Mobile Broadcast Services Architecture

Approved Version 1.0 – 12 Feb 2009

Open Mobile Alliance

OMA-AD-BCAST-V1_0-20090212-A

Contents

Figures

Tables

1. Scope (Informative)

The scope of the Mobile Broadcast Services (BCAST) architecture document is to define the architecture for the Mobile Broadcast services enabler. This architecture is based on the requirements listed for in the BCAST Requirements Document [BCAST10-Requirements].

2. References

2.1 Normative References

[3GPP TS 26.346] “Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs”, 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.346 V6,
URL: http://www.3gpp.org/

[3GPP TS 31.101] “UICC-terminal interface; Physical and logical characteristics”, 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.101 V6,
URL: http://www.3gpp.org/

[3GPP TS 31.102] “Characteristics of the Universal Subscriber Identity Module (USIM) application”, 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.102 V6,
URL: http://www.3gpp.org/

[3GPP TS 33.220] “Generic Authentication Architecture, Generic Bootstrapping Architecture”, 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.220 V6,
URL: http://www.3gpp.org/

[3GPP TS 33.246] “Security of Multimedia Broadcast/Multicast Service”, 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.246 V6,
URL: http://www.3gpp.org/

[3GPP TS 51.011] “Subscriber Identity Module – Mobile Equipment (SIM-ME) interface”, 3rd Generation Partnership Project, Technical Specification 3GPP TS 51.011 V5,
URL: http://www.3gpp.org/

[3GPP2 C.S0023] "Removable User Identity Module for Spread Spectrum Systems", 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0023-B,
URL: http://www.3gpp2.org/

[3GPP2 C.S0065] “cdma2000 Application on UICC for Spread Spectrum Systems”, 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0065-0,
URL: http://www.3gpp2.org/

[3GPP2 S.S0083] “Broadcast-Multicast Service Security Framework”, 3rd Generation Partnership Project 2, Technical Specification 3GPP2 S.S0083-A,
URL: http://www.3gpp2.org/

[3GPP2 X.S0022] “Broadcast and Multicast Service in cdma2000 Wireless IP Network”, 3rd Generation Partnership Project 2, Technical Specification 3GPP2 X.S0022-0,
URL: http://www.3gpp2.org/

[BCAST10-BCMCS-Adaptation] "Broadcast Distribution System Adaptation – 3GPP2/BCMCS", Open Mobile Alliance™, OMA-TS-BCAST_BCMCS_Adaptation-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST10-Distribution] "File and Stream Distribution for Mobile Broadcast Services ", Open Mobile Alliance™, OMA-TS-BCAST_Distribution-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST10-DVBH-IPDC-Adaptation] "Broadcast Distribution System Adaptation – IPDC over DVB-H", Open Mobile Alliance™, OMA-TS-BCAST_DVB_Adaptation-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST10-ESG] "Service Guide for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_ServiceGuide-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST10-MBMS-Adaptation] "Broadcast Distribution System Adaptation – 3GPP/MBMS", Open Mobile Alliance™, OMA-TS-BCAST_MBMS_Adaptation-V1_0, URL: http://www.openmobilealliance.org/

[BCAST10-Requirements] "Mobile Broadcast Services Requirements", Open Mobile Alliance™, OMA-RD-BCAST-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST10-ServContProt] "Service and Content Protection for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_SvcCntProtection-V1_0,
URL: http://www.openmobilealliance.org/

[BCAST10-Services] "Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_Services-V1_0,
URL: http://www.openmobilealliance.org/

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

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

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

[ETSI EN 300 468] Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems, ETSI EN 300 468 V1.x.x,
URL: http://www.etsi.org/

[FIPS197] ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197,
URL: http://csrc.nist.gov/publications/fips/

[FIPS198] The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198,
URL: http://csrc.nist.gov/publications/fips/

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

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

[OSE] “OMA Service Environment”
URL: http://www.openmobilealliance.org/

[RFC2104] “HMAC: Keyed-Hashing for Message Authentication”, H. Krawczyk, M. Bellare, R. Canetti, February 1997,
URL: http://www.ietf.org/rfc/rfc2104.txt

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997,
URL: http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] “Augmented BNF for Syntax Specifications: ABNF”. D. Crocker, Ed., P. Overell. November 1997,
URL: http://www.ietf.org/rfc/rfc2234.txt

[RFC2327] "SDP: Session Description Protocol", M. Handley, V. Jacobson, April 1998,
URL: http://www.ietf.org/rfc/rfc2327.txt

[RFC2401] “Security Architecture for the Internet Protocol”, S. Kent, R. Atkinson, November 1998,
URL: http://www.ietf.org/rfc/rfc2401.txt

[RFC2404] “The Use of HMAC-SHA-1-96 within ESP and AH”, C. Madson, R. Glenn, November 1998,
URL: http://www.ietf.org/rfc/rfc2404.txt

[RFC2406] “IP Encapsulating Security Payload (ESP)”, S. Kent, R. Atkinson, November 1998,
URL: http://www.ietf.org/rfc/rfc2406.txt

[RFC2451] “The ESP CBC-Mode Cipher Algorithms”, R. Pereira, R. Adams, November 1998,
URL: http://www.ietf.org/rfc/rfc2451.txt

[RFC3394] “Advanced Encryption Standard (AES) Key Wrap Algorithm”, J. Schaad, R. Housley, September 2002,
URL: http://www.ietf.org/rfc/rfc3394.txt

[RFC3566] "The AES-XCBC-MAC-96 Algorithm and Its Use With IPSec", S. Frankel, H. Herbert, September 2003,
URL: http://www.ietf.org/rfc/rfc3566.txt

[RFC3602] "The AES-CBC Cipher Algorithm and Its Use with IPSec", S. Frankel, R. Glenn, S. Kelly, September 2003,
URL: http://www.ietf.org/rfc/rfc3602.txt

[RFC3664] "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", P. Hoffman, January 2004,
URL: http://www.ietf.org/rfc/rfc3664.txt

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

2.2 Informative References

[OMADICT] "OMA Dictionary", OMA-Dictionary-V2_1-20040914-A,
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 [RFC 2119].

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

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

3.2 Definitions

(U)SIM A SIM or a USIM application residing in the memory of the UICC.

BCAST Service Application Represents the service application of the BCAST Service, such as streaming audio/video or movie download.

BCAST Service Distribution/Adaptation Responsible for the aggregation and delivery of BCAST Services, and performs the adaptation of the BCAST Enabler to underlying Broadcast Distribution Systems.

BCAST Subscription Management Responsible for service provisioning such as subscription and payment related functions, the provision of information used for BCAST Service reception, and BCAST device management.

BDS Service Distribution Responsible for the coordination and delivery of broadcast services to the BDS for delivery to the terminal, including file and streaming distribution, and Service Guide distribution.

Broadcast Channel The logical channel (usually uni-directional) that provides Broadcast Transport which the Broadcast Enabler uses for broadcast distribution of data to Mobile Terminals.

Typically, the Broadcast Channel supports high bitrates. It is inherently used for downlink purposes and is particularly useful for conveying information that is targeted to all or many Mobile Terminals.

The Broadcast Channel is implemented by a Broadcast Distribution System that can efficiently distribute IP-based services to Mobile Terminals. Typically, this means that a broadcast-capable bearer is used as the underlying network technology.

Broadcast transport mechanisms allow simultaneous distribution of content to many recipients. This requires that all receivers can “receive” the same physical resource (link or radio frequency) and can simultaneously connect to the same transport protocol. Broadcast transport can be accomplished using both broadcast and multicast mechanisms in the underlying broadcast distribution system.

Broadcast Distribution System A system containing the ability to transmit the same IP flow to multiple Terminal devices simultaneously. A Broadcast Distribution System (BDS) typically uses techniques that achieve efficient use of radio resources. A BDS consists of Broadcast/Multicast Network functionality up to the IP layer and optional Service Distribution/Adaptation functionality above the IP layer.

Broadcast Roaming Broadcast Roaming is the ability of a user to receive broadcast services from a Mobile Broadcast Service Provider different from the Home Mobile Broadcast Service Provider with which the user has a contractual relationship.

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

Examples of Broadcast Services are:

pure Broadcast Services:
- mobile TV
- mobile newspaper
- mobile file downloading (clips, games, SW upgrades, other applications, applications)

combined broadcast/interactive Broadcast Services:

- mobile TV for file downloading with voting
- betting Broadcast Services
- auction Broadcast Services
- trading Broadcast Services

Component A Function is further decomposed into Components. Components are used to separate logically separate parts within the Function. This decomposition is helpful in architecture and specification work.

Content Encryption The cipher algorithms applied on data before packetisation for transport or encapsulations in a file occur.

Content Protection This involves the protection of content (files or streams) during the complete lifetime of the content i.e. it is NOT an access control mechanism only as it involves post-acquisition rules. Content protection is enabled for encrypted content through the use of appropriate rules or rights, e.g. using OMA DRM v2.0 for files and OMA DRM Broadcast extensions for streamed content. Content remains protected in the Terminal.

Usage rules are enforced at "consumption time" (typically, based on DRM). In addition to subscription and pay-per-view, typically associate with Service Protection, Content Protection enables also more fine-grained usage rules, such as for displaying, saving in unencrypted form, printing, processing, re-distributing, etc. [DRM v2.0].

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

Device Management Management of the Device configuration and other managed objects of Devices from the point of view of the various Management Authorities.

Digital Rights Management The means to control the usage of media object once it has been downloaded. DRM enables content providers to define rights for media objects. It is possible to associate different rights with a single media object. The rights are required in order to use the media object.

DRM Profile The DRM profile uses the Service & Content Protection solution for BCAST receivers in which the long term key management and registration of devices is based on OMA DRM and the broadcast extensions [XBS DRM extensions-v1.0].

For further details, see [BCAST10-ServContProt].

File Distribution Function The File Distribution Function distributes a file or a bundle of files having any type or any encoding scheme to Terminals.

Function The Mobile Broadcast Service Enabler consists of several Functions. Functions provide finer granularity than Enabler. Function covers a particular end-to-end functionality within the Enabler. For example, Service Guide is a Function that belongs to Mobile Broadcast Service Enabler.

Interaction network A system containing the ability to transmit, for example IP flow, SMS, MMS, through Interaction Channel to a Terminal device and transmitting user's responses through Interaction Channel to a BCAST Service Application. A system containing the ability to transmit IP flow through Interaction Channel to a Terminal device

Interface The common boundary between two associated systems (source: GSM 01.04, ITU-T I.112).

Network Broadcast /Interactive Network for distribution and interaction BCAST services.

Notification Function The Notification Function is responsible for informing a terminal or a group of terminals of the upcoming event about Broadcast Service.

OCSP Online Certificate Status Protocol, RFC 2560,

http://www.ietf.org/rfc/rfc2560.txt Also,

OMA Online Certificate Status Protocol (profile of [OCSP]) V 1.0,

http://www.openmobilealliance.org/

Programme A logical portion of a service with a distinct start and end

R-UIM A Removable User Identity Module corresponds to a non-UICC platform based module as defined in [3GPP2 C.S0023] to register services provided by 3GPP2 mobile networks with the appropriate security.

Reference Point A conceptual point at the conjunction of two non-overlapping functional groups (source: ITU-T I.112). It consists of none or any number of interfaces of any kind.

RI (Rights Issuer) An entity that issues Rights Objects to OMA DRM Conformant Devices.

RO (Rights Object) This is a Rights Object used by DRM profile of the Service and Content Protection. RO is delivered over Interactivity Channel. Encoding of the RO is specified in [DRMDRM-v2.0].

Service Guide Fragment An atomic information component of the Service Guide, which can be compressed, encapsulated and transported in the absence of other parts of the Service Guide.

Service Guide Function The Service Guide Function provides the broadcast users with information on the various broadcast contents available in their region

Service Interaction Function The Service Interaction Function provides the point-to-point communication between a BCAST Service Application in the network and the terminal.

Service Protection This involves protection of content (files or streams) during its delivery, i.e., it is an access control mechanism only. Content is freely available (thus unencrypted) once securely delivered.

For the benefit of allowing Content Protection to be provided for the same service, Service Protection may be limited to immediate consumption / rendering only, allowing recording of encrypted content for future acquisition of post-acquisition rights (see Content Protection).

Service Protection and Content Protection Function The Service and Content Protection function provides a BDS-agnostic way of protecting both content and services delivered within Mobile Broadcast services.

Service Provisioning Function The Service Provisioning Function is responsible for a User subscription to a BCAST service and the payment for a User about his or her subscribed service.

SIM A Subscriber Identity Module is a standalone module defined in [3GPP TS 51.011] to register services provided by 2G mobile networks with the appropriate security.

Smartcard A non-UICC secure function platform which may contain the SIM or R-UIM module, or a UICC-based secure function platform which may contain one or more of the following applications: a 3GPP USIM or 3GPP2 CSIM.

Note that the set of applications/modules residing on the Smartcard are typically governed by the affiliation of the Smartcard to 3GPP or 3GPP2 specifications, as indicated by the definition for “Smartcard Profile”.

Smartcard Profile Alias for a set of Smartcard-based technologies and mechanisms, which provides key establishment and key management, as well as permission and token handling for the Service and Content Protection solution for BCAST Terminals. In particular, Subscriber Key establishment and both Short and Long Term Key Management may be based either (i) on GBA mechanisms and a Smartcard with (U)SIM/as defined by 3GPP, or (ii) on a pre-provisioned shared secret key and a Smartcard with R-UIM/CSIM or a UIM as defined by 3GPP2.

Stream Distribution Function The Stream Distribution Function distributes streams to Terminals.

Terminal The mobile device with which an End-User receives and consumes a Broadcast Service.

Terminal Provisioning Function The Terminal Provisioning Function manages terminal configuration parameters, e.g. data, parameters and applications with the help of OMA DM and distributes them to many terminals over Broadcast Channel.

Transport Encryption The cipher algorithm is applied on data that have been packetised for transport on a network. This can also be referred as Service Encryption but for the sake of clarity, only Transport Encryption term is used.

UICC A Universal Integrated Circuit Card is a physically removable secured device as defined in [3GPP TS 31.101] for communication purposes not restricted to mobile convenience only. It is a platform to all the resident applications (e.g., USIM or CSIM).

UIM A User Identity Module represents a standard device or functionality, which provides secure procedures in support of registration, authentication, and privacy functions in mobile telecommunications. In the context of BCAST, the UIM refers specifically to the non-removable version of this standard device or functionality that is employed by (some) mobile terminals, which operate according to 3GPP2 specifications. In addition, Smartcard Profile based Service and Content Protection functionality can be provided on UIM-equipped BCAST Terminals.

USIM A Universal Subscriber Identity Module is an application defined in [3GPP TS 31.102] residing in the memory of the UICC to register services provided by 3GPP mobile networks with the appropriate security.

3.3 Abbreviations

(U)SIM	SIM or USIM
BCMCS	Broadcast/Multicast Services
BDS	Broadcast Distribution System
BDS-SD	BDS Service Distribution
BDS-SD/A	BDS Service Distribution/Adaptation
BSA	BCAST Service Application
BSD/A	BCAST Service Distribution and Adaptation
BSI-C	BCAST Service Interaction - Client Component
BSI-G	BCAST Service Interaction - Generic Component
BSM	BCAST Subscription Management
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
CSIM	cdma2000 Subscriber Identify Module
DCF	DRM Content Format
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
LTKM	Long Term Key Message

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/Adaptation
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
PDCF	Packetised DRM Content Format
PEAK	Programme Encryption/Authentication Key
PEK	Programme Encryption Key
RI	Rights Issuer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
R-UIM	Removable User Identity Module
SA	Stream Application Component
SD	Stream Delivery Component
SD-C	Stream Delivery Client Component
SDP	Session Description Protocol
SEAK	Service Encryption/Authentication Key
SEK	Service Encryption 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
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Service Protection
SRTP	Secure Real-time Transport Protocol
STKM	Short Term Key Message
TP-C	Terminal Provisioning Client component
TP-M	Terminal Provisioning Management component
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UIM	User Identity Module
URI	Universal Resource Identified
USIM	Universal Subscriber Identity Module
VLR	Visitor Location Register
XML	Extensible Markup Language

4. Introduction (Informative)

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

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

4.1 Version 1.0

The Mobile Broadcast Services Enabler 1.0 addresses functional areas which are generic enough to be common to many Broadcast Services, and which can be defined and implemented in a bearer-independent way. These functional areas (or for short: 'functions') are the following: Service Guide, File Distribution, Stream Distribution, Service Protection, Content Protection, Service Interaction, Service Provisioning, Terminal Provisioning and Notification. Requirements for the above functional areas along with the requirements for the Enabler as whole are given in [BCAST10-Requirements]. Proposed technologies upon which this enabler is specified (e.g. for Service and Content Protection) are based on open standards, or will become part of an open standard; no proprietary parts or extensions are required. Thus, the functions described in this document fully comply with the 'Open' of the Open Mobile Alliance initiative.

This document first defines, in Section 5.2, the overall BCAST Architecture, its logical entities and reference points, respectively. The purpose of the top-level BCAST architecture is two-fold.

Firstly, it puts the BCAST Enabler in the context of underlying Broadcast Distribution Systems (BDS), service operation and content provisioning. BDSs mainly considered in the current version of BCAST architecture include: 3GPP MBMS, 3GPP2 BCMCS and DVB IPDC, not excluding any other BDSs.

Secondly, it defines the logical entities and their relations. Following the top-level definition of BCAST architecture, in section 5.3, the document individually specifies the architecture for each of the BCAST functions in detail, including the definition of functional entities and the corresponding interfaces. These interfaces in turn will be the basis of further specification as the functions are realized in BCAST Technical Specifications. Last, in Section 5.4, the document illustrates the operational side of the functions through call flow diagrams for each of the above-mentioned functions.

4.2 Security Considerations

The Mobile Broadcast Services Enabler 1.0 has two functions related to Security. The first function is Service Protection Function and the second is Content Protection function. Functional Architectures of SP and CP are described in .section 5.3.4 and the corresponding flows are described in section 5.4.4 and 5.4.5 respectively.

BCAST SP and CP are based on OMA DRM [DRMDRM-v2.0] [DRM20-Broadcast-Extensions] and 3G smartcard [3GPP TS 33.246] [3GPP2 S.S0083].

BCAST SP and CP are based on 4 Layer key management architecture, which is explained in detail [BCAST10-ServContProt]

Note: SP and CP of BCAST 1.0 have been reviewed by Security WG.

5. Architectural Model

The architectural model contains a broadcast channel, provided by a Broadcast Distribution System, and an interaction channel, provided by an Interaction Network, such as a cellular network (e.g., CDMA/GSM/GPRS/UMTS). In general, the availability of both broadcast channel and interaction channel are assumed. However, both broadcast channel and interaction channel may be temporarily unavailable, for example due to lack of radio coverage. Further, devices without access to an interaction channel are possible within the BCAST architecture and specifications. However, such devices may have limited functionality. Optimizations for devices without interactive channel are optional to implement in devices with interactive channel, and are optional to use (for details see the SCR tables of the enabler specification documents).

5.1 BCAST Enabler Functions and Dependencies

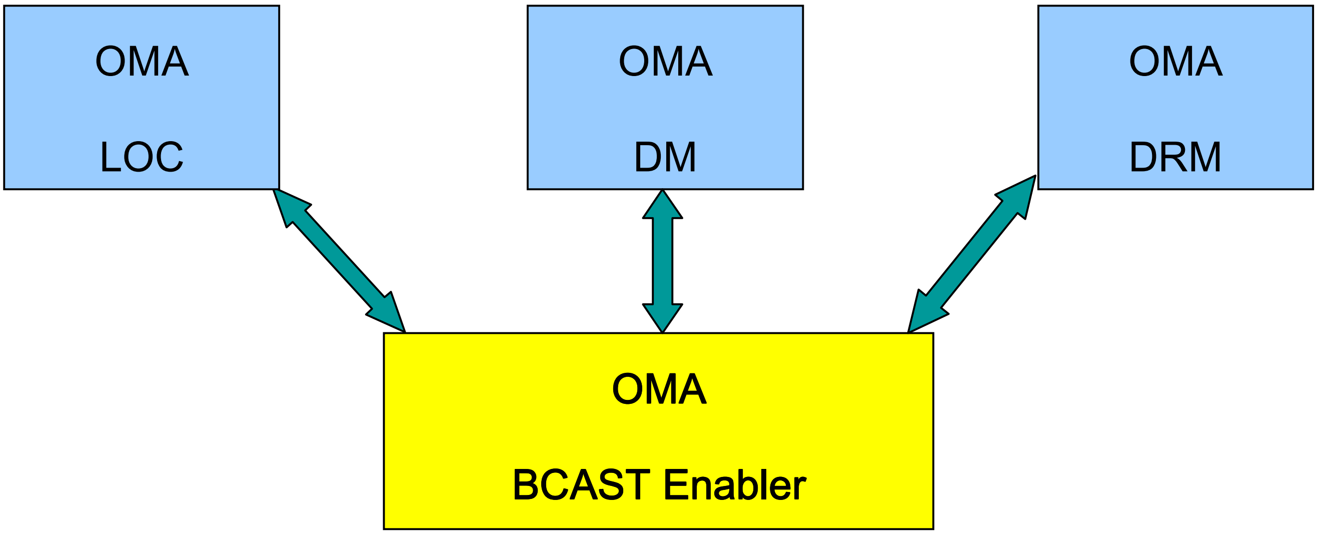


Figure 1 - Relation between BCAST Enabler and Other OMA Enablers

OMA BCAST Enabler combines a set of intrinsic functions that jointly enable the Mobile Broadcast Services. These functions are Service Guide, Stream Distribution, File Distribution, Service Protection, Content Protection, Service Provisioning, Terminal Provisioning, Interaction and Notification functions.

The BCAST Enabler partly builds on other OMA Enablers, partly enhances the existing OMA Enablers and partly defines the BCAST intrinsic functionality. Thus, as illustrated in Figure 1, the other OMA entities provide non-intrinsic functions to the BCAST Enabler. Non-intrinsic functions of other relevant OMA Entities are used as they are, or may be with extensions, according to the required functions by OMA BCAST Enabler.

The typical examples of other OMA BCAST Enablers are Location, Device Management and Digital Right Management.

OMA BCAST Enabler Functions are shown on the left side of the Figure below. These functions may be defined within OMA BCAST, or by making use of (referring to) other OMA Enablers or other existing standards.

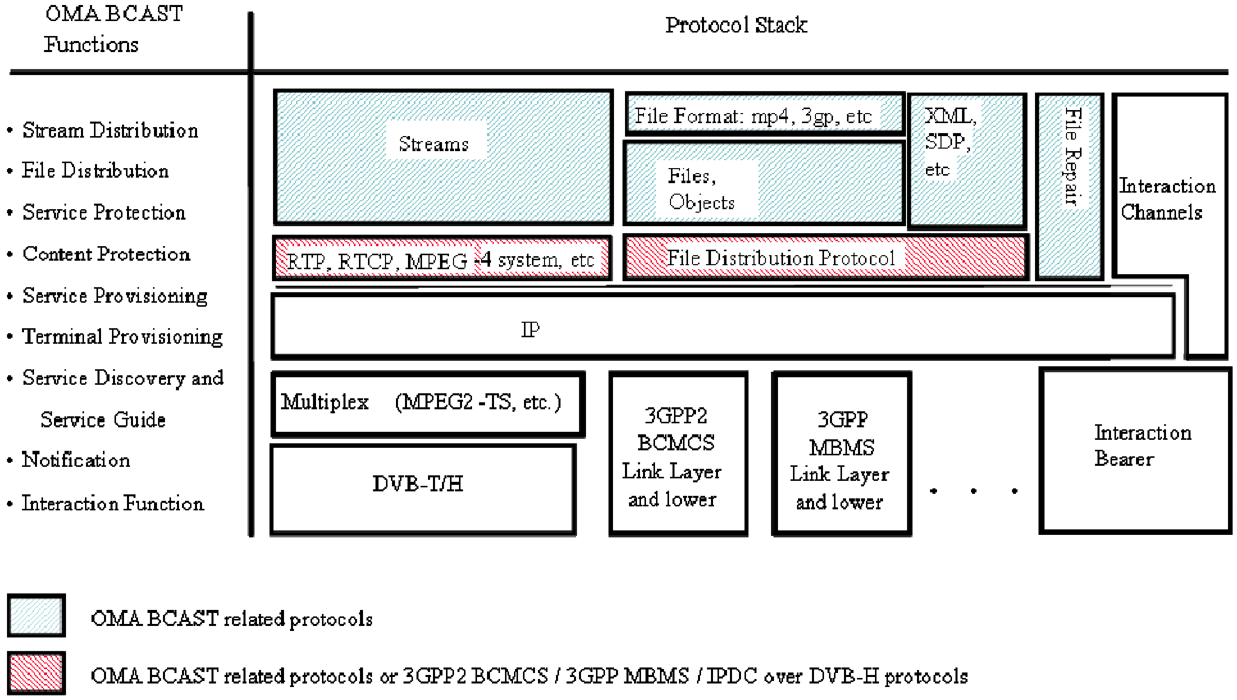

OMA BCAST Functions
Protocol Stack
• Stream Distribution
• File Distribution
• Service Protection
• Content Protection
• Service Provisioning
• Terminal Provisioning
• Service Discovery and Service Guide
• Notification
• Interaction Function
Streams
File Format: mp4, 3gp, etc
Files, Objects
XML, SDP, etc
File Repair
Interaction Channels
RTP, RTCP, MPEG -4 system, etc
File Distribution Protocol
IP
Multiplex (MPEG2 -TS, etc.)
DVB-T/H
3GPP2 BCMCS Link Layer and lower
3GPP MBMS Link Layer and lower
. . .
Interaction Bearer
OMA BCAST related protocols
OMA BCAST related protocols or 3GPP2 BCMCS / 3GPP MBMS / IPDC over DVB-H protocols

Figure 2 - BCAST Functions and Protocol Stack

The right side of the diagram shows the protocol stack of OMA BCAST. OMA BCAST Functions might make use of, interact with, enhance on, or define some protocols that are related to OMA BCAST; such protocols may include: 3GPP2 BCMCS, or 3GPP MBMS protocols.

The lower layers include one-way and two-way directional bearers; hence the BCAST enabler functions might behave differently with different types of bearers.

For example, Service and/or Content Protection might exist in IP layer (IPSec), or UDP/RTP layer (ISMACryp, SRTP, MBMS Download Protection), etc.

Stream Distribution might be over RTP/ SRT, or MPEG-4 systems over IP.

5.2 BCAST Architectural Diagram

The BCAST enabler architecture involves a collection of logical entities over a set of reference points. The BCAST functions are: Service Guide, Streaming Distribution, File Distribution, Service Protection, Content Protection, Service Provisioning, Terminal Provisioning, Interaction and Notification functions. These functions are located in the different BCAST logical entities. The following functional architectural diagram shows the relationships among the BCAST logical entities. Subsequent sections provide additional information for these entities.

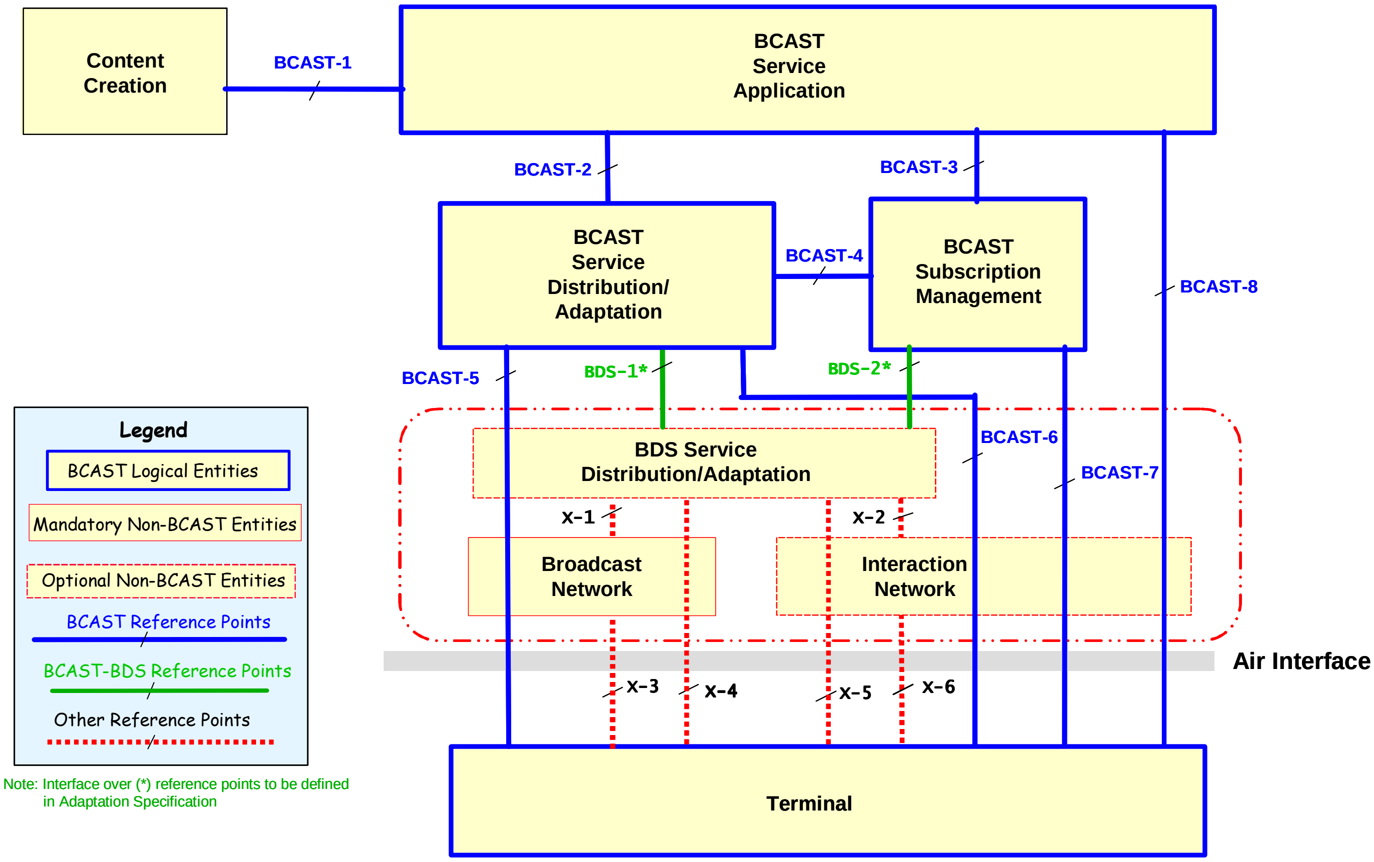

Content Creation
BCAST-1
BCAST Service Application
BCAST-2
BCAST-3
BCAST Service Distribution/ Adaptation
BCAST-4
BCAST Subscription Management
BCAST-8
BCAST-5
BDS-1*
BDS-2*
BDS Service Distribution/Adaptation
BCAST-6
BCAST-7
X-1
X-2
Broadcast Network
Interaction Network
Air Interface
X-3
X-4
X-5
X-6
Terminal
Legend
BCAST Logical Entities
Mandatory Non-BCAST Entities
Optional Non-BCAST Entities
BCAST Reference Points
BCAST-BDS Reference Points
Other Reference Points
Note: Interface over (*) reference points to be defined in Adaptation Specification

Figure 3: BCAST Functional Architecture Diagram

5.2.1 Logical Entities for BCAST Enabler

The BCAST enabler involves a collection of logical entities that work together to realize the needed capabilities. The following table presents these logical entities. The table includes entities that will be driven by the functionality defined in the BCAST enabler and other logical entities that provide services but whose definitions are defined elsewhere.

Logical Entity	Major Functionality
Entities in-scope of OMA BCAST	
BCAST Service Application	Represents the service application of the BCAST Service, such as, streaming audio/video or movie file download. It encompasses the functionality of media encoding and interaction related to BCAST Service. It also provides the BCAST service attributes to the BCAST Service Distribution/Adaptation and BCAST Subscription Management. It may generate charging information, for example, according to the user charging information that it obtains from the BCAST subscription management and the content creator. Legacy mechanisms may be used for charging information generation and delivery.
BCAST Service Distribution/Adaptation	Responsible for the aggregation and delivery of BCAST Services, and performs the adaptation of the BCAST Enabler to underlying Broadcast Distribution Systems. It provides the functionality of File and Stream Distribution, Service Aggregation, Service and Content Protection (i.e., data encryption, TEK generation, and protection

	key message distribution), Service Guide generation and delivery, Notification Delivery, and the adaptation to the underlying BDS. The functionality of adaptation to each BDS may vary depending on the underlying BDS.
BCAST Subscription Management	Responsible for service provisioning such as subscription and payment related functions, the provision of information used for BCAST Service reception, and BCAST Terminal management. It provides the functionality of Notification, Service Protection management, Content Protection management, Service Guide generation support, Terminal Provisioning and interaction with the BDS Service Distribution/Adaptation to communicate/manage subscription information with the Terminal. It may send the user charging information to the BCAST service application.
Terminal	The user device that receives broadcast content as well as the BCAST service related information, such as, service guide, content protection information. The user device may support the interactive channel in which case it would be able to directly communicate to the network regarding the available services.
Entities out-of-scope of OMA BCAST	
Content Creation	Source of content, may provide support for delivery paradigms (e.g., streaming servers); provides base material for content descriptions.
BDS Service Distribution/Adaptation	Responsible for the coordination and delivery of broadcast services to the BDS for delivery to the terminal, including file and stream distribution, and Service Guide distribution. It may also include key distribution, broadcast subscription management, and accounting functionalities. BDS Service Distribution/Adaptation may not exist in certain BDSs. In that case it would be considered a “Null Function”. It works with the interactive network to perform service discovery, BDS-specific service protection and handles other interaction functions. It also works with the BDS for content delivery to the terminal.
Broadcast Network	Specific support for the distribution of content over the broadcast channel. This may involve the same or different radio network from that used by the interactive channel.
Interaction Network	Specific support for the interaction channel. This may involve the same or different radio network from that used by the broadcast channel.

Table 1 - Descriptions of Logical Entities

5.2.2 Reference Points for BCAST Enabler

The logical entities of the BCAST enabler are connected to permit them to provide the functions needed. These points of connection establish the reference points documented in this section. As with the logical entities, certain of these reference points will be fully defined as part of the BCAST enabler. The following table describes these reference points.

Reference Point	Usage
Reference Points within BCAST Scope	
BCAST-1	Content, Content attributes, Notification event, etc.
BCAST-2	Content-unprotected BCAST Service, BCAST Service attributes and content attributes pertaining to the program such as description, rating and genre.
BCAST-3	BCAST Service attributes and content attributes pertaining to service provisioning, such as, targeted user profile and location information. User preference and subscription information, User request, User reporting, notification event and maybe user charging information.
BCAST-4	Notification, Service Guide, fragments (related to provisioning, purchasing, subscription, terminal provisioning, etc.), Long Term Key Messages, Short Term Key Messages, Terminal Provisioning object, Terminal Provisioning message, Terminal management message, etc.

BCAST-5	This reference point provides the distribution of unprotected and/or protected BCAST Service, content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and content attributes Notification, Service Guide, and Security material, over the Broadcast Distribution System, which may include traversing the BDS Service Distribution/Adaptation.
BCAST-6	Unprotected and/or protected BCAST Service, content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and content attributes, Notification, Service Guide, Security material, terminal reports related to stream and file delivery, all distributed over the Interaction Network.
BCAST-7	This interface provides the delivery of Service provisioning, Subscription information, Terminal provisioning, Security material, and device registration, over the Interaction Network. For security material delivery, it is also applicable to implementations whereby the BCAST Subscription Management contains the equivalent BDS Service Distribution/Adaptation functionality pertaining to the transmission of such material over the Interaction Network.
BCAST-8	User interaction, reporting, and user preference.
BDS Specific Reference Points	
BDS-1	Unprotected and/or protected BCAST Service, content-unprotected and/or content-protected BCAST Service, BCAST Service attributes and Content attributes, BCAST Service/Content priority**, Notification, Notification priority, Service Guide and Security material. This reference point is only applicable when the underlying BDS technology is MBMS or BCMCS, and furthermore, whereby the portion of the BDS Service Distribution/Adaptation pertaining to service distribution and adaptation is not functionally integrated in the BCAST Service Distribution/Adaptation. Note: Service protection or Content Protection of RTP streams may be employed by the BDS itself, if available.
BDS-2	Service provisioning, Subscription information, Device management, Security material. This reference point is applicable when the underlying BDS technology is MBMS or BCMCS, and furthermore, whereby the portion of the BDS Service Distribution/Adaptation pertaining to subscription management is not functionally integrated in the BCAST Subscription Management.
Reference Points out of BCAST Scope	
X-1	Reference Point between BDS Service Distribution/Adaptation and BDS.
X-2	Reference Point between BDS Service Distribution/Adaptation and Interaction Network.
X-3	Reference Point between BDS and Terminal.
X-4	Reference Point between BDS Service Distribution/Adaptation and Terminal over Broadcast Channel.
X-5	Reference Point between BDS Service Distribution/Adaptation and Terminal over Interaction Channel.
X-6	Reference Point between Interaction Network and Terminal.

Table 2 - Descriptions of Reference Points

** Note: Higher priority in delivery of broadcast service/content shall be given to service/content intended for public safety/public service, or emergency information.

5.3 Functional Components and Interfaces/reference points definition

This section describes details of all BCAST Functions and Components. The architecture for each BCAST function is covered in detail, in separate sections individually, including the definition of functional entities, components and the corresponding interfaces.

5.3.1 Service Guide Function

The Service Guide Function provides the broadcast users with information on the various broadcast contents available in their region. Depending on the capabilities of the underlying Broadcast Distribution System (BDS), the broadcast content information is transmitted to the terminal either as an IP-based Service Guide, or as BDS-specific messaging, or both. The service guide may be modified according to the BDS, for example by adding BDS specific information. This may either be done in the Service Guide Generation/ Adaptation/Distribution in Broadcast Service Distribution/Adaptation, or in the BDS. The format of the Service Guide information is defined for various interfaces in the following subsections.

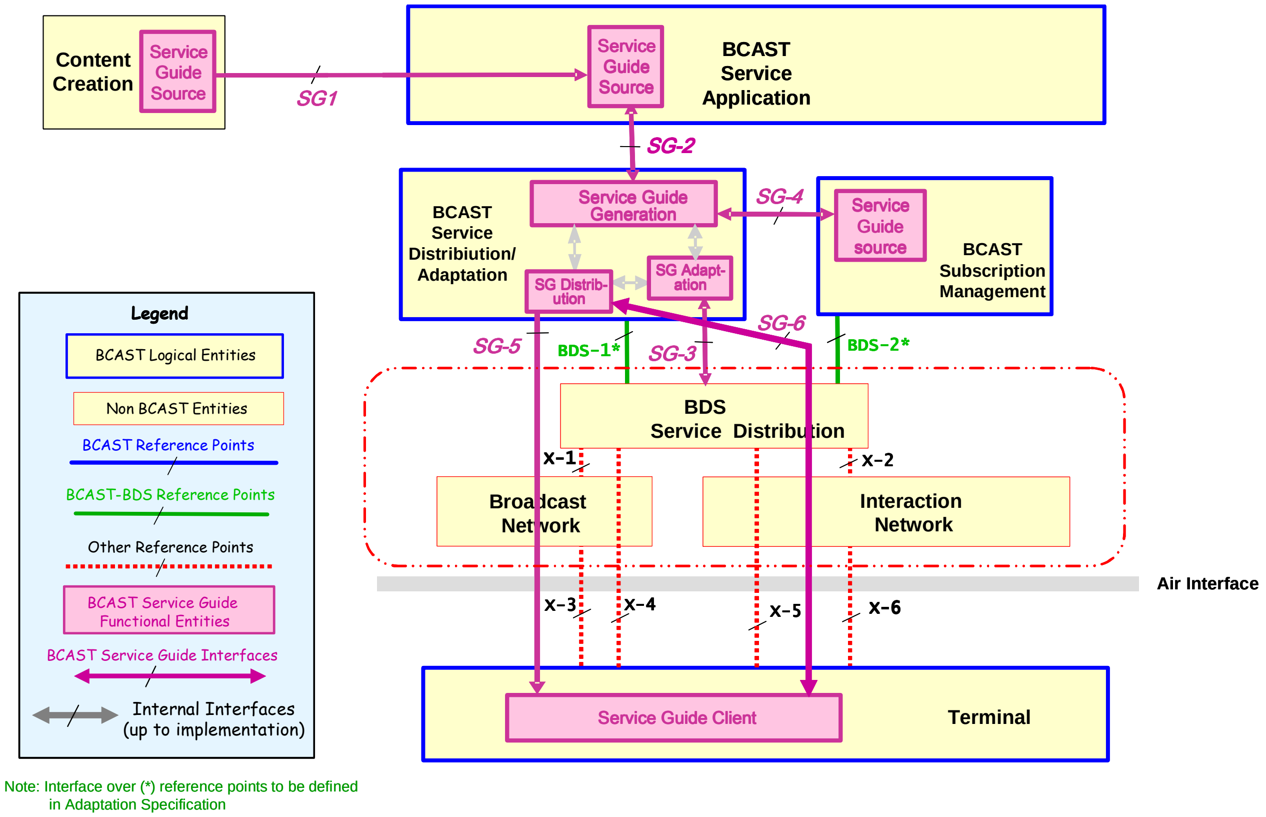


Figure 3 - Service Guide Functional Architecture

The BCAST Service Guide Functional Architecture defines the following interfaces:

Interfaces	Reference Point	Description
SG-1	BCAST-1	Server-to-server communications for delivering content attributes such as description information, location information, target terminal capabilities, target user profile, etc., from one or more SGCCS, either in the form of BCAST service guide fragments; or in a proprietary format.
SG-2	BCAST-2	Server-to-server communications for delivering BCAST content/service attributes, such as, service/content description information, scheduling information, location information, target terminal capabilities, target user profile, etc., in the form of BCAST service guide fragments.
SG-B1	BDS-1	Server-to-server communications for either delivering BDS specific attributes from BDS to BCAST Service Guide Adaptation component, to assist Service Guide adaptation to specific BDS, or to deliver BCAST Service Guide attributes to BDS for BDS specific adaptation and distribution. This interface is applicable to

		implementations whereby the underlying BDS technology is MBMS or BCMCS, and furthermore, whereby that portion of the BDS Service Distribution/Adaptation pertaining to SG distribution is not functionally integrated in the BCAST Service. Distribution/Adaptation.
SG-4	BCAST-4	Server-to-server communications for delivering service/terminal provisioning information, purchase information, subscription information, promotional information, etc., in the form of BCAST service guide fragments.
SG-5	BCAST-5	This interface provides the delivery of BCAST Service Guide over the Broadcast Distribution System, which may include traversing the BDS Service Distribution/Adaptation.
SG-6	BCAST-6	Delivery of BCAST Service Guide through Interaction Channel. Interactive access to retrieve Service Guide or additional information related to Service Guide, for example, by HTTP, SMS, or MMS.

5.3.1.1 Service Guide Source

Service Guide Source in the network exists in various functional entities.

In Content Creation, Service Guide Content Creation Source (SGCCS) may provide contents attributes such as content description information, target terminal capabilities, target user profile, content timing information, file metadata, etc, and sends them over SG1 in the form of standardized BCAST Service Guide fragments, or in a proprietary format.

In BCAST Service Application, Service Guide Application Source (SGAS) provides service/content description information, scheduling information, location information, target terminal capabilities, target user profile, file metadata, etc., and sends them over SG2 in the form of standardized BCAST Service Guide fragments. In case of multiple SGCCSs (including exclusive SGCCSs arranged by the service provider), SGAS acts as an interception point of all received content information and is responsible for combining such content information in a manner that can be managed by SG-G.

In BCAST Subscription Management, Service Guide Subscription Source (SGSS) provides service/terminal provisioning information, purchase information, subscription information, promotional information, etc., and sends them over SG4 in the form of standardised BCAST Service Guide fragments.

BDS Service Distribution/Adaptation can provide specific information about BCAST service, such as, source IP address, transport session identifier, and delivery scheduling information over SG-B1. How BDS Service Distribution/Adaptation generates such information is out of the scope of BCAST.

5.3.1.2 Service Guide Generation/Adaptation/Distribution Component

The Service Guide Generation Component (SG-G) in the network is responsible for receiving Service Guide fragments from various sources, such as, SGAS, SGSS over SG-2 and SG-4 interfaces. SG-G assembles the fragments, such as, services and content access information, according to a standardized schema, and generates a Service Guide which is sent to Service Guide Distribution (SG-D) for transmission. Before transmission, it is optionally adapted in the Service Guide Adaptation Component (SG-A) to suit a specific BDS.

SG-D distributes the Service Guide in one or more of the following ways:

- SG-D generates an IP flow to transmit Service Guide over the SG5 interface and the broadcast channel (which may include traversing the BDS Service Distribution/Adaptation) to the SG-C. Before transmission, the SG-G may send Service Guide to Service Guide Adaptation (SG-A) to adapt the Service Guide to suit specific BDS, according to the BDS attributes sent by BDS Service Distribution/Adaptation over SG-B1. The adaptation might result in modification of Service Guide. Note that, for adaptation purpose, the SG-A may also send the BCAST Service Guide attributes or BCAST Service Guide fragments over SG-B1 to BDS Service Distribution/Adaptation for adaptation, this adaptation within BDS Service Distribution/Adaptation is out of the scope of BCAST
- SG-D may also receive a request for Service Guide information, and send the requested Service Guide information to the terminal directly through the interaction channel. SG-D also may filter Service Guide information from SG-G based on End User’s pre-specified profile.

- SG-D may also send the Service Guide to the BDS, which modifies the Service Guide (e.g., by adding BDS specific information), and further distributes the Service Guide to the SG-C in a BDS specific manner.

5.3.1.3 Service Guide Client Component

The Service Guide Client Component (SG-C) in the terminal is responsible for receiving the Service Guide information from the underlying BDS or the interaction network, and making the Service Guide available to the mobile terminal. The SG-C obtains specific Service Guide information. The SG-C may further filter the Service Guide information to match the terminal specified criteria, e.g. location, user profile, terminal capabilities. The file information included in the Service Guide may be forwarded to other relevant functions in the terminal. Commonly, the user may view the Service Guide information in a menu, list or tabular format.

SG-C may send a request to the network through SG-6 to obtain specific Service Guide information, or the complete Service Guide.

5.3.2 File Distribution Function

The File Distribution Function distributes a file or a bundle of files having any type or any encoding scheme to Terminals. The File Distribution Function mainly distributes a file or a bundle of files over Broadcast Channel, but it also can transmit a file or a bundle of files to Terminals over the Interaction Channel.

In addition to the distribution functionality, the File Distribution Function may use other functionalities provided by other OMA BCAST Functions. The File Distribution Function can protect a file or a bundle of files with content protection capability provided by the Content Protection Function and service protection capability provided by the Service Protection Function. The File Distribution Function provides for error resilience by different methods including in-band broadcast-based methods such as forward error correction and/or repetition as well as post-delivery methods such as file repair over interactive sessions.

