Enabler Test Specification for BCAST Interoperablility

Candidate Version 1.1 – 07 Dec 2010

Open Mobile Alliance

OMA-ETS-BCAST_INT-V1_1-20101207-C

Contents

1. Scope

This document describes interoperability test cases for “Mobile Broadcast Services” according to Open Mobile Alliance™, OMA-TS-BCAST_Services-V1_1, 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

[BCAST1.1-FLO-IP Adaptation] “Broadcast Distribution System Adaptation –Forward Link Only”, Open Mobile Alliance™, OMA-TS-BCAST_FLO_Adaptation-V1_1,
URL: http://www.openmobilealliance.org/

[BCAST1.1WiMAX-Adaptation] “Broadcast Distribution System Adaptation – WiMAX”, Open Mobile Alliance™, OMA-TS-BCAST_WiMAX_Adaptation-V1_1,
URL: http://www.openmobilealliance.org/

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

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

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

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

[BCAST11-ETR] “Enabler Test Requirements for Mobile Broadcast Services”, Open Mobile Alliance™, OMA-ETR-BCAST-V1_1,
URL: http://www.openmobilealliance.org/

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

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

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

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

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

[DRM20-Broadcast-Extensions] “OMA DRM v2.0 Extensions for Broadcast Support”, Open Mobile Alliance™, OMA-TS-DRM_XBS-V1_1-20091027-D

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

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

[OMA DM 1.2] “Enabler Release Definition for OMA Device Management v1.2”, OMA-ERELD-DM-V1_2_0, Open Mobile Alliance™

[OMA DM 1.3] “Enabler Release Definition for OMA Device Management v1.3”, OMA-ERELD-DM-V1_3_0, Open Mobile Alliance™

[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL: http://www.ietf.org/rfc/rfc2119.txt
[SCRRULES]	"SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL: http://www.openmobilealliance.org/

2.2 Informative References

[BCAST11-Architecure]	"Mobile Broadcast Services Architecture", Open Mobile Alliance™, OMA-AD- BCAST-V1_1, URL: http://www.openmobilealliance.org/
[OMADICT]	"Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL: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. [BCAST11-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 1.1”.

5. BCAST IOP Test Cases (Terminal / Server)

5.1 Service Provisioning

5.1.1 Service Guide discovery

Test Case Id	BCAST-1.1-DIST-int-101
Test Object	BCAST Terminal and Server
Test Case Description	This test case tests that the initial reception of the SG is performed correctly.
Specification Reference	[BCAST11 –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.
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031
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-1.1-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	[BCAST11 –Services] Section 5.1.8.
SCR Reference	BCAST-SERVICES-C-010, BCAST-SERVICES-BSM-004
ETR Reference	SPR-002, SPR-006
Tool	None
Test code	None

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.

5.1.3 Service Guide discovery using DNS

Test Case Id	BCAST-1.1-DIST-int-115
Test Object	BCAST Terminal
Test Case Description	Test that the initial reception of the Service Guide is performed correctly when the DNS SRV mechanism is used for Service Guide discovery.
Specification Reference	[BCAST11 –ESG] Section 6.2.1
SCR Reference	BCAST-SG-C-018, BCAST-SGGAD-S-025
ETR Reference	SG-041, SG-056
Tool	None
Test code	None
Preconditions	The DNS server has a SRV record stored which associates the Service Guide entry point URL with the service “oma-bcast-sg” and the domain name which will be derived by the Terminal. BCAST Client UI was not previously provisioned with the BCAST service address.
Test Procedure	• The Terminal is powered-on. • The Terminal issues a DNS SRV lookup to acquire the Service Guide entry point URL. • The Terminal uses the URL to retrieve the Service Guide.
Pass-Criteria	The following things should be visible to the end user • The Service Guide is correctly received by the terminal.

5.2 Service Guide

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

Test Case Id	BCAST-1.1-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	[BCAST11 –ESG] Section 5.4.2.1.2.
SCR Reference	BCAST-SG-C-013
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-005, SG-006, SG-011, SD-001, FD-001, FD-003, SG-018, SG-017, SG-019, SG-020, SG-022, SG-023
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
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.

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

Test Case Id	BCAST-1.1-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	[BCAST11 –ESG] Section 5.4.2.1.2.
SCR Reference	BCAST-SG-C-014
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-003, SG-007, SG-008, SG-009, FD-002, SD-001, SG-020, FD-004
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
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.

5.2.3 Service Guide Update – with additional and removed fragments Broadcast Channel

Test Case Id	BCAST-1.1-DIST-int-105
Test Object	BCAST Terminal and Server
Test Case Description	Updating the Service Guide with new content. Removal of existing SG content.
Specification Reference	[BCAST11 –ESG] Section 5.4.2.1.1.
SCR Reference	BCAST-SG-C-013
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-005, SG-006, SG-011, SD-001, FD-001, FD-003, SG-018, SG-017, SG-019, SG-020, SG-022, SG-023
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 server removing one of the existing programmes. • Update the SG in the terminal. • Browse the SG in the terminal
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 that were not removed and the new programme are visible in the SG. The removed programme is no longer visible.

5.2.4 Service Guide Update with additional and removed fragments – Interaction Channel

Test Case Id	BCAST-1.1-DIST-int-106
Test Object	BCAST Terminal and Server
Test Case Description	Updating the Service Guide with new content. Removal of existing SG content.
Specification Reference	[BCAST11 –ESG] Section 5.4.2.1.1.
SCR Reference	BCAST-SG-C-014
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-003, SG-007, SG-008, SG-009, FD-002, SD-001, SG-020, FD-004
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 server removing one of the existing programmes. • 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 that were not removed and the new programme are visible in the SG.The removed programme is no longer visible.

5.2.5 GZIP compression of Service Guide Delivery Unit

Test Case Id	BCAST-1.1-DIST-int-107
Test Object	BCAST Terminal and Server
Test Case Description	Testing the case where the SGDU is GZIP compressed.
Specification Reference	[BCAST11 –ESG] Section 5.4.1.4.
SCR Reference	BCAST-SG-C-009
ETR Reference	None
Tool	Recommended to use a Protocol analyzer to check the SG is GZIP compressed
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. The package should be delivered through either broadcast channel or interaction channel.
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal
Pass-Criteria	The following things should be visible to the end user • The SG can be displayed by the terminal.

5.2.6 Content hierarchy

Test Case Id	BCAST-1.1-DIST-int-108
Test Object	BCAST Terminal and Server
Test Case Description	Terminal receives a Service Guide containing several content fragments that follow each other in time. The terminal is able to receive the data stream correctly.
Specification Reference	[BCAST11 –ESG] Section 5.1.
SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004

ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-005, SG-006, SG-011, SD-001, FD-001, FD-003, SG-018, SG-017, SG-019, SG-020, SG-022, SG-023
Tool	None
Test code	None
Preconditions	Set up the StartTime and EndTime of the content to match the test time. There are several programmes in the Service Guide which follow each other in time. There are associated audio and video streams available.
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal • Access the associated TV channel (service).
Pass-Criteria	• The SG is available and contains all the available programmes. • Terminal shows the TV channel and the programmes start at the times indicated in the SG.

5.2.7 PreviewData and Service – Broadcast Channel

Test Case Id	BCAST-1.1-DIST-int-109
Test Object	BCAST Terminal and Server
Test Case Description	Associating preview data with service.
Specification Reference	[BCAST11 –ESG] Section 5.1.2.9
SCR Reference	BCAST-SG-C-005
ETR Reference	None
Tool	None
Test code	None
Preconditions	Set up the StartTime and EndTime in the Content Fragment to match the test time. The Server supports one of the Preview Data usages associated with the service: 1. Service-by-Service Switching 2. Service Guide Browsing 3. Service Preview 4. Barker Alternative to blackout
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal
Pass-Criteria	The Used Preview Data method, if supported by the terminal, is correctly shown

5.2.8 PreviewData and Service – Interaction Channel

Test Case Id	BCAST-1.1-DIST-int-110
Test Object	BCAST Terminal and Server
Test Case Description	Associating preview data with service.
Specification Reference	[BCAST11 –ESG] Section 5.1.2.9
SCR Reference	BCAST-SG-C-006
ETR Reference	None
Tool	None
Test code	None
Preconditions	Set up the StartTime and EndTime in the Content Fragment to match the test time. The Server supports one of the PreviewData usages associated with the service: 1. Service-by-Service Switching 2. Service Guide Browsing 3. Service Preview 4. Barker Alternative to blackout
Test Procedure	• Update the SG in the terminal using the test tool as the source • Browse the SG in the terminal
Pass-Criteria	The used Preview Data method, if supported by the terminal, is correctly shown..

5.2.9 Select language specific access parameters

Test Case Id	BCAST-1.1-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	[BCAST11 –ESG] Section 7.2.
SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004 Appendix C.3 (informative)

ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-005, SG-006, SG-011, SD-001, FD-001, FD-003, SG-018, SG-017, SG-019, SG-020, SG-022, SG-023, SG-004, SG-009, SG-012, SG-021, SD-011, SD-012, SD-013, SD-014, SD-015, CODEC-001
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-1.1-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	[BCAST11 –ESG] Section 5.1.2.6.
SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004
ETR Reference	None
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.

5.2.11 Select language specific Service Guide elements

Test Case Id	BCAST-1.1-DIST-int-113
Test Object	BCAST Terminal and Server
Test Case Description	Selecting the correct elements from the Service Guide instance according to the used language.
Specification Reference	[BCAST11 –ESG] Section 7.1.
SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-005, SG-006, SG-011, SD-001, FD-001, FD-003, SG-018, SG-017, SG-019, SG-020, SG-022, SG-023, SG-012
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 where the Name and Description elements are instantiated twice, both with a different language, expressed with the 'xml:lang' attribute. The Service has a programme, where the Content fragment does not have 'xml:lang' attribute defined for the Name and Description elements.
Test Procedure	• Set the preferred language on the terminal • Update the SG in the terminal • Browse the SG in the terminal • View the program information.
Pass-Criteria	The Service Guide is visible, and the selected Content or Service fragment is shown in the proper language. Elements with no language information are also displayed.

5.2.12 TimeGroupingCriteria

Test Case Id	BCAST-1.1-DIST-int-114
Test Object	BCAST Terminal and Server
Test Case Description	Several SGDDs pointing to same Service Guide and the usage of TimeGroupingCriteria.
Specification Reference	[BCAST11 –ESG] Section 5.1.

SCR Reference	BCAST-SG-C-002, BCAST-SG-C-004
ETR Reference	SG-001, SG-002, SG-010, SG-003, SG-013, SG-014, SG-015, SG-024, SG-025, FD-007, FD-008, SG-026, SG-027, FD-009, FD-010, SG-028, SG-029, FD-011, FD-012, SG-030, SG-031, SG-005, SG-006, SG-011, SD-001, FD-001, FD-003, SG-018, SG-017, SG-019, SG-020, SG-022, SG-023
Tool	None
Test code	None
Preconditions	The server sends two SGDDs using the TimeGroupingCriteria E3 element e.g. 1- from 2:00:00-2:29:59 2- from 2:30:00-2:59:59 Both SGDDs point to same Service Guide and contain a different two min Programme (e.g. 1. first programme 2:28-2:30 (SGDD1) 2. second programme 2:30-2:32 (SGDD2). SG is delivered.
Test Procedure	• Update the SG in the terminal • Browse the SG in the terminal
Pass-Criteria	The terminal is able to show the current active Service Guide information (SGDD1). The Terminal MAY also show upcoming Service Guide information (second SGDD2).

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-1.1-DIST-int-201
Test Object	BCAST Terminal and Server
Test Case Description	To test the support of ALC and the interpretation of the file description information on the Service Guide
Specification Reference	[BCAST11-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
ETR Reference	None
Tool	None
Test code	None

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-1.1-DIST-int-202
Test Object	BCAST Terminal and Server
Test Case Description	To test the support of the in-band delivery of the metadata associated with file distributed using FLUTE
Specification Reference	[BCAST11-Distribution] Section 5.2
SCR Reference	BCAST-FD-C-006, BCAST-FD-C-010, BCAST-FD-S-007, BCAST-FD-S-011
ETR Reference	FD-001, FD-016
Tool	None
Test code	None
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-1.1-DIST-int-203
Test Object	BCAST Terminal and Server
Test Case Description	To test the support of the delivery of a file using http over the interaction channel
Specification Reference	[BCAST11-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
ETR Reference	FD-002, FD-004, FD-005
Tool	None
Test code	None
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-1.1-DIST-int-204
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the support of the FEC encoding ID 1 scheme

Specification Reference	[BCAST11-Distribution] – Section 5.2.2
SCR Reference	BCAST-FD-C-007, BCAST-FD-C-009, BCAST-FD-S-008, BCAST-FD-S-010
ETR Reference	FD-001, FD-014
Tool	None
Test code	None
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-1.1-DIST-int-205
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test if the file repair is correctly performed
Specification Reference	[BCAST11-Distribution] – Section 5.3.3
SCR Reference	BCAST-FD-C-014, BCAST-FD-C-015, BCAST-FD-S-015, BCAST-FD-S-016
ETR Reference	None
Tool	None
Test code	None
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-1.1-DIST-int-206
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test the report of the reception of a successful download
Specification Reference	[BCAST11-Distribution] – Section 5.3.2
SCR Reference	BCAST-FD-C-013, BCAST-FD-C-015, BCAST-FD-S-014, BCAST-FD-S-016
ETR Reference	None
Tool	None
Test code	None
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-1.1-DIST-int-207
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the report of the SDP handling and control with RTSP
Specification Reference	[BCAST11-Distribution] – Section 5.5.1.1
SCR Reference	N/A
ETR Reference	None
Tool	None
Test code	None
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.

5.3.1.8 Support of hybrid broadcast/interactive file distribution – FLUTE as fallback

Test Case Id	BCAST-1.1-DIST-int-212
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the support of hybrid broadcast/interactive file distribution using FLUTE as the transport mechanism.
Specification Reference	[BCAST11 –ESG] Section I.3.3, [BCAST11-Distribution] – Section 5.5, 5.6 and D.1

SCR Reference	BCAST-FD-C-010, BCAST-FD-C-018, BCAST-FD-C-028, BCAST-FD-S-001, BCAST-FD-S-011, BCAST-FD-S-027, BCAST-FD-S-035
ETR Reference	FD-001, FD-002, FD-003, FD-004, FD-032, FD-035
Tool	None
Test code	None
Preconditions	The Service Guide signals a file download service, “Service1”, available over both broadcast channel and interactive channel. FLUTE is used as the transport protocol for both broadcast channel and interactive channel.
Test Procedure	• The Terminal is powered-on. • The Terminal receives the Service Guide and displays it to the user. • The user browses the Service Guide and selects “Service1”. • The Terminal is within broadcast coverage and starts to receive “Service1” over broadcast channel. • The Terminal looses broadcast coverage before the complete “Service1” has been received. • The Terminal retrieves the rest of “Service1” using interactive channel.
Pass-Criteria	The following things should be visible to the end user • The Terminal performs an access switch when broadcast coverage is lost and the content described by “Service1” is successfully downloaded.

5.3.1.9 Support of hybrid broadcast/interactive file distribution – HTTP as fallback

Test Case Id	BCAST-1.1-DIST-int-213
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the support of hybrid broadcast/interactive file distribution using HTTP as the transport mechanism for interactive channel.
Specification Reference	[BCAST11 –ESG] Section I.3.3, [BCAST11-Distribution] – Section 5.5 and D.1
SCR Reference	BCAST-FD-C-010, BCAST-FD-C-018, BCAST-FD-C-028, BCAST-FD-S-001, BCAST-FD-S-011, BCAST-FD-S-027, BCAST-FD-S-035
ETR Reference	FD-001, FD-002, FD-003, FD-004
Tool	None
Test code	None
Preconditions	The Service Guide signals a file download service, “Service1”, available over both broadcast channel and interactive channel. FLUTE is used as the transport protocol for both broadcast channel and HTTP is used as the transport protocol for interactive channel.

Test Procedure	• The Terminal is powered-on. • The Terminal receives the Service Guide and displays it to the user. • The user browses the Service Guide and selects “Service1”. • The Terminal is within broadcast coverage and starts to receive “Service1” over broadcast channel. • The Terminal looses broadcast coverage before the complete “Service1” has been received. • The Terminal retrieves the rest of “Service1” using interactive channel.
Pass-Criteria	The following things should be visible to the end user • The Terminal performs an access switch when broadcast coverage is lost and the content described by “Service1” is successfully downloaded.

5.3.2 Streaming Distribution

5.3.2.1 Support of RTP for stream distribution over the broadcast channel

Test Case Id	BCAST-1.1-DIST-int-208
Test Object	BCAST Terminal and Server
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	[BCAST11-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
ETR Reference	SD-001, SD-003, SD-005, SD-006, SD-007, SD-008, SD-009, SD-010
Tool	None
Test code	None
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-1.1-DIST-int-209
Test Object	BCAST Terminal and Server
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	[BCAST11-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
ETR Reference	SD-002, SD-004, SD-005, SD-006, SD-007, SD-008, SD-009, SD-010
Tool	None
Test code	None
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-1.1-DIST-int-210
Test Object	BCAST Terminal and Server

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	[BCAST11-Distribution] – Section 6.7
SCR Reference	BCAST-SD-C-017, BCAST-SD-C-014, BCAST-SD-S-015
ETR Reference	None
Tool	None
Test code	None
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-1.1-DIST-int-211
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the support of the streaming associated procedure
Specification Reference	[BCAST11-Distribution] – Section 6.8.1
SCR Reference	BCAST-SD-C-013, BCAST-SD-S-014
ETR Reference	None
Tool	None
Test code	None
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)

5.3.2.5 Support of hybrid broadcast/interactive stream distribution

Test Case Id	BCAST-1.1-DIST-int-214
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the support of hybrid broadcast/interactive stream distribution.
Specification Reference	[BCAST11 –ESG] Section I.3.2, [BCAST11-Distribution] – Section D.2
SCR Reference	BCAST-SD-C-001, BCAST-SD-C-017, BCAST-SD-S-002, BCAST-SD-S-027
ETR Reference	SD-001, SD-002, SD-003, SD-004
Tool	None
Test code	None
Preconditions	The Service Guide signals a streaming service, “Service1”, available over both broadcast channel and interactive channel.
Test Procedure	• The Terminal is powered-on. • The Terminal receives the Service Guide and displays it to the user. • The user browses the Service Guide and selects “Service1”. • The Terminal is within broadcast coverage and starts to receive “Service1” over broadcast channel. • The Terminal renders “Service1” correctly. • The Terminal looses broadcast coverage. • The Terminal receives and renders “Service1” delivered over interactive channel. • The Terminal regains broadcast channel coverage. • The Terminal receives and renders “Service1” delivered over broadcast channel.
Pass-Criteria	The following things should be visible to the end user • The Terminal performs access switches as the availability of broadcast access and interactive access changes.

5.3.2.6 Support of advisable time ranges for access switch

Test Case Id	BCAST-1.1-DIST-int-213
Test Object	BCAST Terminal and Server
Test Case Description	The purpose of this test is to test the support of advisable time ranges for access switch.
Specification Reference	[BCAST11-Distribution] – Section 6.5.1
SCR Reference	BCAST-SD-C-020, BCAST-SD-S-030
ETR Reference	SD-034, SD-045
Tool	None
Test code	None
Preconditions	The Service Guide signals a streaming service, “Service1”, available over both broadcast channel and interactive channel.
Test Procedure	• The Terminal is powered-on. • The Terminal receives the Service Guide and displays it to the user. • The user browses the Service Guide and selects “Service1”. • The Terminal has no broadcast coverage and issues a request to receive “Service1” over interactive channel. • The Terminal renders “Service1” correctly. • The Terminal regains broadcast channel coverage. • The Terminal issues RTSP GET_PARAMETER to acquire advisable time rages for access switch. • The Terminal makes a controlled access switch to broadcast at a time specified by the acquired advisable time ranges. • The Terminal renders “Service1” correctly.
Pass-Criteria	The following things should be visible to the end user • The access switch from interactive channel to broadcast channel is performed at a time specified by the advisable time ranges.

5.4 Service Interaction

5.4.1 XHTML MP Interactivity – Broadcast Channel

Test Case Id	BCAST-1.1-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	[BCAST11-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
ETR Reference	None
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-1.1-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	[BCAST11-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
ETR Reference	None
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-1.1-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	[BCAST11-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
ETR Reference	SI-001, SI-002, SI-003, SI-004
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-1.1-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	[BCAST11-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
ETR Reference	None
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-1.1-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	[BCAST11-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:
ETR Reference	None
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-1.1-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	[BCAST11-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:
ETR Reference	None
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.

5.4.7 Select language specific Interactivity

Test Case Id	BCAST-1.1-DIST-int-307
Test Object	BCAST Terminal and Server
Test Case Description	Associating a service with interactivity in multiple languages. Selection of interactivity media objects in the preferred language.

Specification Reference	[BCAST11-Services] Section 5.3.6.1.2, 5.3.6.1.4.
SCR Reference	BCAST-SG-C-003, BCAST-SERVICES-C-013, BCAST-SERVICES-C-014, BCAST-SERVICES-C-015, BCAST-SERVICES-C-019, BCAST-SERVICES-C-022
ETR Reference	None
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 that contains interactivity. The InteractivityType element of the InteractivityData fragment has been instantiated twice, both with a different language, expressed with the 'xml:lang' attribute. The InterativityMediaDocument provides MediaObjectSets of different language, expressed with the 'xml:lang' attribute. The terminal supports the interaction method used by the server
Test Procedure	• Set preferred language on the terminal • Update the SG in the terminal • Browse the SG in the terminal • Select a service that contains interactivity. • View the description of the interactivity type. • Use the interactivity
Pass-Criteria	There is a service that contains interactivity. The description of the interactivity type is presented with the preferred language. The interactivity is also presented in the preferred language.

