Enabler Test Specification for BCAST Interoperablility

Candidate Version 1.0 – 07 Aug 2007

Open Mobile Alliance

OMA-ETS-BCAST_INT-V1_0-20070807-C

Contents

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-ERELD] "Enabler Release Definition for Mobile Broadcast Services", Open Mobile Alliance™, OMA-ERELD-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

[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-ERELD-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.

Purchase Item	A purchase item groups one or multiple services or pieces of content that an end-user can purchase or subscribe to as a whole. [BCAST10-ESG].
Rights Object	A collection of Permissions, Constraints, and other attributes which define under what circumstances access is granted to, and what usages are defined for, DRM Content. All OMA DRM Conformant Devices must adhere to the Rights Object associated with DRM Content. [DRMDRM-v2.0]
Rights Issuer	An entity that issues Rights Objects to OMA DRM Conformant Devices. [DRMDRM-v2.0]
User ID	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

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

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

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

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

5.1.2 Web-based Service Provisioning

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

Preconditions	Set up a web portal that provides additional information and ability to handle provisioning requests from a terminal for a particular PurchaseChannel. Setup a Service Guide with a PurchaseChannel fragment identifying a PortalURL pointing to the entry point of a related web-based system.
Test Procedure	• Start the BCAST application in the terminal and update the SG (if not done automatically). • Browse the SG in the terminal. • Select the service to subscribe. • Access portal related to the service.
Pass-Criteria	The following actions should be possible to perform • Browse service information presented by the portal. • The user is able to order the service through the portal. • The user is able to access the service.

5.2 Service Guide

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

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

Pass-Criteria	The following things should be visible to the end user after the first update of the SG • The SG is visible and contains a programme. The following things should be visible to the end user after the second update of the SG • The SG is visible and contains an updated version of the programme. • The updated programme can be received by the terminal.

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

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

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

Test Case Id	BCAST-1.0-DIST-int-105
Test Object	BCAST Terminal and Server

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

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

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

5.2.5 GZIP compression of Service Guide Delivery Unit

Test Case Id	BCAST-1.0-DIST-int-107
Test Object	BCAST Terminal and Server
Test Case Description	Testing the case where the SGDU is GZIP compressed.
Specification Reference	[BCAST10 –ESG] Section 5.4.1.4.
SCR Reference	BCAST-SG-C-009
Tool	None
Test code	None
Preconditions	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.
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal • View the programme.
Pass-Criteria	The following things should be visible to the end user • The SG and the programme can be received by the terminal.

5.2.6 Content hierarchy

Test Case Id	BCAST-1.0-DIST-int-108
Test Object	BCAST Terminal and Server
Test Case Description	Associating content with service.
Specification Reference	[BCAST10 –ESG] Section 5.1.
SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004
Tool	None
Test code	None
Preconditions	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).
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal • View the programmes.

Pass-Criteria	The following things should be visible to the end user • There are two consecutive programmes in the SG. • Both programmes can be seen, one after the other at the right time.

5.2.7 PreviewData and Service – Broadcast Channel

Test Case Id	BCAST-1.0-DIST-int-109
Test Object	BCAST Terminal and Server
Test Case Description	Associating preview data with service.
Specification Reference	[BCAST10 –ESG] Section 5.1.2.9
SCR Reference	BCAST-SG-C-005
Tool	None
Test code	None
Preconditions	Set up the StartTime and EndTime in the Content Fragment to match the test time. There is a preview icon associated with the SG
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal
Pass-Criteria	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

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

Pass-Criteria	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

Test Case Id	BCAST-1.0-DIST-int-111
Test Object	BCAST Terminal and Server
Test Case Description	Applying the associated access and session description parameters with content choose the correct parameters for a specific choice of language.
Specification Reference	[BCAST10 –ESG] Section 7.2.
SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004 Appendix C.3 (informative)
Tool	None
Test code	None
Preconditions	Set up the StartTime and EndTime in the Content Fragment to match the test time. There are several audio languages for a programme.
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal • Select a programme that has several audio languages. • Change the audio language of the programme.
Pass-Criteria	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

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

Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal • Subscibe to a service. • Try to subscribe to the same service again. • Try to stream the programme in the selected service.
Pass-Criteria	• The terminal is able to subscribe to the service. The terminal registers the service as subscribed. • The user is not able to subscribe to the same service again. • The user can stream the programme within the subscribed service.

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

Test Case Id	BCAST-1.0-DIST-int-201
Test Object	BCAST Client
Test Case Description	To test the support of ALC and the interpretation of the file description information on the Service Guide
Specification Reference	[BCAST10-Distribution] Section 5.2
SCR Reference	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
Tool	
Test code	
Preconditions	Set up the Service Guide delivery to use • Broadcast channel The file 1 is available on the broadcast channel The Access fragment describes the file delivery session, to be done through the broadcast channel File is GZIP encoded Compact No-Code FEC is used Ipv4 is used
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file 1 to download • Wait for the file download Note: file1 can be a jpg picture

Pass-Criteria	The following things should be visible to the end user • There is a service "FILE1" that contains a file "File1" • The file is successfully downloaded to the terminal Note: To verify the file was correctly downloaded the picture should be correctly displayed

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

Test Case Id	BCAST-1.0-DIST-int-202
Test Object	BCAST Client
Test Case Description	To test the support of the in-band delivery of the metadata associated with file distributed using FLUTE
Specification Reference	[BCAST10-Distribution] Section 5.2
SCR Reference	BCAST-FD-C-006, BCAST-FD-C-010, BCAST-FD-S-007, BCAST-FD-S-011
Tool	
Test code	
Preconditions	Set up the Service Guide delivery to use • Broadcast channel The access fragment refers a valid Flute Session Descriptor File is GZIP encoded
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file 2 to download • Wait for the file download Note: file2 can be a jpg picture
Pass-Criteria	The following things should be visible to the end user • There is a service "FILE2" that contains a file "File2" • The file is successfully downloaded to the terminal Note: To verify the file was correctly downloaded the picture should be correctly displayed

5.3.1.3 Support the delivery using HTTP over Interaction Channel

Test Case Id	BCAST-1.0-DIST-int-203
Test Object	BCAST Client
Test Case Description	To test the support of the delivery of a file using http over the interaction channel
Specification Reference	[BCAST10-Distribution] Section 5.2
SCR Reference	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

Tool	
Test code	
Preconditions	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
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file 3 to download • Wait for the file download Note: file3 can be a jpg picture
Pass-Criteria	The following things should be visible to the end user • There is a service "FILE3" that contains a file "File3" • The file is successfully downloaded to the terminal Note: To verify the file was correctly downloaded the picture should be correctly displayed

5.3.1.4 Support of FEC RAPTOR

Test Case Id	BCAST-1.0-DIST-int-204
Test Object	BCAST Client
Test Case Description	The purpose of this test is to test the support of the FEC encoding ID 1 scheme
Specification Reference	[BCAST10-Distribution] – Section 5.2.2
SCR Reference	BCAST-FD-C-007, BCAST-FD-C-009, BCAST-FD-S-008, BCAST-FD-S-010
Tool	
Test code	
Preconditions	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
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file4 to download • Wait for the file download Note: file 4 can be a jpg picture
Pass-Criteria	The following things should be visible to the end user • There is a service "FILE4" that contains a file "File4" • The file is successfully downloaded to the terminal 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

Test Case Id	BCAST-1.0-DIST-int-205
Test Object	BCAST Client
Test Case Description	The purpose of this test is to test if the file repair is correctly performed
Specification Reference	[BCAST10-Distribution] – Section 5.3.3
SCR Reference	BCAST-FD-C-014, BCAST-FD-C-015, BCAST-FD-S-015, BCAST-FD-S-016
Tool	
Test code	
Preconditions	Set up the Service Guide The access fragment refers a valid Flute File Descriptor and a valid Associated Delivery Procedure with the relevant file repair information A repair server is available
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file 2 to download • The file is downloaded but some file fragments are not send on purpose • Wait for the file repair procedure Note: file 2 can be a jpg picture
Pass-Criteria	The following things should be visible to the end user • There is a service “FILE2” that contains a file “File2” • The file is incompletely downloaded to the terminal • The terminal enters the repair procedure and the file is successfully downloaded for the second time Note: To verify the file was correctly downloaded the picture should be correctly displayed

5.3.1.6 Support of reception report

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

Preconditions	Set up the Service Guide 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 There is a reception report server available
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file 2 to download • The file is downloaded successfully Note: file 2 can be a jpg picture
Pass-Criteria	The following things should be visible to the end user • There is a service "FILE2" that contains a file "File2" • The file is successfully downloaded • The terminal reports the successful download of the file Note: To verify the file was correctly downloaded the picture should be correctly displayed

5.3.1.7 Support of Flute Session Setup and Control with RTSP

Test Case Id	BCAST-1.0-DIST-int-207
Test Object	BCAST Client
Test Case Description	The purpose of this test is to test the report of the SDP handling and control with RTSP
Specification Reference	[BCAST10-Distribution] – Section 5.5.1.1
SCR Reference	N/A
Tool	
Test code	
Preconditions	Set up the Service Guide Note: All the fragments are associated with the same Service fragment. The access fragment refers a valid Flute File Descriptor with a valid control URI
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the file 5 to download • The user request the file to play • The user request the playing of the file to pause after the rendering has started • The user resumes the rendering of the file by requesting the file to play • The user give up on rendering the file Note: file 5 must be a video or music file, 3gpp and mp3 file types are recommended

Pass-Criteria	The following things should be visible to the end user • There is a service "FILE5" that contains a file "File5" • When the user request to play the file, the transmission stars followed by a rendering of the file • The rendering of the file is correctly paused on request • The rendering of the file is correctly resumed on user request • The rendering of the file is correctly stopped on user request and the transmission ceased.

