**Enabler Test Report**

**Mobile Broadcast (BCAST) v1.0**

OMA TestFest (January 2008)
Version 1st February 2008

Open Mobile Alliance
OMA-EnablerTestReport-TestFest-22-Jan2008-BCAST-10-20080201

This document is a work in process and is not an approved Open Mobile Alliance™ specification. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the Open Mobile Alliance specifications.

# Contents

# 1. Scope

This report describes the results from the testing carried out at OMA TestFest-22 (Janaury 2008) concerning the Mobile Broadcast Version 1.0 Enabler.

# 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 |
| [ERELD] | Enabler Release Definition, OMA-ERELD-BCAST-V1_0-20070529-C, URL:http://www.openmobilealliance.org/ |
| [BCAST_SPEC] | Enabler Release Package, OMA-ERP-BCAST-V1_0-20070529-C, URL:http://www.openmobilealliance.org/ |
| [ETS] | Enabler Test Specification OMA-ETS-BCAST_INT-V1_0-20070807-C, URL:http://www.openmobilealliance.org/ |
| [EVP] | Enabler Validation Plan OMA-EVP-BCAST-V1_0-20070807-C; URL:http://www.openmobilealliance.org/ |
| [BCAST_EICS] | BCAST version 1.0 Enabler Implementation Conformance Statement (EICS), OMA-EICS-BCAST_Client-V1_0-20070712-A, OMA-EICS-BCAST_Server-V1_0-20070712-A http://www.openmobilealliance.org/ |

## 2.2 Informative References

| | |
|---|---|
| [OMADICT] | Dictionary for OMA Specification, OMA-Dictionary http://www.openmobilealliance.org/ |

# 3. Terminology and Conventions

## 3.1 Conventions

This is an informative document which is not intended to provide testable requirements to implementations, i.e. the document does not intend to contain normative statements.

## 3.2 Definitions

TestFest          Multi-lateral interoperability testing event
Trusted Zone      An OMA staff function to provide a neutral confidential information and results collection service to OMA Members. The Trusted Zone is responsible for all reports resulting from an OMA Test Event and to ensure that all general reports cannot attributed to any one individual participating company

## 3.3 Abbreviations

BCAST          Mobile Broadcast

EICS           Enabler Implementation Conformance Statement

ERELD          Enabler Release Definition

ERP            Enabler Release Package

EVP            Enabler Validation Plan

ETS            Enabler Test Specification

INC            Inconclusive

N/A            Not Applicable

OMA            Open Mobile Alliance

OT             Out of Time

PR             Problem Report

TC             Test Case

# 4. Summary

This report gives details of the testing carried out during the OMA TestFest-22 (January 2008) for Mobile Broadcast (BCAST) v1.0.

The report is compiled on behalf of OMA by the OMA Trusted Zone.

The work and reporting has followed the OMA IOP processes and policies [IOPPROC].

# 5.  Test Details

## 5.1    Documentation

This chapter lists the details of the enabler and any documentation, tools or test suites used to prove the enabler.

| | |
|---|---|
| **Date:** | 18th to 25th January 2008 |
| **Location:** | Montréal, Canada |
| **Enabler:** | Mobile Broadcast (BCAST) v1.0 |
| **Process:** | OMA Interoperability Policy and Process [IOPPROC] |
| **Type of Testing** | Interoperability Testing |
| **Products tested:** | Client-to-Server, Client-to-Smartcard-to-Server-to-BSF |
| **Test Validation Plan:** | BCAST 1.0 Enabler Validation Plan - OMA-TP-2007-0479-INP_EVP_BCAST_V1_0_for_candidate_reapproval [EVP] |
| **Test Specification:** | BCAST  Enabler Test Specification -  OMA-ETS-BCAST_INT-V1_0-20070807-C [ETS] |
| **Test Tool:** | None |
| **Test Code:** | None |
| **Type of Test event:** | TestFest |
| **Participants:** | Viaccess, Oberthur Card Systems *plus 7 other participants* |
| **Number of Client Implementations:** | 5 |
| **Participating Technology Providers for clients:** | 5 particpants |
| **Implementation IDs for each client:** | 5 clients. |
| **Number of Smartcard Implementations:** | 2 |
| **Participating Technology Providers for Smartcards:** | Oberthur *plus 1 other participant* |
| **Implementation IDs for each Smartcard:** | BCAST v1.0 *plus 1 other smartcard* |
| **Number of Server Implementations:** | 4 |
| **Participating Technology Providers for servers:** | Viaccess *plus 3 other particpants* |
| **Implementation IDs for each server:** | Purple-TV SCP 1.0 *plus 3 other servers* |