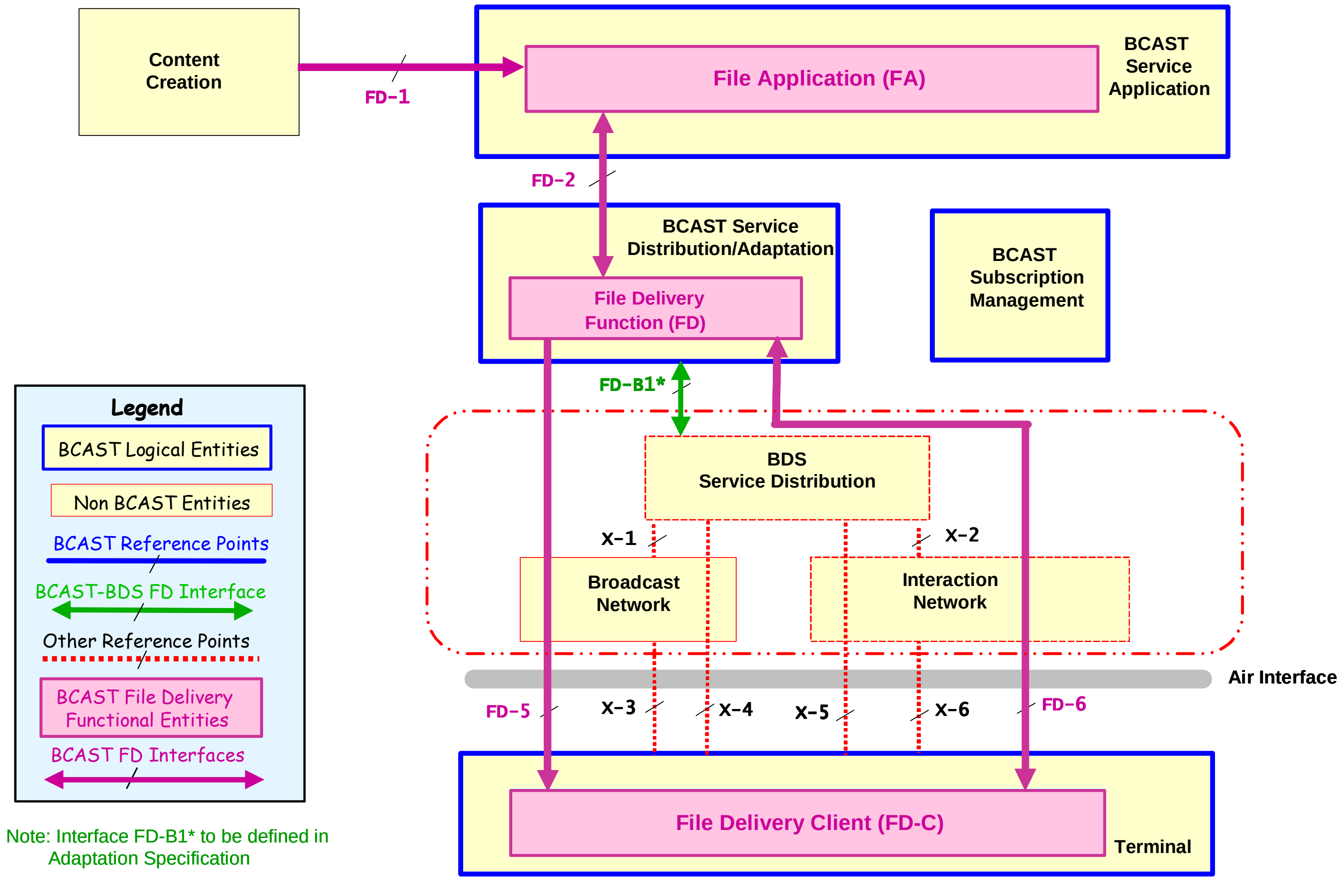


Figure 4 - File Distribution Functional Architecture

The BCAST File Distribution Functional Architecture defines the following interfaces:

Interfaces	Reference Point	Description
FD-1	BCAST-1	Delivery of a file, whose type and encoding scheme may be agnostic to BCAST Standard.
FD-2	BCAST-2	Delivery of a file (or files) or a content protected file (or files) to FD. Delivery of an attribute of a file (or files) to FD.
FD-5	BCAST-5	Unidirectional delivery of a file or a bundle of files some of which may be content protected. Unidirectional delivery of a content and service protected file or a bundle of files. Unidirectional delivery of in-band signalling for File Distribution (e.g., signalling used for file reception either in SG or in-band signalling).
FD-6	BCAST-6	Point-to-point delivery of file parts needed in order to reconstruct a complete file or file bundle on the terminal side following reception of file parts over the broadcast channel. Point-to-Point delivery of a file or a bundle of files. Delivery of a request or a report about file repairing from Terminal.
FD-B1	BDS-1	Delivery of a file or a bundle of files to BDS. Delivery of a service and/or content protected file or a bundle of files to BDS. Delivery of signalling information to a file or bundle of files distribution. Delivery of bearer information used for a file or bundle of files distribution. Signalling of file content priority** to the underlying BDS. This interface is applicable to implementations whereby the underlying BDS technology is MBMS or BCMCS, and furthermore, whereby that portion of the BDS Service Distribution/Adaptation pertaining to file and file metadata distribution is not functionally integrated in the BCAST Service Distribution/Adaptation. Note: If BDS Service Distribution/Adaptation does not exist, then the interface defined for FD-B1 is applied for x-1 and/or x-2.

** Note: Higher priority in delivery of broadcast service/content shall be given to service/content intended for public safety/public service, or emergency information.

5.3.2.1 File Application Component

The File Application Component (FA) in the network is responsible for receiving a file or a bundle of files to be broadcast from the Content Creation and sending the file as well as file attributes (e.g., the type of file and valid period of file) and additional information (e.g., location information and attributes relevant to user profile and preferences) to BCAST Service Distribution/Adaptation.

FA is agnostic to the type and encoding scheme of file delivered over the FD-1 interface.

If the content protection is done by BCAST, the FA may cooperate with the Content Protection function to encrypt the file.

5.3.2.2 File Delivery Component

The File Delivery Component (FD) in the network is responsible for the delivery, aggregation, and adaptation of a file or a bundle of files.

FD receives a file, a bundle of files, some of which may be content protected. FD receives these files with attributes from FA through the FD-2.

File delivery may take place in one of the following modes:

a) BDS Transparent mode: Using configured attributes and attributes received from FA, FD negotiates the bearers to be used for file distribution in cooperation with BDS Service Distribution/Adaptation through the interface FD-B1. If BDS Service Distribution/Adaptation does not exist, then X-1 or X-2 can be used in place of FD-B1 (X-1 and X-2 are within the scope of adaptation specification). FD normally delivers IP flows (containing a file or bundle of files) to Terminals via FD-5. If FD receives a request for retransmission or error reporting form Terminal, FD may transmit parts of a file or parts of a bundle of files over Interaction Channel via FD-6 or broadcast channel via FD-5.

b) BDS Assisted mode 1: In this mode, the BDS Service Distribution/Adaptation manipulates the file content received from the FD over FD-B1, at the application data level, before it distributes the content to the terminal. These operations are out of scope of OMA BCAST.

c) BDS Assisted mode 2: In this mode, the BDS Service Distribution/Adaptation does not manipulate the file content received from the FD over FD-B1, at the application data level, before it distributes the content to the terminal. However, the BDS Service Distribution/Adaptation may perform lower layer processing such as application layer FEC encoding, transport protocol conversion, and unicast-to-multicast IP address translation. These operations are out of scope of OMA BCAST.

FD can aggregate files transmitted from different FAs according to provisioning information and adapt a file or a bundle of files for BDS.

In the BDS transparent mode, the FD takes responsibility for error efficient and error resilient file delivery. Consequently, FD may employ different schemes for improving file delivery success, such as, repetition and forward error correction. The FD may support file-repair components allowing clients which could not fully receive a file or file bundle through broadcast channels to ask for missing file parts in order to reconstruct the file.

If the service protection is done by BCAST, the FD may cooperate with the Service Protection function to encrypt the bearer to be used for file delivery.

5.3.2.3 File Delivery Client Component

The File Delivery Client Component (FD-C) in the terminal is responsible for receiving a file or bundle of files over Broadcast Channel or Interaction Channel through either the FD-5 or FD-6 interfaces or via the BDS (in case of BDS-assisted file delivery).

If the service protection is done by BCAST, the FD-C may cooperate with the Service Protection function to decrypt the bearer containing the file. If the content protection is done by BCAST, the FD-C may cooperate with the Content Protection function to decrypt the file.

If BDS-transparent mode is used, FD-C should be able to receive the FD transmission as it is coded for error resilience

FD-C forwards the information about file received from either in-band or from SG to a relevant function.

For post error recovery the terminal may be able to request missing parts of encoded files in order to fully reconstruct the delivered files.

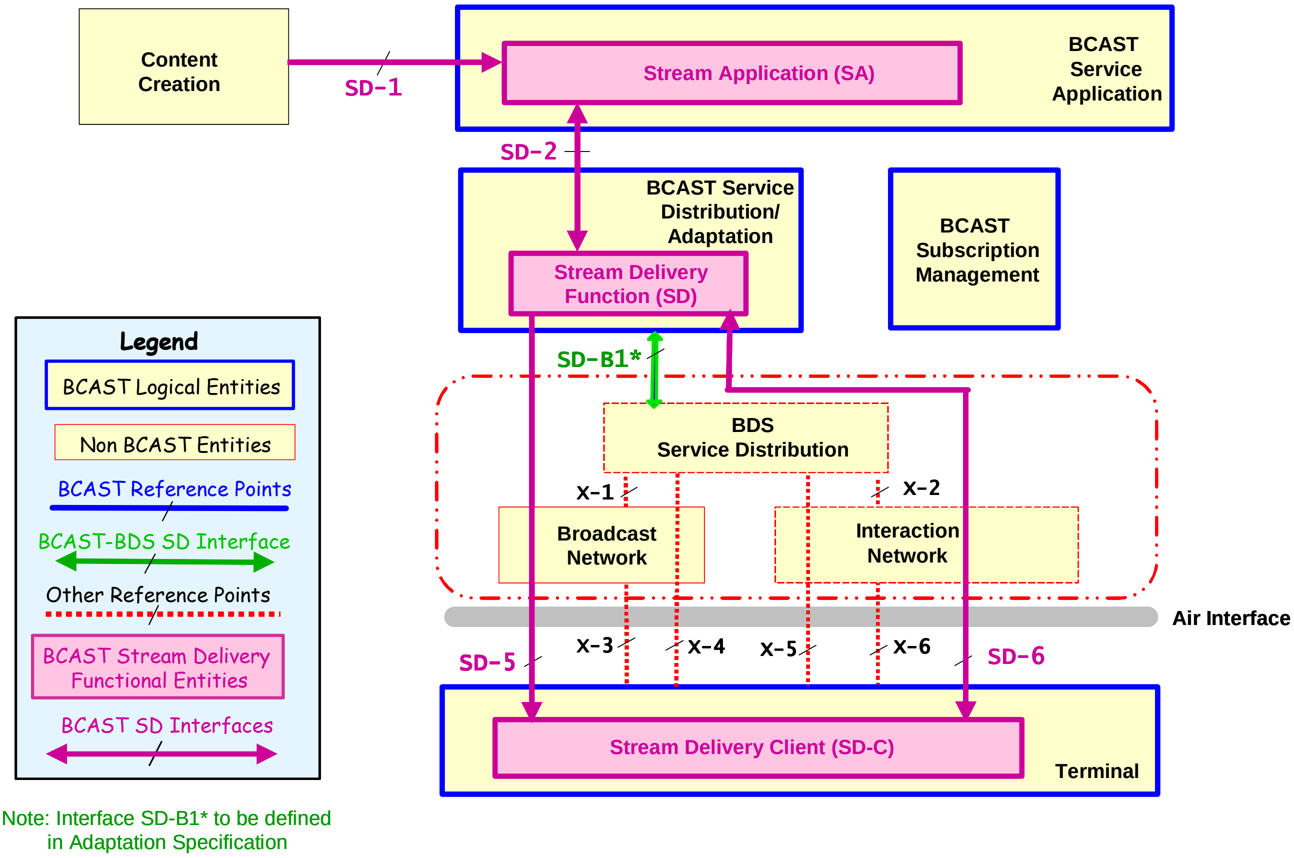
FD-C may send a report about the reception status of a file or a bundle of files, if the Terminal has the interaction ability.

5.3.3 Stream Distribution Function

The Stream Distribution Function distributes streams having CODEC used by BDS to Terminals. The Stream Distribution Function mainly distributes stream over Broadcast Channel; but it can also transmit stream to Terminal over Interaction Channel.

In addition to the distribution functionality, the Stream Distribution Function may perform the Service Protection / Content Protection encryption capability provided by the Service Protection / Content Protection Function. The Stream Distribution Function may provide for error resilience by different methods such as forward error correction coding.

The Stream Distribution Function has CODECs, which are used by BDS.



Note: Interface SD-B1* to be defined in Adaptation Specification

Figure 5 – Stream Distribution Functional Architecture

The BCAST Stream Distribution Functional Architecture defines the following interfaces:

Interfaces	Reference Point	Description
SD-1	BCAST-1	Delivery of an unprocessed stream for BCAST streaming Service. Delivery of stream with media type and CODEC supported by BCAST.
SD-2	BCAST-2	Delivery of a stream having BCAST standard media type and CODEC. Delivery of stream attributes to Stream Distribution. Function in BCAST Service Distribution/Adaptation.
SD-5	BCAST-5	This interface provides the delivery of streams over the Broadcast Distribution System, which may include traversing the BDS Service Distribution/Adaptation.

SD-6	BCAST-6	Delivery of a stream to terminal. Delivery of report about a stream reception. Delivery of request from terminal, e.g., request for the retransmission of a whole stream.
SD-B1	BDS-1	Delivery of a stream to BDS. Delivery of a protected stream to BDS. Delivery of a stream attribute to determine bearers used for stream distribution. Delivery of bearer information used for a stream distribution. Delivery of a BDS specific profile for the adaptation of Stream to BDS. Signalling of stream content priority** to the underlying BDS. This interface is applicable to implementations whereby the underlying BDS technology is MBMS or BCMCS, and furthermore, whereby that portion of the BDS Service Distribution/Adaptation pertaining to stream distribution is not functionally integrated in the BCAST Service Distribution/Adaptation. Note: If BDS Service Distribution/Adaptation does not exist, then the interface defined for FD-B1 is applied for x-1 and/or x-2.

** Note: Higher priority in delivery of stream content shall be given to service/content intended for public safety/public service, or emergency information.

5.3.3.1 Stream Application Component

The Stream Application Component (SA) in the network is responsible for transmission of a stream having BCAST standard media type and CODEC, as defined by BDS, to Stream Distribution Function in BCAST Service Distribution/Adaptation.

SA receives an unprocessed stream, to be encoded by CODEC supported by OMA BCAST, from Content Creation via SD-1. In this case, SA translates unprocessed stream into BCAST standardized stream.

SA may receive a stream encoded by CODEC supported by OMA-BCAST.

SA provides the attributes of stream (e.g., a media type of stream and required data rate) and additional information (e.g., location information and attributes relevant to user profile and preferences) used for BCAST service.

5.3.3.2 Stream Delivery Component

The Stream Delivery Component (SD) in the network is responsible for the delivery of a media stream, the determination of bearers used for stream transmission and the adaptation of a stream to a specific BDS.

SD receives a stream with attributes of a stream from SA via SD-2. Stream delivery may take place in one of the following modes:

a) BDS Transparent mode: Using configured attributes and attributes received from SA, SD negotiates the bearers to be used for stream distribution in cooperation with BDS Service Distribution/Adaptation through the interface SD-B1. If BDS Service Distribution/Adaptation does not exist, then X-1 or X-2 can be used in place of SD-B1. SD normally transmits IP flows (containing a stream) to Terminals via SD-5.

b) BDS Assisted mode 1: In this mode, the BDS Service Distribution/Adaptation manipulates the file content received from the SD over SD-B1 at the application data level, before it distributes the content to the terminal. These operations are out of scope of OMA BCAST.

c) BDS Assisted mode 2: In this mode, the BDS Service Distribution/Adaptation does not manipulate the stream content received from the SD over SD-B1 at the application data level, before it distributes the content to the terminal. However, the BDS Service Distribution/Adaptation may perform lower layer processing such as the application of native BDS service protection, and unicast-to-multicast IP address translation. These operations are out of scope of OMA BCAST.

SD may transcode the OMA BCAST stream into BDS specific stream according to BDS request over the interface SD-B1. SD also can adapt the data rate of stream according to reporting of BDS network condition over the interface SD-B1. If SD-B1 does not exist, then X-1 or X-2 can be used.

If the Service or Content Protection is done by BCAST, the SD may cooperate with the Service or Content Protection function to encrypt the bearer to be used for stream delivery.

SD transmits in-band signalling used for the stream reception and Service or Content Protection (or content protection of RTP streams) through the interface SD-5 and provides the method for media synchronization.

SD can provide the method for adaptive reception and can imply techniques for error resilience based on the characteristics specific to a Broadcast service and a Broadcast Channel.

5.3.3.3 Stream Delivery Client Component

The Stream Delivery Client Component (SD-C) in the terminal is responsible for receiving a stream over Broadcast Channel or Interaction Channel through either the SD-5 interface or via the BDS (in case of BDS-assisted stream delivery)

If the Service or Content Protection is done by BCAST, the SD-C may cooperate with the Service or Content Protection function to decrypt the bearer containing the stream. The SD-C does the operation for error resilience method if error resilience method is applied by SD.

SD-C has the capability for media synchronization and may have the method for adaptive reception.

SD-C forwards the information about a stream to a relevant function.

For post error recovery, SD-C may send the report of a stream reception if the interaction network is available.

Service and Content Protection Functions

5.3.4 Service Protection and Content Protection Functions

5.3.4.1 Overview

The Service and Content Protection functions provide a BDS-agnostic way of protecting both content and services delivered within Mobile Broadcast services. The Figure below illustrates the difference between Service Protection and Content Protection.

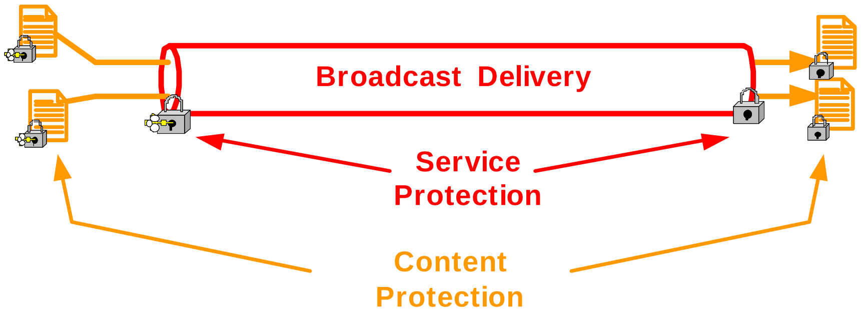


Figure 6 – Roles of Service and Content Protection

Service protection has the purpose of allowing access to a service, i.e., for a defined set of (audio-visual) data for a specified amount of time. Service protection assumes no responsibility for content after have been released to the user terminal; it does not provide any technical means to protect content outside of the bit-pipe that is implementing access control.

Content protection has the purpose of securing the individual pieces of content. Content may or may not have post-delivery usage rights associated with it.

Service Protection, independent from Content Protection, is intended for subscription management. In the absence of content protection, usage rights to content in general may be free, or subject to applicable legislation, business model or other requirements; however such considerations are beyond the scope of these definitions. Content Protection deals with post-delivery usage rights, which specify how contents can be used according to permissions and constraints.

5.3.4.2 Key Hierarchy

The figure below presents the key hierarchy for service protection and content protection.

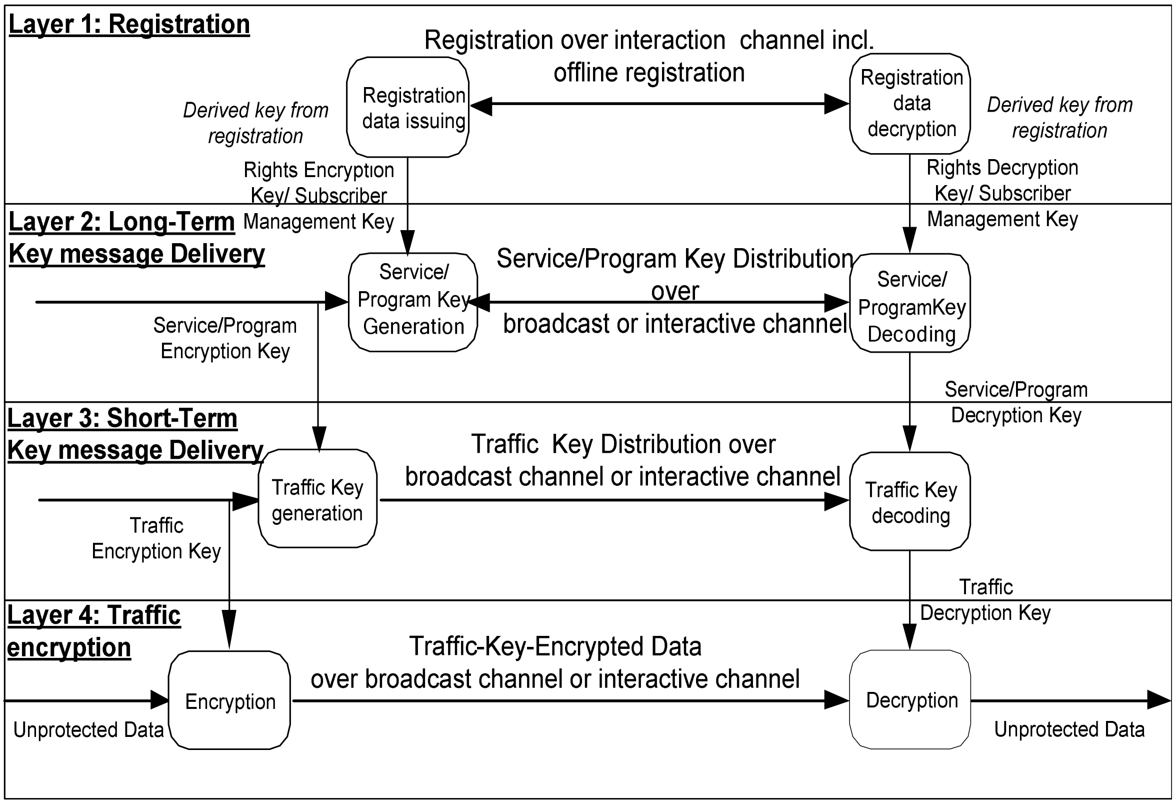

Layer 1: Registration
Registration over interaction channel incl. offline registration
Derived key from registration
Registration data issuing
Registration data decryption
Derived key from registration
Rights Encryption Key/ Subscriber Management Key
Rights Decryption Key/ Subscriber Management Key
Layer 2: Long-Term Key message Delivery
Service/ Program Key Generation
Service/Program Key Distribution over broadcast or interactive channel
Service/ ProgramKey Decoding
Service/Program Encryption Key
Service/Program Decryption Key
Layer 3: Short-Term Key message Delivery
Traffic Key generation
Traffic Key Distribution over broadcast channel or interactive channel
Traffic Key decoding
Traffic Encryption Key
Traffic Decryption Key
Layer 4: Traffic encryption
Encryption
Traffic-Key-Encrypted Data over broadcast channel or interactive channel
Decryption
Unprotected Data
Unprotected Data

Figure 7 – Key Hierarchy for Service Protection and Content Protection of RTP streams

Layer 1 implements registration step. The key material and meta-data acquired during the subscriber identity (SI) or device registration phase will enable the subscriber or device to be authenticated. They are securely stored within a secure storage entity. The key material obtained in Layer 1, and used to protect the Long Term Key delivery in Layer 2, is referred to as the Subscriber Management Key or Rights Encryption Key depending on the key management profile.

Layer 2 implements Long-Term Key Message key (LTKM) delivery over the broadcast or interactive channel. This layer delivers a service encryption key (SEK) or programme encryption key (PEK). The SEK or PEK is an intermediate key, i.e., it does not directly encrypt the content but instead protects the delivery of traffic encryption keys (TEKs). For management and protection of service subscriptions the SEK or PEK will be updated with normally longer crypto-period than the TEK traffic key.

Layer 3 implements Short-Term Key Message (STKM) delivery over the broadcast. The traffic encryption key (TEK), encrypted by a SEK or PEK, or necessary data that can be used for deriving the traffic key, is sent together with the identifiers that allow the traffic key to be linked with the encrypted content.

Layer 4 implements broadcast content encryption with the traffic encryption key (TEK). The encryption can be performed on network layer (i.e., IP), transport layer (e.g., UDP), session layer (e.g., RTP) or content layer (AU encryption) for the service protection.

Cryptographic keys introduced by the key hierarchy for service and content protection shall be stored within a secure storage entity to guarantee the access control, the confidentiality and the integrity of sensitive data.

Cryptographic keys, except for the TEK upon request from authorized applications, shall never be exposed outside the secure storage entity.

5.3.4.3 Functional Architecture for Service Protection

The following diagram describes Service Protection for file and stream and interfaces among BCAST logical entities.

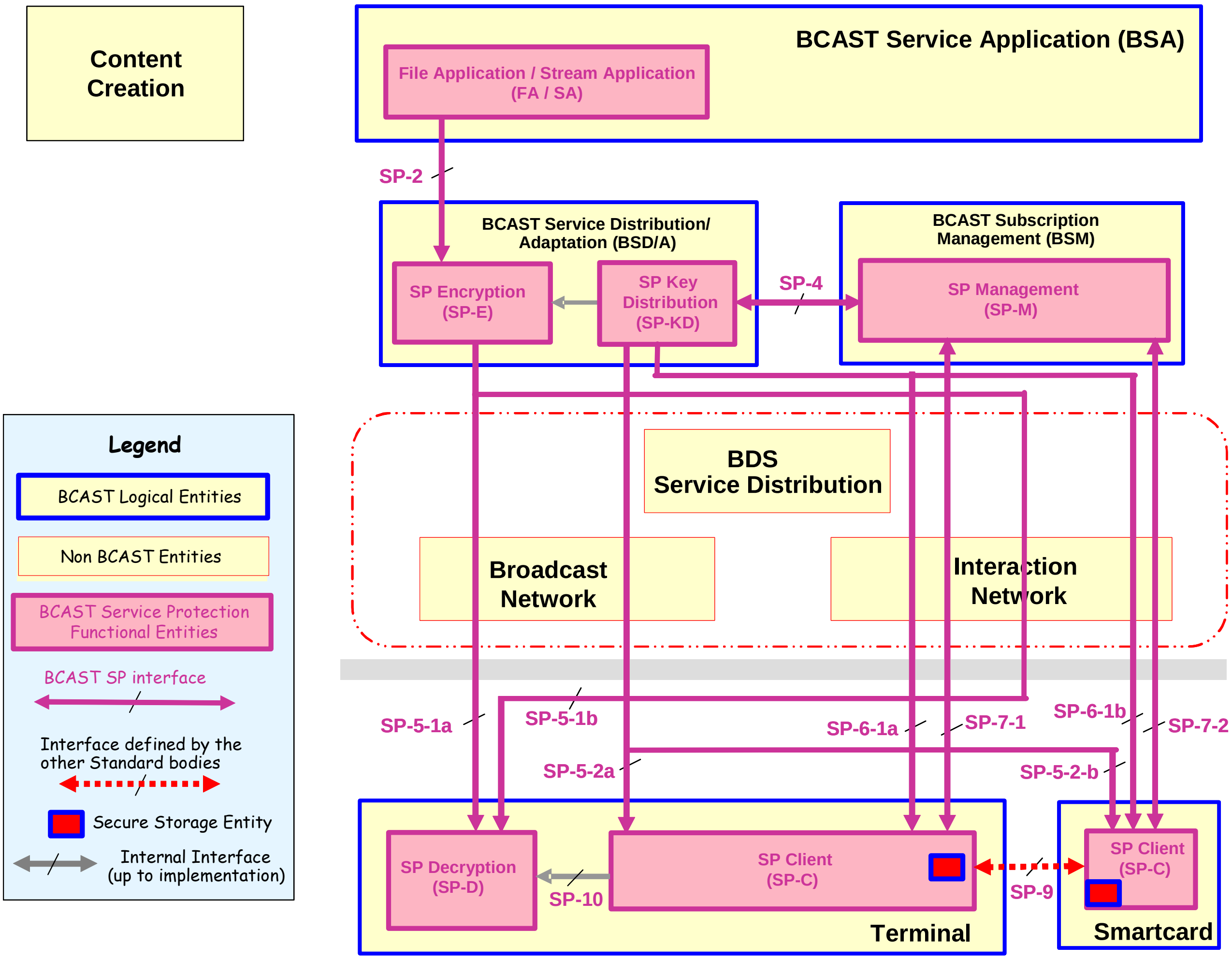


Figure 8 - Service Protection Functional Architecture

Note: The Smartcard can be USIM/(R-)UIM.

It is presumed that the entire service protection functionality can be performed by either the BCAST Enabler or the underlying BDS technology which contains the BDS-SD/A. In the service protection architecture as shown, it is presumed that the service protection functionality is entirely performed by the BCAST Enabler. Therefore, similar service protection capability in the BDS-SD/A is disabled or considered a null function.

The following table explains the interfaces and maps them to BCAST reference points:

Interface	Reference Point	Definition
SP-2	BCAST-2	Delivery of file or stream to SP-E in BSD/A, where encryption is performed.
SP-4	BCAST-4	Exchange of the information related to STKM generation by BSD/A or BSM. Delivery of STKM generated by BSM (for STKM delivery over Broadcast Channel). Delivery of LTKM generated by BSM (for LTKM delivery over Broadcast channel to Terminal supporting only Broadcast channel capability). This interface delivers Long Term Key material from the SP-M to SP-KD, for use in subsequent encryption of Short Term Keys. These Long Term Key materials are SEAK/PEAK for the DRM Profile, and SEK/PEK for the Smartcard Profile. Delivery of registration key materials from the SP-M to SP-KD for the DRM profile (for registration key materials delivery over Broadcast channel to terminal supporting only Broadcast Channel capability).
SP-5-1	BCAST-5	This interface implements layer 4 (“Traffic encryption”) of the 4-layer model. The content delivered across SP-5-1 may also be unencrypted in the case of free-to-air services. The service protected file and stream is distributed to the terminal over Broadcast Channel (SP-5-1a) or Interaction Channel (SP-5-1b), which may include traversing the BDS Service Distribution/Adaptation. Note: This interface is identical to FD-5 and SD-5.
SP-5-2	BCAST-5	Delivery of STKM to terminal over Broadcast channel to SP-C in Terminal (SP 5-2a) or SP-C in Smartcard (SP 5-2b). Delivery of LTKM to terminal which only support Broadcast Channel, which may include traversing the BDS Service Distribution/Adaptation. Delivery of the information related to registration and authentication over Broadcast Channel, which may include traversing the BDS Service Distribution/Adaptation to Broadcast-only terminal. Note: Key materials are stored within a secure storage entity in the SP-C on the terminal or the smartcard depending on key management implementation.
SP-6-1a	BCAST-6	Delivery of STKM by BSD/A over Interaction channel, for the DRM Profile.
SP-6-1b	BCAST-6	Delivery of STKM by BSD/A over Interaction channel, for the Smartcard Profile.
SP-7	BCAST-7	The signalling exchange for registration (layer 1 of 4 layer model) and delivery of LTKM over Interaction channel to SP-C in Terminal (SP-7-1) or SP-C in Smartcard (SP-7-2). Note: Related key materials are stored within a secure storage entity in the SP-C on the terminal or the smartcard depending on key management implementation.
SP-9	N/A	This is the interface between the terminal and the smartcard. This interface is not present for terminals not having a smartcard. This interface should correspond to the relevant specifications in 3GPP (U)SIM [3GPP TS 31.101] and 3GPP2 (R)-UIM [3GPP2 C.S0023-B].

		The secure authenticated channel between terminal and smartcard should correspond to [3GPP TS 33.110], [ETSI TS 102.484]. Note: SP-9 is Terminal internal interface and is not standardized within OMA BCAST.
SP-10	N/A	Transmission of traffic encryption keys (TEKs) from the terminal to the SP-D to decrypt the enciphered content. Note : SP-10 is Terminal internal interface and is not standardized within OMA BCAST.

5.3.4.3.1 File Application/Stream Application Component

The File Application/Stream Application Component (FA/SA) in the BSA is responsible for receiving files and stream from Content Creation and sending the file and stream with attributes and additional information to BCAST Service Distribution/Adaptation.

5.3.4.3.2 SP Management Component

The Service Protection Management Component (SP-M) in the BSM is responsible for the registration of Terminal and the authentication/authorization of User. SP-M is also responsible for the LTKM generation and the LTKM delivery over Interaction Channel. LTKM contains SEK and PEK and it is delivered to SP-C in Terminal (via SP 5-2a or SP-7-1) or SP-C in Smartcard (via SP 5-2b or SP-7-2).

SP-M may generate the STKM and, for this, it exchanges the STKM generation related information with BSD/A. In this case, the STKM is sent by SP-M to SP-KD, and in turn forwarded by SP-KD to the terminal over Broadcast Channel or interaction channel.

To support Broadcast-only terminal, SP-M can provide out of band registration and delivery of LTKM to SP-KD in BSD/A. Such out-of-band communications is outside the scope of BCAST specifications.

The SP-M also supports handling of the secure group management. The secure group management scheme can be used for efficient broadcasting of the long-term key message and revocation procedure. The SP-M is in charge of the domain management. The terminal can join a domain or leave a domain using the SP-M.

5.3.4.3.3 SP Key Distribution Component

The Service Protection Key Distribution Component (SP-KD) in the BSD/A is responsible for the distribution over the broadcast channel of the LTKM and STKM, generation of TEK and the optional generation of STKM. The SP-KD also delivers STKM to Terminal over interaction channel.

When the STKM is natively generated, the SP-KD is responsible for the generation of the TEK and other service protection protocol parameters, which are related to service transmission. In the case that STKM is generated by the SP-M in the BSM, the SP-KD transfers the TEK, and other service protection protocol parameters which are related to service transmission, to the SP-M. If STKM is generated by SP-KD itself, SP-KD exchanges the STKM generation related message with BSM. Upon STKM generation by either the SP-M in the BSM or the SP-KD itself, it is delivered by the SP-KD over the broadcast channel or interaction channel to Terminals.

For Broadcast only Terminal, SP-KD receives LTKM from SP-M in BSM and delivers it over broadcast channel. In addition to this, SP-KD can transmits registration key materials are sent from the SP-M to broadcast-only terminals.

5.3.4.3.4 SP Encryption Component

The Service Protection Encryption Component (SP-E) in the BSD/A is responsible for encrypting file or stream for delivery over the broadcast channel or the interaction channel. The TEK is delivered from the SP-KD and is used for encrypting file or stream (note: this internal interface in BSD/A is not further specified). The format of the encrypted file or stream depends on the specific service protection system. SP-E may be a null function in the transmission of free-to-air services or the Service Guide.

5.3.4.3.5 SP Decryption Component

The Service Protection Decryption Component (SP-D) in the Terminal is responsible for decrypting the encrypted file or stream using the TEK extracted from the STKM. SP-D receives TEK from SP-C in Terminal, or SP-C in Smartcard. SP-D may be a null function in the reception of free-to-air services or the Service Guide.

5.3.4.3.6 SP Client Component

The Service Protection Client Component (SP-C) resides either in the Terminal, for the DRM Profile, or in both the Terminal and the Smartcard for the Smartcard Profile. The SP-C is responsible for terminal registration, user authentication/authorization, and acquisition of the LTKM and the STKM. After the registration, the SP-C may acquire the REK or SMK/GMK which is derived from the registration, depending on the security profile. The LTKM contains the SEK or PEK which is used for encrypting the STKM. In the case of the DRM Profile, the SP-C in the Terminal acquires the TEK by decrypting STKM using SEK. In the case of the Smartcard Profile, SP-C in the Smartcard sends the TEK, via the SP-C in the Terminal, to the SP-D for decryption of the encrypted file or stream.

5.3.4.3.7 Creation of STKMs

There are two options for STKM generation. The first is STKM generation by BSM, and the second is STKM generation by BSD/A, as illustrated in the figure below. STKM is typically generated by the BSM because BSM is the primary entity for Service Protection. However, depending on the business model, the STKM can also be generated by the BSDA.

To support both STKM generation options, the BSM is responsible for generating the SEAK/PEAK (for DRM Profile) or SEK/PEK (for Smartcard Profile), and access criteria descriptors. The BSD/A is responsible for generating the TEKs and other service protection parameters.

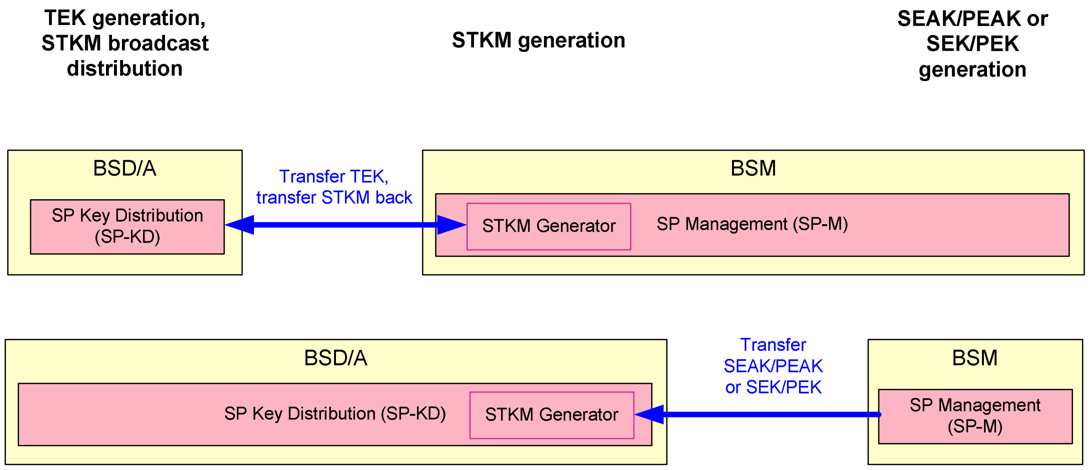


Figure 9 - Options for STKM Creation

5.3.4.4 Functional Architecture for Content Protection

The following diagram describes Content Protection for file and stream and interfaces among BCAST logical entities.

The architecture is agnostic to content protected files: DCF, PDCF files can be distributed just as any other file. For streams, the content protection is determined by the indication of CP-M that post acquisition usage rights are required for the stream.

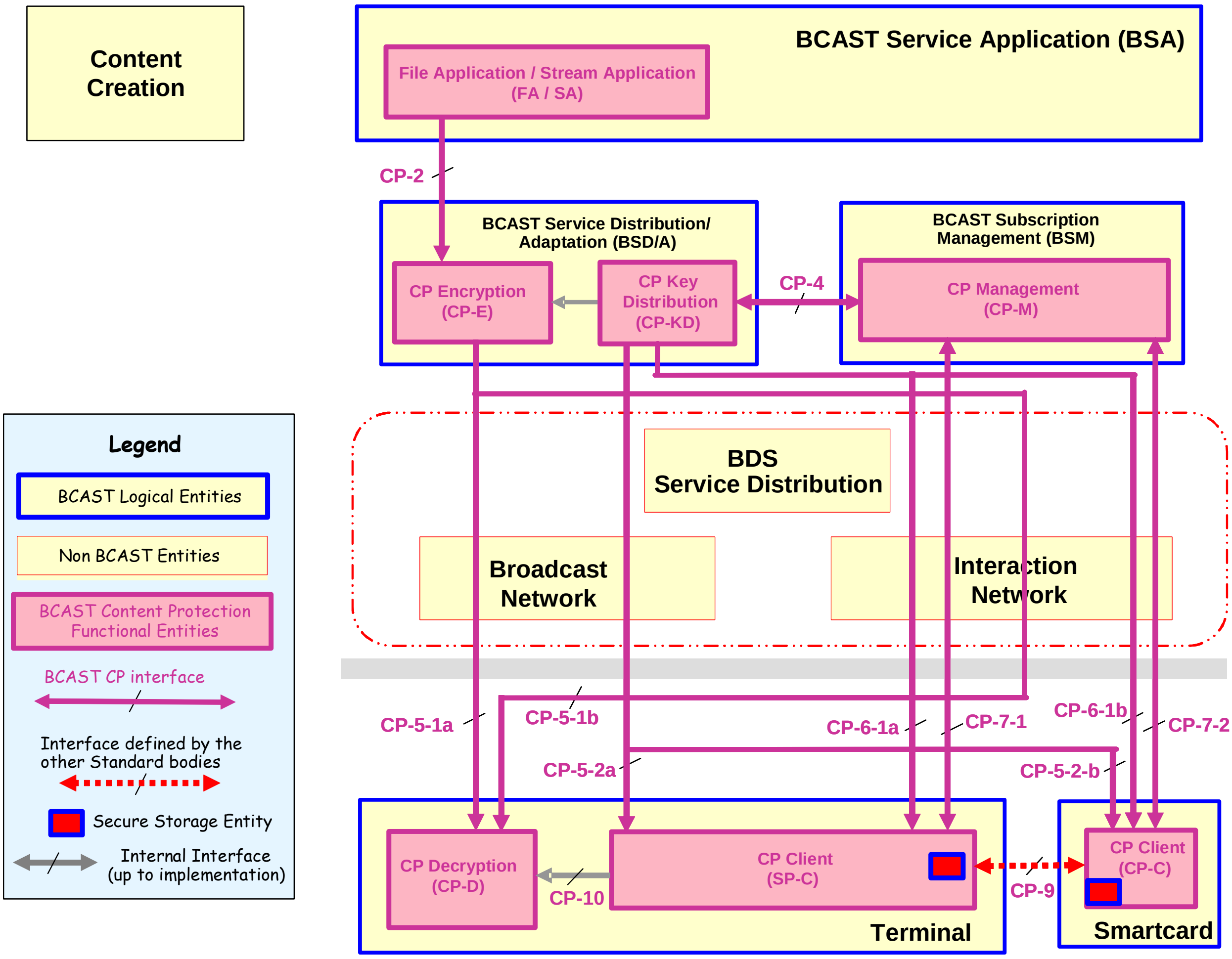


Figure 10 - Content Protection Functional Architecture

The figure above depicts the architecture of the BCAST Content Protection function for files.

It is presumed that the entire content protection functionality can be performed by either the BCAST Enabler or the underlying BDS technology which contains the BDS-SD/A. In the content protection architecture as shown, it is presumed that the content protection functionality is entirely performed by the BCAST Enabler. Therefore, similar content protection capability in the BDS-SD/A is disabled or considered a null function.

The following table explains the interfaces and maps them to BCAST reference points:

Interface	Reference Point	Definition
CP-2	BCAST-2	Delivery of file or stream to CP-E in BSD/A, where encryption is performed.
CP-4	BCAST-4	Exchange of the information related to STKM generation by BSD/A or BSM. Delivery of STKM generated by BSM (for STKM delivery over Broadcast Channel). Delivery of LTKM generated by BSM (for LTKM delivery over Broadcast channel to Terminal supporting only Broadcast channel capability). This interface delivers Long Term Key material from the CP-M to CP-KD, for use in subsequent encryption of Short Term Keys. These

		Long Term Key materials are SEAK/PEAK for the DRM Profile, and SEK/PEK for the Smartcard Profile. Delivery of registration key materials from the CP-M to CP-KD for the DRM profile (for registration key materials delivery over Broadcast channel to terminal supporting only Broadcast Channel capability).
CP-5-1	BCAST-5	This interface implements layer 4 (“Traffic encryption”) of the 4-layer model. The content delivered across CP-5-1 may also be unencrypted in the case of free-to-air services. The content protected file and stream is distributed to the terminal over Broadcast Channel (CP-5-1a) or Interaction Channel (CP-5-1b), which may include traversing the BDS Service Distribution/Adaptation. Note: This interface is identical to FD-5 and SD-5.
CP-5-2	BCAST-5	Delivery of STKM to terminal over Broadcast channel to CP-C in Terminal (CP 5-2a) or CP-C in Smartcard (CP 5-2b). Delivery of LTKM to terminal which only support Broadcast Channel which may include traversing the BDS Service Distribution/Adaptation. Delivery of the information related to registration and authentication over Broadcast Channel which may include traversing the BDS Service Distribution/Adaptation to Broadcast only terminal. Note: Key materials are stored within a secure storage entity in the CP-C on the terminal or the smartcard depending on key management implementation.
CP-6-1a	BCAST-6	Delivery of STKM by BSD/A over Interaction channel, for the DRM Profile.
CP-6-1b	BCAST-6	Delivery of STKM by BSD/A over Interaction channel, for the Smartcard Profile.
CP-7	BCAST-7	The signalling exchange for registration (layer 1 of 4 layer model) and delivery of LTKM over Interaction channel to CP-C in Terminal (CP-7-1 or CP-C in Smartcard (CP -7-2). Note: Related key materials are stored within a secure storage entity in the CP-C on the terminal or the smartcard depending on key management implementation.
CP-9	N/A	This is the interface between the terminal and the smartcard. This interface is not present for terminals not having a smartcard. This interface should correspond to the relevant specifications in 3GPP (U)SIM [3GPP TS 31.101] and 3GPP2 (R)-UIM [3GPP2 C.S0023-C] and 3GPP2 CSIM [3GPP2 C.S0068]. The secure authenticated channel between terminal and smartcard should correspond to [3GPP TS 33.110], [ETSI TS 102.484]. Note: CP-9 is Terminal internal interface and is not standardized within OMA BCAST
CP-10	N/A	Transmission of traffic encryption keys (TEKs) from the terminal to the CP-D to decrypt the enciphered content. Note : CP-10 is Terminal internal interface and is not standardized within OMA BCAST.

5.3.4.4.1 File Application/Stream Application Component

The File Application/Stream Application Component (FA/SA) in the BSA is responsible for receiving files and stream from Content Creation and sending the file and stream with attributes and additional information to BCAST Service Distribution/Adaptation.

5.3.4.4.2 CP Management Component

The Content Protection Management Component (CP-M) in the BSM is responsible for the registration of Terminal and the authentication/authorization of User. CP-M is also responsible for the LTKM generation and the LTKM delivery over Interaction Channel. LTKM contains SEK and PEK and it is delivered to CP-C in Terminal (via CP 5-2a or CP-7-1) or CP-C in Smartcard (via CP 5-2b or CP-7-2).

CP-M may generate the STKM and, for this, it exchanges the STKM generation related information with BSD/A. In this case, the STKM is sent by CP-M to CP-KD, and in turn forwarded by CP-KD to the terminal over Broadcast Channel or interaction channel.

To support broadcast-only terminal, CP-M can provide out of band registration and delivery of LTKM to CP-KD in BSD/A. Such out-of-band communications is outside the scope of BCAST specifications.

The CP-M also supports handling of the secure group management. The secure group management scheme can be used for efficient broadcasting of the long-term key message and revocation procedure. The CP-M is in charge of the domain management. The terminal can join a domain or leave a domain using the CP-M.

5.3.4.4.3 CP Key Distribution Component

The Content Protection Key Distribution Component (CP-KD) in the BSD/A is responsible for the distribution over the broadcast channel of the LTKM and STKM, generation of TEK and the optional generation of STKM. The CP-KD also delivers STKM to Terminal over interaction channel.

When the STKM is natively generated, the CP-KD is responsible for the generation of the TEK and other service protection protocol parameters, which are related to service transmission. In the case that STKM is generated by the CP-M in the BSM, the CP-KD transfers the TEK, and other service protection protocol parameters which are related to service transmission, to the CP-M. If STKM is generated by CP-KD itself, CP-KD exchanges the STKM generation related message with BSM. Upon STKM generation by either the CP-M in the BSM or the CP-KD itself, it is delivered by the CP-KD over the broadcast channel or interaction channel to Terminals.

For broadcast only Terminal, CP-KD receives LTKM from CP-M in BSM and delivers it over Broadcast Channel. In addition to this, CP-KD can transmit registration key materials that are sent from the CP-M to broadcast-only terminals.

5.3.4.4.4 CP Encryption Component

The Content Protection Encryption Component (CP-E) in the BSD/A is responsible for encrypting file or stream for delivery over the broadcast channel or the interaction channel. The TEK is delivered from the CP-KD and is used for encrypting file or stream (note: this internal interface in BSD/A is not further specified). The format of the encrypted file or stream depends on the specific service protection system.