5.5 Service and Content Protection

5.5.1 DRM Profile

5.5.1.1 Delivery of IPSec protected stream

Test Case Id	BCAST-1.1-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	[BCAST11–ServContProt] Section 9.1. [BCAST11–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
ETR Reference	None

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-1.1-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	[BCAST11–ServContProt] Section 9.2. [BCAST11–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
ETR Reference	SCPD-001, SCPD-002, SCPD-003, SCPD-004, SCPD-005, SCPD-006, SCPD-007, SCPD-008, SCPD-009, SCPD010, SCPD-011, SCPD-012, SCPD-013, SCPD-014, SCPD-015, SCPD-016, SCPD-017, SCPD-018, SCPD-019, SCPD-020, SCPD-021
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-1.1-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	[BCAST11–ServContProt] Section 9.3. [BCAST11–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
ETR Reference	None
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 Mobility and Roaming

5.6.1 Availability of Roaming and Showing SG of visited service provider

Test Case Id	BCAST-1.1-MORO-int-101
Test Object	BCAST Terminal and Server
Test Case Description	After terminal receives SGDD(s) from announced session in visited service provider network, terminal acknowledges roaming by matching BSMFiltercode. Terminal requests RoamingRule and shows service guide of visited service provider.
Specification Reference	[BCAST11 –Services] Section 5.7, 5.7.1
SCR Reference	BCAST-SERVICES-C-025, BCAST-SERVICES-C-026, BCAST-SERVICES-BSM-007, BCAST-SERVICES-BSM-008, BCAST-SG-C-002, BCAST-SG-C-004, BCAST-SG-C-008, BCAST-SG-C-010, BCAST-SG-C-011, BCAST-SGGAD-S-001, BCAST-SGGAD-S-005, BCAST-SGGAD-S-015, BCAST-SGGAD-S-016, BCAST-SGGAD-S-018, BCAST-SGGAD-S-019
ETR Reference	None
Tool	None
Test code	None

Preconditions	Terminal is configured to listen to BCAST service guide announcements session on the broadcast channel Terminal is provisioned (e.g. with OMA DM) with the following values: • <X>/BSMFilterCode/Value == ‘Home_BSM’ • <X>/BSMFilterCode/Type == ‘2’ • <X>/BSMFilterCode/IsHomeBSM == ‘true’ • The other leaf node may have value but may skip them in this use case. Announced SGDD from visited service provider has the following value: • ‘id’ of ‘BSMSelector’ element == ‘visitedSP.com/service1’ • ‘type’ of ‘BSMFilterCode’ under “BSMSelector’ == ‘2’ • ‘nonSmartcardCode’ of ‘BSMFilterCode’ under ‘BSMSelector’ == ‘Visited_BSM’ • The other elements and attributes may have value. RomaingRuleRequest message by terminal have the following value: • ‘UserID’ == ‘User_A’ and ‘type’ of ‘UserID’ == ‘0’ • ‘nonSmartcardCode’ of ‘HomeBSMFilterCode’ == ‘Home_BSM’ • ‘BSMSelectorId’ == ‘visitedSP.com/service1’ RoamingRuleResponse message by server have the following value: • ‘id’ of ‘BSMSelectorId’ == ‘visitedSP.com/service1’ • ‘allowAll’ of ‘RoamingRuleType’ == ‘true’
Test Procedure	• Receive SGDD by terminal • Acknowledge no matching BSMFilterCode between SGDD and terminal • Send RoamingRuleRequest message by terminal • Receive RoamingRuleRespone message by terminal • Receive service guide of visited service provider using SGDD • Browse service guide of visited service provider
Pass-Criteria	Service Guide of visited service provider should be visible to the user.

5.7 Parental Control for service ordering

5.7.1 Parental control for service ordering using the Generic Solution

Test Case Id	BCAST-1.1-PCSO-int-102
Test Object	BCAST Terminal and Server

Test Case Description	Test Parental Control for Service Ordering using the Generic Solution.
Specification Reference	Services 5.1.10
SCR Reference	BCAST-SERVICES-C-033, BCAST-SERVICES-C-055, BCAST-SERVICES-BSM-028
ETR Reference	SPR-010, SPR-015
Tool	None
Test code	None
Preconditions	The BSM has stored the level granted and PINCODE associated with the Terminal. The parental control PINCODE associated with the Terminal is 1234. The Service Guide signals a service, “Service1”, for adult with a purchase fragment. The Service Guide is broadcasted. The user has no subscription for “Service1”.
Test Procedure	1. The Terminal is powered-on. 2. The Terminal receives the Service Guide and displays it to the user. 3. The user browses the Service Guide and selects “Service1”. 4. The Terminal asks the user if he wants to purchase the service. 5. The user answers positively. 6. The Terminal sends a Service Request to the BSM. 7. The BSM compares the parental level required for this service with the level granted for the user. It is determined that parental control PINCODE verification is required. 8. The BSM sends a Service Response with the status code 033 “Parental Control Authentication Requested” for the Purchase Item in question. 9. The Terminal requests the user to input PINCODE and the user enters ‘1234’. 10. The Terminal sends a new Service Request message including the PINCODE inputted by the user. 11. The BSM verifies the PINCODE and sends a Service Response with the status code 000 “success”.
Pass-Criteria	1. The BSM sends a Service Response with status code 033. 2. On the Terminal the PINCODE is requested to be inputted by the user. 3. The BSM sends a Service Response with status code 000.

5.8 Parental Control of Unicast Services

5.8.1 Parental control of unicast service consumption – RTSP service

Test Case Id	BCAST-1.1-DIST-int-114
Test Object	BCAST Terminal and Server
Test Case Description	Test Parental Control of Unicast Service consumption for RTSP service.
Specification Reference	Services 5.17

SCR Reference	BCAST-SERVICES-C-058, BCAST-SERVICES-BSM-030, BCAST-SERVICES- BSDA-022
ETR Reference	SD-035, SD-046, SD-047
Tool	None
Test code	None
Preconditions	The MSISDN of the Terminal is 79261234567. The parental control PINCODE associated with the Terminal for unicast consumption is 020579. The BSM has stored the level granted and PINCODE associated with the Terminal. The Service Guide signals a RTSP service, "Service1", for adult which is available on interactive channel.
Test Procedure	1. The Terminal is powered-on. 2. The Terminal receives the Service Guide and displays it to the user. 3. The user browses the Service Guide and selects "Service1". 4. The Terminal issues a RTSP request of "Service1" to be streamed over the interactive channel. 5. The BSM compares the parental level required for this service with the level granted for the user. It is determined that parental control PINCODE verification is required. 6. The Server responds with RTSP status code 401 "Unauthorized " and a realm prefixed with "parental_control@". 7. The Terminal requests the user to input PINCODE and the user enters '020579'. 8. The Terminal issues a new RTSP request including the PINCODE inputted by the user and the MSISDN. 9. The Server starts to stream "Service1".
Pass-Criteria	1. The Server sends a RTSP response with RTSP status code 401 and a realm prefixed with "parental_control@". 2. On the Terminal the PINCODE is requested to be inputted by the user. 3. The Terminal receives "Service1".

5.8.2 Parental control of unicast service consumption – HTTP service

Test Case Id	BCAST-1.1-DIST-int-115
Test Object	BCAST Terminal and Server
Test Case Description	Test Parental Control of Unicast Service consumption for HTTP service.
Specification Reference	Services 5.17
SCR Reference	BCAST-SERVICES-C-058, BCAST-SERVICES-BSM-030, BCAST-SERVICES- BSDA-022
ETR Reference	SD-035, SD-046, SD-047

Tool	None
Test code	None
Preconditions	The MSISDN of the Terminal is 79261234567. The parental control PINCODE associated with the Terminal for unicast consumption is 020579. The BSM has stored the level granted and PINCODE associated with the Terminal. The Service Guide signals a HTTP service, "Service1", for adult which is available on interactive channel.
Test Procedure	1. The Terminal is powered-on. 2. The Terminal receives the Service Guide and displays it to the user. 3. The user browses the Service Guide and selects "Service1". 4. The Terminal issues a HTTP request of "Service1" to be retrieved over the interactive channel. 5. The BSM compares the parental level required for this service with the level granted for the user. It is determined that parental control PINCODE verification is required. 6. The Server responds with HTTP status code 401 "Unauthorized " and a realm prefixed with "parental_control@". 7. The Terminal requests the user to input PINCODE and the user enters '020579'. 8. The Terminal issues a new HTTP request including the PINCODE inputted by the user and the MSISDN. 9. The Server starts to deliver "Service1".
Pass-Criteria	1. The Server sends a HTTP response with HTTP status code 401 and a realm prefixed with "parental_control@". 2. On the Terminal the PINCODE is requested to be inputted by the user. 3. The Terminal receives "Service1".

6. BCAST IOP Test Cases (Terminal / Server / SmartCard)

6.1 Service and Content Protection

6.1.1 Layer 1 Authentication and Service Registration

3G Authentication used in bootstrapping procedures:

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

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

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

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

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

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

6.1.1.1 GBA-U Bootstrapping USIM /BSM with success

Test Case Id	BCAST-1.1-DIST-int-404
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard 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. Smartcard is MBMS only or MBMS/BCAST.
Specification Reference	SPCP spec: 6.10, 6.5
SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-003
ETR Reference	SCPS-001, SCPS-007
Tool	None
Test code	None

Preconditions	○ No bootstrapping context exists between BSM and terminal/smartcard ○ Smartcard contains Key management: Smartcard is GBA and MBMS or BCAST enabled ○ Smartcard contains a valid 3G subscription (IMSI/K and algo Milenage) ○ HSS is able to provide Authentication Vectors (AV, AV=RAND||AUTN||XRES|| CK||IK) associated with the IMSI/K. ○ Session description fragment contains MBMS USD with a service protection description fragment containing ○ the key management element with a key management server definition. ○ And the attribute uiccKeyManagement indicating that the Smartcard based key management is required for the service. ○ Or the information are provided using the SDP. ○ 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 sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid). g. Terminal sends an HTTP request, containing the Digest AKA response calculated using RES, to the BSF. h. BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI i. BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal j. The terminal stores B-TID and key lifetime in the EF_{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.

Test Procedure continued	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.

6.1.1.2 GBA-U Bootstrapping USIM / BSM with synchronization error

Test Case Id	BCAST-1.1-DIST-int-405
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or MBMS/BCAST
Test Case Description	Test that SQN error is detected by the terminal during a GBA bootstrapping Smartcard is MBMS only or MBMS/BCAST
Specification Reference	SPCP spec: 6.10, 6.5
SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-003
ETR Reference	None
Tool	None
Test code	None
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 Smartcard contains Key management Smartcard 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 Smartcard 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	○ reception at BSF of a GET request from Terminal with the appropriate IMPI ○ reception at BSF of AUTS in the second GET request

6.1.1.3 GBA_U: Expired Bootstrapping data

Test Case Id	BCAST-1.1-DIST-int-406
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or MBMS/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. Smartcard is MBMS only or MBMS/BCAST
Specification Reference	SPCP spec 6.5.1

SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-003
ETR Reference	SCPS-001, SCPS-007
Tool	None
Test code	None
Preconditions	○ A bootstrapping context exists between server and terminal/smartcard ○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS security enabled). ○ Smartcard 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 Smartcard based key management is required for the service. ○ The key management server with which the terminal should register. ○ 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. ○ 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. ○ The BSM wishes to renegotiate bootstrapping, i.e. the key lifetime has expired on the BSM side.

<table>
<tr><td><b>Test Procedure</b></td><td>4. The BCAST client is started, re-activated or otherwise prompted to start user registration.
5. 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.
6. The BSM returns a 401 unauthorised response in order to force the terminal to perform bootstrapping.
7. The terminal/smartcard 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}
8. The terminal/smartcard reissues the MBMS User registration request to the BSM using the new BT-ID and Ks_ext_NAF (SRK)
9. .The BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each service.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td>• 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.
• 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.</td></tr>
</table>

6.1.1.4 GBA_U: Different Key K on Client and Server

Test Case Id	BCAST-1.1-DIST-int-407
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or MBMS/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. Smartacrd is MBMS only ir MBMS/BCAST.
Specification Reference	SPCP Spec 6.5.1
SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-003
ETR Reference	None
Tool	None
Test code	None
Preconditions	o No bootstrapping context exists between the server and terminal/smartcard. o Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS-enabled). o Smartcard 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 Smartcard 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 Smartcard 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.

Test Procedure	1. The Terminal and the BSF establish bootstrapped security association between them by running bootstrapping procedure 2. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity.(IMPI found in the USIM derived from IMSI as specified in TS 23 003) 3. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102) 4. The BSF selects an authentication vector AV= RAND||AUTN||XRES||CK||IK 5. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND||AUTN 6. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode 7. The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK 8. USIM sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid). 9. Terminal sends challenge response back to the BSF in GET request 10. 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.
Pass-Criteria	1. Reception at BSF of a GET request from Terminal with the appropriate IMPI to kick off bootstrapping. 2. The BSF returns a response to the terminal which indicates that the authentication failure has occurred or retuens a new challenge.

6.1.1.5 Deregistration

Test Case Id	BCAST-1.1-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. Card is MBMS only or MBMS/BCAST
Specification Reference	SPCP Spec 6.6
SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-003, BCAST-SERVICES-C-007, BCAST-SERVICES-C-008, BCAST-SERVICES-BSM-001, BCAST-SERVICES-BSM-002
ETR Reference	SCPS-001, SCPS-007
Tool	None
Test code	None

Preconditions	○ A bootstrapping context exists between server and terminal/smartcard ○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS security enabled). ○ Smartcard 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 Smartcard 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	1. The BCAST Client is terminated or suspended on the terminal (This should prompt a deregistration flow). 2. The terminal initiates the MBMS user deregistration flow. 3. Terminal sends a HTTP post to the BSM containing the Service ID. 4. The BSM answers with 401 Unauthorized indicating that the BSM wants to authenticate the terminal using the bootstrapped security association 5. Key derivation: Terminal sends NAF_ID and IMPI to USIM using the AUTHENTICATE command in GBA security context: NAF derivation mode. 6. 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). 7. The terminal sends to the BSM a HTTP POST request with B-TID as username and Ks_ext_NAF (SRK) as password as well as the Service IDs. 8. BSM retrieves Ks_ext_NAF from the BSF and verifies the message received from the terminal. 9. If success the BSM sends a 200 OK response to the terminal with Authentication-info header with a list of status code for each service.
Pass-Criteria	The BSM receives a HTTP POST device from the terminal containing the Service Ids. At the end of the flow a 200 OK response (and a list of status codes) is returned by the BSM.

6.1.1.6 Deregistration with Bootstrapping

Test Case Id	BCAST-1.1-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. Card is MBMS only or MBMS/BCAST.
Specification Reference	SPCP Spec 6.6
SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-003, BCAST-SERVICES-C-007, BCAST-SERVICES-C-008, BCAST-SERVICES-BSM-001, BCAST-SERVICES-BSM-002
ETR Reference	SCPS-001, SCPS-007
Tool	None
Test code	None
Preconditions	○ No bootstrapping context exists between server and terminal/smartcard ○ Smartcard contains Key management: Smartcard is GBA and BCAST enabled (if the Smartcard is MBMS only, the BSM being tested must also be MBMS security enabled). ○ Smartcard 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 Smartcard 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. ○ The BSM wishes to renegotiate bootstrapping, i.e. the key lifetime has expired on the BSM side.
Test Procedure	The BCAST Client is terminated or suspended on the terminal (This should prompt a deregistration flow). 1. The terminal initiates the MBMS user deregistration flow. 2. Terminal sends a HTTP post to the BSM containing the Service ID. 3. The BSM answers with 401 Unauthorized indicating that the BSM wants to authenticate the terminal using the bootstrapped security association 4. Key derivation: Terminal sends NAF_ID and IMPI to USIM using the

	AUTHENTICATE command in GBA security context: NAF derivation mode. 5. 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). 6. The terminal sends to the BSM a HTTP POST request with B-TID as username and Ks_ext_NAF (SRK) as password as well as the Service IDs. 7. BSM determines that bootstrapping should be rerun and therefore returns a bootstrapping renegotiation indicator by returning a 401 “Unauthorized” HTTP response 8. Prompted by receiving a bootstrapping regenotiation indication, the terminal initiates bootstrapping. 9. The Terminal sends an initial GET request (HTTP request) to the BSF containing the private user identity. 10. The BSF retrieves Authentication vector from the HSS (Authentication vectors are computed using the Milenage algorithm and function described in TS 33 102) 11. The BSF selects an authentication vector AV= RAND||AUTN||XRES||CK||IK 12. BSF forwards the challenge to the terminal in the HTTP 401 Unauthorized response: RAND||AUTN 13. Terminal sends RAND and AUTN to the USIM using the AUTHENTICATE command in GBA security context: Bootstrapping Mode 14. The USIM verifies MAC and SQN from AUTN and calculates authentication challenge response computes the session keys IK and CK 15. USIM sends the response of AUTHENTICATE command RES authentication challenge response (SQN valid). 16. Terminal sends challenge response back to the BSF in GET request 17. BSF checks that the RES corresponds to the XRES. The BSF generates the bootstrapping Transaction Identifier (B-TID) for the IMPI 18. BSF sends a 200OK message including the B-TID and the Key lifetime of the key Ks to the terminal 19. The terminal stores B-TID and key lifetime in the EF_{GBABP} 20. The terminal reinitiates the MBMS user deregistration flow with the enw bootstrapping data. 21. The terminal sends to the BSM a HTTP POST request with B-TID as username and Ks_ext_NAF (SRK) as password as well as the Service IDs. 22. The BSM returns a 200 OK as well as the status codes of the Service Ids.

Pass-Criteria	1. The terminal initiates bootstrapping on receiving a bootstrapping negotiation indication from the BSM. 2. The BSM returns a 200 ok response after receiving an MBMS user deregistration request from the terminal using the new bootstrapping data.

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

Test Case Id	BCAST-1.1-DIST-int-410
Test Object	BCAST Terminal /Smartcard. Smartcard is BCMCS/BCAST or BCAST
Test Case Description	Test that SMK and SRK derivation from pre-provisioned SCK in the terminal are successful. Smartcard is BCMCS/BCAST or BCAST.
Specification Reference	SPCP spec: 6.10, 6.5.2
SCR Reference	BCAST-SPCP-C-005, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-004
ETR Reference	SCPS-001
Tool	BCAST conformance test tool. Spy of the terminal/Smartcard interface Test Smartcard BCMCS-only or BCAST
Test code	None
Preconditions	○ Pre-provisioned “SmartCard Key” (SCK), corresponding to the Registration Key (RK) in BCMCS, is stored on the Smartcard, from which the SMK and SRK (TK and Auth-Key, respectively, in BCMCS) are derived. ○ Description of service access is provided by BCMCS Information Acquisition as specified in [BCAST-ServContProt] Section 6.10.2. ○ 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 Smartcard /terminal and the BSM share the same SRK.

6.1.2 Layer 2 LTKM

6.1.2.1 OMA BCAST LTKM Terminal processing

6.1.2.1.1 LTKM without SPE, without consumption reporting, MBMS only card

Test Case Id	BCAST-1.1-DIST-int-411
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS/BCMCS only or BCAST
Test Case Description	Test that an LTKM without SPE and without consumption reporting flag can be successfully received over UDP, and that the terminal sends the LTKM to the smartcard which sends back a verification message.
Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005 OR BCAST-SCSPCP-C-006 AND (BCAST-SCSPCP-C-003 OR BCAST-SCSPCP-C-004)
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-003
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-004
SCR Reference III	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-006, BCAST-SCSPCP-C-003
SCR Reference IV	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-006, BCAST-SCSPCP-C-004
ETR Reference	SCPS-002, SCPS-008
Tool	Spy of the terminal / Smartcard interface
Test code	None
Preconditions	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. A Service registration has been performed with the BSM (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used) The LTKM is valid and indicates that a verification message is needed The LTKM contains an EXT BCAST field with security_ext_policy_flag= LTK_FLAG_FALSE, and consumption_reporting_flag=LTK_FLAG_FALSE Card is an MBMS only card, as indicated in EF_UST

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 On the spy. A READ RECORD command on EF_MUK(6FD8) is sent from the terminal to the smartcard, to check timestamp stored. (Anti-replay check performs in terminal) An AUTHENTICATE command in MSK update mode is sent to the smartcard, and a LTKM verification message is returned in the response.

6.1.2.1.2 LTKM without SPE, with consumption reporting, BCAST card

Test Case Id	BCAST-1.1-DIST-int-600
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test that an LTKM without SPE and without Consumption reporting flag can be successfully received over UDP, and that the terminal does not send the LTKM to the BCAST smartcard.
Specification Reference	SPCP spec: 6.6.7
SCR Reference	BCAST-LTKM_SC-C-015 , BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005 AND BCAST-SCSPCP-C-007AND (BCAST-SCSPCP-C-003 OR BCAST-SCSPCP-C-004)
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-003
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-004
ETR Reference	SCPS-002, SCPS-008
Tool	Spy of the terminal / Smartcard interface
Test code	None

Preconditions	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. A Service registration has been performed with the BSM (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used) The LTKM is valid and indicates that a verification message is needed The LTKM contains an EXT BCAST field, with security_ext_policy_flag= LTK_FLAG_FALSE, and consumption_reporting_flag=LTK_FLAG_FALSE Card is an BCAST enabled card, as indicated in EF_UST
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 verifies the BCAST EXT, doesn't send the message to the BCAST card and discards the message
Pass-Criteria	BSM doesn't receive the verification message On the spy, there is no AUTHENTICATE command sent to the smartcard

6.1.2.1.3 LTKM with SPE, MBMS only card

Test Case Id	BCAST-1.1-DIST-int-601
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only
Test Case Description	Test that an LTKM with SPE can be successfully received over UDP, that the terminal does not send the LTKM to the MBMS only smartcard.
Specification Reference	SPCP spec: 6.6.7
SCR Reference	BCAST-LTKM_SC-C-015 , BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-032, (BCAST-SCSPCP-C-005 OR BCAST-SCSPCP-C-006) AND BCAST-SCSPCP-C-003
SCR Reference I	• BCAST-LTKM_SC-C-015 , BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-003
SCR Reference II	• BCAST-LTKM_SC-C-015 , BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-006, BCAST-SCSPCP-C-003
ETR Reference	SCPS-002, SCPS-008
Tool	Spy of the terminal / Smartcard interface
Test code	None
Preconditions	• Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. • A Service registration has been performed with the BSM (i.e. test 6.1.1.1 for GBA-U has been performed first) • The smartcard is MBMS only card, as indicated in EF_UST • The LTKM is valid, indicates that a verification message is needed, and contains EXT BCAST field with Security_policy_ext_flag set to LTK_FLAG_TRUE

Test Procedure	1. BSM pushes an LTKM over UDP to the terminal / smartcard with EXT BCAST payload. Test for GBA_U case. 2. Terminal receives LTKM, 3. Terminal discards the message
Pass-Criteria	BSM doesn't receive a verification message On the spy, there is no AUTHENTICATE command sent to the smartcard

6.1.2.1.4 LTKM with SPE, BCAST card

Test Case Id	BCAST-1.1-DIST-int-602
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test that an LTKM with SPE can be successfully received over UDP, that the terminal sends the LTKM to the BCAST smartcard which sends back a verification message.
Specification Reference	SPCP spec: 6.6.7, 6.6.6.1
SCR Reference	BCAST-LTKM_SC-C-015 , BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005 AND BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-008 AND BCAST-SCSPCP-C-010 AND (BCAST-SCSPCP-C-003 OR BCAST-SCSPCP-C-004)
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-008, BCAST-SCSPCP-C-010, BCAST-SCSPCP-C-003
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-008, BCAST-SCSPCP-C-010, BCAST-SCSPCP-C-004
ETR Reference	SCPS-002, SCPS-008
Tool	Spy of the terminal / Smartcard interface
Test code	None
Preconditions	• Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. • A Service registration has been performed with the BSM (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used) • The smartcard is MBMS/BCAST or BCMCS/BCAST • The LTKM indicates that a verification message is needed • The LTKM is valid and contains EXT BCAST field with Security_policy_ext_flag is set to LTK_FLAG_TRUE

Test Procedure	1. BSM pushes an LTKM over UDP to the terminal / smartcard with EXT BCAST payload. Test for GBA_U case. 2. Terminal receives LTKM, 3. Terminal sends the LTKM to the smartcard, without anti-replay check 4. Smartcard verifies integrity of the message 5. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message 6. Terminal sends the verification message to the BSM.
Pass-Criteria	BSM receives a verification message On the spy. No READ RECORD command on EF_MUK (6FD8) (Anti-replay check not performed by the terminal) An AUTHENTICATE command in MSK update mode is sent to the smartcard, and a LTKM verification message is returned in the response.

