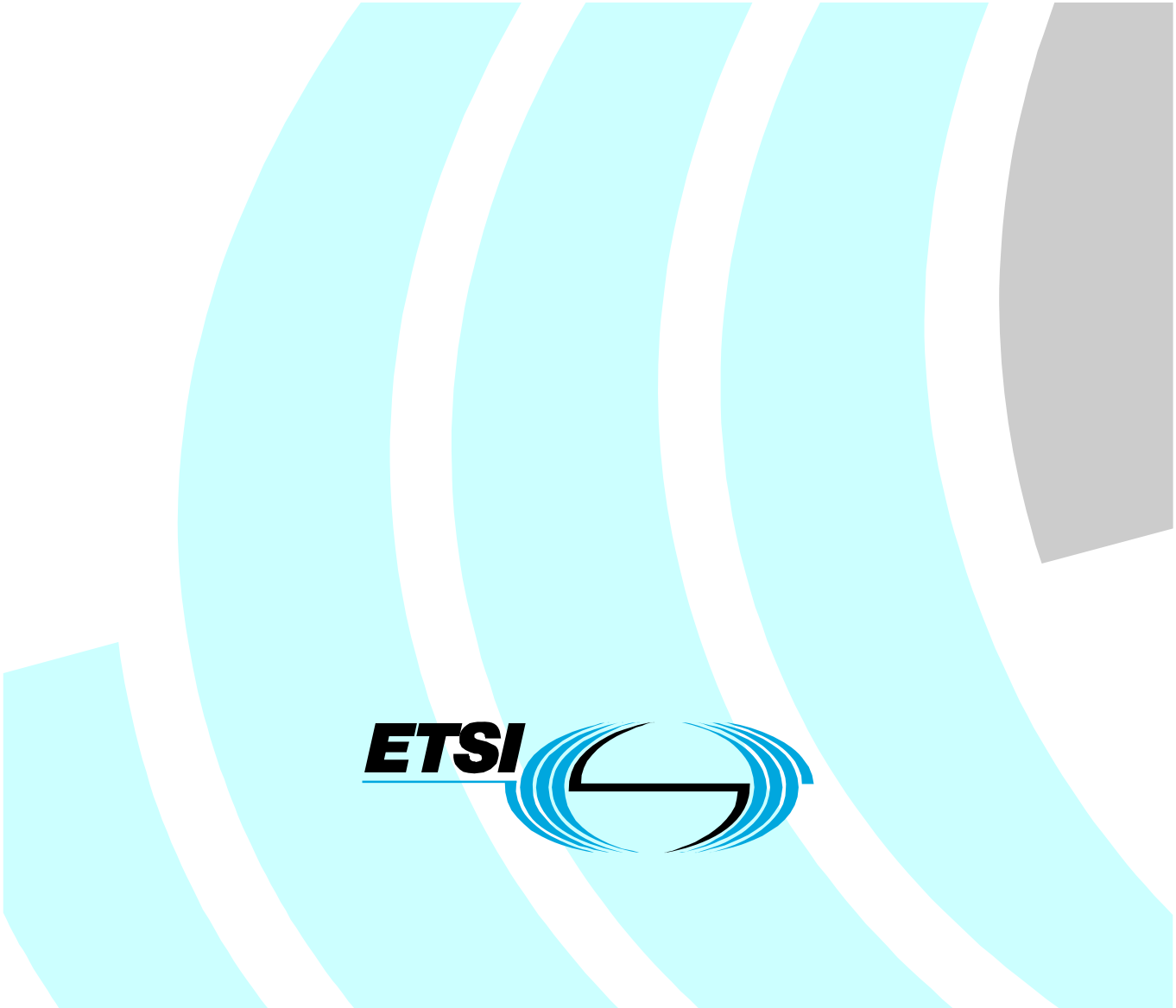
ETSI TR 187 013 V3.1.1 (2011-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on IPTV Security Architecture



Reference
DTR/TISPAN-07033-NGN-R3

Keywords
architecture, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document presents the result of a study of options for the IPTV security architecture supporting TISPAN NGN Release 3 that satisfies the security requirements for IPTV given in TS 187 001 [i.1].