5.3.4.4.5 CP Decryption Component

The Content Protection Decryption Component (CP-D) in the Terminal is responsible for decrypting the encrypted file or stream using the TEK extracted from the STKM. CP-D receives TEK from CP-C in Terminal, or CP-C in Smartcard.

5.3.4.4.6 CP Client Component

The Content Protection Client Component (CP-C) resides either in the Terminal, for the DRM Profile, or in both the Terminal and the Smartcard for the Smartcard Profile. The CP-C is responsible for terminal registration, user authentication/authorization, and acquisition of the LTKM and the STKM. After the registration, the CP-C may acquire the REK or SMK/GMK which is derived from the registration, depending on the security profile. The LTKM contains the SEK or PEK which is used for encrypting the STKM. In the case of the DRM Profile, the CP-C in the Terminal acquires the TEK by decrypting STKM using SEK. In the case of the Smartcard Profile, CP-C in the Smartcard sends the TEK, via the CP-C in the Terminal, to the CP-D for decryption of the encrypted file or stream.

5.3.4.4.7 Creation of STKMs

There are two options for STKM generation. The first is STKM generation by BSM, and the second is STKM generation by BSD/A, as illustrated in Figure 10 - Content Protection Functional Architecture. STKM is typically generated by the BSM because BSM is the primary entity for Content Protection. However, depending on the business model, the STKM can also be generated by the BSDA.

To support both STKM generation options, the BSM is responsible for generating the SEK and PEK, and access criteria descriptors. The BSD/A is responsible for generating the TEKs and other service protection parameters.

5.3.5 Service Interaction Function

The Service Interaction Function provides the point-to-point communication between a BCAST Service Application in the network and the terminal.

The Broadcast Service Interaction Client Component uses the interaction function if BCAST service provides the supplementary service, which requires user interactions (e.g., real-time voting, real-time betting, requests of additional services, etc.).

The Service Interaction Function is supported by the Interaction Network, such as, a cellular mobile network or a messaging system (e.g., SMS or MMS). The Interaction Function supports various types of interaction, such as, Call-in, SMS, MMS, Sending of screenshots, Downloads, Email, links to additional sites (e.g., Chat rooms, WWW, WAP, HTTP and operator portals).

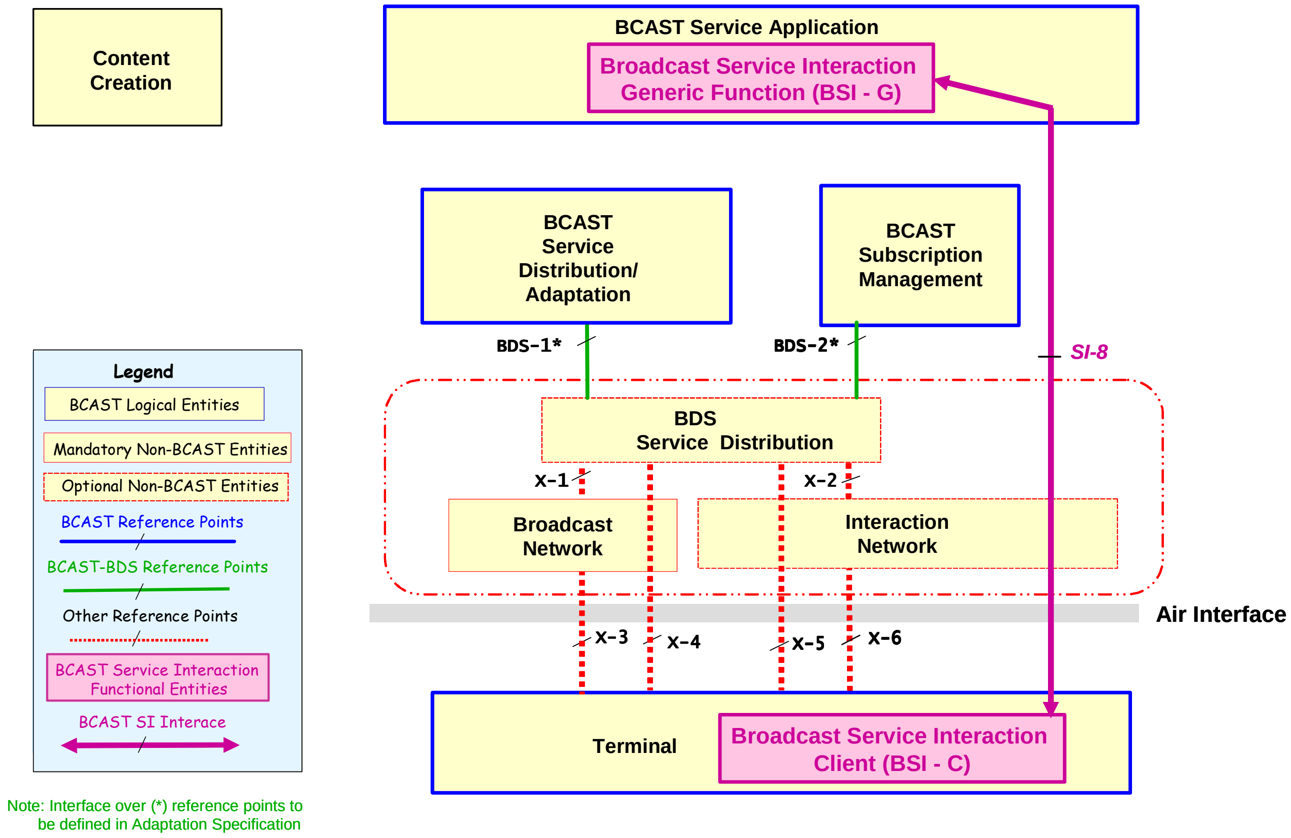

Content Creation
BCAST Service Application
Broadcast Service Interaction Generic Function (BSI - G)
BCAST Service Distribution/ Adaptation
BCAST Subscription Management
BDS-1*
BDS-2*
SI-8
BDS Service Distribution
X-1
X-2
Broadcast Network
Interaction Network
Air Interface
X-3
X-4
X-5
X-6
Terminal
Broadcast Service Interaction Client (BSI - C)
Legend
BCAST Logical Entities
Mandatory Non-BCAST Entities
Optional Non-BCAST Entities
BCAST Reference Points
BCAST-BDS Reference Points
Other Reference Points
BCAST Service Interaction Functional Entities
BCAST SI Interace
Note: Interface over (*) reference points to be defined in Adaptation Specification

Figure 11 - Service Interaction Functionl Architecture

5.3.5.1 BCAST Interaction Function Interfaces

The Service Interaction Functional architecture defines the following interface:

Interface	Reference Point	Usage
SI-8	BCAST-8	Delivery of End user request or response. Delivery of response corresponding to End user request.

5.3.5.2 BCAST Service Interaction Generic Component

The Broadcast Service Interaction Generic Component (BSI-G) is responsible for serving the supplementary service, which requires End user interaction.

The Content Creation provides contents, which requires End user interaction and additional information to be used for the Generation of BCAST service having a supplementary service to the BSI-G. BSI-G generates BCAST service with the contents and information from Content Creation.

BSI-G receives End user request or End User response corresponding to the supplementary service. BSI-G may do the operation about End User request or End User responses or BSI-C may send End User request or End User response to a related application.

5.3.5.3 BCAST Service Interaction Client Component

The Broadcast Service Interaction Client Component (BSI-C) is responsible for serving the supplementary service, which requires End user interaction.

BSI-C sends End User request or End user response corresponding to the supplementary service to BSI-G over the interaction channel and receives the response to the End user request or End user response. BSI-C may do the operation about this response or sends this response to a related application.

5.3.6 Service Provisioning Function

The Service Provisioning Function is responsible for user subscription to a BCAST service and payment related functions

The Service Provisioning Function is primarily applicable to systems and terminals with interaction network capabilities; key functionalities include: subscription (i.e., initiation, changes, and cancellation) of BCAST services, content bundle selection and impulse ordering of pay-per-view content.

The Service Provisioning Function may also provide the additional information about payment (such as, account status) information.

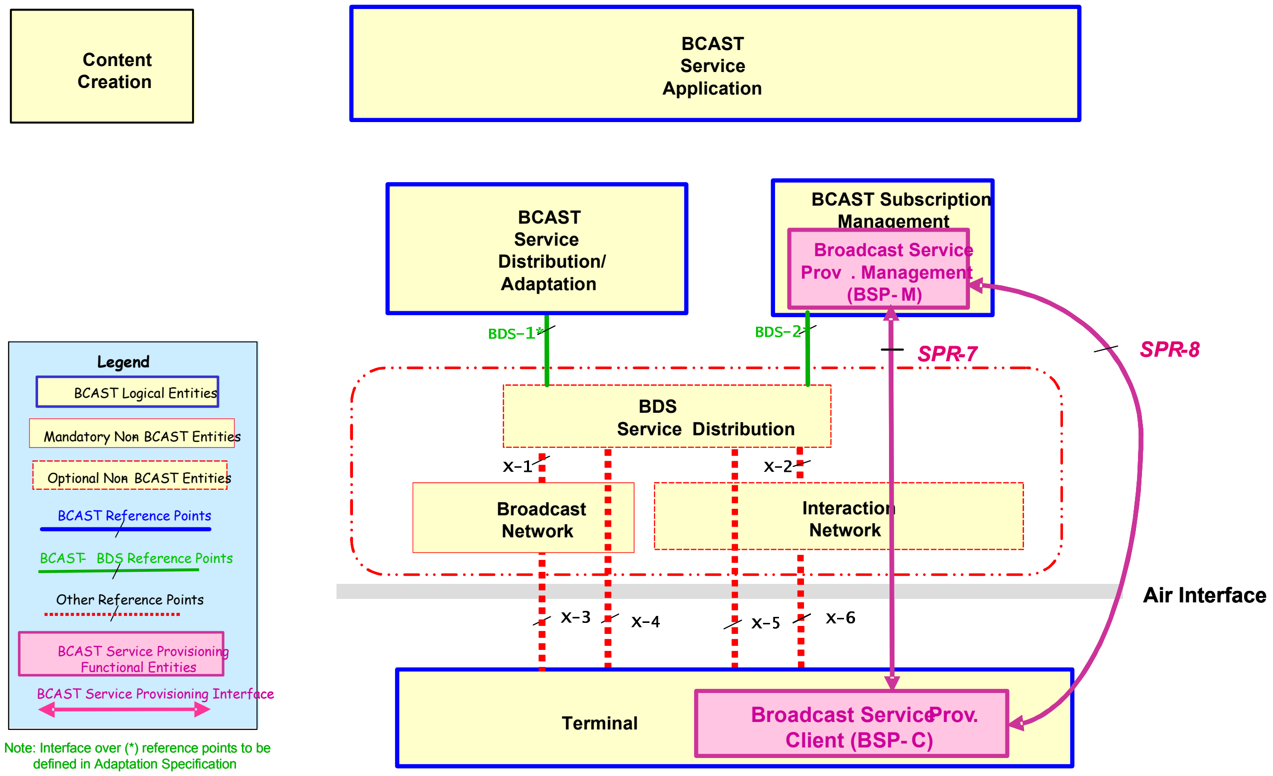

Content Creation
BCAST Service Application
BCAST Service Distribution/ Adaptation
BCAST Subscription Management
Broadcast Service Prov . Management (BSP-M)
BDS-1*
BDS-2*
SPR-7
SPR-8
BDS Service Distribution
X-1*
X-2*
Broadcast Network
Interaction Network
Air Interface
X-3
X-4
X-5
X-6
Terminal
Broadcast Service Prov. Client (BSP-C)
Legend
BCAST Logical Entities
Mandatory Non BCAST Entities
Optional Non BCAST Entities
BCAST Reference Points
BCAST- BDS Reference Points
Other Reference Points
BCAST Service Provisioning Functional Entities
BCAST Service Provisioning Interface
Note: Interface over (*) reference points to be defined in Adaptation Specification

Figure 12 - Service Provisioning Functional Architecture

5.3.6.1 Broadcast Service Provisioning Function Interfaces

The Broadcast Service Provisioning Functional architecture defines the following interfaces:

Interface	Reference Point	Usage
SPR-7	BCAST-7	Delivery of messages used for a subscription such as subscription request of user and response from BCAST Subscription Management. Delivery of payment information
SPR-8	Out of band	The End User subscribes and purchases the services through the out-of-band interfaces. It's out of scope of OMA BCAST.

5.3.6.2 Broadcast Service Provisioning Management Component

The Broadcast Service Provisioning Management Component (BSP-M) is responsible for providing the subscription and the additional purchase information of Broadcast Service. Based on the End User's subscription information, BSP-M provides charging information of the End Users to the entity taking responsibility for charging. BSP-M also supports billing of mobile broadcast services.

BSP-M gets the subscription requests, reporting for charging and personalized requests from the End User (BSP-C) over the interaction channel through the SPR-7 or out-of-band through the SPR-8.

BSP-M sends the confirmation of End user's subscription and may send the additional provisioning information if an End User requests it.

5.3.6.3 Broadcast Service Provisioning Client Component

The Broadcast Service Provisioning Client Component (BSP-C) is responsible for the subscription of BCAST service and the reporting about the consumption of BCAST service.

BSP-C abstracts provisioning information from Service Guide and may filter the received provisioning information for the End User if necessary.

BSP-C may send the End user request to get the additional information about provisioning.

BSP-C sends End User subscription request over the interaction channel and receives the confirmation about End User subscription. BPR-C may report the information used for charging to BPR-M.

5.3.7 Notification Function

The Notification Function is responsible for informing a terminal or a group of terminals of the upcoming event about Broadcast Service. The classification of upcoming event can be determined by the Broadcast Service Provider. For this purpose, Notification Function generates a notification message and sends a notification message to a terminal or a group of terminals. Examples of such upcoming event include the change of the Service Guide, the notice of the start of the user's (or a group of users') preferred service, a promotion of a specific Broadcast Service, Auxiliary Data download or insertion trigger or other Service related notifications (e.g., goal scores of a broadcast sports match). Note that Service Guide function is the mandatory and primary means for Service Guide delivery and update; Notification function is the optional and secondary means.

For efficient delivery of a notification message over Broadcast channel or Interaction Channel, the Notification Function uses the functionality provided by Broadcast Service Distribution/Adaptation.

The Notification Function collaborates with Provisioning Function and Service Guide Function to generate a notification message.

The Notification Function may forward a notification message to BDS or Interaction Network in order that BDS or Interaction Network can send a notification message by their native method.

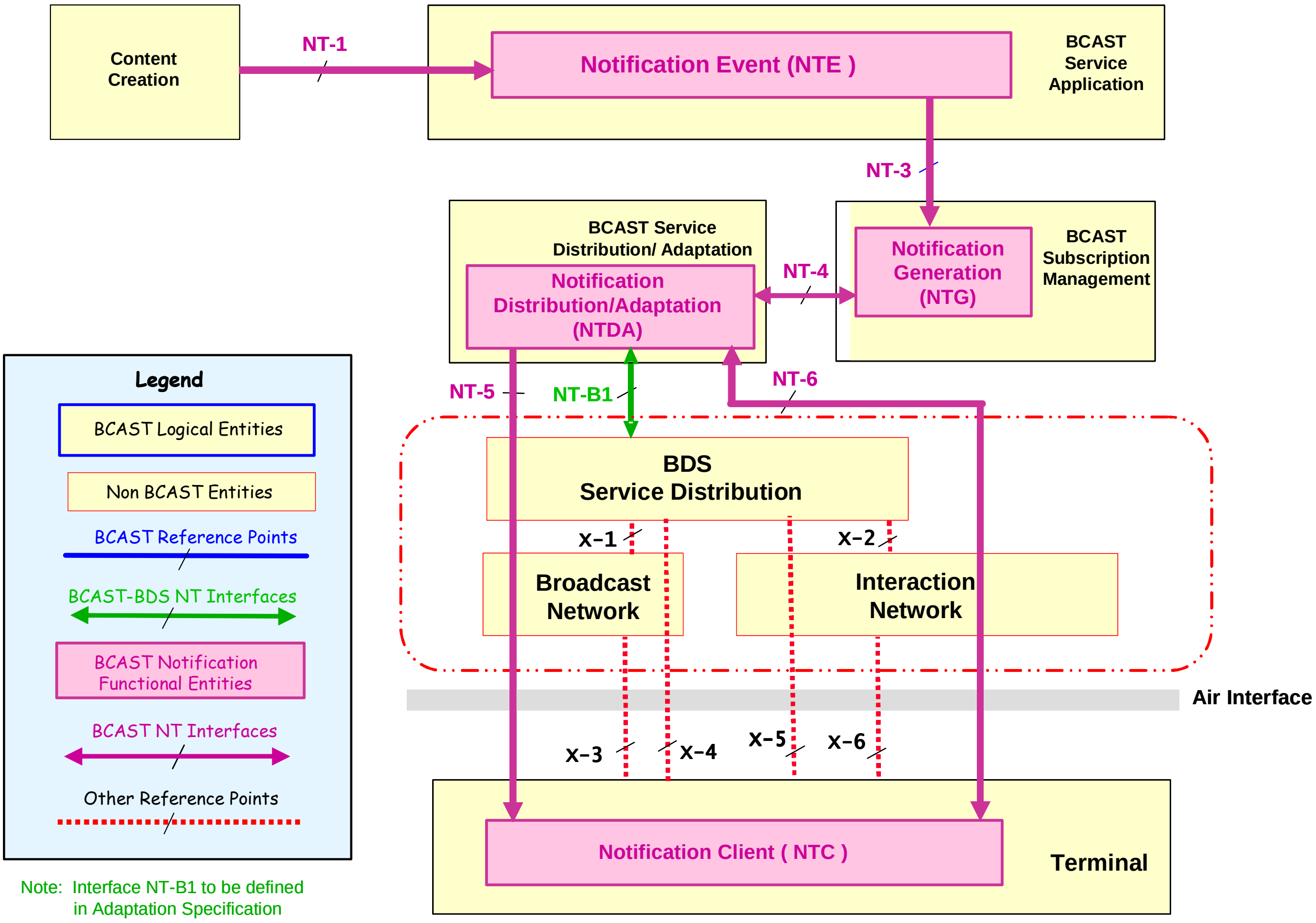

Content Creation
NT-1
Notification Event (NTE)
BCAST Service Application
NT-3
BCAST Service Distribution/ Adaptation
Notification Distribution/Adaptation (NTDA)
NT-4
Notification Generation (NTG)
BCAST Subscription Management
Legend
BCAST Logical Entities
Non BCAST Entities
BCAST Reference Points
BCAST-BDS NT Interfaces
BCAST Notification Functional Entities
BCAST NT Interfaces
Other Reference Points
NT-5
NT-B1
NT-6
BDS Service Distribution
X-1
X-2
Broadcast Network
Interaction Network
Air Interface
X-3
X-4
X-5
X-6
Notification Client (NTC)
Terminal
Note: Interface NT-B1 to be defined in Adaptation Specification

Figure 13 - Notification Functional Architecture

The BCAST Notification Functional Architecture defines the following interfaces:

Interfaces	Reference Point	Description
NT-1	BCAST-1	A notice of notification event from Content Provider. Delivery of notification attributes from Content Provider.
NT-3	BCAST-3	Delivery of attributes related to the generation of a Service Guide specific notification message. Delivery of a notice of notification event from Content Provider.
NT-4	BCAST-4	Delivery of a notification message to Notification Distribution/Adaptation Component. Delivery of A notice of notification event from BDS. Delivery of A notice of notification event from Service Guide Generation Component in BSD/A. Delivery of Service Guide Attributes to be used for the generation of a notification message. The exchange of Service Guide information over BCAST-4 for notification message generation is covered by Notification Functional Architecture.
NT-5	BCAST-5	This interface provides the delivery of a notification message to a terminal or a group of terminals over the Broadcast Distribution System, which may include

		traversing the BDS Service Distribution/Adaptation.
NT-6	BCAST-6	Delivery of a notification message to a terminal over interaction channel. It may be possible that multiple interaction channels are used via NT-6 for the delivery of the same notification. message to multiple terminals.
NT-B1	BDS-1	Delivery of a notice of notification event. Delivery of a notification message to BDS or Interaction Network. Signalling of notification message priority to the underlying BDS. This interface is applicable when the underlying BDS technology is MBMS or BCMCS, and furthermore, whereby that portion of the BDS Service Distribution/Adaptation pertaining to service distribution and adaptation is not functionally integrated in the BCAST Service Distribution/Adaptation.

5.3.7.1 Notification Event Component

The Notification Event Component (NTE) in the network is responsible for forwarding a notice of notification event from Content Creation to Notification Generation Component in BCAST Subscription Management via NT-1 and NT-3. NTE also provides the Service Guide Attributes to be used for the generation of a notification message in Notification Generation Component through NT-3.

5.3.7.2 Notification Generation Component

The Notification Generation Component (NTG) in the network is responsible for the generation of a notification message when a notification event occurs. Notification event can be initiated by Content Creation, BCAST Subscription Management and BCAST Service Distribution and Adaptation, and BDS.

NTG generates a notification message based on a notice of notification event. Generally, a notification event happens in BSM. For this case, a notice of notification event is the internal operation of BSM. For other notification event, NTG receives a notice of notification event from Content Creation through NT-1 and NT-3 and receives a notice of notification event from BSD/A through NT-4, and receives a notice of notification event from BDS through NT-B1 and NT-4.

When NTG generates a notification, it cooperates with other BCAST functions.

The examples for cooperation with other BCAST functions are:

- When NTG generates a notification to a specific user who sets his or her preference on a specific service, NTG refers the user profile in Provisioning function in BSM.
- When NTG generates a notification to a specific user group, NTG refers the user profiles in Provisioning Function in BSM.
- When NTG generates a notification about Service Guide update, NTG receives the related information from Service Guide Generation Component in BSD/A.

5.3.7.3 Notification Distribution/Adaptation Component

The Notification Distribution Adaptation Component (NTDA) in the network is responsible for delivery of a notification message to a terminal or a group of terminals according to a notification event. NTDA determines which channel is used for the delivery of notification message according to the availability of channel and the number of terminals, which will receive a notification message. NTDA sends a notification message to a terminal or a group of terminal over Broadcast Channel via NT-5 and sends a notification message to a terminal over Interaction Channel via NT-6.

NTDA may forward a notification message to BDS or Interaction Network through NT-B1. Based on a received notification message BDS or Interaction Network can generate a notification message and delivers it to a terminal or a group of terminals. How BDS or Interaction Network generates a notification message and sends a notification message is out of OMA BCAST Scope.

If BDS Service Distribution/Adaptation does not exist, NTDA can receive a notice of notification event from BDS through x-1 and NTDA can forward a notification message to BDS or Interaction Network through x-1 and x-2 respectively.

5.3.7.4 Notification Client Component

The Notification Client Component (NTC) in the terminal is responsible for receiving a notification message over the Broadcast Channel or Interaction Channel. NTC informs the relevant BCAST function of the impending occurrence of an event as indicated by the received notification message from the NTDA. For example, if NTC receives events about a change of Service Guide of Broadcast Service, then it sends the event to the Service Guide Client Component.

NTC may directly receive a notification message about an event of Broadcast Service from BDS or Interaction Network.

5.3.8 Terminal Provisioning Function

The Terminal Provisioning Function manages terminal configuration parameters (e.g. data, parameters and applications) through support from OMA DM.

The operation of Terminal Provisioning Function over Interaction Channel is defined in [OMA-DM].

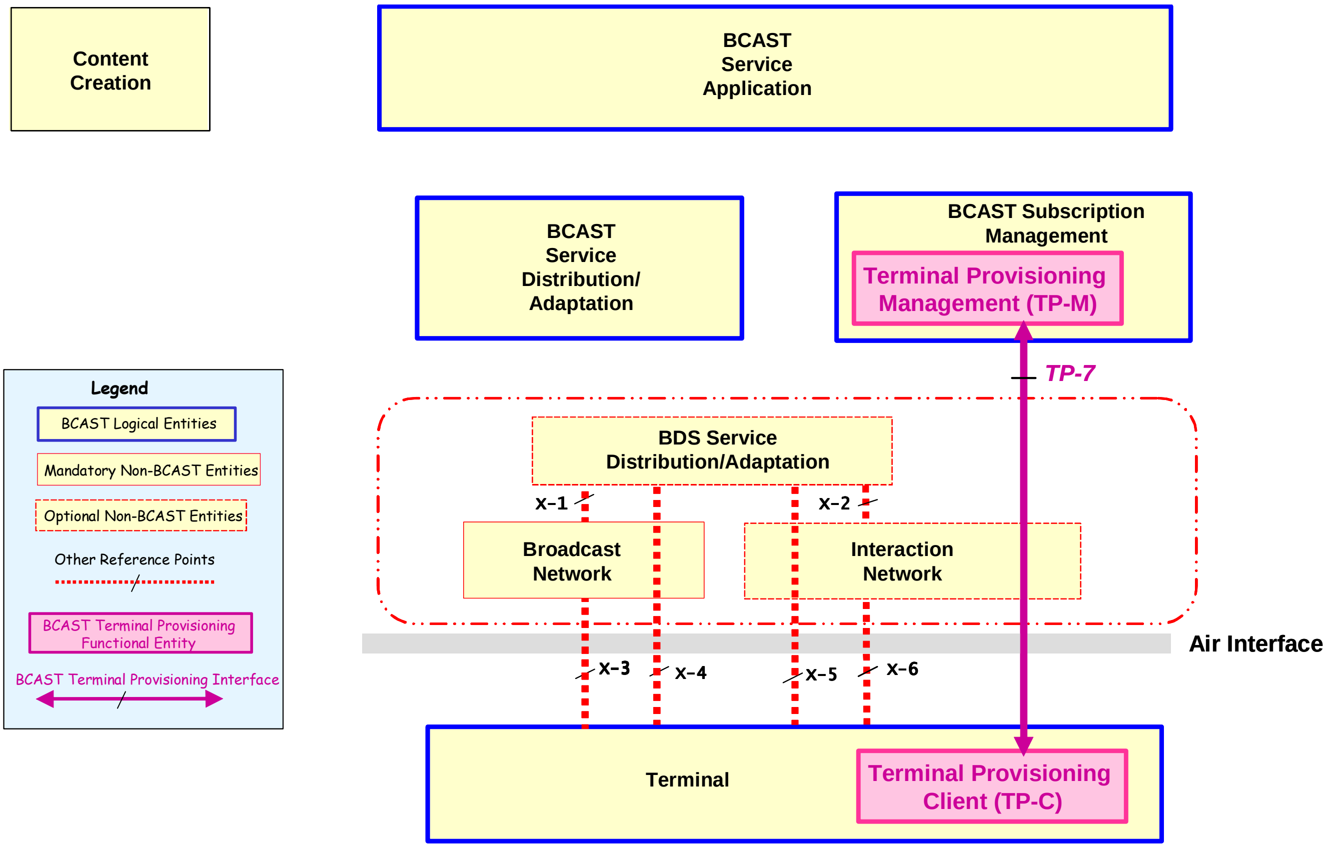

Content Creation
BCAST Service Application
BCAST Service Distribution/ Adaptation
BCAST Subscription Management
Terminal Provisioning Management (TP-M)
TP-7
Legend
BCAST Logical Entities
Mandatory Non-BCAST Entities
Optional Non-BCAST Entities
Other Reference Points
BCAST Terminal Provisioning Functional Entity
BCAST Terminal Provisioning Interface
BDS Service Distribution/Adaptation
x-1
x-2
Broadcast Network
Interaction Network
Air Interface
x-3
x-4
x-5
x-6
Terminal
Terminal Provisioning Client (TP-C)

Figure 14 - Terminal Provisioning Functional Architecture

The above BCAST Terminal Provisioning Functional Architecture defines the following interfaces:

Interface	Reference Point	Description
TP-7	BCAST-7	Delivery of Terminal provisioning messages over Interaction

		Channel Note : The operation on TP-7 is defined in [OMA-DM].

5.3.8.1 Terminal Provisioning Management Component

The Terminal Provisioning Management Component (TP-M) in the network is responsible for managing terminal provisioning.

TP-M generates terminal provisioning message containing a parameter or a command to be used for Terminal Provisioning. Terminal provisioning message is transmitted over the Interaction Channel according to mechanisms defined in [OMA-DM].

TP-M can receive the address of the BCAST Service Guide Server for the interactive mode so that the terminal can retrieve the Service Guide over interaction channel. And if the terminal is roamed, TP-M can provide the roaming specific parameters to the terminal.

In addition, TP-M can receive BDS-specific parameters related to Service Guide entry point and if so processes them into terminal provisioning messages.

All the provided parameters will be converted into terminal provisioning messages called management objects (MO).

5.3.8.2 Terminal Provisioning Client Component

The Terminal Provisioning Client Component (TP-C) in the terminal is responsible for receiving terminal provisioning messages over Interaction Channel through the TP-7 interface.

TP-C does any relevant action which is defined in [OMA-DM] after it receives terminal provisioning message. The delivered terminal provisioning messages may be forwarded to other relevant functions in the terminal.

5.4 Flows

5.4.1 Service Guide Related Flows

5.4.1.1 Service Guide Generation and Delivery over Broadcast channel

Figures 16 and 17 below illustrate examples for the Service Guide Generation and its delivery over the Broadcast Channel.

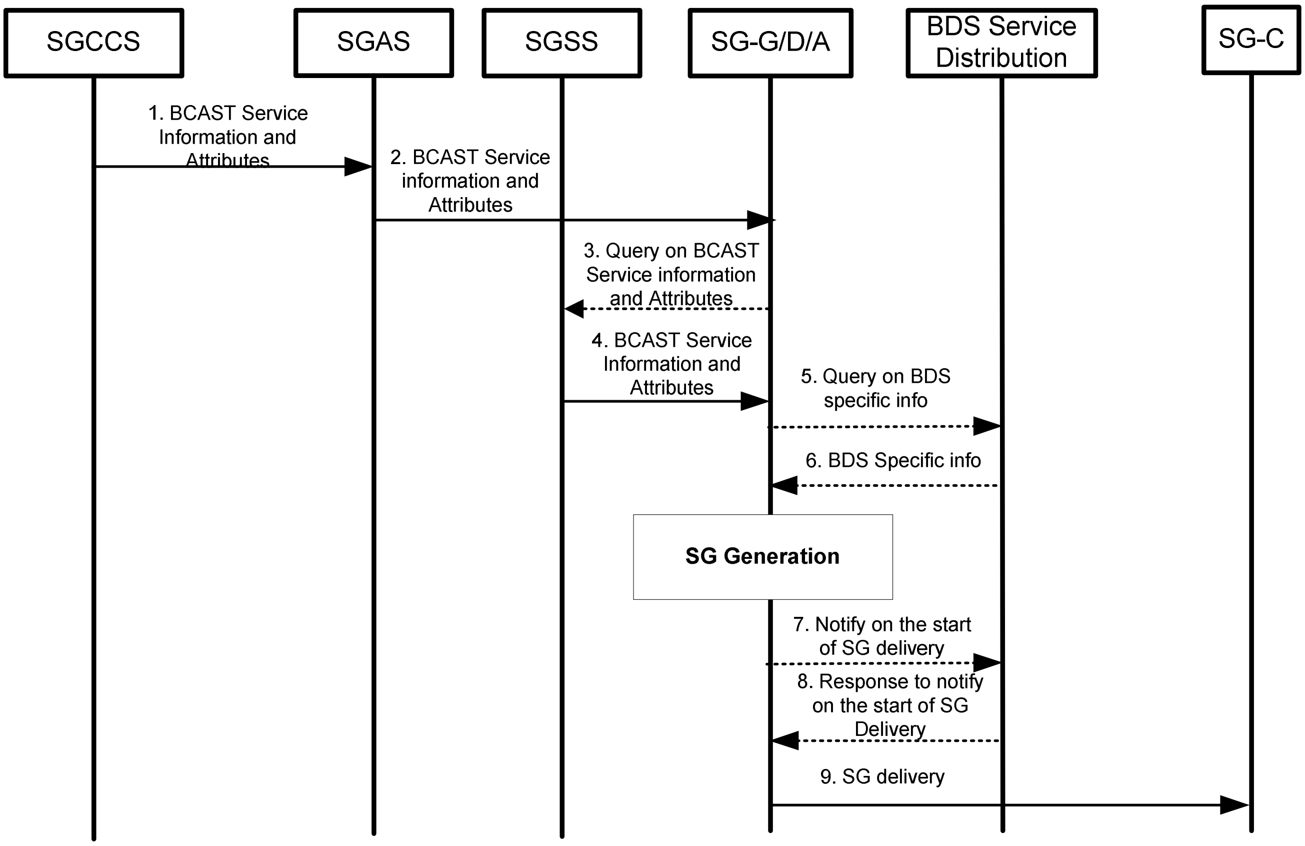

SGCCS
SGAS
SGSS
SG-G/D/A
BDS Service Distribution
SG-C
1. BCAST Service Information and Attributes
2. BCAST Service information and Attributes
3. Query on BCAST Service information and Attributes
4. BCAST Service Information and Attributes
5. Query on BDS specific info
6. BDS Specific info
SG Generation
7. Notify on the start of SG delivery
8. Response to notify on the start of SG Delivery
9. SG delivery

Figure 15 - Service Guide Generation and its delivery over Broadcast channel without traversing the BDS-SD/A

1. SGCCS sends BCAST content information and attributes, such as content description, broadcast area location, parental rating, content genre, user rating, associated preview data and target user profiles, to SGAS. SGCCS can send BCAST content information and attributes as BCAST Service Guide Fragments or non-BCAST standard form (SG1).
2. SGAS sends BCAST service information and attributes, such as, service URI, service description, broadcast area location, parental rating, service genre, user rating, associated preview data and target user profiles, to SG-G/D/A in BSD/A. If BCAST service information and attributes have a non-BCAST Standard form, SGAS changes non-BCAST standard form into BCAST Service Guide Fragment (SG2).
3. The SG-G/D/A in BSD/A may send a request about BCAST service information and attributes to SGSS.(SG4). The BCAST service information and attributes can be service/content protection description information, purchase channel information, service bundling information, pricing information and promotional information, etc.
4. In the response to step 3, the SGSS sends BCAST service information and attributes, such as, service/content protection description information, purchase channel information, service bundling information, pricing information and promotional information to SG-G/D/A (SG4). If step 3 does not exist, SGSS sends BCAST service information and attributes when the information and attributes about a service or bundle of services are changed. After receiving BCAST service information and attributes, SG-G/D/A generates BCAST Service Guide. If the BDS specific info is necessary for Service Guide Generation, the following steps 5 and 6 are performed.
5. The SG-G/D/A may query BDS Service Distribution/Adaptation about the BDS specific information about BCAST service or a bundle of BCAST service (SG-B1).
6. BDS Service Distribution/Adaptation sends the BDS specific information such as source IP address, transport session identifier, and delivery scheduling information (SG-B1).
7. The SG-G/D/A may notify BDS Service Distribution/Adaptation of the start of SG delivery. After the reception of notification, BDS Service Distribution/Adaptation configures the bearers to be used for SG delivery (SG-B1). The

negotiation between SG-G/D/A and BDS Service Distribution/Adaptation may be needed to set the proper parameters (such as data rate) about SG delivery.

8. BDS Service Distribution/Adaptation may responds to the notification of the start of SG delivery. (SG-B1)

9. SG-G/D/A transmits Service Guide over Broadcast Channel. SG-C in terminal receives Service Guide over BCAST channel and it may filter Service Guide based on user profile and user preference before it shows SG to a user. (SG-5)

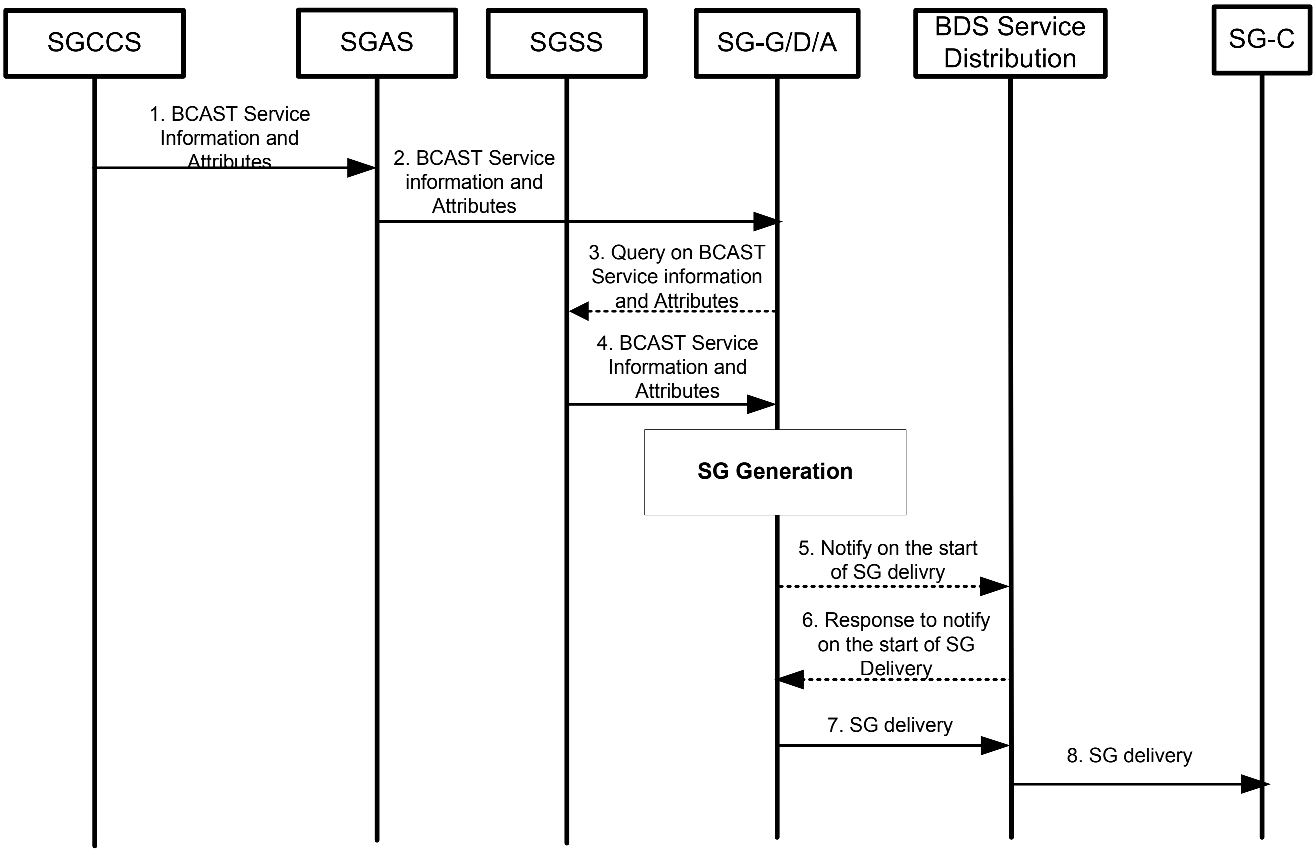

SGCCS
SGAS
SGSS
SG-G/D/A
BDS Service Distribution
SG-C
1. BCAST Service Information and Attributes
2. BCAST Service information and Attributes
3. Query on BCAST Service information and Attributes
4. BCAST Service Information and Attributes
SG Generation
5. Notify on the start of SG delivry
6. Response to notify on the start of SG Delivery
7. SG delivery
8. SG delivery

Figure 16 - Service Guide Generation and its delivery over Broadcast channel, via the BDS-SD/A

1. SGCCS sends BCAST content information and attributes, such as, content description, broadcast area location, parental rating, content genre, user rating, associated preview data and target user profiles, to SGAS. SGCCS can send BCAST content information and attributes as BCAST Service Guide Fragments or non-BCAST standard form (SG1).

2. SGAS sends BCAST service information and attributes, such as service URI, service description, broadcast area location, parental rating, service genre, user rating, associated preview data and target user profiles, to SG-G/D/A in BSD/A. If BCAST service information and attributes have a non-BCAST Standard form, SGAS changes non-BCAST standard form into BCAST Service Guide Fragment (SG2).

3. The SG-G/D/A in BSD/A may send a request about BCAST service information and attributes to SGSS.(SG4). The BCAST service information and attributes can be service/content protection description information, purchase channel information, service bundling information, pricing information and promotional information, etc

4. In the response to step 3, the SGSS sends BCAST service information and attributes, such as, service/content protection description information, purchase channel information, service bundling information, pricing information and promotional information to SG-G/D/A (SG4). If step 3 does not exist, SGSS sends BCAST service information and attributes when the information and attributes about a service or bundle of services are changed. After receiving BCAST service information and attributes, SG-G/D/A generates BCAST Service Guide.

5. The SG-G/D/A may notify BDS Service Distribution/Adaptation of the start of SG delivery. After the reception of notification, BDS Service Distribution/Adaptation configures the bearers to be used for SG delivery (SG-B1). The negotiation between SG-G/D/A and BDS Service Distribution/Adaptation may be needed to set the proper parameters (such as data rate) about SG delivery.
6. BDS Service Distribution/Adaptation may responds to the notification of the start of SG delivery. (SG-B1)
7. SG-G/D/A transmits Service Guide over SG-B1 to the BDS Service Distribution/Adaptation.
8. The BDS Service Distribution/Adaptation subsequently transmits the SG over the Broadcast Channel (X-4). SG-C in terminal receives Service Guide over BCAST channel and it may filter Service Guide based on user profile and user preference before it shows SG to a user.

5.4.1.2 Service Guide Generation and Delivery over Interaction channel

The figure below shows an example for the Service Guide Generation and its delivery over Interaction Channel

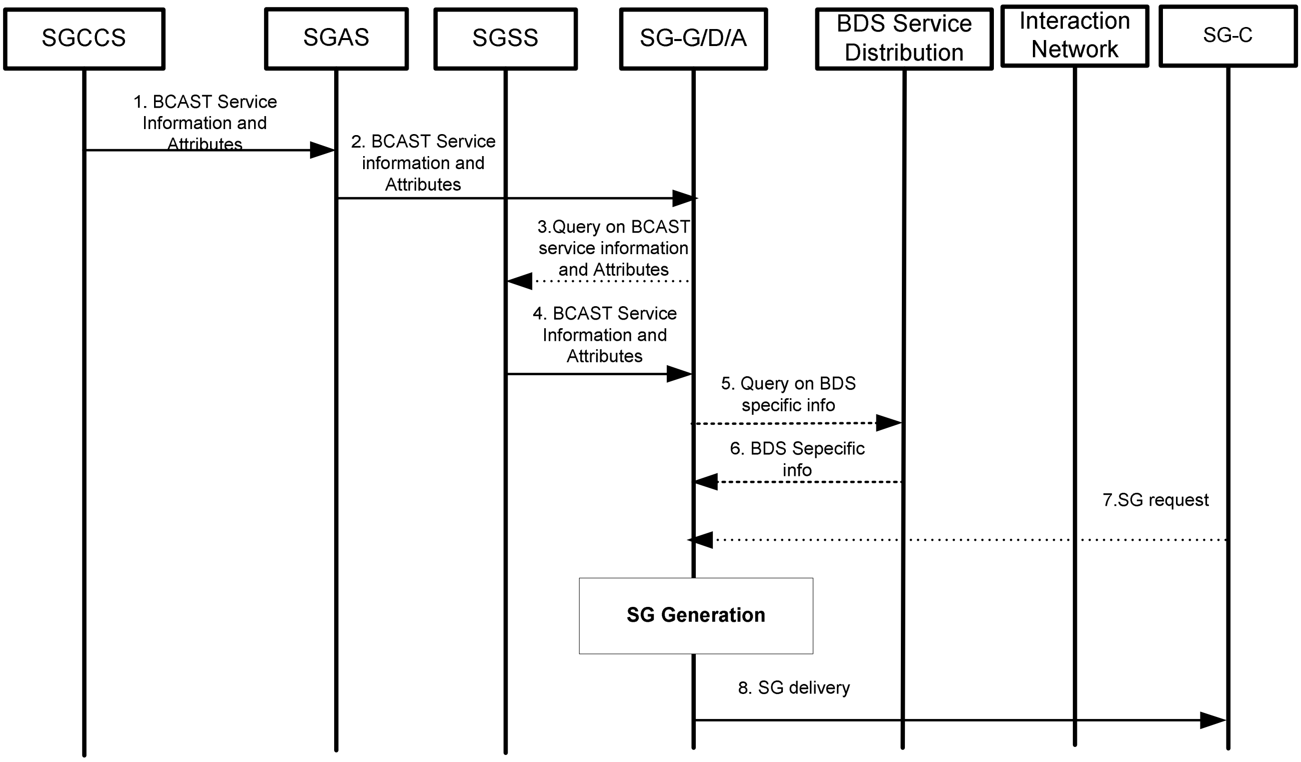

SGCCS
SGAS
SGSS
SG-G/D/A
BDS Service Distribution
Interaction Network
SG-C
1. BCAST Service Information and Attributes
2. BCAST Service information and Attributes
3.Query on BCAST service information and Attributes
4. BCAST Service Information and Attributes
5. Query on BDS specific info
6. BDS Sepecific info
7.SG request
SG Generation
8. SG delivery

Figure 17 - Service Guide Generation and its delivery over Interaction Channel

1-6 The operation of Step 1 to Step 6 is identical to that of Step 1 to Step 6 in Section 5.4.1.1.

7. SG-C in Terminal may request SG-D to transmit the complete Service Guide or subset of the Service Guide over the Interaction Channel (SG-6), or other remote devices (such as, Personal Computer) having SG-C capability may request SG-D to transmit the Service Guide over the Internet and then forward the Service Guide onto the intended terminal. This step is optional. Without step 7, Service Guide also can be delivered over Interaction Channel without prior explicit request.

   There are many possible scenarios for SG transmission over Interaction Channel:
   - SG-C may request SG when a terminal is located in out-of- Broadcast service area.
   - SG-C may request retransmission of all SG/or parts of SG because it failed to receive SG over Broadcast channel.
   - SG-C may request the further information on a specific BCAST service.

   Based on SG-C request, SG-G/D/A may regenerate or reformat SG based on SG-C request.

8. SG-C receives SG through Interaction Channel (SG-6). SG-C may filter SG based on user preference and user profile before it shows SG to a user.

5.4.1.3 Service Guide Delivery to BDS Service Distribution/Adaptation

The figure below shows an example for the Service Guide Delivery to BDS Service Distribution/Adaptation.