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

Test Case Id	BCAST-1.1-DIST-int-412
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS/BCMCS only or BCAST
Test Case Description	Test that an LTKM can be successfully • requested by the terminal • delivered over UDP to the terminal Test that a verification message is sent. MBMS/BCAST smartcard
Specification Reference	SPCP spec: 6.6, 6.6.7
SCR Reference	BCAST-SERVICES-C-007 AND BCAST-SERVICES-C-008 AND BCAST-LTKM_SC-C-015 , BCAST-SERVICES-BSM-001 AND BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005 AND BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-008 AND BCAST-SCSPCP-C-010 AND (BCAST-SCSPCP-C-003 OR BCAST-SCSPCP-C-004)
SCR Reference I	• BCAST-SERVICES-C-007, BCAST-SERVICES-C-008, BCAST-LTKM_SC-C-015 , BCAST-SERVICES-BSM-001, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-008, BCAST-SCSPCP-C-010, BCAST-SCSPCP-C-003
SCR Reference II	• BCAST-SERVICES-C-007, BCAST-SERVICES-C-008, BCAST-LTKM_SC-C-015 , BCAST-SERVICES-BSM-001, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-005, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-008, BCAST-SCSPCP-C-010, BCAST-SCSPCP-C-004
ETR Reference	SCPS-002, SCPS-008
Tool	None
Test code	None

Preconditions	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. Service registration has been performed. . (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used) Terminal has missed an LTKM update because was out of coverage. IP context doesn't exist anymore LTKM contains EXT BCAST field, with SPE The smartcard is BCAST
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 sends the LTKM to the smartcard, without anti-replay check 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 a successful LTKM request BSM receives the verification message

6.1.2.1.6 BSM solicited pull procedure

Test Case Id	BCAST-1.1-DIST-int-413
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard 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. Smartcard is MBMS only or BCAST.
Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-014 , BCAST-SCSPCP-C-005
ETR Reference	None
Tool	None

Test code	None
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. o Service registration has been performed. . (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)
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, Key group part different than 1 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

6.1.2.1.7 BSM solicited pull procedure initiation over SMS Bearer

Test Case Id	BCAST-1.1-DIST-int-414
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard 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. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.2
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-016, BCAST-SCSPCP-C-005
ETR Reference	None
Tool	None
Test code	None
Preconditions	o Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. o Service registration has been performed. (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)
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. MSK ID key group part is different than 1. 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

6.1.2.1.8 BSM solicited pull procedure to initiate the Registration Procedure

Test Case Id	BCAST-1.1-DIST-int-603
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is MBMS only or BCAST

Test Case Description	Test that the BSM solicited pull procedure to initiate the Registration Procedure is correctly understood by the terminal and that the terminal is then able to request the LTKM update. Smartcard is MBMS only or BCAST.
Specification Reference	SPCP spec: 6.6.3
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-017, BCAST-SCSPCP-C-005
ETR Reference	None
Tool	None
Test code	None
Preconditions	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. Service registration has been performed. (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)
Test Procedure	1. BSM sends a MIKEY message with the last SMK known by the BSM and with the key group of MSK-ID= 1 and key number part =0 2. The terminal shall initiate a registration procedure with MBMS User Service ID=”oma-bcast-allservices”
Pass-Criteria	BSM receives a registration request with MBMS User Service ID=”oma-bcast-allservices”

6.1.2.1.9 LTKM Replay Detection in secure function, failure case

Test Case Id	BCAST-1.1-DIST-int-604
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test that an LTKM will be rejected if TS received is less than or equal to the last received TS stored in smartcard. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.7.3
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-014, BCAST-BSMSPCP-S-032, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-010
ETR Reference	None
Tool	Spy of the terminal / Smartcard interface
Test code	None
Preconditions	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal. Service registration has been performed. (i.e. test 6.1.1.1 for GBA-U has been performed first in case USIM is used or test 6.1.1.7 for pre-provisioned SmartCard Key has been performed first in case (R-)UIM/CSIM is used)

Test Procedure	23. BSM pushes an LTKM over UDP to the terminal / smartcard and asks for a verification message. Test for GBA_U case. 24. Terminal receives LTKM, 25. Terminal sends the LTKM to the smartcard 26. Smartcard verifies integrity of the message using SMK (MUK) 27. Smartcard stores TS in EF_MUK 28. Smartcard and then terminal send back a verification message 29. BSM pushes a LTKM with the same TS 30. Terminal receives LTKM, 31. Terminal sends the LTKM to the smartcard 32. Smartcard verifies integrity of the message using SMK (MUK) 33. Smartcard verifies TS against the stored LTKM replay counter value. (failure) 34. Verification message is not returned to the BSM
Pass-Criteria	BSM receives a Verification Message after step1) BSM does not receive a verification message 4 min after step 7) On the spy The first AUTHENTICATE command in MSK update mode returns SW=9000 and a verification message is included in the response. The second AUTHENTICATE command in MSK update mode returns SW=9862 (authentication error, incorrect MAC) is returned

6.1.2.2 Managing purses and counters using OMA BCAST LTKM

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

Test Case Id	preambule for managing purses and counters test cases
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test that an LTKM with EXT BCAST field can be successfully received over UDP at the terminal / smartcard that the purse and counters according to SPE value are successfully updated and that and a verification message and consumption reporting message are sent. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-008
ETR Reference	None
Tool	Noneone
Test code	None

Preconditions	Shared SMK and SRK, as well as valid IP context, exists between BSM and terminal: A Service registration has been performed with the BSM and with a GBA-U (i.e. test 6.1.1.1 with success) The LTKM is valid and indicates that a verification message is needed 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 4. Smartcard verifies integrity of the message 5. Smartcard performs replay protection check 6. Smartcard sees request for acknowledgement. And sends back to the terminal the MIKEY verification message 7. Terminal sends the verification message to the BSM. 8. BSM receives Verification Message 9. BSM push a LTKM2 Message over UDP to the terminal/smartcard with a consumption reporting_flag = 1. V bit =0, same SPE, SEK/PEK id and KV as LTKM1 10. BSM receives LTKM Reporting Message
Pass-Criteria	BSM receives the verification message BSM receives LTKM Reporting Message containing data according to following tests

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

6.1.2.2.1 Set of live ppt purse associated with a key group, SPE=0x00

Test Case Id	BCAST-1.1-DIST-int-605
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Set of live_ppt_purse associated with a key group, SPE=0x00 The live_ppt_purse created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-020, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-013
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preamble for managing purses and counters test cases Smartcard shall support SPE=0x00

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0002 0001 V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x00; purse_flag = 1; purse_mode = 0; token_value = 0x05; cost_value=0x00; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x00 ○ Cost_value= 0x00 ○ Purse_value=0x05 (value of live_ppt_purse)

6.1.2.2.2 Test of set mode for the live_ppt_purse associated with a key group, SPE=0x00

Test Case Id	BCAST-1.1-DIST-int-606
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of set mode for the live_ppt_purse associated with a key group, SPE=0x00 Set mode executed on a already created purse. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-020, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-013
ETR Reference	**None**
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-605 passed successfully first Smartcard shall support SPE=0x00

Test Procedure	See preambule for managing purses and counters test cases LTKM1 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 =0x00; purse_flag = 1; purse_mode = 0; token_value = 0x10; cost_value=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 02 00; Tshigh = 0x00 00 02 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x00 ○ Cost_value= 0x01 ○ Purse_value=0x10 (value of live_ppt_purse)

6.1.2.2.3 Test of add mode for the live_ppt_purse associated with a key group, SPE=0x00

Test Case Id	BCAST-1.1-DIST-int-607
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of add mode for the live_ppt_purse associated with a key group, SPE=0x00 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-020, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-013
ETR Reference	**None**
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-606 passed successfully first Smartcard shall support SPE=0x00

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0002 0002 (same Key_group but different Key_Number part) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x00; purse_flag = 1; purse_mode = 1; token_value = 0x10; cost_value=0x02; access_criteria_flag = 0 KV: Tslow = 0x 00 00 03 00; Tshigh = 0x00 00 03 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x00 ○ Cost_value= 0x02 ○ Purse_value=0x20 (value of live_ppt_purse)

6.1.2.2.4 Test of overflow for the live_ppt_purse associated with a key group, SPE=0x00

Test Case Id	BCAST-1.1-DIST-int-608
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of overflow for the live_ppt_purse associated with a key group, SPE=0x00 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-020, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-013
ETR Reference	None
Tool	None
Test code	None
Preconditions	Seepreambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-607 passed successfully first Smartcard shall support SPE=0x00

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0002 0003 (same Key_group as the previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x00; purse_flag = 1; purse_mode = 1; token_value = 0x7FFFFFFF; cost_value=0x03; access_criteria_flag = 0 KV: Tslow = 0x00 00 04 00; Tshigh = 0x00 00 04 FF
Pass-Criteria	BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 1 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x00 ○ Cost_value= 0x03 ○ Purse_value=0x20 (value of live_ppt_purse)

6.1.2.2.5 Set of playback_ppt_purse associated with a key group, SPE=0x01

Test Case Id	BCAST-1.1-DIST-int-609
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Set of playback_ppt_purse associated with a key group, SPE=0x01 The playback_ppt_purse created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-021, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-014
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Smartcard shall support SPE=0x01

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0003 0001 (new Key_group) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x01; purse_flag = 1; cost_value=0x01; purse_mode = 0; token_value = 0x10; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x01 ○ Cost_value= 0x01 ○ Purse_value=0x10 (value of playback_ppt_purse, managed independently from live_ppt_purse)

6.1.2.2.6 Test of set mode for playback_ppt_purse associated with a key group, SPE=0x01

Test Case Id	BCAST-1.1-DIST-int-610
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for set mode for playback_ppt_purse associated with a key group, SPE=0x01 Set mode executed on a already created purse. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-021, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-014
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-609 passed successfully first Smartcard shall support SPE=0x01

Test Procedure	See preambule for managing purses and counters test cases LTKM fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0003 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 = 0; token_value = 0x20; cost_value=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 02 00; Tshigh = 0x00 00 02 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters o consumption_reporting_flag = 1 o Overflow_flag = 0 o Unsupported_extention_flag = 0 o Not_found_flag = 0 o Security_policy_extension = 0x01 o Cost_value= 0x01 o Purse_value=0x20 (value of playback_ppt_purse, managed independently from live_ppt_purse)

6.1.2.2.7 Test of add mode for playback_ppt_purse associated with a key group, SPE=0x01e

Test Case Id	BCAST-1.1-DIST-int-611
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for add mode for playback_ppt_purse associated with a key group, SPE=0x01 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-021, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-014
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-610 passed successfully first Smartcard shall support SPE=0x01

Test Procedure	See preambule for managing purses and counters test cases LTKM fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0003 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=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 03 00; Tshigh = 0x00 00 03 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x01 ○ Cost_value= 0x01 ○ Purse_value=0x30

6.1.2.2.8 Test of overflow for playback_ppt_purse associated with a key group, SPE=0x01

Test Case Id	BCAST-1.1-DIST-int-612
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of overflow for playback_ppt_purse associated with a key group, SPE=0x01 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-021, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-014
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-611 passed successfully first Smartcard shall support SPE=0x01

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0003 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 = 0x7FFFFFFF; cost_value=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 04 00; Tshigh = 0x00 00 04 FF
Pass-Criteria	BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 1 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x01 ○ Cost_value= 0x01 ○ Purse_value=0x30

6.1.2.2.9 Set of user_purse associated with a NAF/SMK id

Test Case Id	BCAST-1.1-DIST-int-613
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Set of user_purse associated with a NAF/SMK id The user_purse created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-022, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-015
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Card shall support SPE=0x02, 0x03, 0x08 or 0x09 Below test is described with the assumption that the card supports SPE=0x02.

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0004 0001 (newKey_group) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x02; purse_flag = 1; cost_value=0x01; purse_mode = 0; token_value = 0x10; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters o consumption_reporting_flag = 1 o Overflow_flag = 0 o Unsupported_extention_flag = 0 o Not_found_flag = 0 o Security_policy_extension = 0x02 o Cost_value= 0x01 o Purse_value=0x10

6.1.2.2.10 Test of set mode for user_purse associated with a NAF/SMK id

Test Case Id	BCAST-1.1-DIST-int-614
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for set mode for user_purse associated with NAF/SMK id Set mode executed on a already created purse. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-022, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-015
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-613 passed successfully first Card shall support SPE=0x02, 0x03, 0x08 or 0x09 Below test is described with the assumption that the card supports SPE=0x02.

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0004 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 = 0x20; cost_value=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 02 00; Tshigh = 0x00 00 02 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x02 ○ Cost_value= 0x01 ○ Purse_value=0x20 (value of user_purse)

6.1.2.2.11 Test of add mode for user_purse associated with NAF/SMK id

Test Case Id	BCAST-1.1-DIST-int-615
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for add mode for user_purse associated with NAF/SMK id Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-022, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-015
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-614 passed successfully first Card shall support SPE=0x02, 0x03, 0x08 or 0x09 Below test is described with the assumption that the card supports SPE=0x02.

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0004 0002 (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 = 1; token_value = 0x10; cost_value=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 03 00; Tshigh = 0x00 00 03 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x02 ○ Cost_value= 0x01 ○ Purse_value=0x30

6.1.2.2.12 Test of overflow for user_purse associated with NAF/SMK id

Test Case Id	BCAST-1.1-DIST-int-616
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of overflow for user_purse associated with NAF/SMK id Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-022, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-015
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-615 passed successfully first Card shall support SPE=0x02, 0x03, 0x08 or 0x09 Below test is described with the assumption that the card supports SPE=0x02.

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0005 0002 (different Key_group, to test that key group is not associated with user_purse) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x02; purse_flag = 1; purse_mode = 1; token_value = 0x7FFFFFFF; cost_value=0x01; access_criteria_flag = 0 KV: Tslow = 0x00 00 04 00; Tshigh = 0x00 00 04 FF
Pass-Criteria	BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 1 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x02 ○ Cost_value= 0x01 ○ Purse_value=0x30 (purse value not changed)

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

Test Case Id	BCAST-1.1-DIST-int-617
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Set of Playback counter associated with a SEK/PEK id, SPE=0x07 The playback counter created in this test will be used by subsequent tests for set mode, add mode and overflow. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013,BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-025, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-018
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases

Test Procedure	See preambule for managing purses and counters test cases LTKM fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0005 0001 (new key group) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0;add_flag=0, number_playback=3; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters o consumption_reporting_flag = 1 o Overflow_flag = 0 o Unsupported_extention_flag = 0 o Not_found_flag = 0 o Security_policy_extension = 0x07 o Add_flag=0 o Playback_counter=3

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

Test Case Id	BCAST-1.1-DIST-int-618
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for set mode for Playback counter associated with a SEK/PEK id, SPE=0x07 Set mode executed on a already created playback counter Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-025, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-018
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-617 passed successfully first

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0005 0001 (same Key as previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0;add_flag=0, number_playback=5; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x07 ○ Add_flag=0 ○ Playback_counter=5

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

Test Case Id	BCAST-1.1-DIST-int-619
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for add mode for Playback counter associated with a SEK/PEK id, SPE=0x07 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-025, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-018
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-618 passed successfully first

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0005 0001 (same Key as previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0;add_flag=1, number_playback=3; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x07 ○ Add_flag=1 ○ Playback_counter=8

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

Test Case Id	BCAST-1.1-DIST-int-620
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for overflow of Playback counter associated with a SEK/PEK id, SPE=0x07 Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-025, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-018
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preambule for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-619 passed successfully first

Test Procedure	See preambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0005 0001 (same Key as previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x07; purse_flag = 0;add_flag=1, number_playback=0x7F; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 1 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x07 ○ Add_flag=1 ○ Playback_counter=8

6.1.2.2.17 Set of TEK counter associated with a SEK/PEK id

Test Case Id	BCAST-1.1-DIST-int-621
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Set of TEK counter associated with a SEK/PEK id The TEK counter created in this test will be used by subsequent tests for set mode, add mode and overflow Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-029 AND BCAST-BSMSPCP-S-030 AND BCAST-BSMSPCP-S-032 AND BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022 OR BCAST-SCSPCP-C-023
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-023
ETR Reference	None
Tool	None
Test code	None

Preconditions	See preambule for managing purses and counters test cases Card shall support SPE=0x0C or 0x0D Below test is described with the assumption that the card supports SPE=0x0C.
Test Procedure	See preambule for managing purses and counters test cases **LTKM1 fields**: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0006 0001 (newKey_group) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x0C; purse_flag = 0; add_flag=0 ; keep_credit_flag=1 ; number_TEKs=5; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x0C ○ Add_flag= 0 ○ Keep_credit_flag = 1 ○ TEK_counter=5

6.1.2.2.18 Test of set mode for TEK counter associated with a SEK/PEK id

Test Case Id	BCAST-1.1-DIST-int-622
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for set mode for TEK counter associated with SEK/PEK id Set mode executed on a already created TEK counter Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D..
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-029 AND BCAST-BSMSPCP-S-030 AND BCAST-BSMSPCP-S-032 AND BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022 OR BCAST-SCSPCP-C-023
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-023

ETR Reference	None
Tool	None
Test code	None
Preconditions	See preamble for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-621 passed successfully first Card shall support SPE=0x0C or 0x0D Below test is described with the assumption that the card supports SPE=0x0C.
Test Procedure	See preamble for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0006 0001 (same Key_group as the previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x0C; purse_flag = 0; add_flag=0 ; keep_credit_flag=1 ; number_TEKs=10 ; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x0C ○ Add_flag= 0 ○ Keep_credit_flag = 1 ○ TEK_counter=10

6.1.2.2.19 Test of add mode for TEK counter associated with SEK/PEK id

Test Case Id	BCAST-1.1-DIST-int-623
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test for add mode for TEK counter associated with SEK/PEK id Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D..
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-029 AND BCAST-BSMSPCP-S-030 AND BCAST-BSMSPCP-S-032 AND BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022 OR BCAST-SCSPCP-C-

SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029,BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029,BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-023
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preamble for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-622 passed successfully first Card shall support SPE=0x0C or 0x0D Below test is described with the assumption that the card supports SPE=0x0C.
Test Procedure	See preamble for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0006 0001 (same Key_group as the previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x0C; purse_flag = 0; add_flag=1 ; keep_credit_flag=1 ; number_TEKs=10; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM receives the Verification Message for the LTKM1 delivery BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 0 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x0C ○ Add_flag= 1 ○ Keep_credit_flag = 1 ○ TEK_counter=20

6.1.2.2.20 Test of overflow for TEK counterassociated with SEK/PEK id

Test Case Id	BCAST-1.1-DIST-int-624
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test of overflow for TEK counterassociated with SEK/PEK id Smartcard is BCAST and shall support SPE=0x0C or SPE=0x0D..
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7, 6.6.8

SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-029 AND BCAST-BSMSPCP-S-030 AND BCAST-BSMSPCP-S-032 AND BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022 OR BCAST-SCSPCP-C-
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-022
SCR Reference II	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-030, BCAST-BSMSPCP-S-032, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-023
ETR Reference	None
Tool	None
Test code	None
Preconditions	See preamble for managing purses and counters test cases Additionally, test BCAST-1.1-DIST-int-623 passed successfully first Card shall support SPE=0x0C or 0x0D Below test is described with the assumption that the card supports SPE=0x0C.
Test Procedure	See preamble for managing purses and counters test cases LTKM fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0006 0001 (same Key_group as the previous message) V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x0C; purse_flag = 0; add_flag=1 ; keep_credit_flag=1 ; number_TEKs=0x3FFFFF; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM does not receive a Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters ○ consumption_reporting_flag = 1 ○ Overflow_flag = 1 ○ Unsupported_extention_flag = 0 ○ Not_found_flag = 0 ○ Security_policy_extension = 0x0C ○ Add_flag= 1 ○ Keep_credit_flag = 1 ○ TEK_counter=20

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

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

Key group part	Key number part	Security policy	Cost-value	live_ppt _purse	Playback _ppt_purse	User _purse	Play-back counter	TEK counter

0002	0001	0x00	0x00	0x20				
0002	0001	0x00	0x01	0x20				
0002	0002	0x00	0x02	0x20				
0003	0001	0x01	0x01		0x30			
0003	0002	0x01	0x01		0x30			
0003	0002	0x01	0x01		0x30			
0004	0001	0x02	0x01			0x30		
0004	0001	0x02	0x01			0x30		
0004	0002	0x02	0x01			0x30		
0005	0001	0x07					0x08	
0006	0001	0x0C						0x20

6.1.2.3 SPE value not supported by the card

Test Case Id	BCAST-1.1-DIST-int-625
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Send an LTKM with SPE extention, but the value is not supported by the card Smartcard is BCAST.
Specification Reference	SPCP spec: 6.6.4, 6.6.6, 6.6.7
SCR Reference	BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-018 AND BCAST-BSMSPCP-S-029 AND BCAST-BSMSPCP-S-032 AND BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-008 AND NOT BCAST-SCSPCP-C-
SCR Reference I	• BCAST-LTKM_SC-C-015, BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-018; BCAST-BSMSPCP-S-029; BCAST-BSMSPCP-S-032; BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-008; **NOT BCAST-SCSPCP-C-022**
ETR Reference	None
Tool	None
Test code	None
Preconditions	Seepreambule for managing purses and counters test cases Card does not support all SPE Below test is described with the assumption that the card does not support SPE=0x0C. In this case the BCAST-SCSPCP-C-022 shall not be supported by the smartcard. If the card does not support other SPE, the test shall be adapted accordingly.