| | |
|---|---|
| **Number of BSF Implementations:** | 1 |
| **Participating Technology Providers for BSFs:** | 1 |
| **Implementation IDs for each BSF:** | 1 BSF |
| **Number of test sessions completed:** | 15 |

# 5.2    Test Case Statistics

## 5.2.1    Test Case Summary

This chapter gives an overview of the result for all test cases included in [ETS].

The following status is used in the tables below:

- Total number of TCs: Used in the summary to indicate how many test cases there are in total.

- Number of passed: Used in the summary to indicate how many of the total testcases that successfully has been passed.

- Number of failed: Used in the summary to indicate how many of the total testcases that has failed.

- Number of N/A: Used in the summary to indicate how many of the total testcases that has not be run due to that the implementation(s) do not support the functionality required to run this test case.

- Number of OT: Used in the summary to indicate how many of the total testcases that has not be run due to no time to run the test case.

- Number of INC: Used in the summary to indicate how many of the total testcases that has not been run due to that the functionality could not be tested due to an error in the implementation in another functionality that is required to run this test case.

| Test Section: | Number of test sessions: | Total number of TCs: | Number of Passed: | Number of Failed: | Number of N/A: | Number of OT: | Number of INC: | Total: |
|---|---|---|---|---|---|---|---|---|
| Client TCs | 15 | 15 | 4 | 0 | 33 | 0 | 0 | 37 |
| Clients to Server TCs | 15 | 23 | 39 | 4 | 35 | 8 | 0 | 86 |
| Client to Smartcard to Server TCs | 15 | 24 | 49 | 1 | 32 | 156 | 1 | 239 |
| Total | 15 | 62 | 92 | 5 | 100 | 164 | 1 | 362 |

**Table 1. Test Summary Table**

NOTE: The difference between the total possible number of test cases and the actual number of test cases attempted is caused by the OMA Trusted Zone informing participants that certain test cases should not be attempted in a particular test session.

## 5.2.2    Test Case List

This chapter lists the statistics for all all interoperability test cases included in [ETS].

The following status is used in the tables below:

- **Runs (R)**: Used to indicate the total number of times the test case have been run (R = P + F + I).

- **Pass (P):** Used to indicate how many times the test case have been run and successfully passed.

- **Fail (F):** Used to indicate how many times the test cases have been run and failed (used when the failure reason is known).

- **Inconclusive (I)**: Used to indicate how many times the test cases have been run and did not pass due to other nature than conclusive implementation or specification failure (e.g.: the failure reason cannot be clearly determined).

- **Not Applicable (N/A):** Used to indicate how many times the test cases have not be run due to lack of support for the required functionality to run this test case by one or more involved implementations.

- **Out of Time (O):** Used to indicate how many times the test cases have not been run due to lack of time.

- **Problem Report (PR):** Used to indicate how many PRs have been issued for the test case.

- **Note:** Used to indicate the cause of the Inconclusive or Failed results.


## Tests for BROADCAST Enabler TestFest
### taken from OMA-ETS-BCAST_INT-V1_0-20070807-C.doc

Test cases highlighted are void in accordance with the EVP.