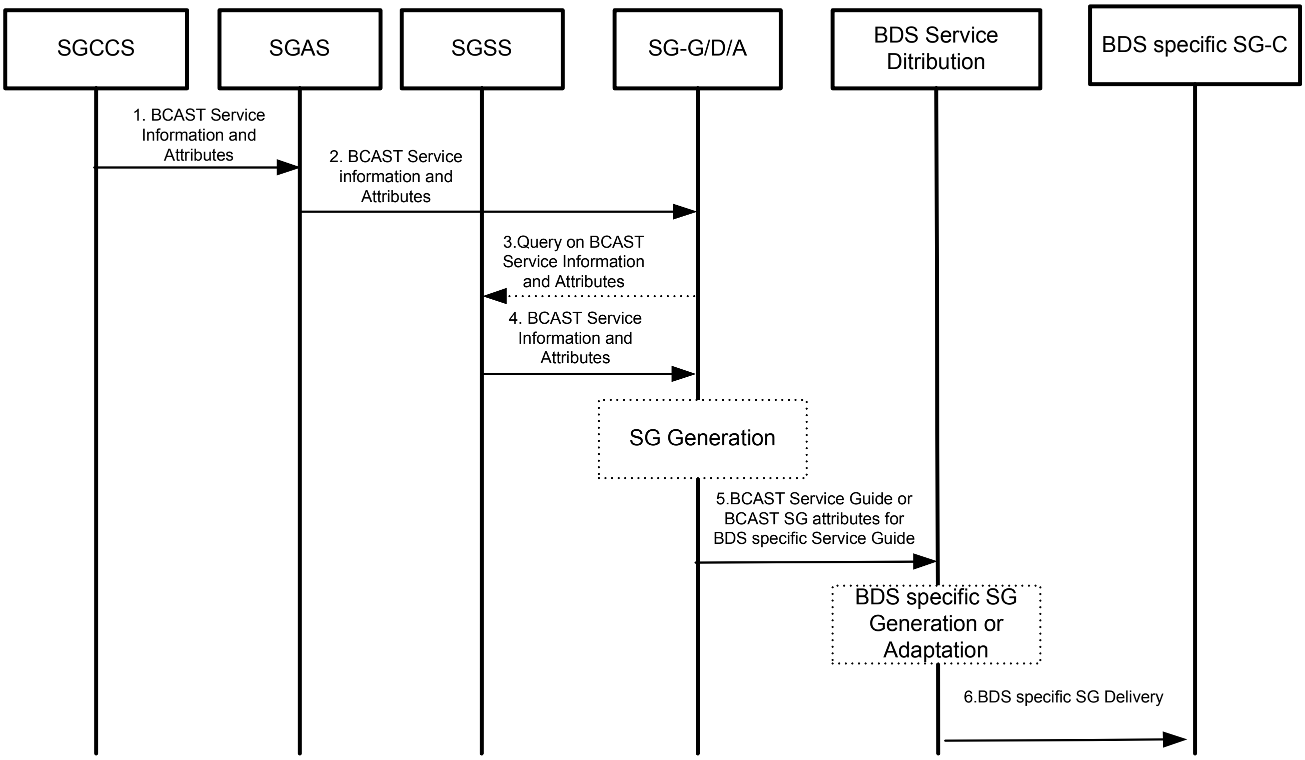

SGCCS
SGAS
SGSS
SG-G/D/A
BDS Service Ditribution
BDS specific SG-C
1. BCAST Service Information and Attributes
2. BCAST Service information and Attributes
3.Query on BCAST Service Information and Attributes
4. BCAST Service Information and Attributes
SG Generation
5.BCAST Service Guide or BCAST SG attributes for BDS specific Service Guide
BDS specific SG Generation or Adaptation
6.BDS specific SG Delivery

Figure 18 - Delivery of Service Guide or Service Guide Attributes to BDS Service Distribution/Adaptation

1. to 4. The operation of Steps 1, 2, 3 and 4 is identical to that of Steps 1, 2, 3, and 4 in Section 5.4.1.1 (SG1, SG2 and SG4).

5. SG-G/D/A generates BCAST Service Guide and transmits it to BDS Service Distribution/Adaptation in order that BDS Service Distribution/Adaptation generates BDS specific Service Guide. SG-G/D/A may transmit BCAST Service Guide attributes to BDS Service Distribution/Adaptation in order that BDS Service Distribution/Adaptation can generate Service Guide with the BCAST Service Guide attributes (SG-B1). BDS Service Distribution/Adaptation receives BCAST Service Guide or BCAST Service Guide attributes and generates BDS specific Service Guide. This operation is out of OMA BCAST Scope.

6. BDS Service Distribution/Adaptation generates BDS Specific SG and delivers it to BDS Specific Service Guide Client in a terminal. The generation, delivery, and reception of BDS-specific Service Guide are out of OMA BCAST scope.

5.4.2 File Distribution Function Related Flows

5.4.2.1 File Distribution over Broadcast channel

The figure below shows an example for File Distribution over Broadcast Channel.

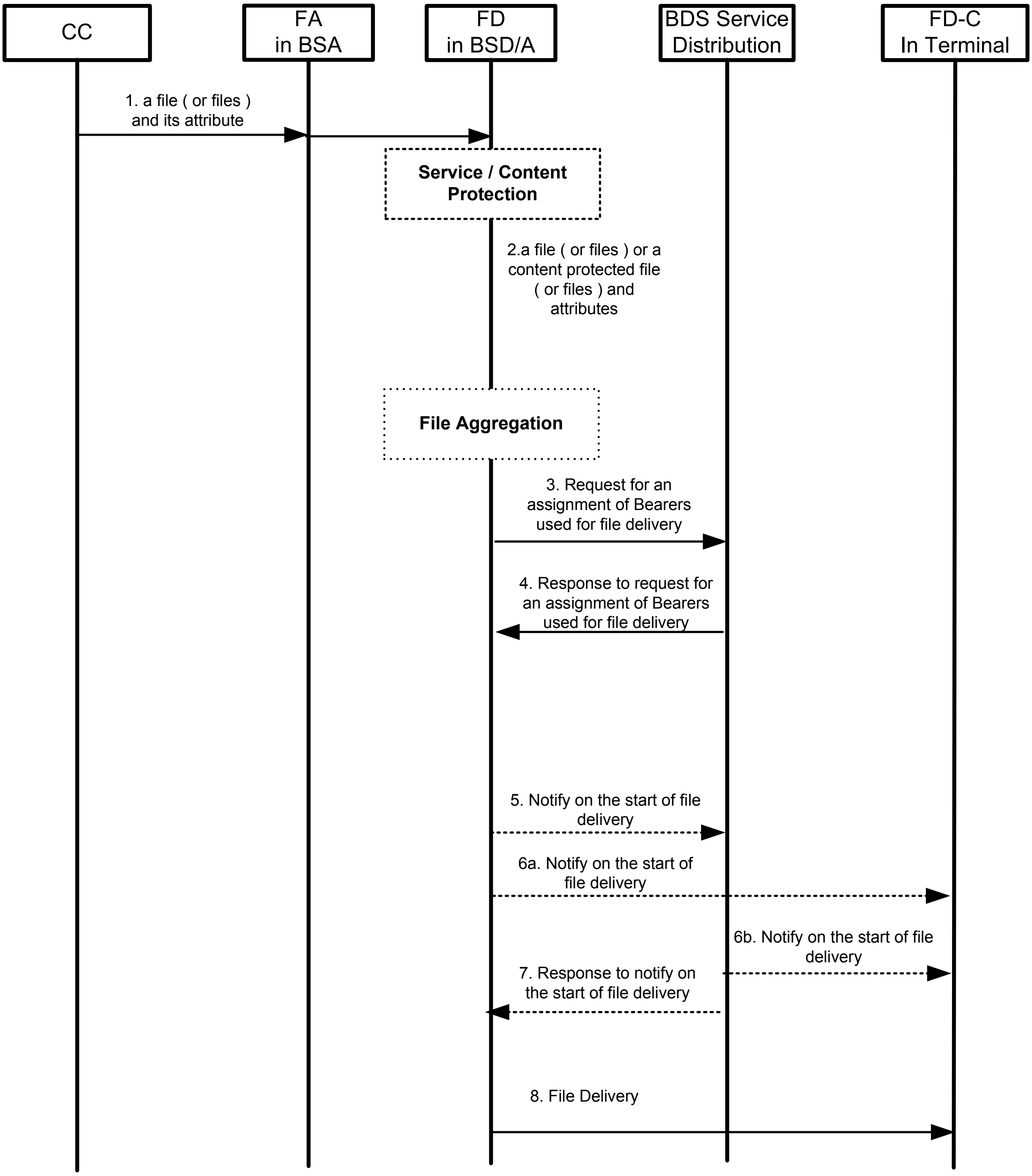

CC
FA in BSA
FD in BSD/A
BDS Service Distribution
FD-C In Terminal
1. a file (or files) and its attribute
Service / Content Protection
2.a file (or files) or a content protected file (or files) and attributes
File Aggregation
3. Request for an assignment of Bearers used for file delivery
4. Response to request for an assignment of Bearers used for file delivery
5. Notify on the start of file delivery
6a. Notify on the start of file delivery
6b. Notify on the start of file delivery
7. Response to notify on the start of file delivery
8. File Delivery

Figure 19 - File Distribution over Broadcast channel

1. The CC sends a file (or files) and its (or their) attributes such as file type to FA in BSA (FD-1).

2. The FA in BSA sends a file (or files) to FD in BSD/A (FD-2). FA also sends the attribute of a file (or files) to FD in BSD/A in order that FD can negotiate bearers to be used for file (or files) distribution with BDS Service

Distribution/Adaptation. The FD in BSD/A may do encryption for Service or Content Protection with the functionality provided by Service or Content Protection Function.

3. Before FD in BSD/A requests bearers to be used for file distribution, FD may aggregate files from a few FAs in order to make a bundle of files. The configuration information of a bundle of files is provided by Service Provisioning Function in BSM. After the aggregation is over, the FD requests the assignment of bearers to be used for file distribution to BDS Service Distribution/Adaptation with the file (or a bundle of files) attributes (FD-B1).

4. To the response to step 3, BDS Service Distribution/Adaptation responds to the request (FD-B1). Normally, BDS Service Distribution/Adaptation assigns the bearers used for file distribution. If BDS Service Distribution/Adaptation does not have a resource for file distribution, it may reject that request. The description about reject case is out of scope of this example. If BDS Service Distribution/Adaptation does not have enough resource, then it may assign bearers which having low data rate than the requested data rate.

5. If Service Protection is required, then FD performs service protection for the file (or bundle of files). After that, FD may notify BDS Service Distribution/Adaptation of the start of file distribution (FD-B1).

6a. FD may notify FD-C in Terminal of the start of file distribution with in-band notification (over FD-5) or out-of-band notification (over FD-6).

6b. BDS Service Distribution/Adaptation may notify FD-C in Terminal of the start of file distribution; how this operates is out of OMA BCAST scope (X4 or X5).

7. If Step 5 exists, BDS Service Distribution/Adaptation may respond to the notification of the start of file distribution (FD-B1).

8. FD in BSD/A distributes the file (or bundle of files) over Broadcast Channel (FD-6). Before the real data transmission, some in-band signaling message can be distributed over the same Broadcast Channel (FD-6).

5.4.2.2 File Repair over Broadcast Channel when Interaction Channel exists

The figure below shows an example for the file repairing over Broadcast Channel. This example can be used if there are many terminals requires the retransmission of a file (or bundle of files) or the retransmission of a portion of a file (or a bundle of files)

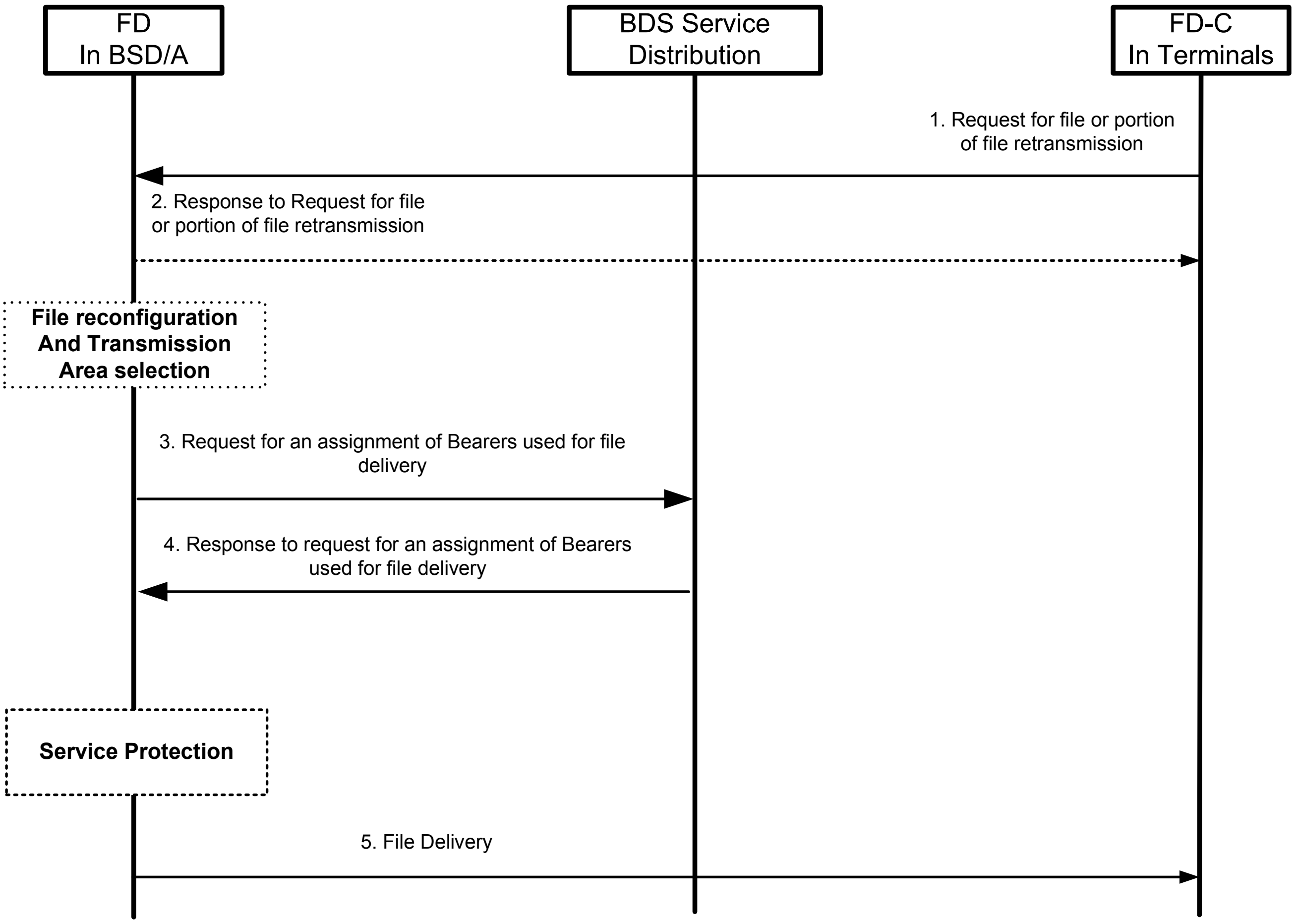

FD
In BSD/A
BDS Service
Distribution
FD-C
In Terminals
1. Request for file or portion of file retransmission
2. Response to Request for file or portion of file retransmission
File reconfiguration And Transmission Area selection
3. Request for an assignment of Bearers used for file delivery
4. Response to request for an assignment of Bearers used for file delivery
Service Protection
5. File Delivery

Figure 20 - File Repairing over Broadcast Channel when Interaction Channel exists

1. The FD-C in the terminal sends the request about the retransmission of a file (or a bundle of files) or the retransmission of a portion of a file (or a bundle of files) to FD in BDS/A (FD-6).
2. The FD in BSD/A may respond to the request from terminals (FD-8).
3. Before FD in BSD/A requests bearers to be used for file distribution (FD-B1), FD may do file reconfiguration (such as, select the missing file or bundle of missing files) in order to avoid transmission of any unnecessary portion of the file or bundle of files. FD may also select transmission area based on terminal request. For this, terminal should include the location information about terminal (e.g., Cell ID) into the terminal request. After the reconfiguration and transmission area selection are over, the FD requests the assignment of bearers to be used for the reconfigured file (or bundle of files) to BDS Service Distribution/Adaptation with the reconfigured file (or a bundle of files) attributes.
4. To the response to step 3, BDS Service Distribution/Adaptation responds to the request (FD-B1). Normally, BDS Service Distribution/Adaptation assigns the bearers used for file distribution. If BDS Service Distribution/Adaptation does not have a resource for file distribution, it may reject that request. The description about reject case is out of scope of this example. If BDS Service Distribution/Adaptation does not have enough resource, then it may assign bearers which having low data rate than the requested data rate.
5. If FD transmits the missing file (or bundle of files) to terminal, then FD transmits the reconfigured file (or bundle of files) to FD-C in Terminal (FD-5). The FD in BSD/A may do encryption for Service or Content Protection with the functionality provided by Service or Content Protection Function before it transmits the missing file to terminal.

5.4.2.3 File transmission or repairing over Interaction Channel when BDS Service Distribution/Adaptation exists

The figure below shows an example for File transmission or repairing over Interaction Channel when BSD Service Distribution exists.

In technical point of view, the file retransmission over Interaction Channel is almost identical to the file transmission over Interaction channel. Therefore, even though the figure below focuses on the file retransmission case, the figure can also cover the file transmission over Interaction channel.

The figure also depicts the file transmission by FD in BSD/A as well as Interaction Channel.

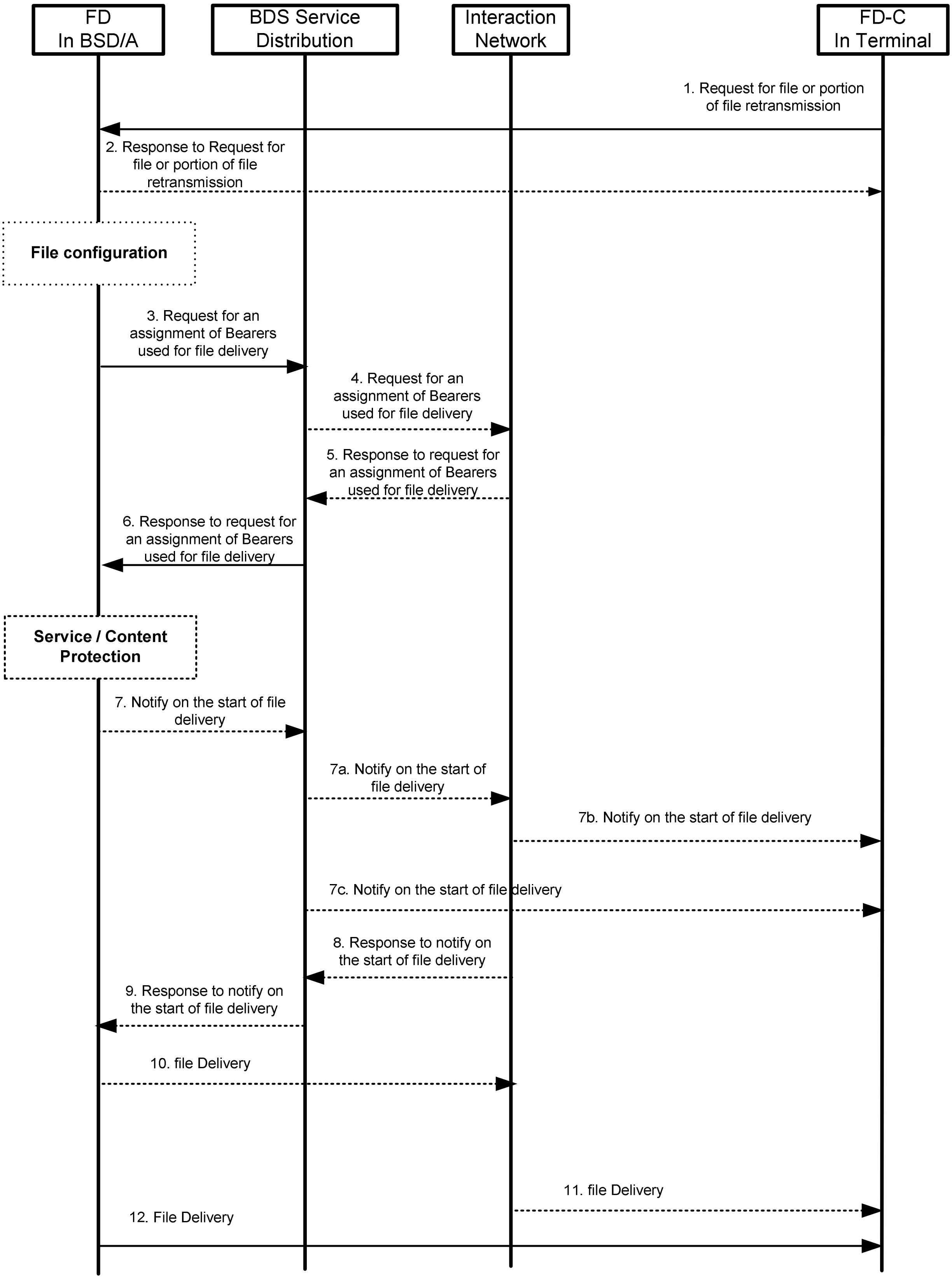

FD
In BSD/A
BDS Service
Distribution
Interaction
Network
FD-C
In Terminal
1. Request for file or portion of file retransmission
2. Response to Request for file or portion of file retransmission
File configuration
3. Request for an assignment of Bearers used for file delivery
4. Request for an assignment of Bearers used for file delivery
5. Response to request for an assignment of Bearers used for file delivery
6. Response to request for an assignment of Bearers used for file delivery
Service / Content Protection
7. Notify on the start of file delivery
7a. Notify on the start of file delivery
7b. Notify on the start of file delivery
7c. Notify on the start of file delivery
8. Response to notify on the start of file delivery
9. Response to notify on the start of file delivery
10. file Delivery
11. file Delivery
12. File Delivery

Figure 21 - File transmission or repairing over Interaction Channel when BSD Service Distribution exists

1. The FD-C in terminals sends the request about the retransmission of a file (or a bundle of files) or the retransmission of a portion of a file (or a bundle of files) to FD in BDS/A (FD-6).
2. The FD in BSD/A may respond to the request from terminals (FD-6).
3. Before FD in BSD/A requests bearers to be used for file distribution, FD may reconfigure the file (or bundle of files) in order not to the unnecessary portion of file or bundle of files is transmitted. After the reconfiguration is over, the FD requests the assignment of bearers to be used for the reconfigured file (or bundle of files) to BDS Service Distribution/Adaptation with the reconfigured file (or a bundle of files) attributes (FD-B1).
4. BDS Service Distribution/Adaptation requests the bearers used for the file transmission to Interaction Network (X-2).
5. Interaction Network responds to the request from BDS Service Distribution/Adaptation (X-2).
6. To the response to step 3, BDS Service Distribution/Adaptation responds to the request from FD in BSD/A (FD-B1).
7. FD may do encryption for Service or Content Protection before it notifies BDS Service Distribution/Adaptation of the start of File transmission. After the encryption for Service or Content Protection is over, FD notifies BDS Service Distribution/Adaptation of the start of file transmission (FD-B1).

7a. BDS Service Distribution/Adaptation notifies Interaction Network of the start of file transmission (X-2).

7b. Interaction Network may notify FD-C in Terminal of the start of File transmission (X-6).

7c. If step 7b does not exist, BDS Service Distribution/Adaptation notifies FD-C in Terminal of the start of file transmission (X-5).

8. To the response to step 7a, Interaction Network may send the response to BDS Service Distribution/Adaptation (X-2).
9. If step 7 exists, BDS Service Distribution/Adaptation may send the response to FD (FD-B1)
10. If Interaction Channel transmits the reconfigured file (or bundle of files) to Terminal, then FD delivers the file (or bundle of files) to Interaction Network (FD-B1 and X-2).
11. As Interaction Network transmits the reconfigured file (or bundle of files), the reconfigured file (or bundle of files) is transmitted to FD-C in the Terminal (X-6).
12. If FD transmits the reconfigured file (or bundle of files) to terminal, then FD transmits the reconfigured file (or bundle of files) to FD-C in Terminal (FD-8).

5.4.2.4 File Delivery to BDS Service Distribution/Adaptation

The figure below shows an example for the file delivery to BDS Service Distribution/Adaptation

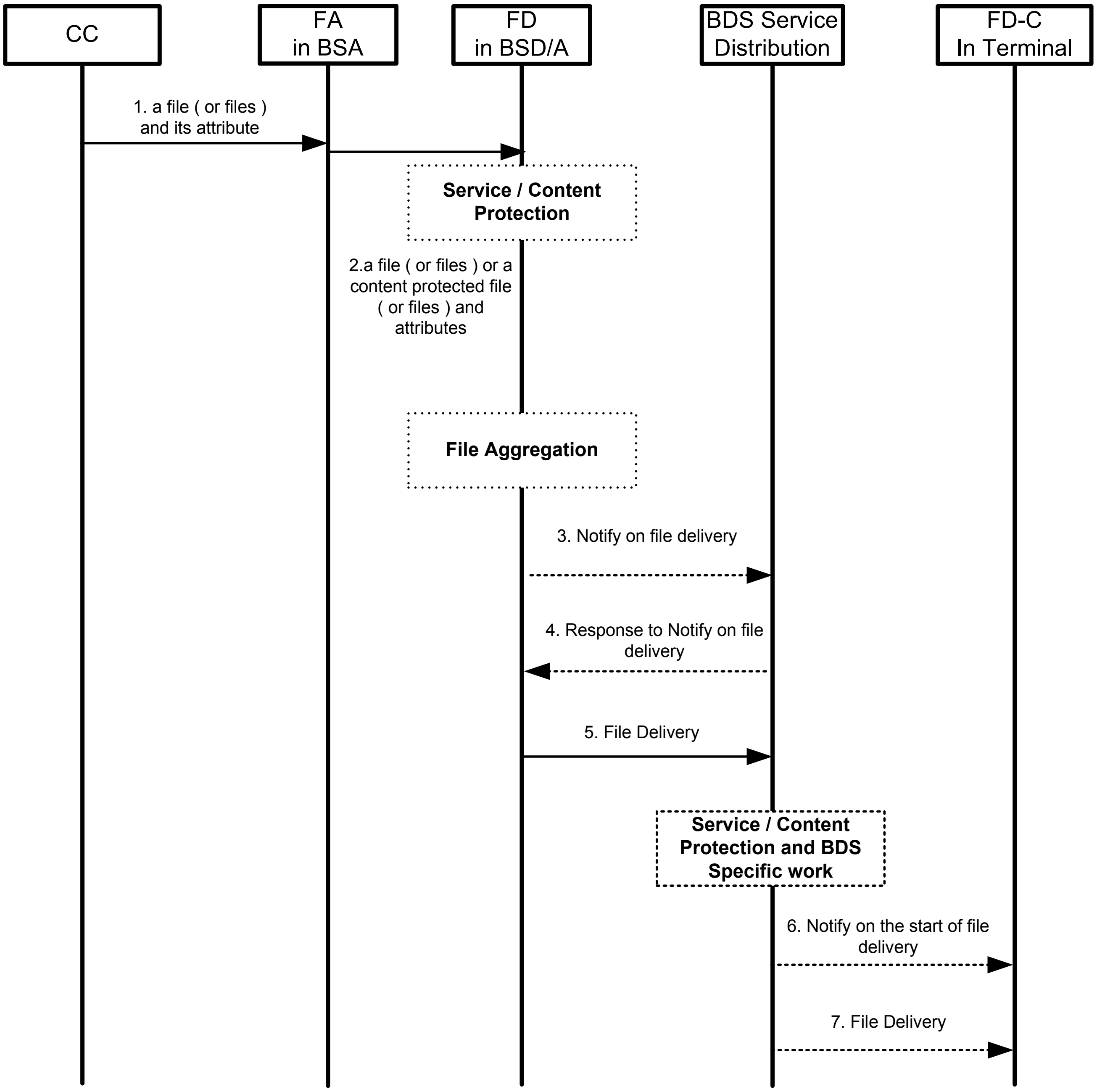


Figure 22 - File Delivery to BDS Service Distribution/Adaptation

1. The CC sends a file (or files) and its (or their) attribute such as file type to FA in BSA.

2. The FA in BSA sends a file (or files) to FD in BSD/A (FD-2). FA also sends the attribute of a file (or files) to FD in BSD/A in order that BDS Service Distribution/Adaptation can determine bearers to be used for file (or files) distribution. The FD in BSD/A may do encryption for Service or Content Protection with the functionality provided by Service or Content Protection Function in BSD/A.

3. Before FD in BSD/A sends a file (or files), FD may aggregate files from a few FAs in order to make a bundle of files. The configuration information of a bundle of files is provided by Service Provisioning Function in BSM. After the aggregation is over, the FD may notify BDS Service Distribution/Adaptation of the start of the file (or bundle of files) delivery (FD-B1).

4. If step 3 exists, BDS Service Distribution/Adaptation may respond about the start of file (or a bundle of files) delivery to FD (FD-B1).
5. FD delivers the file (or a bundle of files) to BDS Service Distribution/Adaptation (FD-B1). BDS Service Distribution/Adaptation may do encryption for Service or Content Protection and BDS Specific work before it distributes the file (or a bundle of files) to Terminals.
6. BDS Service Distribution/Adaptation may notify FD-C in Terminal of the start of the file (or bundle of files) distribution (X-4). The detail operation is out of BCAST scope.
7. BDS Service Distribution/Adaptation distributes the file (or bundle of files) to Terminal (X-1, X-3). The detailed operation is out of BCAST scope.

5.4.2.5 Terminal report about the file reception to FD in BSD/A

The figure below shows an example for Terminal report about the file reception to FD in BSD/A

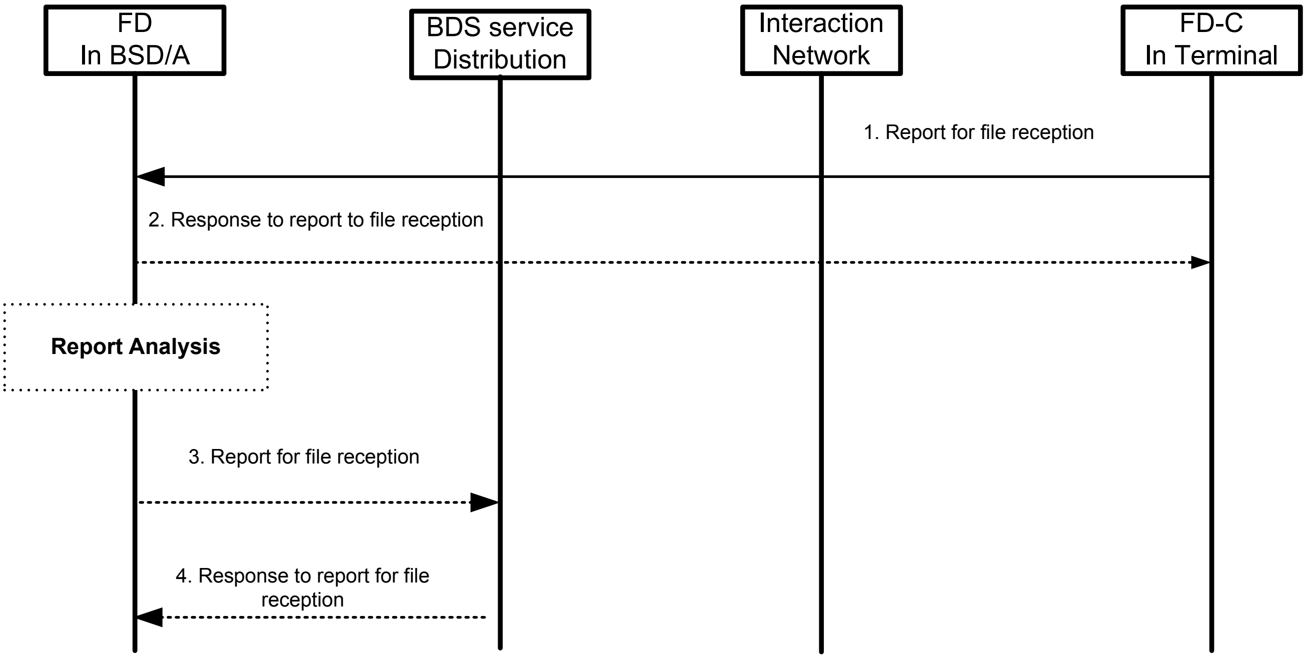

FD
In BSD/A
BDS service
Distribution
Interaction
Network
FD-C
In Terminal
1. Report for file reception
2. Response to report to file reception
Report Analysis
3. Report for file reception
4. Response to report for file
reception

Figure 23 - Terminal report about the file reception to FD in BSD/A

1. The FD-C in Terminal sends the report about the file (or a bundle of files) reception to FD in BSD/A (FD-6). The reports may contain the received quality of file (or a bundle of files) and others.
2. The FD in BSD/A may respond to the terminal report (FD-6). After FD analyzes the terminal report, FD may do some works such as change of Forward Error Correction Scheme in order to improve file reception quality.
3. FD may send the report about file reception to BDS Service Distribution/Adaptation in order that BDS Service Distribution/Adaptation improves file reception quality (FD-B1).
4. BDS Service Distribution/Adaptation may send the response about the report of file reception to FD (FD-B1).

5.4.2.6 Terminal report about the file reception to BDS Service Distribution/Adaptation

The figure below shows an example for Terminal report about the file reception to BDS Service Distribution/Adaptation.

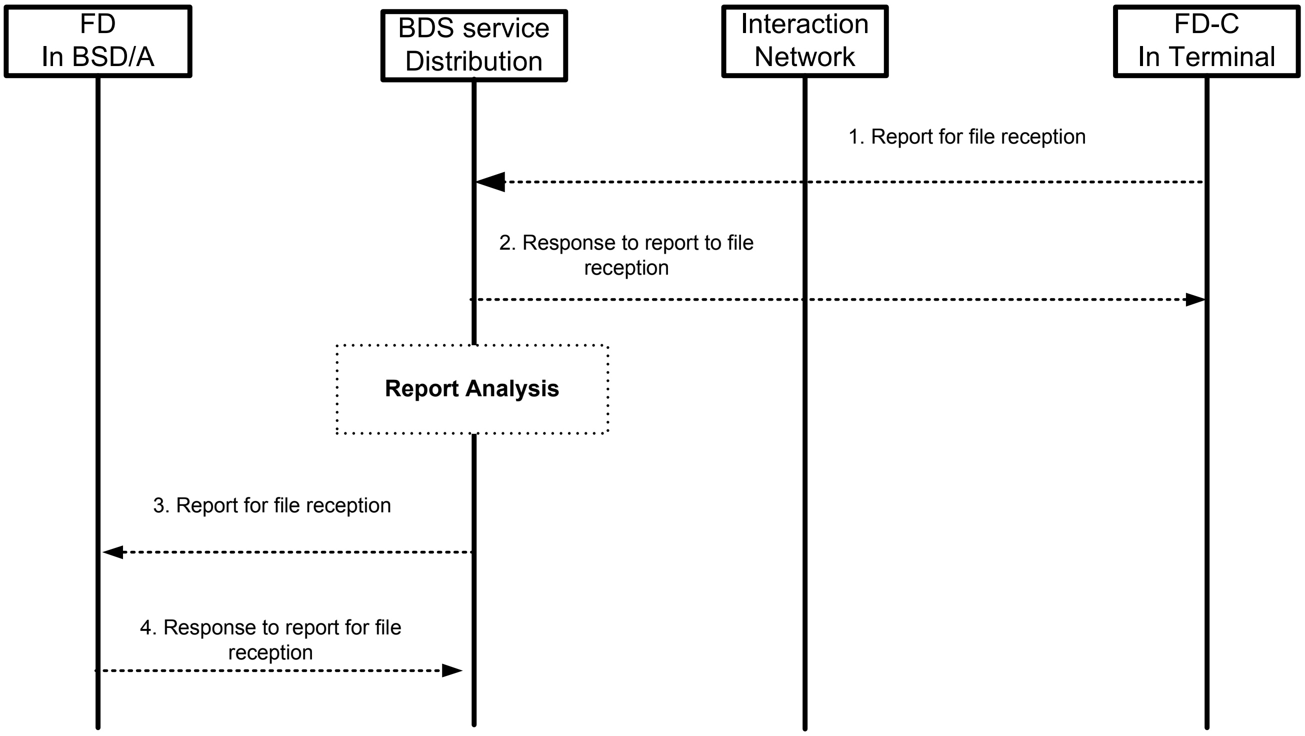

FD
In BSD/A
BDS service
Distribution
Interaction
Network
FD-C
In Terminal
1. Report for file reception
2. Response to report to file reception
Report Analysis
3. Report for file reception
4. Response to report for file reception

Figure 24 - Terminal reports about the file reception to BDS Service Distribution/Adaptation

1. The FD-C in Terminal sends the report about the file (or a bundle of files) reception to BDS Service Distribution/Adaptation. The reports may contain the received quality of file (or a bundle of files) and others (X-5).
2. The BDS Service Distribution/Adaptation may respond to the terminal report (X-5). After BDS Service Distribution/Adaptation analyzes the terminal report, BDS Service Distribution/Adaptation may do some works such as the change of Forward Error Correction Scheme or change of transmission power of file (or bundle of files) in order to improve file reception quality.
3. BDS Service Distribution/Adaptation may send the report about file reception to FD in BSD/A in order that FD improves file reception quality such as the change of Forward Error Collection scheme (FD-B1).
4. FD may send the response about the report of file (or bundle of files) reception to BDS Service Distribution/Adaptation (FD-B1).

5.4.3 Stream Distribution Function Related Flows

5.4.3.1 Stream Distribution over Broadcast channel

The figure below shows an example for Stream Distribution over Broadcast Channel.

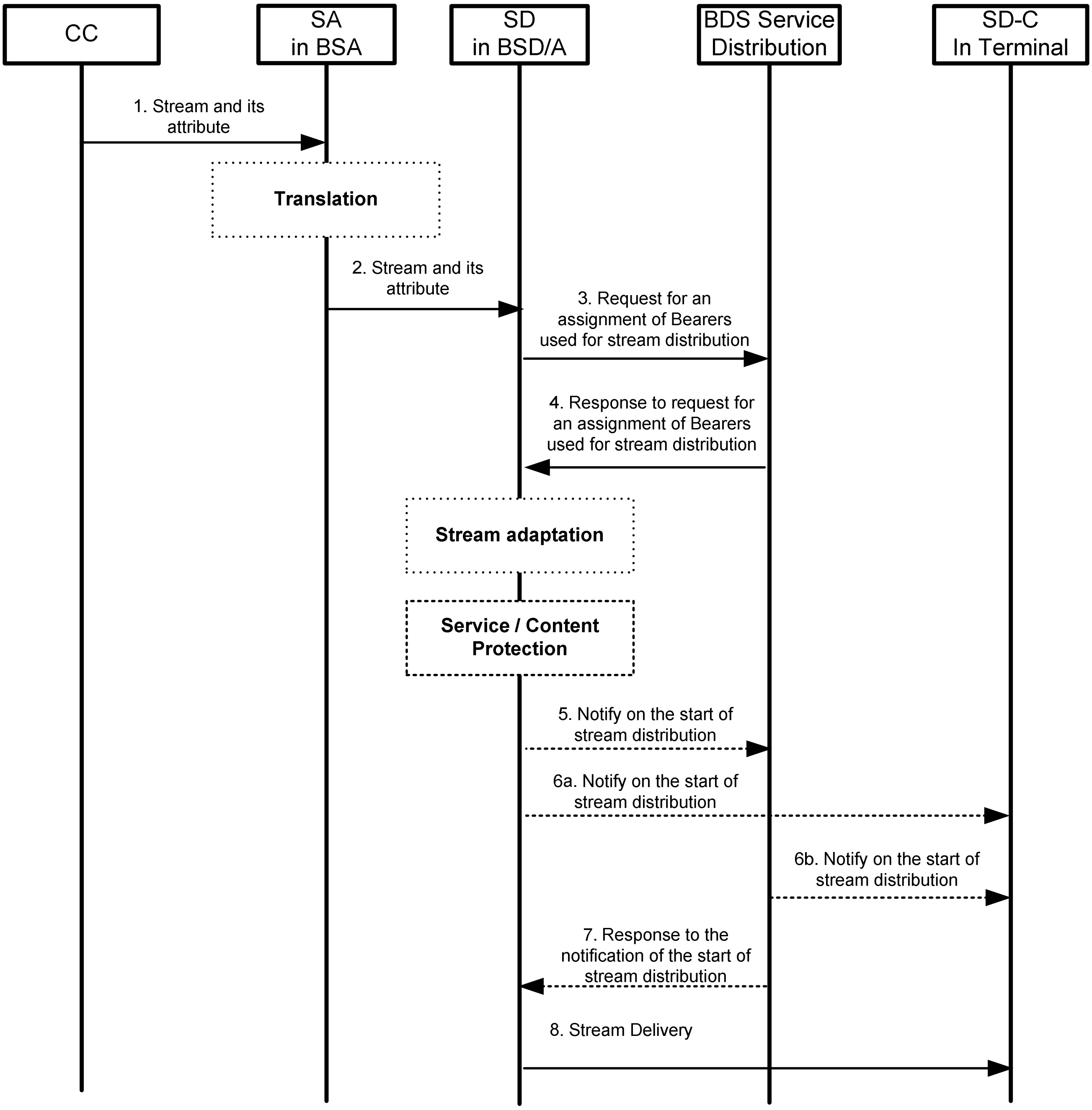

CC
SA in BSA
SD in BSD/A
BDS Service Distribution
SD-C In Terminal
1. Stream and its attribute
Translation
2. Stream and its attribute
3. Request for an assignment of Bearers used for stream distribution
4. Response to request for an assignment of Bearers used for stream distribution
Stream adaptation
Service / Content Protection
5. Notify on the start of stream distribution
6a. Notify on the start of stream distribution
6b. Notify on the start of stream distribution
7. Response to the notification of the start of stream distribution
8. Stream Delivery

Figure 25 - Stream Distribution over Broadcast channel

1. The CC sends stream and its attribute such as media type and CODEC information to SA in BSA. If a media type and CODEC of that stream are different from those of OMA BCAST Standard, then SA translates a stream to BCAST Standard Stream. (SD-1)
2. The SA in BSA sends a stream having BCAST Standard media type and CODEC to SD in BSD/A (SD-2). SA also sends the attribute of a stream to SD in BSD/A in order that SD can negotiate bearers to be used for stream distribution with BDS Service Distribution/Adaptation.
3. The SD in BSD/A requests the assignment of bearers to be used for stream distribution to BDS Service Distribution/Adaptation with the stream attributes (SD-B1).

4. To the response to step 3, BDS Service Distribution/Adaptation responds to the request (SD-B1). Normally, BDS Service Distribution/Adaptation assigns the bearers used for stream distribution. If BDS Service Distribution/Adaptation does not have a resource for stream distribution, it may reject that request. The description about reject case is out of scope of this example. BDS Service Distribution/Adaptation also may request the adaptation of a stream in case that the required data rate for stream delivery is too high or some BDS Specific media type or CODEC should be used for a stream.

5. If BDS specific request exists, SD in BSD/A may adapt BCAST Standard stream for BDS specific stream (SD-B1). If Service or Content Protection is required, then SD provides encryption for service protection or content protection for the stream. After that, SD may notify BDS Service Distribution/Adaptation of the start of stream distribution.

6a. SD may notify SD-C in Terminal of the start of stream distribution via SD-5.

6b. BDS Service Distribution/Adaptation may notify SD-C in Terminal of the start of stream distribution (X-4). How BDS Service Distribution/Adaptation notifies SD-C in Terminal of the start of stream distribution is covered by OMA-TS-BDS- Adaptation Specifications.

7. If Step 5 exists, BDS Service Distribution/Adaptation may respond to the notification of the start of stream distribution (SD-B1).

8. SD in BSD/A distributes the stream over Broadcast Channel (SD-6). Before the real data transmission, some in-band signaling message can be distributed over the same Broadcast Channel.

5.4.3.2 Stream Delivery to BDS Service Distribution/Adaptation

The figure below shows an example for the stream delivery to BDS Service Distribution/Adaptation

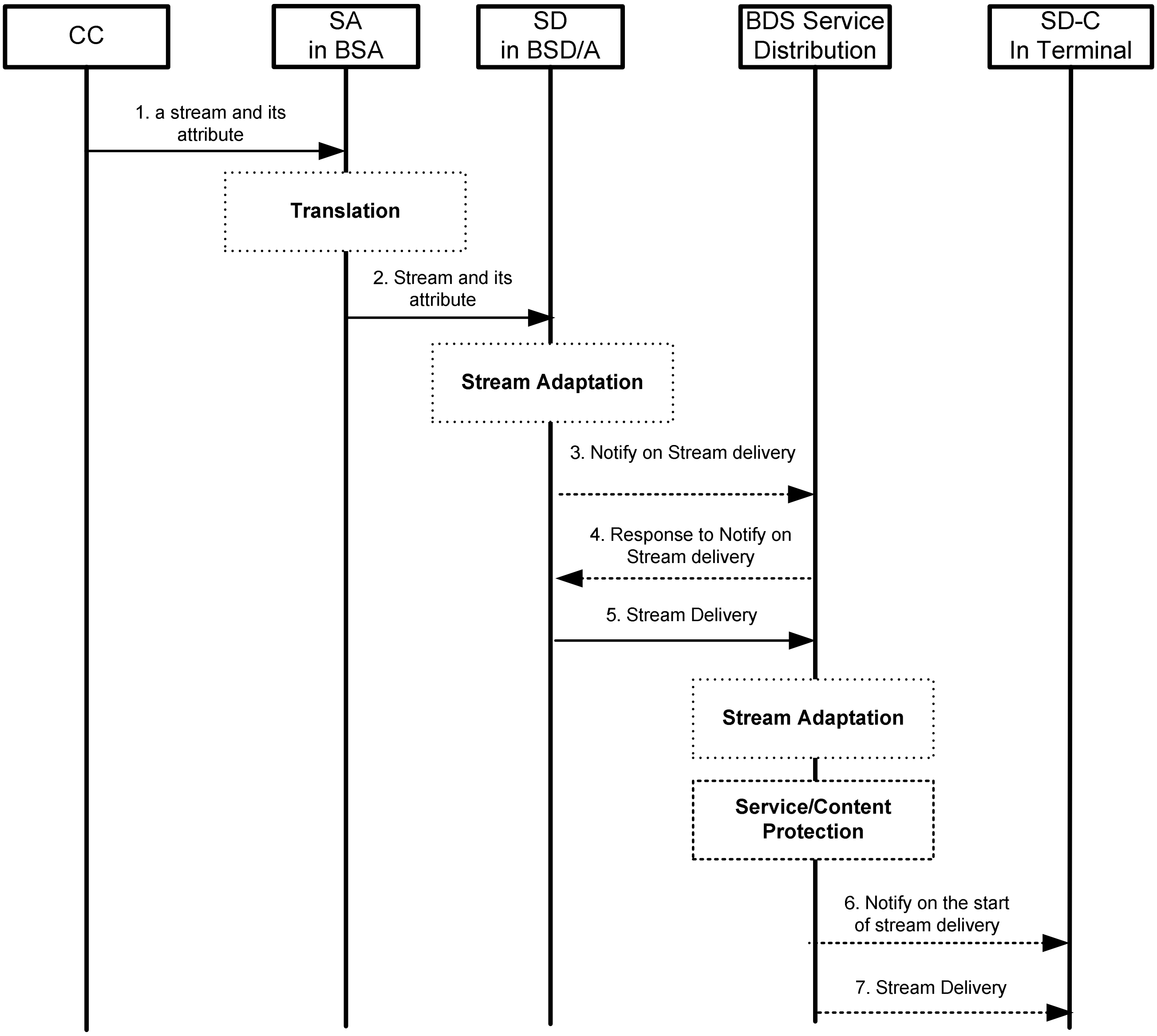

CC
SA in BSA
SD in BSD/A
BDS Service Distribution
SD-C In Terminal
1. a stream and its attribute
Translation
2. Stream and its attribute
Stream Adaptation
3. Notify on Stream delivery
4. Response to Notify on Stream delivery
5. Stream Delivery
Stream Adaptation
Service/Content Protection
6. Notify on the start of stream delivery
7. Stream Delivery

Figure 26 - Stream Delivery to BDS Service Distribution/Adaptation

1. The CC sends stream and its attribute such as media type and CODEC information to SA in BSA. If a media type and CODEC of that stream are different from those of OMA BCAST Standard, then SA translates a stream to BCAST Standard Stream. (SD-1)
2. The SA in BSA sends a stream having BCAST Standard media type and CODEC to SD in BSD/A (SD-2). SA also sends the attribute of a stream to SD in BSD/A in order that SD can inform BDS Service Distribution/Adaptation of the attributes of stream. Before SD delivers a stream to BDS Service Distribution/Adaptation, SD may adapt BCAST Standard Stream to BDS Specific Stream on condition that BDS Specific Codec and media type are known to SD.
3. SD may notify BDS Service Distribution/Adaptation of the start of stream delivery (SD-B1).
4. BDS Service Distribution/Adaptation may send the response about the start of stream delivery to SD (SD-B1).
5. SD delivers the stream to BDS Service Distribution/Adaptation (SD-B1). BDS Service Distribution/Adaptation may do Stream Adaptation and encryption for Service or Content Protection (or Content Protection of RTP streams) before it distributes the stream to Terminals.

