-A].

In this chapter, "BCAST Smartcard" means "MBMS/BCAST or BCMCS/BCAST smartcard".

#### 5.5.2.1.1 GBA-U Bootstrapping USIM /BSM with success

<b>Test Case Id</b>	BCAST-1.0-DIST-int-404
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or BCAST
<b>Test Case Description</b>	Test that GBA bootstrapping with the BSM is successfully achieved. Test that the SRK is correctly generated in the terminal. Smartcard is MBMS only or MBMS/BCAST.
<b>Specification Reference</b>	SPCP spec: 6.10, 6.5
<b>SCR Reference</b>	BCAST-SPCP-C-005, BCAST-KeyManagement-C-016
<b>Tool</b>	none
<b>Test code</b>	

<b>Preconditions</b>	<ul style="list-style-type: none"><li>○ No bootstrapping context exists between BSM and terminal/smartcard</li><li>○ Smartcard contains Key management: Smartcard is GBA and MBMS or BCAST enabled</li><li>○ Smartcard contains a valid 3G subscription (IMSI/K and algo Milenage)</li><li>○ HSS is able to provide Authentication Vectors (AV, AV=RAND  AUTN  XRES  CK  IK) associated with the IMSI/K.</li><li>○ Session description fragment contains MBMS USD with a service protection description fragment containing<ul style="list-style-type: none"><li>○ the key management element with a key management server definition.</li><li>○ And the attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service.</li></ul></li><li>○ Or the information are provided using the SDP.</li><li>○ The Service Guide declares a service for which subscription is possible, allowing the Terminal to send a Service Registration</li></ul>
----------------------	---

**Test Procedure**

1. Update the SG in the terminal using the BSM as the source
2. User selects the service for subscription
3. Terminal retrieves, in the USD, FQDN of the key management server (BSM), the uiccKeyManagement indication, identifiers of MSKs for the user service (Key domain ID and MSK ID)
4. Terminal detects that a bootstrapping procedure is needed (no SRK available)
5. The Terminal and the BSF establish bootstrapped security association between them by running bootstrapping procedure
  - a. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity.(IMPI found in the USIM derived from IMSI as specified in TS 23 003)
  - b. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102)
  - c. The BSF selects an authentication vector AV=  
RAND||AUTN||XRES||CK||IK
  - d. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND||AUTN
  - e. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode
  - f. The USIM sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid).
  - g. Terminal sends an HTTP request, containing the Digest AKA response calculated using RES, to the BSF.
  - h. BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI
  - i. BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal
  - j. The terminal stores B-TID and key lifetime in the EF<sub>GBABP</sub>

At this time BSF and USIM share bootstrap Key material KS associated with B-TID
6. Terminal initiates an HTTP digest authentication using the User service registration procedure and information in USD or SDP and establish an IP connection with the BSM.
  - a. Terminal sends a GET request to the BSM to gain access to a service and to establish an IP connection with the BSM.
  - b. The BSM answer with 401 Unauthorized indicating that the BSM choose to AUTHENTICATE the terminal using the bootstrapped security association
  - c. Key derivation: Terminal sends NAF\_ID and IMPI to USIM using the AUTHENTICATE command in GBA security context: NAF derivation mode.
  - d. USIM derives Ks\_ext\_NAF (SRK) and Ks\_Int\_NAF (SMK), updates the EF<sub>GBANL</sub> and sends back to the terminal the Ks\_ext\_NAF (SRK).
  - e. The terminal sends to the BSM a GET request with B-TID as username and Ks\_ext\_NAF (SRK) as password
  - f. BSM retrieves Ks\_ext\_NAF from the BSF and verifies the message received from the terminal.
  - g. If success the BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each service.

<b>Pass-Criteria</b>	<ol style="list-style-type: none"> <li>1. reception at BSF of a GET request from Terminal with the appropriate IMPI</li> <li>2. reception at BSF of a correct authentication challenge response in the Second GET request with RES (compared with the test data proposed in TS 35 207 and TS 35 208)</li> <li>3. Reception at BSM of a correct GET request from the terminal a 200OK message is sent back to the terminal. This ensures that the Ks derivation is correct as the SRK is correct.</li> </ol>
----------------------	---

**5.5.2.1.2 GBA-U Bootstrapping USIM / BSM with synchronization error**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-405
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or MBMS/BCAST
<b>Test Case Description</b>	Test that SQN error is detected by the terminal during a GBA bootstrapping Smartcard is MBMS only or MBMS/BCAST
<b>Specification Reference</b>	SPCP spec: 6.10, 6.5
<b>SCR Reference</b>	BCAST-SPCP-C-005, BCAST-KeyManagement-C-016
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ A bootstrapping context exists between BSM and terminal/smartcard (the test 1.1.1 has been run first) but the lifetime of the key has expired.</li> <li>○ Smartcard contains Key management Smartcard is GBA and MBMS or BCAST enabled</li> <li>○ Session description fragment contains MBMS USD with a service protection description fragment containing             <ul style="list-style-type: none"> <li>○ The key management element with a key management server definition.</li> <li>○ And the attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service.</li> <li>○ Or the information are provided using the SDP.</li> </ul> </li> <li>○ The Service Guide declares a service for which subscription is possible, allowing the Terminal to send a Service Request</li> <li>○ Authentication vector AV stored in HSS contains an error in the AUTN: SQN is the same as for the test 1.1.1 that run first. Then SQN is false</li> </ul>

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Update the SG in the terminal using the BSM as the source</li> <li>2. User selects the service for subscription</li> <li>3. Terminal retrieves, in the USD or SDP, FQDN of the key management server (BSM), the uiccKeyManagement indication, identifiers of MSKs for the user service (Key domain ID and MSK ID)</li> <li>4. Terminal detects that a bootstrapping procedure is needed (Key lifetime has expired)</li> <li>5. The Terminal and the BSF establish bootstrapped security association between them by running bootstrapping procedure <ol style="list-style-type: none"> <li>a. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity.(IMPI found in the USIM)</li> <li>b. The BSF retrieves Authentication vector from the HSS</li> <li>c. The BSF selects an authentication vector AV= RAND  AUTN  XRES  CK  IK</li> <li>d. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND  AUTN containing an error in SQN (same SQN as for the test 1.1.1)</li> <li>e. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode</li> <li>f. The USIM verifies MAC and SQN from AUTN and the SQN value is invalid. USIM computes AUTS</li> <li>g. USIM sends the response of AUTHENTICATE command: AUTS: SQN is invalid (Synchronization error)</li> <li>h. Terminal sends AUTS back to the BSF in GET request</li> <li>i. BSF gets the corresponding AV (indicated by the AUTS) from the HSS and selects the AV</li> <li>j. BSF sends a new 401 Unauthorized response with another challenge based on the new range of sequence number: RAND  AUTN (go to step 5.d of previous test with success) .....</li> </ol> </li> </ol>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>○ reception at BSF of a GET request from Terminal with the appropriate IMPI</li> <li>○ reception at BSF of AUTS in the second GET request</li> </ul>

### 5.5.2.1.3 GBA\_U: Expired Bootstrapping data

<b>Test Case Id</b>	BCAST-1.0-DIST-int-406
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or MBMS/BCAST.
<b>Test Case Description</b>	<p>Test that correct behaviour is observed when bootstrapping data has expired.</p> <p>Test that a new SRK is correctly generated in the terminal. Smartcard is MBMS only or MBMS/BCAST</p>
<b>Specification Reference</b>	SPCP spec 6.5.1
<b>SCR Reference</b>	BCAST-SPCP-C-005
<b>Tool</b>	None

Test code	None
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ A bootstrapping context exists between server and terminal/smartcard</li> <li>○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS security enabled).</li> <li>○ Smartcard contains a valid 3G subscription (IMSI/K and also Milenage)</li> <li>○ HSS also contains the secret K associated with the IMSI/IMPI</li> <li>○ The URLs of the GBA and registration servers must be available to the terminal. This can be provided via an access and session description fragment (or MBMS USD in SDP) containing the following information or in some other way (e.g. hard coding URLs in the terminal) for the purposes of testing. <ul style="list-style-type: none"> <li>○ The key management element with a key management server definition.</li> <li>○ The attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service.</li> <li>○ The key management server with which the terminal should register.</li> </ul> </li> <li>○ The terminal can be prompted to perform GBA bootstrapping and MBMS user registration either via the service guide and services interaction or in another fashion for testing purposes.</li> <li>○ A value for the ServiceID field in the registration request should be agreed by the terminal and server. This value should be one or more valid concatenation of a GlobalPurchaseItemID and a PurchaseDataReference. This can be done via a previous Service Request flow or by using pre-defined data.</li> <li>○ The BSM wishes to renegotiate bootstrapping, i.e. the key lifetime has expired on the BSM side.</li> </ul>

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. The BCAST client is started, re-activated or otherwise prompted to start user registration.</li> <li>2. The terminal/smartcard initiates user Registration (using information in the USD or SDP to get the BSM FQDN) by sending an MBMS user registration request to the BSM's NAF. The GET request contains the latest BT-ID as the user name and the current SRK as the password.</li> <li>3. The BSM returns a 401 unauthorised response in order to force the terminal to perform bootstrapping.</li> <li>4. The terminal/smartcard and the BSF establish bootstrapped security association between them by running bootstrapping procedure. <ol style="list-style-type: none"> <li>a. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity.(IMPI found in the USIM derived from IMSI as specified in TS 23 003)</li> <li>b. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102)</li> <li>c. The BSF selects an authentication vector AV= RAND  AUTN  XRES  CK  IK</li> <li>d. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND  AUTN</li> <li>e. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode</li> <li>f. The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK</li> <li>g. USIM sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid).</li> <li>h. Terminal sends challenge response back to the BSF in GET request</li> <li>i. BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI</li> <li>j. BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal</li> <li>k. The terminal stores B-TID and key lifetime in the EF<sub>GBABP</sub></li> </ol> </li> <li>5. The terminal/smartcard reissues the MBMS User registration request to the BSM using the new BT-ID and Ks_ext_NAF (SRK)</li> <li>6. .The BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each service.</li> </ol>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• Reception at BSF of a GET request from Terminal with the appropriate IMPI to kick off bootstrapping.</li> <li>• The BSM's NAF receives an MBMS User registration request containing the new BT-ID and SRK.</li> <li>• A 200 OK message is sent back to the terminal from the BSM to indicate the successful conclusion of MBMS user registration. This indicates that the Ks derivation is correct as the new SRK is correct.</li> </ul>

**5.5.2.1.4 GBA\_U: Different Key K on Client and Server**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-407
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or MBMS/BCAST.



<b>Test Case Description</b>	Test that bootstrapping will not succeed when a different secret key K has been provisioned on the terminal and the server. Smartacrd is MBMS only ir MBMS/BCAST.
<b>Specification Reference</b>	SPCP Spec 6.5.1
<b>SCR Reference</b>	BCAST-SPCP-C-005
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ No bootstrapping context exists between the server and terminal/smartcard.</li> <li>○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS-enabled).</li> <li>○ Smartcard contains a valid 3G subscription (IMSI/K and also Milenage).</li> <li>○ HSS contains a different secret key K associated with the IMPI to that available on the Smartcard</li> <li>○ The URLs of the GBA and registration servers must be available to the terminal. This can be provided via an access and session description fragment (or MBMS USD in SDP) containing the following information or in some other way (e.g. hard coding URLs in the terminal) for the purposes of testing. <ul style="list-style-type: none"> <li>○ The key management element with a key management server definition.</li> <li>○ The attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service.</li> <li>○ The key management server with which the terminal should register.</li> </ul> </li> <li>○ The terminal can be prompted to perform GBA bootstrapping and MBMS user registration either via the service guide and services interaction or in another fashion for testing purposes.</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. The Terminal and the BSF establish bootstrapped security association between them by running bootstrapping procedure</li> <li>2. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity.(IMPI found in the USIM derived from IMSI as specified in TS 23 003)</li> <li>3. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102)</li> <li>4. The BSF selects an authentication vector AV= RAND  AUTN  XRES  CK  IK</li> <li>5. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND  AUTN</li> <li>6. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode</li> <li>7. The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK</li> <li>8. USIM sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid).</li> <li>9. Terminal sends challenge response back to the BSF in GET request</li> <li>10. BSF compares the RES corresponds to the XRES and discovers that they do not correspond</li> </ol> <p>The BSF returns a response indicating to the terminal than an authentication failure has occurred or sends a new challenge to restart bootstrapping.</p>

<b>Pass-Criteria</b>	<ol style="list-style-type: none"> <li>1. Reception at BSF of a GET request from Terminal with the appropriate IMPI to kick off bootstrapping.</li> <li>2. The BSF returns a response to the terminal which indicates that the authentication failure has occurred or returns a new challenge.</li> </ol>
----------------------	---

### 5.5.2.1.5 Deregistration

<b>Test Case Id</b>	BCAST-1.0-DIST-int-408
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	<p>Test that a deregistration flow can be processed by the server and terminal.</p> <p>Card is MBMS only or MBMS/BCAST</p>
<b>Specification Reference</b>	SPCP Spec 6.6
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-01
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ A bootstrapping context exists between server and terminal/smartcard</li> <li>○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS security enabled).</li> <li>○ Smartcard contains a valid 3G subscription (IMSI/K and also Milenage)</li> <li>○ HSS also contains the secret K associated with the IMSI/IMPI</li> <li>○ The URLs of the GBA and registration servers must be available to the terminal. This can be provided via an access and session description fragment (or MBMS USD in SDP) containing the following information or in some other way (e.g. hard coding URLs in the terminal) for the purposes of testing. <ul style="list-style-type: none"> <li>○ The key management element with a key management server definition.</li> <li>○ The attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service.</li> <li>○ The key management server with which the terminal should register.</li> </ul> </li> <li>○ A value for the ServiceID field in the deregistration request should be agreed by the terminal and server. This value should be one or more valid concatenation of a GlobalPurchaseItemID and a PurchaseDataReference. This can be done via a previous service provisioning flow or using pre-defined data.</li> </ul>

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. The BCAST Client is terminated or suspended on the terminal (This should prompt a deregistration flow).</li> <li>2. The terminal initiates the MBMS user deregistration flow.</li> <li>3. Terminal sends a HTTP post to the BSM containing the Service ID.</li> <li>4. The BSM answers with 401 Unauthorized indicating that the BSM wants to authenticate the terminal using the bootstrapped security association</li> <li>5. Key derivation: Terminal sends NAF_ID and IMPI to USIM using the AUTHENTICATE command in GBA security context: NAF derivation mode.</li> <li>6. USIM derives Ks_ext_NAF (SRK) and Ks_Int_NAF (SMK), updates the EF<sub>GBANL</sub> and sends back to the terminal the Ks_ext_NAF (SRK).</li> <li>7. The terminal sends to the BSM a HTTP POST request with B-TID as username and Ks_ext_NAF (SRK) as password as well as the Service IDs.</li> <li>8. BSM retrieves Ks_ext_NAF from the BSF and verifies the message received from the terminal.</li> <li>9. If success the BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each service.</li> </ol>
<b>Pass-Criteria</b>	The BSM receives a HTTP POST device from the terminal containing the Service IDs. At the end of the flow a 200 OK response (and a list of status codes) is returned by the BSM.