The present document offers the results of analysis of the options for security architecture and mechanisms to provide IPTV service protection where service protection refers to the protection offered during the period when IPTV media is transmitted in the NGN. A security architecture for a general content protection framework to allow comparison of existing content protection solutions (e.g. DRM systems) is required for the NGN, but is not covered by the present document. Content protection includes the provision of post-delivery protection of IPTV media and may include controls to ensure that the user can only use the content in accordance with the license it has been granted, e.g. the times of the content can be viewed.

NOTE: The functional architecture for IMS based IPTV without security entities conforms to TS 182 027 [i.5]. The functional architecture for dedicated IPTV subsystem without security entities conforms to TS 182 028 [i.6].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[i.2] Void.

[i.3] ETSI TS 181 016: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN Services and IPTV".

[i.4] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[i.5] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[i.6] ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem Architecture".

[i.7] ETSI TS 183 063: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based IPTV stage 3 specification".

[i.8] OMA-TS-BCAST-SvcCntProtection - v1-0: "Service and Content Protection for Mobile Broadcast Services", version 1.0, Open Mobile Alliance.

[i.9] ETSI TS 103 197: "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".

[i.10] ETSI TS 133 246: "Security of Multimedia Broadcast/Multicast Service (MBMS) Release 8".

[i.11] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220 Release 8)".

[i.12] ETSI TS 123 246: "Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (3GPP TS 23.246 Release 8)".

[i.13] ETSI TS 126 237: "Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) based Packet Switch Streaming (PSS) and Multimedia Broadcast/Multicast Service (MBMS) User Service; Protocols (3GPP TS 26.237 Release 8)".

[i.14] OMA-AD-BCAST-v1-0: "Open Mobile Alliance: "Mobile Broadcast Services Architecture".

[i.15] OIPF Release 1 Specification "Authentication, Content Protection and Service Protection", V1.1, 2009-10-08 (volume 7).

[i.16] Marlin Developer Community: "Marlin Broadband Transport Stream Specification", Version 1.0.1, July 2008.

[i.17] Marlin Developer Community: "Marlin - Broadband Network Service Profile Specification", Version 1.0, July 2008.

[i.18] Marlin Developer Community: "Marlin - Core System Specification", Version 1.3, latest Marlin Errata: Marlin Core System v1.3.

[i.19] Marlin Developer Community: "Marlin - File Formats Specification", Version 1.1, and latest version of "Marlin Errata: Marlin - File Formats Specification V1.1".

[i.20] Marlin Developer Community: "OMArlin Specification", Version 1.0.1, July 2008.

[i.21] OASIS: "Assertions and Protocols for the OASIS Security Markup Language (SAML) V2.0".

[i.22] OASIS: "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0".

[i.23] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[i.24] IEC 62455: "Internet protocol (IP) and transport stream (TS) based service access".

[i.25] ISO/IEC 13818-1:2000/Amd.3:2004: "Generic coding of moving pictures and associated audio information: Systems".

[i.26] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.27] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[i.28] Making better standards.

NOTE: See http://portal.etsi.org/mbs/.

[i.29] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[i.30] ETSI TS 133 110: "Universal Mobile Telecommunications System (UMTS); LTE; Key establishment between a UICC and a terminal (3GPP TS 33.110)".

[i.31] ETSI TS 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)".

[i.32] IETF RFC 3310: "HTTP Digest Authentication Using AKA".

[i.33] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102)".

[i.34] ETSI TS 131 103: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103)".

[i.35] ETSI TS 126 346: "Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs (3GPP TS 26.346)".

[i.36] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[i.37] ETSI TS 124 109: "Universal Mobile Telecommunications System (UMTS); LTE; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details (3GPP TS 24.109)".

[i.38] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[i.39] ETSI TS 184 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN".

[i.40] ETSI TS 184 009: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Rules covering the use of TV URIs for the Identification of Television Channels".

[i.41] ETSI TS 133 203 (V9.4.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services (3GPP TS 33.203 version 9.4.0 Release 9)".

[i.42] ETSI TS 102 474: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection".

[i.43] ETSI ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".