6. BDS Service Distribution/Adaptation may notify SD-C in Terminal of the start of stream distribution (X-4). The detailed operation is covered by OMA-TS-BDS- Adaptation Specifications.

7. BDS Service Distribution/Adaptation distributes the stream to Terminal (X-1, X-3). The detailed operation is covered by OMA-TS-BDS- Adaptation Specifications.

The figure below shows an example of stream delivery whereby adaptation is performed by the BSD/A and native BDS service protection is performed by the BDS Service Distribution/Adaptation.

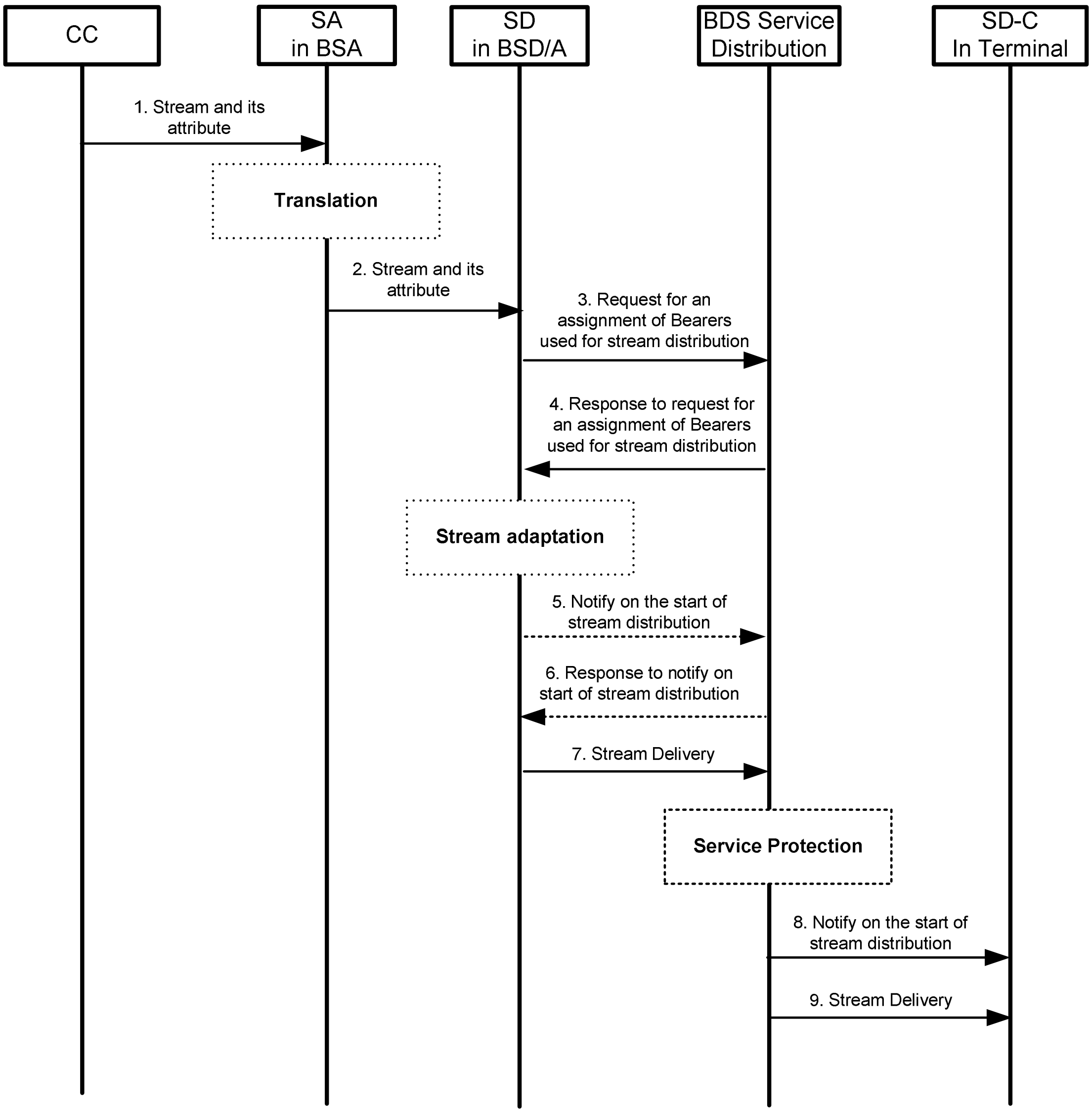

CC
SA in BSA
SD in BSD/A
BDS Service Distribution
SD-C In Terminal
1. Stream and its attribute
Translation
2. Stream and its attribute
3. Request for an assignment of Bearers used for stream distribution
4. Response to request for an assignment of Bearers used for stream distribution
Stream adaptation
5. Notify on the start of stream distribution
6. Response to notify on start of stream distribution
7. Stream Delivery
Service Protection
8. Notify on the start of stream distribution
9. Stream Delivery

Figure 27 -- Stream Distribution with Stream Adaptation Performed by BSD/A and Service Protection by BDS-SD/A

1. The CC sends stream and its attribute such as media type and CODEC information to SA in BSA. If a media type and CODEC of that stream are different from those of OMA BCAST Standard, then SA translates a stream to BCAST Standard Stream (SD-1).

2. The SA in BSA sends a stream having BCAST Standard media type and CODEC to SD in BSD/A (SD-2). SA also sends the attribute of a stream to SD in BSD/A in order that SD can negotiate bearers to be used for stream distribution with BDS Service Distribution/Adaptation.

3. The SD in BSD/A requests the assignment of bearers to be used for stream distribution to BDS Service Distribution/Adaptation with the stream attributes (SD-B1).
4. To the response to step 3, BDS Service Distribution/Adaptation responds to the request (SD-B1). Normally, BDS Service Distribution/Adaptation assigns the bearers used for stream distribution. If BDS Service Distribution/Adaptation does not have a resource for stream distribution, it may reject that request. The description about reject case is out of scope of this example. BDS Service Distribution/Adaptation also may request the adaptation of a stream in case that the required data rate for stream delivery is too high or some BDS Specific media type or CODEC should be used for a stream.
5. SD notifies BDS Service Distribution/Adaptation of the start of stream delivery (SD-B1).
6. BDS Service Distribution/Adaptation may send the response about the start of stream delivery to SD (SD-B1).
7. SD delivers the stream to BDS Service Distribution/Adaptation (SD-B1). BDS Service Distribution/Adaptation performs native BDS Service Protection of RTP stream before it distributes the stream to Terminals.
8. BDS Service Distribution/Adaptation may notify SD-C in Terminal of the start of stream distribution (X-4). The detailed operation is BDS-dependent and described in the corresponding BDS adaptation specifications.
9. BDS Service Distribution/Adaptation distributes the stream to Terminal (X-1, X-3). The detailed operation is BDS-dependent and described in the corresponding BDS adaptation specifications.

5.4.3.3 Terminal report about the stream reception to SD in BSD/A

The figure below shows an example for Terminal report about the stream reception to SD in BSD/A.

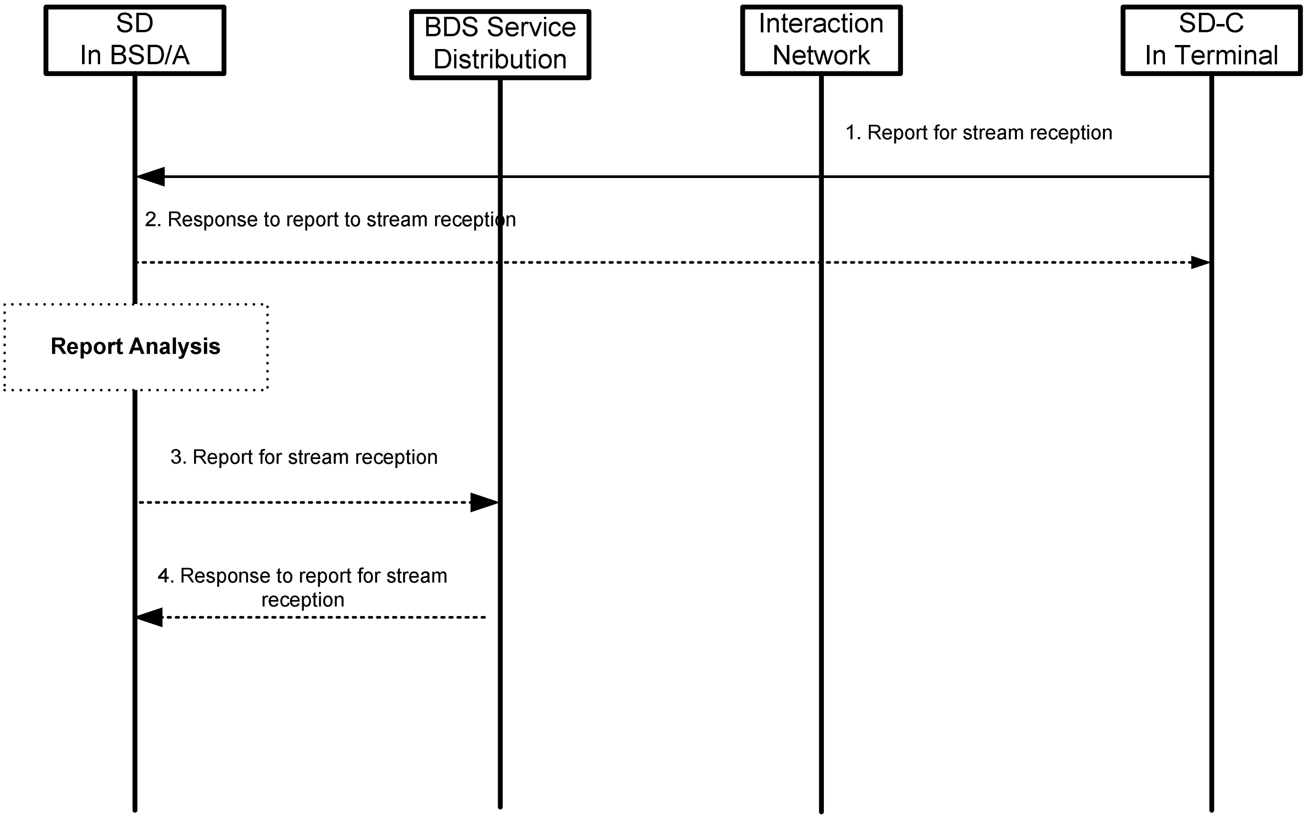

SD
In BSD/A
BDS Service
Distribution
Interaction
Network
SD-C
In Terminal
1. Report for stream reception
2. Response to report to stream reception
Report Analysis
3. Report for stream reception
4. Response to report for stream
reception

Figure 28 - Terminal report about the stream reception to SD in BSD/A

1. The SD-C in Terminal sends the report about the stream reception to SD in BSD/A. The reports may contain the received quality of stream and others (SD-6).

2. The SD in BSD/A may respond to the terminal report (SD-6). After SD analyzes the terminal report, SD may do some works, such as, change of Forward Error Correction Scheme in order to improve stream reception quality.
3. SD may send the report about stream reception to BDS Service Distribution/Adaptation in order that BDS Service Distribution/Adaptation improves stream reception quality (SD-B1).
4. BDS Service Distribution/Adaptation may send the response about the report of stream reception to SD (SD-B1).

5.4.3.4 Terminal report about the stream reception to BDS Service Distribution/Adaptation

The figure below shows an example for Terminal report about the stream reception to SD in BSD/A.

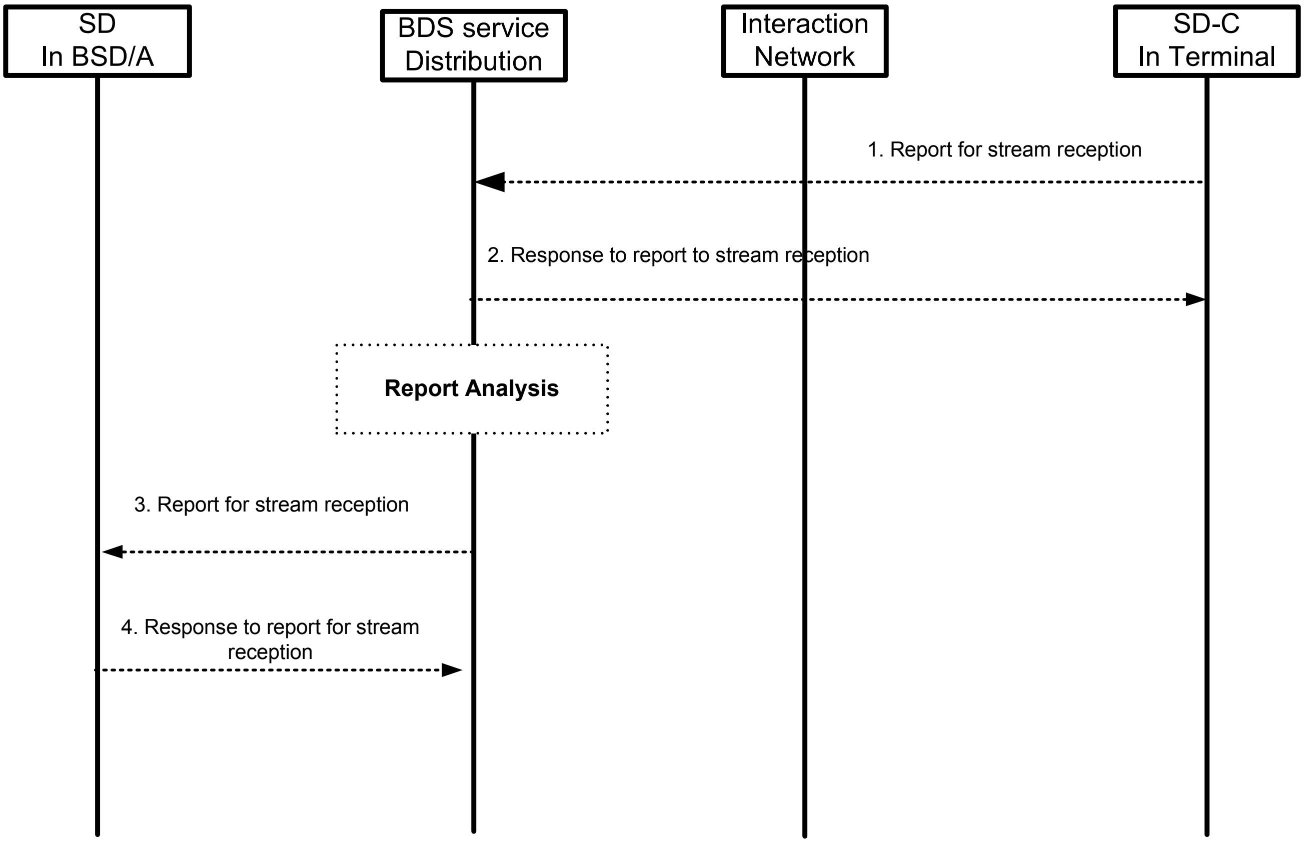

SD
In BSD/A
BDS service
Distribution
Interaction
Network
SD-C
In Terminal
1. Report for stream reception
2. Response to report to stream reception
Report Analysis
3. Report for stream reception
4. Response to report for stream
reception

Figure 29 - Terminal report about the stream reception to BDS Service Distribution/Adaptation

1. The SD-C in Terminal sends the report about the stream reception to BDS Service Distribution/Adaptation. The reports may contain the received quality of stream and others (SD-6).
2. The BDS Service Distribution/Adaptation may respond to the terminal report (SD-6). After BDS Service Distribution/Adaptation analyzes the terminal report, BDS Service Distribution/Adaptation may do some works such as the change of Forward Error Correction Scheme or change of transmission power of stream in order to improve stream reception quality.
3. BDS Service Distribution/Adaptation may send the report about stream reception to SD in BSD/A in order that SD improves stream reception quality, such as, the change of Forward Error Collection scheme (SD-B1).
4. SD may send the response about the report of stream reception to BDS Service Distribution/Adaptation.(SD-B1).

5.4.4 Service Protection Function Related Flows

5.4.4.1 Service Protection Function Flows for DRM Profile

5.4.4.1.1 The Overall Flow for Terminal with Interaction Channel Capability Supporting DRM Profile

The figure shows an example for the general service protection flow for Terminals with an interaction channel in the case the BSM generates the STKM.

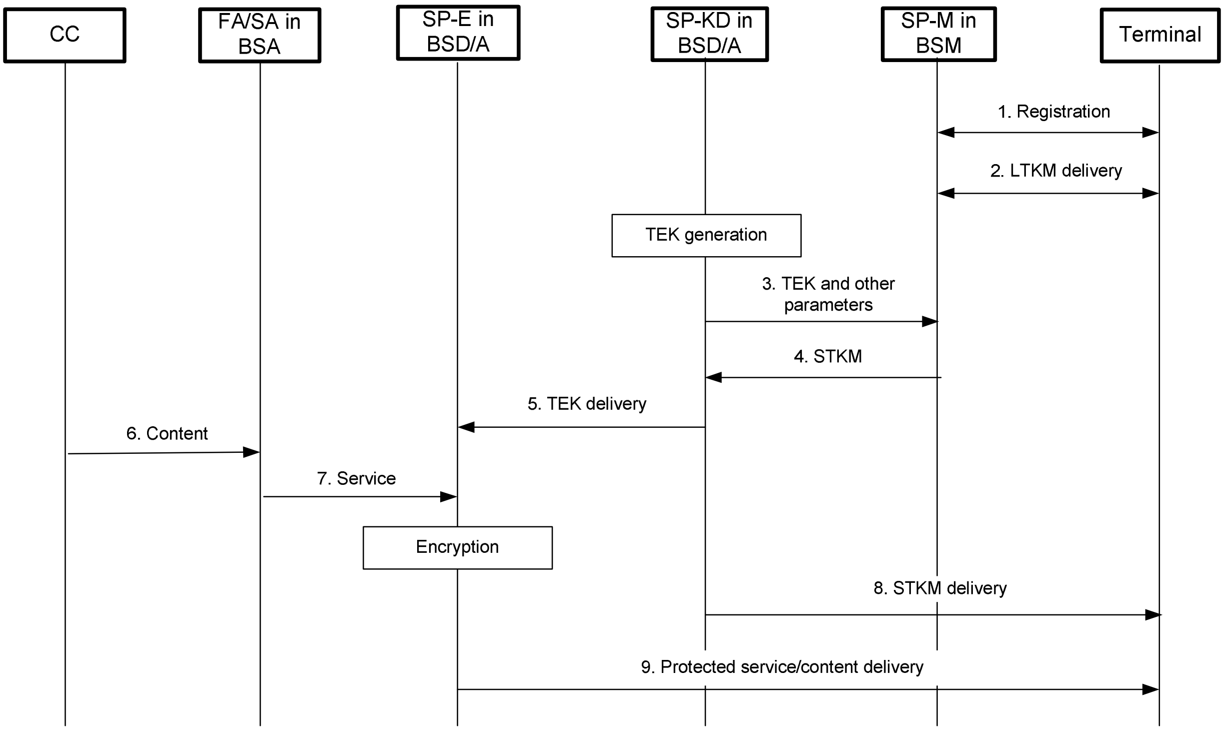


Figure 30 - Service Protection Function Flow for Interaction Terminal supporting DRM Profile

1. The Terminal initiates the registration procedure following OMA DRM 4-pass Registration Protocol.
2. The SP-M in BSM delivers a LTKM to the SP-C using 2-pass Rights Object Acquisition Protocol.
3. The BSD/A generates a TEK for encryption of file or stream and delivers it with other parameters to the SP-M in BSM for STKM generation
4. The SP-M in BSM generates a STKM and delivers it to the BSD/A. STKM can also be generated by the BSD/A. In this case, the BSD/A acquires SEAK or PEAK from the BSM for encryption of STKM.
5. The SP-KD in BSD/A delivers TEK to the SP-E in BSD/A for encryption.
6. The CC delivers contents to the FA/SA in BSA.
7. The FA/SA in BSA generates a service from content and delivers service to the SP-E in BSD/A.
8. The SP-KD in BSD/A broadcasts STKM to Terminals.
9. The SP-E in BSD/A sends encrypted file or stream to the Terminal over the broadcast channel or interaction channel.

5.4.4.1.1.1 Registration

The registration procedure for interaction terminals is same as 4-pass Registration Protocol from OMA DRM v2.0.

5.4.4.1.1.2 LTKM Delivery

The LTKM delivery procedure for interaction terminals is same as 2-pass Rights Object Acquisition Protocol from OMA DRM v2.0.

5.4.4.1.1.3 STKM Delivery over Broadcast Channel or Interaction Channel

The figure shows an example for STKM delivery procedure over broadcast channel or interaction channel.

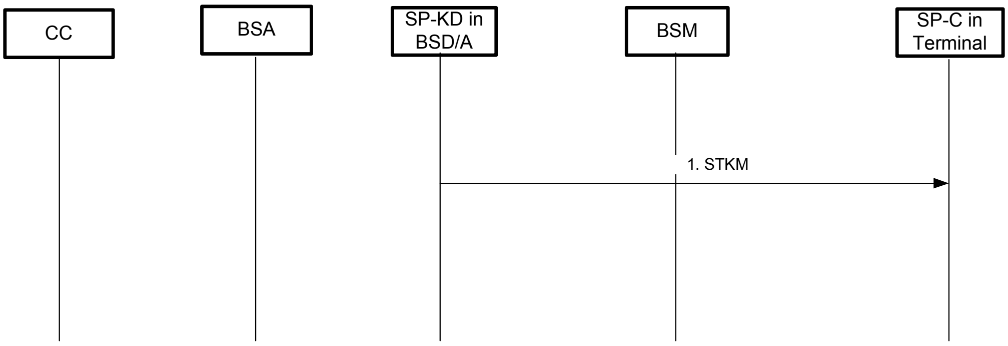


Figure 31 - STKM Delivery Flow for Broadcast-only Terminal

1. STKM from the BSD/A is delivered over the broadcast channel or interaction channel to the Terminal.

5.4.4.1.1.4 Re-Keying

The figure shows an example of the Terminal acquiring an updated SEAK/PEAK by 2-pass Rights Object Acquisition Protocol with ROAP Trigger.

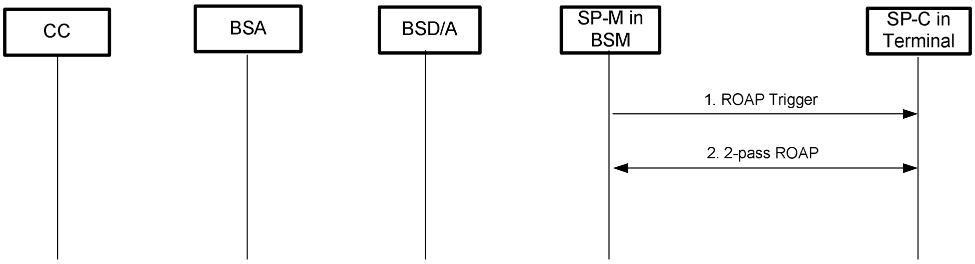


Figure 32 - Re-Keying Flow for DRM Profile with Interaction Channel

1. When it is required to change a SEAK or PEAK, the BSM sends a ROAP Trigger message to Terminal.
2. After receiving a ROAP Trigger message from the BSM, the Terminal starts 2-pass Rights Object Acquisition Protocol with the BSM to acquire a new SEAK or PEAK.

5.4.4.1.2 The Overall Flow for Broadcast-only Terminal Supporting DRM Profile

The figure shows an example of service protection function flow for broadcast-only terminal.

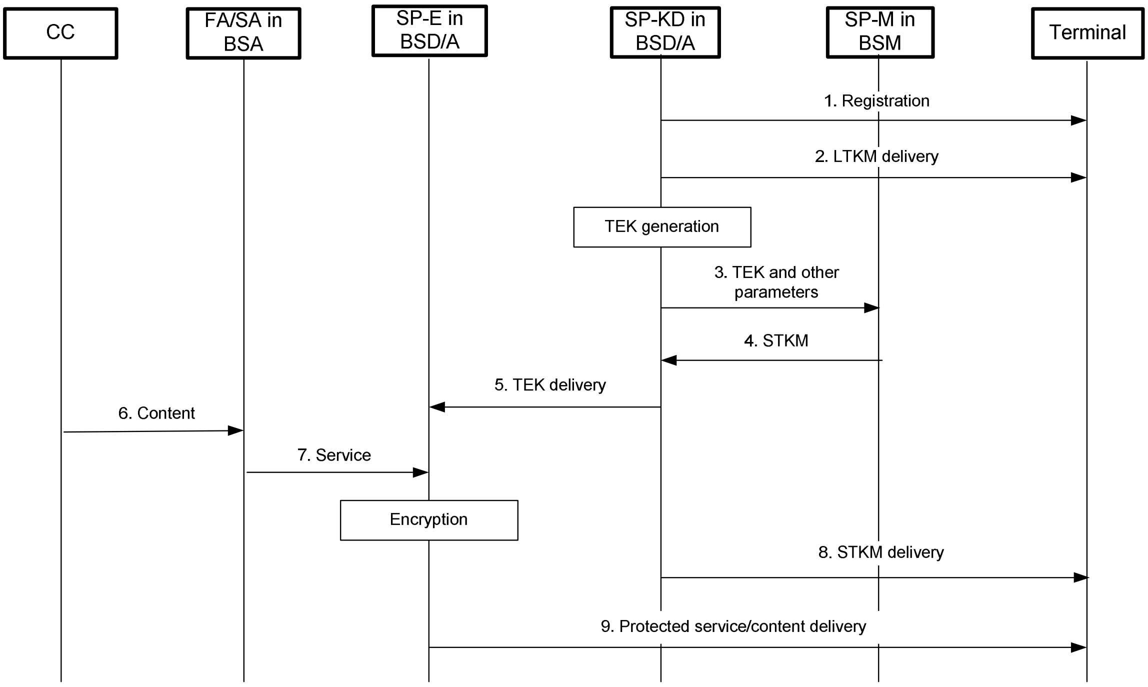


Figure 33 - Service Protection Function Flow for Broadcast-only Terminal with DRM Profile

1. The Terminal sends Registration request to the SP-M in BSM using out-of-band channel. The Terminal receives Registration message using broadcast channel.
2. The Terminal also receives LTKM over broadcast channel.
3. The BSD/A generates a TEK for encryption of file or stream and delivers it with other parameters to the SP-M in BSM for STKM generation
4. The SP-M in BSM generates a STKM and delivers it to the BSD/A. STKM can also be generated by the BSD/A. In this case, the BSD/A acquires SEAK or PEAK from the BSM for encryption of STKM.
5. The SP-KD in BSD/A delivers TEK to the SP-E in BSD/A for encryption.
6. The CC delivers contents to the FA/SA in BSA.
7. The FA/SA in BSA generates a service from content and delivers service to the SP-E in BSD/A.
8. The SP-KD in BSD/A broadcasts STKM to Terminals.
9. The SP-E in BSD/A broadcasts encrypted file or stream to the Terminal.

5.4.4.1.2.1 Registration

The figure shows an example for the broadcast-only terminal to have a registration procedure.

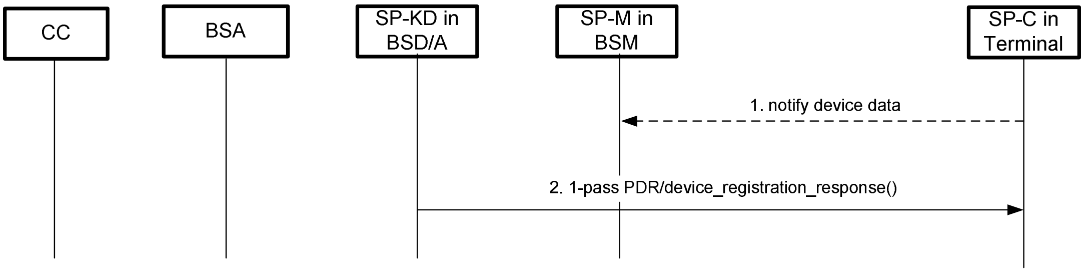


Figure 34 - Registration Flow for Broadcast-only Terminal

1. The SP-C in Terminal delivers device data to the BSM using out-of-band channel. There can be many possible ways to deliver device data to BSM using out of band channel.
2. The SP-KD in BSD/A broadcasts device_registration_response message() to the Terminal.

5.4.4.1.2.2 LTKM Delivery

The figure shows an example for a Terminal to acquire a LTKM(BCRO) using the broadcast channel.

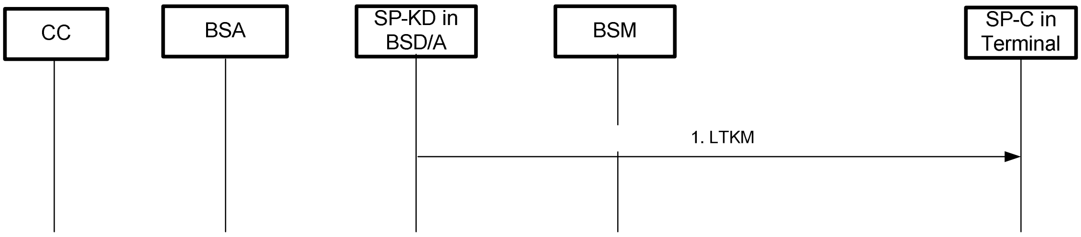


Figure 35 - LTKM Delivery Flow for Broadcast-only Terminal

1. The SP-KD in BSD/A delivers a LTKM(BCRO) to the Terminal.

5.4.4.1.2.3 STKM Delivery over Broadcast Channel

This section is identical to the Sect.5.4.4.1.1.3.

5.4.4.1.2.4 Re-Keying Flow

The figure shows an example for re-keying procedure for broadcast-only terminal.

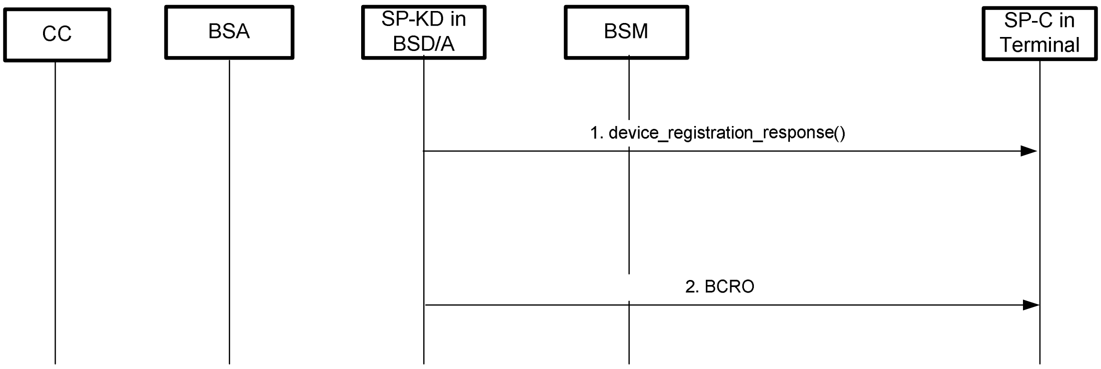


Figure 36 - Re-Keying Flow for Broadcast-only Terminal

1. The SP-KD in BSD/A sends device_registration_response() to the SP-C in Terminal. The Terminal acquires a new registration material.
2. The Terminal acquires BCRO from the SP-KD in BSD/A. The Terminal can decrypt BCRO using the registration material acquired from the step 1.

5.4.4.2 Service Protection Function Flows for Smartcard Profile

5.4.4.2.1 The Overall Flow for Smartcard Profile with Interaction Channel

The following figure shows an example of overall service protection function flow for terminal with the Smartcard Profile in the case the BSM generates the STKM.

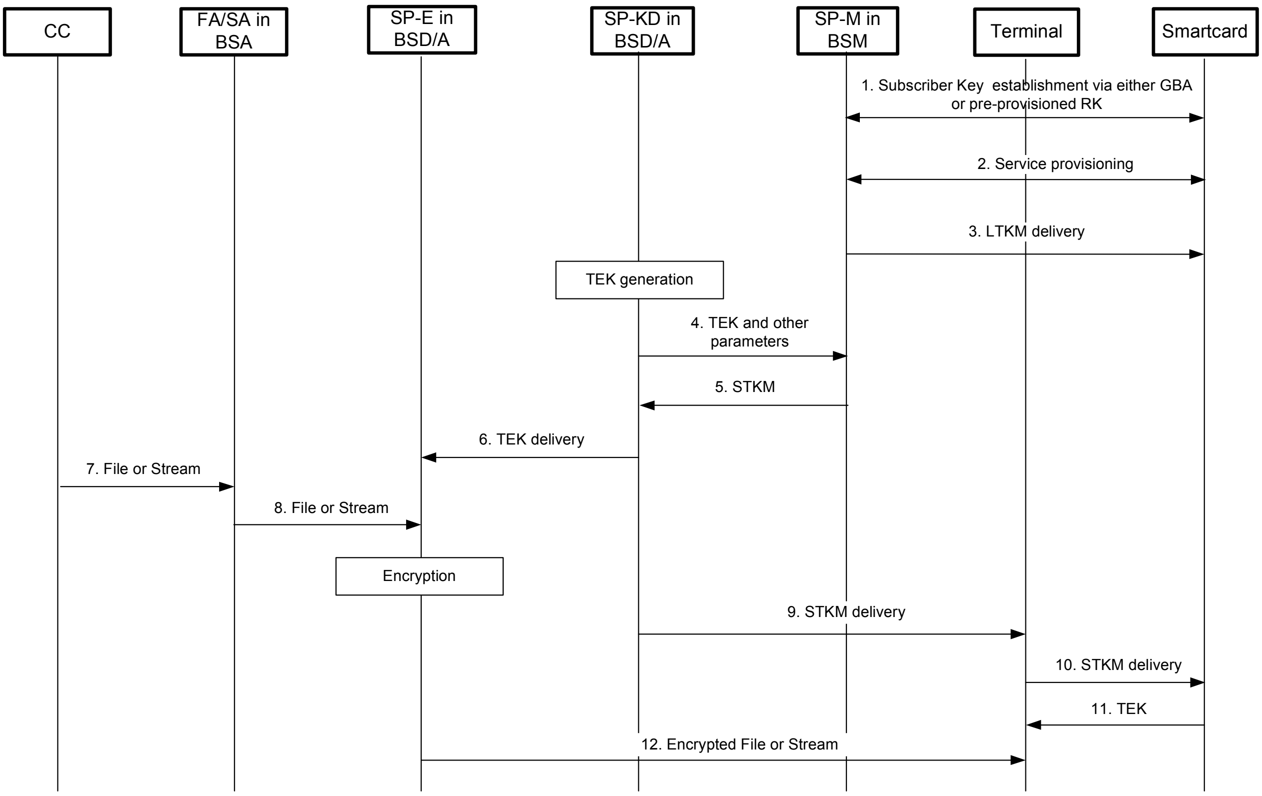


Figure 37 - Service Protection Function Flow for Terminal with Smartcard Profile

1. The Smartcard executes Subscriber Key establishment procedure via either GBA or pre-provisioned RK with the SP-M in BSM.
2. Service Provisioning messages are exchanged in order to subscribe to services or purchase tokens.
3. The Smartcard receives LTKM from the SP-M in BSM.
4. The BSD/A generates a TEK for encryption of file or stream and delivers it with other parameters to the SP-M in BSM for STKM generation
5. The SP-M in BSM generates a STKM and delivers it to the BSD/A for distribution. STKM can also be generated by the BSD/A. In this case, the BSD/A acquires SEK or PEK from the BSM for encryption of STKM.
6. The SP-KD in BSD/A delivers TEK to the SP-E in BSD/A for encryption.
7. The CC delivers contents to the FA/SA in BSA.
8. The FA/SA in BSA generates a service from content and delivers service to the SP-E in BSD/A.
9. The SP-KD in BSD/A broadcasts STKM to the Smartcard.
10. The Terminal sends STKM to the Smartcard.
11. The Smartcard extracts TEK from STKM and delivers it to the Terminal.
12. The SP-E in BSD/A sends encrypted file or stream to the Terminal over the broadcast channel or the interaction channel. The Terminal can decrypt encrypted file or stream using TEK received from the Smartcard.

5.4.4.2.1.1 Subscriber Key Establishment

The following figure shows an example of the subscriber key establishment procedure for the Smartcard Profile with Service Protection.

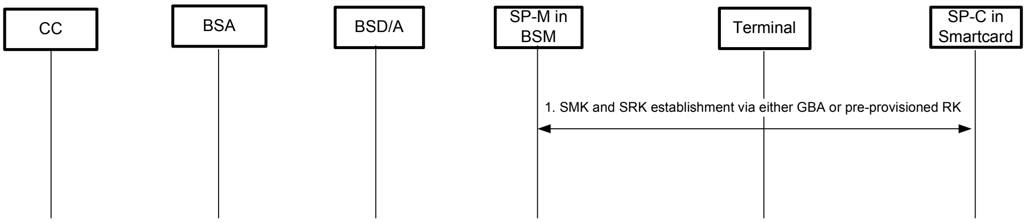

CC
BSA
BSD/A
SP-M in BSM
Terminal
SP-C in Smartcard
1. SMK and SRK establishment via either GBA or pre-provisioned RK

Figure 38 - Subscriber Key Establishment Flow for Smartcard Profile with Service Protection

1. The SP-C in Smartcard acquires SMK and SRK via either GBA or pre-provisioned RK. SMK is used to protect a SEK or PEK.

For (U)SIM Smartcard Profile, the SMK and SRK are established via the GBA bootstrapping and bootstrap usage procedures as described in [3GPP TS 33.246] Section 6.1. For (R-)UIM/CSIM Smartcard Profile, the SMK and SRK are derived from the pre-provisioned Registration Key (RK) in the Smartcard, as described in [3GPP2 S.S0083-A].

5.4.4.2.1.2 Push LTKM Delivery

The figure shows an example of LTKM delivery flow for Smartcard Profile with Service Protection.

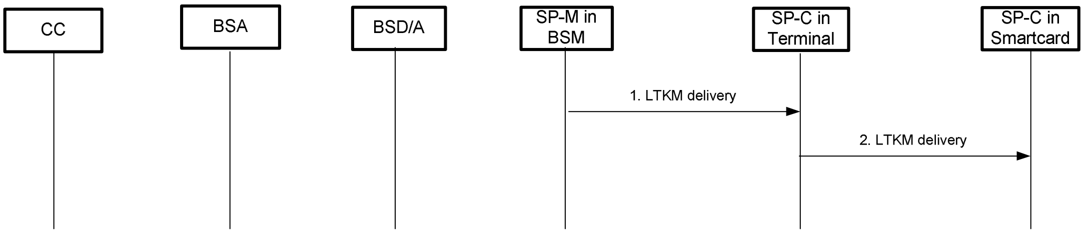


Figure 39 - Push LTKM Delivery Flow

1. The SP-M in BSM pushes LTKMs to the Terminal over UDP.
2. The Terminal with Smartcard acquires the LTKM from the BSM and delivers the LTKM to the Smartcard.
3. The SP-C in Smartcard acquires the LTKM from the Terminal.

5.4.4.2.1.3 STKM Delivery over Broadcast Channel or Interaction Channel

The following figure shows an example of STKM delivery over broadcast channel or interaction channel for the Smartcard Profile.

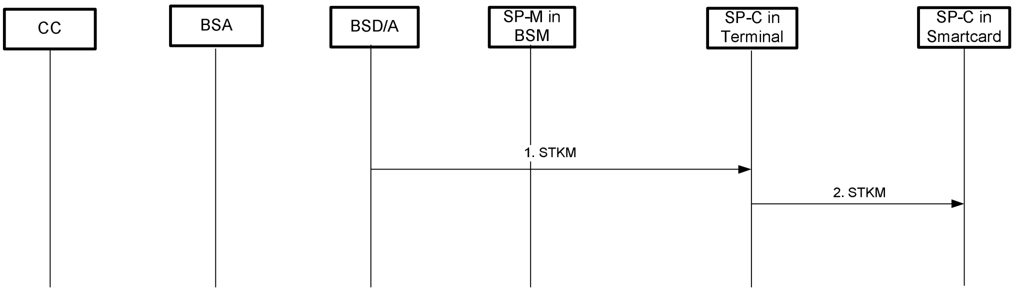


Figure 40 - STKM Delivery Flow over Broadcast Channel or Interaction Channel

1. The SP-C in Terminal receives the STKM over broadcast channel or interaction channel from the BSD/A.
2. The Terminal forwards the STKM to the Smartcard.

5.4.4.2.1.4 LTKM Request Procedure

The following figure shows an example of the LTKM request procedure for the Smartcard Profile with Service Protection.

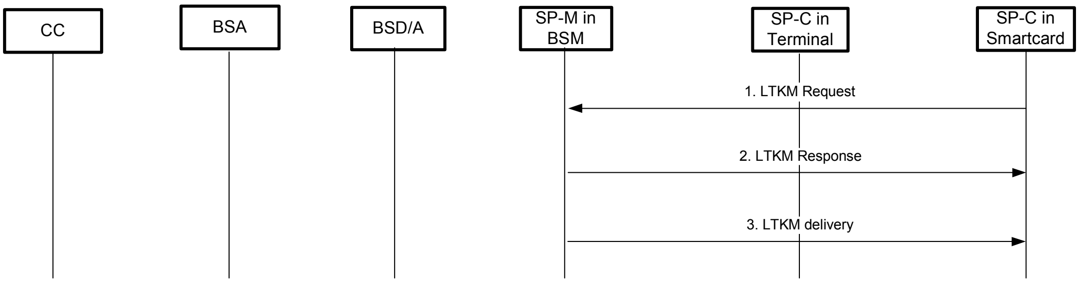


Figure 41 - LTKM Request Procedure Flow

1. The SP-C in Smartcard runs the LTKM Request procedure to request a missed LTKM.
2. The BSM sends the LTKM Response to the Terminal.
3. The Terminal receives the LTKM from the BSM. The Terminal delivers the LTKM to the Smartcard.

5.4.4.3 Backend Interface Function Flows

This backend interface functions flows apply to both DRM Profile and Smartcard Profile.

5.4.4.3.1 Registration Key Material Delivery

The following figure shows an example of the registration key material delivery flow from the BSM to the BSD/A. After that, the BSD/A can deliver the registration key material to the Terminal over broadcast channel.

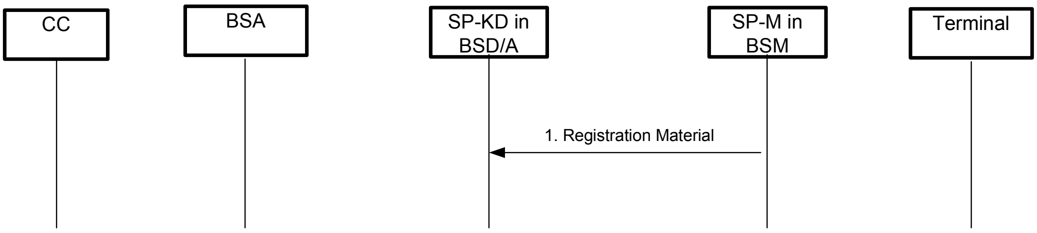


Figure 42 – Registration Key Material Delivery Flow

10. Registration material is delivered from the BSM to the BSD/A for broadcast delivery to Terminals.

5.4.4.3.2 LTKM Delivery

The following figure shows an example of the LTKM delivery flow from the BSM to the BSD/A. After that, the BSD/A can deliver the LTKM to the Terminal over broadcast channel.

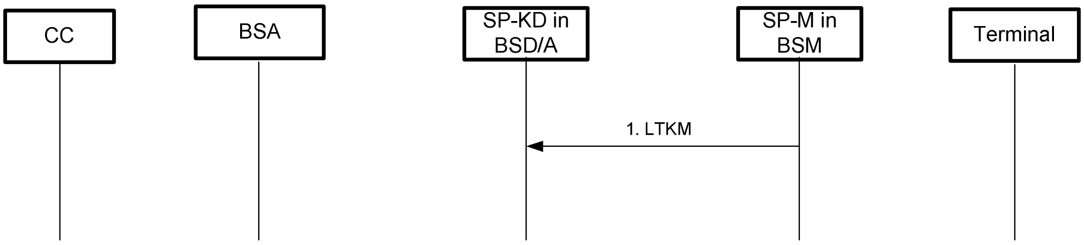


Figure 43 – LTKM Delivery Flow

1. The LTKM is delivered from the BSM to the BSD/A for broadcast delivery to Terminals.

5.4.4.3.3 STKM Generation

There are two ways for STKM generation. One way is STKM generation by BSD/A and the other way is STKM generation by BSM.

5.4.4.3.3.1 STKM Generation by BSM

The figure shows an example flow of the STKM generation procedure by the BSM.

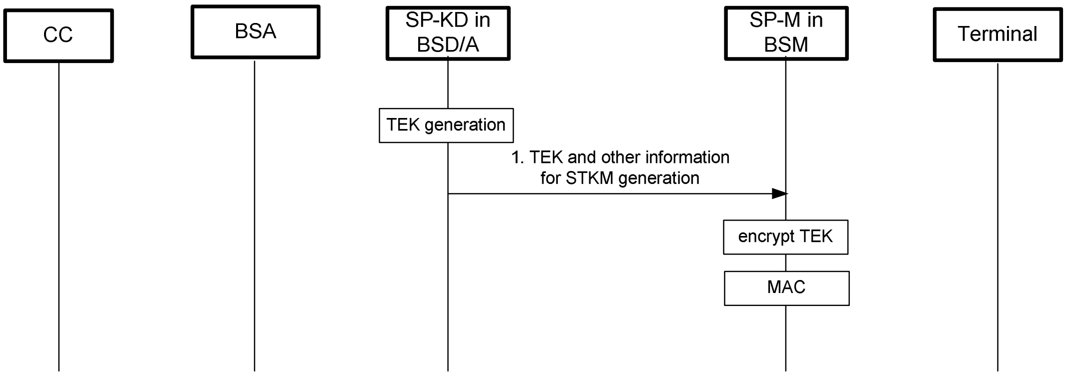


Figure 44 –Flow of STKM Generation by BSM

1. The BSD/A delivers the TEK and other information to the BSM for STKM generation. The BSM encrypts TEK using SEK or PEK and MACs a STKM using SAK or PAK (DRM Profile) or derived authentication key (Smartcard Profile).

The BSM can deliver the STKM to the BSD/A for delivery over broadcast channel or interaction channel to the Terminal.

5.4.4.3.3.2 STKM Generation by BSD/A

The figure shows an example flow of the STKM generation procedure by the BSD/A.

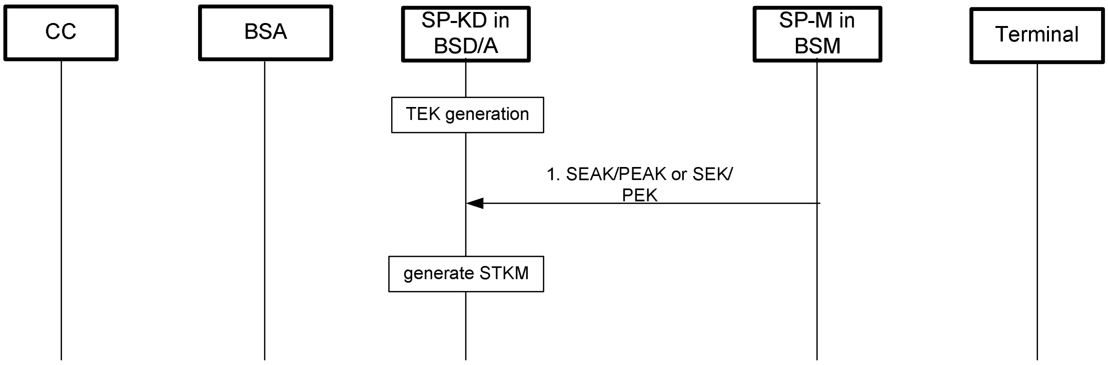


Figure 45 – Flow for STKM Generation by BSD/A

1. The BSM delivers SEAK/PEAK (DRM Profile) or SEK/PEK (Smartcard Profile) to the BSD/A for generation of a STKM. The BSD/A encrypts and MACs a STKM using SEAK/PEAK or SEK/PEK. The BSD/A delivers STKM over broadcasts broadcast channel or interaction channel the STKM to the Terminal.