5.3.2 Streaming Distribution

5.3.2.1 Support of RTP for stream distribution over the broadcast channel

Test Case Id	BCAST-1.0-DIST-int-208
Test Object	BCAST Client
Test Case Description	The purpose of this test is to test the supports of RTP as a transport protocol for streaming distribution over the broadcast channel
Specification Reference	[BCAST10-Distribution] – Section 6.2
SCR Reference	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
Tool	
Test code	
Preconditions	Set up the Service Guide The access fragment refers a valid SDP Session Descriptor The SDP points a stream available on broadcast channel The SDP has the RTCP receiver reports turned off
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the stream 1 to render • The stream starts to be correctly rendered • The server sends the RTCP packets (sender reports) Note: stream 1 must be a video or music file, 3gpp and mp3 file types are recommended
Pass-Criteria	The following things should be visible to the end user • There is a service "STREAM1" that contains a service "Stream1" • The rendering of the stream starts correctly

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

Test Case Id	BCAST-1.0-DIST-int-209
Test Object	BCAST Client
Test Case Description	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
Specification Reference	[BCAST10-Distribution] – Section 6.2
SCR Reference	BCAST-SD-C-016, BCAST-SD-C-017, BCAST-SD-C-018¸ BCAST-SD-S-026, BCAST-SD-S-027, BCAST-SD-S-028
Tool	
Test code	
Preconditions	Set up the Service Guide The access fragment refers a valid SDP Session Descriptor The SDP points a stream available on interactive channel The SDP has the RTCP receiver reports turned off
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the stream 2 to render • The stream starts to be correctly rendered • The server sends the RTCP packets (sender reports) Note: stream 2 must be a video or music stream, 3gpp and mp3 file types are recommended
Pass-Criteria	The following things should be visible to the end user • There is a service “STREAM2” that contains a service “Stream2” • The rendering of the stream starts correctly • The terminal does not send RTCP packets (receiver reports)

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

Test Case Id	BCAST-1.0-DIST-int-210
Test Object	BCAST Client
Test Case Description	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
Specification Reference	[BCAST10-Distribution] – Section 6.7
SCR Reference	BCAST-SD-C-017, BCAST-SD-C-014, BCAST-SD-S-015
Tool	
Test code	

Preconditions	Set up the Service Guide The access fragment has all the description information for the streaming session The media type of stream 3 doesn't have a corresponding RTP definition
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the stream 3 to render • The stream starts to be correctly rendered Note: stream 3 must be a video or music file, 3gpp and mp3 file types are recommended
Pass-Criteria	The following things should be visible to the end user • There is a service "STREAM3" that contains a service "Stream3" • The rendering of the stream starts correctly

5.3.2.4 Support of streaming associated procedure

Test Case Id	BCAST-1.0-DIST-int-211
Test Object	BCAST Client
Test Case Description	The purpose of this test is to test the support of the streaming associated procedure
Specification Reference	[BCAST10-Distribution] – Section 6.8.1
SCR Reference	BCAST-SD-C-013, BCAST-SD-S-014
Tool	
Test code	
Preconditions	Set up the Service Guide The access fragment refers a valid SDP Session Descriptor and a URI for an streaming associated procedure description The streaming associated procedure description is valid and requests a fixed duration based measurements
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal and select the stream 4 to render • The stream starts to be correctly rendered • The server receives the correct streaming reception reports at the requested time Note: stream 4 must be a video or music file, 3gpp and mp3 file types are recommended
Pass-Criteria	The following things should be visible to the end user • There is a service "STREAM2" that contains a service "Stream2" • The rendering of the stream starts correctly • The terminal does not send RTCP packets (receiver reports)

5.4 Service Interaction

5.4.1 XHTML MP Interactivity – Broadcast Channel

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

5.4.2 XHTML MP Interactivity – Interaction Channel

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

Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal • Select a programme that contains XHTML MP interactivity. • Use the XHTML MP interactivity.
Pass-Criteria	• User is able to use the XHTML MP interactivity. • The user input is correctly received by the recipient. • The XHTML MP interactivity can be used without interrupting the "regular" broadcast stream.

5.4.3 SMS interactivity – Broadcast Channel

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

5.4.4 SMS interactivity – Interaction Channel

Test Case Id	BCAST-1.0-DIST-int-304
Test Object	BCAST Terminal and Server

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

5.4.5 MMS Interactivity – Broadcast Channel

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

Pass-Criteria	• User is able to use the MMS interactivity. • The recipient receives an MMS from the terminal formatted correctly according to the MMS Template and it contains the the user input. • The MMS interactivity can be used without interrupting the "regular" broadcast stream.

5.4.6 MMS Interactivity – Interaction Channel

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

5.5 Service and Content Protection

5.5.1 DRM Profile

5.5.1.1 Delivery of IPSec protected stream

Test Case Id	BCAST-1.0-DIST-int-401
Test Object	BCAST Terminal and Server

Test Case Description	Opening an Ipsec encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST10–ServContProt] Section 9.1. [BCAST10–ServContProt] Section 5.6.1
SCR Reference	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.
Tool	None
Test code	None
Preconditions	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.
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal • Subscibe to a IPSec protected service • View an IPSec encrypterd programme.
Pass-Criteria	• The terminal is able to subscribe to the service. • The terminal registers the service to be subscribed and disallows the end user to subscribe again. • The terminal is able to decrypt and render the IPSec encrypted audio and video streams belonging to the programme.

5.5.1.2 Delivery of SRTP protected stream

Test Case Id	BCAST-1.0-DIST-int-402
Test Object	BCAST Terminal and Server
Test Case Description	Opening an SRTP encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST10–ServContProt] Section 9.2. [BCAST10–ServContProt] Section 5.6.1
SCR Reference	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.
Tool	None
Test code	None
Preconditions	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.

Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal • Subscibe to a SRTP protected service • View an SRTP encrypterd programme.
Pass-Criteria	• The terminal is able to subscribe to the service. • The terminal registers the service to be subscribed and disallows the end user to subscribe again. • The terminal is able to decrypt and render the SRTP encrypted audio and video streams belonging to the programme.

5.5.1.3 Delivery of ISMACrypt protected stream

Test Case Id	BCAST-1.0-DIST-int-403
Test Object	BCAST Terminal and Server
Test Case Description	Opening an ISMACrypt encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST10–ServContProt] Section 9.3. [BCAST10–ServContProt] Section 5.6.1.
SCR Reference	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.
Tool	None
Test code	None
Preconditions	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.
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal • Subscibe to a ISMACrypt protected service • View an ISMACrypt encrypterd programme.
Pass-Criteria	• The terminal is able to subscribe to the service. • The terminal registers the service to be subscribed and disallows the end user to subscribe again. • The terminal is able to decrypt and render the Ipsec encrypted audio and video streams belonging to the programme.

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 data 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].

5.5.2.1.1 GBA-U Bootstrapping USIM /BSM with success

Test Case Id	BCAST-1.0-DIST-int-404
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS only or BCAST
Test Case Description	Test that GBA bootstrapping with the BSM is successfully achieved. Test that the SRK is correctly generated in the terminal
Specification Reference	SPCP spec: 6.10, 6.5
SCR Reference	BCAST-SPCP-C-005, BCAST-KeyManagement-C-016
Tool	Spy of the terminal / smartcard interface
Test code	
Preconditions	o No bootstrapping context exists between BSM and terminal/smartcard o UICC contains Key management: UICC is GBA and MBMS or BCAST enabled o UICC contains a valid 3G subscription (IMSI/K and algo Milenage) o HSS contains also the secret K associated with the IMSI o Session description fragment contains MBMS USD with a service protection description fragment containing o the key management element with a key management server definition. o And the attribute uiccKeyManagement indicating that the UICC based key management is required for the service. o Or the information are provided using the SDP. o The Service Guide declares a service for which subscription is possible, allowing the Terminal to send a Service Registration

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 verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK g. USIM sends the response of authenticate command RES authentication challenge response (SQN valid). h. Terminal sends challenge response back to the BSF in GET request i. BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI j. BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal k. The terminal stores B-TID and key lifetime in the EF_{GBABP} 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_{GBANL} 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.

Pass-Criteria	1. reception at BSF of a GET request from Terminal with the appropriate IMPI 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) 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.

5.5.2.1.2 GBA-U Bootstrapping USIM / BSM with synchronization error

Test Case Id	BCAST-1.0-DIST-int-405
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS only or BCAST
Test Case Description	Test that SQN error is detected by the terminal during a GBA bootstrapping
Specification Reference	SPCP spec: 6.10, 6.5
SCR Reference	BCAST-SPCP-C-005, BCAST-KeyManagement-C-016
Tool	none
Test code	
Preconditions	o 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. o UICC contains Key management UICC is GBA and MBMS or BCAST enabled o Session description fragment contains MBMS USD with a service protection description fragment containing o The key management element with a key management server definition. o And the attribute uiccKeyManagement indicating that the UICC based key management is required for the service. o Or the information are provided using the SDP. o The Service Guide declares a service for which subscription is possible, allowing the Terminal to send a Service Request o 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

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 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) 4. Terminal detects that a bootstrapping procedure is needed (Key lifetime has expired) 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) b. The BSF retrieves Authentication vector from the HSS 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 containing an error in SQN (same SQN as for the test 1.1.1) e. Terminal sends RAND and AUTN to the USIM using the Authenticate command in GBA security context: Bootstrapping Mode f. The USIM verifies MAC and SQN from AUTN and the SQN value is invalid. USIM computes AUTS g. USIM sends the response of authenticate command: AUTS: SQN is invalid (Synchronization error) h. Terminal sends AUTS back to the BSF in GET request i. BSF gets the corresponding AV (indicated by the AUTS) from the HSS and selects the AV 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) …..
Pass-Criteria	1. reception at BSF of a GET request from Terminal with the appropriate IMPI 2. reception at BSF of AUTS in the second GET request

5.5.2.1.3 GBA_U: Expired Bootstrapping data

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

Preconditions	o A bootstrapping context exists between server and terminal/smartcard o UICC contains Key management: UICC is GBA and BCAST enabled (if the UICC is MBMS only, the BSM being tested must also be MBMS security enabled). o UICC contains a valid 3G subscription (IMSI/K and also Milenage) o HSS also contains the secret K associated with the IMSI/IMPI o 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. o The key management element with a key management server definition. o The attribute uiccKeyManagement indicating that the UICC based key management is required for the service. o The key management server with which the terminal should register. o 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. o 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. o The BSM wishes to renegotiate bootstrapping, i.e. the key lifetime has expired on the BSM side.