**5.5.2.1.6 Deregistration with Bootstrapping**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-409
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Test that a deregistration flow can be processed by the server and terminal when bootstrapping is required. Card is MBMS only or MBMS/BCAST.
<b>Specification Reference</b>	SPCP Spec 6.6
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-02
<b>Tool</b>	None
<b>Test code</b>	None

<p><b>Preconditions</b></p>	<ul style="list-style-type: none"> <li>○ No bootstrapping context exists between server and terminal/smartcard</li> <li>○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS security enabled).</li> <li>○ Smartcard contains a valid 3G subscription (IMSI/K and also Milenage)</li> <li>○ HSS also contains the secret K associated with the IMSI/IMPI</li> <li>○ The URLs of the GBA and registration servers must be available to the terminal. This can be provided via an access and session description fragment (or MBMS USD in SDP) containing the following information or in some other way (e.g. hard coding URLs in the terminal) for the purposes of testing. <ul style="list-style-type: none"> <li>○ The key management element with a key management server definition.</li> <li>○ The attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service.</li> <li>○ The key management server with which the terminal should register.</li> </ul> </li> <li>○ A value for the ServiceID field in the deregistration request should be agreed by the terminal and server. This value should be one or more valid concatenation of a GlobalPurchaseItemID and a PurchaseDataReference. This can be done via a previous service provisioning flow or using pre-defined data.</li> <li>○ The BSM wishes to renegotiate bootstrapping, i.e. the key lifetime has expired on the BSM side.</li> </ul>
<p><b>Test Procedure</b></p>	<p>The BCAST Client is terminated or suspended on the terminal (This should prompt a deregistration flow).</p> <ol style="list-style-type: none"> <li>1. The terminal initiates the MBMS user deregistration flow.</li> <li>2. Terminal sends a HTTP post to the BSM containing the Service ID.</li> <li>3. The BSM answers with 401 Unauthorized indicating that the BSM wants to authenticate the terminal using the bootstrapped security association</li> <li>4. Key derivation: Terminal sends NAF_ID and IMPI to USIM using the AUTHENTICATE command in GBA security context: NAF derivation mode.</li> <li>5. USIM derives Ks_ext_NAF (SRK) and Ks_Int_NAF (SMK), updates the EF<sub>GBANL</sub> and sends back to the terminal the Ks_ext_NAF (SRK).</li> <li>6. The terminal sends to the BSM a HTTP POST request with B-TID as username and Ks_ext_NAF (SRK) as password as well as the Service IDs.</li> <li>7. BSM determines that bootstrapping should be rerun and therefore returns a bootstrapping renegotiation indicator by returning a 401 “Unauthorized” HTTP response</li> <li>8. Prompted by receiving a bootstrapping renegotiation indication, the terminal initiates bootstrapping.</li> <li>9. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity.</li> <li>10. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102)</li> <li>11. The BSF selects an authentication vector AV= RAND  AUTN  XRES  CK  IK</li> </ol>

	<ol style="list-style-type: none"> <li>12. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND  AUTN</li> <li>13. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode</li> <li>14. The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK</li> <li>15. USIM sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid).</li> <li>16. Terminal sends challenge response back to the BSF in GET request</li> <li>17. BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI</li> <li>18. BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal</li> <li>19. The terminal stores B-TID and key lifetime in the EF<sub>GBABP</sub></li> <li>20. The terminal reinitiates the MBMS user deregistration flow with the enw bootstrapping data.</li> <li>21. The terminal sends to the BSM a HTTP POST request with B-TID as username and Ks_ext_NAF (SRK) as password as well as the Service IDs.</li> <li>22. The BSM returns a 200 OK as well as the status codes of the Service IDs.</li> </ol>
<b>Pass-Criteria</b>	<ol style="list-style-type: none"> <li>1. The terminal initiates bootstrapping on receiving a bootstrapping negotiation indication from the BSM.</li> <li>2. The BSM returns a 200 ok response after receiving an MBMS user deregistration request from the terminal using the new bootstrapping data.</li> </ol>

**5.5.2.1.7 Subscriber Key Establishment for (R-)UIM/CSIM**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-410
<b>Test Object</b>	BCAST Terminal /Smartcard. Smartcard is BCMCS/BCAST or BCAST
<b>Test Case Description</b>	Test that SMK and SRK derivation from pre-provisioned SCK in the terminal are successful. Smartcard is BCMCS/BCAST or BCAST.
<b>Specification Reference</b>	SPCP spec: 6.10, 6.5.2
<b>SCR Reference</b>	BCAST-SPCP-C-005, BCAST-KeyManagement-C-016
<b>Tool</b>	BCAST conformance test tool. Spy of the terminal/Smartcard interface Test Smartcard BCMCS-only or BCAST
<b>Test code</b>	

<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ Pre-provisioned “SmartCard Key” (SCK), corresponding to the Registration Key (RK) in BCMCS, is stored on the Smartcard, from which the SMK and SRK (TK and Auth-Key, respectively, in BCMCS) are derived.</li> <li>○ Description of service access is provided by BCMCS Information Acquisition as specified in [BCAST-ServContProt] Section 6.10.2.</li> <li>○ The Service Guide declares a service for which subscription is possible, allowing the Terminal to send a Service Request.</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Update the SG in the terminal using the test tool as the source.</li> <li>2. User selects a service for subscription.</li> <li>3. The terminal and BSM perform the Service Request transaction by using HTTP Digest for access authentication and integrity protection: <ol style="list-style-type: none"> <li>a. Terminal sends to the BSM “HTTP POST” containing the Service Request message.</li> <li>b. BSM responds with “HTTP 401 Unauthorized WWW-Authenticate” containing a digest-challenge.</li> <li>c. The terminal computes the challenge-response using the SRK and sends back to the BSM “HTTP POST Authorization Request” containing the digest-response.</li> <li>d. If the digest-response is correct, the BSM returns “HTTP 200 OK POST” with Authentication-Info containing the successful Service Request Response.</li> </ol> </li> </ol>
<b>Pass-Criteria</b>	Reception at the terminal the HTTP 200 OK message containing the successful status code for Service Request, as verification that the Smartcard /terminal and the BSM share the same SRK.

## 5.5.2.2 Layer 2 LTKM

### 5.5.2.2.1 OMA BCAST LTKM Terminal processing

#### 5.5.2.2.1.1. LTKM without SPE, without consumption reporting, MBMS only card

<b>Test Case Id</b>	BCAST-1.0-DIST-int-411
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS/BCMCS only or BCAST
<b>Test Case Description</b>	Test that an LTKM without SPE and without consumption reporting flag can be successfully received over UDP, and that the terminal sends the LTKM to the smartcard which sends back a verification message.
<b>Specification Reference</b>	SPCP spec: 6.6
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	Spy of the terminal / Smartcard interface
<b>Test code</b>	

<b>Preconditions</b>	<p>Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal.</p> <p>A Service registration has been performed with the BSM (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)</p> <p>The LTKM is valid and indicates that a verification message is needed</p> <p>The LTKM contains an EXT BCAST field with security_ext_policy_flag=LTK_FLAG_FALSE, and consumption_reporting_flag=LTK_FLAG_FALSE</p> <p>Card is an MBMS only card, as indicated in EF_UST</p>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case.</li> <li>2. Terminal receives LTKM,</li> <li>3. Terminal retrieves the TS stored along with the associated MUK-ID</li> <li>4. Terminal checks replay attacks</li> <li>5. Terminal sends the LTKM to the smartcard</li> <li>6. Smartcard verifies integrity of the message</li> <li>7. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message</li> <li>8. Terminal sends the verification message to the BSM.</li> </ol>
<b>Pass-Criteria</b>	<p>BSM receives the verification message</p> <p>On the spy.</p> <p>A READ RECORD command on EF_MUK(6FD8) is sent from the terminal to the smartcard, to check timestamp stored. (Anti-replay check performs in terminal)</p> <p>An AUTHENTICATE command in MSK update mode is sent to the smartcard, and a LTKM verification message is returned in the response.</p>

#### 5.5.2.2.1.2. LTKM without SPE, with consumption reporting, BCAST card

<b>Test Case Id</b>	BCAST-1.0-DIST-int-600
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test that an LTKM without SPE and without Consumption reporting flag can be successfully received over UDP, and that the terminal does not send the LTKM to the BCAST smartcard.
<b>Specification Reference</b>	SPCP spec: 6.6.7
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	Spy of the terminal / Smartcard interface
<b>Test code</b>	

<b>Preconditions</b>	<p>Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal.</p> <p>A Service registration has been performed with the BSM (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)</p> <p>The LTKM is valid and indicates that a verification message is needed</p> <p>The LTKM contains an EXT BCAST field, with security_ext_policy_flag=LTK_FLAG_FALSE, and consumption_reporting_flag=LTK_FLAG_FALSE</p> <p>Card is an BCAST enabled card, as indicated in EF_UST</p>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case.</li> <li>2. Terminal receives LTKM,</li> <li>3. Terminal verifies the BCAST EXT, doesn't send the message to the BCAST card and discards the message</li> </ol>
<b>Pass-Criteria</b>	<p>BSM doesn't receive the verification message</p> <p>On the spy, there is no AUTHENTICATE command sent to the smartcard</p>

#### 5.5.2.2.1.3. LTKM with SPE, MBMS only card

<b>Test Case Id</b>	BCAST-1.0-DIST-int-601
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only
<b>Test Case Description</b>	Test that an LTKM with SPE can be successfully received over UDP, that the terminal does not send the LTKM to the MBMS only smartcard.
<b>Specification Reference</b>	SPCP spec: 6.6.7
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	Spy of the terminal / Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>• Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal.</li> <li>• A Service registration has been performed with the BSM (i.e. test 5.5.2.1.1 for GBA-U has been performed first )</li> <li>• The smartcard is MBMS only card, as indicated in EF_UST</li> <li>• The LTKM is valid, indicates that a verification message is needed, and contains EXT BCAST field with Security_policy_ext_flag set to LTK_FLAG_TRUE</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM pushes an LTKM over UDP to the terminal / smartcard with EXT BCAST payload.. Test for GBA_U case.</li> <li>2. Terminal receives LTKM,</li> <li>3. Terminal discards the message</li> </ol>
<b>Pass-Criteria</b>	<p>BSM doesn't receive a verification message</p> <p>On the spy, there is no AUTHENTICATE command sent to the smartcard</p>



## 5.5.2.2.1.4. LTKM with SPE, BCAST card

<b>Test Case Id</b>	BCAST-1.0-DIST-int-602
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. smartcard is BCAST
<b>Test Case Description</b>	Test that an LTKM with SPE can be successfully received over UDP, that the terminal sends the LTKM to the BCAST smartcard which sends back a verification message.
<b>Specification Reference</b>	SPCP spec: 6.6.7, 6.6.6.1
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	Spy of the terminal / Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>• Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal.</li> <li>• A Service registration has been performed with the BSM (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)</li> <li>• The smartcard is MBMS/BCAST or BCMCS/BCAST</li> <li>• The LTKM indicates that a verification message is needed</li> <li>• The LTKM is valid and contains EXT BCAST field with Security_policy_ext_flag is set to LTK_FLAG_TRUE</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM pushes an LTKM over UDP to the terminal / smartcard with EXT BCAST payload.. Test for GBA_U case.</li> <li>2. Terminal receives LTKM,</li> <li>3. Terminal sends the LTKM to the smartcard, without anti-replay check</li> <li>4. Smartcard verifies integrity of the message</li> <li>5. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message</li> <li>6. Terminal sends the verification message to the BSM.</li> </ol>
<b>Pass-Criteria</b>	<p>BSM receives a verification message</p> <p>On the spy.</p> <p>No READ RECORD command on EF_MUK (6FD8) (Anti-replay check not performed by the terminal)</p> <p>An AUTHENTICATE command in MSK update mode is sent to the smartcard, and a LTKM verification message is returned in the response.</p>

## 5.5.2.2.1.5. LTKM request from the terminal, LTKM reception at the terminal / smartcard

<b>Test Case Id</b>	BCAST-1.0-DIST-int-412
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS/BCMCS only or BCAST

<b>Test Case Description</b>	<p>Test that an LTKM can be successfully</p> <ul style="list-style-type: none"> <li>• requested by the terminal</li> <li>• delivered over UDP to the terminal</li> </ul> <p>Test that a verification message is sent. MBMS/BCAST smartcard</p>
<b>Specification Reference</b>	SPCP spec: 6.6, 6.6.7
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. Service registration has been performed. . (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used) Terminal has missed an LTKM update because was out of coverage. IP context doesn't exist anymore LTKM contains EXT BCAST field, with SPE The smartcard is BCAST</p>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Terminal initiates an HTTP digest authentication using the LTKM request procedure and information in USD or SDP and establish an IP connection with the BSM. <ol style="list-style-type: none"> <li>a. The terminal sends to the BSM a GET request with B-TID, as username and Ks_ext_NAF (SRK) as password and with the list of one or more Key domain ID- MSK-ID</li> <li>b. BSM retrieves Ks_ext_NAF from the BSF and verifies that the terminal has performed the registration and is authorized to receive the LTKM. The BSM verifies the message received from the terminal.</li> </ol> </li> <li>2. If success the BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each LTKM requested.</li> <li>3. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case.</li> <li>4. Terminal receives LTKM,</li> <li>5. Terminal sends the LTKM to the smartcard, without anti-replay chack</li> <li>6. Smartcard verifies integrity of the message</li> <li>7. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message</li> <li>8. Terminal sends the verification message to the BSM.</li> </ol>
<b>Pass-Criteria</b>	<p>BSM receives a successful LTKM request BSM receives the verification message</p>

#### 5.5.2.2.1.6. BSM solicited pull procedure

<b>Test Case Id</b>	BCAST-1.0-DIST-int-413
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS/BCMCS only or BCAST

<b>Test Case Description</b>	Test that the BSM solicited pull procedure is correctly understood by the terminal and that the terminal is then able to request the LTKM update. Smartcard is MBMS only or BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal.</li> <li>○ Service registration has been performed. (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM sends a MIKEY message with the last SMK known by the BSM and with the key number part of MSK-ID= 0x0, Key group part different than 1</li> <li>2. The terminal sends a HTTP POST to request the LTKM with the KeyDomainID-MSK-ID pair</li> </ol>
<b>Pass-Criteria</b>	BSM receives a successful LTKM request

#### 5.5.2.2.1.7. BSM solicited pull procedure initiation over SMS Bearer

<b>Test Case Id</b>	BCAST-1.0-DIST-int-414
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS/BCMCS only or BCAST
<b>Test Case Description</b>	Test that the BSM solicited pull procedure initiation over SMS bearer is correctly understood by the terminal and that the terminal is then able to request the LTKM update. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.2
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal.</li> <li>○ Service registration has been performed. (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM sends in a SMS, a MIKEY message with the last SMK known by the BSM and with the key number part of MSK-ID= 0x0, KEMAC Encr Data Len = 0 and V bit in Hdr is not set. MSK ID key group part is different than 1.</li> <li>2. The terminal sends a HTTP POST to request the LTKM with the KeyDomainID-MSK-ID pair</li> </ol>
<b>Pass-Criteria</b>	BSM receives a successful LTKM request