Test Procedure	Seepreambule for managing purses and counters test cases LTKM1 fields: Key domain ID= MCC1 || MNC1 SEK/PEK ID = 0006 0001 V bit = 1; EXT BCAST present with security_policy_extension_flag = 1, security_policy_extension =0x0C; purse_flag = 0; add_flag=0 ; keep_credit_flag=1 ; number_TEKs=0x05; access_criteria_flag = 0 KV: Tslow = 0x00 00 01 00; Tshigh = 0x00 00 01 FF
Pass-Criteria	BSM does not receive a LTKM Verification Message for the LTKM1 delivery, but instead BSM receives the LTKM Reporting Message with following parameters o consumption_reporting_flag = 0 o Overflow_flag = 0 o Unsupported_extention_flag = 1 o Not_found_flag = 0

6.1.3 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.

6.1.3.1 Correct STKM parsing by a BCAST Smartcard

Test Case Id	BCAST-1.1-DIST-int-430
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Test that the Smartcard correctly parses STKMs Smartcard is BCAST
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.3
SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-SCSPCP-C-007
ETR Reference	SCPS-003, SCPS-009
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	○ Smartcard has valid LTKM allowing the Smartcard to verify the STKM ○ BSM sends an LTKM for the service: ○ Key domainID= MCC1|| MNC1 ○ SEK/PEK ID = 0003 0001 ○ with a security_policy_extension = 0x04 ○ KV: Tslow= 0x00 00 00; Tshigh= 0x00 00 00 0F 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 Smartcard is BCAST
Test Procedure	1. BSM / BSDA generates STKMs for the service 03 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. TS starts with 0x00 00 00 01 and TEK_ID with 0x00 01. 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	Video is displayed by the terminal during 20 s Terminal forwards only the first STKM received every cryptoperiod, Terminal does not forward resent STKM (=STKM with same TEK ID) to the smartcard If the video is displayed during 15*10=150s, this means that TEK ID field is used for the checking of KV of SEK/PEK, instead of TS, as required by BCAST. This is an error. On the spy; Only one AUTHENTICATE command is sent to the card every cryptoperiod (10s). Smartcard returns decrypted material.

6.1.3.2 Correct STKM parsing by Smartcard (MBMS)

Test Case Id	BCAST-1.1-DIST-int-431
Test Object	BCAST Terminal / Smartcard/ Server.Smartcard is MBMSonly
Test Case Description	Test that the Smartcard correctly parses STKMs
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.3

SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-SCSPCP-C-006
ETR Reference	SCPS-003, SCPS-009
Tool	Spy of the terminal/Smartcard interface
Test code	None
Preconditions	o Smartcard has valid LTKM allowing the Smartcard to verify the STKM o BSM sends an LTKM for the service with o security_policy_extension: flag=0 and consumption_reporting_flag=0 : o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0004 0001 o KV: SEQl= 0x00 00; SEQu = 0x00 0F (KV coding TEK ID interval) 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 150 s (2,50 mns). On the spy The response of the AUTHENTICATE command in MTK generation mode, containing decrypted key material, is conform to 3GPP TS 33,246

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

Test Case Id	BCAST-1.1-DIST-int-432
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test that an STKM cannot be processed by a smartcard that doesn’t store the correcponding SEK/PEK (wrong Key Domain ID) and that the TEK isn’t returned. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.3
SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-SCSPCP-C-009

ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None
Preconditions	The Bootstrapping exists, but **SEK/PEK** used doesn't exist. The BSM sends a STKM for the key domain ID = MCC2|| MNC2 and with a SEK/PEK ID key group = 0x0003 (wrong key domain ID) The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means
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

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

Test Case Id	BCAST-1.1-DIST-int-433
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test that an STKM cannot be processed by a smartcard that doesn't store the correcponding SEK/PEK (wrong Key Domain ID)and that the TEK isn't returned. Smartcard is BCAST.
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.3
SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-SCSPCP-C-009
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None
Preconditions	The Bootstrapping exists, but **SEK/PEK** used doesn't exist. The BSM sends a STKM for the key domain ID = MCC1|| MNC1 and with a SEK/PEK ID key group = 0x0010 (Wrong SEK/PEK ID) The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means
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

6.1.3.5 STKM processing, Key Validity data check

Test Case Id	BCAST-1.1-DIST-int-626
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	Key Validity data check. Test that an STKM cannot processed by the smartcard and the TEK isn’t returned when TS is lower that Tslow or higher than Tshigh.
Specification Reference	SPCP spec: 6.7; 6.7.2, 6.7.3, 6.7.3.5
SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-SCSPCP-C-007
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None
Preconditions	Smartcard has valid LTKM allowing the Smartcard to verify the STKM BSM sends an LTKM for the service: • Key domainID= MCC1‖ MNC1 • SEK/PEK ID = 0003 0001 • with a security_policy_extension = 0x04 • KV: Tslow= 0x00 00 00 01; Tshigh= 0x00 00 00 06 No other LTKM has been sent previously 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, with TS from 0x00 00 00 00 to 0x00 00 00 00 07 , and TS increase by one for each cryptoperiod (10s) • Terminal receives the message and sends it to the smartcard At reception of the2 first STKM with TS=0x00 00 00 00 and TS=0x00 00 00 01, Smartcard detects that the Key Validity daT check fails and returns the status code ‘9865’ (Key freshness failure) Terminal may display an error message and may ask the user to register to that service. In this case cancel the procedure to allow execution of next steps of the test. • From TS=0x00 00 00 02 to TS=0x00 00 00 06, Key Validity data check is successful, and smartcard returns decrypted material to terminal • Video is displayed during 50s • At reception of last STKM with TS=0x00 00 00 07, Smartcard detects that the Key Validitu data check fails and returns the status code ‘9865’ (Key freshness failure)
Pass-Criteria	No video is displayed during the first 20s Then video is displayed during 50s On the spy: For the 2 first AUTHENTICATE command, the status word returned by the smartcard is ‘9865’ (Key freshness failure) For the 3rd to 7th AUTHENTICATE command, the status word returned by the smartcard is 9000 and the key material is returned in the response. For the last AUTHENTICATE command, the status word returned by the smartcard is ‘9865’ (Key freshness failure)

6.1.3.6 Key deletion from server

This test is relative to the layer2 but the test procedure and pass criteria needs that the test 6.1.3.3 and 6.1.3.4 passed successfully first.

Test Case Id	BCAST-1.1-DIST-int-439
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard 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. SPE=0x0A is supported by the smartcard
Specification Reference	SPCP spec: 6.6
SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-028, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-021
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.1 passed successfully. The smartcard has the following valid SEK/PEK ○ Key domainID= MCC1|| MNC1 ○ SEK/PEK ID = 0003 0001 ○ with a security_policy_extension = 0x04 ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F ○ 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 0x00 00 00 05), BSM sends a LTKM for the same SEK/PEK ID but with a security policy extension equals to 0x0A, and KV: Tslow = Tshigh=0x00 00 00 00 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 6.1.3.3 and 6.1.3.4) 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 2,50 min. It is decrypted during 10*5=50s 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

6.1.3.7 SPE deletion from the server

This test is relative to the layer2 but the test procedure and pass criteria needs that the test 6.1.3.3 and 6.1.3.4 passed successfully first.

Test Case Id	BCAST-1.1-DIST-int-627
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	BSM / BSDA sends an LTKM with Tslow>Tshigh to delete data associated to the given SPE and SEK/PEK ID.
Specification Reference	SPCP spec: 6.6, 6.6.7.4
SCR Reference	BCAST-STKM_SC-C-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-SCSPCP-C-007
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.1 passed successfully. The smartcard has the following valid SEK/PEK • Key domainID= MCC1|| MNC1 • SEK/PEK ID = 0003 0001 • with a security_policy_extension = 0x04 • KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Key domainID= MCC1|| MNC1 • SEK/PEK ID = 0003 0001 • with a security_policy_extension = 0x05 • KV: Tslow= 0x00 00 01 00; Tshigh= 0x00 00 01 0F 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 0x00 00 00 05), BSM sends a LTKM for the same SEK/PEK ID, with a SPE=0x04, and KV: Tslow = 0x FF FF FF FF Tshigh=0x00 00 00 00 2. The terminal sends the LTKM to the smartcard 3. The smartcard detects that the LTKM is for a deletion of SPE 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 SPE=0x04 is not existent for this SEK/PEK ID, and Key validity check fails with SPE=0x05. 7. The smartcard doesn't generate the TEK and the status code is '9865' (Key freshness failure). 8. BSM sends a LTKM for the same SEK/PEK ID, with a SPE=0x05, and KV: Tslow =0x FF FF FF FF Tshigh=0x00 00 00 00 9. The terminal sends the LTKM to the smartcard 10. The smartcard detects that the LTKM is for a deletion of SPE, and delete the SEK/PEK as no other SPE are associated to this SEK/PEK ID 11. The terminal receives the next STKM for the decryption of video 12. The terminal sends the STKM to the smartcard 13. The smartcard detects that SEK/PEK is not existent for this SEK/PEK ID (see 6.1.3.3 and 6.1.3.4) 14. The smartcard doesn't generate the TEK and the status code is '6A88' (referenced data not found).

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

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

6.1.3.8.1 STKM processing when LTKM SPE=0x00; testing live_ppt_purse

Test Case Id	BCAST-1.1-DIST-int-628
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when LTKM SPE=0x00, with token decrease in live_ppt_purse
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
SCR Reference	BCAST-SPCP-C-005, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-020, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-013
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The 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. STKM replay detection counter in the card corresponding to this SEK/PEK ID is set to 0x00 00 00 00 A LTKM is sent by the BSM for the SEK/PEK: • Key domainID= MCC1|| MNC1 • SEK/PEK ID = 0003 0001 • With security-policy-extension = 0x00 • KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Token-value = 0x11 • Purse-mode = 0x00 (set mode) • Cost-value: 0x02

Test Procedure	1. Test of the service token PPT live (SPE=0x00) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 50s 2. checking live_ppt_purse value: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with purse_value=0x07 3. Test of STKM replay detection check: a. STKM are resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS 0x00 00 00 01 b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPE that allows replay content, but no SPE is corresponding (failure) e. no video is displayed during 10s. 4. Test of lack of credit in live_ppt_purse 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 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 30s (here Purse_value=0x01) e. Smartcard send back error message “lack of credit in live_ppt_purse”

Pass-Criteria	Video is displayed during 50s, then not displayed during 10s, and displayed during 30s. On the server side a Reporting Message is received with • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x00 • Cost_value= 0x02 • Purse_value=0x07 (value of live_ppt_purse) At the end, Terminal may display a message indicating lack of credit. On the spy: AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times) AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message, then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (3 times) then AUTHENTICATE (in MTK generation mode) command response with “BCAST management data status code” (tag80) equal to 0x01 (lack of credit in live_ppt_purse)

6.1.3.8.2 STKM processing when LTKM SPE=0x01; testing playback_ppt_purse

Test Case Id	BCAST-1.1-DIST-int-629
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when LTKM SPE=0x01, with token decrease in playback_ppt_purse
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
SCR Reference	BCAST-SPCP-C-005, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-021, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-014
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means Previous test BCAST-1.1-DIST-int-628 is passed successfully, STKM replay detection counter in the card corresponding to SEK/PEK ID = 0003 0001 is set to 0x00 00 00 08 A LTKM is sent by the BSM for the SEK/PEK: Key domainID= MCC1|| MNC1 SEK/PEK ID = 0003 0001 With security-policy-extension = 0x01 KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F Token-value = 0x11 Purse-mode = 0x00 (set mode) Cost-value = 0x02

Test Procedure	1. Test of playback ppt mode a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 00 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPE=0x01 (success) e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 50s 2. Checking playback_ppt_purse value: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID =0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x01 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting message with purse_value=0x07 3. Test of STKM replay detection check 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 receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard perform Key Validity check for SPE that allows live content, but no SPE is corresponding (failure) e. no video is displayed during 10s 4. Test of lack of credit in playback_ppt_purse: a. After a cryptoperiod, STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 04 and TS increasing by one for each crypto-period (10 s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPE=0x01 (success) e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 30 s (here purse value becomes 0x01) g. Smartcard send back error message' lack of credit in playback_ppt_purse'

Pass-Criteria	Video is displayed during 50s, then not displayed during 10s, and then displayed during 30s On the server side, a Reporting Message is received with is received with • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x01 • Cost_value= 0x02 • Purse_value=0x07 (value of playback_ppt_purse) At the end, a message is displayed on the handset indicating lack of credit. On the spy: AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times) AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message then AUTHENTICATE (in MTK generation mode) command response with SW=9865 (key freshness failure) then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (3 times) then AUTHENTICATE (in MTK generation mode) command response with "BCAST management data status code" (tag80) equal to 0x02 (lack of credit in playback_ppt_purse)

6.1.3.8.3 STKM processing when LTKM SPE=0x02; testing user_purse

Test Case Id	BCAST-1.1-DIST-int-630
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when LTKM SPE=0x02, with decrease of user_purse token
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
SCR Reference	BCAST-SPCP-C-005, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-022, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-015
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001. STKM replay counter in the card corresponding this SEK/PEK is set to 0x00 00 00 00. • A LTKM is sent by the BSM for the SEK/PEK: • Key domainID= MCC1|| MNC1 • SEK/PEK ID = 0003 0001 • With security-policy-extension = 0x02 • KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Token-value= 0x11 • Purse-mode= 0x00 (set mode) • Cost-value= 0x02
Test Procedure	1. Test of the user token ppt live a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 50s 2. checking user_purse value: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with purse_value=0x07 3. test of lack of credit in user_purse a. STKM are sent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 06 to 0x00 00 00 09 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 30s (here Purse_value=0x01) e. Smartcard send back error message “lack of credit in user_purse”

Pass-Criteria	Video is displayed during 50s + 30s On the server side, a Reporting Message is received with is received with • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x02 • Cost_value= 0x02 • Purse_value=0x07 (value of user_purse) At the end, a message may be displayed on the handset indicating lack of credit. On the spy: AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times) AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message, then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (3 times) then AUTHENTICATE (in MTK generation mode) command response with "BCAST management data status code" (tag80) equal to 0x04 (lack of credit in the user_purse)

6.1.3.8.4 STKM processing when LTKM SPE=0x07; testing playback_counter

Test Case Id	BCAST-1.1-DIST-int-631
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when LTKM SPE=0x07, with decrease of playback_counter
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
SCR Reference	BCAST-SPCP-C-005, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-025, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-018
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means BCAST-1.1-DIST-int-630 is passed successfully, STKM replay detection counter in the card corresponding to SEK/PEK ID = 0003 0001 is set to 0x00 00 00 08 A LTKM is sent by the BSM for the SEK/PEK: • Key domainID= MCC1‖ MNC1 • SEK/PEK ID = 0003 0001 • With security-policy-extension = 0x07 • KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Purse_flag= 0 • add_flag = 0x00 (set mode) • number_playback = 0x05 Current_TS_counter is set automatically in the card with 0x00 00 00 0F. (=Tshigh)

Test Procedure	1. Test of playback PPP mode a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS set to 0x00 00 00 01 o Video data sent during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPE=0x07 (success) e. Smartcard perform current_TS_counter check, and STKM TS is lower. o Current_TS_counter is set to STKM TS value=0x00 00 00 01 o Playback_counter is decreased f. Smartcard decrypts the TEK and sends them to the terminal g. Video is then displayed during 10 s h. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS set to 0x00 00 00 02 o Video data sent during 10s i. Terminal receives the messages and sends them to the smartcard j. Smartcard perform STKM replay detection check against TS (failure) k. Smartcard perform Key Validity check for SPE=0x07 (success) l. Smartcard perform current_TS_counter check, and STKM TS is greater. o Current_TS_counter is set to STKM TS value=0x00 00 00 02 o Playback_counter is NOT decreased m. Smartcard decrypts the TEK and sends them to the terminal n. Video is then displayed during 10 s 2. checking playback_counter value: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x07 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting value with playback_counter=0x04 3. Test of STKM replay detection check a. STKM are resent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS 0x00 00 00 10 b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard perform Key Validity check for SPE that allows live content, but no SPE is corresponding (failure)

Test Procedure (continued)	4. Test of lack of credit in playback_counter a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS set to 0x00 00 00 01. ○ For each crypto-period (10 s), TEK_ID increase by 1 but TS value is the same. Video data sent during 60s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPE=0x07 (success) e. Smartcard decrypts the TEK and sends them to the terminal f. Smartcard perform current_TS_counter check, and STKM TS is equal or lower. ○ Playback_counter is decreased g. Video is then displayed during 40 s (here playback_counter becomes 0x00) h. Smartcard send back error message 'playback counter invalid or equal to zero'
Pass-Criteria	Video is displayed during 20s, then not displayed during 10s, and then displayed during 40s On the server side, a Reporting Message is received with • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x07 • Add_flag= 0x00 • Playback_counter=0x04 If returned Playback_counter is equal to 0x03 after 20s streaming, this means playback_counter has been decreased despite TS sent was greater than current_TS_counter. This is an error. After 70sec, a message may be displayed on the handset indicating playback_counter equal to zero. On the spy: AUTHENTICATE (in MTK generation mode) command response contains decrypted material (2 times) AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message, then AUTHENTICATE (in MTK generation mode) command response with error SW then AUTHENTICATE (in MTK generation mode) command response contains decrypted material (4 times) then AUTHENTICATE (in MTK generation mode) command response with "BCAST management data status code" (tag80) equal to 0x05 (playback_counter invalid or equal to zero)

6.1.3.8.5 STKM processing when LTKM SPE=0x0C; testing TEK counter

Test Case Id	BCAST-1.1-DIST-int-632
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when LTKM SPE=0x0C, with decrease of TEK counter
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.6, 6.7.3.10
SCR Reference	BCAST-SPCP-C-005, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-029, BCAST-BSMSPCP-S-033, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-022
ETR Reference	None
Tool	Spy of the terminal/Smartcard interface
Test code	None
Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001. STKM replay conter in the card is set to 0x00 00 00 00 A LTKM is sent by the BSM for the SEK/PEK ID = 0003 0001 • SPE = 0x0C • KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Purse_flag= 0 • Add_flag = 0 • Keep_credit_flag = 1 • Number_TEK= 0x08 A LTKM is sent by the BSM for the SEK/PEK ID = 0003 0002 • SPE = 0x0C • KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Purse_flag= 0 • Add_flag = 0 • Keep_credit_flag = 0 • Number_TEK= 0x05

Test Procedure	1. Test of the Pay per time Live a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 05 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 50s 2. checking TEK counter: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with TEK_counter=0x00 00 00 03 d. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0002, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C e. The terminal receives the LTKM and sends it to the smartcard f. The smartcard sends back a LTKM Reporting Message with TEK_counter=0x00 00 00 05 3. testing reporting of TEK over different SEK/PEK with same key group part a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0002 with TS from 0x00 00 00 01 b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Kept TEK counter value (0x00 00 00 03) shall be added to the TEK counter e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 10s g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0002, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with TEK_counter=0x00 00 00 07 4. test of lack of credit in TEK counter a. STKM are sent by the BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0002 with TS from 0x00 00 00 02 to 0x00 00 00 0F 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 70s (here TEK_counter=0x00) e. Smartcard send back error message “lack of credit in TEK counter”

Pass-Criteria	Video is displayed during 50s + 10s + 70s After 130sec (2min10s), a message may be displayed on the handset indicating lack of credit. On the server side, a Reporting Message is received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0C • Add_flag= 0x00 • Keep_credit_flag=0x01 • TEK_counter=0x00 00 00 03 LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0C • Add_flag= 0x00 • Keep_credit_flag=0x01 • TEK_counter=0x00 00 00 05 LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0C • Add_flag= 0x00 • Keep_credit_flag=0x01 • TEK_counter=0x00 00 00 07 On the spy: AUTHENTICATE (in MTK generation mode) command response contains decrypted material (5 times) AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message with TEK counter value (2 times), AUTHENTICATE (in MTK generation mode) command response contains decrypted material (1 times) AUTHENTICATE command (in MSK update mode) response contains the LTKM reporting message with TEK counter value (1 times), then AUTHENTICATE command response contains decrypted material (7 times) then AUTHENTICATE command response with “BCAST management data status code” (tag80) equal to 0x03 (lack of credit in the TEK counter)

6.1.3.9 STKM processing by priority order

6.1.3.9.1 Testing SPE priorities : live content with subscription

Test Case Id	BCAST-1.1-DIST-int-633
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when several SPE allowing live content are available. Test that STKM are processed by LTKM SPE priority order. Subscrption valid (SPE=0x04) case
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
SCR Reference	BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013 AND BCAST-BSDASPCP-S-014 AND BCAST-BSDASPCP-S-016 AND BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 AND BCAST-BSMSPCP-S-035 AND BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-019 AND (BCAST-BSMSPCP-S-020 OR BCAST-BSMSPCP-S-022 OR BCAST-BSMSPCP-S-026 OR BCAST-BSMSPCP-S-029) ; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-013 OR BCAST-SCSPCP-C-015 OR BCAST-SCSPCP-C-019 OR BCAST-SCSPCP-C-022;
SCR Reference I	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 ; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-020 ; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-013
SCR Reference II	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 ; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-022 ; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-015
SCR Reference III	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 ; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-026 ; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-019
SCR Reference IV	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 ; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-029 ; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-022
ETR Reference	None
Tool	None
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001. STKM replay detection counter in the card is set to 0x00 00 00 00 Smartcard shall support SPE=0x04, 0x08, 0x0C, 0x00 and 0x02. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly. Following LTKM are sent by the BSM, • SPE=0x04 (subscription) • SPE=0x08 (user token PPV) ○ Token-value: 0x03 (user_purse for SPE=0x08) ○ Purse-mode : 0x00 (set mode) ○ Cost-value: 0x01 • SPE=0x0C (PPT) ○ Purse_flag=0 ○ Add_flag=0 ○ Keep_credit_flag=1 ○ Number_TEKs=0x03 • SPE=0x00 (service token PPT) ○ Token-value: 0x03 (live_ppt_purse) ○ Purse-mode : 0x00 (set mode) ○ Cost-value: 0x01 • SPE=0x02 (user token PPT) ○ Token-value: 0x03 (user_purse for SPE=0x02) ○ Purse-mode : 0x00 (set mode) ○ Cost-value: 0x01 • Common to all SPE : ○ Key domainID= MCC1|| MNC1 ○ SEK/PEK ID = 0003 0001, ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 01 00

Test Procedure	1. Test of subscription mode (SPE=0x04) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 10 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 160s 2. checking purse/counter values a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with purse value=3 d. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C e. The terminal receives the LTKM and sends it to the smartcard f. The smartcard sends back a LTKM Reporting Message with TEK_counter=3 g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00 h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with live_ppt_purse=3 j. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02 k. The terminal receives the LTKM and sends it to the smartcard l. The smartcard sends back a LTKM Reporting Message with purse value=3

Pass-Criteria	Video is displayed during 160s =2.5min On the server side, Reporting Message are received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x08 • Cost_value= 0x01 • Purse_value=0x03 (value of user_purse) LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0C • Add_flag= 0x00 • Keep_credit_flag =0x01 • TEK_counter=0x03 LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x00 • Cost_value= 0x01 • Purse_value=0x03 (value of live_ppt_purse) LTKM Reporting Message 4: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x02 • Cost_value= 0x01 • Purse_value=0x03 (value of user_purse) ○ If one of above purse/counter is decreased, this is an error since subscription mode (SPE=0x04) shall have highest priority among all SPE allowing live content consumption.