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-101 | Bootstraping a service with content. Associating content with service. This test case also tests that the reception of the SG is performed correctly. | 1 | 1 | 0 | 1 | 0 | 0 | | |
| BCAST-1.0-DIST-int-102 | Use Web portal URL in Purchase fragment of Service Guide to provide entry point for web based provisioning. | 0 | 0 | 0 | 1 | 0 | 1 | | |
| BCAST-1.0-DIST-int-103 | Updating description of content. This test case also tests that the update of the SG is performed correctly – Broadcast channel. | 4 | 4 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-104 | Updating description of content. This test case also tests that the update of the SG is performed correctly – Interaction channel. | 0 | 0 | 0 | 0 | 0 | 4 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | **R** | **P** | **F** | **O** | **I** | **N/A** | | |
| BCAST-1.0-DIST-int-105 | Applying the associated access and session description parameters with content – Broadcast channel. | 4 | 4 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-106 | Applying the associated access and session description parameters with content – Interaction channel. | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-107 | Testing the case where the SGDU is GZIP compressed. | 4 | 4 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-108 | Associating content with service. | 4 | 4 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-109 | Associating preview data with service. | 4 | 4 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-110 | Associating preview data with service. | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-111 | Applying the associated access and session description parameters with content choose the correct parameters for a specific choice of language. | 0 | 0 | 0 | 0 | 0 | 2 | | |
| BCAST-1.0-DIST-int-112 | Associating Service with provisioning information and applying the latter for subscription. | 0 | 0 | 0 | 0 | 0 | 1 | | |
| BCAST-1.0-DIST-int-201 | To test the support of ALC and the interpretation of the file description information on the Service Guide | 0 | 0 | 0 | 0 | 0 | 3 | | |
| BCAST-1.0-DIST-int-202 | To test the support of the in-band delivery of the metadata associated with file distributed using FLUTE | 0 | 0 | 0 | 0 | 0 | 3 | | |
| BCAST-1.0-DIST-int-203 | To test the support of the delivery of a file using http over the interaction channel | 0 | 0 | 0 | 0 | 0 | 3 | | |
| BCAST-1.0-DIST-int-204 | The purpose of this test is to test the support of the FEC encoding ID 1 scheme | 0 | 0 | 0 | 0 | 0 | 3 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | **R** | **P** | **F** | **O** | **I** | **N/A** | | |
| BCAST-1.0-DIST-int-205 | The purpose of this test is to test if the file repair is correctly performed | 0 | 0 | 0 | 0 | 0 | 3 | | |
| BCAST-1.0-DIST-int-206 | The purpose of this test the report of the reception of a successful download | 0 | 0 | 0 | 0 | 0 | 3 | | |
| BCAST-1.0-DIST-int-207 | The purpose of this test is to test the report of the SDP handling and control with RTSP | 0 | 0 | 0 | 0 | 0 | 3 | | |
| BCAST-1.0-DIST-int-208 | The purpose of this test is to test the supports of RTP as a transport protocol for streaming distribution over the broadcast channel | 4 | 4 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-209 | 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 | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-210 | 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 | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-211 | The purpose of this test is to test the support of the streaming associated procedure | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-301 | Associating content with interactivity. Reception of InteractivityMediaDocuments over broadcast file distribution. XHTML MP as an interaction method. | 4 | 3 | 1 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-302 | Associating content with interactivity. Retrieval of InteractivityMediaDocuments over interaction channel. XHTML MP as an interaction method. | 0 | 0 | 0 | 0 | 0 | 4 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-303 | Associating content with interactivity. Reception of InteractivityMediaDocuments over broadcast file distribution. SMS as an interaction method. | 3 | 3 | 0 | 0 | 0 | 1 | | |
| BCAST-1.0-DIST-int-304 | Associating content with interactivity. Retrieval of InteractivityMediaDocuments over interaction channel. SMS as an interaction method. | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-305 | Associating content with interactivity. Reception of InteractivityMediaDocuments over broadcast file distribution. MMS as an interaction method. | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-306 | Associating content with interactivity. Retrieval of InteractivityMediaDocuments over interaction channel. MMS as an interaction method. | 0 | 0 | 0 | 0 | 0 | 4 | | |
| BCAST-1.0-DIST-int-401 | Opening an Ipsec encrypted stream with key material associated to the subscription. | 1 | 0 | 1 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-402 | Opening an SRTP encrypted stream with key material associated to the subscription. | 0 | 0 | 0 | 0 | 0 | 1 | | |
| BCAST-1.0-DIST-int-403 | Opening an ISMACrypt encrypted stream with key material associated to the subscription. | 1 | 0 | 1 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-404 | Test that GBA bootstrapping with the BSM is successfully achieved. Test that the SRK is correctly generated in the terminal | 9 | 9 | 0 | 1 | 0 | 0 | | |
| BCAST-1.0-DIST-int-405 | Test that SQN error is detected by the terminal during a GBA bootstrapping | 3 | 3 | 0 | 2 | 0 | 5 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-406 | Test that correct behaviour is observed when bootstrapping data has expired.<br>Test that a new SRK is correctly generated in the terminal | 7 | 6 | 1 | 2 | 0 | 1 | | |