## 5.5.2.2.1.8. BSM solicited pull procedure to initiate the Registration Procedure

<b>Test Case Id</b>	BCAST-1.0-DIST-int-603
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. smartcard is MBMS only or BCAST
<b>Test Case Description</b>	Test that the BSM solicited pull procedure to initiate the Registration Procedure is correctly understood by the terminal and that the terminal is then able to request the LTKM update. Smartcard is MBMS only or BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.3
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	None
<b>Test code</b>	
<b>Preconditions</b>	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. Service registration has been performed. (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM sends a MIKEY message with the last SMK known by the BSM and with the key group of MSK-ID= 1 and key number part =0</li> <li>2. The terminal shall initiate a registration procedure with MBMS User Service ID="oma-bcast-allservices"</li> </ol>
<b>Pass-Criteria</b>	BSM receives a registration request with MBMS User Service ID="oma-bcast-allservices"

## 5.5.2.2.1.9. LTKM Replay Detection in secure function, failure case

<b>Test Case Id</b>	BCAST-1.0-DIST-int-604
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test that an LTKM will be rejected if TS received is less than or equal to the last received TS stored in smartcard. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.7.3
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	Spy of the terminal / Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. Service registration has been performed. (i.e. test 5.5.2.1.1 for GBA-U has been performed first in case USIM is used or test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case.</li> <li>2. Terminal receives LTKM,</li> <li>3. Terminal sends the LTKM to the smartcard</li> <li>4. Smartcard verifies integrity of the message using SMK (MUK)</li> <li>5. Smartcard stores TS in EF_MUK</li> <li>6. Smartcard and then terminal send back a verification message</li> <li>7. BSM pushes a LTKM with the same TS</li> <li>8. Terminal receives LTKM,</li> <li>9. Terminal sends the LTKM to the smartcard</li> <li>10. Smartcard verifies integrity of the message using SMK (MUK)</li> <li>11. Smartcard verifies TS against the stored LTKM replay counter value. (failure)</li> <li>12. Verification message is not returned to the BSM</li> </ol>
<b>Pass-Criteria</b>	<p>BSM receives a Verification Message after step1)                      BSM does not receive a verification message 4 min after step 7)</p> <p>On the spy                      The first AUTHENTICATE command in MSK update mode returns SW=9000 and a verification message is included in the response.                      The second AUTHENTICATE command in MSK update mode returns SW=9862 (authentication error, incorrect MAC) is returned</p>

**5.5.2.2.2 Managing purses and counters using OMA BCAST LTKM**

Note: The test describes below is a generic test procedure that shall apply to following tests (from 5.5.2.2.2.1 to 5.5.2.2.2.20 and 5.5.2.2.3). Depending of the test, LTKM1 field are defined in each procedure.

<b>Test Case Id</b>	preamble for managing purses and counters test cases
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test that an LTKM with EXT BCAST field can be successfully received over UDP at the terminal / smartcard that the purse and counters according to SPE value are successfully updated and that and a verification message and consumption reporting message are sent. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	

<b>Preconditions</b>	<p>Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal:  A Service registration has been performed with the BSM and with a GBA-U (i.e. test 5.5.2.1.1.: GBA-U Bootstrapping USIM /BSM with success)  The LTKM is valid and indicates that a verification message is needed  The LTKM contains EXT BCAST field</p>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case.</li> <li>2. Terminal receives LTKM,</li> <li>3. Terminal sends the LTKM to the smartcard</li> <li>4. Smartcard verifies integrity of the message</li> <li>5. Smartcard performs replay protection check</li> <li>6. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message</li> <li>7. Terminal sends the verification message to the BSM.</li> <li>8. BSM receives Verification Message</li> <li>9. BSM push a LTKM2 Message over UDP to the terminal/smartcard with a consumption reporting_flag = 1. V bit =0, same SPE, SEK/PEK id and KV as LTKM1</li> <li>10. BSM receives LTKM Reporting Message</li> </ol>
<b>Pass-Criteria</b>	<p>BSM receives the verification message  BSM receives LTKM Reporting Message containing data according to following tests</p>

Note: The following tests (from 5.5.2.2.2.1 to 5.5.2.2.2.20) shall be run in sequence. The pass criteria depends on this sequence

#### 5.5.2.2.2.1. Set of live ppt purse associated with a key group, SPE=0x00

<b>Test Case Id</b>	BCAST-1.0-DIST-int-605
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Set of live_ppt_purse associated with a key group, SPE=0x00  The live_ppt_purse created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases  Smartcard shall support SPE=0x00</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p>LTKM1 fields:</p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0002 0001</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x00; purse_flag = 1; purse_mode = 0; token_value = 0x05; cost_value=0x00; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x00</li> <li>○ Cost_value= 0x00</li> <li>○ Purse_value=0x05 (value of live_ppt_purse)</li> </ul>

#### 5.5.2.2.2. Test of set mode for the live\_ppt\_purse associated with a key group, SPE=0x00

<b>Test Case Id</b>	BCAST-1.0-DIST-int-606
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Test of set mode for the live_ppt_purse associated with a key group, SPE=0x00</p> <p>Set mode executed on a already created purse. Smartcard is BCAST.</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test BCAST-1.0-DIST-int-605 passed successfully first</p> <p>Smartcard shall support SPE=0x00</p>
<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p>LTKM1 fields:</p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0002 0001 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x00; purse_flag = 1; purse_mode = 0; token_value = 0x10; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 02 00; TShigh = 0x00 00 02 FF</p>

<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x00</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x10 (value of live_ppt_purse)</li> </ul>
----------------------	--

#### 5.5.2.2.3. Test of add mode for the live\_ppt\_purse associated with a key group, SPE=0x00

Test Case Id	BCAST-1.0-DIST-int-607
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of add mode for the live_ppt_purse associated with a key group, SPE=0x00 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015
Tool	none
Test code	
Preconditions	See preamble for managing purses and counters test cases Additionally, test BCAST-1.0-DIST-int-606 passed successfully first Smartcard shall support SPE=0x00
Test Procedure	See preamble for managing purses and counters test cases  LTKM1 fields: Key domain ID= MCC1    MNC1 SEK/PEK ID = 0002 0002 (same Key_group but different Key_Number part) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x00; purse_flag = 1; purse_mode = 1; token_value = 0x10; cost_value=0x02; access_criteria_flag = 0 KV: TSlow = 0x 00 00 03 00; TShigh = 0x00 00 03 FF
Pass-Criteria	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x00</li> <li>○ Cost_value= 0x02</li> <li>○ Purse_value=0x20 (value of live_ppt_purse)</li> </ul>

#### 5.5.2.2.4. Test of overflow for the live\_ppt\_purse associated with a key group, SPE=0x00

Test Case Id	BCAST-1.0-DIST-int-608
--------------	------------------------



<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test of overflow for the live_ppt_purse associated with a key group, SPE=0x00 Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	Seepreamble for managing purses and counters test cases Additionally, test <b>BCAST-1.0-DIST-int-607</b> passed successfully first Smartcard shall support SPE=0x00
<b>Test Procedure</b>	See preamble for managing purses and counters test cases  LTKM1 fields: Key domain ID= MCC1    MNC1 SEK/PEK ID = 0002 0003 (same Key_group as the previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x00; purse_flag = 1; purse_mode = 1; token_value = 0x7FFFFFFF; cost_value=0x03; access_criteria_flag = 0 KV: TSlow = 0x00 00 04 00; TShigh = 0x00 00 04 FF
<b>Pass-Criteria</b>	BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 1</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x00</li> <li>○ Cost_value= 0x03</li> <li>○ Purse_value=0x20 (value of live_ppt_purse)</li> </ul>

#### 5.5.2.2.5. Set of playback\_ppt\_purse associated with a key group, SPE=0x01

<b>Test Case Id</b>	BCAST-1.0-DIST-int-609
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Set of playback_ppt_purse associated with a key group, SPE=0x01 The playback_ppt_purse created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	

<b>Preconditions</b>	See preamble for managing purses and counters test cases Smartcard shall support SPE=0x01
<b>Test Procedure</b>	See preamble for managing purses and counters test cases  LTKM1 fields:  Key domain ID= MCC1    MNC1  SEK/PEK ID = 0003 0001 (new Key_group)  V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x01; purse_flag = 1; cost_value=0x01; purse_mode = 0; token_value = 0x10; access_criteria_flag = 0  KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF
<b>Pass-Criteria</b>	BSM receives the Verification Message for the LTKM1 delivery  BSM receives the LTKM Reporting Message with following parameters <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x01</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x10 (value of playback_ppt_purse, managed independently from live_ppt_purse)</li> </ul>

#### 5.5.2.2.2.6. Test of set mode for playback\_ppt\_purse associated with a key group, SPE=0x01

<b>Test Case Id</b>	BCAST-1.0-DIST-int-610
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for set mode for playback_ppt_purse associated with a key group, SPE=0x01 Set mode executed on a already created purse. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	See preamble for managing purses and counters test cases Additionally, test <b>BCAST-1.0-DIST-int-609</b> passed successfully first Smartcard shall support SPE=0x01

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p>LTKM fields:</p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0003 0002 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x01; purse_flag = 1; purse_mode = 0; token_value = 0x20; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 02 00; TShigh = 0x00 00 02 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x01</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x20 (value of playback_ppt_purse, managed independently from live_ppt_purse)</li> </ul>

#### 5.5.2.2.7. Test of add mode for playback\_ppt\_purse associated with a key group, SPE=0x01e

<b>Test Case Id</b>	BCAST-1.0-DIST-int-611
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for add mode for playback_ppt_purse associated with a key group, SPE=0x01 Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-610</b> passed successfully first</p> <p>Smartcard shall support SPE=0x01</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p>LTKM fields:</p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0003 0002 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x01; purse_flag = 1; purse_mode = 1; token_value = 0x10; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 03 00; TShigh = 0x00 00 03 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x01</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x30</li> </ul>

#### 5.5.2.2.8. Test of overflow for playback\_ppt\_purse associated with a key group, SPE=0x01

<b>Test Case Id</b>	BCAST-1.0-DIST-int-612
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test of overflow for playback_ppt_purse associated with a key group, SPE=0x01 Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-611</b> passed successfully first</p> <p>Smartcard shall support SPE=0x01</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p>LTKM1 fields:</p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0003 0002 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x01; purse_flag = 1; purse_mode = 1; token_value = 0x7FFFFFFF; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 04 00; TShigh = 0x00 00 04 FF</p>
<b>Pass-Criteria</b>	<p>BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 1</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x01</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x30</li> </ul>

#### 5.5.2.2.9. Set of user\_purse associated with a NAF/SMK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-613
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Set of user_purse associated with a NAF/SMK id</p> <p>The user_purse created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Card shall support SPE=0x02, 0x03, 0x08 or 0x09</p> <p>Below test is described with the assumption that the card supports SPE=0x02.</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p>LTKM1 fields:</p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0004 0001 (newKey_group)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x02; purse_flag = 1; cost_value=0x01; purse_mode = 0; token_value = 0x10; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x02</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x10</li> </ul>

#### 5.5.2.2.10. Test of set mode for user\_purse associated with a NAF/SMK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-614
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for set mode for user_purse associated with NAF/SMK id Set mode executed on a already created purse. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-613</b> passed successfully first</p> <p>Card shall support SPE=0x02, 0x03, 0x08 or 0x09</p> <p>Below test is described with the assumption that the card supports SPE=0x02.</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0004 0001 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x02; purse_flag = 1; purse_mode = 0; token_value = 0x20; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 02 00; TShigh = 0x00 00 02 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x02</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x20 (value of user_purse)</li> </ul>

#### 5.5.2.2.11. Test of add mode for user\_purse associated with NAF/SMK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-615
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for add mode for user_purse associated with NAF/SMK id Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	None
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-614</b> passed successfully first</p> <p>Card shall support SPE=0x02, 0x03, 0x08 or 0x09</p> <p>Below test is described with the assumption that the card supports SPE=0x02.</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0004 0002 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x02; purse_flag = 1; purse_mode = 1; token_value = 0x10; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 03 00; TShigh = 0x00 00 03 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x02</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x30</li> </ul>

#### 5.5.2.2.12. Test of overflow for user\_purse associated with NAF/SMK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-616
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test of overflow for user_purse associated with NAF/SMK id Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	None
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-615</b> passed successfully first</p> <p>Card shall support SPE=0x02, 0x03, 0x08 or 0x09</p> <p>Below test is described with the assumption that the card supports SPE=0x02.</p>



<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0005 0002 (different Key_group, to test that key group is not associated with user_purse)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x02; purse_flag = 1; purse_mode = 1; token_value = 0x7FFFFFFF; cost_value=0x01; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 04 00; TShigh = 0x00 00 04 FF</p>
<b>Pass-Criteria</b>	<p>BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 1</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x02</li> <li>○ Cost_value= 0x01</li> <li>○ Purse_value=0x30 (purse value not changed)</li> </ul>

#### 5.5.2.2.13. Set of Playback counter associated with a SEK/PEK id, SPE=0x07

<b>Test Case Id</b>	BCAST-1.0-DIST-int-617
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Set of Playback counter associated with a SEK/PEK id, SPE=0x07</p> <p>The playback counter created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	See preamble for managing purses and counters test cases

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0005 0001 (new key group )</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0;add_flag=0, number_playback=3; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x07</li> <li>○ Add_flag=0</li> <li>○ Playback_counter=3</li> </ul>

#### 5.5.2.2.14. Test of set mode for Playback counter associated with a SEK/PEK id, SPE=0x07

<b>Test Case Id</b>	BCAST-1.0-DIST-int-618
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Test for set mode for Playback counter associated with a SEK/PEK id, SPE=0x07</p> <p>Set mode executed on a already created playback counter</p> <p>Smartcard is BCAST.</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-617</b> passed successfully first</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0005 0001 (same Key as previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x07; purse_flag = 0; add_flag=0, number_playback=5; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x07</li> <li>○ Add_flag=0</li> <li>○ Playback_counter=5</li> </ul>

#### 5.5.2.2.15. Test of add mode for Playback counter associated with a SEK/PEK id, SPE=0x07

<b>Test Case Id</b>	BCAST-1.0-DIST-int-619
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for add mode for Playback counter associated with a SEK/PEK id, SPE=0x07 Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	See preamble for managing purses and counters test cases Additionally, test <b>BCAST-1.0-DIST-int-618</b> passed successfully first

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0005 0001 (same Key as previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x07; purse_flag = 0; add_flag=1, number_playback=3; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x07</li> <li>○ Add_flag=1</li> <li>○ Playback_counter=8</li> </ul>

#### 5.5.2.2.16. Test for overflow of Playback counter associated with a SEK/PEK id, SPE=0x07

<b>Test Case Id</b>	BCAST-1.0-DIST-int-620
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for overflow of Playback counter associated with a SEK/PEK id, SPE=0x07 Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	See preamble for managing purses and counters test cases Additionally, test <b>BCAST-1.0-DIST-int-619</b> passed successfully first