Test Procedure	1. The BCAST client is started, re-activated or otherwise prompted to start user registration. 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. 3. The BSM returns a 401 unauthorised response in order to force the terminal to perform bootstrapping. 4. The terminal/smartcard and the BSF establish bootstrapped security association between them by running bootstrapping procedure. 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) The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102) The BSF selects an authentication vector AV= RAND||AUTN||XRES||CK||IK BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND||AUTN Terminal sends RAND and AUTN to the USIM using the Authenticate command in GBA security context: Bootstrapping Mode The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK USIM sends the response of authenticate command RES authentication challenge response (SQN valid). Terminal sends challenge response back to the BSF in GET request BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal The terminal stores B-TID and key lifetime in the EF_{GBABP} 5. The terminal/smartcard reissues the MBMS User registration request to the BSM using the new BT-ID and Ks_ext_NAF (SRK) 6. .The BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each service.
Pass-Criteria	7. Reception at BSF of a GET request from Terminal with the appropriate IMPI to kick off bootstrapping. The BSM's NAF receives an MBMS User registration request containing the new BT-ID and SRK. 8. 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.

5.5.2.1.4 GBA_U: Different Key K on Client and Server

Test Case Id	BCAST-1.0-DIST-int-407

Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS only or BCAST.
Test Case Description	Test that bootstrapping will not succeed when a different secret key K has been provisioned on the terminal and the server.
Specification Reference	6.5.1
SCR Reference	BCAST-SPCP-C-005
Tool	None
Test code	None
Preconditions	o No bootstrapping context exists between the server and terminal/smartcard. o UICC contains Key management: UICC is GBA and BCAST enabled (if the UICC is MBMS only, the BSM being tested must also be MBMS-enabled). o UICC contains a valid 3G subscription (IMSI/K and also Milenage). o HSS contains a different secret key K associated with the IMPI to that available on the UICC o 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. o The key management element with a key management server definition. o The attribute uiccKeyManagement indicating that the UICC based key management is required for the service. o The key management server with which the terminal should register. o 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. o

Test Procedure	The Terminal and the BSF establish bootstrapped security association between them by running bootstrapping procedure 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) The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102) The BSF selects an authentication vector AV= RAND||AUTN||XRES||CK||IK BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND||AUTN Terminal sends RAND and AUTN to the USIM using the Authenticate command in GBA security context: Bootstrapping Mode The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK USIM sends the response of authenticate command RES authentication challenge response (SQN valid). Terminal sends challenge response back to the BSF in GET request BSF compares the RES corresponds to the XRES and discovers that they do not correspond The BSF returns a response indicating to the terminal than an authentication failure has occurred or sends a new challenge to restart bootstrapping. 9.
Pass-Criteria	Reception at BSF of a GET request from Terminal with the appropriate IMPI to kick off bootstrapping. 10. The BSF returns a response to the terminal which indicates that the authentication failure has occurred or retuens a new challenge.

5.5.2.1.5 Deregistration

Test Case Id	BCAST-1.0-DIST-int-408
Test Object	BCAST Terminal and Server
Test Case Description	Test that a deregistration flow can be processed by the server and terminal.
Specification Reference	6.6
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-01
Tool	None
Test code	None

Preconditions	○ A bootstrapping context exists between server and terminal/smartcard ○ UICC contains Key management: UICC is GBA and BCAST enabled (if the UICC is MBMS only, the BSM being tested must also be MBMS security enabled). ○ UICC contains a valid 3G subscription (IMSI/K and also Milenage) ○ HSS also contains the secret K associated with the IMSI/IMPI ○ 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. ○ The key management element with a key management server definition. ○ The attribute uiccKeyManagement indicating that the UICC based key management is required for the service. ○ The key management server with which the terminal should register. ○ 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 provisioining flow or using pre-defined data.
Test Procedure	The BCAST Client is terminated or suspended on the terminal (This should prompt a deregistration flow). 11. The terminal initiates the MBMS user deregistration flow. Terminal sends a HTTP post to the BSM containing the Service ID. The BSM answers with 401 Unauthorized indicating that the BSM wants to authenticate the terminal using the bootstrapped security association Key derivation: Terminal sends NAF_ID and IMPI to USIM using the authenticate command in GBA security context: NAF derivation mode. USIM derives Ks_ext_NAF (SRK) and Ks_Int_NAF (SMK), updates the EF_{GBANL} and sends back to the terminal the Ks_ext_NAF (SRK). 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. BSM retrieves Ks_ext_NAF from the BSF and verifies the message received from the terminal. 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.
Pass-Criteria	12. The BSM receives a HTTP POST device from the terminal containing the Service IDs. 13. 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

Test Case Id	BCAST-1.0-DIST-int-409
Test Object	BCAST Terminal and Server

Test Case Description	Test that a deregistration flow can be processed by the server and terminal when bootstrapping is required.
Specification Reference	6.6
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-02
Tool	None
Test code	None
Preconditions	o No bootstrapping context exists between server and terminal/smartcard o UICC contains Key management: UICC is GBA and BCAST enabled (if the UICC is MBMS only, the BSM being tested must also be MBMS security enabled). o UICC contains a valid 3G subscription (IMSI/K and also Milenage) o HSS also contains the secret K associated with the IMSI/IMPI o 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. o The key management element with a key management server definition. o The attribute uiccKeyManagement indicating that the UICC based key management is required for the service. o The key management server with which the terminal should register. o 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 provisioining flow or using pre-defined data. o The BSM wishes to renegotiate bootstrapping, i.e. the key lifetime has expired on the BSM side. •

Test Procedure	14. The BCAST Client is terminated or suspended on the terminal (This should prompt a deregistration flow). 15. The terminal initiates the MBMS user deregistration flow. Terminal sends a HTTP post to the BSM containing the Service ID. The BSM answers with 401 Unauthorized indicating that the BSM wants to authenticate the terminal using the bootstrapped security association Key derivation: Terminal sends NAF_ID and IMPI to USIM using the authenticate command in GBA security context: NAF derivation mode. USIM derives Ks_ext_NAF (SRK) and Ks_Int_NAF (SMK), updates the EF_{GBANL} and sends back to the terminal the Ks_ext_NAF (SRK). 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. BSM determines that bootstrapping should be rerun and therefore returns a bootstrapping renegotiation indicator by returning a 401 “Unauthorized” HTTP response Prompted by receiving a bootstrapping regenotiation indication, the terminal initiates bootstrapping. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102) The BSF selects an authentication vector AV= RAND||AUTN||XRES||CK||IK BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND||AUTN Terminal sends RAND and AUTN to the USIM using the Authenticate command in GBA security context: Bootstrapping Mode The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK USIM sends the response of authenticate command RES authentication challenge response (SQN valid). Terminal sends challenge response back to the BSF in GET request BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal The terminal stores B-TID and key lifetime in the EF_{GBABP} The terminal reinitiates the MBMS user deregistration flow with the enw bootstrapping data. 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. The BSM returns a 200 OK as well as the status codes of the Service IDs.
Pass-Criteria	The terminal initiates bootstrapping on receiving a bootstrapping negotiation indication from the BSM . 16. The BSM returns a 200 ok response after receiving an MBMS user deregistration request from the terminal using the new bootstrapping data.

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

Test Case Id	BCAST-1.0-DIST-int-410
Test Object	BCAST Terminal /Smartcard. UICC is BCMCS-only or BCAST
Test Case Description	Test that SMK and SRK derivation from pre-provisioned SCK in the terminal are successful.
Specification Reference	SPCP spec: 6.10, 6.5
SCR Reference	BCAST-SPCP-C-005, BCAST-KeyManagement-C-016
Tool	BCAST conformance test tool. Spy of the terminal/Smartcard interface Test Smartcard BCMCS-only or BCAST
Test code	
Preconditions	o Pre-provisioned "SmartCard Key" (SCK), corresponding to the Registration Key (RK) in BCMCS, is stored on the UICC, from which the SMK and SRK (TK and Auth-Key, respectively, in BCMCS) are derived. o Description of service access is provided by BCMCS Information Acquisition as specified in [BCAST-ServContProt] Section 6.10.2. o The Service Guide declares a service for which subscription is possible, allowing the Terminal to send a Service Request.
Test Procedure	1. Update the SG in the terminal using the test tool as the source. 2. User selects a service for subscription. 3. The terminal and BSM perform the Service Request transaction by using HTTP Digest for access authentication and integrity protection: a. Terminal sends to the BSM "HTTP POST" containing the Service Request message. b. BSM responds with "HTTP 401 Unauthorized WWW-Authenticate" containing a digest-challenge. c. The terminal computes the challenge-response using the SRK and sends back to the BSM "HTTP POST Authorization Request" containing the digest-response. d. If the digest-response is correct, the BSM returns "HTTP 200 OK POST" with Authentication-Info containing the successful Service Request Response.
Pass-Criteria	Reception at the terminal the HTTP 200 OK message containing the successful status code for Service Request, as verification that the UICC/terminal and the BSM share the same SRK.