| BCAST-1.0-DIST-int-407 | Test that bootstrapping will not succeed when a different secret key K has been provisioned on the terminal and the server. | 7 | 7 | 0 | 3 | 0 | 0 | | |
| BCAST-1.0-DIST-int-408 | Test that a deregistration flow can be processed by the server and terminal. | 7 | 7 | 0 | 3 | 0 | 0 | | |
| BCAST-1.0-DIST-int-409 | Test that a deregistration flow can be processed by the server and terminal when bootstrapping is required. | 6 | 5 | 1 | 3 | 0 | 1 | | |
| BCAST-1.0-DIST-int-410 | Test that SMK and SRK derivation from pre-provisioned SCK in the terminal are successful. | 0 | 0 | 0 | 0 | 0 | 9 | | |
| BCAST-1.0-DIST-int-411 | Test that an LTKM can be successfully received over UDP at the smartcard which sends a verification message. | 6 | 5 | 0 | 4 | 1 | 0 | | |
| BCAST-1.0-DIST-int-412 | Test that an LTKM can be successfully requested by the terminal and successfully be delivered over UDP at the terminal / smartcard and send a verification message. | 7 | 7 | 0 | 3 | 0 | 0 | | |
| BCAST-1.0-DIST-int-413 | 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. | 0 | 0 | 0 | 8 | 0 | 2 | | Note 001 |
| BCAST-1.0-DIST-int-414 | 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. | 0 | 0 | 0 | 5 | 0 | 5 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-415 | Test that an LTKM with EXT BCAST field can be successfully received over UDP at the terminal / smartcard and a verification message is sent. | | | | | | | | Void |
| BCAST-1.0-DIST-int-416 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-417 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-418 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-419 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-420 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-421 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-422 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-423 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-424 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-425 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-426 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-427 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-428 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-429 | Test that the BSM receives a verification message when a BSM pushes an LTKM message to the terminal/Smartcard.  (See BCAST-1.0-DIST-int-415) | | | | | | | | Void |
| BCAST-1.0-DIST-int-430 | Test that the Smartcard correctly parses STKMs | 2 | 2 | 0 | 8 | 0 | 0 | | |
| BCAST-1.0-DIST-int-431 | Test that the Smartcard correctly parses STKMs | 2 | 2 | 0 | 8 | 0 | 0 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-432 | Test that an STKM cannot be processed by the smartcard and the TEK isn't returned. | 2 | 2 | 0 | 8 | 0 | 0 | | |
| BCAST-1.0-DIST-int-433 | Test that an STKM cannot be processed by the smartcard and the TEK isn't returned. | 2 | 2 | 0 | 8 | 0 | 0 | | |
| BCAST-1.0-DIST-int-434 | Test that an LTKM delivery protected with invalid validity data cannot be used by the terminal | 2 | 2 | 0 | 8 | 0 | 0 | | |
| BCAST-1.0-DIST-int-435 | Test that an STKM cannot processed by the smartcard and the TEK isn't returned. | | | | | | | | Void |
| BCAST-1.0-DIST-int-436 | Test that an STKM cannot be processed by the smartcard when the SEK/PEK has been invalidated and that the TEK isn't returned. | | | | | | | | Void |
| BCAST-1.0-DIST-int-437 | Test that an STKM cannot processed by the smartcard and the TEK isn't returned. | | | | | | | | Void |
| BCAST-1.0-DIST-int-438 | Test that an STKM cannot processed by the smartcard and the TEK isn't returned. | | | | | | | | Void |
| BCAST-1.0-DIST-int-439 | BSM / BSDA sends an LTKM with the security policy extension 0x0A to delete keys associated to the given SEK/PEK ID. | 0 | 0 | 0 | 10 | 0 | 0 | | |
| BCAST-1.0-DIST-int-440 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-441 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-442 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-443 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-444 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-445 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | 0 | 0 | 0 | 10 | 0 | 0 | | |
| BCAST-1.0-DIST-int-446 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | 0 | 0 | 0 | 10 | 0 | 0 | | |
| BCAST-1.0-DIST-int-447 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-448 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-449 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-450 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-451 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-452 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | R | P | F | O | I | N/A | | |
| BCAST-1.0-DIST-int-453 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-454 | BSM / BSDA deliberately sends an STKM already sent to the terminal / smartcard (32-bit counter timestamp field has previously been used). Repeat STKM is not detected by the terminal and sent to the Smartcard. Depending on LTKM security_policy_extension value, smartcard accepts or rejects the STKM (replay allowed or not) | | | | | | | | Void |
| BCAST-1.0-DIST-int-455 | BSM / BSDA sends several identical STKMs to the terminal / smartcard with the same TEK (MTK ID field in MIKEY EXT payload is the same) and the same TS. Ensure repeat STKM is detected by the terminal and STKM is not sent to the smartcard. | 2 | 2 | 0 | 8 | 0 | 0 | | |
| BCAST-1.0-DIST-int-456 | BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value | 0 | 0 | 0 | 10 | 0 | 0 | | |
| BCAST-1.0-DIST-int-457 | BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value | | | | | | | | Void |
| BCAST-1.0-DIST-int-458 | Test that video and audio streams protected with same STKM stream can be processed.. | 0 | 0 | 0 | 8 | 0 | 2 | | |