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0005 0001 (same Key as previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x07; purse_flag = 0; add_flag=1, number_playback=0x7F; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 1</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x07</li> <li>○ Add_flag=1</li> <li>○ Playback_counter=8</li> </ul>

#### 5.5.2.2.17. Set of TEK counter associated with a SEK/PEK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-621
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Set of TEK counter associated with a SEK/PEK id</p> <p>The TEK counter created in this test will be used by subsequent tests for set mode, add mode and overflow</p> <p>Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D.</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Card shall support SPE=0x0C or 0x0D</p> <p>Below test is described with the assumption that the card supports SPE=0x0C.</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0006 0001 (newKey_group)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x0C; purse_flag = 0; add_flag=0 ; keep_credit_flag=1 ; number_TEKs=5; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x0C</li> <li>○ Add_flag=0</li> <li>○ Keep_credit_flag = 1</li> <li>○ TEK_counter=5</li> </ul>

#### 5.5.2.2.18. Test of set mode for TEK counter associated with a SEK/PEK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-622
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	<p>Test for set mode for TEK counter associated with SEK/PEK id</p> <p>Set mode executed on a already created TEK counter</p> <p>Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D..</p>
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-621</b> passed successfully first</p> <p>Card shall support SPE=0x0C or 0x0D</p> <p>Below test is described with the assumption that the card supports SPE=0x0C.</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0006 0001 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x0C; purse_flag = 0; add_flag=0 ; keep_credit_flag=1 ; number_TEKs=10 ; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x0C</li> <li>○ Add_flag= 0</li> <li>○ Keep_credit_flag = 1</li> <li>○ TEK_counter=10</li> </ul>

#### 5.5.2.2.19. Test of add mode for TEK counter associated with SEK/PEK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-623
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test for add mode for TEK counter associated with SEK/PEK id Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D..
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-622</b> passed successfully first</p> <p>Card shall support SPE=0x0C or 0x0D</p> <p>Below test is described with the assumption that the card supports SPE=0x0C.</p>

<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM1 fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0006 0001 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x0C; purse_flag = 0; add_flag=1 ; keep_credit_flag=1 ; number_TEKs=10; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM receives the Verification Message for the LTKM1 delivery</p> <p>BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 1</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 0</li> <li>○ Not_found_flag = 0</li> <li>○ Security_policy_extension = 0x0C</li> <li>○ Add_flag= 1</li> <li>○ Keep_credit_flag = 1</li> <li>○ TEK_counter=20</li> </ul>

#### 5.5.2.2.20. Test of overflow for TEK counterassociated with SEK/PEK id

<b>Test Case Id</b>	BCAST-1.0-DIST-int-624
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test of overflow for TEK counterassociated with SEK/PEK id Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D..
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>See preamble for managing purses and counters test cases</p> <p>Additionally, test <b>BCAST-1.0-DIST-int-623</b> passed successfully first</p> <p>Card shall support SPE=0x0C or 0x0D</p> <p>Below test is described with the assumption that the card supports SPE=0x0C.</p>



<b>Test Procedure</b>	<p>See preamble for managing purses and counters test cases</p> <p><b>LTKM fields:</b></p> <p>Key domain ID= MCC1    MNC1</p> <p>SEK/PEK ID = 0006 0001 (same Key_group as the previous message)</p> <p>V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension = 0x0C; purse_flag = 0; add_flag=1 ; keep_credit_flag=1 ; number_TEKs=0x3FFFFFF; access_criteria_flag = 0</p> <p>KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF</p>
<b>Pass-Criteria</b>	<p>BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters</p> <ul style="list-style-type: none"> <li>o consumption_reporting_flag = 1</li> <li>o Overflow_flag = 1</li> <li>o Unsupported_extention_flag = 0</li> <li>o Not_found_flag = 0</li> <li>o Security_policy_extension = 0x0C</li> <li>o Add_flag= 1</li> <li>o Keep_credit_flag = 1</li> <li>o TEK_counter=20</li> </ul>

At the end of this sequence of tests, Smartcard contains the following SEK/PEK ID:

Note: Key Domain ID = MCC1 || MNC1 for all keys

Key group part	Key number part	Security policy	Cost-value	live_ppt_purse	Playback_ppt_purse	User_purse	Play-back counter	TEK counter
0002	0001	0x00	0x00	0x20				
0002	0001	0x00	0x01	0x20				
0002	0002	0x00	0x02	0x20				
0003	0001	0x01	0x01		0x30			
0003	0002	0x01	0x01		0x30			
0003	0002	0x01	0x01		0x30			
0004	0001	0x02	0x01			0x30		
0004	0001	0x02	0x01			0x30		
0004	0002	0x02	0x01			0x30		
0005	0001	0x07					0x08	
0006	0001	0x0C						0x20

### 5.5.2.2.3 SPE value not supported by the card

<b>Test Case Id</b>	BCAST-1.0-DIST-int-625
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Send an LTKM with SPE extention, but the value is not supported by the card Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.6.4, 6.6.6, 6.6.7
<b>SCR Reference</b>	BCAST-LTKM_SC-C-015
<b>Tool</b>	None
<b>Test code</b>	
<b>Preconditions</b>	Seepreamble for managing purses and counters test cases Card does not support all SPE Below test is described with the assumption that the card does not support SPE=0x0C.
<b>Test Procedure</b>	Seepreamble for managing purses and counters test cases  <b>LTKM1 fields:</b>  Key domain ID= MCC1    MNC1  SEK/PEK ID = 0006 0001  V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x0C; purse_flag = 0; add_flag=0 ; keep_credit_flag=1 ; number_TEKs=0x05; access_criteria_flag = 0  KV: TSlow = 0x00 00 01 00; TShigh = 0x00 00 01 FF
<b>Pass-Criteria</b>	BSM does not receive a LTKM Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters <ul style="list-style-type: none"> <li>○ consumption_reporting_flag = 0</li> <li>○ Overflow_flag = 0</li> <li>○ Unsupported_extention_flag = 1</li> <li>○ Not_found_flag = 0</li> </ul>

### 5.5.2.3 Layer 3 STKM

For this part, encrypted content (video) with the appropriate keys is sent by the BSDA.

The server provides a valid SRTP and STKM stream to the device

The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means

#### 5.5.2.3.1 Correct STKM parsing by a BCAST Smartcard

<b>Test Case Id</b>	BCAST-1.0-DIST-int-430
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Test that the Smartcard correctly parses STKMs Smartcard is BCAST
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.2, 6.7.3
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>o Smartcard has valid LTKM allowing the Smartcard to verify the STKM</li> <li>o BSM sends an LTKM for the service:</li> <li>o Key domainID= MCC1   MNC1</li> <li>o SEK/PEK ID = 0003 0001</li> <li>o with a security_policy_extension = 0x04</li> <li>o KV: TSlow= 0x00 00 00; TShigh= 0x00 00 0F</li> </ul> <p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>Smartcard is BCAST</p>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM / BSDA generates STKMs for the service 03 of the Key domain ID= MCC1   MNC1</li> </ol> <p>TEK ID of STKM is incremented for each STKM renewal with a cryptoperiod of 10s Within a crypto period TEK ID is not changed (STKM sent every second; i.e 10 times within the crypto period) but TS changes for each STKM within the crypto period. TS starts with 0x00 00 00 01 and TEK_ID with 0x00 01.</p> <p>If this requires too much processing on the server side, it is also possible to test without TS change during the crypto period but with for example an increment of 10 for each cryptoperiod</p> <ol style="list-style-type: none"> <li>2. STKMs are received by the Smartcard.</li> <li>3. The TEK are sent back to the terminal</li> <li>4. The terminal decrypts the content using the TEK for the SRTP protocol</li> </ol>
<b>Pass-Criteria</b>	<p>Video is displayed by the terminal during 20 s</p> <p>Terminal forwards only the first STKM received every cryptoperiod, Terminal does not forward resent STKM (=STKM with same TEK ID) to the smartcard</p> <p>If the video is displayed during 15*10=150s, this means that TEK ID field is used for the checking of KV of SEK/PEK, instead of TS, as required by BCAST. This is an error.</p> <p>On the spy;</p> <p>Only one AUTHENTICATE command is sent to the card every cryptoperiod (10s). Smartcard returns decrypted material.</p>

### 5.5.2.3.2 Correct STKM parsing by Smartcard (MBMS)

<b>Test Case Id</b>	BCAST-1.0-DIST-int-431
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server.Smartcard is MBMSonly
<b>Test Case Description</b>	Test that the Smartcard correctly parses STKMs
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.2, 6.7.3
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<ul style="list-style-type: none"> <li>○ Smartcard has valid LTKM allowing the Smartcard to verify the STKM</li> <li>○ BSM sends an LTKM for the service with</li> <li>○ security_policy_extension: flag=0 and consumption_reporting_flag=0 :</li> <li>○ Key domainID= MCC1   MNC1</li> <li>○ SEK/PEK ID = 0004 0001</li> <li>○ KV: SEQl= 0x00 00; SEQu = 0x00 0F (KV coding TEK ID interval)</li> <li>○ The server provides a valid SRTP and STKM stream to the device</li> <li>○ The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. BSM / BSDA generates STKMs for the service 04 of the Key domain ID= MCC1   MNC1 TEK ID of STKM is incremented for each STKM renewal with a cryptoperiod of 10s Within a crypto period TEK ID is not changed (STKM sent every second; i.e 10 times within the crypto period) but TS changes for each STKM within the crypto period. If this requires too much processing on the server side, it is also possible to test without TS change during the crypto period but with for example an increment of 10 for each cryptoperiod</li> <li>2. STKMs are received by the Smartcard.</li> <li>3. The TEK are sent back to the terminal</li> <li>4. The terminal decrypts the content using the TEK for the SRTP protocol</li> </ol>
<b>Pass-Criteria</b>	<p>Smartcard returns no error message, thus validating the STKMs are correctly parsed by the smartcard, Video is displayed by the terminal during 150 s (2,50 mns).</p> <p>On the spy</p> <p>The response of the AUTHENTICATE command in MTK generation mode, containing decrypted key material, is conform to 3GPP TS 33,246</p>

### 5.5.2.3.3 Incorrect STKM generation – inexistent SEK/PEK (wrong key domain ID)

<b>Test Case Id</b>	BCAST-1.0-DIST-int-432
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server.

<b>Test Case Description</b>	Test that an STKM cannot be processed by a smartcard that doesn't store the corresponding SEK/PEK (wrong Key Domain ID) and that the TEK isn't returned. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.2, 6.7.3
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	The Bootstrapping exists, but <b>SEK/PEK</b> used doesn't exist. The BSM sends a STKM for the key domain ID = MCC2   MNC2 and with a SEK/PEK ID key group = 0x0003 (wrong key domain ID)  The server provides a valid SRTP and STKM stream to the device  The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means
<b>Test Procedure</b>	The UE receives the STKM message.  Smartcard detects that the SEK/PEK ID is not available for the decryption of STKM and doesn't generate the TEK. The return status code is '6A88' (referenced data not found).
<b>Pass-Criteria</b>	No video displayed by the terminal On the spy: the status code returned by the card is '6A88' Terminal asks user to register to that service BSM receives a LTKM request from the terminal

#### 5.5.2.3.4 Incorrect STKM generation – inexistent SEK/PEK (wrong SEK ID)

<b>Test Case Id</b>	BCAST-1.0-DIST-int-433
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server.
<b>Test Case Description</b>	Test that an STKM cannot be processed by a smartcard that doesn't store the corresponding SEK/PEK (wrong Key Domain ID)and that the TEK isn't returned. Smartcard is BCAST.
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.2, 6.7.3
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	The Bootstrapping exists, but <b>SEK/PEK</b> used doesn't exist. The BSM sends a STKM for the key domain ID = MCC1   MNC1 and with a SEK/PEK ID key group = 0x0010 (Wrong SEK/PEK ID)  The server provides a valid SRTP and STKM stream to the device  The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means
<b>Test Procedure</b>	The UE receives the STKM message.  Smartcard detects that the SEK/PEK ID is not available for the decryption of STKM and doesn't generate the TEK. The return status code is '6A88' (referenced data not found).

<b>Pass-Criteria</b>	<p>No video displayed by the terminal</p> <p>On the spy: the status code returned by the card is '6A88'</p> <p>Terminal asks user to register to that service</p> <p>BSM receives a LTKM request from the terminal</p>
----------------------	--

### 5.5.2.3.5 STKM processing, Key Validity data check

<b>Test Case Id</b>	BCAST-1.0-DIST-int-626
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	Key Validity data check. Test that an STKM cannot processed by the smartcard and the TEK isn't returned when TS is lower that TSlow or higher than TShigh.
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.2, 6.7.3, 6.7.3.5
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<p>Smartcard has valid LTKM allowing the Smartcard to verify the STKM</p> <p>BSM sends an LTKM for the service:</p> <ul style="list-style-type: none"> <li>• Key domainID= MCC1   MNC1</li> <li>• SEK/PEK ID = 0003 0001</li> <li>• with a security_policy_extension = 0x04</li> <li>• KV: TSlow= 0x00 00 00 01; TShigh= 0x00 00 00 06</li> </ul> <p>No other LTKM has been sent previously</p> <p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p>
<b>Test Procedure</b>	<p>A valid STKM is sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with TS from 0x00 00 00 00 to 0x00 00 00 07 , and TS increase by one for each cryptoperiod (10s)</p> <ul style="list-style-type: none"> <li>• Terminal receives the message and sends it to the smartcard</li> </ul> <p>At reception of the 2 first STKM with TS=0x00 00 00 00 and TS=0x00 00 00 01, Smartcard detects that the Key Validity daT check fails and returns the status code '9865' (Key freshness failure)</p> <p>Terminal may display an error message and may ask the user to register to that service. In this case cancel the procedure to allow execution of next steps of the test.</p> <ul style="list-style-type: none"> <li>• From TS=0x00 00 00 02 to TS=0x00 00 00 06, Key Validity data check is successful, and smartcard returns decrypted material to terminal</li> <li>• Video is displayed during 50s</li> <li>• At reception of last STKM with TS=0x00 00 00 07, Smartcard detects that the Key Validitu data check fails and returns the status code '9865' (Key freshness failure)</li> </ul>

<b>Pass-Criteria</b>	<p>No video is displayed during the first 20s Then video is displayed during 50s On the spy:</p> <p>For the 2 first AUTHENTICATE command, the status word returned by the smartcard is '9865' (Key freshness failure)</p> <p>For the 3<sup>rd</sup> to 7<sup>th</sup> AUTHENTICATE command, the status word returned by the smartcard is 9000 and the key material is returned in the response.</p> <p>For the last AUTHENTICATE command, the status word returned by the smartcard is '9865' (Key freshness failure)</p>
----------------------	---

### 5.5.2.3.6 Key deletion from server

This test is relative to the layer2 but the test procedure and pass criteria needs that the test [5.5.2.3.3](#) and [5.5.2.3.4](#) passed successfully first.