5.5.2.2 Layer 2 LTKM

5.5.2.2.1 LTKM (without EXT BCAST: MBMS like) reception at the smartcard

Test Case Id	BCAST-1.0-DIST-int-411
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS/BCMCS only or BCAST
Test Case Description	Test that an LTKM can be successfully received over UDP at the smartcard which sends a verification message.

Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-LTKM_SC-C-015
Tool	none
Test code	
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. o 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 usedor test 5.5.2.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used) o The LTKM is valid and indicates that a verification message is needed o The LTKM contains no EXT BCAST field
Test Procedure	1. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case. 2. Terminal receives LTKM, 3. Terminal retrieves the TS stored along with the associated MUK-ID 4. Terminal checks replay attacks 5. Terminal sends the LTKM to the smartcard 6. Smartcard verifies integrity of the message 7. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message 8. Terminal sends the verification message to the BSM.
Pass-Criteria	BSM receives the verification message

5.5.2.2.2 LTKM request from the terminal, LTKM reception at the terminal / smartcard

Test Case Id	BCAST-1.0-DIST-int-412
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS/BCMCS only or BCAST
Test Case Description	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.
Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-LTKM_SC-C-015
Tool	none
Test code	
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. o Service registration has been performed. o Terminal has missed an LTKM update because was out of coverage. IP context doesn't exist anymore o LTKM doesn't contains EXT BCAST field

Test Procedure	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. 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 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. 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. 3. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case. 4. Terminal receives LTKM, 5. Terminal retrieves the TS stored along with the associated MUK-ID 6. Terminal checks replay attacks 7. Terminal sends the LTKM to the smartcard 8. Smartcard verifies integrity of the message 9. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message 10. Terminal sends the verification message to the BSM.
Pass-Criteria	BSM receives a successful LTKM request BSM receives the verification message

5.5.2.2.3 BSM solicited pull procedure

Test Case Id	BCAST-1.0-DIST-int-413
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS/BCMCS only or BCAST
Test Case Description	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.
Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-LTKM_SC-C-015
Tool	none
Test code	
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. o Service registration has been performed. (test 5.5.2.1.1 has been performed before)
Test Procedure	1. BSM sends a MIKEY message with the last SMK known by the BSM and with the key number part of MSK-ID= 0x0 2. The terminal sends a HTTP POST to request the LTKM with the KeyDomainID-MSK-ID pair
Pass-Criteria	BSM receives a successful LTKM request

5.5.2.2.4 BSM solicited pull procedure initiation over SMS Bearer

Test Case Id	BCAST-1.0-DIST-int-414
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS/BCMCS only or BCAST
Test Case Description	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.
Specification Reference	SPCP spec: 6.6.1
SCR Reference	BCAST-LTKM_SC-C-015
Tool	none
Test code	
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. o Service registration has been performed. (test 5.5.2.1.1 has been performed before)
Test Procedure	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 2. The terminal sends a HTTP POST to request the LTKM with the KeyDomainID-MSK-ID pair
Pass-Criteria	BSM receives a successful LTKM request

5.5.2.2.5 LTKM with OMA BCAST extension and security policy extension

Test Case Id	BCAST-1.0-DIST-int-415
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	Test that an LTKM with EXT BCAST field can be successfully received over UDP at the terminal / smartcard and a verification message is sent.
Specification Reference	SPCP spec: 6.6, 6.6.2, 6.6.3, 6.6.4
SCR Reference	BCAST-LTKM_SC-C-015
Tool	none
Test code	
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal: o 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) o The LTKM is valid and indicates that a verification message is needed o The LTKM contains EXT BCAST field

Test Procedure	1. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case. 2. Terminal receives LTKM, 3. Terminal sends the LTKM to the smartcard 9. Smartcard verifies integrity of the message 10. Smartcard performs replay protection check 11. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message according to the EXT BCAST received in the LTKM (see 1.2.10.X below) 12. Terminal sends the verification message to the BSM.
Pass-Criteria	BSM receives the verification message (according to following tests)

The following tests shall be run in sequence. The pass criteria depends on this sequence

5.5.2.2.5.1. Set of service purse associated with service: Key domain ID =MCC1 || MNC1 and SEK/PEK ID key group = 0001

The BSM sends a LTKM with the following fields:

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0000

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_control_flag = 0

KV: Tslow = 0x0100; Tshigh = 0x01FF

Test Case Id	BCAST-1.0-DIST-int-416
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x00 o Purse_flag = 1 o Cost_value= 0x00 o Token_value= 0x05

5.5.2.2.5.2. LTKM with OMA BCAST extension and security policy extension 0x00 and the purse flag set to 1: test of set mode for the service purse

Precondition: the 5.5.2.2.5.1 test passes successfully first.

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0001 (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 = 0; token_value = 0x10; cost_value=0x01; access_control_flag = 0

KV: Tslow = 0x0200; Tshigh = 0x02FF

Test Case Id	BCAST-1.0-DIST-int-417
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x00 o Purse_flag = 1 o Cost_value= 0x01 o Token_value= 0x10

5.5.2.2.5.3. LTKM with OMA BCAST extension and security policy extension 0x01 and the purse flag set to 1: test of add mode for the service purse

Precondition: the 5.5.2.2.5.2 test passes successfully first.

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0002 (same Key_group as the previous message)

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=0x02; access_control_flag = 0

KV: Tslow = 0x0300; Tshigh = 0x03FF

Test Case Id	BCAST-1.0-DIST-int-418
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x01 o Purse_flag = 1 o Cost_value= 0x02 o Token_value= 0x20

5.5.2.2.5.4. LTKM with OMA BCAST extension and security policy extension 0x01 and the purse flag set to 1: test of overflow of the service purse

Precondition: the 5.5.2.2.5.3 test passes successfully first.

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0003 (same Key_group as the previous message)

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=0x03; access_control_flag = 0

KV: Tslow = 0x0400; Tshigh = 0x04FF

Test Case Id	BCAST-1.0-DIST-int-419
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 1 o Security_policy_extension = 0x01 o Purse_flag = 1 o Cost_value= 0x03 o Token_value= 0x20

5.5.2.2.5.5. Set of user purse associated with the SMK

The BSM sends a LTKM with the following fields:

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0002 0000

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x02; purse_flag = 1; purse_mode = 0; token_value = 0x02; cost_value=0x00; access_control_flag = 0

KV: Tslow = 0x0100; Tshigh = 0x01FF

Test Case Id	BCAST-1.0-DIST-int-420
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x02 o Purse_flag = 1 o Cost_value= 0x00 o Token_value= 0x02

5.5.2.2.5.6. LTKM with OMA BCAST extension and security policy extension 0x02 and the purse flag set to 1: test of set mode for the user purse

Precondition: the 5.5.2.2.5.5 test passes successfully first.

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0002 0001 (same Key_group as the previous message)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x02; purse_flag = 1; purse_mode = 0; token_value = 0x30; cost_value=0x04; access_control_flag = 0

KV: Tslow = 0x0200; Tshigh = 0x02FF

Test Case Id	BCAST-1.0-DIST-int-421
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x02 o Purse_flag = 1 o Cost_value= 0x04 o Token_value= 0x30

5.5.2.2.5.7. LTKM with OMA BCAST extension and security policy extension 0x03 and the purse flag set to 1: test of add mode for the user purse

Precondition: the 5.5.2.2.5.6 test passes successfully first.

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0002 0002 (same Key_group as the previous message)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x03; purse_flag = 1; purse_mode = 1; token_value = 0x10; cost_value=0x05; access_control_flag = 0

KV: Tslow = 0x0300; Tshigh = 0x03FF

Test Case Id	BCAST-1.0-DIST-int-422

Pass-Criteria	the BSM receives the following verification message: The verification message contains consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x03 o Purse_flag = 1 o Cost_value= 0x05 o Token_value= 0x40

5.5.2.2.5.8. LTKM with OMA BCAST extension and security policy extension 0x03 and the purse flag set to 1: test of overflow of the user purse

Precondition: the 5.5.2.2.5.7 test passes successfully first.