5.4.4.3.4 STKM Delivery from BSM to BSD/A

The STKM generated by the BSM can be delivered to the BSD/A for delivery to Terminals using broadcast channel or interaction channel.

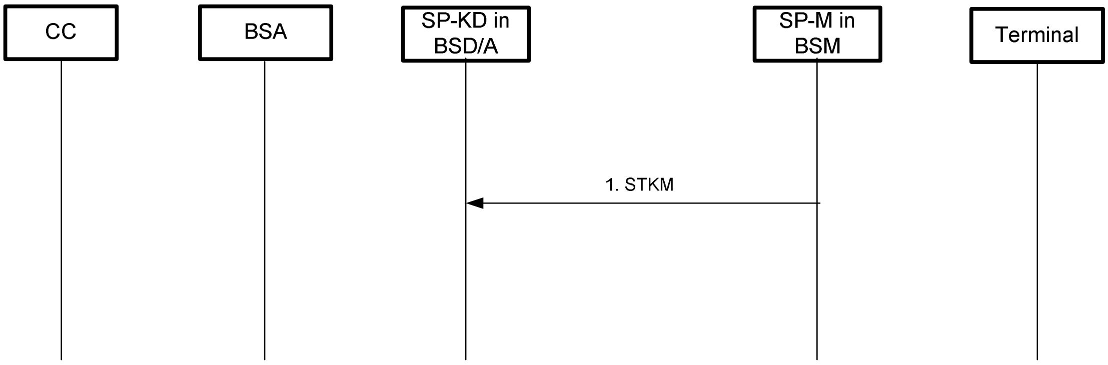


Figure 46 –Flow for STKM Delivery from BSM to BSD/A

1. The STKM generated by BSM is delivered from the SP-M in BSM to the SP-KD in BSD/A for delivery over broadcast channel or interaction channel to Terminal.

5.4.5 Content Protection Function Related Flows

In this section, descriptions on function flows for Content Protection are provided. Section 5.4.5.1 shows function flows for DRM Profile and Section 5.4.5.2 shows function flows for Smartcard Profile.

5.4.5.1 Content Protection Function Flows for DRM Profile

5.4.5.1.1 The Overall flow for Terminal with Interaction Channel Capability supporting DRM Profile

The following figure shows an example of the overall content protection flow for a Terminal with an interaction channel in the case the BSM generates the STKM.

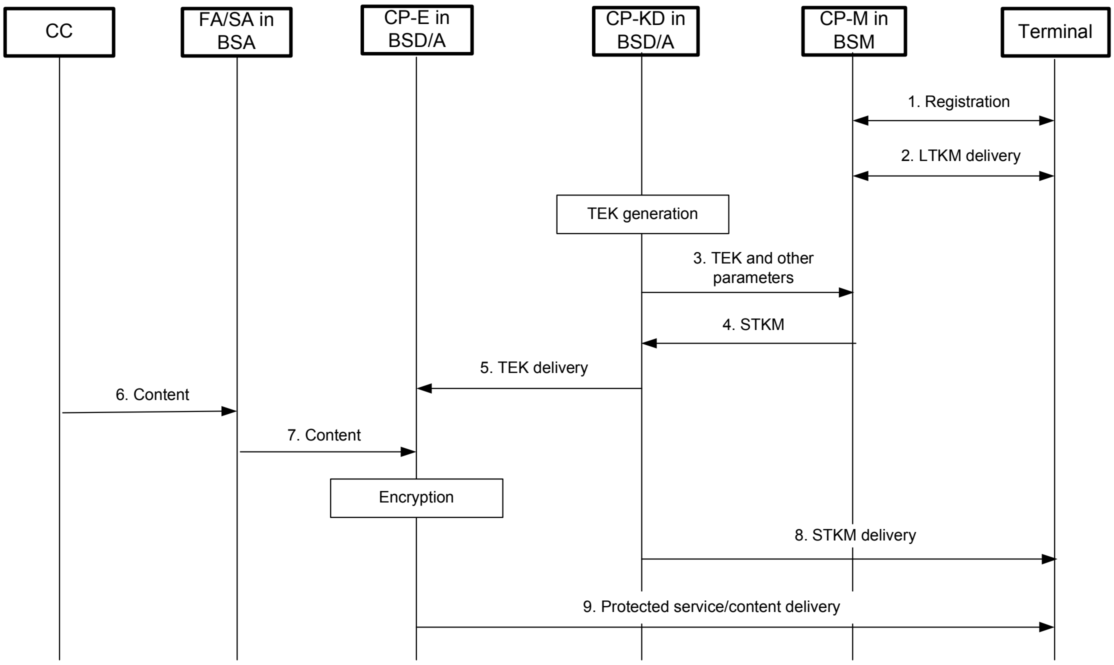


Figure 47 - Content Protection Flow for DRM Profile

1. The Terminal initiates the registration procedure following OMA DRM 4-pass Registration Protocol.
2. The CP-KD in BSD/A delivers a LTKM to the Terminal using 2-pass ROAP Rights Object Acquisition Protocol.

3. The BSD/A generates a TEK for encryption of content and delivers it with other parameters to the CP-M in BSM for STKM generation
4. The CP-M in BSM generates a STKM and delivers it to the BSD/A. STKM can also be generated by the BSD/A. In this case, the BSD/A acquires SEAK or PEAK from the BSM for encryption of STKM.
5. The CP-KD in BSD/A delivers TEK to the CP-E in BSD/A for encryption.
6. The CC delivers contents to the FA/SA in BSA.
7. The FA/SA in BSA delivers content to the CP-E in BSD/A.
8. The CP-KD in BSD/A broadcasts STKM to Terminals.
9. The CP-E in BSD/A sends encrypted content to the Terminal over the broadcast channel or the interaction channel.

5.4.5.1.1.1 Registration

This procedure is the same as 4-pass Registration Protocol from OMA DRM v2.0.

5.4.5.1.1.2 LTKM delivery

This procedure is the same as 2-pass Rights Object Acquisition Protocol from OMA DRM v2.0.

5.4.5.1.1.3 STKM delivery over Broadcast Channel or Interaction Channel

The figure shows an example for STKM delivery procedure over broadcast channel or interaction channel.

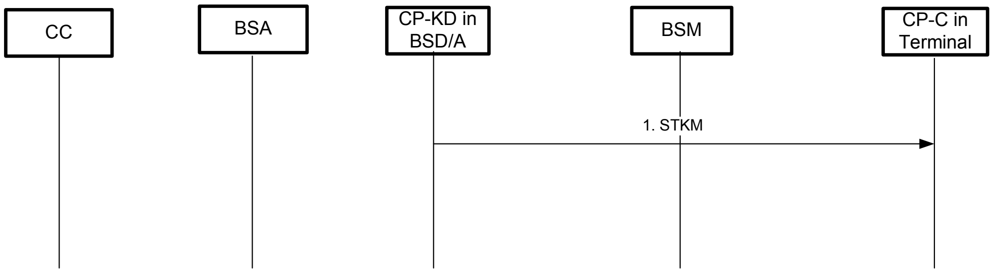


Figure 48 – STKM Delivery Flow for DRM Profile

1. The STKM is delivered from the CP-KD in BSD/A to the CP-C in Terminal over the broadcast channel or interaction channel.

5.4.5.1.1.4 Re-Keying

The Terminal can acquire an updated SEAK/PEAK by 2-pass Rights Object Acquisition Protocol with ROAP Trigger.

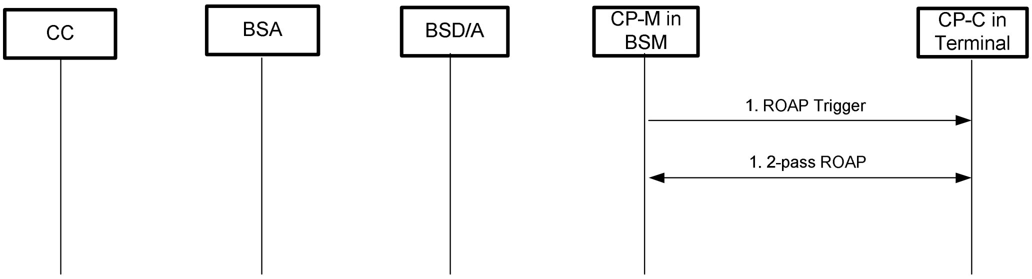


Figure 49– Re-Keying Flow for DRM Profile

1. The CP-M in BSM sends a ROAP Trigger to the CP-C in Terminal.
2. The CP-C in Terminal runs a 2-pass Rights Object Acquisition Protocol with the CP-M in BSM to acquire a new SEAK/PEAK.

5.4.5.1.2 The Overall Flow for Broadcast-only Terminal supporting DRM Profile

The figure shows an example of content protection function flow for broadcast-only terminal.

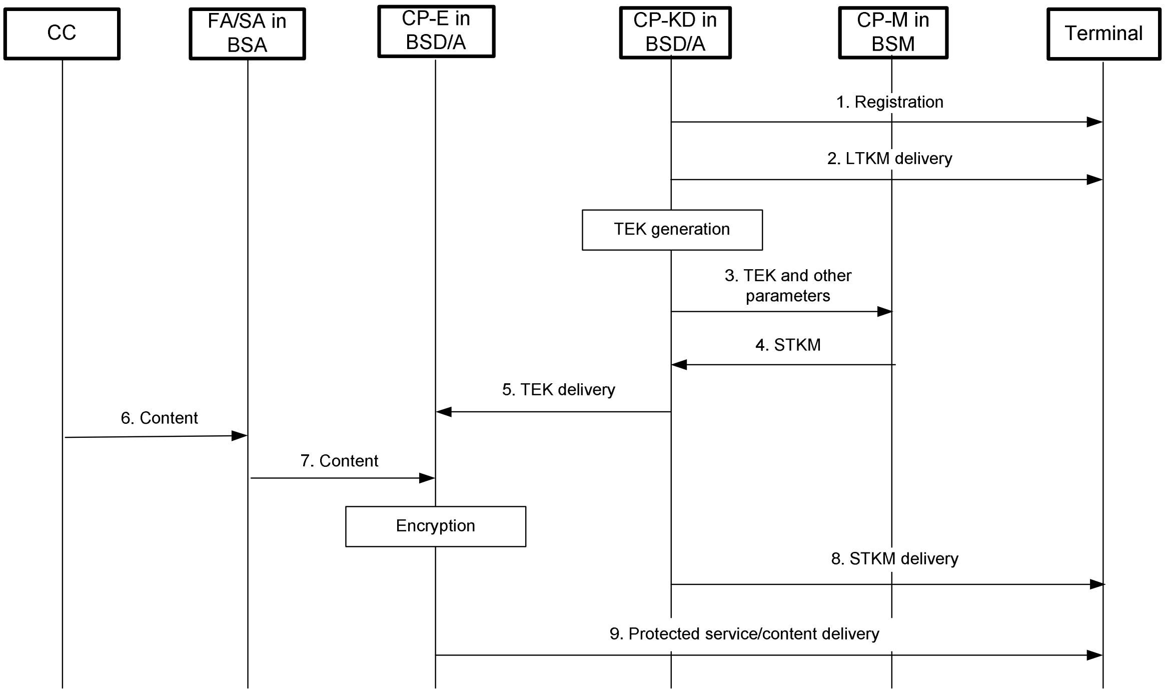


Figure 50 - Content Protection Flow for DRM Profile with Broadcast-only Terminal

1. The Terminal sends Registration request to the CP-M in BSM using out-of-band channel. The Terminal receives Registration message using broadcast channel.
2. The Terminal also receives LTKM over broadcast channel.
3. The BSD/A generates a TEK for encryption of content and delivers it with other parameters to the CP-M in BSM for STKM generation
4. The CP-M in BSM generates a STKM and delivers it to the BSD/A. STKM can also be generated by the BSD/A. In this case, the BSD/A acquires SEAK or PEAK from the BSM for encryption of STKM.
5. The CP-KD in BSD/A delivers TEK to the CP-E in BSD/A for encryption.
6. The CC delivers contents to the FA/SA in BSA.
7. The FA/SA in BSA delivers content to the CP-E in BSD/A.
8. The CP-KD in BSD/A broadcasts STKM to Terminals.
9. The CP-E in BSD/A broadcasts encrypted file or stream to the Terminal.

5.4.5.1.2.1 Registration

The figure shows an example of registration flow for DRM profile with broadcast-only terminals.

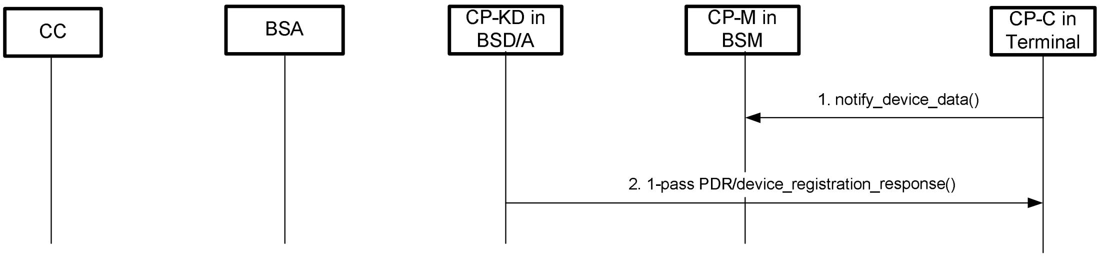


Figure 51 - Registration Flow

1. The CP-C in Terminal delivers device data to the BSM using out-of-band channel.
2. The CP-KD in BSD/A broadcasts device_registration_response message to the Terminal.

5.4.5.1.2.2 LTKM delivery

The figure shows an example of LTKM delivery flow for DRM Profile with Broadcast-only terminals.

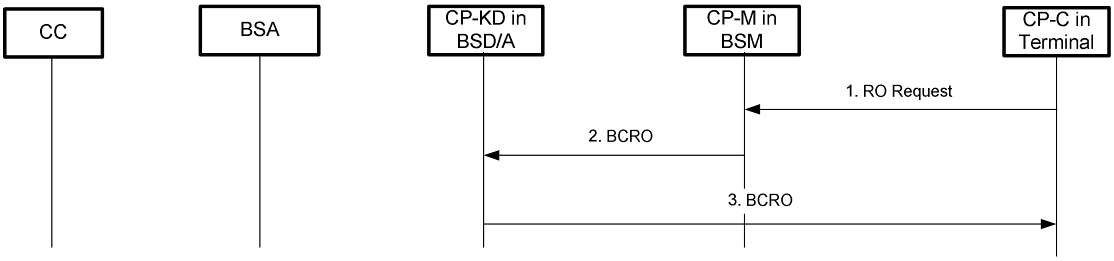


Figure 52 – LTKM Delivery Flow

1. The CP-C in Terminal makes a request to the BSM to deliver a LTKM(BCRO).
2. The BSM generates a LTKM(BCRO) and delivers it to the CP-KD in BSD/A.
3. The CP-KD in BSD/A sends a LTKM(BCRO) to the CP-C in Terminal.

5.4.5.1.2.3 STKM Delivery over Broadcast Channel

This procedure is identical to Sect.5.4.5.1.1.3.

5.4.5.1.2.4 Re-Keying

The figure shows an example of re-keying flow for DRM Profile with Broadcast-only terminals.

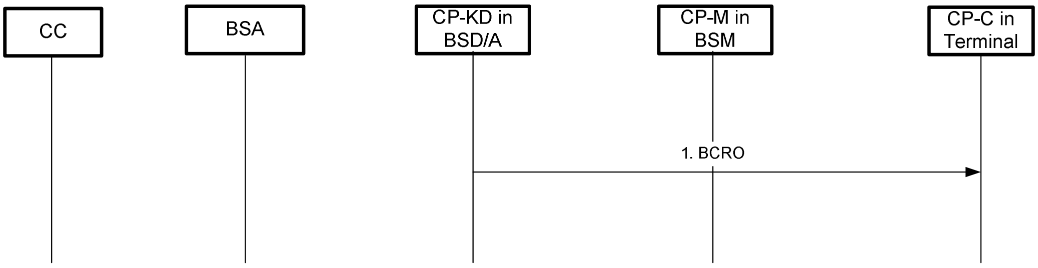


Figure 53 – Re-Keying Flow

1. The Terminal acquires BCRO from the CP-KD in BSD/A over the broadcast channel.

5.4.5.2 Content Protection Function Flows for Smartcard Profile

5.4.5.2.1 The Overall Flow for Interaction Terminal supporting Smartcard Profile

The following figure shows an overall content protection function flow for the Smartcard Profile in the case where the BSM generates the STKM.

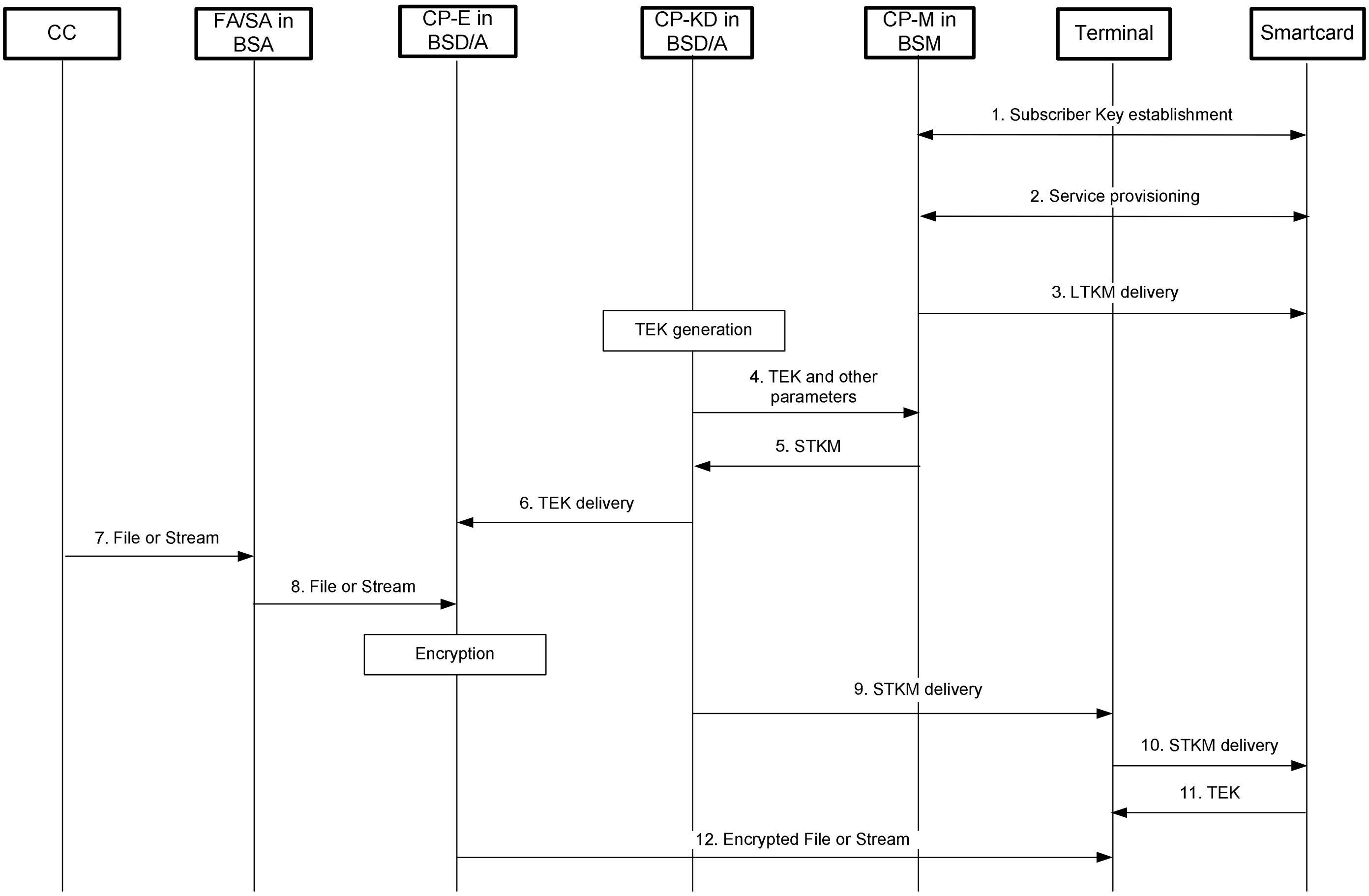


Figure 54 - Content Protection Function Flow for Smartcard Profile

1. The Smartcard executes SMK and SRK establishment procedure via either GBA or pre-provisioned RK with the CP-M in BSM.
2. Service Provisioning messages are exchanged in order to subscribe to services or purchase tokens.
3. The Smartcard receives LTKM from the CP-M in BSM.
4. The BSD/A generates a TEK for encryption of content and delivers it with other parameters to the CP-M in BSM for STKM generation.
5. The CP-M in BSM generates a STKM and delivers it to the BSD/A for distribution. STKM can also be generated by the BSD/A. In this case, the BSD/A acquires SEK or PEK from the BSM for encryption of STKM.
6. The CP-KD in BSD/A delivers TEK to the CP-E in BSD/A for encryption.
7. The CC delivers contents to the FA/SA in BSA.

8. The FA/SA in BSA delivers content to the CP-E in BSD/A.
9. The CP-KD in BSD/A broadcasts STKM to the Smartcard.
10. The Terminal sends STKM to the Smartcard.
11. The Smartcard extracts TEK from STKM and delivers it to the Terminal.
12. The CP-E in BSD/A sends encrypted file or stream to the Terminal over the broadcast channel or the interaction channel. The Terminal can decrypt encrypted file or stream using TEK received from the Smartcard.

The following figure shows an example of rights management with Smartcard Profile.

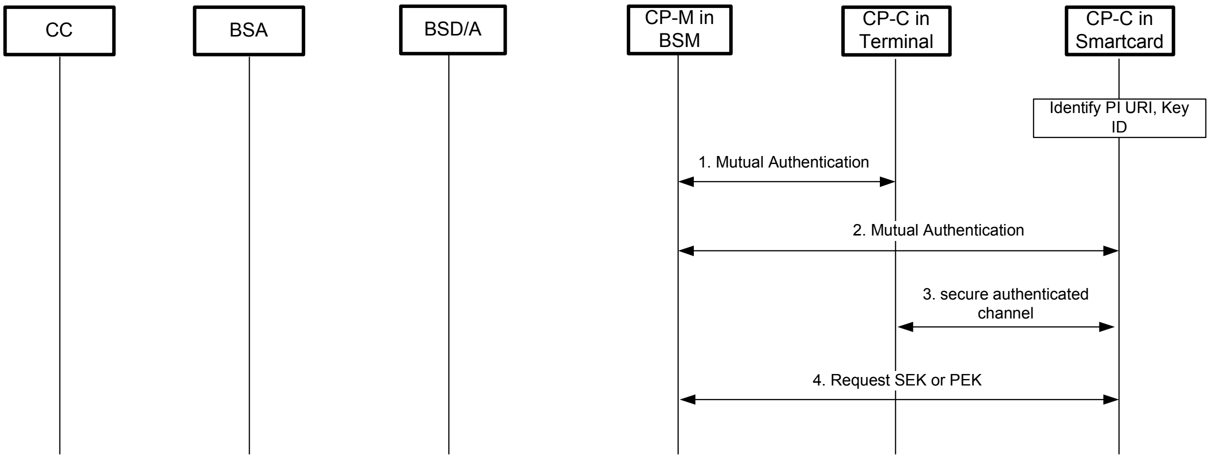


Figure 55 –Content Protection Flow for Rights Management with Smartcard Profile

1. Identify the Permissions Issuer URI and Key ID.
2. Initiate mutual terminal-server authentication.
3. Initiate mutual smartcard-server authentication.
4. Establish/enable the secure authenticated channel between the smartcard and terminal.
5. Request the appropriate SEK or PEK.

5.4.5.2.1.1 Subscriber Key Establishment

The figure shows an example of the subscriber key establishment flow for Smartcard Profile with Content Protection.

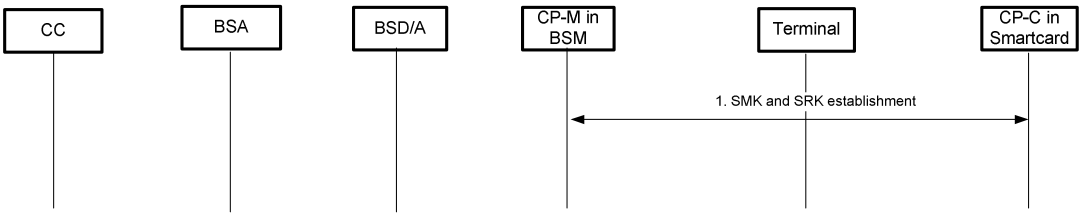


Figure 56 – Subscriber Key establishment Flow for Smartcard Profile

1. The CP-C in Smartcard acquires SMK and SRK via either GBA or pre-provisioned RK. SMK is used to protect a SEK or PEK.

For (U)SIM Smartcard Profile, the SMK and SRK are established via the GBA bootstrapping and bootstrap usage procedures as described in [3GPP TS 33.246] Section 6.1. For (R-)UIM/CSIM Smartcard Profile, the SMK and SRK are derived from the pre-provisioned Registration Key (RK) in the Smartcard, as described in [3GPP2 S.S0083-A].

5.4.5.2.1.2 Push LTKM delivery

The figure shows an example of LTKM delivery flow for Smartcard Profile with Content Protection.

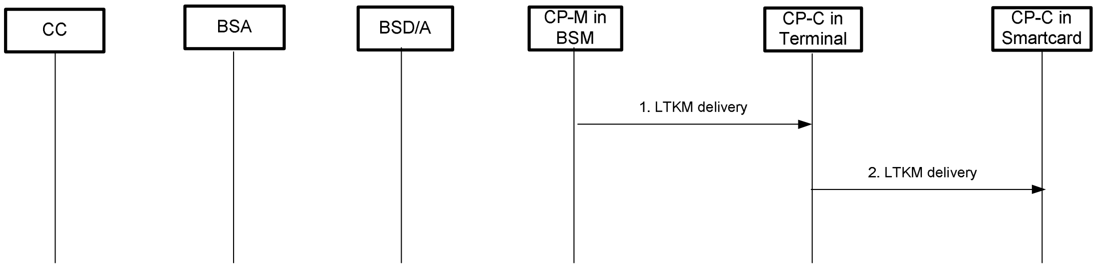


Figure 57 – Push LTKM Delivery Flow

1. The SP-M in BSM pushes LTKMs to the Terminal over UDP.
2. The Terminal with Smartcard acquires the LTKM from the BSM and delivers the LTKM to the Terminal.
3. The SP-C in Smartcard acquires the LTKM from the Terminal.

5.4.5.2.1.3 STKM Delivery over Broadcast Channel or Interaction Channel.

The following figure shows an example of STKM delivery over broadcast channel or interaction for the Smartcard Profile.

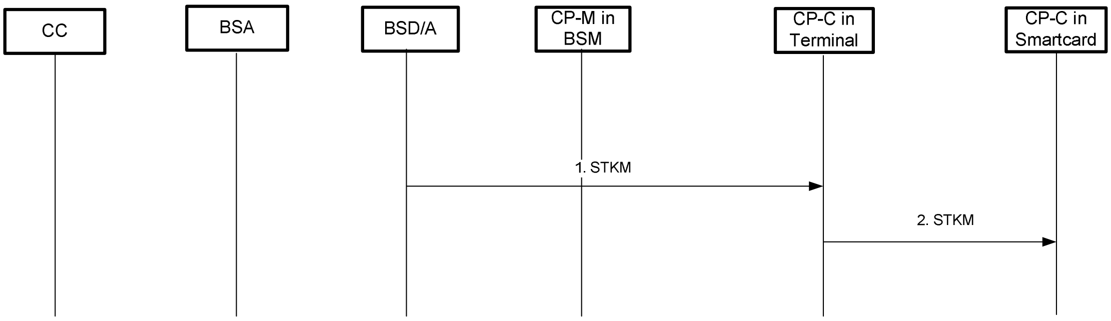


Figure 58 – STKM Delivery Flow over Broadcast Channel or Interaction Channel

1. The CP-C in Terminal receives the STKM over broadcast channel or interaction channel from the BSD/A.
2. The Terminal transmits STKMs to CP-C in the Smartcard.

5.4.5.2.1.4 LTKM Request Procedure

The figure shows an example of the LTKM request procedure for the Smartcard Profile with Content Protection.

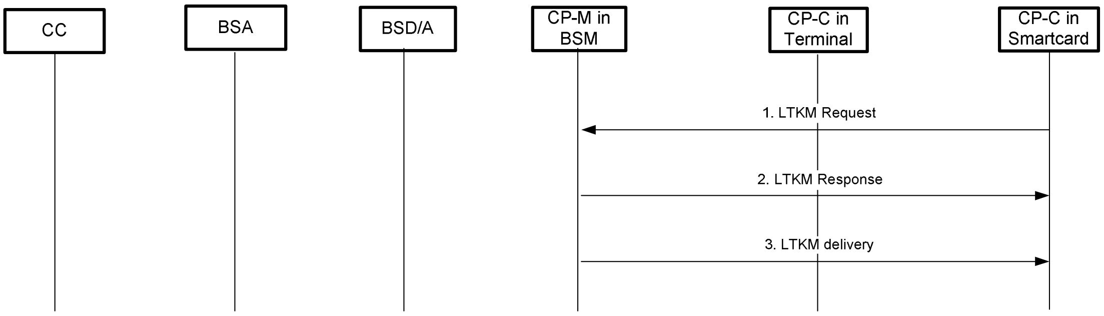


Figure 59 – LTKM Request Procedure Flow for Smartcard Profile

1. The CP-C in Smartcard the runs LTKM Request procedure to request a missed LTKM.
2. The BSM sends the LTKM Response to the Terminal.
3. The Terminal receives the LTKM from the BSM. The Terminal delivers the LTKM to the Smartcard.

5.4.5.3 Backend Interface Function Flows

This backend interface functions flows apply to both DRM Profile and Smartcard Profile.

5.4.5.3.1 Registration Key Material Delivery

The following figure shows an example of the registration key material delivery flow from the BSM to the BSD/A. After this, the BSD/A can deliver the registration key material to the Terminal over broadcast channel.

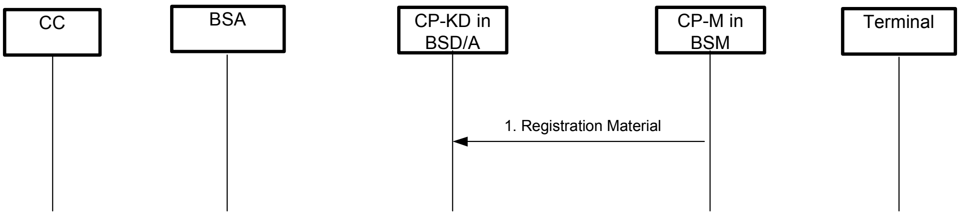


Figure 60 – Registration Key Material Delivery Flow

1. The Registration Material is delivered from the BSM to the BSD/A for broadcast delivery to Terminals.

5.4.5.3.2 LTKM Delivery

The following figure shows an example of the LTKM delivery flow from the BSM to the BSD/A. After this, the BSD/A can deliver the LTKM to the Terminal over broadcast channel.

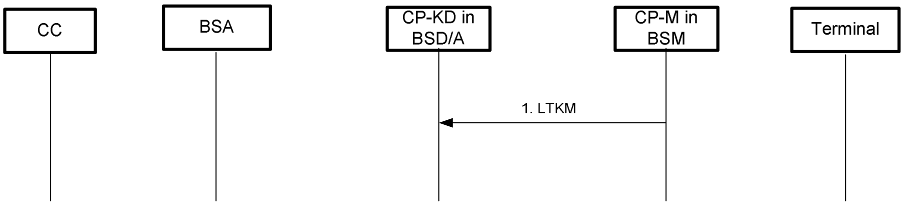


Figure 61 – LTKM Delivery Flow

1. The LTKM is delivered from the BSM to the BSD/A for broadcast delivery to Terminals.

5.4.5.3.3 STKM Generation

There are two ways for STKM generation. One is by BSM and the other is by BSD/A.

5.4.5.3.3.1 STKM Generation by BSM

The figure shows an example flow of the STKM generation procedure by the BSM.

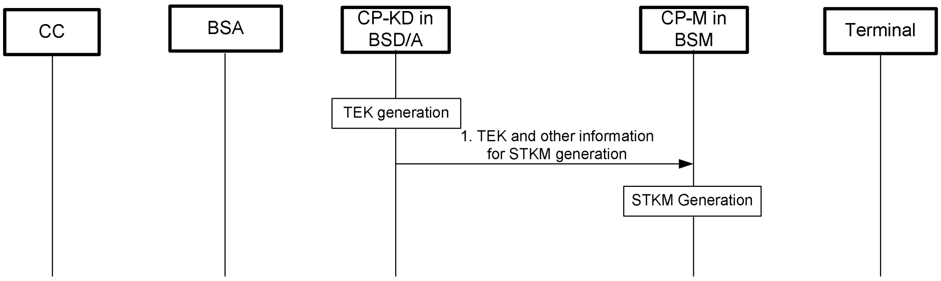


Figure 62 – Function Flow for STKM Generation by BSM

1. The CP-KD in BSD/A delivers the TEK and other information to the BSM for the generation of STKM.

5.4.5.3.3.2 STKM Generation by BSD/A

The figure shows an example flow of the STKM generation procedure by the BSD/A.

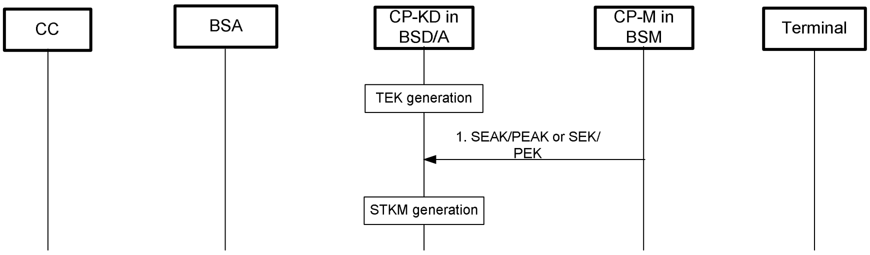


Figure 63 – Function Flow for STKM Generation by BSD/A

1. The BSM sends the SEAK/PEAK (DRM Profile) or SEK/PEK (Smartcard Profile) containing the SEAK/PEAK or SEK/PEK to the BSD/A for generation of STKM.

5.4.5.3.4 STKM Delivery from BSM to BSD/A

The STKM generated by the BSM can be delivered to the BSD/A for delivery to Terminals using broadcast channel or interaction channel.

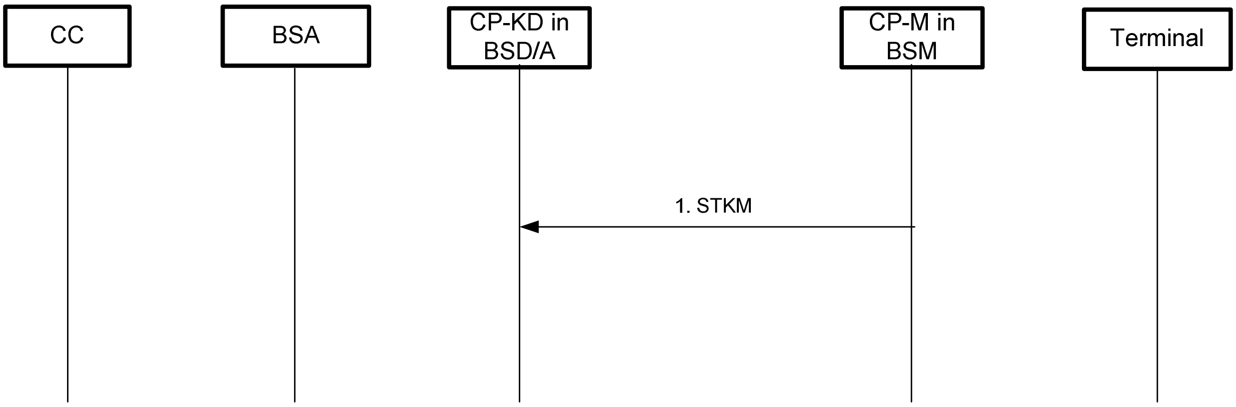


Figure 64 – Function Flow for STKM Delivery from BSM to BSD/A

1. The STKM generated by BSM is delivered from the CP-M in BSM to the CP-KD in BSD/A for delivery over broadcast channel or interaction channel to Terminal.

5.4.6 Interaction Channel Function Related Flows

5.4.6.1 General Interaction Flow

This chapter presents the flow message types for communicating over the Interaction Channel.

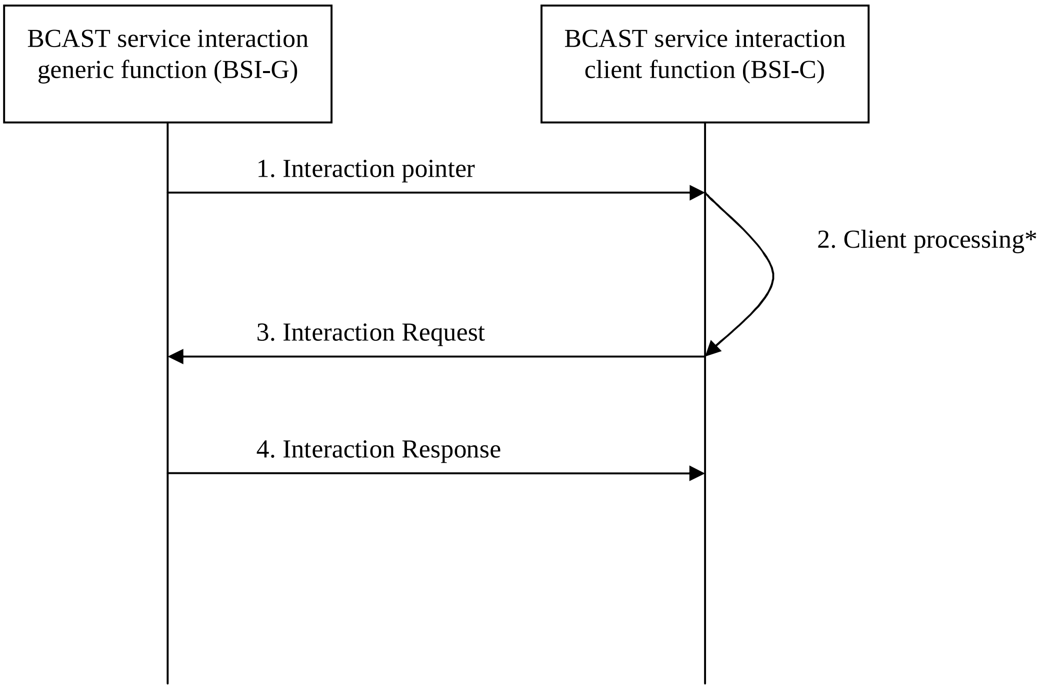

BCAST service interaction generic function (BSI-G)
BCAST service interaction client function (BSI-C)
1. Interaction pointer
2. Client processing*
3. Interaction Request
4. Interaction Response

Figure 65 – Message Types for Interaction Channel Flow

*Not in the scope of OMA BCAST.

1. BSI-G sends an interaction pointer to BSI-C over either Broadcast Channel or Interaction Channel, or out of band (in which case, this is optional step). This pointer contains one or several URIs to the service offered over Interaction Channel.
2. BSI-C processes the interaction pointer. The process is not in the scope of the specification in OMA BCAST. For example, the user makes decision whether the interaction is wanted or not.
3. BSI-C sends an Interaction Request to the Server. This request contains parameters for the service wanted, e.g. voting or browsing. It may or may not contain the URI acquired by the interaction pointer. For example, the User decides to initiate the interaction.
4. BSI-G sends an Interaction Response to BSI-C containing information on the service requested. If the BSI-C sends the Interaction Request (step 3) it may be followed by the Interaction Response.

5.4.6.2 Interactive Service example Flow – Case1

This case represents that the End User participates to the one-round services such as real-time betting, voting, usage monitoring, etc. After participating at the certain services, the response from BSI-G is not needed directly.

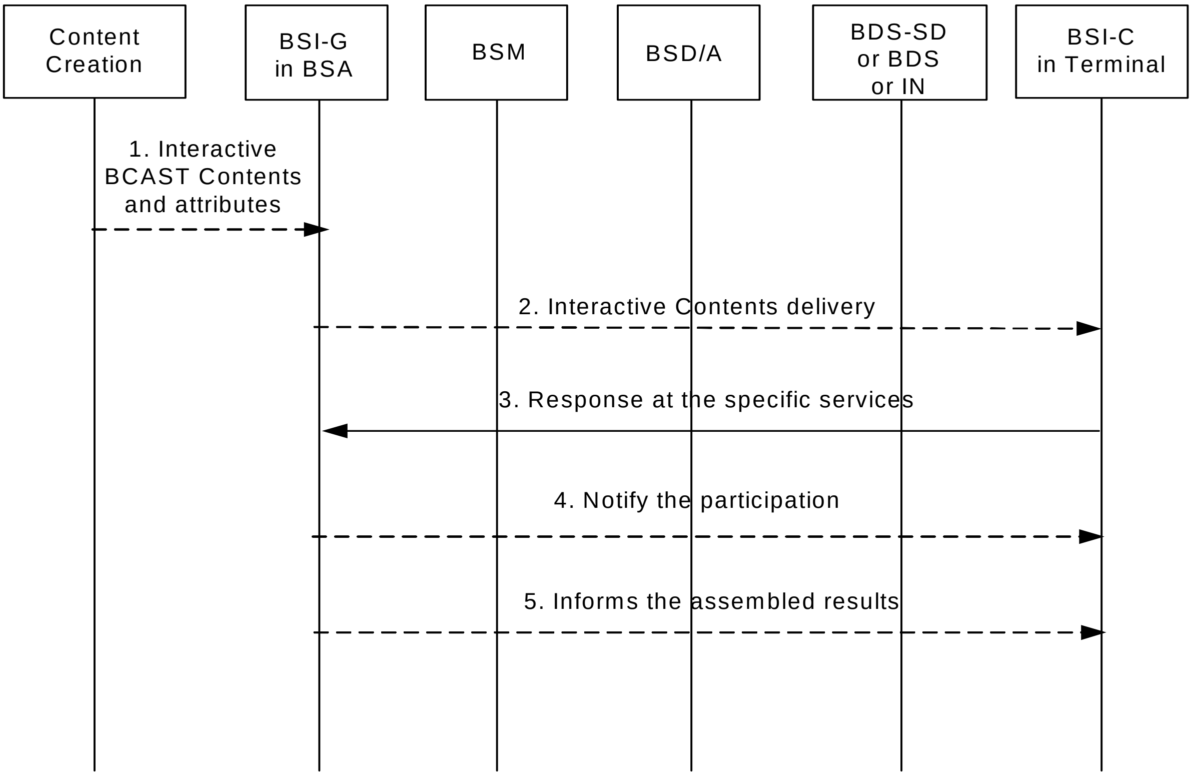

Content Creation
BSI-G in BSA
BSM
BSD/A
BDS-SD or BDS or IN
BSI-C in Terminal
1. Interactive BCAST Contents and attributes
2. Interactive Contents delivery
3. Response at the specific services
4. Notify the participation
5. Informs the assembled results

Figure 66 – Interaction Channel Flow: Client's participation of specific service

1. CC sends the interactive contents to the BSI-G in BSA, which requires the End User's participation at the certain part of services such as real-time voting, betting, usage monitoring, etc.
2. BSI-G receives the interactive contents from CC and broadcasts interactive content to the subscribed clients.

   The detail process of interactive contents delivery would be handled by Stream Distribution Function or File Distribution Function.
3. According to the contents, BSI-C in the Terminal responses to the specific services. The received contents have the interaction pointer that linked to the BSI-G in BSA. These would be individual end-to-end interaction pointer that were connected with each client or the public interaction pointer that requires the End User's information at each time. This interaction pointer would refer to interface SI-8.

   BSI-G receives the End User's participation information from the BSI-C and modifies this information to be fit for purpose. For example, in the statistical research, the received information would be assembled and calculated.
4. After participating at the specific interactive services, the BSI-G in BSA could send the BSI-C in terminal notification which the End User participated successfully.
5. The results would be broadcasted to the participated End Users show interests through interface SI-8.

5.4.6.3 Interactive Service example Flow – Case2

This case represents that the End User participates to the interactive services such as requests of additional or supplementary information. After requesting additional services at the related certain services, the End User gets the direct response from BSI-G or CC or third parties.

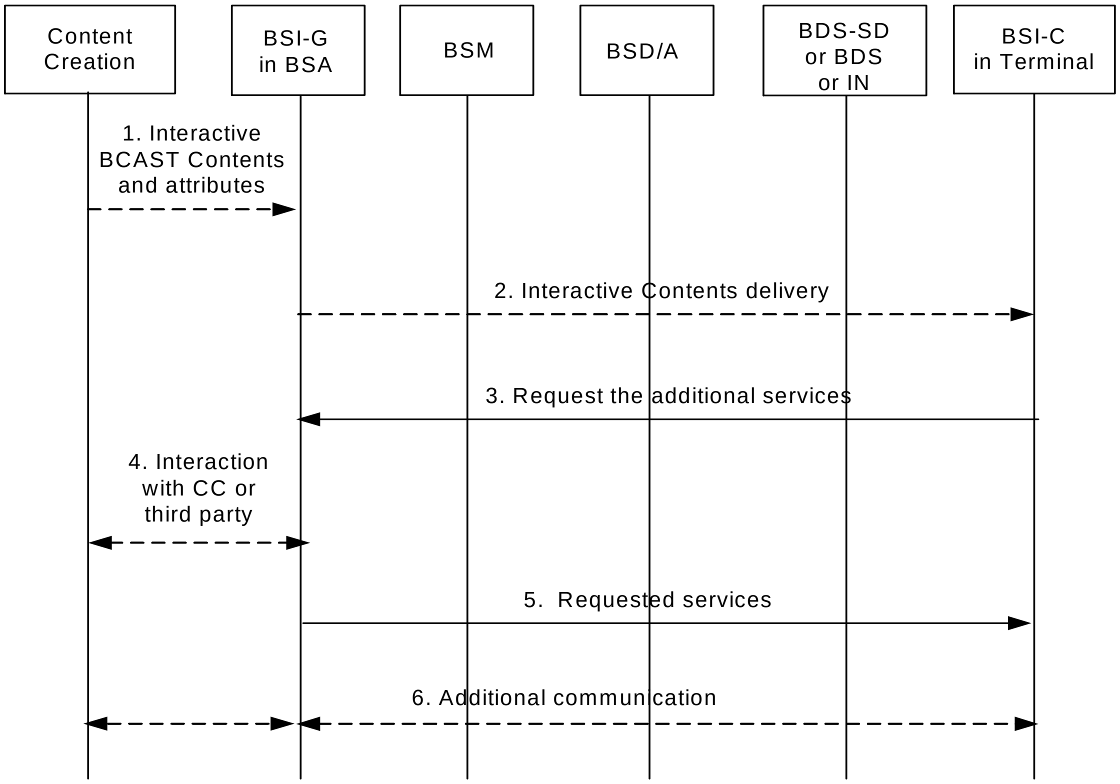

Content Creation
BSI-G in BSA
BSM
BSD/A
BDS-SD or BDS or IN
BSI-C in Terminal
1. Interactive BCAST Contents and attributes
2. Interactive Contents delivery
3. Request the additional services
4. Interaction with CC or third party
5. Requested services
6. Additional communication

Figure 67 – Interaction Channel Flow: Client's additional information requests

1. CC sends the contents that support the interactive services to the BSI-G in BSA.
2. BSI-G gets the interactive contents from CC and broadcasts interactive content to the subscribed clients. These contents have the interaction pointer which the End User can request additional information and supplementary services to the BSI-G in BSA or third party.