<b>Test Case Id</b>	BCAST-1.0-DIST-int-439
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	BSM / BSDA sends an LTKM with the security policy extension 0x0A to delete keys associated to the given SEK/PEK ID. SPE=0x0A is supported by the smartcard
<b>Specification Reference</b>	SPCP spec: 6.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <a href="#">5.5.2.3.1: 'Correct STKM parsing by the Smartcard'</a> passed successfully. The smartcard has the following valid SEK/PEK</p> <ul style="list-style-type: none"> <li>○ Key domainID= MCC1   MNC1</li> <li>○ SEK/PEK ID = 0003 0001</li> <li>○ with a security_policy_extension = 0x04</li> <li>○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F</li> <li>○ The video is decrypted successfully</li> </ul>

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Before the end of the Key validity of the SEK/PEK (when TS of the STKM reaches 0x00 00 00 05), BSM sends a LTKM for the same SEK/PEK ID but with a security policy extension equals to 0x0A, and KV: TSlow = TShigh=0x00 00 00 00</li> <li>2. The terminal sends the LTKM to the smartcard</li> <li>3. The smartcard detects that the LTKM is for a deletion of all SEK/PEK associated to the SEK/PEK ID.</li> <li>4. The terminal receives the next STKM for the decryption of video</li> <li>5. The terminal sends the STKM to the smartcard</li> <li>6. The smartcard detects that SEK/PEK is inexistent for this SEK/PEK ID (see <a href="#">5.5.2.3.3</a> and <a href="#">5.5.2.3.4: Incorrect STKM generation – inexistent SEK/PEK</a>)</li> <li>7. The smartcard doesn't generate the TEK and the status code is '6A88' (referenced data not found).</li> </ol>
<b>Pass-Criteria</b>	<p>Video is decrypted less than 2,50 min. It is decrypted during 10*5=50s</p> <p>On the spy: the status code returned by the card is '6A88' (referenced data not found).</p> <p>Terminal asks user to register to that service.</p> <p>BSM receives a LTKM request from the terminal</p>

### 5.5.2.3.7 SPE deletion from the server

This test is relative to the layer2 but the test procedure and pass criteria needs that the test [5.5.2.3.3](#) and [5.5.2.3.4](#) passed successfully first.

<b>Test Case Id</b>	BCAST-1.0-DIST-int-627
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	BSM / BSDA sends an LTKM with TSlow>TShigh to delete data associated to the given SPE and SEK/PEK ID.
<b>Specification Reference</b>	SPCP spec: 6.6, 6.6.7.4
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	



<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test 5.5.2.3.1: 'Correct STKM parsing by the Smartcard' passed successfully. The smartcard has the following valid SEK/PEK</p> <ul style="list-style-type: none"> <li>• Key domainID= MCC1   MNC1</li> <li>• SEK/PEK ID = 0003 0001</li> <li>• with a security_policy_extension = 0x04</li> <li>• KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li> <li>• Key domainID= MCC1   MNC1</li> <li>• SEK/PEK ID = 0003 0001</li> <li>• with a security_policy_extension = 0x05</li> <li>• KV: TSlow= 0x00 00 01 00; TShigh= 0x00 00 01 0F</li> </ul> <p>The video is decrypted successfully</p>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Before the end of the Key validity of the SEK/PEK (when TS of the STKM reaches 0x00 00 00 05), BSM sends a LTKM for the same SEK/PEK ID, with a SPE=0x04, and KV: TSlow =0x00 00 00 01 TShigh=0x00 00 00 00</li> <li>2. The terminal sends the LTKM to the smartcard</li> <li>3. The smartcard detects that the LTKM is for a deletion of SPE associated to the SEK/PEK ID.</li> <li>4. The terminal receives the next STKM for the decryption of video</li> <li>5. The terminal sends the STKM to the smartcard</li> <li>6. The smartcard detects that SPE=0x04 is not existent for this SEK/PEK ID, and Key validity check fails with SPE=0x05.</li> <li>7. The smartcard doesn't generate the TEK and the status code is '9865' (Key freshness failure).</li> <li>8. BSM sends a LTKM for the same SEK/PEK ID, with a SPE=0x05, and KV: TSlow =0x00 00 00 01 TShigh=0x00 00 00 00</li> <li>9. The terminal sends the LTKM to the smartcard</li> <li>10. The smartcard detects that the LTKM is for a deletion of SPE, and delete the SEK/PEK as no other SPE are associated to this SEK/PEK ID</li> <li>11. The terminal receives the next STKM for the decryption of video</li> <li>12. The terminal sends the STKM to the smartcard</li> <li>13. The smartcard detects that SEK/PEK is not existent for this SEK/PEK ID (see 5.5.2.3.3 and 5.5.2.3.4: Incorrect STKM generation – inexistent SEK/PEK)</li> <li>14. The smartcard doesn't generate the TEK and the status code is '6A88' (referenced data not found).</li> </ol>

<b>Pass-Criteria</b>	<p>Video is decrypted less than 2.50 min. It is decrypted during 10*5=50s</p> <p>Terminal may asks user to register to that service.</p> <p>BSM may receive a LTKM request from the terminal</p> <p>On the spy:</p> <p>After receiving the first LTKM for SPE deletion, the status word returned by the card is '9865' (Key freshness failure)</p> <p>After receiving the second LTKM for SPE deletion, the status word returned by the card is '6A88' (referenced data not found).</p>
----------------------	---

### 5.5.2.3.8 STKM processing based on the LTKM security policy extension (SPE)

#### 5.5.2.3.8.1. STKM processing when LTKM SPE=0x00; testing live\_ppt\_purse

<b>Test Case Id</b>	BCAST-1.0-DIST-int-628
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when LTKM SPE=0x00, with token decrease in live_ppt_purse
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.7: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001. STKM replay detection counter in the card corresponding to this SEK/PEK ID is set to 0x00 00 00 00</p> <p>A LTKM is sent by the BSM for the SEK/PEK:</p> <ul style="list-style-type: none"> <li>• Key domainID= MCC1   MNC1</li> <li>• SEK/PEK ID = 0003 0001</li> <li>• With security-policy-extension = 0x00</li> <li>• KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li> <li>• Token-value = 0x11</li> <li>• Purse-mode = 0x00 (set mode)</li> <li>• Cost-value: 0x02</li> </ul>

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of the service token PPT live (SPE=0x00) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 50s</li> </ol> </li> <li>2. checking live_ppt_purse value: <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with purse_value=0x07</li> </ol> </li> <li>3. Test of STKM replay detection check: <ol style="list-style-type: none"> <li>a. STKM are resent by the BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS 0x00 00 00 01</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPE that allows replay content, but no SPE is corresponding (failure)</li> <li>e. no video is displayed during 10s.</li> </ol> </li> <li>4. Test of lack of credit in live_ppt_purse <ol style="list-style-type: none"> <li>a. STKM are resent by the BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard decrypts the TEK and sends them to the terminal</li> <li>d. Video is then displayed during 30s (here Purse_value=0x01)</li> <li>e. Smartcard send back error message “lack of credit in live_ppt_purse”</li> </ol> </li> </ol>
-----------------------	--

<b>Pass-Criteria</b>	<p>Video is displayed during 50s, then not displayed during 10s, and displayed during 30s.</p> <p>On the server side a Reporting Message is received with</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x00</li> <li>• Cost_value= 0x02</li> <li>• Purse_value=0x07 (value of live_ppt_purse)</li> </ul> <p>At the end, Terminal may display a message indicating lack of credit.</p> <p>On the spy:</p> <p>AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times)</p> <p>AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message,</p> <p>then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (3 times)</p> <p>then AUTHENTICATE (in MTK generation mode) command response with “BCAST management data status code” (tag80) equal to 0x01 (lack of credit in live_ppt_purse)</p>
----------------------	--

**5.5.2.3.8.2. STKM processing when LTKM SPE=0x01; testing playback\_ppt\_purse**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-629
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when LTKM SPE=0x01, with token decrease in playback_ppt_purse
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	

<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>Previous test <b>BCAST-1.0-DIST-int-628</b> is passed successfully, STKM replay detection counter in the card corresponding to SEK/PEK ID = 0003 0001 is set to 0x00 00 00 08</p> <p>A LTKM is sent by the BSM for the SEK/PEK:</p> <p>Key domainID= MCC1   MNC1</p> <p>SEK/PEK ID = 0003 0001</p> <p>With security-policy-extension = 0x01</p> <p>KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</p> <p>Token-value = 0x11</p> <p>Purse-mode = 0x00 (set mode)</p> <p>Cost-value = 0x02</p>
----------------------	--

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of playback ppt mode <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 00 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPE=0x01 (success)</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 50s</li> </ol> </li> <li>2. Checking playback_ppt_purse value: <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID =0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x01</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting message with purse_value=0x07</li> </ol> </li> <li>3. Test of STKM replay detection check <ol style="list-style-type: none"> <li>a. STKM are resent by the BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard perform Key Validity check for SPE that allows live content, but no SPE is corresponding (failure)</li> <li>e. no video is displayed during 10s</li> </ol> </li> <li>4. Test of lack of credit in playback_ppt_purse: <ol style="list-style-type: none"> <li>a. After a cryptoperiod, STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 04 and TS increasing by one for each crypto-period (10 s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPE=0x01 (success)</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 30 s (here purse value becomes 0x01)</li> <li>g. Smartcard send back error message ' lack of credit in playback_ppt_purse'</li> </ol> </li> </ol>
-----------------------	--

<b>Pass-Criteria</b>	<p>Video is displayed during 50s, then not displayed during 10s, and then displayed during 30s</p> <p>On the server side, a Reporting Message is received with is received with</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x01</li> <li>• Cost_value= 0x02</li> <li>• Purse_value=0x07 (value of playback_ppt_purse)</li> </ul> <p>At the end, a message is displayed on the handset indicating lack of credit.</p> <p>On the spy:</p> <p>AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times)</p> <p>AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message</p> <p>then AUTHENTICATE (in MTK generation mode) command response with SW=9865 (key freshness failure)</p> <p>then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (3 times)</p> <p>then AUTHENTICATE (in MTK generation mode) command response with “BCAST management data status code” (tag80) equal to 0x02 (lack of credit in playback_ppt_purse)</p>
----------------------	--

#### 5.5.2.3.8.3. STKM processing when LTKM SPE=0x02; testing user\_purse

<b>Test Case Id</b>	BCAST-1.0-DIST-int-630
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when LTKM SPE=0x02, with decrease of user_purse token
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	

<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001. STKM replay counter in the card corresponding this SEK/PEK is set to 0x00 00 00 00.</p> <ul style="list-style-type: none"> <li>• A LTKM is sent by the BSM for the SEK/PEK:</li> <li>• Key domainID= MCC1   MNC1</li> <li>• SEK/PEK ID = 0003 0001</li> <li>• With security-policy-extension = 0x02</li> <li>• KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li> <li>• Token-value= 0x11</li> <li>• Purse-mode= 0x00 (set mode)</li> <li>• Cost-value= 0x02</li> </ul>
<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of the user token ppt live       <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 50s</li> </ol> </li> <li>2. checking user_purse value:       <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with purse_value=0x07</li> </ol> </li> <li>3. test of lack of credit in user_purse       <ol style="list-style-type: none"> <li>a. STKM are sent by the BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 06 to 0x00 00 00 09</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard decrypts the TEK and sends them to the terminal</li> <li>d. Video is then displayed during 30s (here Purse_value=0x01)</li> <li>e. Smartcard send back error message “lack of credit in user_purse”</li> </ol> </li> </ol>



<b>Pass-Criteria</b>	<p>Video is displayed during 50s + 30s</p> <p>On the server side, a Reporting Message is received with is received with</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x02</li> <li>• Cost_value= 0x02</li> <li>• Purse_value=0x07 (value of user_purse)</li> </ul> <p>At the end, a message may be displayed on the handset indicating lack of credit.</p> <p>On the spy:</p> <p>AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times)</p> <p>AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message,</p> <p>then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (3 times)</p> <p>then AUTHENTICATE (in MTK generation mode) command response with “BCAST management data status code” (tag80) equal to 0x04 (lack of credit in the user_purse)</p>
----------------------	---

**5.5.2.3.8.4. STKM processing when LTKM SPE=0x07; testing playback\_counter**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-631
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when LTKM SPE=0x07, with decrease of playback_counter
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	

<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p><b>BCAST-1.0-DIST-int-630</b> is passed successfully, STKM replay detection counter in the card corresponding to SEK/PEK ID = 0003 0001 is set to 0x00 00 00 08</p> <p>A LTKM is sent by the BSM for the SEK/PEK:</p> <ul style="list-style-type: none"><li>• Key domainID= MCC1   MNC1</li><li>• SEK/PEK ID = 0003 0001</li><li>• With security-policy-extension = 0x07</li><li>• KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li><li>• Purse_flag= 0</li><li>• add_flag = 0x00 (set mode)</li><li>• number_playback = 0x05</li></ul> <p>Current_TS_counter is set automatically in the card with 0x00 00 00 0F. (=TShigh)</p>
----------------------	--

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of playback PPP mode <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS set to 0x00 00 00 01 <ol style="list-style-type: none"> <li>o Video data sent during 10s</li> </ol> </li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPE=0x07 (success)</li> <li>e. Smartcard perform current_TS_counter check, and STKM TS is lower. <ol style="list-style-type: none"> <li>o Current_TS_counter is set to STKM TS value=0x00 00 00 01</li> <li>o Playback_counter is decreased</li> </ol> </li> <li>f. Smartcard decrypts the TEK and sends them to the terminal</li> <li>g. Video is then displayed during 10 s</li> <li>h. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS set to 0x00 00 00 02 <ol style="list-style-type: none"> <li>o Video data sent during 10s</li> </ol> </li> <li>i. Terminal receives the messages and sends them to the smartcard</li> <li>j. Smartcard perform STKM replay detection check against TS (failure)</li> <li>k. Smartcard perform Key Validity check for SPE=0x07 (success)</li> <li>l. Smartcard perform current_TS_counter check, and STKM TS is greater. <ol style="list-style-type: none"> <li>o Current_TS_counter is set to STKM TS value=0x00 00 00 02</li> <li>o Playback_counter is NOT decreased</li> </ol> </li> <li>m. Smartcard decrypts the TEK and sends them to the terminal</li> <li>n. Video is then displayed during 10 s</li> </ol> </li> <li>2. checking playback_counter value: <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x07</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting value with playback_counter=0x04</li> </ol> </li> <li>3. Test of STKM replay detection check <ol style="list-style-type: none"> <li>a. STKM are resent by the BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS 0x00 00 00 10</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard perform Key Validity check for SPE that allows live content, but no SPE is corresponding (failure)</li> </ol> </li> </ol>
-----------------------	---