6.1.3.9.2 Testing SPE priorities: live content without subscription

Test Case Id	BCAST-1.1-DIST-int-634
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when several SPE allowing live content are available. Test that STKM are processed by LTKM SPE priority order. No subscription (SPE=0x04)
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
SCR Reference	BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013 AND BCAST-BSDASPCP-S-014 AND BCAST-BSDASPCP-S-016 AND BCAST-BSDASPCP-S-039 AND BCAST-BSMSPCP-S-034 AND BCAST-BSMSPCP-S-035 AND BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-019 AND (BCAST-BSMSPCP-S-020 OR BCAST-BSMSPCP-S-022 OR BCAST-BSMSPCP-S-026 OR BCAST-BSMSPCP-S-029) AND BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-013 OR BCAST-SCSPCP-C-015 OR BCAST-SCSPCP-C-019 OR BCAST-SCSPCP-C-022;
SCR Reference I	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-020; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-013
SCR Reference II	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-022; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-015
SCR Reference III	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-026; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-019
SCR Reference IV	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-019; BCAST-BSMSPCP-S-029; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-022
ETR Reference	None
Tool	None
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001. STKM replay detection counter in the smartcard is set to 0x00 00 00 00 Smartcard shall support SPE=0x08, 0x0C, 0x00 and 0x02. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly. Following LTKM are sent by the BSM, • SPE=0x08 (user token PPV) ○ Token-value: 0x03 (user_purse for SPE=0x08) ○ Purse-mode : 0x00 (set mode) ○ Cost-value: 0x01 ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 03 • SPE=0x0C (PPT) ○ Purse_flag=0 ○ Add_flag=0 ○ Keep_credit_flag=1 ○ Number_TEKs=0x03 ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 06 • SPE=0x00 (service token PPT) ○ Token-value: 0x03 (live_ppt_purse) ○ Purse-mode : 0x00 (set mode) ○ Cost-value: 0x01 ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 09 • SPE=0x02 (user token PPT) ○ Token-value: 0x03 (user_purse for SPE=0x02) ○ Purse-mode : 0x01 (add mode) ○ Cost-value: 0x01 ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0C • Common to all SPE : ○ Key domainID= MCC1|| MNC1 ○ SEK/PEK ID = 0003 0001

Test Procedure	1. Test of user token PPV mode (SPE=0x08) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is displayed for 30s f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08 g. The terminal receives the LTKM and sends it to the smartcard h. The smartcard sends back a LTKM Reporting Message with purse value=3 2. Test of PPT live mode (SPE=0x0C) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is displayed for 30s f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0C g. The terminal receives the LTKM and sends it to the smartcard h. The smartcard sends back a LTKM Reporting Message with TEK_counter=0 3. Test of service token PPT mode (SPE=0x00) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 07 to 0x00 00 00 09 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is displayed for 30s f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00 g. The terminal receives the LTKM and sends it to the smartcard e. The smartcard sends back a LTKM Reporting Message with live_ppt_purse=0

Procedure **(continued)**	4. Test of user token PPT mode (SPE=0x02) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 0A to 0x00 00 00 0F and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is displayed for 30s f. Smartcard send back error message (because all purse are out of credit) g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02 h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with user_purse=0

Pass-Criteria	Video is displayed during 30s+30s+30s+30s =2min After 2min, a message is displayed on the handset indicating lack of credit. On the server side, Reporting Message are received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x08 • Cost_value= 0x01 • Purse_value=0x03 (value of user_purse) LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0C • Add_flag= 0x00 • Keep_credit_flag =0x01 • TEK_counter=0x00 LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x00 • Cost_value= 0x01 • Purse_value=0x00 (value of live_ppt_purse) LTKM Reporting Message 4: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x02 • Cost_value= 0x01 • Purse_value=0x00 (value of user_purse) If one of above purse/counter value is not equal to 0, this means another purse/counter has been decreased instead, this is an error.

6.1.3.9.3 Testing SPE priorities : playback modes including SPE=0x05

Test Case Id	BCAST-1.1-DIST-int-635

Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when several SPE allowing playback are available. Test that STKM are processed by LTKM SPE priority order. Unlimited playback (SPE=0x05) case
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
SCR Reference	BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013 AND BCAST-BSDASPCP-S-014 AND BCAST-BSDASPCP-S-016 AND BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 AND BCAST-BSMSPCP-S-035 AND BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-024 AND (BCAST-BSMSPCP-S-025 OR BCAST-BSMSPCP-S-027 OR BCAST-BSMSPCP-S-030 OR BCAST-BSMSPCP-S-021 OR BCAST-BSMSPCP-S-023) AND BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-017 AND (BCAST-SCSPCP-C-014 OR BCAST-SCSPCP-C-016 OR BCAST-SCSPCP-C-018 OR BCAST-SCSPCP-C-020 OR BCAST-SCSPCP-C-023);
SCR Reference I	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-024; BCAST-BSMSPCP-S-021; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-017; BCAST-SCSPCP-C-014;
SCR Reference II	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-024; BCAST-BSMSPCP-S-023; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-017; BCAST-SCSPCP-C-016;
SCR Reference III	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-024; BCAST-BSMSPCP-S-025; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-017; BCAST-SCSPCP-C-018;
SCR Reference IV	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-024; BCAST-BSMSPCP-S-027; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-017; BCAST-SCSPCP-C-020;
SCR Reference V	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-024; BCAST-BSMSPCP-S-030; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-017; BCAST-SCSPCP-C-023;
ETR Reference	None
Tool	None
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means. The preceding test BCAST-1.1-DIST-int-634 passed successfully. STKM replay conter in the card is set to 0x00 00 00 0F and Current_TS_counter is set to 0x00 00 00 06. (Tshigh) Smartcard shall support SPE=0x05, 0x07, 0x09, 0x0D, 0x01 and 0x03. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly. Following LTKM are sent by the BSM, • SPE=0x05 (unlimited playback) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • SPE=0x07 (PPP playback) o Purse_flag=0 o Add_flag =0 o Number_playback=2 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 03 • SPE=0x09 (user token PPP playback) o Purse_flag=1 o Cost_value=1 o Purse_mode=0 (set mode) o Token_value : 0x02 (user purse for SPE=0x09) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 06 • SPE=0x0D (PPT playback) o Purse_flag=0 o Add_flag=0 o Number_TEKs=0x02 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 09 • SPE=0x01 (service token PPT playback) o Purse_flag=1 o Cost_value=1 o Purse_mode=0 (set mode) o Token_value : 0x02 (playback ppt_purse) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0C • SPE=0x03 (user token PPT playback) o Purse_flag=1 o Cost_value=1 o Purse_mode=1 (add mode) o Token_value : 0x02 (user purse for SPE=0x03) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Common to all SPE : o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001

Test Procedure	1. Test of unlimited playback mode (SPE=0x05) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 01 01 during 10s and then with TS=0x00 00 01 02 during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard returns an error, as there is no SPE allowing live content rendering e. Error message appear on the screen, Video is not displayed f. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 01 during 10s and then with TS=0x00 00 00 02 during 10s g. Terminal receives the messages and sends them to the smartcard h. Smartcard perform STKM replay detection check against TS (failure) i. Smartcard returuns decrypted material to terminal j. Video is displayed during 20s k. Repeat step f to j 10 times. Video is displayed 200s (3min20s) 2. checking purse/counter values a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x07 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with playback_counter=2 d. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x09 e. The terminal receives the LTKM and sends it to the smartcard f. The smartcard sends back a LTKM Reporting Message with purse value=4 g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0D h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with TEK_counter=2 j. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x01 k. The terminal receives the LTKM and sends it to the smartcard l. The smartcard sends back a LTKM Reporting Message with playback_ppt_purse=2 m. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x03 n. The terminal receives the LTKM and sends it to the smartcard o. The smartcard sends back a LTKM Reporting Message with purse value=4

Pass-Criteria	During first 20s, no video is displayed and an error message appears. Then the same 20sec video sequence is displayed 11 times, total display time is 220s=3min40s On the server side, Reporting Message are received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x07 • playback_counter=0x02 LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x09 • Cost_value= 0x01 • Purse_value=0x04 (value of user_purse) LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0D • Add_flag= 0x00 • TEK_counter=0x02 LTKM Reporting Message 4: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x01 • Cost_value= 0x01 • Purse_value=0x02 (value of playback_ppt_purse)

Pass-Criteria (continued)	LTKM Reporting Message 5: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x03 • Cost_value= 0x01 • Purse_value=0x04 (value of user_purse) If one of above purse/counter is decreased, this is an error since unlimited playback mode (SPE=0x05) has highest priority among all SPE allowing playback.

6.1.3.9.4 Testing SPE priorities: playback modes without SPE=0x05

Test Case Id	BCAST-1.1-DIST-int-636
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when several SPE allowing playback are available. Test that STKM are processed by LTKM SPE priority order. No unlimited playback (SPE=0x05) case
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
SCR Reference	BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013 AND BCAST-BSDASPCP-S-014 AND BCAST-BSDASPCP-S-016 AND BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 AND BCAST-BSMSPCP-S-035 AND BCAST-BSMSPCP-S-013 AND (BCAST-BSMSPCP-S-025 OR BCAST-BSMSPCP-S-027 OR BCAST-BSMSPCP-S-030 OR BCAST-BSMSPCP-S-021 OR BCAST-BSMSPCP-S-023) AND BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-014 OR BCAST-SCSPCP-C-016 OR BCAST-SCSPCP-C-018 OR BCAST-SCSPCP-C-020 OR BCAST-SCSPCP-C-023;
SCR Reference I	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-021; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-014
SCR Reference II	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-023; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-016
SCR Reference III	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-025; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-018
SCR Reference IV	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-027; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-020
SCR Reference V	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-030; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-023

ETR Reference	None
Tool	None
Test code	None
Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001. STKM replay conter in the card is set to 0x00 00 00 00. Smartcard shall support SPE=0x04, 0x07, 0x09, 0x0D, 0x01 and 0x03. If smartcard supports only a subset of these SPEs, the test shall be adapted accordingly. Following LTKM are sent by the BSM, • SPE=0x04 (subscription live) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 01 00 • SPE=0x07 (PPP playback) o Purse_flag=0 o Add_flag =0 o Number_playback=2 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 03 • SPE=0x09 (user token PPP playback) o Purse_flag=1 o Cost_value=1 o Purse_mode=0 (set mode) o Token_value : 0x02 (user purse for SPE=0x09) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 06 • SPE=0x0D (PPT playback) o Purse_flag=0 o Add_flag=0 o Number_TEKs=0x04 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 09 • SPE=0x01 (service token PPT playback) o Purse_flag=1 o Cost_value=1 o Purse_mode=0 (set mode) o Token_value : 0x04 (playback ppt_purse) o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0C • SPE=0x03 (user token PPT playback) o Purse_flag=1 o Cost_value=1

	○ Purse_mode=1 (add mode) ○ Token_value : 0x04 (user purse for SPE=0x03) ○ KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 0F • Common to all SPE : ○ Key domainID= MCC1|| MNC1 ○ SEK/PEK ID = 0003 0001, Current_TS_counter is set to 0x00 00 01 00.

Test Procedure	1. test preparation : setting STKM replay counter a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 10 during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. SPE=0x04 allows live content access. STKMreplay detection counter is set to TS=0x00 00 00 10 e. Smartcard decrypt the TEK and sends them to terminal f. Video is displayed during 10s 2. Test of playback PPP mode (SPE=0x07) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 01 during 10s and then with TS=0x00 00 00 02 during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPEs allowing playback (success) e. Smartcard returuns decrypted material to terminal f. Video is displayed during 20s g. Repeat step a to e. Video is displayed another 20s h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x07 i. The terminal receives the LTKM and sends it to the smartcard j. The smartcard sends back a LTKM Reporting Message with playback_counter=0 3. Test of user token PPP playback mode (SPE=0x09) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 04 during 10s and then with TS=0x00 00 00 05 during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPEs allowing playback (success) e. Smartcard returuns decrypted material to terminal f. Video is displayed during 20s g. Repeat step a to e. Video is displayed another 20s h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x09 i. The terminal receives the LTKM and sends it to the smartcard j. The smartcard sends back a LTKM Reporting Message with purse value=2

Test Procedrue (continued)	4. Test of PPT playback mode (SPE=0x0D) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 07 during 10s and then with TS=0x00 00 00 08 during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPEs allowing playback (success) e. Smartcard returuns decrypted material to terminal f. Video is displayed during 20s g. Repeat step a to e. Video is displayed another 20s h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x0D i. The terminal receives the LTKM and sends it to the smartcard j. The smartcard sends back a LTKM Reporting Message with TEK_counter =0 5. Test of service token PPT playback mode (SPE=0x01) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 0A during 10s and then with TS=0x00 00 00 0B during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPEs allowing playback (success) e. Smartcard returuns decrypted material to terminal f. Video is displayed during 20s g. Repeat step a to e. Video is displayed another 20s h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x01 i. The terminal receives the LTKM and sends it to the smartcard j. The smartcard sends back a LTKM Reporting Message with playback_ppt_purse =0 6. Test of user token PPT playback mode (SPE=0x03) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS=0x00 00 00 0D during 10s and then with TS=0x00 00 00 0E during 10s b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. Smartcard perform Key Validity check for SPEs allowing playback (success) e. Smartcard returuns decrypted material to terminal f. Video is displayed during 20s g. Repeat step a to e. Video is displayed another 20s

Test Procedrue (continued)	h. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x03 i. The terminal receives the LTKM and sends it to the smartcard j. The smartcard sends back a LTKM Reporting Message with purse value=0 k. Repeat step a to e. This time no video is displayed and an error message is displayed
Pass-Criteria	During first 10s, video is displayed (live content). Then the same 20sec video sequence is displayed 10 times, total display time is 200s=3min20s Finally, an error message is displayed indicating lack of credit in user purse. On the server side, Reporting Message are received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x07 • playback_counter=0x00 LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x09 • Cost_value= 0x01 • Purse_value=0x02 (value of user_purse) LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x0D • Add_flag= 0x00 • TEK_counter=0x00 LTKM Reporting Message 4: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x01 • Cost_value= 0x01 • Purse_value=0x00 (value of playback_ppt_purse)

Pass-Criteria (continued)	LTKM Reporting Message 5: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x03 • Cost_value= 0x01 • Purse_value=0x00 (value of user_purse) If one of above purse/counter is not equal to 0, this means another purse with lower priority has been decreased instead This is an error.

6.1.3.9.5 Testing KV priorities when several LTKM available with same SPE

Test Case Id	BCAST-1.1-DIST-int-637
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when several LTKM are available with same SPE. Testing that STKM are processed in KV priority order. Test with SPE=0x00 (service token PPT)
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6
SCR Reference	BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013 AND BCAST-BSDASPCP-S-014 AND BCAST-BSDASPCP-S-016 AND BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 AND BCAST-BSMSPCP-S-035 AND BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-020 OR BCAST-BSMSPCP-S-021 OR BCAST-BSMSPCP-S-022 OR BCAST-BSMSPCP-S-023 OR BCAST-BSMSPCP-S-026 OR BCAST-BSMSPCP-S-027 AND BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-013 OR BCAST-SCSPCP-C-014 OR BCAST-SCSPCP-C-015 OR BCAST-SCSPCP-C-016 OR BCAST-SCSPCP-C-019 OR BCAST-SCSPCP-C-020;
SCR Reference I	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-020; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-013
SCR Reference II	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-021; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-014
SCR Reference III	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-022; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-015
SCR Reference IV	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-023; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-016

SCR Reference V	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-026; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-019
SCR Reference VI	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-027; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-020
ETR Reference	None
Tool	None
Test code	None
Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 Smartcard shall support SPE=0x00. If SPE=0x00 is not supported, test can be adapted with other SPE value with purse. Following LTKM are sent by the BSM, • LTKM1 o Token-value: 0x00 00 03 00 (live_ppt_purse) o Purse-mode : 0x00 (set mode) o Cost-value: 0x01 00 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 03 • LTKM2 o Token-value: 0x00 00 00 30 (live_ppt_purse) o Purse-mode : 0x01 (add mode) o Cost-value: 0x00 10 o KV: Tslow= 0x00 00 00 02; Tshigh= 0x00 00 00 06 • LTKM3 o Token-value: 0x00 00 00 03 (live_ppt_purse) o Purse-mode : 0x01 (add mode) o Cost-value: 0x00 01 o KV: Tslow= 0x00 00 00 02; Tshigh= 0x00 00 00 09 • Common to all LTKM : o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001, o Security Policy Extension = 0x00 STKM replay conter in the card corresponding to SEK/PEK ID = 0003 0001 is set to 0x00 00 00 00

Test Procedure	1. chekcking live_ppt_purse value: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 03 33 2. Test that LTKM1 has first priority (lowest Tslow value) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 30s f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00 g. The terminal receives the LTKM and sends it to the smartcard h. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 33 3. Test that LTKM2 has second priority (same Tslow, lowest Tshigh value) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 30s f. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x00 g. The terminal receives the LTKM and sends it to the smartcard h. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 03 4. Test that switch to LTKM3 (lowest priority) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 07 to 0x00 00 00 09 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. Smartcard decrypts the TEK and sends them to the terminal e. Video is then displayed during 30s (here Purse_value=0x00) f. Smartcard send back error message “lack of credit in live_ppt_purse”

Pass-Criteria	Video is displayed during 30s+30s+30s=1min30s After 90sec, a message may be displayed on the handset indicating lack of credit. On the server side, a Reporting Message is received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x00 • Cost_value= 0x00 01 • Purse_value=0x00 00 03 33 (value of live_ppt_purse) LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x00 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 33 (value of live_ppt_purse) LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x00 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 03 (value of live_ppt_purse)

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

Test Case Id	BCAST-1.1-DIST-int-638
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	STKM processing when sent to different SPE sharing the same user purse. User purse common to SPE=0x02, 0x03, 0x08, 0x09. Card is BCAST
Specification Reference	SPCP spec: 6.7; 6.7.3, 6.7.3.5, 6.7.3.6

SCR Reference	BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013 AND BCAST-BSDASPCP-S-014 AND BCAST-BSDASPCP-S-016 AND BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034 AND BCAST-BSMSPCP-S-035 AND BCAST-BSMSPCP-S-013 AND BCAST-BSMSPCP-S-022 OR BCAST-BSMSPCP-S-023 OR BCAST-BSMSPCP-S-026 OR BCAST-BSMSPCP-S-027 AND BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007 AND BCAST-SCSPCP-C-015 OR BCAST-SCSPCP-C-016 OR BCAST-SCSPCP-C-019 OR BCAST-SCSPCP-C-020;
SCR Reference I	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-022; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-015
SCR Reference II	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-023; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-016
SCR Reference III	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-026; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-019
SCR Reference IV	• BCAST-SPCP-C-005; BCAST-BSDASPCP-S-013; BCAST-BSDASPCP-S-014; BCAST-BSDASPCP-S-016; BCAST-BSDASPCP-S-039; BCAST-BSMSPCP-S-034; BCAST-BSMSPCP-S-035; BCAST-BSMSPCP-S-013; BCAST-BSMSPCP-S-027; BCAST-BSMSPCP-S-033; BCAST-SCSPCP-C-007; BCAST-SCSPCP-C-020
ETR Reference	None
Tool	None
Test code	None

Preconditions	The server provides a valid SRTP and STKM stream to the device The terminal knows the IP address and port on which the STKM stream and SRTP stream are being broadcast, e.g. via pre-provisioned SDP or other means The test 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 Smartcard shall support SPE=0x02, 0x03, 0x08, 0x09. If one of these SPEs is not supported, test can be adapted accordingly. Following LTKM are sent by the BSM, • SPE=0x08 (user token PPV) o Token-value: 0x00 00 00 01 o Purse-mode : 0x01 (set mode) o Cost-value: 0x00 01 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 03 • SPE=0x09 (user token PPP playback) o Token-value: 0x00 00 00 01 o Purse-mode : 0x01 (add mode) o Cost-value: 0x00 01 o KV: Tslow= 0x00 00 00 00; Tshigh= 0x00 00 00 03 • SPE=0x02 (user token PPT) o Token-value: 0x00 00 00 03 o Purse-mode : 0x01 (add mode) o Cost-value: 0x00 01 o KV: Tslow= 0x00 00 00 03; Tshigh= 0x00 00 00 06 • SPE=0x03 (user token PPT playback) o Token-value: 0x00 00 00 03 o Purse-mode : 0x01 (add mode) o Cost-value: 0x00 01 o KV: Tslow= 0x00 00 00 03; Tshigh= 0x00 00 00 06 • Common to all LTKM : o Key domainID= MCC1|| MNC1 o SEK/PEK ID = 0003 0001,