   The detail process of interactive contents delivery would be handled by Stream Distribution Function or File Distribution Function.
3. After receiving services that supports the interactive services, BSI-C requests the additional or supplementary information such as items' purchase information, selling shop, etc. This would be the individual end-to-end service that means interactive contents support individual access.
4. According to the services, the additional or supplementary information would be supported in the BSI-G or CC or third parties. If the CC provides whole additional information to the BSI-G at the beginning, then all requests of BSI-C would be handled all at the BSI-G. Except that, the additional requests of clients would be handled by CC or third parities that have additional information.
5. BSI-G or CC or third parties provides the requested additional information to the BSI-C.
6. Above simple interaction, BSI-C could want to, request more additional information additionally, etc. At this time, the BSI-C interacts with BSI-G or external charging entities.

5.4.7 Provisioning Function Related Flows

5.4.7.1 General Service Provisioning Messages

5.4.7.1.1 Pricing Information Request

The figure below describes the flow for requesting price information of a particular PurchaseItem.

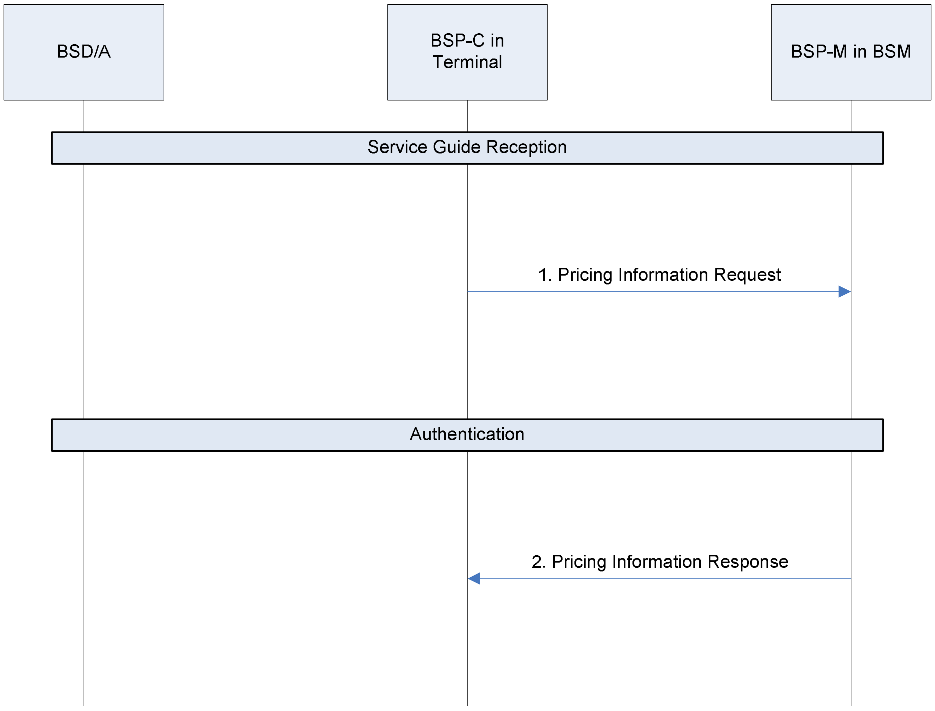


Figure 68 – Flow for requesting Price information of a particular PurchaseItem

1. After receiving the Service Guide the terminal may send a request for pricing information of PurchaseItem or a group of PurchaseItems shown in the Service Guide to the BSM. After receiving a pricing information request the BSM initiates the related operation. Before BSM starts generating the pricing information, BSM may initiate terminal (or user) authentication.
2. The BSM sends the pricing information of the requested PurchaseItems and may optionally send Service Guide fragments related to the requested PurchaseItem. If an error occurs during the generation of the pricing information, then BSM sends the response message containing a Global Status Code and an Item-wise Status Code to the terminal.

5.4.7.1.2 Service Request

The figure below describes the flow for service ordering.

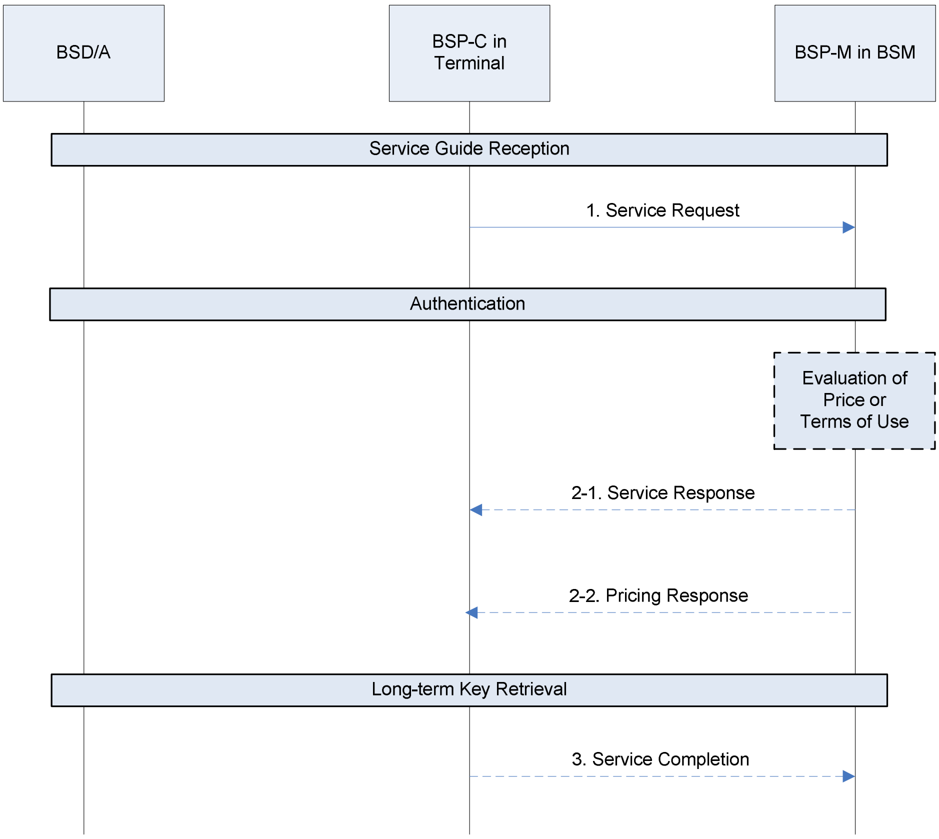


Figure 69 – Service Ordering Flow

1. After receiving the Service Guide the terminal sends a service ordering request to purchase services to the BSM. After receiving a service ordering request the BSM initiates the related operation. Before BSM starts the operation for service ordering, BSM may initiate terminal (or user) authentication and shall evaluate:

   – price information in the service request message to check whether it differs from the price calculated by BSM or if the request message doesn't contain the price information.

   – Terms of Use status (if supported) in the service request message to check whether the user has provided an answer for the Terms of Use notice, in the case such answer is required.

2-1 If the price information has no difference after evaluation and the user answered the Terms of Use notice (in case this was required), the Service Response message sent by BSM may contain some triggering message in order that the terminal can get the appropriate security material for service reception. For example, in BCAST DRM profile, the BSM sends the ROAP RO acquisition trigger to the terminal if the request was processed successfully; optionally, a registration trigger may be sent for unregistered terminals. If an error occurs on service ordering procedure, then BSM sends the response message containing a Global Status Code and an Item-wise Status Code to the terminal.

2-2. If the price information has difference after evaluation or if the request message does not contain the price information, or the user has not answered the Terms of Use as required, the BSM stops the operation for service ordering

– in the first two cases, sends a pricing response specified in Section 5.4.7.1.1 containing the price information. If User accepts the price, then Terminal sends a new "Service Request" with the price in the pricing response as agreed by the User.

– in the third case, sends a pricing response specified in Section 5.4.7.1.1 containing the Terms of Use or sends a service response containing the error code that the user must agree the Terms of Use. The terminal can then sends a new “Service Request” containing the user’s answer to the Terms of Use, possibly after having retrieved the Terms of Use via a pricing information request.

3. After Terminal receives “Service Response” and retrieves Long Term Key, Terminal may send a Service Completion message to the BSM after it confirms it is subscribed to the service that it requested, or it confirms that it received all security material required for the service reception.

5.4.7.1.3 Renewal Request

Subscription Renewal Request can be done in many ways. The figure below shows one example that can be done by Terminal supporting DRM profile.

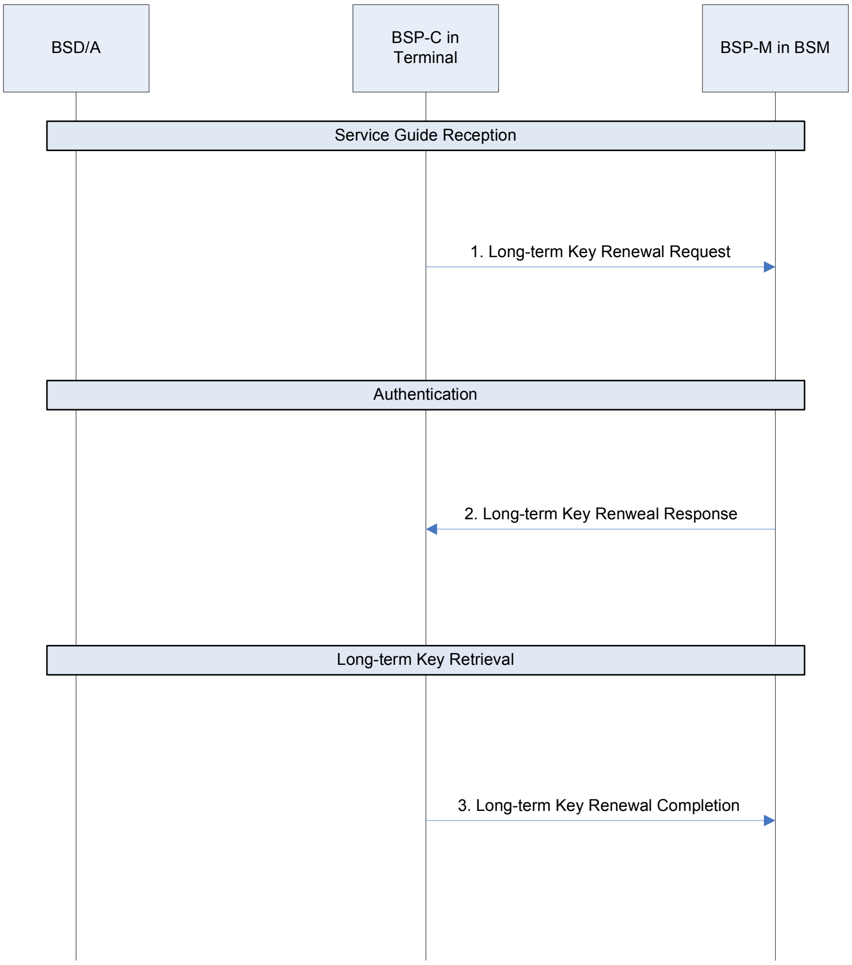

BSD/A
BSP-C in Terminal
BSP-M in BSM
Service Guide Reception
1. Long-term Key Renewal Request
Authentication
2. Long-term Key Renweal Response
Long-term Key Retrieval
3. Long-term Key Renewal Completion

Figure 70 – Flow for Subscription Renewal Request

1. If a user wants to renew a certain PurchaseItem or group of PurchaseItems, the terminal sends a list of PurchaseItems to be renewed to the BSM. Before BSM starts the operation for subscription renewal, BSM may re-authenticate the terminal or an User

2. The BSM sends the ROAP RO acquisition trigger to the terminal to renew the Long-term Key if the request was processed successfully. If an error occurs on subscription renewal procedure, then BSM sends the response message containing a Global Status Code and an Item-wise Status Code to the terminal. The BSM may send a registration trigger may be sent for unregistered terminals.

3, After acquiring the Long-term Key from the information given in the ROAP RO acquisition trigger, the terminal may send a Long-term Key Renewal Completion message to the BSM.

5.4.7.1.4 Unsubscription

The figure below describes the flow for an Unsubscribe request.

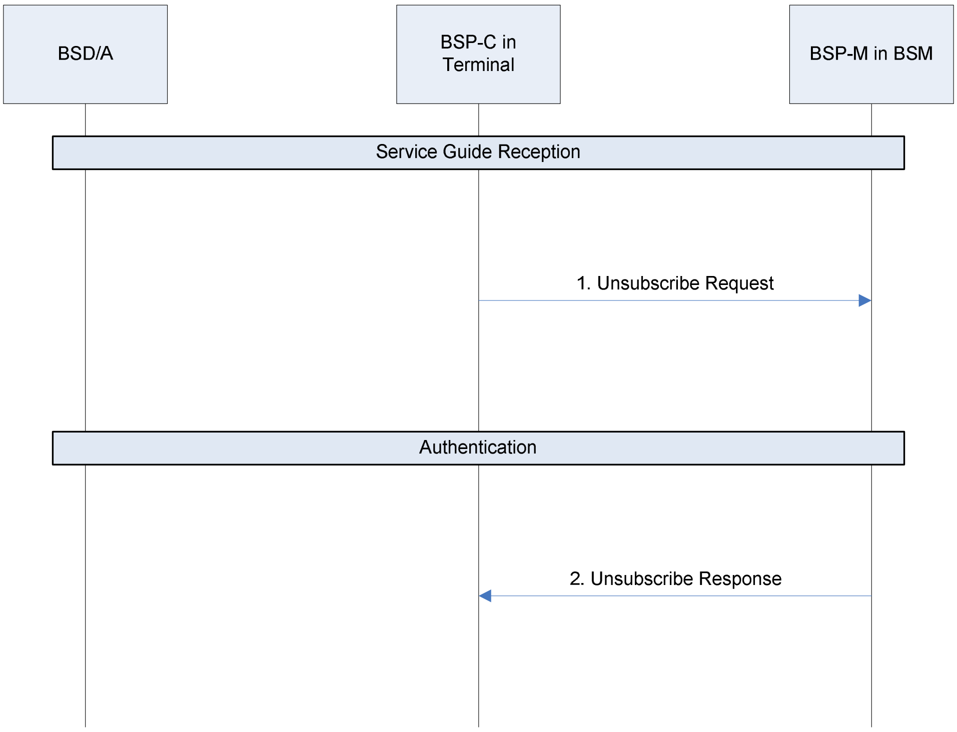


Figure 71 – Flow for Unsubscribe Request

1. The terminal sends a request unsubscribe a PurchaseItem or a group of PurchaseItems to the BSM.
2. After receiving a request the BSM initiates the related operation. Before BSM starts the operation for service unsubscription, BSM may initiate terminal (or user) authentication. The BSM sends the unsubscribe request result to the terminal. If an error occurs on service ordering procedure, then BSM sends the response message containing a Global Status Code and an Item-wise Status Code to the terminal.

5.4.7.1.5 Token Purchase

The figure below describes the flow for a Token Purchase request.

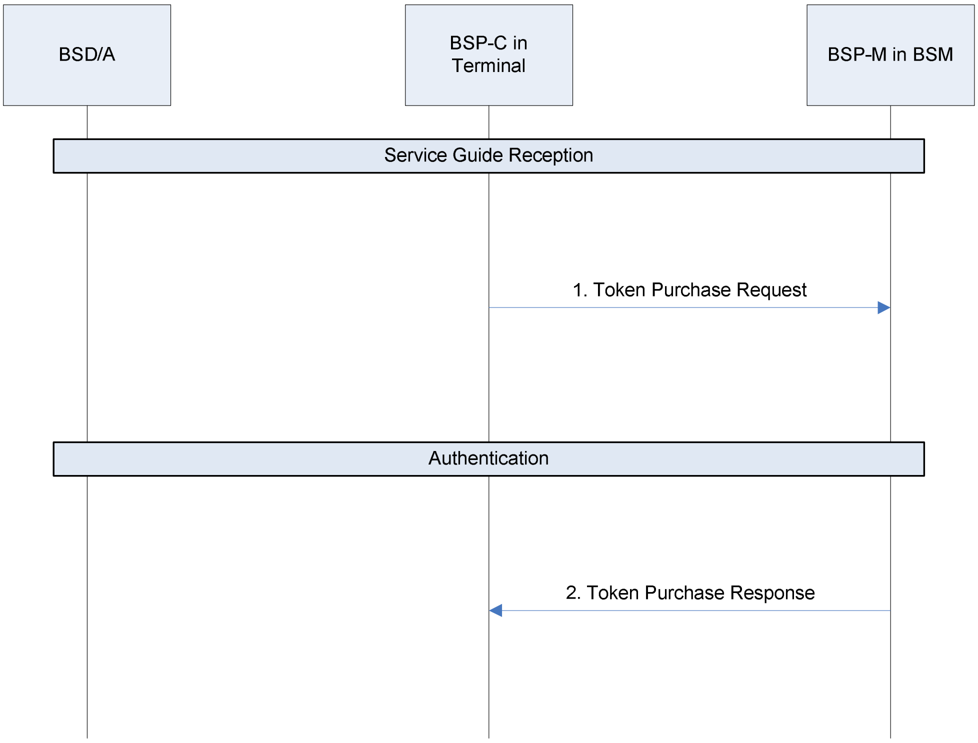


Figure 72 – Flow for Token Purchase Request

1. The terminal may send a request to purchase tokens to the BSM. Before BSM starts the operation for Token Purchase, BSM may authenticate the terminal or a User.
2. The BSM sends the Token purchase request result to the terminal. If an error occurs on service ordering procedure, then BSM sends the response message containing a Global Status Code and an Item-wise Status Code to the terminal.

5.4.7.1.6 Account Inquiry

The figure below describes the flow for an Account Inquiry request.

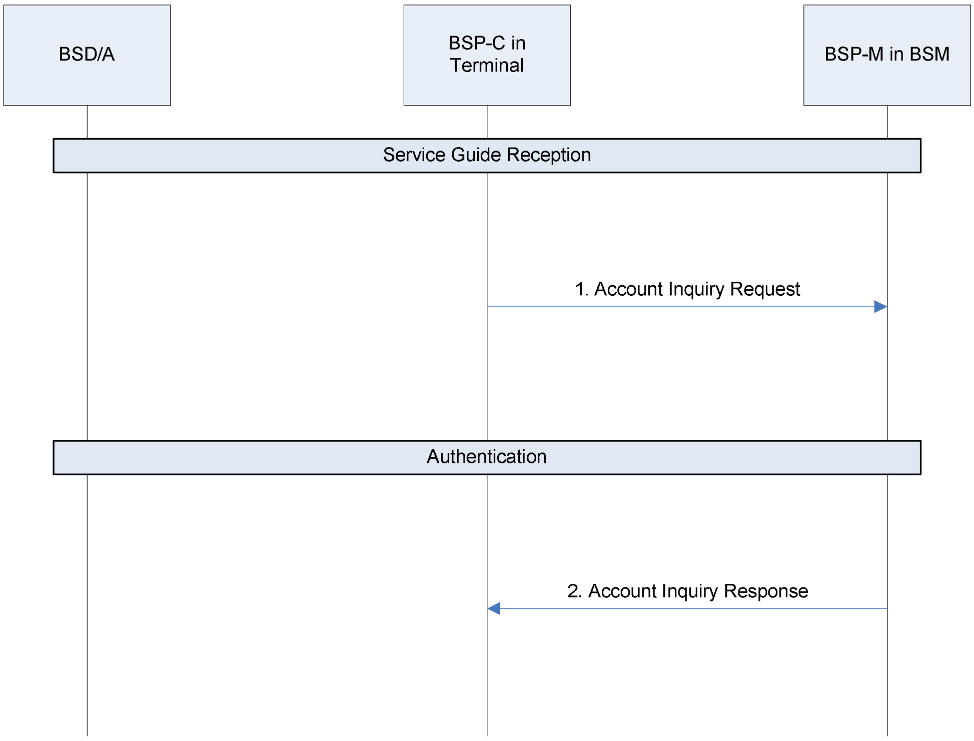


Figure 73 – Flow for Account Inquiry Request

1. The terminal may send a request to receive account information to the BSM. Information, such as, subscribed PurchaseItems or billing information may be requested. Before BSM starts the operation for an Account Inquiry request, BSM may initiate terminal (or user) authentication.
2. The BSM sends the account information to the terminal. If an error occurs on service ordering procedure, then BSM sends the response message containing a Global Status Code and an Item-wise Status Code to the terminal.

5.4.7.2 Service Provisioning Function Related Flows for Smartcard Profile

For the Smartcard Profile, all Service Provisioning messages and Registration procedures between the BSP-C and BSP-M SHALL be secured using HTTP digest. The key material used for the HTTP digest based access authentication and integrity protection, namely, the Smartcard Profile Subscriber Request Key (SRK), is either established through bootstrapping procedures (as described in Section 5.4.7.2.1 for the (U)SIM Smartcard Profile), or derived from a pre-provisioned shared secret between the BSP-C and BSP-M (as described in Section 5.4.7.2.2 for the (R-)UIM/CSIM Smartcard Profile). Note that the Smartcard Profile Subscriber Management Key (SMK), which is used to protect SEK/PEK delivery within LTKMs (with SEK/PEK subsequently protecting the TEK delivery within STKM) is established as part of the same procedure that establishes SRK.

5.4.7.2.1 Key Bootstrapping and Bootstrap Usage Procedures

For (U)SIM Smartcard Profile, the SMK and SRK are established via the GBA bootstrapping and bootstrap usage procedures as described in [3GPP TS 33.246] Section 6.1. These procedures establish two keys; the MBMS User Key (MUK) and MBMS Request Key (MRK), which correspond to the SMK and SRK, respectively. It should be noted that the way in which SMK and SRK are derived is dependent on whether GBA_U or GBA_ME is used (see [3GPP TS 33.246] for details). The BSP-M can control whether or not GBA_ME and/or GBA_U can be used for a particular service.

In addition to establishing the keys SMK and SRK, the GBA bootstrapping procedure also establishes a Bootstrapping Transaction Identifier (B-TID), which is used to bind the subscriber identity to the keying material at the BSP-M.

5.4.7.2.2 Key Derivation from Pre-Provisioned Secret Key

For (R-)UIM/CSIM Smartcard Profile, the SMK and SRK are derived from the pre-provisioned Registration Key (RK) in the Smartcard, as described in [3GPP2 S.S0083]. Two keys are derived from the RK: the Temporary Key (TK) and Authentication Key (Auth-Key), which correspond to the SMK and SRK, respectively.

5.4.7.2.3 Use of HTTP Digest to Secure Service Provisioning Messages

After SMK and SRK have been established between the BSP-C and the BSP-M, the BSP-C MAY send the BSP-M any of the following types of Service Provisioning messages:

- Service Request
- Subscription Renewal
- Unsubscribe Request
- Token Request
- LTKM Request

The Service Provisioning messages SHALL use HTTP Digest for access authentication and integrity protection. The use of HTTP digest SHALL be as defined in [BCAST10-ServContProt]..

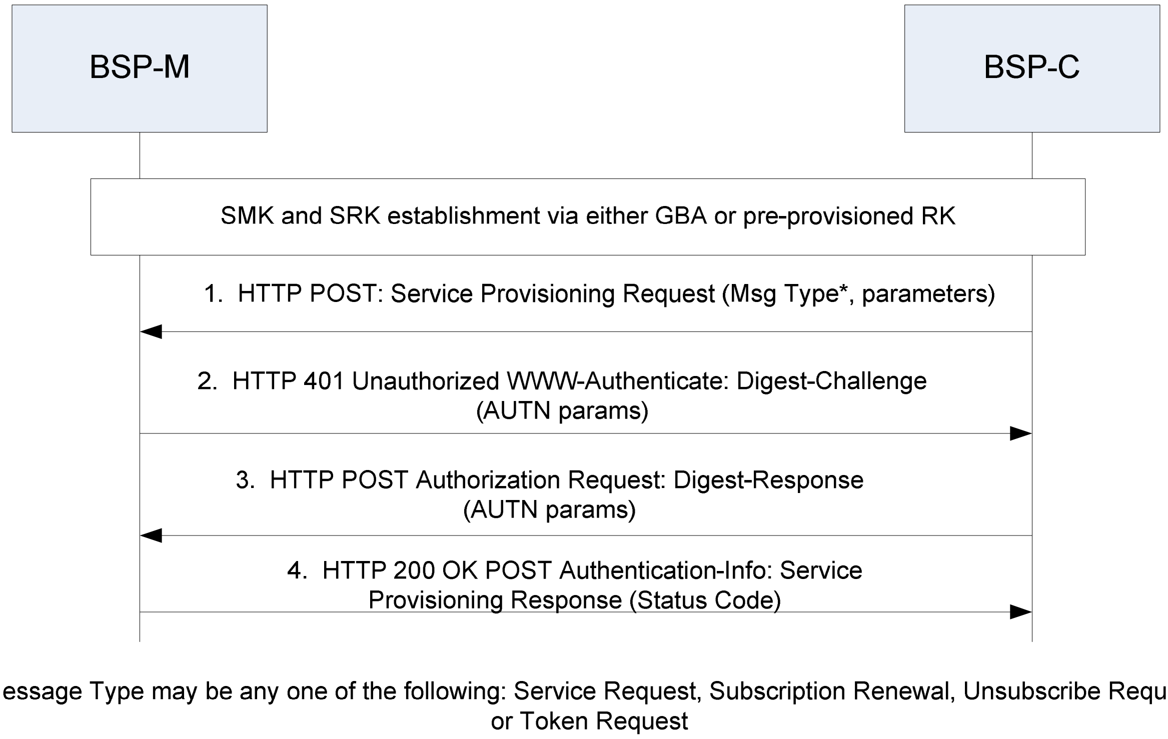

BSP-M
BSP-C
SMK and SRK establishment via either GBA or pre-provisioned RK
1. HTTP POST: Service Provisioning Request (Msg Type*, parameters)
2. HTTP 401 Unauthorized WWW-Authenticate: Digest-Challenge (AUTN params)
3. HTTP POST Authorization Request: Digest-Response (AUTN params)
4. HTTP 200 OK POST Authentication-Info: Service Provisioning Response (Status Code)
*Message Type may be any one of the following: Service Request, Subscription Renewal, Unsubscribe Request, or Token Request

Figure 74 – Generic Call Flow for Smartcard Profile's Service Provisioning Message Exchange using HTTP Digest

It is assumed that SMK and SRK have been established, as described in Section 5.4.7.2 prior to the start of the service provisioning message exchange described below.

1. The BSP-C sends the service provisioning request message using the HTTP POST message to the BSP-M. . As described in [BCAST10-ServContProt], if the BSP-C has the required authentication credentials it includes the Authorization header line in the HTTP POST request.

2. An acceptable Authorization header is not included in the request message received by the BSP-M, the BSP-M responds with a “401 Unauthorized” status code, along with a WWW-Authenticate header containing the digest challenge. If an Authorization header was included in the request message but the BSP-M determined the nonce value used to be stale, the BSP-M sets the stale directive of the digest challenge to “true”.
3. If the BSP-C receives a digest challenge from the BSP-M, the BSP-C retries the request including in the HTTP POST the Authorization header line which contains the digest response using the SRK as the password, and B-TID or NAI (Network Access Identifier) as the username, for the (U)SIM Smartcard Profile or (R-)UIM/CSIM Smartcard Profile, respectively.
4. The BSP-M authenticates the BSP-C by computing the digest response. If authentication is successful, the BSP-M sends the 200 OK along with the appropriate status code for the message type.

NOTE: In figure 75 the dashed box contains the additional messages between the BSP-M and BSP-C that are required when the initial HTTP post message from the BSP-C does not include an acceptable.

5.4.7.2.4 Service Request/

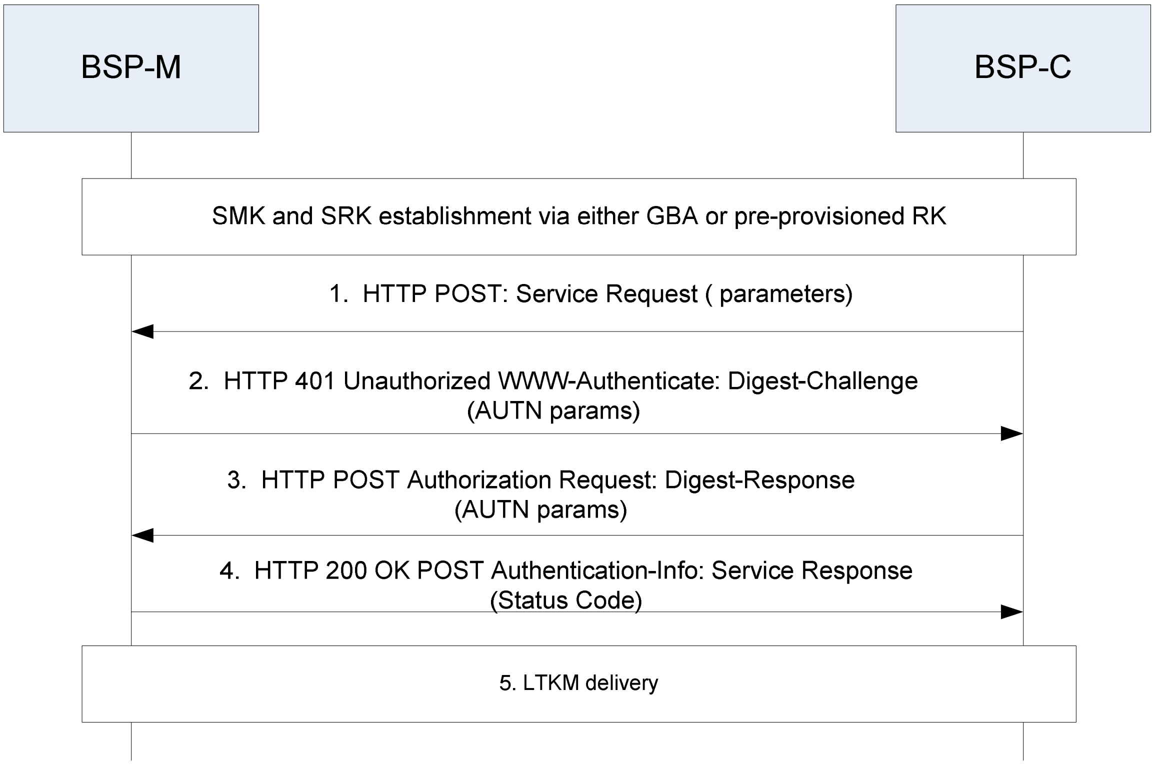

BSP-M
BSP-C
SMK and SRK establishment via either GBA or pre-provisioned RK
1. HTTP POST: Service Request (parameters)
2. HTTP 401 Unauthorized WWW-Authenticate: Digest-Challenge (AUTN params)
3. HTTP POST Authorization Request: Digest-Response (AUTN params)
4. HTTP 200 OK POST Authentication-Info: Service Response (Status Code)
5. LTKM delivery

Figure 75 – Call Flow for Smartcard Profile’s Service Request/Response Message Exchange

It is assumed that SMK and SRK have been established as described in Section 5.4.7.2.1 prior to the start of the service provisioning message exchange described below.

1. The BSP-C sends the Service Request message to the BSP-M. The Service Request message is an HTTP message. The format of the Service Request message is specified in [BCAST10-Services].
2. As the request is for an access-protected object, and the appropriate Authorization header is not included in the request message received by the BSP-M, the BSP-M responds with a “401 Unauthorized” status code, along with WWW-Authenticate header containing the digest challenge.

3. The BSP-C retries the request, this time including in the HTTP POST the Authorization header line which contains the digest response using the SRK as the password, and B-TID or NAI (Network Access Identifier) as the username, for the (U)SIM Smartcard Profile or (R-)UIM/CSIM Smartcard Profile, respectively.
4. The BSP-M authenticates the BSP-C by computing the digest response. If authentication is successful, the BSP-M sends the 200 OK along with the appropriate status code for the message type. This message is the Service Response message defined in [BCAST10-Services]. If the Service Request is unsuccessful, the status code in the HTTP status line shall indicate the appropriate error.
5. The LTKM is delivered to the BSP-C from the BSP-M. The BSP-M SHOULD push LTKMs to the terminal over UDP following a successful Service Request/Response procedure. However, if the BSP-C does not receive the LTKM related to the successful Service Request/Response procedure, the BSP-C SHOULD request the relevant LTKM from the BSP-M by sending it an HTTP message containing a list of one or more SEK/PEK ID(s), as explained in section 5.4.4.2.1.4" LTKM Request Procedure".

Note that the BSM SHALL register the terminal to the corresponding service if the Service Request was successful, i.e. the Service Provisioning procedure includes an implicit registration with the BSP-M.

5.4.7.2.5 Token Purchase Request/

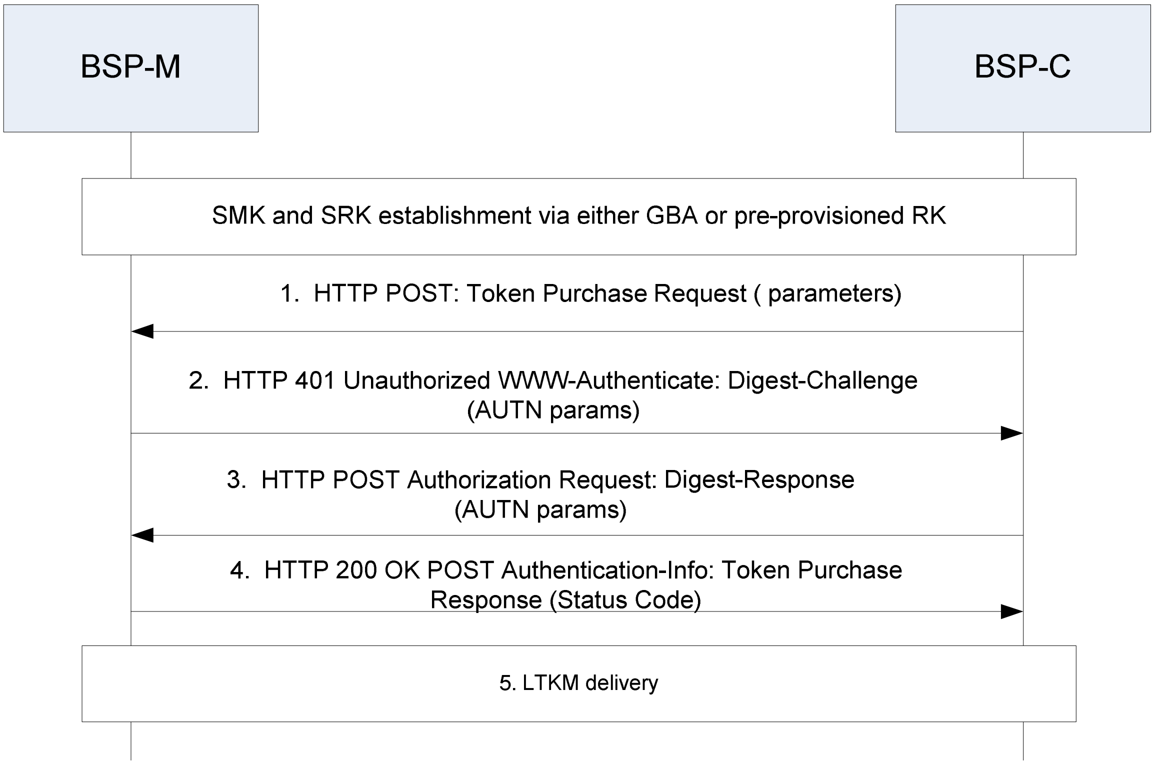

BSP-M
BSP-C
SMK and SRK establishment via either GBA or pre-provisioned RK
1. HTTP POST: Token Purchase Request (parameters)
2. HTTP 401 Unauthorized WWW-Authenticate: Digest-Challenge (AUTN params)
3. HTTP POST Authorization Request: Digest-Response (AUTN params)
4. HTTP 200 OK POST Authentication-Info: Token Purchase Response (Status Code)
5. LTKM delivery

Figure 76 – Call Flow for Smartcard Profile's Token Purchase Request/Response Message Exchange

It is assumed that SMK and SRK have been established as described in Section 5.4.7.2.1 prior to the start of the service provisioning message exchange described below.

1. The BSP-C sends Token Purchase Request message to the BSP-M. The Token Purchase Request message is an HTTP message. The format of the Token Purchase Request message is specified in [BCAST10-Services].

2. As the request is for an access-protected object, and the appropriate Authorization header is not included in the request message received by the BSP-M, the BSP-M responds with a "401 Unauthorized" status code, along with WWW-Authenticate header containing the digest challenge.
3. The BSP-C retries the request, this time including in the HTTP POST the Authorization header line which contains the digest response using the SRK as the password, and B-TID or NAI (Network Access Identifier) as the username, for the (U)SIM Smartcard Profile or (R-)UIM/CSIM Smartcard Profile, respectively.
4. The BSP-M authenticates the BSP-C by computing the digest response. If authentication is successful, the BSP-M sends the 200 OK along with the appropriate status code for the message type. This message is the Token Purchase Response message defined in [BCAST10-Services].
5. The LTKM is delivered to the BSP-C from the BSP-M. The BSP-M SHOULD push LTKMs to the terminal over UDP following a successful Token Purchase Request/Response procedure. However, if the BSP-C does not receive the LTKM related to the successful Token Purchase Request/Response procedure, the BSP-C SHOULD request the relevant LTKM from the BSP-M by sending it an HTTP message containing a list of one or more SEK/PEK ID(s), as explained in [BCAST10-Services] Section 5.1.6.8 "LTKM Request Procedure". Note that some tokens are not associated with a SEK/PEK ID, in which case the LTKM request procedure can NOT be used. In order to avoid this situation, if LTKMs with tokens not associated with a SEK/PEK ID are delivered, an acknowledgment from the terminal SHOULD be requested.

Note that the BSM SHALL register the terminal to the corresponding service if the Token Purchase Request was successful, i.e. the Service Provisioning procedure includes an implicit registration.

5.4.7.2.6 Registration Request/Response Message Flow

The Registration message is sent by the BSP-C to the BSP-M to indicate to the BSP-M that the BSP-C is available to receive from the BSP-M any LTKM updates related to the services to which the BSP-C is subscribed. The Registration message is sent when the terminal re-establishes connectivity with the interactive communication channel, e.g., after being switched on or coming back into coverage, or as defined in the flows within this section.

The Registration message is not a BCAST service provisioning message i.e., it is not related to subscription or a token purchase. The message format and message exchanged is defined in [3GPP TS 33.246] Section 6.3.2.1(a) "MBMS User Service Registration procedure".

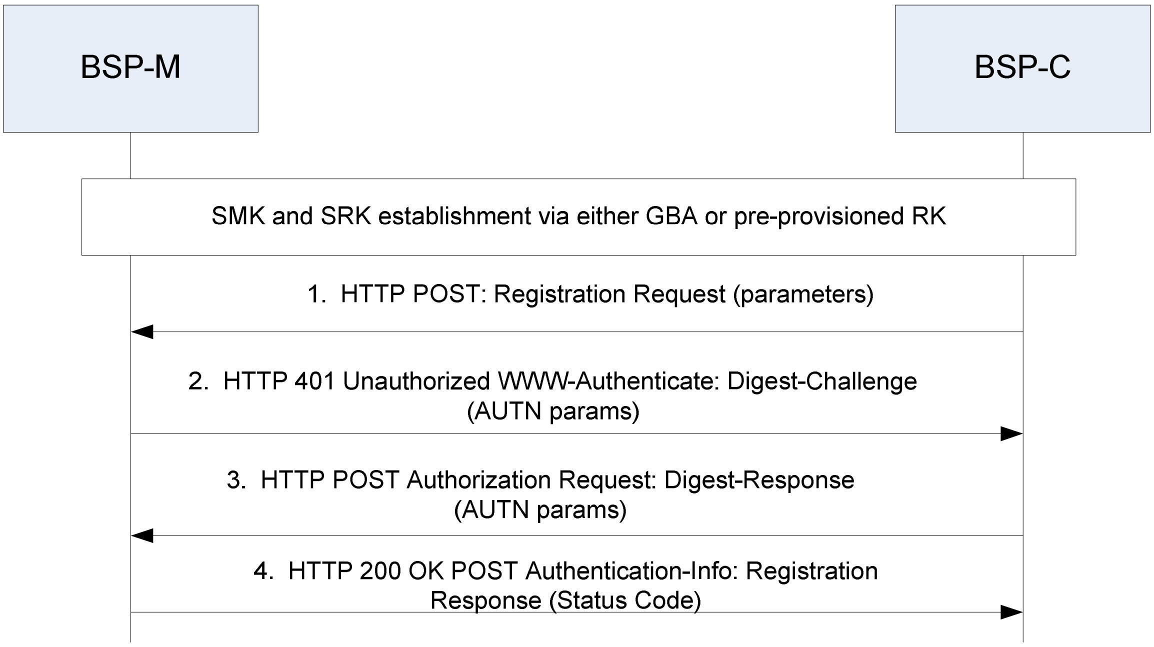

BSP-M
BSP-C
SMK and SRK establishment via either GBA or pre-provisioned RK
1. HTTP POST: Registration Request (parameters)
2. HTTP 401 Unauthorized WWW-Authenticate: Digest-Challenge (AUTN params)
3. HTTP POST Authorization Request: Digest-Response (AUTN params)
4. HTTP 200 OK POST Authentication-Info: Registration Response (Status Code)

Figure 77 – Call Flow for Smartcard Profile's Registration Request/Response Message Exchange

It is assumed that SMK and SRK have been established as described in Section 5.4.7.2.1 prior to the start of the service provisioning message exchange described below.

1. The BSP-C sends the Registration message to the BSP-M. The Registration message is an HTTP message. The format of the Registration message is specified in [3GPP TS 33.246].
2. As the request is for an access-protected object, and the appropriate Authorization header is not included in the request message received by the BSP-M, the BSP-M responds with a “401 Unauthorized” status code, along with WWW-Authenticate header containing the digest challenge.
3. The BSP-C retries the request, this time including in the HTTP POST the Authorization header line, which contains the digest response using the SRK as the password, and B-TID or NAI (Network Access Identifier) as the username, for the (U)SIM Smartcard Profile or (R-)UIM/CSIM Smartcard Profile, respectively.
4. The BSP-M authenticates the BSP-C by computing the digest response. If authentication is successful the BSP-M sends the 200 OK along with the appropriate status code for the message type.

Once the above steps have been completed, the terminal is "registered" at the BSP-M.

5.4.7.2.7 De-registration Request/Response Message Flow

The De-registration message is sent by the BSP-C to the BSP-M to indicate that the BSP-C is no longer available to receive from the BSP-M any LTKM updates related to the services to which the it is subscribed. The De-registration message is sent when the terminal looses connectivity with the interactive communication channel.

The De-registration message is not a BCAST service provisioning message, i.e., it is not related to subscription or a token purchase. The message format and message exchanged is defined in [3GPP TS 33.246] Section 6.3.2.1 (b) "MBMS User Service De-registration procedure".

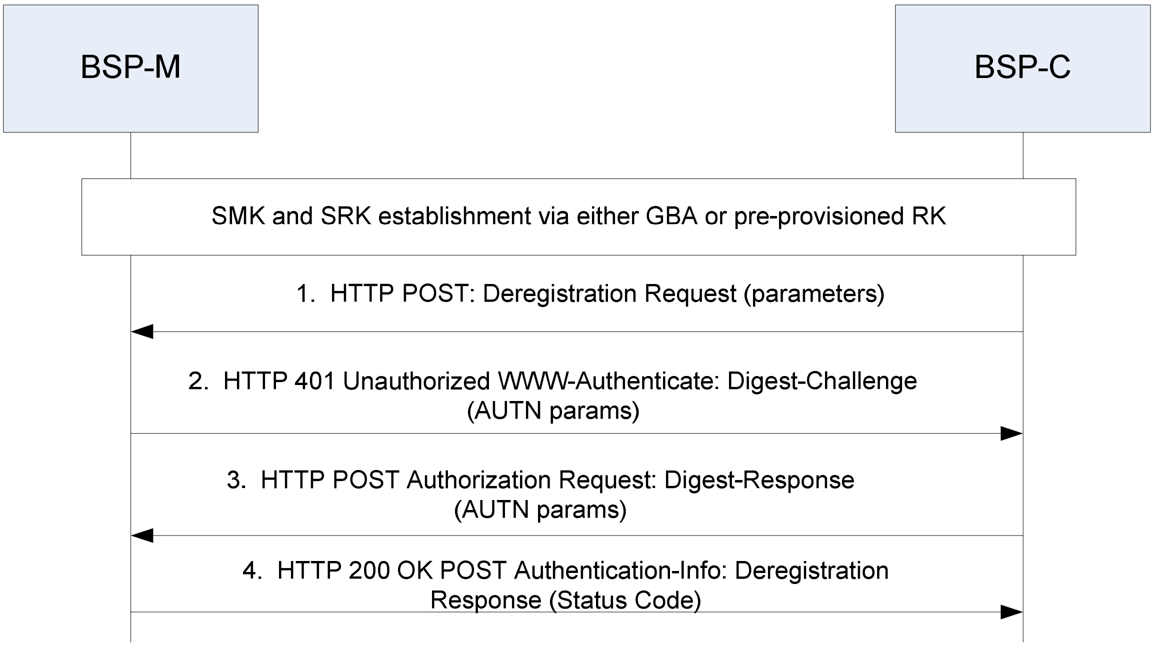

BSP-M
BSP-C
SMK and SRK establishment via either GBA or pre-provisioned RK
1. HTTP POST: Deregistration Request (parameters)
2. HTTP 401 Unauthorized WWW-Authenticate: Digest-Challenge (AUTN params)
3. HTTP POST Authorization Request: Digest-Response (AUTN params)
4. HTTP 200 OK POST Authentication-Info: Deregistration Response (Status Code)

Figure 78 – Call Flow for Smartcard Profile’s De-registration Request/Response Message Exchange

It is assumed that SMK and SRK have been established as described in Section 5.4.7.2.1 prior to the start of the message exchange described below.

1. The BSP-C sends the De-registration message to the BSP-M. The De-registration message is an HTTP message. The format of the De-registration message is specified in [3GPP TS 33.246].

2. As the request is for an access-protected object, and the appropriate Authorization header is not included in the request message received by the BSP-M, the BSP-M responds with a “401 Unauthorized” status code, along with WWW-Authenticate header containing the digest challenge.
3. The BSP-C retries the request, this time including in the HTTP POST the Authorization header line which contains the digest response using the SRK as the password, and B-TID or NAI (Network Access Identifier) as the username, for the (U)SIM Smartcard Profile or (R-)UIM/CSIM Smartcard Profile, respectively.
4. The BSP-M authenticates the BSP-C by computing the digest response. If authentication is successful the BSP-M sends the 200 OK along with the appropriate status code for the message type.

Once the above steps have been completed, the terminal is "deregistered" at the BSP-M. After the BSP-C has successfully deregistered the BSP-M SHOULD stop sending LTKM updates to the terminal as it is no longer contactable.

5.4.7.2.8 LTKM Request Procedure Messages

The messages exchanged between the BSP-C and BSP-M when the terminal requests LTKMs it has not received are those defined by 3GPP MBMS. The LTKM Request message is not a BCAST service provisioning message, i.e., it is not related to subscription or a token purchase. The message format and message exchanged is defined in [3GPP TS 33.246] in section 6.3.2.2 "MSK request procedures".