<p><b>Test Procedure</b> (continued)</p>	<p>4. Test of lack of credit in playback_counter</p> <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1  MNC1; SEK/PEK ID = 0003 0001 with TS set to 0x00 00 00 01. <ul style="list-style-type: none"> <li>o For each crypto-period (10 s), TEK_ID increase by 1 but TS value is the same. Video data sent during 60s</li> </ul> </li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPE=0x07 (success)</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Smartcard perform current_TS_counter check, and STKM TS is equal or lower. <ul style="list-style-type: none"> <li>o Playback_counter is decreased</li> </ul> </li> <li>g. Video is then displayed during 40 s (here playback_counter becomes 0x00)</li> <li>h. Smartcard send back error message 'playback counter invalid or equal to zero'</li> </ol>
<p><b>Pass-Criteria</b></p>	<p>Video is displayed during 20s, then not displayed during 10s, and then displayed during 40s</p> <p>On the server side, a Reporting Message is received with</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x07</li> <li>• Add_flag= 0x00</li> <li>• Playback_counter=0x04</li> </ul> <p>If returned Playback_counter is equal to 0x03 after 20s streaming, this means playback_counter has been decreased despite TS sent was greater than current_TS_counter. This is an error.</p> <p>After 70sec, a message may be displayed on the handset indicating playback_counter equal to zero.</p> <p>On the spy:</p> <p>AUTHENTICATE (in MTK generation mode) command response contains decrypted material (2 times)</p> <p>AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message,</p> <p>then AUTHENTICATE (in MTK generation mode) command response with error SW</p> <p>then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (4 times)</p> <p>then AUTHENTICATE (in MTK generation mode) command response with "BCAST management data status code" (tag80) equal to 0x05 (playback_counter invalid or equal to zero)</p>

## 5.5.2.3.8.5. STKM processing when LTKM SPE=0x0C; testing TEK counter

<b>Test Case Id</b>	BCAST-1.0-DIST-int-632
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when LTKM SPE=0x0C, with decrease of TEK counter
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	Spy of the terminal/Smartcard interface
<b>Test code</b>	
<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001. STKM replay counter in the card is set to 0x00 00 00 00</p> <p>A LTKM is sent by the BSM for the SEK/PEK ID = 0003 0001</p> <ul style="list-style-type: none"> <li>• SPE = 0x0C</li> <li>• KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li> <li>• Purse_flag= 0</li> <li>• Add_flag = 0</li> <li>• Keep_credit_flag = 1</li> <li>• Number_TEK= 0x08</li> </ul> <p>A LTKM is sent by the BSM for the SEK/PEK ID = 0003 0002</p> <ul style="list-style-type: none"> <li>• SPE = 0x0C</li> <li>• KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li> <li>• Purse_flag= 0</li> <li>• Add_flag = 0</li> <li>• Keep_credit_flag = 0</li> <li>• Number_TEK= 0x05</li> </ul>

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of the Pay per time Live             <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 50s</li> </ol> </li> <li>2. checking TEK counter:             <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with TEK_counter=0x00 00 00 03</li> <li>d. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0002, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C</li> <li>e. The terminal receives the LTKM and sends it to the smartcard</li> <li>f. The smartcard sends back a LTKM Reporting Message with TEK_counter=0x00 00 00 05</li> </ol> </li> <li>3. testing reporting of TEK over different SEK/PEK with same key group part             <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0002 with TS from 0x00 00 00 01</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Kept TEK counter value (0x00 00 00 03) shall be added to the TEK counter</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 10s</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0002, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with TEK_counter=0x00 00 00 07</li> </ol> </li> <li>4. test of lack of credit in TEK counter             <ol style="list-style-type: none"> <li>a. STKM are sent by the BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0002 with TS from 0x00 00 00 02 to 0x00 00 00 0F</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard decrypts the TEK and sends them to the terminal</li> <li>d. Video is then displayed during 70s (here TEK_counter=0x00)</li> <li>e. Smartcard send back error message “lack of credit in TEK counter”</li> </ol> </li> </ol>
-----------------------	--

<b>Pass-Criteria</b>	<p>Video is displayed during 50s + 10s + 70s</p> <p>After 130sec (2min10s), a message may be displayed on the handset indicating lack of credit.</p> <p>On the server side, a Reporting Message is received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x0C</li> <li>• Add_flag= 0x00</li> <li>• Keep_credit_flag=0x01</li> <li>• TEK_counter=0x00 00 00 03</li> </ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x0C</li> <li>• Add_flag= 0x00</li> <li>• Keep_credit_flag=0x01</li> <li>• TEK_counter=0x00 00 00 05</li> </ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x0C</li> <li>• Add_flag= 0x00</li> <li>• Keep_credit_flag=0x01</li> <li>• TEK_counter=0x00 00 00 07</li> </ul> <p>On the spy:</p> <p>AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times)</p> <p>AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message with TEK counter value (2 times),</p> <p>AUTHENTICATE (in MTK generation mode) command response contains decrypted material (1 times)</p> <p>AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message with TEK counter value (1 times),</p> <p>then AUTHENTICATE command response contains decrypted material (7 times)</p> <p>then AUTHENTICATE command response with “BCAST management data status code” (tag80) equal to 0x03 (lack of credit in the TEK counter)</p>
----------------------	---

### 5.5.2.3.9 STKM processing by priority order

#### 5.5.2.3.9.1. Testing SPE priorities : live content with subscription

<b>Test Case Id</b>	BCAST-1.0-DIST-int-633
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when several SPE allowing live content are available. Test that STKM are processed by LTKM SPE priority order. Subscription valid (SPE=0x04) case
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	none
<b>Test code</b>	



<p><b>Preconditions</b></p>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001. STKM replay detection counter in the card is set to 0x00 00 00 00</p> <p>Smartcard shall support SPE=0x04, 0x08, 0x0C, 0x00 and 0x02. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly.</p> <p>Following LTKM are sent by the BSM,</p> <ul style="list-style-type: none"> <li>• SPE=0x04 (subscription)</li> <li>• SPE=0x08 (user token PPV) <ul style="list-style-type: none"> <li>○ Token-value: 0x03 (user_purse for SPE=0x08)</li> <li>○ Purse-mode : 0x00 (set mode)</li> <li>○ Cost-value: 0x01</li> </ul> </li> <li>• SPE=0x0C (PPT) <ul style="list-style-type: none"> <li>○ Purse_flag=0</li> <li>○ Add_flag=0</li> <li>○ Keep_credit_flag=1</li> <li>○ Number_TEKs=0x03</li> </ul> </li> <li>• SPE=0x00 (service token PPT) <ul style="list-style-type: none"> <li>○ Token-value: 0x03 (live_ppt_purse)</li> <li>○ Purse-mode : 0x00 (set mode)</li> <li>○ Cost-value: 0x01</li> </ul> </li> <li>• SPE=0x02 (user token PPT) <ul style="list-style-type: none"> <li>○ Token-value: 0x03 (user_purse for SPE=0x02)</li> <li>○ Purse-mode : 0x00 (set mode)</li> <li>○ Cost-value: 0x01</li> </ul> </li> <li>• Common to all SPE : <ul style="list-style-type: none"> <li>○ Key domainID= MCC1   MNC1</li> <li>○ SEK/PEK ID = 0003 0001,</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 01 00</li> </ul> </li> </ul>
-----------------------------	--

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of subscription mode (SPE=0x04) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 10 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 160s</li> </ol> </li> <li>2. checking purse/counter values <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with purse value=3</li> <li>d. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C</li> <li>e. The terminal receives the LTKM and sends it to the smartcard</li> <li>f. The smartcard sends back a LTKM Reporting Message with TEK_counter=3</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with live_ppt_purse=3</li> <li>j. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02</li> <li>k. The terminal receives the LTKM and sends it to the smartcard</li> <li>l. The smartcard sends back a LTKM Reporting Message with purse value=3</li> </ol> </li> </ol>
-----------------------	--

<b>Pass-Criteria</b>	<p>Video is displayed during 160s =2.5min</p> <p>On the server side, Reporting Message are received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x08</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x03 (value of user_purse)</li> </ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x0C</li> <li>• Add_flag= 0x00</li> <li>• Keep_credit_flag =0x01</li> <li>• TEK_counter=0x03</li> </ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x00</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x03 (value of live_ppt_purse)</li> </ul> <p>LTKM Reporting Message 4:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x02</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x03 (value of user_purse)</li> <li>○</li> </ul> <p>If one of above purse/counter is decreased, this is an error since subscription mode (SPE=0x04) shall have highest priority among all SPE allowing live content consumption.</p>
----------------------	---

#### 5.5.2.3.9.2. Testing SPE priorities : live content without subscription

<b>Test Case Id</b>	BCAST-1.0-DIST-int-634
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when several SPE allowing live content are available. Test that STKM are processed by LTKM SPE priority order. No subscription (SPE=0x04)
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	none
<b>Test code</b>	

<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001. STKM replay detection counter in the smartcard is set to 0x00 00 00 00</p> <p>Smartcard shall support SPE=0x08, 0x0C, 0x00 and 0x02. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly.</p> <p>Following LTKM are sent by the BSM,</p> <ul style="list-style-type: none"> <li>• SPE=0x08 (user token PPV) <ul style="list-style-type: none"> <li>○ Token-value: 0x01 (user_purse for SPE=0x08)</li> <li>○ Purse-mode : 0x00 (set mode)</li> <li>○ Cost-value: 0x01</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 03</li> </ul> </li> <li>• SPE=0x0C (PPT) <ul style="list-style-type: none"> <li>○ Purse_flag=0</li> <li>○ Add_flag=0</li> <li>○ Keep_credit_flag=1</li> <li>○ Number_TEKs=0x03</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 06</li> </ul> </li> <li>• SPE=0x00 (service token PPT) <ul style="list-style-type: none"> <li>○ Token-value: 0x03 (live_ppt_purse)</li> <li>○ Purse-mode : 0x00 (set mode)</li> <li>○ Cost-value: 0x01</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 09</li> </ul> </li> <li>• SPE=0x02 (user token PPT) <ul style="list-style-type: none"> <li>○ Token-value: 0x03 (user_purse for SPE=0x02)</li> <li>○ Purse-mode : 0x01 (add mode)</li> <li>○ Cost-value: 0x01</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0C</li> </ul> </li> <li>• Common to all SPE : <ul style="list-style-type: none"> <li>○ Key domainID= MCC1   MNC1</li> <li>○ SEK/PEK ID = 0003 0001</li> </ul> </li> </ul>
----------------------	--

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of user token PPV mode (SPE=0x08) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is displayed for 30s</li> <li>f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08</li> <li>g. The terminal receives the LTKM and sends it to the smartcard</li> <li>h. The smartcard sends back a LTKM Reporting Message with purse value=3</li> </ol> </li> <li>2. Test of PPV mode (SPE=0x0C) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is displayed for 30s</li> <li>f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C</li> <li>g. The terminal receives the LTKM and sends it to the smartcard</li> <li>h. The smartcard sends back a LTKM Reporting Message with TEK_counter=0</li> </ol> </li> <li>3. Test of service token PPT mode (SPE=0x00) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 07 to 0x00 00 00 09 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is displayed for 30s</li> <li>f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00</li> <li>g. The terminal receives the LTKM and sends it to the smartcard</li> <li>e. The smartcard sends back a LTKM Reporting Message with live_ppt_purse=0</li> </ol> </li> </ol>
-----------------------	--

<b>Procedure (continued)</b>	<ol style="list-style-type: none"><li>4. Test of user token PPT mode (SPE=0x02)<ol style="list-style-type: none"><li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 0A to 0x00 00 00 0F and TS increasing by one for each crypto-period (10s)</li><li>b. Terminal receives the messages and sends them to the smartcard</li><li>c. Smartcard perform STKM replay detection check against TS (success)</li><li>d. Smartcard decrypts the TEK and sends them to the terminal</li><li>e. Video is displayed for 30s</li><li>f. Smartcard send back error message (because all purse are out of credit)</li><li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02</li><li>h. The terminal receives the LTKM and sends it to the smartcard</li><li>i. The smartcard sends back a LTKM Reporting Message with live_ppt_purse=0</li></ol></li></ol>
----------------------------------	--

<b>Pass-Criteria</b>	<p>Video is displayed during 30s+30s+30s+30s =2min                  After 2min, a message is displayed on the handset indicating lack of credit.</p> <p>On the server side, Reporting Message are received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x08</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x03 (value of user_purse)</li> </ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x0C</li> <li>• Add_flag= 0x00</li> <li>• Keep_credit_flag =0x01</li> <li>• TEK_counter=0x00</li> </ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x00</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x00 (value of live_ppt_purse)</li> </ul> <p>LTKM Reporting Message 4:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x02</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x00 (value of user_purse)</li> </ul> <p>If one of above purse/counter value is not equal to 0, this means another purse/counter has been decreased instead, this is an error.</p>
----------------------	--

**5.5.2.3.9.3. Testing SPE priorities : playback modes including SPE=0x05**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-635
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST



<b>Test Case Description</b>	STKM processing when several SPE allowing playback are available. Test that STKM are processed by LTKM SPE priority order. Unlimited playback (SPE=0x05) case
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	None
<b>Test code</b>	

**Preconditions**

The server provides a valid SRTP and STKM stream to the device

The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means

The preceding test **BCAST-1.0-DIST-int-634** passed successfully. STKM replay counter in the card is set to 0x00 00 00 0F and Current\_TS\_counter is set to 0x00 00 00 06. (TShigh)

Smartcard shall support SPE=0x05, 0x07, 0x09, 0x0D, 0x01 and 0x03. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly.