[i.44] DVB bluebook A125: "Digital Video Broadcasting (DVB); Support for use of DVB Scrambling Algorithm version 3 within digital broadcast systems, DVB Document A125", July 2008.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

content protection: protection of content or content assets during its entire lifetime

NOTE: The content provider defines the lifetime that the protection is required for.

Content Provider (CP): entity that owns or is licensed to sell content or content assets

license: data package which represents the granted Rights to a specific user and the key related to the protected Content

rights: pre-defined set of usage entitlement to the content. The entitlement may include the permissions (e.g. to view/hear, copy, modify, record, distribute, etc.), constraints (e.g. play/view/hear multiple times or hours), etc.

service protection: protection of content (e.g. files or streams) and service information during delivery which may include content already protected and meta data that the service provider adds to the content

NOTE: The service may be composed of the content to be transferred and other data and service components. Service protection addresses protecting this composition while in transit and regulates authorized access to the service. Additionally it addresses ensuring the service availability, as defined in the service level agreements.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard (AES)
AKA	Authentication and Key Agreement
AU	Access Unit
AV	Authentication Vector
BC	BroadCast
BCAST	BROADCAST
BCRO	Broadcast Rights Object
BDS	Broadcast Distribution Service
BSD/A	BCAST Service Distribution/Application
BSF	Boostrapping Strapping Function
BSM	BCAST Subscription Management
CA	Certificate Authority
CA	Conditional Access
CAS	Conditional Access System
CEF	Content Encryption Function
CND	Customer Network Device
CNG	Customer Network Gateway
CoD	Content on Demand
CP	Content Provider
CSA	Common Scrambling Algorithm
CSP	Communication Service Provider
CSPG	Communication Service Provider Group
DRM	Digital Rights Management
DTCP-IP	Digital Transmission Content Protection-IP
DVB	Digital Video Broadcasting
ECM	Entitlement Checking Message
FA	File Application Component
FD	File Delivery Component
FFS	For Further Study
FMC-IPTV	Fixed Mobile Convergence-IP Television
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber Server
ID	IDentifier
IMPI	IM Private Identity
IMS	IP Multimedia Subsystem
IPSEC	Internet Protocol SECure transmission
IPTV	IP Television
ISIM	IMS Subscriber Identity Module
KMF	Key Management Function
LTKM	Long Term Key Message
MBMS	Mobile Broadcast/Multicast Service
MCF	Media Control Function
MDF	Media Delivery Function
MF	Media Function
MNO	Mobile Network Operator
MSK	MBMS Service Key
MTK	MBMS Transport Key
MUK	MBMS User Key
NAF	Network Application Function

NASS	Network Access SubSystem
NBA	Nass Bundled Authentication
NGN	Next Generation Network
OIPF	Open IPTV Forum
OITF	Open IPTV Terminal Function
OMA	Open Mobile Alliance
PC	Personal Conputer
PEK	Programme Encryption Key
PID	Packet Identifier
PMT	Programme Map Table
QoS	Quality of Service
REK	Rights Encryption Key
ROAP	Rights Object Acquisition Protocol
RTCP	Real Time Control Protocol
RTP	Realtime Transmission protocol
SA	Service Authorization
SAA	Standard Authentication Algorithm
SAML	Security Access Markup Language
SCF	Service Control Function
SCP	SmartCard Profile
S-CSCF	Server - Call Session Control Function
SDF	Service Discovery Function
SDP	Session Description Protocol
SEK	Service Encryption Key
SG	Service Guide
SKMF	Service Key Management Function
SLF	Server Local Function
SMF	Secure Management Function
SP	Service Protection
SP-E	Service Protection Encryption component
SPF	Service Provider Function
SP-KD	Service Protection Key Distribution Component
SP-M	Service Protection Management Component
SRTP	Secure Real Time Protocol
SSEK	Sealed Service Encryption Key
SSF	Service Selection Function
SSO	Single Sign On
STB	Set-Top Box
STKM	Short Term Key Message
TEK	Traffic Encryption Key
TLS	Transaction Layer Security
TMPI	Temporary IP Multimedia Private Identity
TS	Transport Stream
UA	User Authentication
UDP	Unicast Datagram Packet
UE	User Equipment
UICC	Universal Integrated Circuit Card
UPSF	User Profile Server Function
URK	User Root Key
USIM	Universal Subscriber Identity Module

4 Security Requirements on IPTV Content and Service Protection

The Security Requirements are for IPTV are defined in clause of 4.13 of TS 187 001 [i.1] and captured in table 4.1 classified by the form of countermeasure required to satisfy the requirement.