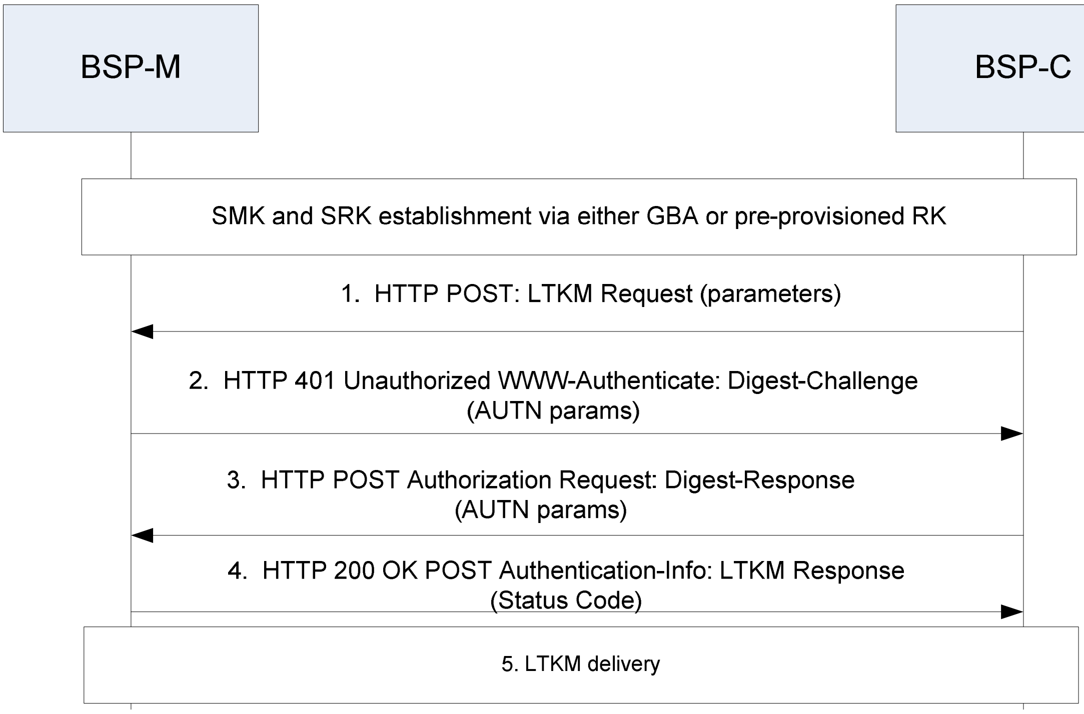

BSP-M
BSP-C
SMK and SRK establishment via either GBA or pre-provisioned RK
1. HTTP POST: LTKM Request (parameters)
2. HTTP 401 Unauthorized WWW-Authenticate: Digest-Challenge (AUTN params)
3. HTTP POST Authorization Request: Digest-Response (AUTN params)
4. HTTP 200 OK POST Authentication-Info: LTKM Response (Status Code)
5. LTKM delivery

Figure 79 – Call Flow for Smartcard Profile’s LTKM Request Procedure

It is assumed that SMK and SRK have been established as described in Section 5.4.7.2.1 prior to the start of the message exchange described below.

1. The BSP-C sends the LTKM request message to the BSP-M. The LTKM request message is an HTTP message. This corresponds to the "MSK request" message is specified in [3GPP TS 33.246]. The MSK ID(s) correspond to the SEK / PEK ID(s).
2. As the request is for an access-protected object, and the appropriate Authorization header is not included in the request message received by the BSP-M, the BSP-M responds with a “401 Unauthorized” status code, along with WWW-Authenticate header containing the digest challenge.

3. The BSP-C retries the request, this time including in the HTTP POST the Authorization header line, which contains the digest response using the SRK as the password, and B-TID or NAI (Network Access Identifier) as the username, for the (U)SIM Smartcard Profile or (R-)UIM/CSIM Smartcard Profile, respectively.
4. The BSP-M authenticates the BSP-C by computing the digest response. If authentication is successful the BSP-M sends the 200 OK along with the appropriate status code for the message type.
5. The LTKM is delivered to the BSP-C from the BSP-M. The BSP-M SHOULD push LTKMs to the terminal over UDP following a successful Service Request/Response procedure. However, if the BSP-C does not receive the LTKM related to the successful LTKM request procedure, the BSP-C SHOULD repeat the "LTKM Request Procedure".

5.4.7.2.9 Other Service Provisioning Messages

Similar to Section 5.4.7.2.1, after the establishment of SMK and SRK between the BSP-C and BSP-M, the BSP-C can now send to the BSP-M either of the following types of Service Provisioning messages:

- Pricing Information Request
- Account Inquiry Request

Figure 50 shows the call flow for such service provisioning message exchange. Prior to the message exchange, the BSP-C and BSP-M are mutually authenticated, and the contents of the message may be encrypted by a secret key shared between these entities.

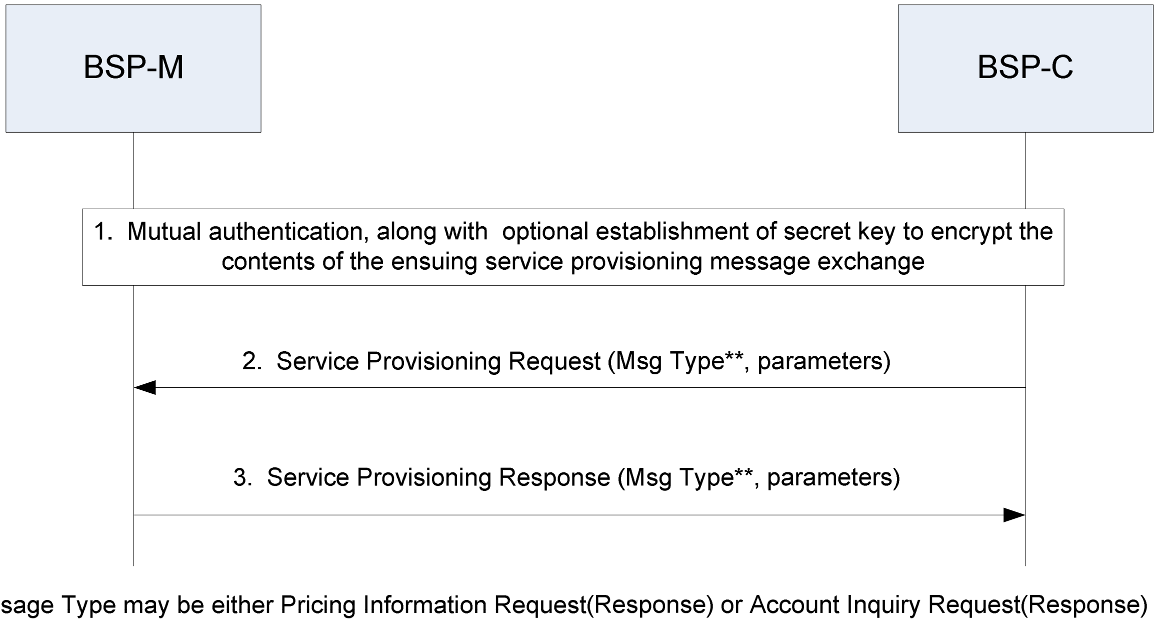

BSP-M
BSP-C
1. Mutual authentication, along with optional establishment of secret key to encrypt the contents of the ensuing service provisioning message exchange
2. Service Provisioning Request (Msg Type**, parameters)
3. Service Provisioning Response (Msg Type**, parameters)
**Message Type may be either Pricing Information Request(Response) or Account Inquiry Request(Response)

Figure 80 – Call Flow for Smartcard Profile's Pricing Information and Account Information Message Exchange

1. The BSP-M and BSP-C mutually authenticates each other, and may establish a shared secret key to protect subsequent communications between them.
2. The BSP-C sends the service provisioning request message to the BSP-M.
3. The BSP-M provides the response to the service provisioning message.

5.4.7.3 Web Service Provisioning Flows (Informative)

Service Provisioning can be achieved by webshop/web portal. This section shows the subscription flows in for both DRM Profile and Smartcard Profile. It should be noted that this section is informative considering various possibilities of implementation to support web portal based service provisioning.

5.4.7.3.1 Subscription procedure in case that terminal supports DRM profile

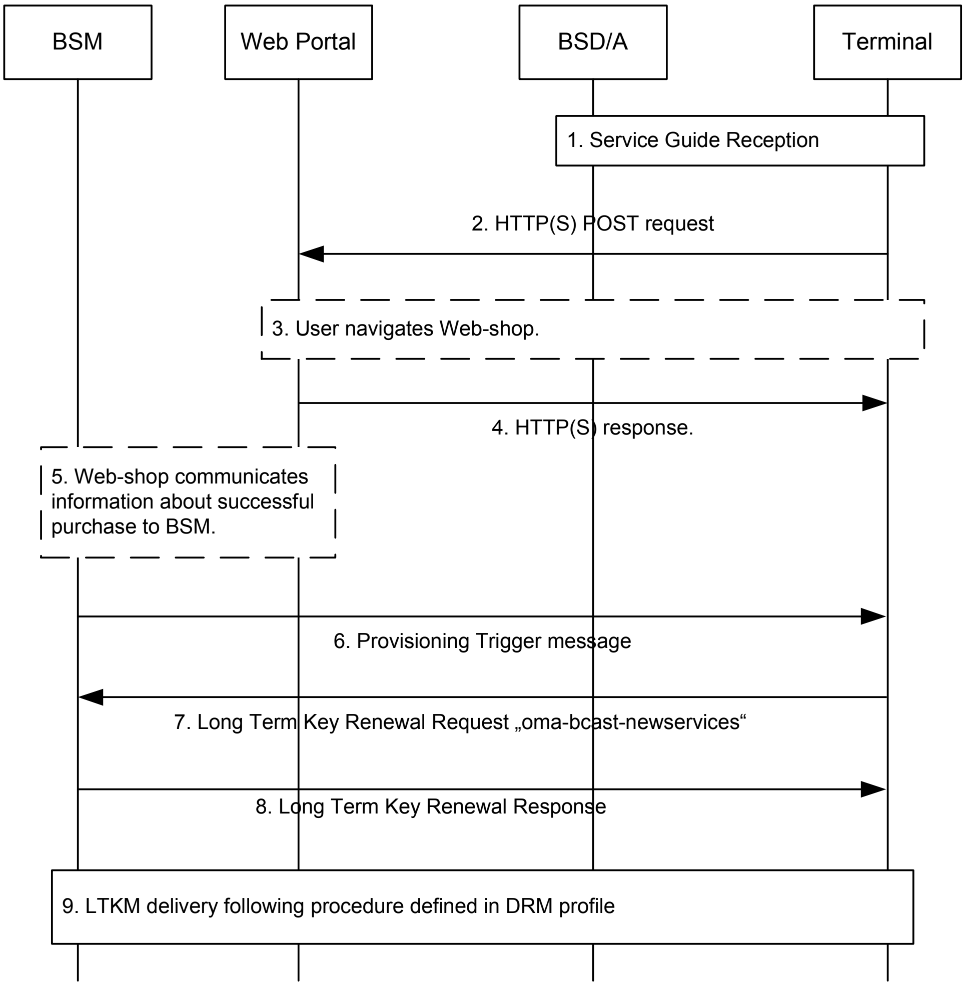

BSM
Web Portal
BSD/A
Terminal
1. Service Guide Reception
2. HTTP(S) POST request
3. User navigates Web-shop.
4. HTTP(S) response.
5. Web-shop communicates information about successful purchase to BSM.
6. Provisioning Trigger message
7. Long Term Key Renewal Request „oma-bcast-newservices“
8. Long Term Key Renewal Response
9. LTKM delivery following procedure defined in DRM profile

Figure 81. Subscription flows in case of DRM profile

1. The Terminal receives the Service Guide and presents it to the User. The user proceeds to a web-portal to subscribe to or purchase one or more purchase item(s). The entry point to web-portal is given by the ‘PortalURL’ in Purchase Channel fragment of the Service Guide. GlobalPurchaseItemID(s) and PurchaseDataIDs may be used as request parameters if the user has selected one or more specific purchase items ([BCAST10-Services], section 5.1.8).

2. The Terminal sends a HTTP(s) POST to the web portal’s URL, constructed as described in step 1, and the user is presented with a page from which the navigation begins.

3. The user browses the web-portal to get information related to Purchase Item(s) provided by Service Provider. The Service Provider may offer user specific purchase options.

4. After the user has subscribed to or purchased one or more purchase item(s), the web portal sends a 200 OK message to the Terminal to indicate success. . With this message, that usually also delivers an HTML page, the interaction with the web portal is finished and the purchase is considered completed.

5. The web portal communicates the results of the purchase transaction to the BSM via means that are out of scope of this specification.

6. The BSM sends the terminal a Provisioning Trigger message via SMS.

7. Reacting on this trigger, the terminal sends a Long Term Key Renewal Request to the BSM, requesting keys for purchase items for which the terminal has not yet received information how to acquire the rights.

8. The BSM sends a Long Term Key Renewal Response to the terminal which lists all newly subscribed purchase items and contains a ROAP trigger allowing to acquire the rights for all these items.

9. On reception of the Trigger message the Terminal requests the relevant LTKM(s) following the procedure defined for the DRM profile.

5.4.7.3.2 Subscription procedure in case that terminal supports Smartcard profile

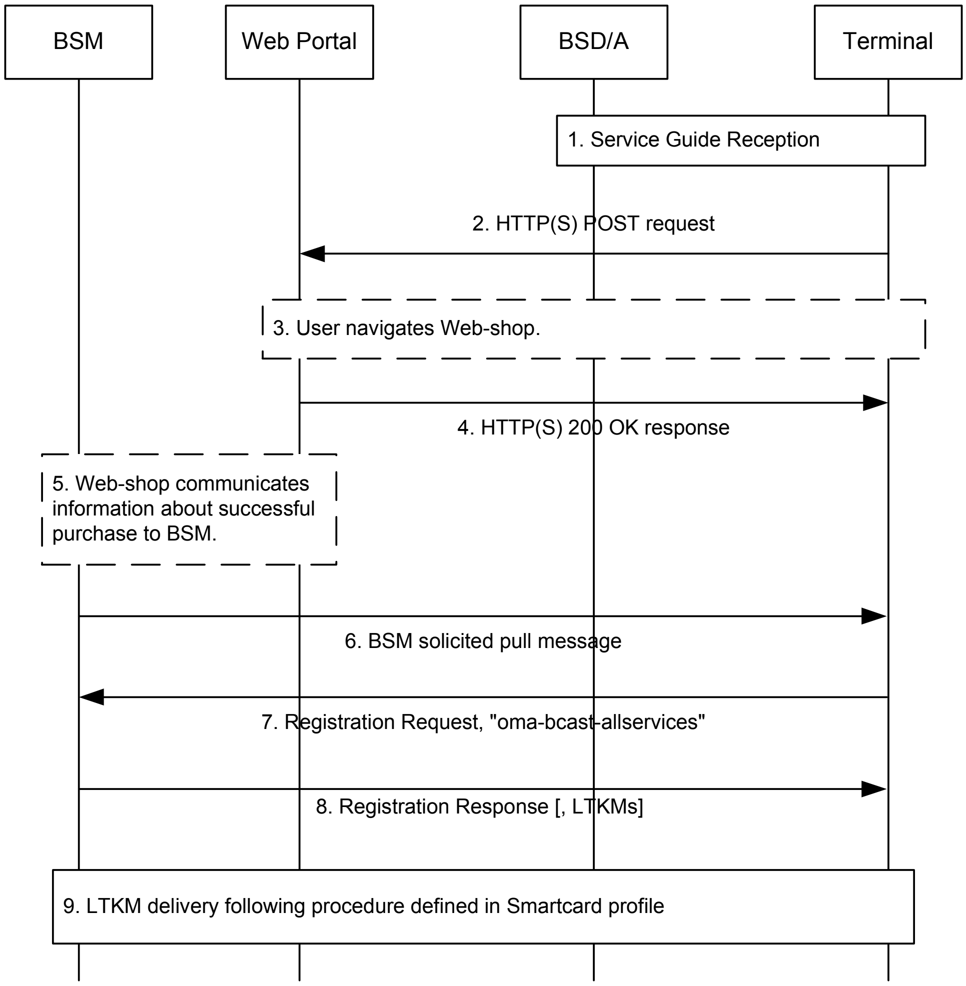

BSM
Web Portal
BSD/A
Terminal
1. Service Guide Reception
2. HTTP(S) POST request
3. User navigates Web-shop.
4. HTTP(S) 200 OK response
5. Web-shop communicates information about successful purchase to BSM.
6. BSM solicited pull message
7. Registration Request, "oma-bcast-allservices"
8. Registration Response [, LTKMs]
9. LTKM delivery following procedure defined in Smartcard profile

Figure 82. Subscription flows in case of Smartcard profile

1. The Terminal receives the Service Guide and presents it to the user. The user proceeds to web-portal to subscribe to or purchase one or more purchase item(s). The entry point to web-portal is given by the ‘PortalURL’ in Purchase Channel fragment of the Service Guide. GlobalPurchaseItemID(s) and PurchaseDataIDs may be used as request parameters if the user has selected one or more specific purchase items ([BCAST10-Services], section 5.1.8).

2. The Terminal sends a HTTP(s) POST to the web portal’s URL, constructed as described in step 1, and the user is presented with a page from which the navigation begins.

3. The user browses the web-portal to get information related to Purchase Item(s) provided by the Service Provider. The Service Provider may offer user specific purchase options.

4. After the user has subscribed to or purchased one or more purchase items, the web portal sends a 200 OK message to the Terminal to indicate success. With this message, that usually also delivers an HTML page, the purchase is considered completed.

5. The web portal communicates the results of the purchase transaction to the BSM via means that are out of scope of this specification.

6. If the terminal is in a registered state in the BSM, the BSM sends the terminal a BSM solicited pull message via one of the LTKM trigger bearers (UDP or SMS) negotiated in last registration procedure.

7. Reacting on this trigger, the Terminal sends a Registration Request for “oma-bcast-allservices” to BSM. If the NAF determines from the registration procedure that the terminal is not authenticated, it will also prompt a GBA run.
8. The BSM sends to the terminal a Registration Response which lists all subscribed purchase items, including the newly subscribed purchase items. If HTTP is part of the negotiated LTKM delivery mechanisms, the BSM may also include in the response all the LTKMs needed for the terminal, including the LTKMs associated to the newly subscribed purchase items.
9. After Registration, and if no LTKMs were included in the Registration Response, the Terminal will receive relevant LTKM(s) over UDP in accordance to the procedure defined in Smartcard profile.

5.4.8 Notification Function Related Flows

The Notification Function is responsible for informing a terminal or a group of terminals about broadcast service events, like for example a change in the service guide, or new availability of service and programs. The classification of events is done by the Broadcast Service Provider. For this purpose, the Notification Function generates a notification message and sends it to a terminal or a group of terminals, either direct or via the notification function in the BDS (if available), which further distributes the notification via broadcast or interactive channel.

A notification is a one-way (push) signaling towards the terminal. It may or may not trigger subsequent action, for example interactive download of service guide or fragments thereof.

The examples in this section illustrate notification delivery flows for certain events. Notification events for other purposes are also possible, but are not listed here exhaustively.

5.4.8.1 Notification Generation and Delivery over Broadcast Channel by OMA BCAST

The figure below shows the message flow for notification delivery over Broadcast Channel:

1a to 1c. A notification event is triggered either by the NTE, NTG, NTDA, BDS or NTG. If the notification event occurs in CC or BSA, then NTE in BSA send the Event notice to NTG in BSM over interface NT-3. If the notification event occurs in BDS, BDS sends the Event notice to NTG in BSM via NTDA over interface NT-B1 and NT-4. If the notification event occurs in BSD/A, then NTDA in BSD/A sends the Event notice to NTG in BDS over interface NT-4. If some service guide attributes are required for notification message generation, then NTE or NTDA may send them. If the notification event is triggered by the NTE, it sends a trigger for a notification message, notification attributes, and possibly service guide attributes to the NTG, over interface NT-3. Notification event can also occur by BSM itself. After notification notice is received, NTG in BSM generates notification message and also set the list of receiver who will receive this notification message.

2. The NTG generates the notification message. The notification message generated by NTG is transmitted to NTD/A in BSM over interface NT-4. NTDA may adapt the receive message then, it sends it to BDS for the delivery of notification message. The NTG sends the generated notification message to the NTDA for adaptation and distribution. A description of the receivers that shall receive the notification must be included at this point.
3. The notification message, which is possibly adapted by NTD/A is sent to a terminal or a group of terminals through BDS. After receiving notification message, a terminal or a User may take corresponding actions.

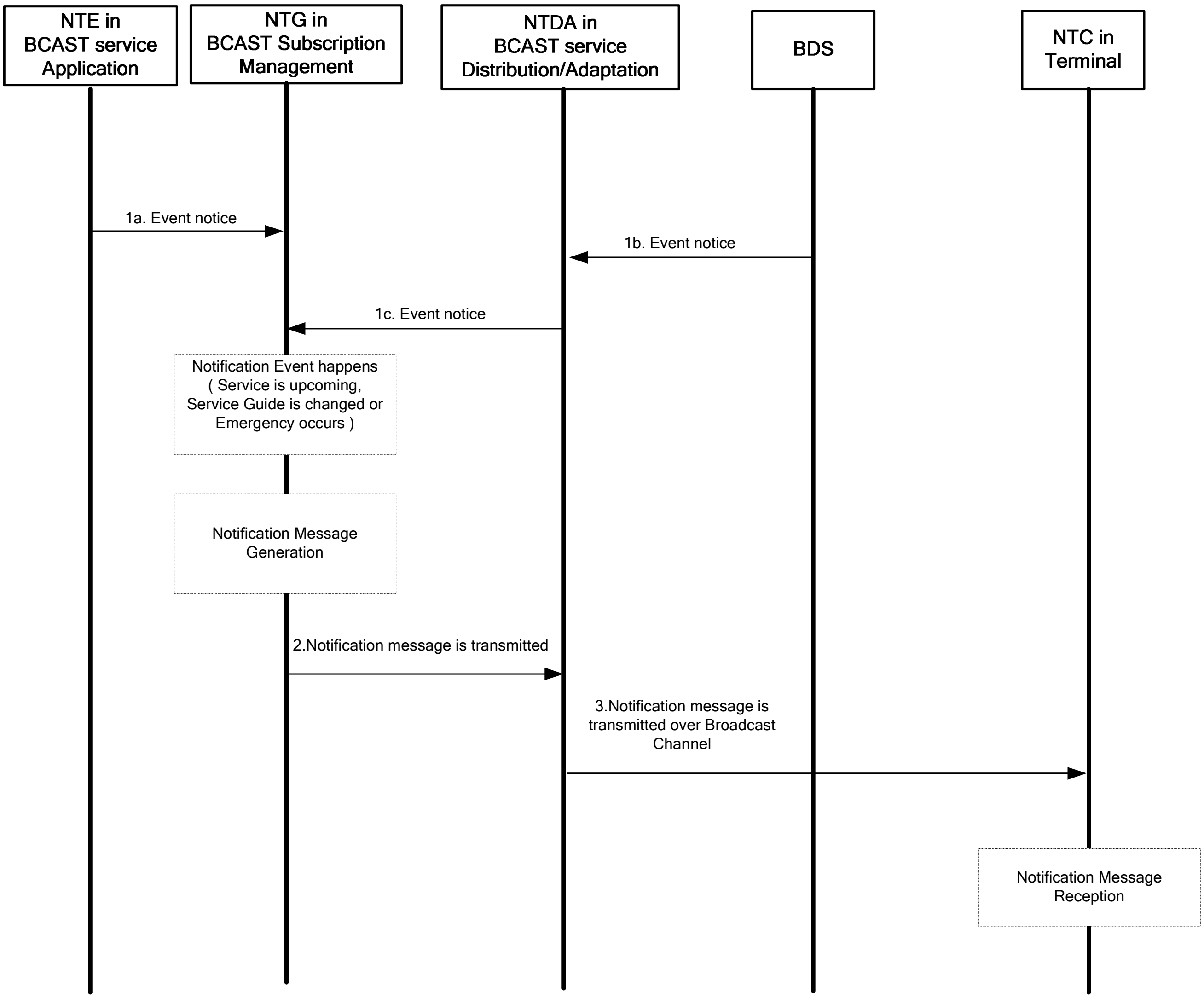


Figure 83 - Delivery of Notifications over Broadcast Channel by OMA BCAST

5.4.8.2 Notification Delivery over Broadcast channel by BDS

The figure below shows the message flow for notification delivery over Broadcast Channel:

1a to 1c. The operation of these flows is identical to those of 1a, 1b and 1c in section 5.4.8.1.

2. The operation of this flow is identical to that of 2 in section 5.4.8.1.
3. The notification message, which is possibly adapted by NTD/A is sent to BDS (via NT-B1). BDS having its own notification distribution component may transform OMA BCAST notification message to its own notification message form.
4. BDS sends a notification message to a terminal or a group of terminal. After receiving notification message, a terminal or a User may take corresponding actions.

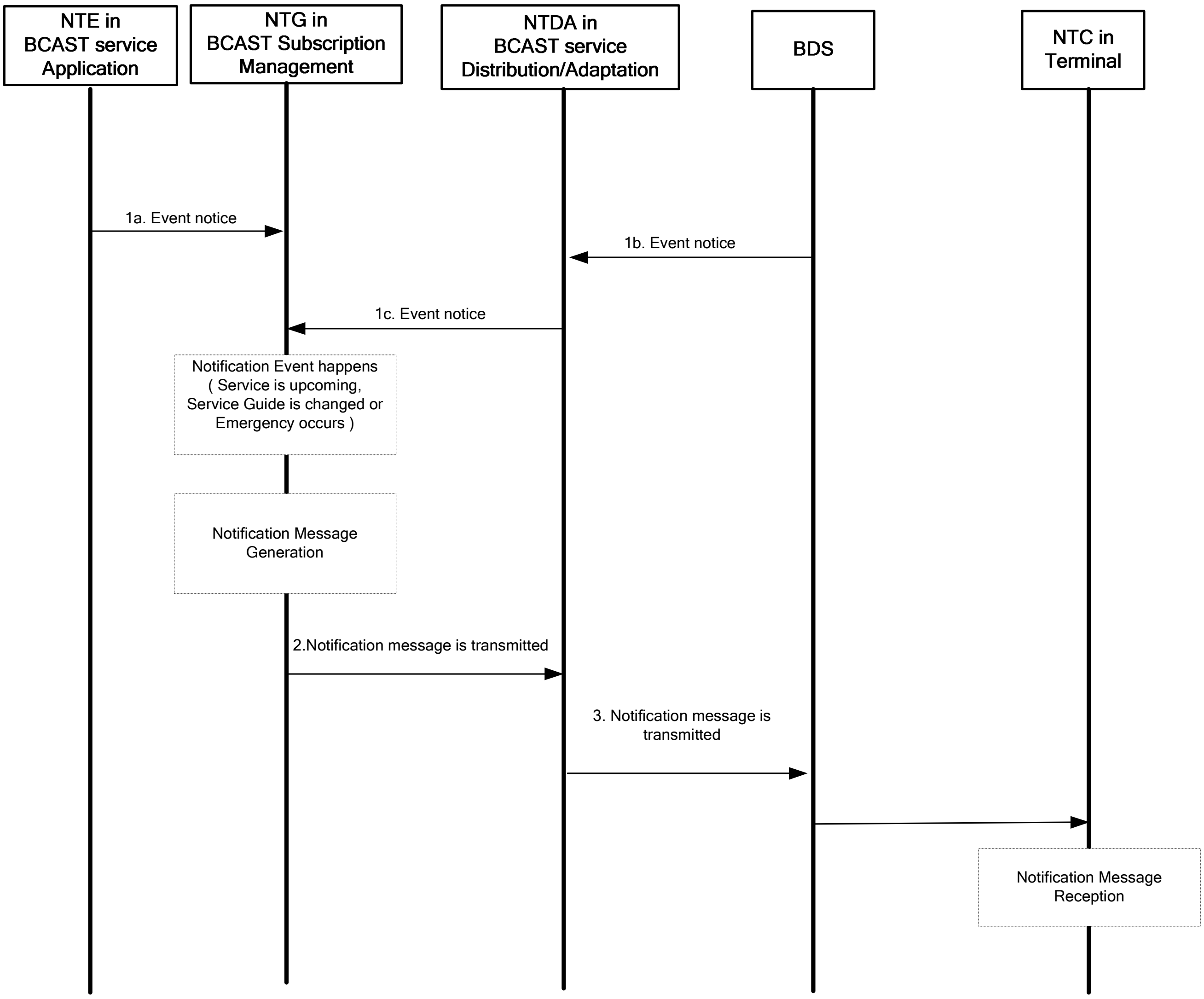

NTE in BCAST service Application
NTG in BCAST Subscription Management
NTDA in BCAST service Distribution/Adaptation
BDS
NTC in Terminal
1a. Event notice
1b. Event notice
1c. Event notice
Notification Event happens (Service is upcoming, Service Guide is changed or Emergency occurs)
Notification Message Generation
2.Notification message is transmitted
3. Notification message is transmitted
Notification Message Reception

Figure 84 - Delivery of Notification over Broadcast Channel by BDS

5.4.8.3 Notification Delivery over Interaction Channel by OMA BCAST

The figure below shows the message flow for notification delivery over Interaction Channel:

1a to 1c. The operation of these flows is identical to those of 1a, 1b and 1c in section 5.4.7.1.

2. The operation of this flow is identical to that of 2 in section 5.4.7.1.
3. The notification message, which is possible adapted by NTD/A is sent to a terminal via Interaction Network. After receiving notification message, a terminal or a User may take corresponding actions.

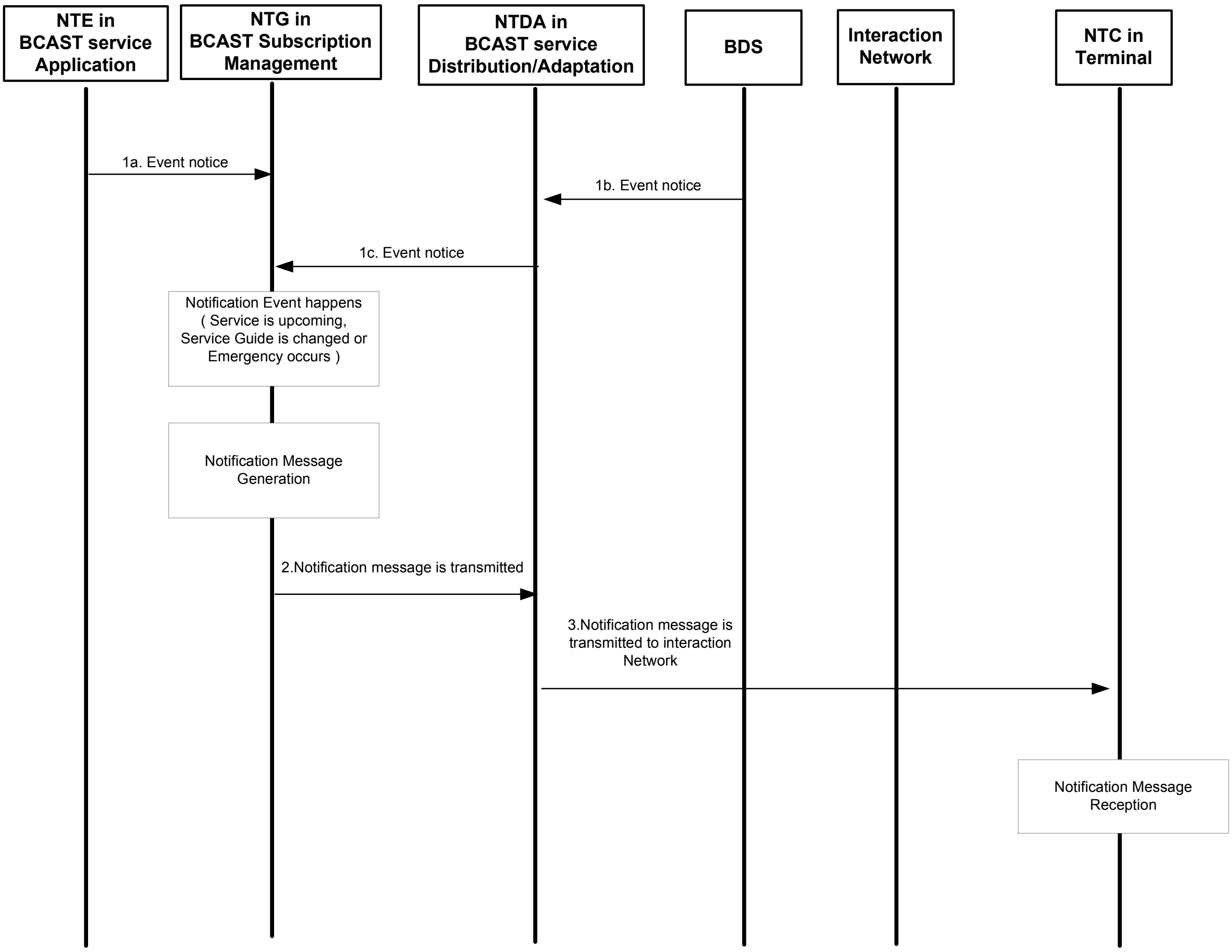

NTE in BCAST service Application
NTG in BCAST Subscription Management
NTDA in BCAST service Distribution/Adaptation
BDS
Interaction Network
NTC in Terminal
1a. Event notice
1b. Event notice
1c. Event notice
Notification Event happens (Service is upcoming, Service Guide is changed or Emergency occurs)
Notification Message Generation
2.Notification message is transmitted
3.Notification message is transmitted to interaction Network
Notification Message Reception

Figure 85 - Delivery of Notification over Interaction Network by OMA BCAST

5.4.8.4 Notification Delivery over Interaction Channel by Interaction Network

The figure below shows the message flow for notification delivery over Interaction Channel:

1a to 1c. The operation of these flows is identical to those of 1a, 1b and 1c in section 5.4.7.1.

2. The operation of this flow is identical to that of 2 in section 5.4.7.1.
3. The notification message, which is possibly adapted by NTD/A is sent to Interaction Network via BDS Service Distribution/Adaptation (through NT-B1). Interaction Network may transform OMA BCAST notification message to is own notification message form.
4. Interaction Network sends a notification message to a terminal over Interaction Channel. After receiving notification message, a terminal or a User may take corresponding actions.

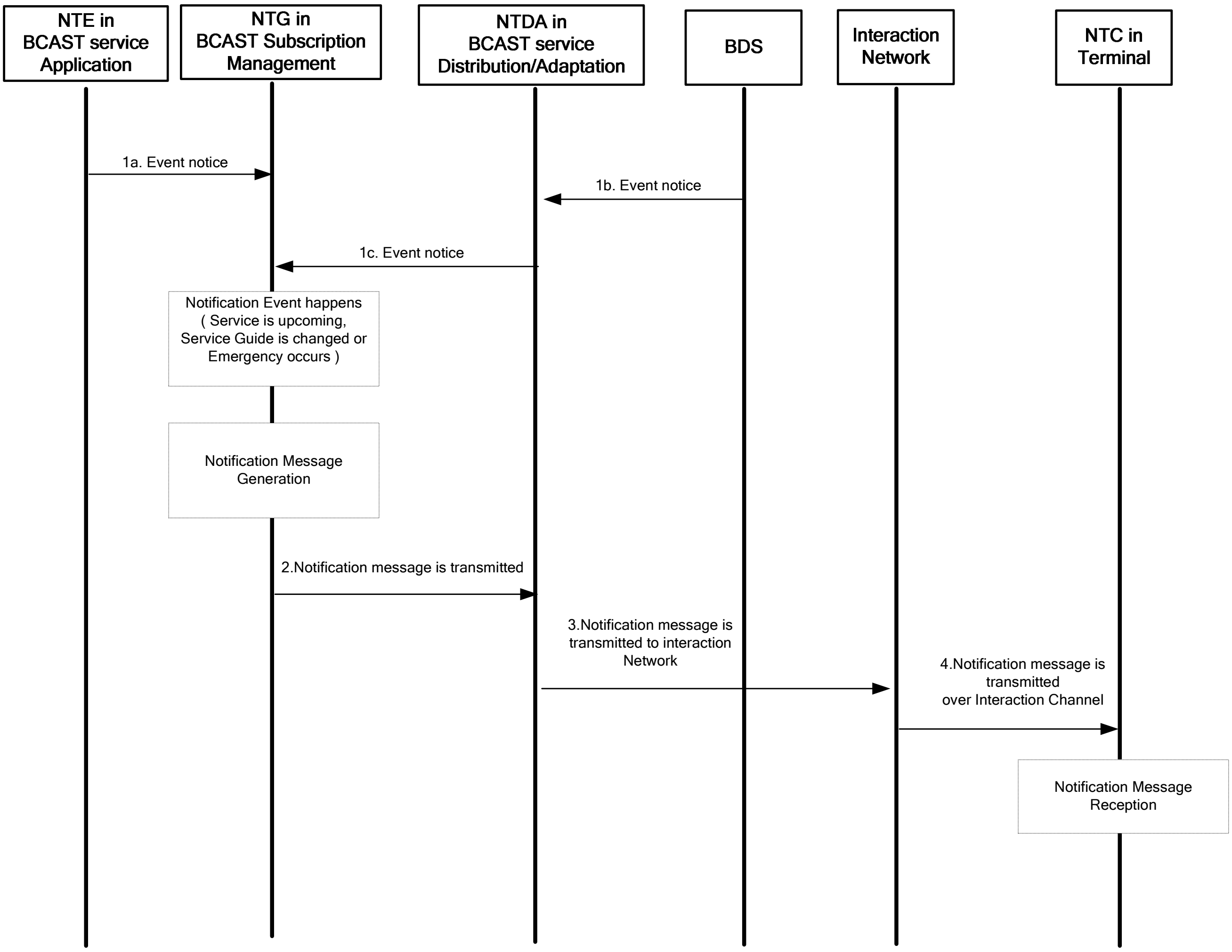

NTE in BCAST service Application
NTG in BCAST Subscription Management
NTDA in BCAST service Distribution/Adaptation
BDS
Interaction Network
NTC in Terminal
1a. Event notice
1b. Event notice
1c. Event notice
Notification Event happens (Service is upcoming, Service Guide is changed or Emergency occurs)
Notification Message Generation
2.Notification message is transmitted
3.Notification message is transmitted to interaction Network
4.Notification message is transmitted over Interaction Channel
Notification Message Reception

Figure 86 - Delivery of Notification over Interaction Channel by Interaction Network

5.4.9 Roaming Related Flows

There are only two possible scenarios for BCAST roaming:

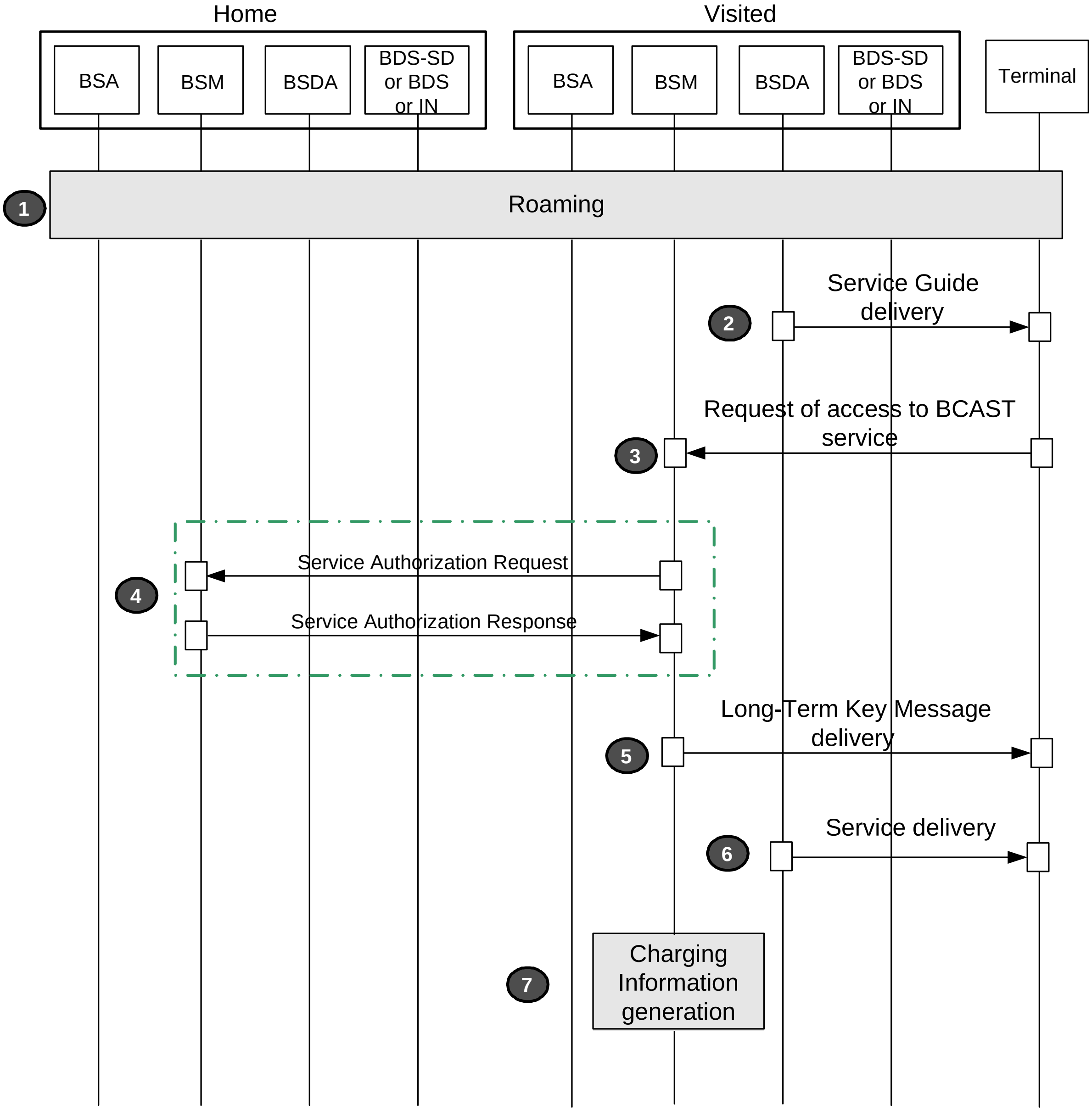
a) Roamer receives content provided by the Home Network BCAST Service Provider (SP); or

b) Roamer receives content provided by the Visited Network BCAST SP, but with usage captured and charging information reported back to the Home Network BCAST SP.

Scenario (b) Roaming allows a user to receive Broadcast Services from a Broadcast Service Provider different from his Home Broadcast Service Provider. The change of the Mobile Broadcast Service Provider allows the user to receive Broadcast Services from another Broadcast Service Provider independent of the underlying Broadcast Distribution System.

This section provides flows for scenario (b) roaming.

5.4.9.1 Broadcast services in the Visited Network


Home
Visited
BSA
BSM
BSDA
BDS-SD or BDS or IN
BSA
BSM
BSDA
BDS-SD or BDS or IN
Terminal
1
Roaming
2
Service Guide delivery
3
Request of access to BCAST service
4
Service Authorization Request
Service Authorization Response
5
Long-Term Key Message delivery
6
Service delivery
7
Charging Information generation

BCAST Service Application = BSA
BCAST Service Distribution/Adaptatation = BSDA
BCAST Subscribtion Management = BSM
BCAST Distribution System-Service Distribution = BDS-SD
Interaction Network = IN

Figure 87 - BCAST Services in Visited Network

1. The End User has subscribed the BCAST roaming services at the Home Network before he/she moves to the Visited Network. The exact mechanism to roam from the Home Network to the Visited Network is out of scope of BCAST services. The End User has to register over cellular network (e.g., VLR or IMS) mechanisms to the Visited Network. The details of registration are out of scope of BCAST.

2. The terminal of the roaming user receives the Service Guide from the Visited Network without any contact to the Home Network.
3. After reviewing the Service Guide, the End User requests Long-Term Key Messages for the access to a particular BCAST service from the BCAST Subscription Management (BSM) of the Visited Network.
4. The BSM of the Visited Network obtains authorization from the BSM of the Home Network.
5. The requested Long-Term Key Messages are delivered to the End User by the BSM of the Visited Network.
6. The terminal of the End User starts receiving the service broadcast by the BSDA, decrypts and consumes it.
7. The BSM of the Visited Network generates charging information. The details of how this charging information is generated and how it is sent to the Home Network are out of scope of BCAST Services.

Note: In case of Free-to-Air services, Steps 1, 2 and 6 are applicable; Steps 3, 4, 5 and 7 may or maybe not applicable.

5.4.10 Terminal Provisioning Related Flows

5.4.10.1 Terminal Provisioning over Interaction Channel

The figure below shows an example for the Terminal Provisioning over Interaction Channel.

Note: The operation of Terminal Provisioning over interaction channel follows [OMA-DM].

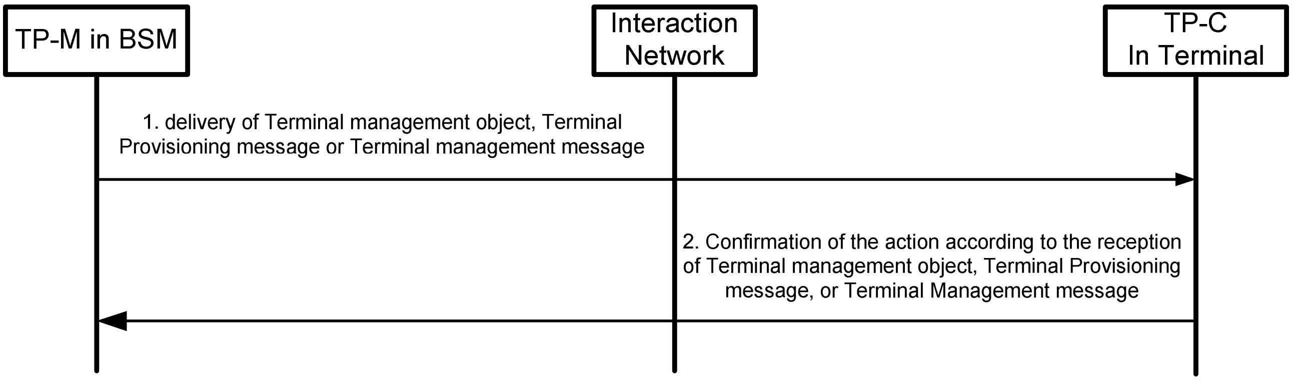

TP-M in BSM
Interaction Network
TP-C In Terminal
1. delivery of Terminal management object, Terminal Provisioning message or Terminal management message
2. Confirmation of the action according to the reception of Terminal management object, Terminal Provisioning message, or Terminal Management message

Figure 88 - Terminal Provisioning over Interaction Channel

1. TP-M in BSM generates Terminal Provisioning messages including BDS-specific parameters or roaming specific parameters or Service Guide Server Address and delivers them to TP-C through Interaction Network (TP-7). They contain parameters and/or command to be used for Terminal Provisioning to TP-C in Terminal.

   Note: The operation on TP-7 is defined in [OMA-DM].

2. TP-C in Terminal confirms the action according to the reception of Terminal Provisioning Message, which contains parameters and/or command to be used for Terminal Provisioning to TP-M in BSM through Interaction Network (TP-7).

   Note: The operation on TP-7 is defined in [OMA-DM].

5.4.11 Other Cross-Function Flows

Nil.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-BCAST-V1_0-20090212-A	12 Feb 2009	Approved by TP TP ref# OMA-TP-2009-0071-INP_BCAST_V1_0_ERP_for_Notification_and_Final_Approval