Following LTKM are sent by the BSM,

- SPE=0x05 (unlimited playback)
  - KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F
- SPE=0x07 (PPP playback)
  - Purse\_flag=0
  - Add\_flag =0
  - Number\_playback=2
  - KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 03
- SPE=0x09 (user token PPP playback)
  - Purse\_flag=1
  - Cost\_value=1
  - Purse\_mode=0 (set mode)
  - Token\_value : 0x02 (user purse for SPE=0x09)
  - KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 06
- SPE=0x0D (PPT playback)
  - Purse\_flag=0
  - Add\_flag=0
  - Number\_TEKs=0x02
  - KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 09
- SPE=0x01 (service token PPT playback)
  - Purse\_flag=1
  - Cost\_value=1
  - Purse\_mode=0 (set mode)
  - Token\_value : 0x02 (playback ppt\_purse)
  - KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0C
- SPE=0x03 (user token PPT playback)
  - Purse\_flag=1
  - Cost\_value=1
  - Purse\_mode=1 (add mode)
  - Token\_value : 0x02 (user purse for SPE=0x03)
  - KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F
- Common to all SPE :
  - Key domainID= MCC1|| MNC1
  - SEK/PEK ID = 0003 0001

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Test of unlimited playback mode (SPE=0x05) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 01 01 during 10s and then with TS=0x00 00 01 02 during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard returns an error, as there is no SPE allowing live content rendering</li> <li>e. Error message appear on the screen, Video is not displayed</li> <li>f. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 01 during 10s and then with TS=0x00 00 00 02 during 10s</li> <li>g. Terminal receives the messages and sends them to the smartcard</li> <li>h. Smartcard perform STKM replay detection check against TS (failure)</li> <li>i. Smartcard returns decrypted material to terminal</li> <li>j. Video is displayed during 20s</li> <li>k. Repeat step f to j 10 times. Video is displayed 200s (3min20s)</li> </ol> </li> <li>2. checking purse/counter values <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x07</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with playback_counter=2</li> <li>d. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x09</li> <li>e. The terminal receives the LTKM and sends it to the smartcard</li> <li>f. The smartcard sends back a LTKM Reporting Message with purse value=4</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0D</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with TEK_counter=2</li> <li>j. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x01</li> <li>k. The terminal receives the LTKM and sends it to the smartcard</li> <li>l. The smartcard sends back a LTKM Reporting Message with playback_ppt_purse=2</li> <li>m. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x03</li> <li>n. The terminal receives the LTKM and sends it to the smartcard</li> <li>o. The smartcard sends back a LTKM Reporting Message with purse value=4</li> </ol> </li> </ol>
-----------------------	--

<b>Pass-Criteria</b>	<p>During first 20s, no video is displayed and an error message appears.</p> <p>Then the same 20sec video sequence is displayed 11 times, total display time is 220s=3min40s</p> <p>On the server side, Reporting Message are received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"><li>• Consumption_reporting_flag=1</li><li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li><li>• Security_policy_extension = 0x07</li><li>• playback_counter=0x02</li></ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"><li>• Consumption_reporting_flag=1</li><li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li><li>• Security_policy_extension = 0x09</li><li>• Cost_value= 0x01</li><li>• Purse_value=0x04 (value of user_purse)</li></ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"><li>• Consumption_reporting_flag=1</li><li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li><li>• Security_policy_extension = 0x0D</li><li>• Add_flag= 0x00</li><li>• TEK_counter=0x02</li></ul> <p>LTKM Reporting Message 4:</p> <ul style="list-style-type: none"><li>• Consumption_reporting_flag=1</li><li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li><li>• Security_policy_extension = 0x01</li><li>• Cost_value= 0x01</li><li>• Purse_value=0x02 (value of playback_ppt_purse)</li></ul>
----------------------	---

<b>Pass-Criteria (continued)</b>	<p>LTKM Reporting Message 5:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x03</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x04 (value of user_purse)</li> </ul> <p>If one of above purse/counter is decreased, this is an error since unlimited playback mode (SPE=0x05) has highest priority among all SPE allowing playback.</p>
----------------------------------	---

**5.5.2.3.9.4. Testing SPE priorities : playback modes without SPE=0x05**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-636
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when several SPE allowing playback are available. Test that STKM are processed by LTKM SPE priority order. No unlimited playback (SPE=0x05) case
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	None
<b>Test code</b>	
<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001. STKM replay conter in the card is set to 0x00 00 00 00.</p> <p>Smartcard shall support SPE=0x04, 0x07, 0x09, 0x0D, 0x01 and 0x03. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly.</p> <p>Following LTKM are sent by the BSM,</p> <ul style="list-style-type: none"> <li>• SPE=0x04 (subscription live)             <ul style="list-style-type: none"> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 01 00</li> </ul> </li> <li>• SPE=0x07 (PPP playback)             <ul style="list-style-type: none"> <li>○ Purse_flag=0</li> <li>○ Add_flag =0</li> <li>○ Number_playback=2</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 03</li> </ul> </li> <li>• SPE=0x09 (user token PPP playback)             <ul style="list-style-type: none"> <li>○ Purse_flag=1</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>○ Cost_value=1</li><li>○ Purse_mode=0 (set mode)</li><li>○ Token_value : 0x02 (user purse for SPE=0x09)</li><li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 06</li><li>• SPE=0x0D (PPT playback)<ul style="list-style-type: none"><li>○ Purse_flag=0</li><li>○ Add_flag=0</li><li>○ Number_TEKs=0x02</li><li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 09</li></ul></li><li>• SPE=0x01 (service token PPT playback)<ul style="list-style-type: none"><li>○ Purse_flag=1</li><li>○ Cost_value=1</li><li>○ Purse_mode=0 (set mode)</li><li>○ Token_value : 0x02 (playback ppt_purse)</li><li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0C</li></ul></li><li>• SPE=0x03 (user token PPT playback)<ul style="list-style-type: none"><li>○ Purse_flag=1</li><li>○ Cost_value=1</li><li>○ Purse_mode=1 (add mode)</li><li>○ Token_value : 0x02 (user purse for SPE=0x03)</li><li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 0F</li></ul></li><li>• Common to all SPE :<ul style="list-style-type: none"><li>○ Key domainID= MCC1   MNC1</li><li>○ SEK/PEK ID = 0003 0001,</li></ul></li></ul> <p>Current_TS_counter is set to 0x00 00 01 00.</p>
--	---

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. test preparation : setting STKM replay counter <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 10 during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. SPE=0x04 allows live content access. STKMreplay detection counter is set to TS=0x00 00 00 10</li> <li>e. Smartcard decrypt the TEK and sends them to terminal</li> <li>f. Video is displayed during 10s</li> </ol> </li>   <li>2. Test of playback PPP mode (SPE=0x07) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 01 during 10s and then with TS=0x00 00 00 02 during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPEs allowing playback (success)</li> <li>e. Smartcard returuns decrypted material to terminal</li> <li>f. Video is displayed during 20s</li> <li>g. Repeat step a to e. Video is displayed another 20s</li> <li>h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x07</li> <li>i. The terminal receives the LTKM and sends it to the smartcard</li> <li>j. The smartcard sends back a LTKM Reporting Message with playback_counter=0</li> </ol> </li>   <li>3. Test of user token PPP playback mode (SPE=0x09) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 04 during 10s and then with TS=0x00 00 00 05 during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPEs allowing playback (success)</li> <li>e. Smartcard returuns decrypted material to terminal</li> <li>f. Video is displayed during 20s</li> <li>g. Repeat step a to e. Video is displayed another 20s</li> <li>h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x09</li> <li>i. The terminal receives the LTKM and sends it to the smartcard</li> <li>j. The smartcard sends back a LTKM Reporting Message with purse value=2</li> </ol> </li> </ol>
-----------------------	--

<p><b>Test Procedure (continued)</b></p>	<ol style="list-style-type: none"> <li>4. Test of PPT playback mode (SPE=0x0D) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 07 during 10s and then with TS=0x00 00 00 08 during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPEs allowing playback (success)</li> <li>e. Smartcard returns decrypted material to terminal</li> <li>f. Video is displayed during 20s</li> <li>g. Repeat step a to e. Video is displayed another 20s</li> <li>h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0D</li> <li>i. The terminal receives the LTKM and sends it to the smartcard</li> <li>j. The smartcard sends back a LTKM Reporting Message with TEK_counter =0</li> </ol> </li>   <li>5. Test of service token PPT playback mode (SPE=0x01) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 0A during 10s and then with TS=0x00 00 00 0B during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPEs allowing playback (success)</li> <li>e. Smartcard returns decrypted material to terminal</li> <li>f. Video is displayed during 20s</li> <li>g. Repeat step a to e. Video is displayed another 20s</li> <li>h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x01</li> <li>i. The terminal receives the LTKM and sends it to the smartcard</li> <li>j. The smartcard sends back a LTKM Reporting Message with playback_ppt_purse =0</li> </ol> </li>   <li>6. Test of user token PPT playback mode (SPE=0x03) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 0D during 10s and then with TS=0x00 00 00 0E during 10s</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. Smartcard perform Key Validity check for SPEs allowing playback (success)</li> <li>e. Smartcard returns decrypted material to terminal</li> <li>f. Video is displayed during 20s</li> <li>g. Repeat step a to e. Video is displayed another 20s</li> </ol> </li> </ol>
--	--



<p><b>Test Procedure (continued)</b></p>	<ul style="list-style-type: none"> <li>h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1  MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x03</li> <li>i. The terminal receives the LTKM and sends it to the smartcard</li> <li>j. The smartcard sends back a LTKM Reporting Message with purse value=0</li> <li>k. Repeat step a to e. This time no video is displayed and an error message is displayed</li> </ul>
<p><b>Pass-Criteria</b></p>	<p>During first 10s, video is displayed (live content).                  Then the same 20sec video sequence is displayed 10 times, total display time is 200s=3min20s                  Finally, an error message is displayed indicating lack of credit in user purse.</p> <p>On the server side, Reporting Message are received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x07</li> <li>• playback_counter=0x00</li> </ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x09</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x02 (value of user_purse)</li> </ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x0D</li> <li>• Add_flag= 0x00</li> <li>• TEK_counter=0x00</li> </ul> <p>LTKM Reporting Message 4:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x01</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x00 (value of playback_ppt_purse)</li> </ul>

<b>Pass-Criteria (continued)</b>	<p>LTKM Reporting Message 5:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x03</li> <li>• Cost_value= 0x01</li> <li>• Purse_value=0x00 (value of user_purse)</li> </ul> <p>If one of above purse/counter is not equal to 0, this means another purse with lower priority has been decreased instead This is an error.</p>
--------------------------------------	--

#### 5.5.2.3.9.5. Testing KV priorities when several LTKM available with same SPE

<b>Test Case Id</b>	BCAST-1.0-DIST-int-637
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when several LTKM are available with same SPE. Testing that STKM are processed in KV priority order. Test with SPE=0x00 (service token PPT)
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	none
<b>Test code</b>	

<p><b>Preconditions</b></p>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001</p> <p>Smartcard shall support SPE=0x00. If SPE=0x00 is not supported, test can be adapted with other SPE value with purse.</p> <p>Following LTKM are sent by the BSM,</p> <ul style="list-style-type: none"> <li>• LTKM1 <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 03 00 (live_ppt_purse)</li> <li>○ Purse-mode : 0x00 (set mode)</li> <li>○ Cost-value: 0x01 00</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 03</li> </ul> </li> <li>• LTKM2 <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 00 30 (live_ppt_purse)</li> <li>○ Purse-mode : 0x01 (add mode)</li> <li>○ Cost-value: 0x00 10</li> <li>○ KV: TSlow= 0x00 00 00 02; TShigh= 0x00 00 00 06</li> </ul> </li> <li>• LTKM3 <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 00 03 (live_ppt_purse)</li> <li>○ Purse-mode : 0x01 (add mode)</li> <li>○ Cost-value: 0x00 01</li> <li>○ KV: TSlow= 0x00 00 00 02; TShigh= 0x00 00 00 09</li> </ul> </li> <li>• Common to all LTKM : <ul style="list-style-type: none"> <li>○ Key domainID= MCC1   MNC1</li> <li>○ SEK/PEK ID = 0003 0001,</li> <li>○ Security Policy Extension = 0x00</li> </ul> </li> </ul> <p>STKM replay conter in the card corresponding to SEK/PEK ID = 0003 0001 is set to 0x00 00 00 00</p>
-----------------------------	--

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. checking live_ppt_purse value:             <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 03 33</li> </ol> </li> <li>2. Test that LTKM1 has first priority (lowest TSlow value)             <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 30s</li> <li>f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00</li> <li>g. The terminal receives the LTKM and sends it to the smartcard</li> <li>h. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 33</li> </ol> </li> <li>3. Test that LTKM2 has second priority (same TSlow, lowest TShigh value)             <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 30s</li> <li>f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00</li> <li>g. The terminal receives the LTKM and sends it to the smartcard</li> <li>h. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 03</li> </ol> </li> <li>4. Test that switch to LTKM3 (lowest priority)             <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 07 to 0x00 00 00 09 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. Smartcard decrypts the TEK and sends them to the terminal</li> <li>e. Video is then displayed during 30s (here Purse_value=0x00)</li> <li>f. Smartcard send back error message “lack of credit in live_ppt_purse”</li> </ol> </li> </ol>
-----------------------	--

<b>Pass-Criteria</b>	<p>Video is displayed during 30s+30s+30s=1min30s</p> <p>After 90sec, a message may be displayed on the handset indicating lack of credit.</p> <p>On the server side, a Reporting Message is received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x00</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 03 33 (value of live_ppt_purse)</li> </ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x00</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 33 (value of live_ppt_purse)</li> </ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x00</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 03 (value of live_ppt_purse)</li> </ul>
----------------------	--

**5.5.2.3.10 STKM processing when sent to different SPE sharing the same user purse**

<b>Test Case Id</b>	BCAST-1.0-DIST-int-638
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	STKM processing when sent to different SPE sharing the same user purse. User purse common to SPE=0x02, 0x03, 0x08, 0x09. Card is BCAST
<b>Specification Reference</b>	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	none
<b>Test code</b>	

<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <p>The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</p> <p>The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001</p> <p>Smartcard shall support SPE=0x02, 0x03, 0x08, 0x09. If one of these SPEs is not supported, test can be adapted accordingly.</p> <p>Following LTKM are sent by the BSM,</p> <ul style="list-style-type: none"> <li>• SPE=0x08 (user token PPV) <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 00 01</li> <li>○ Purse-mode : 0x01 (set mode)</li> <li>○ Cost-value: 0x00 01</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 03</li> </ul> </li> <li>• SPE=0x09 (user token PPP playback) <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 00 01</li> <li>○ Purse-mode : 0x01 (add mode)</li> <li>○ Cost-value: 0x00 01</li> <li>○ KV: TSlow= 0x00 00 00 00; TShigh= 0x00 00 00 03</li> </ul> </li> <li>• SPE=0x02 (user token PPT) <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 00 03</li> <li>○ Purse-mode : 0x01 (add mode)</li> <li>○ Cost-value: 0x00 01</li> <li>○ KV: TSlow= 0x00 00 00 04; TShigh= 0x00 00 00 06</li> </ul> </li> <li>• SPE=0x03 (user token PPT playback) <ul style="list-style-type: none"> <li>○ Token-value: 0x00 00 00 03</li> <li>○ Purse-mode : 0x01 (add mode)</li> <li>○ Cost-value: 0x00 01</li> <li>○ KV: TSlow= 0x00 00 00 04; TShigh= 0x00 00 00 06</li> </ul> </li> <li>• Common to all LTKM : <ul style="list-style-type: none"> <li>○ Key domainID= MCC1   MNC1</li> <li>○ SEK/PEK ID = 0003 0001,</li> </ul> </li> </ul>
----------------------	---

<b>Test Procedure</b>	<ol style="list-style-type: none"> <li>1. Checking user_purse value: <ol style="list-style-type: none"> <li>a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08</li> <li>b. The terminal receives the LTKM and sends it to the smartcard</li> <li>c. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 08</li> </ol> </li>   <li>2. Test SPE=0x08 (user token PPV) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. SPE=0x08 is an SPE allowing live content, and KV check pass. Smartcard decrease user_purse.</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 30s</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 07</li> </ol> </li>   <li>3. Test SPE=0x09 (user token PPP playback) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. SPE=0x09 is an SPE allowing playback content, and KV check pass. Smartcard decrease user_purse.</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 30s</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x09</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 06</li> </ol> </li> </ol>
-----------------------	---

<p><b>Test procedure (continued)</b></p>	<ol style="list-style-type: none"> <li>4. Test SPE=0x02 (user token PPT) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (success)</li> <li>d. SPE=0x02 is an SPE allowing live content, and KV check pass. Smartcard decrease user_purse at each crypto-period</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 30s</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 03</li> </ol> </li>   <li>5. Test SPE=0x03 (user token PPT playback) <ol style="list-style-type: none"> <li>a. STKM are sent by BSDA for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s)</li> <li>b. Terminal receives the messages and sends them to the smartcard</li> <li>c. Smartcard perform STKM replay detection check against TS (failure)</li> <li>d. SPE=0x03 is an SPE allowing playback content, and KV check pass. Smartcard decrease user_purse at each crypto-period.</li> <li>e. Smartcard decrypts the TEK and sends them to the terminal</li> <li>f. Video is then displayed during 30s</li> <li>g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x03</li> <li>h. The terminal receives the LTKM and sends it to the smartcard</li> <li>i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 00</li> </ol> </li> </ol>
--	--



<b>Pass-Criteria</b>	<p>Video is displayed during 30s+30s+30s+30s=2min</p> <p>On the server side, a Reporting Message is received with</p> <p>LTKM Reporting Message 1:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x08</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 08</li> </ul> <p>LTKM Reporting Message 2:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x08</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 07</li> </ul> <p>LTKM Reporting Message 3:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x09</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 06</li> </ul> <p>LTKM Reporting Message 4:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x02</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 03</li> </ul> <p>LTKM Reporting Message 5:</p> <ul style="list-style-type: none"> <li>• Consumption_reporting_flag=1</li> <li>• Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0</li> <li>• Security_policy_extension = 0x03</li> <li>• Cost_value= 0x00 01</li> <li>• Purse_value=0x00 00 00 00</li> </ul>
----------------------	--

### 5.5.2.3.11 STKM reception with parental control without PIN defined in the card

The test is not exhaustive and tests only one rating-type.