Table 4.1: IPTV security requirements and countermeasure class implied

Req-Id	Requirement statement	Countermeasure class
R-IPTV-C-1	The NGN IPTV service allows several kinds of users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users.	Identification
R-IPTV-C-2	The NGN IPTV service assigns unique and non-forgeable user identities to users.	Identification
R-IPTV-C-3	The NGN IPTV service allows several (number to be decided) users to be associated with one subscription.	Identification
R-IPTV-C-4	The NGN IPTV service uniquely authenticates all users to the IPTV service using unique and non-forgeable authentication credentials on a subscription basis.	Authentication
R-IPTV-C-5	The NGN IPTV service uniquely authorizes all users to the IPTV service on a subscription basis.	Authorisation
R-IPTV-C-6	The NGN IPTV service assigns unique and non-forgeable identities to all subscribers and named groups of subscribers.	Identification
R-IPTV-C-7	The NGN IPTV service uniquely authenticates all subscribers and named groups of subscribers to the IPTV service using unique authentication credentials.	Authentication
R-IPTV-C-8	The NGN IPTV service uniquely authorizes all subscribers and named groups of subscribers to the IPTV service.	Authorisation
R-IPTV-C-9	The NGN IPTV service assigns unique and non-forgeable identities to all user devices.	Identification
R-IPTV-C-10	The NGN IPTV service uniquely authorizes all devices to the IPTV service.	Authorisation
R-IPTV-C-11	The NGN IPTV service assigns unique and non-forgeable identities to all IPTV sessions that are verifiable to users and devices.	Identification
R-IPTV-C-12	The NGN IPTV service assigns unique and non-forgeable identities to all IPTV service providers that are verifiable to users.	Identification
R-IPTV-C-13	The NGN IPTV service provides a mechanism to authenticate and authorize the RTSP control messages from users.	Authorisation
R-IPTV-C-14	The NGN IPTV service assigns unique and non-forgeable identities to all IPTV content that are verifiable for users.	Identification
R-IPTV-CN-1	The NGN IPTV service protection functions supports distribution of access keys coming from the network according to the corresponding rights.	Key Management
R-IPTV-CN-2	The NGN IPTV service protection functions supports means to protect the service-associated keys against unauthorized access, and ensure their integrity and confidentiality.	Key Management
R-IPTV-CN-3	The NGN IPTV service protection functions is able to authenticate and ensure the integrity and confidentiality of communication between the service and the user.	Authentication
R-IPTV-CN-4	The NGN IPTV service protection functions provides a means for protecting time-restricted services (e.g. subscription and pay-per-view).	Authorization
R-IPTV-CN-5	The NGN IPTV service protection functions provides an open framework allowing the operator to choose one or more protection solution.	Availability
R-IPTV-CN-6	The NGN IPTV service protection functions applied on a service providing access to IPTV content is not making any constraint on the way the content is protected.	Availability
R-IPTV-CN-7	The NGN IPTV service protection functions applied on a service providing access to IPTV content interoperates with Content Protection solutions.	Availability
R-IPTV-CP-1	The NGN IPTV content protection authenticates and authorize the origin of all IPTV content to the receiving users.	Authorisation
R-IPTV-CP-2	The NGN IPTV content protection verifies the authenticity of the origin of all IPTV content to the receiving users.	Authentication
R-IPTV-CP-3	The NGN IPTV content protection provides end-to-end content confidentiality protection within regulatory constrains.	Confidentiality