LTKM 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 =0x03; purse_flag = 1; purse_mode = 1; token_value = 0x7FFFFFFF; cost_value=0x06; access_control_flag = 0

KV: Tslow = 0x0400; Tshigh = 0x04FF

Test Case Id	BCAST-1.0-DIST-int-423
Pass-Criteria	the BSM receives the following verification message: The verification message contains consumption_reporting_flag = 1 o Overflow_flag = 1 o Security_policy_extension = 0x03 o Purse_flag = 1 o Cost_value= 0x06 o Token_value= 0x40

5.5.2.2.5.9. LTKM with OMA BCAST extension and security policy extension 0x06 and the purse flag set to 0 and number_play_back: test of play_back counter setting and deduction of token in service purse at reception of LTKM

Precondition: the 5.5.2.2.5.4 test passes successfully first. Then the service purse associated to key domain ID: MCC1 || MNC1 and Key group: 01 contains 0x20 token

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0004 (same Key_group as 1.2.5.4)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x06; purse_flag = 0; cost_value=0x05; number_play_back = 2, access_control_flag = 0

KV: Tslow = 0x0500; Tshigh = 0x05FF

Test Case Id	BCAST-1.0-DIST-int-424
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x06 o Purse_flag = 1 o Cost_value= 0x05 o Number_play_back = 0x02 o Token_value= 0x16

5.5.2.2.5.10. LTKM with OMA BCAST extension and security policy extension 0x07 and the purse flag set to 0 and number_play_back: test of play_back counter setting and deduction of token in user purse at reception of LTKM

Precondition: the 5.5.2.2.5.8 test passes successfully first. Then the user purse contains 0x40 token

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0002 0004 (same Key_group as 1.2.5.5)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0; cost_value=0x06; number_play_back = 3, access_control_flag = 0

KV: Tslow = 0x0500; Tshigh = 0x05FF

Test Case Id	BCAST-1.0-DIST-int-425
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x06 o Purse_flag = 1 o Cost_value= 0x06 o Number_play_back = 0x03 o Token_value= 0x2E

5.5.2.2.5.11. LTKM with OMA BCAST extension and security policy extension 0x08 and the purse flag set to 0 and number_play_back: test of play_back counter setting with no deduction of token in service purse at reception of LTKM

Precondition: the 5.5.2.2.5.9 test passes successfully first. Then the service purse associated to key domain ID: MCC1 || MNC1 and Key group: 01 contains 0x16 token

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0005 (same Key_group as 1.2.5.4)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x08; purse_flag = 0; cost_value=0x05; number_play_back = 4, access_control_flag = 0

KV: Tslow = 0x0600; Tshigh = 0x06FF

Test Case Id	BCAST-1.0-DIST-int-426
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x08 o Purse_flag = 1 o Cost_value= 0x05 o Number_play_back = 0x04 o Token_value= 0x16

5.5.2.2.5.12. LTKM with OMA BCAST extension and security policy extension 0x09 and the purse flag set to 0 and number_play_back: test of play_back counter setting with no deduction of token in user purse at reception of LTKM

Precondition: the 5.5.2.2.5.10 test passes successfully first. Then the user purse contains 0x2E token

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0002 0005 (same Key_group as 1.2.5.5)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x09; purse_flag = 0; cost_value=0x08; number_play_back = 5, access_control_flag = 0

KV: Tslow = 0x0600; Tshigh = 0x06FF

Test Case Id	BCAST-1.0-DIST-int-427
Pass-Criteria	the BSM receives the following verification message: The verification message contains o consumption_reporting_flag = 1 o Overflow_flag = 0 o Security_policy_extension = 0x09 o Purse_flag = 1 o Cost_value= 0x08 o Number_play_back = 0x05 o Token_value= 0x2E

5.5.2.2.5.13. LTKM with OMA BCAST extension and security policy extension 0x06 and the purse flag set to 0 and number_play_back: test of lack of balance in service purse

Precondition: the 5.5.2.2.5.11 test passes successfully first. Then the service purse associated to key domain ID: MCC1 || MNC1 and Key group: 01 contains 0x16 token

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0001 0006 (same Key_group as 1.2.5.4)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x06; purse_flag = 0; cost_value=0x06; number_play_back = 4, access_control_flag = 0

KV: Tslow = 0x0700; Tshigh = 0x07FF

Test Case Id	BCAST-1.0-DIST-int-428
Pass-Criteria	The BSM doesn't receive the verification message within the 4mns. On the spy: the response of authenticate command is lack of credit in the service purse The Terminal informs the user of lack of credit in the service purse for the rights received.

5.5.2.2.5.14. LTKM with OMA BCAST extension and security policy extension 0x07 and the purse flag set to 0 and number_play_back: test of lack of balance in user purse

Precondition: the 5.5.2.2.5.12 test passes successfully first. Then the user purse contains 0x2E token

LTKM fields:

Key domain ID= MCC1 || MNC1

SEK/PEK ID = 0002 0006 (same Key_group as 1.2.5.5)

V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0; cost_value=0x08; number_play_back = 6, access_control_flag = 0

KV: Tslow = 0x0700; Tshigh = 0x07FF

Test Case Id	BCAST-1.0-DIST-int-429
Pass-Criteria	The BSM doesn't receive the verification message within the 4 mns. On the spy: the response of authenticate command is lack of credit in the user purse The Terminal informs the user of lack of credit in the user purse for the rights received.

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

Key domain ID	Key group part	Key number part	Security policy	Cost-value	User purse	Service purse	Play-back counter	KV
MCC1 ||	0001	0000	0x00	0x00		0x16		0x0100-

MNC1								0x01FF
MCC1 || MNC1	0001	0001	0x00	0x01		0x16		0x0200-0x02FF
MCC1 || MNC1	0001	0002	0x01	0x02		0x16		0x0300-0x03FF
MCC1 || MNC1	0001	0004	0x06	0x05		0x16	2	0x0500-0x05FF
MCC1 || MNC1	0001	0005	0x08	0x05		0x16	4	0x0600-0x06FF
MCC1 || MNC1	0002	0000	0x02	0x00	2E			0x0100-0x01FF
MCC1 || MNC1	0002	0001	0x02	0x04	2E			0x0200-0x02FF
MCC1 || MNC1	0002	0002	0x03	0x05	2E			0x0300-0x03FF
MCC1 || MNC1	0002	0004	0x07	0x06	2E		3	0x0500-0x05FF
MCC1 || MNC1	0002	0005	0x09	0x08	2E		5	0x0600-0x06FF

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 Smartcard (BCAST)

Test Case Id	BCAST-1.0-DIST-int-430
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	Test that the Smartcard correctly parses STKMs
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	

Preconditions	o Smartcard has valid LTKM allowing the Smartcard to verify the STKM o BSM sends an LTKM for the service: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o with a security_policy_extension = 0x04 o KV: Tslow= 0x00; Tshigh= 0x0F 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 o
Test Procedure	1. BSM / BSDA generates STKMs for the service 03 of the Key domain ID= MCC1|| MNC1 TS and TEK ID of STKM is incremented for each STKM renewal with a crypto-period of 10s Within a crypto period TS and TEK ID are not changed (STKM sent every second; i.e 10 times within the crypto period) 2. STKMs are received by the Smartcard. 3. The TEK are sent back to the terminal 4. The terminal decrypts the content using the TEK for the SRTP protocol
Pass-Criteria	Smartcard returns no error message, thus validating the STKMs are correctly parsed by the smartcard, Video is displayed by the terminal during 160 s (2,66 mns)

5.5.2.3.2 Correct STKM parsing by Smartcard (MBMS)

Test Case Id	BCAST-1.0-DIST-int-431
Test Object	BCAST Terminal / Smartcard/ Server. UICC is MBMS or BCAST
Test Case Description	Test that the Smartcard correctly parses STKMs
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	o Smartcard has valid LTKM allowing the Smartcard to verify the STKM o BSM sends an LTKM for the service without security_policy_extension: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0004 0001 o KV: Tslow= 0x00; Tshigh= 0x0F o The server provides a valid SRTP and STKM stream to the device o 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

Test Procedure	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 2. STKMs are received by the Smartcard. 3. The TEK are sent back to the terminal 4. The terminal decrypts the content using the TEK for the SRTP protocol
Pass-Criteria	Smartcard returns no error message, thus validating the STKMs are correctly parsed by the smartcard, Video is displayed by the terminal during 160 s (2,66 mns). If video is displayed during 16s only, this means that the TS field is used for the checking of KV of the SEK/PEK instead of TEK ID as MBMS requires. This is then an error.

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

Test Case Id	BCAST-1.0-DIST-int-432
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test that an STKM cannot be processed by the smartcard and the TEK isn't returned.
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The Bootstrapping exists, but **SEK/PEK** used doesn't exist. o 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 o 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
Test Procedure	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).
Pass-Criteria	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)

Test Case Id	BCAST-1.0-DIST-int-433
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test that an STKM cannot be processed by the smartcard and the TEK isn't returned.
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The Bootstrapping exists, but **SEK/PEK** used doesn't exist. o The BSM sends a STKM for the key domain ID = MCC1|| MNC1 and with a SEK/PEK ID key group = 0x0005 (Wrong SEK/PEK ID) The server provides a valid SRTP and STKM stream to the device o 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
Test Procedure	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).
Pass-Criteria	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

5.5.2.3.5 LTKM with invalid validity data

Test Case Id	BCAST-1.0-DIST-int-434
Test Object	BCAST Terminal and Server
Test Case Description	Test that an LTKM delivery protected with invalid validity data cannot be used by the terminal
Specification Reference	SPCP spec:6.6
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-03
Tool	None
Test code	None
Preconditions	1. A bootstrapping context exists between server and terminal. 2. The server provides a valid SRTP and STKM stream to the device protected using an SEK not currently available to the terminal. 3. 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. 4. The current IP address of the terminal is available to the server.

Test Procedure	▪ The terminal receives a TEK protected with an SEK it does not currently possess. ▪ The terminal should not be able to decrypt the TEK and therefore the content. ▪ The server pushes the SEK currently being used to encrypt TEKs in the STKM stream in an LTKM with validity data in the past or otherwise not usable. ▪ The terminal still should not be able to decrypt the content.
Pass-Criteria	The terminal could decrypt the content protected using the SEK.

5.5.2.3.6 Incorrect STKM generation – invalid TS range or SEK/PEK has been invalidated

Test Case Id	BCAST-1.0-DIST-int-435
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	Test that an STKM cannot processed by the smartcard and the TEK isn't returned.
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	o The Bootstrapping exist, SEK/PEK exists but the SEK/PEK is either invalid (Seql>Sequ see 5.5.2.3.6.1) or TS isn't in the valid range (see 5.5.2-3.6.2 and 5.5.2.3.6.3). The server provides a valid SRTP and STKM stream to the device o 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
Test Procedure	The UE receives the STKM message.
Pass-Criteria	Smartcard detects the error and doesn't generate the TEK. Smartcard returns the status which corresponds to the error (see 5.5.2.3.6.1, 5.5.2.3.6.2, 5.5.2.3.6.3) No video displayed by the terminal.