Test Procedure	1. Checking user_purse value: a. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08 b. The terminal receives the LTKM and sends it to the smartcard c. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 08 2. Test SPE=0x08 (user token PPV) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. SPE=0x08 is an SPE allowing live content, and KV check pass. Smartcard decrease user_purse. e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 30s g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x08 h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 07 3. Test SPE=0x09 (user token PPP playback) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 01 to 0x00 00 00 03 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. SPE=0x09 is an SPE allowing playback content, and KV check pass. Smartcard decrease user_purse. e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 30s g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x09 h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 06

Test procedure (continued)	4. Test SPE=0x02 (user token PPT) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (success) d. SPE=0x02 is an SPE allowing live content, and KV check pass. Smartcard decrease user_purse at each crypto-period e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 30s g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x02 h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 03 5. Test SPE=0x03 (user token PPT playback) a. STKM are sent by BSDA for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 with TS from 0x00 00 00 04 to 0x00 00 00 06 and TS increasing by one for each crypto-period (10s) b. Terminal receives the messages and sends them to the smartcard c. Smartcard perform STKM replay detection check against TS (failure) d. SPE=0x03 is an SPE allowing playback content, and KV check pass. Smartcard decrease user_purse at each crypto-period. e. Smartcard decrypts the TEK and sends them to the terminal f. Video is then displayed during 30s g. The BSM sends a LTKM for the SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001, with V bit = 0, with the consumption_reporting_flag=1 and security_policy_extension=0x03 h. The terminal receives the LTKM and sends it to the smartcard i. The smartcard sends back a LTKM Reporting Message with purse_value=0x00 00 00 00

Pass-Criteria	Video is displayed during 30s+30s+30s+30s=2min On the server side, a Reporting Message is received with LTKM Reporting Message 1: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x08 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 08 LTKM Reporting Message 2: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x08 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 07 LTKM Reporting Message 3: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x09 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 06 LTKM Reporting Message 4: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x02 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 03 LTKM Reporting Message 5: • Consumption_reporting_flag=1 • Overflow_flag=0, Unsupported_extention_flag=0, not_found_flag=0 • Security_policy_extension = 0x03 • Cost_value= 0x00 01 • Purse_value=0x00 00 00 00

6.1.3.11 STKM reception with parental control without PIN defined in the card

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

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

0x04 : minimum age = 7 years old

0x07 : minimum age = 10 years old

0x09 : minimum age = 12 years old

0x0B : minimum age = 14 years old

0x0D : minimum age = 16 years old

0x0F : minimum age = 18 years old

As the example given in the specification SPCP

Test Case Id	BCAST-1.1-DIST-int-456
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value
Specification Reference	SPCP spec: 6.6.5, 6.7; 6.7.3.9.1
SCR Reference	BCAST-SPCP-C-005, BCAST-SC_ParentalControl-C-033, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-019, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-025
ETR Reference	None
Tool	None
Test code	None
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 6.1.3.6 passed successfully and then in the smartcard there is no key for SEK/PEK ID: Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001 No PINCODE is defined in the smartcard

Test Procedure	BSM sends a Parental Control Message with a setting of parental control in the card: Level_granted is 0x0B and rating-type 0x00 without PINCODE in KEMAC (Encr Data len =0) BSM sends a LTKM for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001; KV is set from Tslow= 0x00 FF 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 0x04 From TS = 0110 to TS = 011F: rating-value is 0x0F From TS = 0120 to TS= 012F : rating-value is 0x07 From TS = 0130 to TS= 013F : rating-value is 0x0d From TS = 0140 to TS= 014F : rating-value is 0x09 From TS = 0150 to TS= 015F : rating-value is 0x0B
Pass-Criteria	The video is displayed during 2,50 mns Video is not displayed during 2,50 mns and a message indicating that the user is not allowed to watch the program is displayed to the user The video is displayed during 2,50 mns Video is not displayed during 2,50 mns and a message indicating that the user is not allowed to watch the program is displayed to the user The video is displayed during 5,00 mns

6.1.3.12 STKM reception with parental control and with PIN defined in the card

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

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

0x04 : minimum age = 7 years old

0x07 : minimum age = 10 years old

0x09 : minimum age = 12 years old

0x0B : minimum age = 14 years old

0x0D : minimum age = 16 years old

0x0F : minimum age = 18 years old

Test Case Id	BCAST-1.1-DIST-int-457
Test Object	BCAST Terminal / Smartcard/ Server. Smartcard is BCAST
Test Case Description	BSM / BSDA sends several STKMs to the terminal / smartcard with different parental rating-value
Specification Reference	SPCP spec: 6.6.5, 6.7; 6.7.3.9.1

SCR Reference	BCAST-SPCP-C-005, BCAST-SC_ParentalControl-C-033, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-016, BCAST-BSDASPCP-S-039, BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-019, BCAST-SCSPCP-C-007, BCAST-SCSPCP-C-025, BCAST-SCSPCP-C-026
ETR Reference	None
Tool	None
Test code	None
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 6.1.3.6 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 Parental Control Message with a setting of parental control in the card: Level_granted is 0x0B and rating-type 0x00 with a PINCODE encrypted in the KEMAC (PINCODE = 020579 as example given in the SPCP TS specification) BSM sends a LTKM for the service Key domainID= MCC1|| MNC1; SEK/PEK ID = 0003 0001; KV is set from Tslow= 0x00 FF 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 0x04 From TS = 0110 to TS = 011F: rating_value is 0x0F From TS = 0120 to TS= 012F : rating_value is 0x07 From TS = 0130 to TS= 013F : rating_value is 0x0D From TS = 0140 to TS= 014F : rating_value is 0x09 From TS = 0150 to TS= 015F : rating_value is 0x0B
Pass-Criteria	1. The video is displayed during 2,50 mns 2. Then a message to the user is sent for the verification of PIN: verify PIN 3. Pin code is correctly entered (value of PINCODE 020579) and then 4. Video is displayed during 5 mns 5. Then a message to the user is sent for the verification of PIN: verify PIN 6. Pin code is correctly entered (value of PINCODE 020579) and then 7. Video is displayed during 7.50 mns

6.1.3.13 Multiple streams protected with same STKM stream

Test Case Id	BCAST-1.1-DIST-int-458
Test Object	BCAST Terminal / Smartcard/ 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-010, BCAST-BSDASPCP-S-013, BCAST-BSMSPCP-S-003, BCAST-SCSPCP-C-007
ETR Reference	None
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.

6.1.3.14 Multiple streams protected with different STKM streams

Test Case Id	BCAST-1.1-DIST-int-459
Test Object	BCAST Terminal / Smartcard/ 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-010, BCAST-BSDASPCP-S-013, AND BCAST-BSDASPCP-S-014, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-007
ETR Reference	None
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.

6.1.4 Layer 4: Traffic Encryption layer

6.1.4.1 Delivery of IPSec protected stream

Test Case Id	BCAST-1.1-DIST-int-460
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Opening an Ipsec encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST11–ServContProt] Section 9.1. [BCAST11–ServContProt] Section 6.8.1.
SCR Reference	BCAST-SPCP-C-001, BCAST-ContentLayer-C-008, BCAST-SDP-C-014, BCAST-TerminalCapability-C-003, BCAST-SPCP-C-005, BCAST-CP_RTP_SC-C-021, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-028, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-007
ETR Reference	None
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.

6.1.4.2 Delivery of SRTP protected stream

Test Case Id	BCAST-1.1-DIST-int-461
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Opening an SRTP encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST11–ServContProt] Section 9.2. [BCAST11–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-CP_RTP_SC-C-021, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-029, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-007
ETR Reference	SCPS-004, SCPS-005, SCPS-006, SPR-003, SCPS-010, SCPS-011, SCPS-012, SCPS-013, SCPS-014, SCPS-015, SCPS-016, SCPS-017, SCPS-018, SCPS-019, SCPS-020
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.

6.1.4.3 Delivery of ISMACrypt protected stream

Test Case Id	BCAST-1.1-DIST-int-462
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Opening an ISMACrypt encrypted stream with key material associated to the subscription.
Specification Reference	[BCAST11–ServContProt] Section 9.3. [BCAST11–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-CP_RTP_SC-C-021, BCAST-BSDASPCP-S-013, BCAST-BSDASPCP-S-014, BCAST-BSDASPCP-S-030, BCAST-BSMSPCP-S-008, BCAST-SCSPCP-C-007
ETR Reference	None
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.

6.2 Smartcard Broadcast Provisioning

6.2.1 Sending a file to a group of Smartcards through Smartcard Broadcast provisioning using ENVELOPE technology

Test Case Id	BCAST-1.1-SCBP-int-101
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test the Smartcard broadcast provisioning of a file requesting the Smartcard to issue a DISPLAY TEXT command, sent to a group of 256 Smartcards, using the ENVELOPE technology.
Specification Reference	Services 5.19
SCR Reference	BCAST-SERVICES-C-047, BCAST-SERVICES-BSA-003, BCAST-SERVICES-BSM-025
ETR Reference	SCBP-001, SCBP-002, SCBP-003, SCBP-004
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. Smartcard supports the Smartcard broadcast provisioning function: this is signaled in the EF_{BST} The Unique Smartcard Filter of the Smartcard is: 0x123456789A and this value is indicated in the EF_{USF} (group: 0x12345678, position in group: 0x9A) The Key used to receive the secured packets is Key1

Test Procedure	1. The Handset is power-on. 2. The server broadcasts a service guide signaling the availability of a service of type 13 “Smartcard Provisioning Services”. The access fragment of this service indicates: • Type of addressing: “0”; Group Size: ‘n’ = 8 (group size = 256 devices) • The whole group is addressed : only the <subscriberGroupBase> element is present in the <subscriberGroupIdentifier> element. The group base is: • 00010010001101000101011001111000 (12345678) = b64:‘EjRWeA==’ • The technology used is Envelope 3. The BSD/A broadcast a file using Flute. This file contains Command packet encapsulated in secure packet. The key used is Key1. The Command sent requests the smartcard to issue a DISPLAY TEXT containing the following text: Test BCAST-1.1-SCBP-int-101 is OK 4. The terminal receives the service guide and discovers the Smartcard Provisioning service. 5. Terminal discovers the support of Smartcard Broadcast Provisioning function in the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 6. Terminal performs the filtering of Smartcard Broadcast Provisioning service reading the EF_{USF} in the Smartcard (under ADF BSIM or under DF BCAST of USIM application, or from the BCAST-MO) and comparing the SubscriberGroupBase value to the 32 MSB of the USF. 7. Terminal transmits the file received on Flute to the Smartcard using ENVELOPE COMMAND 8. The text “Test BCAST-1.1-SCBP-int-101 is OK” is displayed on the terminal.
Pass-Criteria	The text “Test BCAST-1.1-SCBP-int-101 is OK” is displayed on the terminal.

6.2.2 Sending a file to a specific Smartcard through Smartcard Broadcast provisioning using ENVELOPE technology

Test Case Id	BCAST-1.1-SCBP-int-102
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test the Smartcard broadcast provisioning of a file requesting the Smartcard to issue a DISPLAY TEXT command, sent to a specific Smartcard, using the ENVELOPE technology.
Specification Reference	Services 5.19
SCR Reference	BCAST-SERVICES-C-047, BCAST-SERVICES-BSA-003, BCAST-SERVICES-BSM-025
ETR Reference	SCBP-001, SCBP-002, SCBP-003, SCBP-004
Tool	None
Test code	None

Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. Smartcard supports the Smartcard broadcast provisioning function: this is signaled in the EF_{BST} The Unique Smartcard Filter of the Smartcard is: 0x123456789A and this value is indicated in the EF_{USF} (group: 0x12345678, position in group: 0x9A) The Key used to receive the secured packets is Key1
Test Procedure	1. The Handset is power-on. 2. The server broadcasts a service guide signaling the availability of a service of type 13 “Smartcard Provisioning Services”. The access fragment of this service indicates: • Type of addressing: “0”; Group Size: ‘n’ = 8 (group size = 256 devices) • The Smartcard of the group: 0x12345678, and at the position in group: 0x9A is addressed: <subscriberGroupBase> element and <subscriberPosition> element are present in the <subscriberGroupIdentifier> element. • The group base is: 00010010001101000101011001111000 (12345678) => b64:‘EjRWeA==’ • The position is: 10011010 (9A) => b64: ‘mg==’ • The technology used is Envelope 3. The BSD/A broadcast a file using Flute. This file contains Command packet encapsulated in secure packet. The key used is Key1. The Command sent requests the smartcard to issue a DISPLAY TEXT containing the following text: Test BCAST-1.1-SCBP-int-102 is OK 4. The terminal receives the service guide and discovers the Smartcard Provisioning service. 5. Terminal discovers the support of Smartcard Broadcast Provisioning function in the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 6. Terminal performs the filtering of Smartcard Broadcast Provisioning service reading the EF_{USF} in the Smartcard (under ADF BSIM or under DF BCAST of USIM application, or from the BCAST-MO) and comparing the SubscriberGroupBase value to the 32 MSB of the USF, and the subscriberPosition value to 8 LSB bits of the USF. 7. Terminal transmits the file received on Flute to the Smartcard using ENVELOPE COMMAND 8. The text “Test BCAST-1.1-SCBP-int-102 is OK” is displayed on the terminal.
Pass-Criteria	The text “Test BCAST-1.1-SCBP-int-102 is OK” is displayed on the terminal.

6.2.3 Sending a file to a set of Smartcards in a group through Smartcard Broadcast provisioning using ENVELOPE technology

Test Case Id	BCAST-1.1-SCBP-int-103
Test Object	BCAST Terminal / Smartcard/ Server.

Test Case Description	Test the Smartcard broadcast provisioning of a file requesting the Smartcard to issue a DISPLAY TEXT command, sent to a set of Smartcards in a group of 256 Smartcards, using the ENVELOPE technology.
Specification Reference	Services 5.19
SCR Reference	BCAST-SERVICES-C-047, BCAST-SERVICES-BSA-003, BCAST-SERVICES-BSM-025
ETR Reference	SCBP-001, SCBP-002, SCBP-003, SCBP-004
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. Smartcard supports the Smartcard broadcast provisioning function: this is signaled in the EF_{BST} The Unique Smartcard Filter of the Smartcard is: 0x123456789A and this value is indicated in the EF_{USF} (group: 0x12345678, position in group: 0x9A) The Key used to receive the secured packets is Key1
Test Procedure	1. The Handset is power-on. 2. The server broadcasts a service guide signaling the availability of a service of type 13 “Smartcard Provisioning Services”. The access fragment of this service indicates: • Type of addressing: “0”; Group Size: ‘n’ = 8 (group size = 256 devices) • A set of 5 Smartcards of the group: 0x12345678, and at the positions determined by the Access Mask (0x12, 0x34, 0x56, 0x78, 0x9A) are addressed: <subscriberGroupBase> element and <subscriberAccessMask> element are present in the <subscriberGroupIdentifier> element. • The group base is: 00010010001101000101011001111000 (12345678) => b64:‘EjRWeA==’ • The Access Mask is : ‘AAAAAAAAAAAAAAAAAgAAAACAAAAAIAAAAAgAAAACAAA=’ • The technology used is Envelope 3. The BSD/A broadcast a file using Flute. This file contains Command packet encapsulated in secure packet. The key used is Key1. The Command sent requests the smartcard to issue a DISPLAY TEXT containing the following text: Test BCAST-1.1-SCBP-int-103 is OK 4. The terminal receives the service guide and discovers the Smartcard Provisioning service. 5. Terminal discovers the support of Smartcard Broadcast Provisioning function in the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 6. Terminal performs the filtering of Smartcard Broadcast Provisioning service reading the EF_{USF} in the Smartcard (under ADF BSIM or under DF BCAST of USIM application, or from the BCAST-MO) and comparing the SubscriberGroupBase value to the 32 MSB of the USF, and bits set to one in the subscriberAccessMask value with the position value of the Smartcard in the group defined by the 8 LSB bits of the USF. 7. Terminal transmits the file received on Flute to the Smartcard using ENVELOPE COMMAND 8. The text “Test BCAST-1.1-SCBP-int-103 is OK” is displayed on the terminal.
Pass-Criteria	The text “Test BCAST-1.1-SCBP-int-103 is OK” is displayed on the terminal.

6.2.4 Sending a file to a group of Smartcards through Smartcard Broadcast provisioning using SCWS technology

Test Case Id	BCAST-1.1-SCBP-int-104
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test the Smartcard broadcast provisioning of a file requesting the Smartcard to issue a DISPLAY TEXT command, sent to a group of 256 Smartcards, using SCWS technology.
Specification Reference	Services 5.19
SCR Reference	BCAST-SERVICES-C-047, BCAST-SERVICES-C-051, BCAST-SERVICES-BSA-003, BCAST-SERVICES-BSM-025
ETR Reference	SCBP-001, SCBP-002, SCBP-003, SCBP-004
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. Smartcard supports the Smartcard broadcast provisioning function: this is signaled in the EF_{BST} The Unique Smartcard Filter of the Smartcard is: 0x123456789A and this value is indicated in the EF_{USF} (group: 0x12345678, position in group: 0x9A) The Smartcard contains a HTML page containing the text: “Test BCAST-1.1-SCBP-int-104 in progress” at the following URL:

Test Procedure	1. The Handset is power-on. 2. The user browses the HTML page in the Smartcard, The terminal display this page using the SCWS and the text "Test BCAST-1.1-SCBP-int-104 in progress" appears on the screen 3. The server broadcasts a service guide signaling the availability of a service of type 13 "Smartcard Provisioning Services". The access fragment of this service indicates: • Type of addressing: "0"; Group Size: 'n' = 8 (group size = 256 devices) • The whole group is addressed : only the <subscriberGroupBase> element is present in the <subscriberGroupIdentifier> element. The group base is: 00010010001101000101011001111000 (12345678) = b64:'EjRWeA==' • The technology used is SCWS • The URL is: • The type of request is PUT 4. The BSD/A broadcast a file using Flute. This file contains a HTML page which is an update of the HTML page stored in the Smartcard, this page contains the text: "Test BCAST-1.1-SCBP-int-104 is OK" 5. The terminal receives the service guide and discovers the Smartcard Provisioning service. 6. Terminal discovers the support of Smartcard Broadcast Provisioning function in the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 7. Terminal performs the filtering of Smartcard Broadcast Provisioning service reading the EF_{USF} in the Smartcard (under ADF BSIM or under DF BCAST of USIM application, or from the BCAST-MO) and comparing the SubscriberGroupBase value to the 32 MSB of the USF. 8. Terminal transmits the file received on Flute to the Smartcard using the SCWS with a PUT command 9. The user browses continuously the HTML page in the Smartcard until the text "Test BCAST-1.1-SCBP-int-104 is OK" is displayed on the terminal.
Pass-Criteria	1. The text "Test BCAST-1.1-SCBP-int-104 in progress" is displayed on the terminal. 2. The text "Test BCAST-1.1-SCBP-int-104 is OK" is displayed on the terminal.

6.3 Parental Control for service ordering

6.3.1 Parental control for service ordering using the Smartcard Profile Extension: Service provisioning protection enabled

Test Case Id	BCAST-1.1-PCSO-int-101
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test the Parental Control for service ordering using the Smartcard Profile Extension.
Specification Reference	Services 5.1.10

SCR Reference	BCAST-SERVICES-C-033, BCAST-SERVICES-BSM-029
ETR Reference	SPR-016, SPR-019, SPR-012
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. The Smartcard supports the Parental control for service ordering and this is signaled in the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). The parental control PINCODE is 1234 The parental control for service provisioning protection is enabled in the Smartcard: the Service_Provisioning_Local_Protection_Flag is set to 0x01 in EF_{SP} of the Smartcard. The Service guide signals a Service (service1) for adult with a purchase fragment. The service guide is broadcast. The user has no subscription for the Service1 The server supports the Smartcard Profile extension.
Test Procedure	1. The Handset is power-on. 2. The terminal receives the service guide and display the service guide to the user 3. The user browses the service guide and select the Service1 4. The Terminal asks the user if he wants to purchase the service 5. The user answer positively 6. The terminal send a Service Request to the BSM 7. The BSM checks the Parental level required for this service with the level granted for the user. 8. The BSM sends a Service Response containing a challenge element and the Status Code 033 “Parental Control Authentication Requested” 9. The Terminal checks the support of the Service Provisioning Message protection by the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 10. The terminal sends an Authenticate Command in Parental Control Service Provisioning Mode to the Smartcard with the Service Provisioning type set to 0x00 and the RequestID of the Service Request. 11. The Smartcard answers to the Authenticate command containing a status code indicating that the PINCODE is required and with the Key reference to be used. 12. The Terminal requests the PINCODE to the user. The user enters the PINCODE ‘1234’. 13. The Terminal sends a VERIFY PIN command to the Smartcard that ends successfully. 14. The Terminal re-sends the Authenticate Command to obtain the MAC of the service Provisioning data 15. The Smartcard sends back the Authenticate command response including the HMAC data. 16. The terminal sends a new service provisioning message including the MAC received from the Smartcard. 17. The BSM verified the MAC and sends a service response with the status code 000 “success”.