Req-Id	Requirement statement	Countermeasure class
R-IPTV-CP-4	The NGN IPTV service provides end-to-end content integrity protection for an IPTV session.	Integrity
R-IPTV-CP-5	The NGN IPTV service controls and restrict content on a content metadata basis for users.	Identification
R-IPTV-CP-6	The NGN IPTV service and content protection functions provide the means for retrieving related rights and/or keys for chosen protected content items.	Key Management
R-IPTV-CP-7	The NGN IPTV service has a measure to restrict unauthorized usage of content (viewing, re-viewing, copying, etc.) for users.	Authorisation
R-IPTV-CP-8	The NGN IPTV service has a measure to restrict unauthorized distribution of content for users.	Authorisation
R-IPTV-CP-9	The NGN IPTV content protection functions provide a means for protecting time-restricted content usage.	Integrity
R-IPTV-CP-10	The NGN IPTV content protection functions provide an open framework allowing the operator to choose one or more protection solution.	Availability
R-IPTV-NIMS-1	The NGN IPTV service for each IPTV session uniquely links devices, users, named groups of users, entities acting on behalf of users to an IPTV session.	Identification
R-IPTV-NIMS-2	The NGN IPTV service for each combined IPTV session uniquely links devices, users to an IPTV session.	Identification
R-IPTV-NIMS-3	The NGN IPTV service assigns unique identities to critical IPTV service logics on the devices that are verifiable for users.	Identification
R-IPTV-NIMS-4	The NGN IPTV service assigns non-forgeable identities to critical IPTV service logics on the devices that are verifiable for users.	Identification
R-IPTV-NIMS-5	The NGN IPTV service authenticates and authorize critical IPTV service logics on the devices to the receiving user.	Authorisation
R-IPTV-NIMS-6	The NGN IPTV service verifies the authenticity of critical IPTV service logics on the devices to the receiving users.	Authentication
R-IPTV-NIMS-7	Refinement of DSF9: The NGN IPTV service uniquely authenticates all subscribers and named groups of subscribers when accessing private or sensitive information using unique authentication credentials.	Authentication
R-IPTV-NIMS-8	Refinement of DSF10: The NGN IPTV service uniquely authorizes all subscribers and named groups of subscribers when accessing private or sensitive information.	Authorisation
R-IPTV-NIMS-9	The NGN IPTV service provides end-to-end encryption of private or sensitive information on an IPTV session basis.	Confidentiality
R-IPTV-AD-1	The NGN IPTV service is accessible to the authorized users, subscribers and devices according to the requirements of the IPTV service regarding timeliness and quality.	Availability
R-IPTV-AD-2	The NGN IPTV service has measures to prevent DoS attacks posed upon the IPTV service to ensure fulfilment of the requirements of the IPTV service regarding timeliness and quality.	Availability
R-IPTV-AD-3	The NGN IPTV service has measures to detect and act upon all DoS attacks posed upon the IPTV service (note that act might mean inform e.g. the system administrator of the event) to ensure fulfilment of the requirements of the IPTV service regarding timeliness and quality.	Availability

5 Identification and authentication in IPTV

A large number of the IPTV requirements require unique identification of the IPTV user, or of the IPTV Service, with assignments made by the IPTV Service (see table 5.1).

TS 184 002 [i.39] identifies public and private identifiers for NGN subscribers in the NGN as being in the form of either a SIP URI or a tel-URI maintained in either the UPSF or the S-CSCF (which entity holds the identity depends on the nature of the access to the NGN). In addition TS 184 009 [i.40] identifies the use of the tv:URI to uniquely identify television broadcasts. These mechanisms do not fully comply with the requirements stated for IPTV identification in TS 187 001 [i.1].

Security requirements R-IPTV-NIMS-1/2/3 identify a need to link users, devices and user-agents for each IPTV session, whereas TS 184 009 [i.40] only defines identities for broadcasters and not for sessions. A number of views can be taken that may allow this requirement to be met by building on IMS and NGN-R3 capabilities. If registration requires explicit notification of service invocation (such as when using the MBMS capabilities) and where media is protected using service protection the key management audit trail may be used to satisfy these criteria with the root identity of the user and device being visible in IMS and NASS.

Where authentication and authorisation services are required there is an implicit understanding of a security association for these services between the IPTV user and the IPTV service provider. This security association needs to be made explicit. Where the service is provided to a group of users it is strongly recommended that the activities of each member of the group is maintained private from the other members, i.e. the IPTV service should implement an Unlinkability service as defined in ISO/IEC 15408-2 [i.26].