5.5.2.3.6.1. STKM error: The SEK/PEK is invalid (Seql>Sequ) the SmartCard returns the status word '6985'

Test Case Id	BCAST-1.0-DIST-int-436
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	Test that an STKM cannot be processed by the smartcard when the SEK/PEK has been invalidated and that the TEK isn't returned.
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	

Preconditions	○ The Bootstrapping exist, SEK/PEK exists but the SEK/PEK is either invalid (Seql>Sequ) ○ The test 5.5.2.3.1: 'Correct STKM parsing by the Smartcard' passed successfully 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
Test Procedure	• Terminal sends to the BSM an unsubscribe request for the following service: ○ Key domain ID= MCC1|| MNC1 ○ SEK/PEK ID = 0003 0001 • BSM sends back a new LTKM to invalidate the SEK/PEK with invalid KV data (lower bound greater than the upper bound) • A valid STKM is sent for the service Key domain ID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 • Terminal receives the message and sends it to the smartcard • Smartcard detects that the SEK/PEK is invalid and returns the status code '6985' (conditions of use not satisfied)
Pass-Criteria	Smartcard detects the error and doesn't generate the TEK. No video is displayed On the spy: the status code returned by the smartcard is '6985' (conditions of use not satisfied) The terminal informs the user that he has no rights for this program and asks user to register to that service

5.5.2.3.6.2. STKM error: The TS present in the STKM is such TS < Seql (Tslow) the SmartCard returns the status word '9865'

Test Case Id	BCAST-1.0-DIST-int-437
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	Test that an STKM cannot processed by the smartcard and the TEK isn't returned.
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	○ The Bootstrapping exist, SEK/PEK exists but the TS isn't in the valid range ○ The test 5.5.2.3.1: 'Correct STKM parsing by the Smartcard' passed successfully 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

Test Procedure	A valid STKM is sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 but with a timestamp TS< Tslow • Terminal receives the message and sends it to the smartcard • Smartcard detects that the TS is invalid and returns the status code '9865' (Key freshness failure)
Pass-Criteria	Smartcard detects the error and doesn't generate the TEK. No video is displayed On the spy: the status code returned by the smartcard is '9865' (Key freshness failure) The terminal informs the user that he has no rights for this program and asks user to register to that service

5.5.2.3.6.3. STKM error: The TS present in the STKM is such Sequ (Tshigh) < TS the SmartCard returns the status word '9865'

Test Case Id	BCAST-1.0-DIST-int-438
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	Test that an STKM cannot processed by the smartcard and the TEK isn't returned.
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	o The Bootstrapping exist, SEK/PEK exists but the TS isn't in the valid range o The test 5.5.2.3.1: 'Correct STKM parsing by the Smartcard' passed successfully The server provides a valid SRTP and STKM stream to the device o 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
Test Procedure	A valid STKM is sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 but with a timestamp TS> Tshigh Terminal receives the message and sends it to the smartcard Smartcard detects that the TS is invalid and returns the status code '9865' (Key freshness failure)
Pass-Criteria	Smartcard detects the error and doesn't generate the TEK. No video is displayed On the spy: the status code returned by the smartcard is '9865' (Key freshness failure) The terminal informs the user that he has no rights for this program and asks user to register to that service

5.5.2.3.7 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.

Test Case Id	BCAST-1.0-DIST-int-439
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	BSM / BSDA sends an LTKM with the security policy extension 0x0A to delete keys associated to the given SEK/PEK ID.
Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.1: 'Correct STKM parsing by the Smartcard' passed successfully. The smartcard has the following valid SEK/PEK o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o with a security_policy_extension = 0x04 o KV: Tslow= 0x00; Tshigh= 0x0F o The video is decrypted successfully
Test Procedure	1. Before the end of the Key validity of the SEK/PEK (when TS of the STKM reaches 0x05), BSM sends a LTKM for the same SEK/PEK ID but with a security policy extension equals to 0x0A. 2. The terminal sends the LTKM to the smartcard 3. The smartcard detects that the LTKM is for a deletion of all SEK/PEK associated to the SEK/PEK ID. 4. The terminal receives the next STKM for the decryption of video 5. The terminal sends the STKM to the smartcard 6. The smartcard detects that SEK/PEK is inexistent for this SEK/PEK ID (see 5.5.2.3.3 and 5.5.2.3.4: Incorrect STKM generation – inexistent SEK/PEK) 7. The smartcard doesn't generate the TEK and the status code is '6A88' (referenced data not found).
Pass-Criteria	Video is decrypted less than 2,66 mns. It is decrypted during 10*6=60s On the spy: the status code returned by the card is '6A88' (referenced data not found). Terminal asks user to register to that service. BSM receives a LTKM request from the terminal

5.5.2.3.8 Replayed STKM reception; test of Pay-per-time and pay-per-view

5.5.2.3.8.1. Precondition 1 – no security_policy_extension in LTKM, pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-440
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST

Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server, passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o Without security-policy-extension o KV: Tslow= 0x00; Tshigh= 0x0F
Test Procedure	STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TEK-ID from 0x00 to 0x0F and TS increasing by one for each sending ▪ Terminal receives the messages and sends them to the smartcard ▪ Smartcard decrypts the TEK and sends them to the terminal ▪ Video is then displayed during 2,66 mns ▪ STKM are resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TEK-ID from 0x00 to 0x0F and the same TS as for the previous stream of STKM ▪ Terminal doesn't perform the replay checking and sends the STKM to the smartcard. ▪ Smartcard detects the replay of STKM and sends back to the terminal the status code '9865' (key freshness failure)
Pass-Criteria	Video is displayed only once. On the spy: Authenticate command response is the sending of TEK (16 times) and then the status code '9865' is returned for the 16 other Authenticate command.

5.5.2.3.8.2. Precondition 2 – security_policy_extension in LTKM: 0x00, pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-441
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST

Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x00 o KV: Tslow= 0x00; Tshigh= 0x0F o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x01

Test Procedure	1. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 2. Test of the pay-per-time: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x00 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x00 iii. Purse_flag = 1 iv. Cost_value= 0x01 v. Token_value= 0x10 3. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard detects the replay comparing the TS received with the stored TS in the card along with the SEK/PEK d. The smartcard detects the replay of STKM and sends back to the terminal the status code '9865' (Key freshness failure).
Pass-Criteria	Video is displayed only once. On the server side a verification message is received with the values described above On the spy: Authenticate command response is the sending of TEK (16 times) and then the status code '9865' is returned for the 16 other Authenticate command.

5.5.2.3.8.3. Precondition 3 – security_policy_extension in LTKM: 0x01, pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-442
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2

SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x01 o KV: Tslow= 0x00; Tshigh= 0x0F o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x01

Test Procedure	1. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 2. Test of the pay-per-time: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0301, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x01 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x01 iii. Purse_flag = 1 iv. Cost_value= 0x01 v. Token_value= 0x10 3. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard decrypts the TEK as the play-back of content is allowed for this Security-policy-extension and there are enough token for the play-back d. Video is then displayed once more during 2,66mns 4. Test of the pay-per-time: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x01 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x01 iii. Purse_flag = 1 iv. Cost_value= 0x01 v. Token_value= 0x00 5. Test of a new replay a. A new STKM is resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS equals to 0x00 b. Terminal sends the STKM to the card c. Smartcard detects that there are no more token in the purse and then returns to the terminal the response: 'lack of credit in the service purse' d. TEK is not returned and video is not displayed

Pass-Criteria	Video is displayed two times. On the server side two verification messages are received with the values described above On the spy: Authenticate command response is the sending of TEK (32 times), the last authenticate command fails and the response is 'lack of credit in the service purse' The terminal informs the user that he has no more credit in the service purse and proposes to the user to buy more tokens.

5.5.2.3.8.4. Precondition 4 – security_policy_extension in LTKM: 0x02, pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-443
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x02 o KV: Tslow= 0x00; Tshigh= 0x0F o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x01

Test Procedure	1. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 2. Test of the pay-per-time: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x02 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x02 iii. Purse_flag = 1 iv. Cost_value= 0x01 v. Token_value= 0x10 3. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard detects the replay comparing the TS received with the stored TS in the card along with the SEK/PEK d. The smartcard detects the replay of STKM and sends back to the terminal the status code '9865 e. ' (Key freshness failure).
Pass-Criteria	Video is displayed only once. On the server side a verification message is received with the values described above On the spy: Authenticate command response is the sending of TEK (16 times) and then the status code '9865' is returned for the 16 other Authenticate command.

5.5.2.3.8.5. Precondition 5 – security_policy_extension in LTKM: 0x03, pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-444
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2

SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x03 o KV: Tslow= 0x00; Tshigh= 0x0F o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x01

Test Procedure	1. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 2. Test of the pay-per-time: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0301, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x03 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x03 iii. Purse_flag = 1 iv. Cost_value= 0x01 v. Token_value= 0x10 3. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard decrypts the TEK as the play-back of content is allowed for this Security-policy-extension and there are enough token for the play-back d. Video is then displayed once more during 2,66mns 4. Test of the pay-per-time: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0301, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x03 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x03 iii. Purse_flag = 1 iv. Cost_value= 0x01 v. Token_value= 0x00 5. Test of a new replay a. A new STKM is resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS equals to 0x00 b. Terminal sends the STKM to the card c. Smartcard detects that there are no more token in the purse and then returns to the terminal the response: 'lack of credit in the user purse' d. TEK is not returned and video is not displayed

Pass-Criteria	Video is displayed two times. On the server side two verification messages are received with the values described above On the spy: Authenticate command response is the sending of TEK (32 times), the last authenticate command fails and the response is 'lack of credit in the user purse' The terminal informs the user that he has no more credit in the user purse and proposes to the user to buy more tokens.