Pass-Criteria	The BSM sends a Service response with status code 033 On the Terminal the PINCODE is requested to the user The BSM sends a Service response with status code 000

6.3.2 Parental control for service ordering using the Smartcard Profile Extension: Service provisioning disallowed in Smartcard

Test Case Id	BCAST-1.1-PCSO-int-103
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test the Parental Control for service ordering using the Smartcard Profile Extension.
Specification Reference	Services 5.1.10
SCR Reference	BCAST-SERVICES-C-033, BCAST-SERVICES-BSM-029
ETR Reference	SPR-016, SPR-019, SPR-012
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. The Smartcard supports the Parental control for service ordering and this is signaled in the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). The parental control PINCODE is 1234 The parental control for service provisioning protection is disallowed in the Smartcard: the Service_Provisioning_Local_Protection_Flag is set to 0x02 in EF_{SP} of the Smartcard. The Service guide signals a Service (service1) for adult with a purchase fragment. The service guide is broadcast. The user has no subscription for the Service1

Test Procedure	12. The Handset is power-on. 13. The terminal receives the service guide and display the service guide to the user 14. The user browses the service guide and select the Service1 15. The Terminal asks the user if he wants to purchase the service 16. The user answer positively 17. The terminal sends a Service Request to the BSM 18. The BSM checks the Parental level required for this service with the level granted for the user. 19. The BSM sends a Service Response containing a challenge element and the Status Code 033 “Parental Control Authentication Requested” 20. The Terminal checks the support of the Service Provisioning Message protection by the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 21. The terminal sends an Authenticate Command in Parental Control Service Provisioning Mode to the Smartcard with the Service Provisioning type set to 0x00 and the RequestID of the Service Request. 22. The Smartcard answers to the Authenticate command containing a status code indicating that the Service Provisioning is locally disallowed. 23. The Terminal informs the user that the Service provisioning is disallowed.
Pass-Criteria	The BSM sends a Service response with status code 033 The terminal informs the user that the Service Provisioning is disallowed.

6.3.3 Parental control for token purchase using the Smartcard Profile Extension: No local protection

Test Case Id	BCAST-1.1-PCSO-int-103
Test Object	BCAST Terminal / Smartcard/ Server.
Test Case Description	Test the Parental Control for token purchase using the Smartcard Profile Extension.
Specification Reference	Services 5.1.10
SCR Reference	BCAST-SERVICES-C-033, BCAST-SERVICES-BSM-029
ETR Reference	SPR-016, SPR-019, SPR-012
Tool	None
Test code	None

Preconditions	Smartcard is USIM or CSIM There is a reference terminal or terminal emulator available. The Smartcard supports the Parental control for service ordering and this is signaled in the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). The parental control PINCODE is 1234 There is no local parental control protection for the service provisioning in the Smartcard: the Service_Provisioning_Local_Protection_Flag is set to 0x00 in EF_{SP} of the Smartcard. The Service guide signals a Service (service1) for which the consumption uses tokens as described in the purchase fragment. The service guide is broadcast. The user needs token for the consumption of Service1 The server supports the Smartcard Profile extension.
Test Procedure	1. The Handset is power-on. 2. The terminal receives the service guide and display the service guide to the user 3. The user browses the service guide and select the Service1 4. The Terminal asks the user if he wants to purchase token to access to the service 5. The user answer positively 6. The terminal send a Token Purchase Request to the BSM 7. The BSM checks the Parental level required for this purchase with the level granted for the user. 8. The BSM sends a Token Purchase Response containing a challenge element and the Status Code 033 “Parental Control Authentication Requested” 9. The Terminal checks the support of the Service Provisioning Message protection by the Smartcard reading the EF_{BST} (under ADF BSIM or under DF BCAST of USIM application). 10. The terminal sends an Authenticate Command in Parental Control Service Provisioning Mode to the Smartcard with the Service Provisioning type set to 0x01 and the RequestID of the Service Request. 11. The Smartcard sends back the Authenticate command response including the HMAC data. 12. The terminal sends a new Token Purchase Request provisioning message including the MAC received from the Smartcard. 13. The BSM verified the MAC and sends a Token Purchase Response with the status code 000 “success”.
Pass-Criteria	The BSM sends a Token Purchase Response with status code 033 The BSM sends a Token Purchase Response with status code 000

7. BCAST IOP Test Cases (AM-server / Smartcard)

7.1 Audience Measurement

7.1.1 Smartcard-Centric Audience Measurement

7.1.1.1 Registration Process and Opt_in trigger process using SMS-PP bearer

Test Case Id	BCAST-1.1-SC-AM-int-101
Test Object	AM-server/Smartcard.
Test Case Description	Test the registration process of the Smartcard-centric Audience Measurement. Test the OPT-IN Process of the Smartcard-centric Audience Measurement using a OPT_IN_NOTIFICATION_TRIGGER
Specification Reference	Services 5.20.2.1.1 and 5.20.2.1.2
SCR Reference	BCAST-AM-SC-002, BCAST-AM-M-025, BCAST-AM-SC-006, BCAST-AM-M-029, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-029, BCAST-AM-C-030
ETR Reference	AMS-001, AMS-002, AMS-004, AMS-009, AMS-011
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM. Terminal supporting SCR references available. The registration has never been performed. Kamue, Kamus and UserId have not been set in the Smartcard. Address of the SMSC is set in the Smartcard. TPDA address of the BCAST AM-M is set in the Smartcard A key Km is stored in the Smartcard The server stores Km keys associated to each card. The key version for the Kic field of the SMS shall be set to 0x00 for the server and the Smartcard. The key version for the KID field of the SMS shall be set to 0x00 for the server and the Smartcard. The Audience Measurement PIN is ‘1234’

Test Procedure	1. The Handset is power-on. 2. BCAST AM-C sends to the Terminal a proactive command PROVIDE_LOCAL_INFORMATION (IMEI) to request the IMEI to the Terminal 3. The Terminal sends the IMEI value in the response of the PROVIDE_LOCAL_INFORMATION to the card 4. BCAST AM-C sends a REGISTRATION_REQUEST in a SMS-MO using the address of SMSC and TPDA of BCAST AM-M stored in the Smartcard. The Smartcard inserts in the REGISTRATION_REQUEST message a. The IMSI of the card stored in the Smartcard b. The ICCID of the card stored in the Smartcard c. The IMEI received from the Terminal d. A random value (CardRandom) 5. The BCAST AM-M sends back a REGISTRATION-RESPONSE in a class 2 SMS-MO using the address of the Smartcard corresponding to the IMSI and a TAR value equal to 'B2 02 02'. The server inserts in the REGISTRATION_RESPONSE message: a. A unique Identifier UserID b. A random value (ServerRandom) 6. The Server computes Kamue and Kamus 7. The Smartcard at the reception of REGISTRATION_ RESPONSE message computes Kamue and Kamus 8. To test the successful establishment of Keys and then the communication between AM-M server and AM-C, a secure SMS is sent to the Smartcard with a text to be display on the terminal. Then OPT_IN_TRIGGER message is sent from the server AM-M to the AM-C in the Smartcard using a secured packet SMS-PP. In the command header of the Secure SMS, the security parameters are set in the following way: a. SPI indicates Digital signature (to test Kamus), ciphering, no counter, POR sent to the SE with Digital signature and ciphering b. Kic indicates uses of DES with mode 00, and key reference to be used (0x00). c. KID indicates uses of DES with mode 00, and key reference to be used (0x00) d. The TAR value is for Smartcard-centric Audience measurement (B2 02 02). The secured data contain the OPT_IN_INVITATION_TRIGGER with the following text in English language: "Registration test is OK." 9. The AM-C requests the Audience's measurement PIN to the user, using a proactive command (implementation dependant) 10. The user enters the Audience measurement PIN '1234' 11. The AM-C in the Smartcard sends a proactive command (should be GET INKEY) to the terminal to display the text received in the OPT_IN_INVITATION_TRIGGER message and request the consent of user for a campaign. 12. The user accepts the campaign entering the text requested on the display. 13. The AM-C sends back a SMS with the OPT_IN_STATE_NOTIFICATION message with the Opt_in state value to 0x01

Pass-Criteria	1. Reception on the server side (AM-M) of the POR of the SMS without error of decryption and signature. 2. The AM PIN is requested on the handset display. 3. Display on the handset: “Registration is OK”, following by a request of consent for a campaign. 4. The AM-M receives an Opt-in state indicating that the user has Opt-in.

7.1.1.2 Configuration process, activation and reporting using SMS-PP bearer in Push Mode

Test Case Id	BCAST-1.1-SC-AM-int-102
Test Object	AM-server/Smartcard.
Test Case Description	Test the configuration of AM-C, the activation of AM function in AM-C and the reporting for Smartcard-centric Audience Measurement
Specification Reference	Services 5.20.2.1.3, Services 5.20.2.1.4, Services 5.20.2.1.5, Services 5.20.2.1.6,
SCR Reference	BCAST-AM-SC-001, BCAST-AM-SC-017, BCAST-AM-M-024, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-030
ETR Reference	AMS-001, AMS005, AMS-006, AMS-008, AMS-012, AMS-013, AMS-015
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The test BCAST-1.1-SC-AM-int-101 has been performed successfully. The user has Opt-in for the campaign. Reception of Mobile TV encrypted contents using the Smartcard profile. Minimum 2 channels available, with Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1 and SEK/PEKID Key group part = 0002 for channel 2

Test Procedure	1. The Server AM-M sends CONFIGURATION message using secure SMS-PP and containing the following parameters: a. Reporting bearer: SMS-PP b. SMSC address c. TPDA address d. Reporting mode: Push e. Reporting frequency: 1 hour f. Reporting trigger: 20 bytes (the reporting will be sent in short term) g. No additional metrics 2. The server sends an AUDIT_REQUEST command with the tag ‘E5’ (buffer filling level) to verify that the buffer is empty. 3. The AM-C sends a AUDIT_RESPONSE command with the buffer filling level set to 0x00 4. The server AM-M sends ACTIVATION message with an activation state set to 0x01. 5. The user zaps from one channel to other (1 time) 6. The server sends an AUDIT_REQUEST command with the tag ‘E5’ (buffer filling level) to verify that the buffer is no more empty. 7. The AM-C sends a AUDIT_RESPONSE command with the buffer filling level set to a value1 > 0x00 8. The user zaps from one channel to other (2 times) 9. The server sends an AUDIT_REQUEST command with the tag ‘E5’ (buffer filling level) to verify that the buffer is filling. 10. The AM-C sends a AUDIT_RESPONSE command with the buffer filling level set to a value2 >Value1 11. The user zaps from one channel to other (1 time) 12. The AM-C sends a report to AM-M in a SMS 13. The AM-M sends a REPORTING_RESPONSE with a reporting message state set to ‘0x00’ (successful) 14. The server sends an AUDIT_REQUEST command with the tag ‘E5’ (buffer filling level) to verify that the buffer has been flushed. 15. The AM-C sends a AUDIT_RESPONSE command with the buffer filling level set to value3 < value2
Pass-Criteria	1. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level set to 0x00 2. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level value1 > 0x00 3. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level value2 >Value1 4. Reception on the server side (AM-M) of report in a SMS containing the 4 zapping events. 5. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level value3 < value2

7.1.1.3 Opt_in Message using SMS-PP bearer

Test Case Id	BCAST-1.1-SC-AM-int-103
Test Object	AM-server/Smartcard.
Test Case Description	Test the OPT-IN state update in the Smartcard for Smartcard-centric Audience Measurement. An Opt-out is sent to the card that will stop the reporting process. An Opt_in is sent to the card and the reporting process resumes.
Specification Reference	Services 5.20.2.1.2
SCR Reference	BCAST-AM-SC-005, BCAST-AM-M-028, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-030
ETR Reference	AMS-001, AMS-003, AMS-010
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The test BCAST-1.1-SC-AM-int-101 has been performed successfully. The user has Opt-in for the campaign. The test BCAST-1.1-SC-AM-int-102 has been performed successfully.
Test Procedure	1. The user resumes the zapping from one channel to the other and reports are sent to the AM-M every 4 zapping events more or less. 2. The Server AM-M sends an OPT-IN message using secure SMS-PP. a. The opt-in state sent in the message is opt-out (0x00) 3. At the reception of the OPT_IN message, the AM_C stops the sending of reports even though the zapping is carried on. 4. The server AM-M sends an AUDIT_REQUEST command with the tag ‘E5’ (buffer filling level) to verify the level of the buffer 5. The AM-C sends a AUDIT_RESPONSE command with the buffer filling level set to value 1 6. The zapping is carried on 7. The server AM-M sends an AUDIT_REQUEST command with the tag ‘E5’ (buffer filling level) to verify that level of the buffer is unchanged. 8. The AM-C sends a AUDIT_RESPONSE command with the buffer filling level set to value 2 = value1 9. The Server AM-M sends an OPT-IN message using secure SMS-PP. a. The opt-in state sent in the message is opt-in (0x01) 10. The zapping is carried on. At the reception of the OPT_IN message, the AM_C resumes the sending of reports.

Pass-Criteria	1. Reception on the server side (AM-M) of several reports in SMS containing 4 zapping events more or less. 2. After sending of OPT_IN message for Opt-out, the reception of SMS with reports stops. 3. The two buffers filling level received are identical. 4. After sending of OPT_IN message for Opt-in, the reception of SMS with reports resumes.

7.1.1.4 Configuration process, activation and reporting using SMS-PP bearer in Push Mode with additional metrics

Test Case Id	BCAST-1.1-SC-AM-int-104
Test Object	AM-server/Smartcard.
Test Case Description	Test the configuration of AM-C, the activation of AM function in AM-C and the reporting with location information for Smartcard-centric Audience Measurement
Specification Reference	Services 5.20.2.1.3, Services 5.20.2.1.4, Services 5.20.2.1.5, Services 5.20.2.1.6,
SCR Reference	BCAST-AM-SC-001, BCAST-AM-SC-017, BCAST-AM-M-024, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-030
ETR Reference	AMS-001, AMS005, AMS-006, AMS-008, AMS-012, AMS-013, AMS-015
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The test BCAST-1.1-SC-AM-int-101 has been performed successfully. The user has Opt-in for the campaign. Reception of Mobile TV encrypted contents using the Smartcard profile. Minimum 2 channels available, with Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1 and SEK/PEKID Key group part = 0002 for channel 2 The location type supported by the couple Terminal/Smartcard is 3GPP location for USIM and 3GPP2 for CSIM

Test Procedure	1. The server sends an AUDIT_REQUEST command with the tag 'E3' (location type supported). 2. The AM-C sends an AUDIT_RESPONSE command with the location types supported by the couple Terminal/Smartcard. (3GPP for USIM and 3GPP2 for CSIM) 3. The Server AM-M sends CONFIGURATION message using secure SMS-PP and containing the following parameters: a. Reporting bearer: SMS-PP b. SMSC address c. TPDA address d. Reporting mode: Push e. Reporting frequency: 1 hour f. Reporting trigger: 40 bytes (the reporting will be sent in short term) g. Location Type: 3GPP (0x01) if the Smartcard is USIM and 3GPP2 (0x02) if Smartcard is CSIM h. Additional metrics indicates that Location_In is needed 4. The server AM-M sends ACTIVATION message with an activation state set to 0x01. 5. The user zaps from one channel to other (x times) 6. AM_C sends a proactive command PROVIDE_LOCAL_INFORMATION to the Terminal to get the location at each zapping. 7. The Terminal sends the Location information in the response. 8. The AM-C sends a report to AM-M in a SMS containing the Location_In information for each zapping. 9. The AM-M sends a REPORTING_RESPONSE with a reporting message state set to '0x00' (successful)
Pass-Criteria	1. Reception on the server side (AM-M) of report in a SMS containing the x zapping events with Location_In information.

7.1.1.5 Reporting using SMS-PP bearer in Pull Mode without additional metrics

Test Case Id	BCAST-1.1-SC-AM-int-105
Test Object	AM-server/Smartcard.
Test Case Description	Test the configuration of AM-C, the activation of AM function in AM-C and the reporting for Smartcard-centric Audience Measurement
Specification Reference	Services 5.20.2.1.3, Services 5.20.2.1.4, Services 5.20.2.1.5, Services 5.20.2.1.6,
SCR Reference	BCAST-AM-SC-001, BCAST-AM-SC-017, BCAST-AM-M-024, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-030
ETR Reference	AMS-001, AMS-005, AMS-007, AMS-012, AMS-014
Tool	None
Test code	None

Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The test BCAST-1.1-SC-AM-int-101 has been performed successfully. The user has Opt-in for the campaign. Reception of Mobile TV encrypted contents using the Smartcard profile. Minimum 2 channels available, with Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1 and SEK/PEKID Key group part = 0002 for channel 2 The test BCAST-1.1-SC-AM-int-104 has been performed successfully
Test Procedure	1. The Server AM-M sends CONFIGURATION message using secure SMS-PP and containing the following parameters: a. Reporting bearer: SMS-PP b. SMSC address c. TPDA address d. Reporting mode: Pull e. Reporting trigger: 100 bytes f. No Additional metrics 2. The user zaps from one channel to other (x times) 3. The AM-M sends a REPORTING_REQUEST message using secure SMS-PP 4. The AM-C sends a report to AM-M in a SMS. 5. The AM-M sends a REPORTING_RESPONSE with a reporting message state set to ‘0x00’ (successful)
Pass-Criteria	1. Reception on the server side (AM-M) of report in a SMS containing the x zapping events.

7.1.1.6 Registration Process and Opt_in trigger process using security at application level

Test Case Id	BCAST-1.1-SC-AM-int-106
Test Object	AM-server/Smartcard.
Test Case Description	Test the registration process of the Smartcard-centric Audience Measurement. Test the OPT-IN Process of the Smartcard-centric Audience Measurement using a OPT_IN_NOTIFICATION_TRIGGER
Specification Reference	Services 5.20.2.1.1 and 5.20.2.1.2
SCR Reference	BCAST-AM-SC-002, BCAST-AM-M-025, BCAST-AM-SC-006, BCAST-AM-M-029, BCAST-AM-SC-018, BCAST-AM-SC-022, BCAST-AM-M-036, BCAST-AM-M-041, BCAST-SPCP-C-005, BCAST-AM-C-029, BCAST-AM-C-030
ETR Reference	AMS-001, AMS-002, AMS-004, AMS-009, AMS-011
Tool	None
Test code	None

Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The registration has never been performed. Kamue, Kamus and UserId have not been set in the Smartcard. Address of the SMSC is set in the Smartcard. TPDA address of the BCAST AM-M is set in the Smartcard A key Km is stored in the Smartcard The server stores Km keys associated to each card. The Audience Measurement PIN is ‘1234’

Test Procedure	1. The Handset is power-on. 2. BCAST AM-C sends to the Terminal a proactive command PROVIDE_LOCAL_INFORMATION (IMEI) to request the IMEI to the Terminal 3. The Terminal sends the IMEI value in the response of the PROVIDE_LOCAL_INFORMATION to the card 4. BCAST AM-C sends a REGISTRATION_REQUEST in a SMS-MO using the address of SMSC and TPDA of BCAST AM-M stored in the Smartcard. The Smartcard inserts in the REGISTRATION_REQUEST message a. The IMSI of the card stored in the Smartcard b. The ICCID of the card stored in the Smartcard c. The IMEI received from the Terminal d. A random value (CardRandom) 5. The BCAST AM-M sends back a REGISTRATION-RESPONSE in a class 2 SMS-MO using the address of the Smartcard corresponding to the IMSI and a TAR value equal to ‘B2 02 02’. The server inserts in the REGISTRATION_RESPONSE message: a. A unique Identifier UserID b. A random value (ServerRandom) 6. The Server computes Kamue and Kamus 7. The Smartcard at the reception of REGISTRATION_ RESPONSE message computes Kamue and Kamus. To test the successful establishment of Keys and then the communication between AM-M server and AM-C, a secure OPT_IN_TRIGGER message is sent from the server AM-M to the AM-C in the Smartcard using applicative security and SMS-PP bearer. The OPT_IN_INVITATION_TRIGGER message is sent encrypted and signed (tag ‘C3’), the key set used is Kamue and Kamus. The secured message payload contain the following prompt message in English language: “Registration test is OK.” 8. The AM-C requests the Audience’s measurement PIN to the user, using a proactive command (implementation dependant) 9. The user enters the Audience measurement PIN ‘1234’ 10. The AM-C in the Smartcard sends a proactive command (should be GET INKEY) to the terminal to display the text received in the OPT_IN_INVITATION_TRIGGER message and request the consent of user for a campaign. 11. The user accepts the campaign entering the text requested on the display. 12. The AM-C sends back a SMS with the OPT_IN_STATE_NOTIFICATION message with the Opt_in state value to 0x01
Pass-Criteria	1. The AM PIN is requested on the handset display. 2. Display on the handset: “Registration is OK.”, following by a request of consent for a campaign. 3. The AM-M receives an Opt-in state indicating that the user has Opt-in.