The rating-type is 0x00 and we work with the following rating values:

0x04 : minimum age = 7 years old

0x07 : minimum age = 10 years old

0x09 : minimum age = 12 years old

0x0B : minimum age = 14 years old

0x0D : minimum age = 16 years old

0x0F : minimum age = 18 years old

As the example given in the specification SPCP

<b>Test Case Id</b>	BCAST-1.0-DIST-int-456
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value
<b>Specification Reference</b>	SPCP spec: 6.6.5, 6.7; 6.7.3.9.1
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	none
<b>Test code</b>	
<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <ul style="list-style-type: none"> <li>○ The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</li> <li>○ The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001</li> </ul> <p>No PINCODE is defined in the smartcard</p>

<b>Test Procedure</b>	<p>BSM sends a Parental Control Message with a setting of parental control in the card: Level_granted is 0x0B and rating-type 0x00 without PINCODE in KEMAC (Encr Data len =0)</p> <p>BSM sends a LTKM for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001; KV is set from TSlow= 0x0100 to TShigh= 0x015F; security_policy_extension = 0x04</p> <p>BSM/BSDA pushes STKM over UDP to the terminal / smartcard, with different rating values:</p> <p>From TS= 0100 to TS= 010F : rating_value is 0x04</p> <p>From TS = 0110 to TS = 011F: rating-value is 0x0F</p> <p>From TS = 0120 to TS= 012F : rating-value is 0x07</p> <p>From TS = 0130 to TS= 013F : rating-value is 0x0d</p> <p>From TS = 0140 to TS= 014F : rating-value is 0x09</p> <p>From TS = 0150 to TS= 015F : rating-value is 0x0B</p>
<b>Pass-Criteria</b>	<p>The video is displayed during 2,50 mns</p> <p>Video is not displayed during 2,50 mns and a message indicating that the user is not allowed to watch the program is displayed to the user</p> <p>The video is displayed during 2,50 mns</p> <p>Video is not displayed during 2,50 mns and a message indicating that the user is not allowed to watch the program is displayed to the user</p> <p>The video is displayed during 5,33 mns</p>

**5.5.2.3.12 STKM reception with parental control and with PIN defined in the card**

The test is not exhaustive and tests only one rating-type.

The rating-type is 0x00 and we work with the following rating values:

0x04 : minimum age = 7 years old

0x07 : minimum age = 10 years old

0x09 : minimum age = 12 years old

0x0B : minimum age = 14 years old

0x0D : minimum age = 16 years old

0x0F : minimum age = 18 years old

<b>Test Case Id</b>	BCAST-1.0-DIST-int-457
<b>Test Object</b>	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
<b>Test Case Description</b>	BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value
<b>Specification Reference</b>	SPCP spec: 6.6.5, 6.7; 6.7.3.9.1
<b>SCR Reference</b>	BCAST-STKM_SC-C-010
<b>Tool</b>	none

<b>Test code</b>	
<b>Preconditions</b>	<p>The server provides a valid SRTP and STKM stream to the device</p> <ul style="list-style-type: none"> <li>○ The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means</li> <li>○ The test <b>5.5.2.3.6: Key deletion from server</b> passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001</li> </ul>
<b>Test Procedure</b>	<p>BSM sends a Parental Control Message with a setting of parental control in the card: Level_granted is 0x0B and rating-type 0x00 with a PINCODE encrypted in the KEMAC (PINCODE = 020579 as example given in the SPCP TS specification)</p> <p>BSM sends a LTKM for the service Key domainID= MCC1   MNC1; SEK/PEK ID = 0003 0001; KV is set from TSlow= 0x0100 to TShigh= 0x015F; security_policy_extension = 0x04</p> <p>BSM/BSDA pushes STKM over UDP to the terminal / smartcard, with different rating values:</p> <p>From TS= 0100 to TS= 010F : rating_value is 0x04</p> <p>From TS = 0110 to TS = 011F: rating_value is 0x0F</p> <p>From TS = 0120 to TS= 012F : rating_value is 0x07</p> <p>From TS = 0130 to TS= 013F : rating_value is 0x0D</p> <p>From TS = 0140 to TS= 014F : rating_value is 0x09</p> <p>From TS = 0150 to TS= 015F : rating_value is 0x0B</p>
<b>Pass-Criteria</b>	<ol style="list-style-type: none"> <li>1. The video is displayed during 2,50 mns</li> <li>2. Then a message to the user is sent for the verification of PIN: verify PIN</li> <li>3. Pin code is correctly entered (value of PINCODE 020579) and then</li> <li>4. Video is displayed during 5 mns</li> <li>5. Then a message to the user is sent for the verification of PIN: verify PIN</li> <li>6. Pin code is correctly entered (value of PINCODE 020579) and then</li> <li>7. Video is displayed during 7.50 mns</li> </ol>

### 5.5.2.3.13 Multiple streams protected with same STKM stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-458
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Test that video and audio streams protected with same STKM stream can be processed..
<b>Specification Reference</b>	6.7
<b>SCR Reference</b>	BCAST-STKM_SC-C-01, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-03
<b>Tool</b>	None
<b>Test code</b>	None

<b>Preconditions</b>	<ol style="list-style-type: none"> <li>1. A bootstrapping context exists between server and terminal.</li> <li>2. LTKMs containing the SEKs being used to protect the audio and video STKMs have already been sent to the device.</li> <li>3. The terminal knows the IP address and port on which the STKM streams and SRTP streams are being broadcast, e.g. via pre-provisioned SDP or other means.</li> </ol>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>▪ The terminal receives one STKM stream (for both audio and video content) protected with the SEKs it possesses.</li> <li>▪ The terminal can decrypt the content – audio and video.</li> </ul>
<b>Pass-Criteria</b>	The content (audio and video) can be accessed.

#### 5.5.2.3.14 Multiple streams protected with different STKM streams

<b>Test Case Id</b>	BCAST-1.0-DIST-int-459
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Test that video and audio streams protected with different STKM streams can only be accessed when both streams are available.
<b>Specification Reference</b>	6.7
<b>SCR Reference</b>	BCAST-STKM_SC-C-02, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-04
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	<ol style="list-style-type: none"> <li>1. A bootstrapping context exists between server and terminal.</li> <li>2. LTKMs containing the SEKs being used to protect the video (but not the audio) STKMs has already been sent to the device.</li> <li>3. The terminal knows the IP address and port on which the STKM streams and SRTP streams are being broadcast, e.g. via pre-provisioned SDP.</li> </ol>
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>▪ The terminal receives two STKM streams (for audio and video content). The video is protected with the SEKs it possesses but the audio is not.</li> <li>▪ The terminal can decrypt the video content but not the audio.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>▪ The video content can be accessed but the audio cannot.</li> </ul>

#### 5.5.2.4 Layer 4: Traffic Encryption layer

Tests of this layer are covered by common tests for DRM profile and Smartcard profile.

##### 5.5.2.4.1 Delivery of IPSec protected stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-460
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Opening an Ipv4 encrypted stream with key material associated to the subscription.
<b>Specification Reference</b>	[BCAST10–ServContProt] Section 9.1. [BCAST10–ServContProt] Section 6.8.1.

<b>SCR Reference</b>	BCAST-SPCP-C-002, BCAST-ContentLayer-C-008, BCAST-SDP-C-014. BCAST-TerminalCapability-C-003, BCAST-SPCP-C-005, BCAST-STKM –C-010, BCAST-LTKM-SC-C-015, BCAST-CP_RTP_SC-C-021, BCAST-SAC-C-028.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a service which is IPsec encrypted. subscriptionType is open-ended.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a IPsec protected service</li> <li>• View an IPsec encrypted programme.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service.</li> <li>• The terminal registers the service to be subscribed and disallows the end user to subscribe again.</li> <li>• The terminal is able to decrypt and render the IPsec encrypted audio and video streams belonging to the programme.</li> </ul>

#### 5.5.2.4.2 Delivery of SRTP protected stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-461
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Opening an SRTP encrypted stream with key material associated to the subscription.
<b>Specification Reference</b>	[BCAST10–ServContProt] Section 9.2. [BCAST10–ServContProt] Section 6.8.1.
<b>SCR Reference</b>	BCAST-SPCP-C-002, BCAST-ContentLayer-C-007, BCAST-SDP-C-014, BCAST-SRTPsignal-C-030. BCAST-TerminalCapability-C-003, BCAST-SPCP-C-005, BCAST-STKM –C-010, BCAST-LTKM-SC-C-015, BCAST-CP_RTP_SC-C-021, BCAST-SAC-C-028.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a service which is SRTP encrypted. subscriptionType is open-ended.

<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a SRTP protected service</li> <li>• View an SRTP encrypted programme.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service.</li> <li>• The terminal registers the service to be subscribed and disallows the end user to subscribe again.</li> <li>• The terminal is able to decrypt and render the SRTP encrypted audio and video streams belonging to the programme.</li> </ul>

### 5.5.2.4.3 Delivery of ISMACrypt protected stream

<b>Test Case Id</b>	BCAST-1.0-DIST-int-462
<b>Test Object</b>	BCAST Terminal and Server
<b>Test Case Description</b>	Opening an ISMACrypt encrypted stream with key material associated to the subscription.
<b>Specification Reference</b>	[BCAST10–ServContProt] Section 9.3. [BCAST10–ServContProt] Section 6.8.1.
<b>SCR Reference</b>	BCAST-SPCP-C-002, BCAST-ContentLayer-C-009, BCAST-SDP-C-014, BCAST-CP_Form-C-023. BCAST-TerminalCapability-C-003, BCAST-SPCP-C-005, BCAST-STKM –C-010, BCAST-LTKM-SC-C-015, BCAST-CP_RTP_SC-C-021, BCAST-SAC-C-028.
<b>Tool</b>	None
<b>Test code</b>	None
<b>Preconditions</b>	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a service which is ISMACrypt encrypted. subscriptionType is open-ended.
<b>Test Procedure</b>	<ul style="list-style-type: none"> <li>• Update the SG in the terminal using the test tool as the source</li> <li>• Browse the SG in the terminal</li> <li>• Subscribe to a ISMACrypt protected service</li> <li>• View an ISMACrypt encrypted programme.</li> </ul>
<b>Pass-Criteria</b>	<ul style="list-style-type: none"> <li>• The terminal is able to subscribe to the service.</li> <li>• The terminal registers the service to be subscribed and disallows the end user to subscribe again.</li> <li>• The terminal is able to decrypt and render the Ipsec encrypted audio and video streams belonging to the programme.</li> </ul>

## 5.6 Terminal Provisioning

### 5.6.1 Receiving terminal provisioning messages using TP-7

<b>Test Case Id</b>	BCAST-1.0-DIST-int-501
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to check that the terminal correctly receives provisioning messages using TP-7 over the interactive channel.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.2
<b>SCR Reference</b>	BCAST-SERVICES-C-011, BCAST-SERVICES-C-012
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	
<b>Test Procedure</b>	
<b>Pass-Criteria</b>	

### 5.6.2 Update terminal provisioning messages using TP-7

<b>Test Case Id</b>	BCAST-1.0-DIST-int-502
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to check that the terminal correctly receives an update of an provisioning messages using TP-7 over the interactive channel.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.2
<b>SCR Reference</b>	BCAST-SERVICES-C-011, BCAST-SERVICES-C-012
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	
<b>Test Procedure</b>	
<b>Pass-Criteria</b>	

### 5.6.3 Declaring Terminal Provisioning as a Service within Service Guide

<b>Test Case Id</b>	BCAST-1.0-DIST-int-503
<b>Test Object</b>	BCAST Client



<b>Test Case Description</b>	The purpose of this test is to check that the terminal declares the Terminal Provisioning as a Service within Service Guide correctly and the fragments are correctly send to the tool and checked.
<b>Specification Reference</b>	[BCAST10-Services] Section 5.2.2.1
<b>SCR Reference</b>	BCAST-G-T-009
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	
<b>Test Procedure</b>	
<b>Pass-Criteria</b>	

#### 5.6.4 Declaring Terminal Provisioning as an Access of a Service within Service Guide

<b>Test Case Id</b>	BCAST-1.0-DIST-int-504
<b>Test Object</b>	BCAST Client
<b>Test Case Description</b>	The purpose of this test is to check that the terminal declares the Terminal Provisioning as an access of a Service within Service Guide correctly and the fragments are correctly send to the tool and checked.
<b>Specification Reference</b>	[BCAST10-Ser vices] Section 5.2.1.1
<b>SCR Reference</b>	BCAST-G-T-008
<b>Tool</b>	
<b>Test code</b>	
<b>Preconditions</b>	
<b>Test Procedure</b>	

## Appendix A. Change History (Informative)

### A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

### A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ETS-BCAST_INT-V1_0	09 May 2007	all	First draft.
	17 May 2007	n/a	IOP WG decision to make the present draft public
	27 Jun 2007	All	SCR references updated. Broadcast and interaction channel operations separated.
	19 Jul 2007	Mainly 5.1, 5.3 and 5.5	Addition of CRs IOP BRO 98R01, 105 and 129R02
	24 Jul 2007	Title page and ToC	Minor typo in date and history updated.
Candidate Versions OMA-ETS-BCAST_INT-V1_0	07 Aug 2007	All	Status changed to Candidate by TP TP ref # OMA-TP-2007-0300- INP_ETS_BCAST_INT_V1_0_for_Candidate_Approval
Draft Versions OMA-ETS-BCAST_INT-V1_0	30 Jan 2008	All	Incorporation of CR: OMA-IOP-BRO-2007-0293R01
Candidate Versions OMA-ETS-BCAST_INT-V1_0	26 Feb 2008	All	Status changed to Candidate by TP TP ref # OMA-TP-2008-0071- INP_BCAST_1.0_INT_ETS_for_Notification