5.5.2.3.8.6. Precondition 6 – security_policy_extension in LTKM: 0x04, pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-445
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x04 o KV: Tslow= 0x00; Tshigh= 0x0F

Test Procedure	1. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period 2. Terminal receives the messages and sends them to the smartcard 3. Smartcard decrypts the TEK and sends them to the terminal 4. Video is then displayed during 2,66 mns 5. STKM are resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F 6. Terminal sends the STKM to the card 7. Smartcard detects the replay comparing the TS received with the stored TS in the card along with the SEK/PEK 8. The smartcard detects the replay of STKM and sends back to the terminal the status code '9865 ' (Key freshness failure).
Pass-Criteria	Video is displayed only once. On the spy: Authenticate command response is the sending of TEK (16 times) and then the status code '9865' is returned for the 16 other Authenticate command.

5.5.2.3.8.7. Precondition 7 – security_policy_extension in LTKM: 0x05, pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-446
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	

Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x05 o KV: Tslow= 0x00; Tshigh= 0x0F
Test Procedure	1. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period 2. Terminal receives the messages and sends them to the smartcard 3. Smartcard decrypts the TEK and sends them to the terminal 4. Video is then displayed during 2,66 mns 5. STKM are resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F 6. Terminal sends the STKM to the card 7. Smartcard decrypts the TEK as the play-back of content is allowed for this Security-policy-extension 8. Video is then displayed once more during 2,66mns
Pass-Criteria	Video is displayed two times. On the spy: Authenticate command response is the sending of TEK (32 times)

5.5.2.3.8.8. Precondition 8 – security_policy_extension in LTKM: 0x06 and play-counter not equal to 0, pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-447
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	

Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x06 o KV: Tslow= 0x00; Tshigh= 0x0F o Number-play-back = 0x01 o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x02

Test Procedure

1. Test of pay-per-view with deduction of token first
    a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x06
    b. The terminal receives the LTKM and sends it to the smartcard
    c. The smartcard sends back a verification message with the following values:
        i. Consumption_reporting_flag=1
        ii. Security_policy_extension = 0x06
        iii. Purse_flag = 1
        iv. Cost_value= 0x02
        v. Number_play_back = 0x01
        vi. Token_value= 0x1E
2. Test of the first viewing
    a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period
    b. Terminal receives the messages and sends them to the smartcard
    c. Smartcard decrypts the TEK and sends them to the terminal
    d. Video is then displayed during 2,66 mns
3. Test of pay-per-view play-back counter unchanged as no play-back occurs at this step
    a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x06
    b. The terminal receives the LTKM and sends it to the smartcard
    c. The smartcard sends back a verification message with the following values:
        i. Consumption_reporting_flag=1
        ii. Security_policy_extension = 0x06
        iii. Purse_flag = 1
        iv. Cost_value= 0x02
        v. Number_play_back = 0x01
        vi. Token_value= 0x1E
4. Test of the replay
    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
    b. Terminal sends the STKM to the card
    c. Smartcard detects the key freshness failure, decrease the play-back counter, decrypts the TEK as one play-back of content is allowed. After this step the play-back counter is 0
    d. Video is then displayed once more during 2,66mns
5. Test of pay-per-view: play-back counter equals to 0 as a play-back occurs
    a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x06
    b. The terminal receives the LTKM and sends it to the smartcard
    c. The smartcard sends back a verification message with the following values:
        i. Consumption_reporting_flag=1
        ii. Security_policy_extension = 0x06
        iii. Purse_flag = 1
        iv. Cost_value= 0x02
        v. Number_play_back = 0x00
        vi. Token_value= 0x1E

Pass-Criteria	Video is displayed two times. On the server side: three verification messages are received with the values described above On the spy: Authenticate command response is the sending of TEK (32 times)

5.5.2.3.8.9. Precondition 9 – security_policy_extension in LTKM: 0x06 and play-counter equal to 0, pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-448
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.8.8: Precondition 8 passed successfully and then in the smartcard there is a SEK/PEK for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, security-policy-extension = 0x06 and with a play-back counter= 0x00 o
Test Procedure	1. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period 2. Terminal receives the messages and sends them to the smartcard 3. Smartcard detects the freshness failure and as the play-back counter is already to 0, the smartcard delete the key and sends back the response to the authenticate command with a status code 'Play-back counter invalid or equal to zero' 4. Video is then not displayed
Pass-Criteria	Video is not displayed. On the spy: Authenticate command response is the sending of status code 'Play-back counter invalid or equal to zero' The terminal informs the user that he has no more authorized play-backs

5.5.2.3.8.10. Precondition 10 – security_policy_extension in LTKM: 0x07, and play-counter not equal to 0 pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-449
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x07 o KV: Tslow= 0x00; Tshigh= 0x0F o Number-play-back = 0x01 o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x02

Test Procedure	1. Test of pay-per-view with deduction of token first a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x07 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x07 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x01 vi. Token_value= 0x1E 2. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 3. Test of pay-per-view play-back counter unchanged as no play-back occurs at this step a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x07 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x07 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x01 vi. Token_value= 0x1E 4. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard detects the key freshness failure, decrease the play-back counter, decrypts the TEK as one play-back of content is allowed. After this step the play-back counter is 0 d. Video is then displayed once more during 2,66mns 5. Test of pay-per-view: play-back counter equals to 0 as a play-back occurs a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x07 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x07 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x00 vi. Token_value= 0x1E

Pass-Criteria	Video is displayed two times. On the server side: three verification messages are received with the values described above On the spy: Authenticate command response is the sending of TEK (32 times)

5.5.2.3.8.11. Precondition 11 – security_policy_extension in LTKM: 0x07, and play-counter equal to 0 pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-450
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.8.10 Precondition 10 passed successfully and then in the smartcard there is a SEK/PEK for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, security-policy-extension = 0x07 and with a play-back counter= 0x00 o
Test Procedure	1. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period 2. Terminal receives the messages and sends them to the smartcard 3. Smartcard detects the freshness failure and as the play-back counter is already to 0, the smartcard delete the key and sends back the response to the authenticate command with a status code 'Play-back counter invalid or equal to zero' 4. Video is then not displayed
Pass-Criteria	Video is not displayed. On the spy: Authenticate command response is the sending of status code 'Play-back counter invalid or equal to zero' The terminal informs the user that he has no more authorized play-backs

5.5.2.3.8.12. Precondition 12 – security_policy_extension in LTKM: 0x08, and play-counter not equal to 0 pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-451
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x08 o KV: Tslow= 0x00; Tshigh= 0x0F o Number-play-back = 0x01 o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x02

Test Procedure	1. Test of pay-per-view without deduction of token at the reception of LTKM a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x08 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x08 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x01 vi. Token_value= 0x20 2. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 3. Test of pay-per-view play-back counter unchanged and without deduction of token as no play-back occurs at this step a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x08 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x08 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x01 vi. Token_value= 0x20 4. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard detects the key freshness failure, decrease the play-back counter, decrypts the TEK as one play-back of content is allowed. After this step the play-back counter is 0 d. Video is then displayed once more during 2,66mns 5. Test of pay-per-view: play-back counter equals to 0 and deduction of token as a play-back occurs a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x08 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x08 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x00 vi. Token_value= 0x1E

Pass-Criteria	Video is displayed two times. On the server side: three verification messages are received with the values described above On the spy: Authenticate command response is the sending of TEK (32 times)

5.5.2.3.8.13. Precondition 13 – security_policy_extension in LTKM: 0x08, and play-counter equal to 0 pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-452
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.8.12 Precondition 12 passed successfully and then in the smartcard there is a SEK/PEK for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, security-policy-extension = 0x08 and with a play-back counter= 0x00 o
Test Procedure	1. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period 2. Terminal receives the messages and sends them to the smartcard 3. Smartcard detects the freshness failure and as the play-back counter is already to 0, the smartcard delete the key and sends back the response to the authenticate command with a status code 'Play-back counter invalid or equal to zero' 4. Video is then not displayed
Pass-Criteria	Video is not displayed. On the spy: Authenticate command response is the sending of status code 'Play-back counter invalid or equal to zero' The terminal informs the user that he has no more authorized play-backs

5.5.2.3.8.14. Precondition 14 – security_policy_extension in LTKM: 0x09, and play-counter not equal to 0 pass criteria: STKM accepted, no error

Test Case Id	BCAST-1.0-DIST-int-453
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 o o A LTKM is sent by the BSM for the SEK/PEK: o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001 o With security-policy-extension = 0x09 o KV: Tslow= 0x00; Tshigh= 0x0F o Number-play-back = 0x01 o Token-value: 0x20 o Purse-mode : 0x00 (set mode) o Cost-value: 0x02

Test Procedure	1. Test of pay-per-view without deduction of token at the reception of LTKM a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x09 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x09 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x01 vi. Token_value= 0x20 2. Test of the first viewing a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period b. Terminal receives the messages and sends them to the smartcard c. Smartcard decrypts the TEK and sends them to the terminal d. Video is then displayed during 2,66 mns 3. Test of pay-per-view play-back counter unchanged and without deduction of token as no play-back occurs at this step a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x09 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x09 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x01 vi. Token_value= 0x20 4. Test of the replay 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 b. Terminal sends the STKM to the card c. Smartcard detects the key freshness failure, decrease the play-back counter, decrypts the TEK as one play-back of content is allowed. After this step the play-back counter is 0 d. Video is then displayed once more during 2,66mns 5. Test of pay-per-view: play-back counter equals to 0 and deduction of token as a play-back occurs a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 1, with the consumption_reporting_flag=1 and security_policy_extension=0x09 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a verification message with the following values: i. Consumption_reporting_flag=1 ii. Security_policy_extension = 0x09 iii. Purse_flag = 1 iv. Cost_value= 0x02 v. Number_play_back = 0x00 vi. Token_value= 0x1E