| Test Case id: | Description: | Test Counts | | | | | | PR: | Note: |
|---|---|---|---|---|---|---|---|---|---|
| | | **R** | **P** | **F** | **O** | **I** | **N/A** | | |
| BCAST-1.0-DIST-int-459 | Test that video and audio streams protected with different STKM streams can only be accessed when both streams are available. | 0 | 0 | 0 | 8 | 0 | 2 | | |
| BCAST-1.0-DIST-int-460 | Opening an Ipsec encrypted stream with key material associated to the subscription. | 0 | 0 | 0 | 8 | 0 | 2 | | |
| BCAST-1.0-DIST-int-461 | Opening an SRTP encrypted stream with key material associated to the subscription. | 0 | 0 | 0 | 8 | 0 | 2 | | |
| BCAST-1.0-DIST-int-462 | Opening an ISMACrypt encrypted stream with key material associated to the subscription. | 0 | 0 | 0 | 8 | 0 | 2 | | |
| BCAST-1.0-DIST-int-501 | The purpose of this test is to check that the terminal correctly receives provisioning messages using TP-7 over the interactive channel. | 0 | 0 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-502 | 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. | 0 | 0 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-503 | 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. | 0 | 0 | 0 | 0 | 0 | 0 | | |
| BCAST-1.0-DIST-int-504 | 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. | 0 | 0 | 0 | 0 | 0 | 0 | | |

**Table 2. Test Case Counts**

## 5.3 Problem Reports

During the activities for TestFest-22, the following problem reports were generated relating to the test materials and test process:

| PR Number | Affecting | Description | Test Case reference / Specification reference |
|---|---|---|---|
| 0018 | OMA-TS-BCAST_SvcCntProtection-V1_0-20070907-C | BCAST Specifications trailing 3gpp specifications and TestFest confusion. | 3GPP TS 33.220 |
| 0019 | OMA-TS-BCAST_SvcCntProtection-V1_0-20070529-C | Misleading interpretation of Ua protocol identifier and LTKM delivery port number | - |

Full details of the Problem Reports can be found at:

http://www.openmobilealliance.org/TestFests/Problem_Reporting.aspx

# 6. Confirmation

This signature states that the included information is true and valid.

_____

OMA Trusted Zone

# Appendix A.   Change History                              (Informative)

| Type of Change | Date | Section | Description |
|---|---|---|---|
| Initial Release | 1<sup>st</sup> February 2008 | All | First Version  from TestFest-22 |
|  |  |  |  |