7.1.1.7 Configuration process, activation and reporting using HTTP bearer in Push Mode using security at applicative level

Test Case Id	BCAST-1.1-SC-AM-int-107
Test Object	AM-server/Smartcard.
Test Case Description	Test the configuration of AM-C, the activation of AM function in AM-C and the reporting for Smartcard-centric Audience Measurement
Specification Reference	Services 5.20.2.1.3, Services 5.20.2.1.4, Services 5.20.2.1.5, Services 5.20.2.1.6,
SCR Reference	BCAST-AM-SC-001, BCAST-AM-SC-017, BCAST-AM-M-024, BCAST-AM-SC-018, BCAST-AM-SC-019, BCAST-AM-SC-022, BCAST-AM-M-036, BCAST-AM-M-037, BCAST-AM-M-041, BCAST-SPCP-C-005, BCAST-AM-C-031
ETR Reference	AMS-001, AMS005, AMS-006, AMS-008, AMS-012, AMS-013, AMS-015
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The test BCAST-1.1-SC-AM-int-106 has been performed successfully. The user has Opt-in for the campaign. Reception of Mobile TV encrypted contents using the Smartcard profile. Minimum 2 channels available, with Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1 and SEK/PEKID Key group part = 0002 for channel 2

Test Procedure	1. The Server AM-M sends CONFIGURATION message (tag ‘C6’) using SMS-PP and security at applicative level and containing the following parameters: a. Reporting bearer: HTTP b. BCAST AM-M address c. Reporting mode: Push d. Reporting frequency: 1 hour e. Reporting trigger: 20 bytes (the reporting will be sent in short term) f. No additional metrics 2. The server sends an AUDIT_REQUEST command (tag ‘CB’) using SMS-PP with the tag ‘E5’ (buffer filling level) in the tag list to verify that the buffer is empty. 3. The AM-C sends a AUDIT_RESPONSE command (tag ‘CC’) using SMS-PP with the buffer filling level set to 0x00 4. The server AM-M sends ACTIVATION message (tag ‘C7’) using SMS-PP with an activation state set to 0x01. 5. The user zaps from one channel to other (1 time) 6. The server sends an AUDIT_REQUEST command (tag ‘CB’) using SMS-PP with the tag ‘E5’ (buffer filling level) in the tag list to verify that the buffer is no more empty. 7. The AM-C sends a AUDIT_RESPONSE command (tag ‘CC’) using SMS-PP with the buffer filling level set to a value1 > 0x00 8. The user zaps from one channel to other (2 times) 9. The server sends an AUDIT_REQUEST command (tag ‘CB’) using SMS-PP with the tag ‘E5’ (buffer filling level) in the tag list to verify that the buffer is filling. 10. The AM-C sends a AUDIT_RESPONSE command (tag ‘CC’) using SMS-PP with the buffer filling level set to a value2 >Value1 11. The user zaps from one channel to other (1 time) 12. The AM-C opens a channel using the Bearer Independent Protocol. The AM-C sends the proactive command OPEN CHANNEL related to default (network) bearer to the terminal. The parameters are : BCAST AM-M Address as data destination address 13. The AM-C sends a report to AM-M in a POST message 14. The AM-M sends a REPORTING_RESPONSE with a reporting message state set to ‘0x00’ (successful) over HTTP. 15. The server sends an AUDIT_REQUEST command (tag ‘CB’) using SMS-PP with the tag ‘E5’ (buffer filling level) in the tag list to verify that the buffer has been flushed. 16. The AM-C sends a AUDIT_RESPONSE command (tag ‘CC’) using SMS-PP with the buffer filling level set to value3 < value2
Pass-Criteria	1. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level set to 0x00 2. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level value1 > 0x00 3. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level value2 >Value1 4. Reception on the server side (AM-M) of report over HTTP containing the 4 zapping events. 5. Reception on the server side (AM-M) of AUDIT_RESPONSE command with the buffer filling level value3 < value2

7.1.1.8 Audience Measurement disallowed for a specific encrypted content

Test Case Id	BCAST-1.1-SC-AM-int-108
Test Object	AM-server/ Smartcard.
Test Case Description	Test Audience Measurement prohibition for critical encrypted content
Specification Reference	Services 5.20.2.1.5,
SCR Reference	BCAST-AM-SC-001, BCAST-AM-SC-017, BCAST-AM-M-024, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-030
ETR Reference	AMS-001, AMS-005, AMS-007, AMS-012, AMS-014
Tool	None
Test code	None
Preconditions	Smartcard is USIM or CSIM Terminal supporting SCR references available. The test BCAST-1.1-SC-AM-int-101 has been performed successfully. The user has Opt-in for the campaign. Reception of Mobile TV encrypted contents using the Smartcard profile. Minimum 2 channels available, with Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1 and SEK/PEKID Key group part = 0002 for channel 2. The STKM stream for the channel 2 contains Smartcard-Centric_Audience_Measurement_control descriptor with the flag Audience_Measurement_disallowed set to 1 The test BCAST-1.1-SC-AM-int-104 has been performed successfully
Test Procedure	1. The Server AM-M sends CONFIGURATION message using secure SMS-PP and containing the following parameters: g. Reporting bearer: SMS-PP h. SMSC address i. TPDA address j. Reporting mode: Pull k. Reporting trigger: 100 bytes l. No Additional metrics 2. The user zaps from one channel to other (x times) 3. The AM-M sends a REPORTING_REQUEST message using secure SMS-PP 4. The AM-C sends a report to AM-M in a SMS. 5. The AM-M sends a REPORTING_RESPONSE with a reporting message state set to ‘0x00’ (successful)
Pass-Criteria	1. Reception on the server side (AM-M) of report in a SMS without events for channel2

8. BCAST IOP Test Cases (AM-server / Terminal/ Smartcard)

8.1 Audience Measurement

8.1.1 Smartcard-Centric Audience Measurement

8.1.1.1 STKM-based and Event signalling-based Audience Measurement for clear to air services

Test Case Id	BCAST-1.1-SC-AM-int-109
Test Object	AM-server/Terminal/Smartcard.
Test Case Description	Test the signaling of Smartcard-Centric AM capability and the Audience measurement of clear to air services with a content for which the AM is disallowed.
Specification Reference	Services 5.20.2.1.8, Services 5.20.2.1.9,
SCR Reference	BCAST-AM-SC-001, BCAST-AM-SC-017, BCAST-AM-M-024, BCAST-AM-SC-018, BCAST-AM-SC-021, BCAST-AM-M-036, BCAST-AM-M-040, BCAST-SPCP-C-005, BCAST-AM-C-028,
ETR Reference	AMS-001, AMS-005, AMS-007, AMS-012, AMS-014
Tool	None
Test code	None

Preconditions	Smartcard is USIM or CSIM The EFBST in the Smartcard indicates that the Smartcard supports the Smartcard-centric Audience Measurement function. A SEK is available in the Smartcard for the clear to air service (Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1). And for the encrypted service 2 (SEK/PEKID Key group part = 0002 for channel 2 encrypted service) The service guide signals Service 1: in the Access fragment of the Service 1, the KmsType in the KeyManagementSystem element indicates that the protection is the Smartcard profile using the GBA-U oma-bcast-gba_u-mbms = “1” if USIM is used or using bcmcs oma-bcast-prov-bcmcs = “3” if CSIM is used. The Encryption type is absent, and the associated STKM stream is signalled in the SDP. AmAllowed attribute is set to 1 for the content1 in the associated ‘Content’ fragments of the BCAST Service Guide and AmAllowed attribute is set to 0 for the Content2 in the associated ‘Content’ fragment. The GlobalServiceID of this service is CLEAR (ASCII-encoded), and the GlobalContentID is CONTENT1 (ASCII-encoded) for Content1 and CONTENT2 (Ascii-encoded) for the Content2 Reception of Mobile TV contents using the Smartcard profile. Minimum 2 channels available, with Key_domain_id= MCC1 || MNC1; SEK/PEK_ID Key group part = 0001 for channel 1(clear to air service) and SEK/PEKID Key group part = 0002 for channel 2 encrypted service). Reception of STKM streams associated with the two services. The STKM stream of channel 1, when the clear content1 is broadcasted has no Smartcard-Centric_Audience_Measurement_control descriptor, and the STKM stream of channel 1, when the clear content2 is broadcasted contains Smartcard-Centric_Audience_Measurement_control descriptor with the flag Audience_Measurement_disallowed set to 1. Traffic_protection_protocol of the STKM stream associated to channel1 is set to TKM_ALGO_NULL corresponding to NULL encryption (0x4). The registration has never been performed. Kamue, Kamus and UserId have not been set in the Smartcard.

Test Procedure	1. The Handset is power-on. 2. The handset reads the EFBST file in the Smartcard and discovers that the Smartcard supports the Smartcard-centric Audience measurement function 3. The handset sends a OMA BCAST Command in the Event Signalling Mode with the event ‘Smartcard-Centric AM support’ to indicate to the Smartcard that the Terminal supports the Smartcard-centric Audience Measurement. 4. Then the steps 2 to 13 of the test BCAST-1.1-SC-AM-int-101 are performed (Registration process and OPT-IN process) 5. The server sends an AUDIT_REQUEST command with the tag ‘E7’ (Terminal Smartcard-Centric AM Capability). 6. The AM-C sends an AUDIT_RESPONSE command with the Terminal Smartcard-Centric AM Capabilityfield set to 0x01 indicating that the Terminal supports the Smartcard-Centric AM 7. The Server AM-M sends CONFIGURATION message using secure SMS-PP and containing the following parameters: i. Reporting bearer: SMS-PP j. SMSC address k. TPDA address l. Reporting mode: Push m. Reporting frequency: 1 hour n. Reporting trigger: 40 bytes (the reporting will be sent in short term) o. Additional metrics indicates that Consumption_time and Service/Content ID are needed 8. The server AM-M sends ACTIVATION message with an activation state set to 0x01. 9. The user zaps from one channel to other (x times) 10. At each zapping,on Content1 of the clear service, the Terminal sends the STKM stream with NULL encryption to the Smartcard and the Terminal signals “AM Allowed Service/Content” event (‘0x02’) to the Smartcard using the Event Signalling command, with GlobalServiceID and GlobalContentID TLV and with Accumulated_Time TLV for each service. On each zapping on Content2 of the clear service, the Terminal signals “AM Disallowed Service/Content” event (0x03) to the Smartcard using the Event Signalling command, with GlobalServiceID, GlobalContentID TLV and with Accumulated_Time TLV
Pass-Criteria	1. After the sending of the AUDIT_REQUEST command with the tag ‘E7’, reception on the server side (AM-M) of AUDIT_RESPONSE with the Terminal Smartcard-Centric AM Capability set to 0x01. 2. Reception on the server side (AM-M) of report in a SMS containing the y zapping events from Service 1 (clear to air) to Service 2 (encrypted service) containing the Service/Content ID : CLEAR/CONTENT1 and the consumption _time in the additional metrics. The report contains no event for the CONTENT2.

9. BCAST IOP Test Cases (AM-server / Terminal)

9.1 Terminal-Centric Audience Measurement

9.1.1 AM campaign initiated over broadcast channel (SG-based trigger) with scheduled AM data reporting

Test Case Id	BCAST-1.1-TCAM-int-101
Test Object	BCAST Terminal / AM-server
Test Case Description	Test that the AM campaign is succesfully initiated by SG –based AM Trigger over broadcast channel, user accepts the invitation to the AM campaign, terminal measures user consumption and reports periodically the measured data to the AM-server.
Specification Reference	[BCAST11–Services], section 5.20.1 [BCAST11-SG], section 5.4.1.5.2
SCR Reference	BCAST-AM-C-005, BCAST-AM-C-007, BCAST-AM-C-013, BCAST-AM-C-015, BCAST-AM-C-021, (BCAST-AM-C-023) BCAST-AM-M-005, BCAST-AM-M-007, BCAST-AM-M-010, BCAST-AM-M-012, BCAST-AM-M-017, (BCAST-AM-M-019)
ETR Reference	AMT-001 to AMT-014
Tool	None
Test code	None
Preconditions	• Service Guide is sent over broadcast channel. • The SGDD includes the AM Trigger information. o The ‘randomSelector’ is 100 (%). o The ‘consentRequired’ attribute is “True”. • The ‘ReportInfo’ is selected to ‘PeriodicReporting’. The ‘reportingPeriod’ is set to a reasonable value (e.g., 5 minutes).

Test Procedure	• Power-on the Terminal and activate the BCAST client. o The Terminal receives the SGDD, generates a random value between 0…100, compares the value to the ‘randomSelector’, and passes the criteria to become a candidate to participate the AM campaign. • The Terminal asks the user to “Accept” or “Refuse” to participate the AM campaign. The user selects “Accept”. o The Terminal sends the “Opt-in” (‘userConsent’ = “True”) in the AM Request message to the AM-server. • The AM-server responds with the AM Response message that includes the AM Configuration Data. • The user watches the TV content. o The terminal measures the content consumption. • The terminal sends an AMRD message that includes the consumption report over the reporting period. o The terminal continues the consumption measurement during the reporting. • The AM-server sends an AMRR message to the Terminal. (Optional)
Pass-Criteria	• The user is presented with an option to either “Accept” or “Refuse” the campaign. • As a result of user accepting the campaign, the AM-server receives AM Request message from the Terminal with ‘userConsent’ = “True”. • The AM-server receives the AMRD message after the predefined reporting period. The consumption report corresponds to the user activity.

9.1.2 AM campaign initiated over broadcast channel (SG-based trigger) with user rejecting the Opt-in

Test Case Id	BCAST-1.1-TCAM-int-102
Test Object	BCAST Terminal / AM-server
Test Case Description	Test that the AM campaign is succesfully initiated by SG –based AM Trigger over broadcast channel but the user rejects the invitation to the AM campaign.
Specification Reference	[BCAST11–Services], section 5.20.1 [BCAST11-SG], section 5.4.1.5.2
SCR Reference	BCAST-AM-C-005, BCAST-AM-C-007, BCAST-AM-C-013, BCAST-AM-C-015 BCAST-AM-M-005, BCAST-AM-M-007, BCAST-AM-M-010, BCAST-AM-M-012
ETR Reference	AMT-001 to AMT-006, AMT-008 to AMT-012, AMT-014
Tool	None
Test code	None

Preconditions	• Service Guide is sent over broadcast channel. • The SGDD includes the AM Trigger information. o The 'randomSelector' is 100 (%). o The 'consentRequired' attribute is "True". •
Test Procedure	• Power-on the Terminal and activate the BCAST client. o The Terminal receives the SGDD, generates a random value between 0…100, compares the value to the 'randomSelector', and passes the criteria to become a candidate to participate the AM campaign. • The Terminal asks the user to "Accept" or "Refuse" to participate the AM campaign. The user selects "Refuse". o The Terminal sends the "Opt-in" ('userConsent' = "False") in the AM Request message to the AM-server. o Optionally, the Terminal sends "Opt-in" ('userConsent' attribute is missing) in the AM request message. • The AM-server removes the Terminal/user combination from the panel of users of the campaign. • The AM-server sends an AM Response message to the Terminal with campaignEndTime set to past. • The Terminal compares the campaignEndTime with its current time and concludes the campaign is closed for the user.
Pass-Criteria	• The user is presented with an option to either "Accept" or "Refuse" the campaign. • As a result of user rejecting the campaign, the AM-server receives AM Request message from the Terminal with 'userConsent' = "False". o Optionally, the 'userConsent' attribute is missing in the AM request message. • The user/terminal combination is not in the panel of users of the campaign in the AM-server.

9.1.3 AM campaign initiated over interaction channel (SMS –based trigger) with AM Report Trigger initiated AM data reporting

Test Case Id	BCAST-1.1-TCAM-int-103
Test Object	BCAST Terminal / AM-server
Test Case Description	Test that the AM campaign is succesfully initiated by SMS –based AM Trigger over interaction channel, user accepts the invitation to the AM campaign, terminal measures user consumption and reports the measured data to the AM-server when triggered by the AM Report Trigger message.
Specification Reference	[BCAST11–Services], section 5.20.1 [BCAST11-SG], section 5.4.1.5.2

SCR Reference	BCAST-AM-C-003, BCAST-AM-C-005, BCAST-AM-C-013, BCAST-AM-C-015, BCAST-AM-C-021, (BCAST-AM-C-023) BCAST-AM-M-003, BCAST-AM-M-005, BCAST-AM-M-010, BCAST-AM-M-012, BCAST-AM-M-017, (BCAST-AM-M-019)
ETR Reference	AMT-001 to AMT-014
Tool	None
Test code	None
Preconditions	• Service Guide is sent over broadcast channel. o The SGDD includes the AudienceMeasurement.CampaignInfo information. • The SMS trigger message type ‘1’ contains: o AMTrigger.flags bit 5 signaling that the ‘consentRequired’is “True”. o AMTrigger.serverAddressURL matching the ServerAddressURL of the AudienceMeasurement.CampaignInfo element in the SGDD. • The SMS trigger message type ‘2’ contains: o ‘Download.url’ matching the ServerAddressURL of the AudienceMeasurement.CampaignInfo element in the SGDD. o The interval between Download.validFrom and Download.validTo matching the current time. • The ‘ReportInfo’ is selected to ‘TriggeredReporting’.

Test Procedure	• Power-on the Terminal and activate the BCAST client. o The Terminal receives the SGDD. • The Terminal receives a SMS trigger message type ‘1’ over the interaction channel. o The terminal authenticates the server by mapping the AMTrigger.serverAddressURL in the SMS trigger message with the ServerAddressURL of AudienceMeasurement.CampaignInfo element received in the SGDD. • The Terminal asks the user to “Accept” or “Refuse” to participate the AM campaign. The user selects “Accept”. o The Terminal sends the “Opt-in” (‘userConsent’ = “True”) in the AM Request message to the AM-server. • The AM-server responds with the AM Response message that includes the AM Configuration Data. • The user watches the TV content. o The terminal measures the content consumption. • The Terminal receives a SMS trigger message type ‘2’ o The terminal authenticates the server by mapping the Download.url in the SMS trigger with the ServerAddressURL of the AudienceMeasurement.CampaignInfo element in the SGDD. • The Terminal sends an HTTP(S) request to the URL indicated in the field ‘Download.url of the SMS trigger type ‘2’. • The AM ‐ server responds with the AMRT message. • The terminal sends an AMRD message that includes the consumption report. o The terminal continues the consumption measurement during the reporting. • The AM-server sends an AMRR message to the Terminal. (Optional)
Pass-Criteria	• The AM ‐ server authentication is successful (for SMS trigger type ‘1’). • The user is presented with an option to either “Accept” or “Refuse” the campaign. • As a result of user accepting the campaign, the AM-server receives AM Request message from the Terminal with ‘userConsent’ = “True”. • The AM-server authentication is successful (for SMS trigger type ‘2’). • The AM-server receives the AMRD message after the AMRT initiated reporting. The consumption report corresponds to the user activity.

9.1.4 Server initiated silent Opt-out for an active AM campaign (SMS triggered)

Test Case Id	BCAST-1.1-TCAM-int-104
Test Object	BCAST Terminal / AM-server

Test Case Description	Test that user participation in the ongoing AM campaign is succesfully closed (initiated by the server 'silent Opt-out') using SMS –based AM Trigger.
Specification Reference	[BCAST11–Services], section 5.20.1 [BCAST11-SG], section 5.4.1.5.2
SCR Reference	BCAST-AM-C-003, BCAST-AM-C-005, BCAST-AM-C-011, BCAST-AM-C-013, BCAST-AM-C-015, BCAST-AM-C-021, (BCAST-AM-C-023) BCAST-AM-M-003, BCAST-AM-M-005, BCAST-AM-M-010, BCAST-AM-M-012, BCAST-AM-M-017, (BCAST-AM-M-019)
ETR Reference	AMT-001 to AMT-014
Tool	None
Test code	None
Preconditions	• The user is participating in an AM Campaign. • The SMS trigger message type '1' contains: o AMTrigger.flags bit 5 signaling that the 'consentRequired'is "False". o AMTrigger.serverAddressURL matching the ServerAddressURL of the AudienceMeasurement.CampaignInfo element in the SGDD.
Test Procedure	• The Terminal receives a SMS trigger message type '1' over the interaction channel. o The terminal authenticates the server by mapping the AMTrigger.serverAddressURL in the SMS trigger message with the ServerAddressURL of AudienceMeasurement.CampaignInfo element received in the SGDD. • The Terminal silently responds with an AM Request message. • The AM-server sends an AM Response message to the Terminal with campaignEndTime set to past. • The Terminal compares the campaignEndTime with its current time and stops the Audience Measurement campaign. o The Terminal sends an AMRD message that includes the consumption report of all the remaining measured but not-reported data. (Optional) o The AM-server responds with an AMRR message to the Terminal. (Optional)
Pass-Criteria	• The AM – server authentication is successful (SMS trigger type '1'). • The AM campaign is stopped in the terminal. • The user/terminal combination is not in the panel of active users of the campaign in the AM-server. 2.

9.1.5 Blocking of Audience Measurement for a particular service/content

Test Case Id	BCAST-1.1-TCAM-int-105

Test Object	BCAST Terminal / AM-server
Test Case Description	Test that the Audience Measurement is blocked for a particular TV program content even if the user has accepted ‘Opt-in’ for an AM Campaign (i.e., test the usage of “amAllowed” attribute in the Service Guide).
Specification Reference	[BCAST11–Services], section 5.20.1 [BCAST11-SG], section 5.4.1.5.2
SCR Reference	BCAST-AM-C-012, BCAST-AM-C-034 BCAST-AM-M-042
ETR Reference	AMT-003, AMT-008, AMT-014
Tool	None
Test code	None
Preconditions	• The Service Guide includes ‘amAllowed’ = “False” for “Content 2”.
Test Procedure	• The Terminal is powered-on and the BCAST client is activated. • The Terminal receives the Service Guide. • The Terminal accepts ‘Opt-in’ for the AM Campaign. • The user watches the TV programme (“Content 1”). o The Terminal measures the content consumption for “Content 1”. • The user watches the TV programme (“Content 2”). o The Terminal does not measure the content consumption for “Content 2”. • The user watches the TV programme (“Content 3”). o The Terminal measures the content consumption for “Content 3”. • The terminal sends the consumption report to the AM –server.
Pass-Criteria	• The consumption report in the AM –server corresponds to the user activity but does not include record of the consumption of “Content 2”. • The Terminal does not have a record of the consumption of “Content 2”.

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 1.1 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ETS-BCAST_INT-V1_1	23 Jun 2010	all	First draft baseline Agreed
	29 Jul 2010	5.8 all, 5.9 all, 5.10 all	Incorporated the following agreed CRs: OMA-IOP-BRO-2010-0047R01-CR_ETS_BCAST_1_1_Smartcard_Centric_AM OMA-IOP-BRO-2010-0046R01-CR_ETS_BCAST_1_1_Smartcard_Broadcast_Provisioning_ OMA-IOP-BRO-2010-0045R01-CR_ETS_BCAST_1_1_Parental_control_service_ordering_SCPExt Editorial changes
	21 Sep 2010	5, 5.1.3, 5.3.1.8,5.3.1.9, 5.3.2.5, 5.3.2.6, 5.6 all, 5.7, 5.8, 5.10.4, 6 all, 7 all	Incorporated the following agreed CRs: OMA-IOP-BRO-2010-0060-CR_BCAST_ETS_structure OMA-IOP-BRO-2010-0062R02-CR_ETS_BCAST_1_1_Service_guide_discovery_using_DNS OMA-IOP-BRO-2010-0063R01-CR_ETS_BCAST_1_1_Hybrid_file_distributio OMA-IOP-BRO-2010-0064R01-CR_ETS_BCAST_1_1_Hybrid_stream_distribution OMA-IOP-BRO-2010-0065R01-CR_ETS_BCAST_1_1_Advisable_time_ranges_for_access_switch OMA-IOP-BRO-2010-0066R01-CR_ETS_BCAST_1_1_Parental_control_service_ordering_Generic OMA-IOP-BRO-2010-0067R01-CR_ETS_BCAST_1_1_Parental_control_unicast_service_consumption
	27 Oct 2010	7all, 8 all	Incorporated the following agreed CRs: OMA-IOP-BRO-2010-0072R01-CR_ETS_BCAST_1_1_Clear_to_air_and_Control_SC_AM.doc
	08 Nov 2010	9 all	Incorporates the following CR: OMA-IOP-BRO-2010-0082-CR_Terminal_Centric_AM
Candidate Version OMA-ETS-BCAST_INT-V1_1	07 Dec 2010	n/a	Status changed to Candidate by TP TP Ref# OMA-TP-2010-0503-INP_BCAST_11_ETS_for_Candidate_Approval