Pass-Criteria	Video is displayed two times. On the server side: three verification messages are received with the values described above On the spy: Authenticate command response is the sending of TEK (32 times)

5.5.2.3.8.15. Precondition 15 – security_policy_extension in LTKM: 0x09, and play-counter equal to 0 pass criteria: error

Test Case Id	BCAST-1.0-DIST-int-454
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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)
Specification Reference	SPCP spec: 6.7; 6.7.2
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.8.14 Precondition 14 passed successfully and then in the smartcard there is a SEK/PEK for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, security-policy-extension = 0x09 and with a play-back counter= 0x00
Test Procedure	1. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 to 0x0F and TS increasing by one for each crypto-period 2. Terminal receives the messages and sends them to the smartcard 3. Smartcard detects the freshness failure and as the play-back counter is already to 0, the smartcard delete the key and sends back the response to the authenticate command with a status code 'Play-back counter invalid or equal to zero' 4. Video is then not displayed
Pass-Criteria	Video is not displayed. On the spy: Authenticate command response is the sending of status code 'Play-back counter invalid or equal to zero' The terminal informs the user that he has no more authorized play-backs

5.5.2.3.9 STKM reception within the same cryptoperiod – terminal filtering

Test Case Id	BCAST-1.0-DIST-int-455
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	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.
Specification Reference	SPCP spec: 6.7; 6.7.2,
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	○
Test Procedure	BSM/BSDA pushes the same STKM over UDP to the terminal / smartcard. Ensure terminal rejects the STKM i.e. does not send it to the smartcard.
Pass-Criteria	Terminal detects the repeat TEK (STKM) and does not send the STKM to the Smartcard On the spy: just the first STKM is sent to the smartcard. Then no more Authenticate message is sent to the smartcard.

5.5.2.3.10 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 10 and we assume that:

0 = none

1 = -10

2 = -12

3 = -14

4 = -16

5 = -18

As the example given in the specification SPCP

Test Case Id	BCAST-1.0-DIST-int-456
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST
Test Case Description	BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.2.1
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	

Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001
Test Procedure	BSM sends a LTKM for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with a setting of parental control in the card: Level_granted is 3; KV is set from Tslow= 0x0100 to Tshigh= 0x015F; security_policy_extension = 0x04 BSM/BSDA pushes STKM over UDP to the terminal / smartcard, with different rating values: From TS= 0100 to TS= 010F : rating_value is 0 From TS = 0110 to TS = 011F: rating-value is 5 From TS = 0120 to TS= 012F : rating-value is 1 From TS = 0130 to TS= 013F : rating-value is 4 From TS = 0140 to TS= 014F : rating-value is 2 From TS = 0150 to TS= 015F : rating-value is 3
Pass-Criteria	The video is displayed during 2,66 mns Video is not displayed during 2,66 mns and a message indicating that the user is not allowed to watch the program is displayed to the user The video is displayed during 2,66 mns Video is not displayed during 2,66 mns and a message indicating that the user is not allowed to watch the program is displayed to the user The video is displayed during 5,33 mns

5.5.2.3.11 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 10 and we assume that:

0 = none

1 = -10

2 = -12

3 = -14

4 = -16

5 = -18

As the example given in the specification SPCP

Test Case Id	BCAST-1.0-DIST-int-457
Test Object	BCAST Terminal / Smartcard/ Server. UICC is BCAST

Test Case Description	BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.2.1
SCR Reference	BCAST-STKM_SC-C-010
Tool	none
Test code	
Preconditions	The server provides a valid SRTP and STKM stream to the device o 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 o The test 5.5.2.3.7: Key deletion from server passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001
Test Procedure	BSM sends a LTKM for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with a setting of parental control in the card: Level_granted is 3; KV is set from Tslow= 0x0100 to Tshigh= 0x015F; security_policy_extension = 0x04 BSM/BSDA pushes STKM over UDP to the terminal / smartcard, with different rating values: From TS= 0100 to TS= 010F : rating_value is 0 From TS = 0110 to TS = 011F: rating_value is 5 From TS = 0120 to TS= 012F : rating_value is 1 From TS = 0130 to TS= 013F : rating_value is 4 From TS = 0140 to TS= 014F : rating_value is 2 From TS = 0150 to TS= 015F : rating_value is 3
Pass-Criteria	1. The video is displayed during 2,66 mns 2. Then a message to the user is sent for initialization of the PIN; and a change PIN is proposed to the user 3. Then a message to the user is sent for the verification of PIN: verify PIN 4. Pin code is correctly entered and then 5. Video is displayed during 5,33 mns 6. Then a message to the user is sent for the verification of PIN: verify PIN 7. Pin code is correctly entered and then 8. Video is displayed during 8 mns

5.5.2.3.12 Multiple streams protected with same STKM stream

Test Case Id	BCAST-1.0-DIST-int-458
Test Object	BCAST Terminal and Server
Test Case Description	Test that video and audio streams protected with same STKM stream can be processed..

Specification Reference	6.7
SCR Reference	BCAST-STKM_SC-C-01, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-04
Tool	None
Test code	None
Preconditions	1. A bootstrapping context exists between server and terminal. 2. LTKMs containing the SEKs being used to protect the audio and video STKMs have already been sent to the device. 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.
Test Procedure	▪ The terminal receives one STKM stream (for both audio and video content) protected with the SEKs it possesses. ▪ The terminal can decrypt the content – audio and video.
Pass-Criteria	The content (audio and video) can be accessed.

5.5.2.3.13 Multiple streams protected with different STKM streams

Test Case Id	BCAST-1.0-DIST-int-459
Test Object	BCAST Terminal and Server
Test Case Description	Test that video and audio streams protected with different STKM streams can only be accessed when both streams are available.
Specification Reference	6.7
SCR Reference	BCAST-STKM_SC-C-02, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-05
Tool	None
Test code	None
Preconditions	1. A bootstrapping context exists between server and terminal. 2. LTKMs containing the SEKs being used to protect the video (but not the audio) STKMs has already been sent to the device. 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.
Test Procedure	▪ 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. ▪ The terminal can decrypt the video content but not the audio.
Pass-Criteria	▪ The video content can be accessed but the audio cannot.

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

Test Case Id	BCAST-1.0-DIST-int-460
Test Object	BCAST Terminal and Server
Test Case Description	Opening an Ipsec encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST10–ServContProt] Section 9.1. [BCAST10–ServContProt] Section 6.8.1.
SCR Reference	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.
Tool	None
Test code	None
Preconditions	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.
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal • Subscibe to a IPSec protected service • View an IPSec encrypterd programme.
Pass-Criteria	• The terminal is able to subscribe to the service. • The terminal registers the service to be subscribed and disallows the end user to subscribe again. • The terminal is able to decrypt and render the IPSec encrypted audio and video streams belonging to the programme.

5.5.2.4.2 Delivery of SRTP protected stream

Test Case Id	BCAST-1.0-DIST-int-461
Test Object	BCAST Terminal and Server
Test Case Description	Opening an SRTP encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST10–ServContProt] Section 9.2. [BCAST10–ServContProt] Section 6.8.1.
SCR Reference	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.
Tool	None
Test code	None

Preconditions	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.
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal • Subscibe to a SRTP protected service • View an SRTP encrypterd programme.
Pass-Criteria	• The terminal is able to subscribe to the service. • The terminal registers the service to be subscribed and disallows the end user to subscribe again. • The terminal is able to decrypt and render the SRTP encrypted audio and video streams belonging to the programme.

5.5.2.4.3 Delivery of ISMACrypt protected stream

Test Case Id	BCAST-1.0-DIST-int-462
Test Object	BCAST Terminal and Server
Test Case Description	Opening an ISMACrypt encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST10–ServContProt] Section 9.3. [BCAST10–ServContProt] Section 6.8.1.
SCR Reference	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.
Tool	None
Test code	None
Preconditions	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.
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal • Subscibe to a ISMACrypt protected service • View an ISMACrypt encrypterd programme.

Pass-Criteria	• The terminal is able to subscribe to the service. • The terminal registers the service to be subscribed and disallows the end user to subscribe again. • The terminal is able to decrypt and render the Ipsec encrypted audio and video streams belonging to the programme.

5.6 Terminal Provisioning

5.6.1 Receiving terminal provisioning messages using TP-7

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

5.6.2 Update terminal provisioning messages using TP-7

Test Case Id	BCAST-1.0-DIST-int-502
Test Object	BCAST Client
Test Case Description	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.
Specification Reference	[BCAST10-Services] Section 5.2
SCR Reference	BCAST-SERVICES-C-011, BCAST-SERVICES-C-012
Tool	
Test code	
Preconditions	
Test Procedure	
Pass-Criteria	

5.6.3 Declaring Terminal Provisioning as a Service within Service Guide

Test Case Id	BCAST-1.0-DIST-int-503
Test Object	BCAST Client
Test Case Description	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.
Specification Reference	[BCAST10-Services] Section 5.2.2.1
SCR Reference	BCAST-G-T-009
Tool	
Test code	
Preconditions	
Test Procedure	
Pass-Criteria	

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

Test Case Id	BCAST-1.0-DIST-int-504
Test Object	BCAST Client
Test Case Description	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.
Specification Reference	[BCAST10-Ser vices] Section 5.2.1.1
SCR Reference	BCAST-G-T-008
Tool	
Test code	
Preconditions	
Test Procedure	

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