Table 5.1: IPTV security requirements where identification is an explicit requirement

Req-Id	Requirement statement	Countermeasure class
R-IPTV-C-1	The NGN IPTV service allows several kinds of users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users.	Identification
R-IPTV-C-2	The NGN IPTV service assigns unique and non-forgeable user identities to users.	Identification
R-IPTV-C-3	The NGN IPTV service allows several (number to be decided) users to be associated with one subscription.	Identification
R-IPTV-C-6	The NGN IPTV service assigns unique and non-forgeable identities to all subscribers and named groups of subscribers.	Identification
R-IPTV-C-9	The NGN IPTV service assigns unique and non-forgeable identities to all user devices.	Identification
R-IPTV-C-11	The NGN IPTV service assigns unique and non-forgeable identities to all IPTV sessions that are verifiable to users and devices.	Identification
R-IPTV-C-12	The NGN IPTV service assigns unique and non-forgeable identities to all IPTV service providers that are verifiable to users.	Identification
R-IPTV-C-14	The NGN IPTV service assigns unique and non-forgeable identities to all IPTV content that are verifiable for users.	Identification
R-IPTV-CP-5	The NGN IPTV service controls and restrict content on a content metadata basis for users.	Identification
R-IPTV-NIMS-1	The NGN IPTV service for each IPTV session uniquely links devices, users, named groups of users, entities acting on behalf of users to an IPTV session.	Identification
R-IPTV-NIMS-2	The NGN IPTV service for each combined IPTV session uniquely links devices, users to an IPTV session.	Identification
R-IPTV-NIMS-3	The NGN IPTV service assigns unique identities to critical IPTV service logics on the devices that are verifiable for users.	Identification
R-IPTV-NIMS-4	The NGN IPTV service assigns non-forgeable identities to critical IPTV service logics on the devices that are verifiable for users.	Identification

6 Generic stage 2 model for IPTV service protection

6.1 Overview of model

The purpose of the generic model is to provide a non-specific stage 2 like description to allow the evaluation of candidate stage 3 service protection solutions. The model is designed to provide (cryptographic) separation of users accessing a service in a manner consistent with the aims of providing identity and privacy protection in the NGN.

NOTE: The reference to stage 2 and stage 3 is to the approach to standardisation described in ITU-T Recommendation I.130 [i.27] and which is also described for use in ETSI standardisation in the ETSI Making Better Standards website [i.28].

The model for service protection of IPTV as identified in the key hierarchy uses a set of keys that provide cryptographic isolation of services and content for both unicast and multicast distribution of IPTV content. The keys are described in table 6.1.

Table 6.1: Keys in the IPTV key hierarchy

Key	Description
User Root Key (URK)	A symmetric key used for the protected transfer of SEK in multicast service, or for protection of TEK in unicast service. This key is known only to the IPTV user and the SKMF and should be derived as part of an authentication and authorisation service (e.g. IMS-AKA).
Session Encryption Key (SEK)	A symmetric key used for the transfer of traffic encryption keys on a multicast service. This key is known to the session members and to the SKMF.
Traffic Encryption Key (TEK)	A short lifetime symmetric key used to encrypt the IPTV media within the NGN. This key is shared with all IPTV users for a specific channel or programme and with the MDF containing the CEF.

The cryptographic transforms outlined in table 6.2 are defined for the purposes of key management and protection of the media stream within the NGN.

Table 6.2: Outline of cryptographic transforms in IPTV security

Transform identity (note 1)	Purpose
IPTV-KM-CF1	Used to derive the URK.
IPTV-KM-CF21 (note 2)	Used to seal the SEK with URK for delivery to the User, output is a cryptographically sealed SEK (SSEK).
IPTV-KM-CF22	Used to unseal the SSEK when received by the User (partner algorithm to IPTV-KM-CF21).
IPTV-KM-CF31 (note 2)	User to seal the TEK for delivery to the user, output is a cryptographically sealed TEK (STEK).
IPTV-KM-CF32	Used to unseal the STEK when received by the User (partner algorithm to IPTV-KM-CF31).
IPTV-MD-CF1	Used to encrypt the IPTV media using TEK.
NOTE 1: The transform naming convention uses KM to indicate a Key Management transform, and MD to indicate a Media Delivery transform. NOTE 2: For unicast only traffic where the TEK is only to be distributed to a single user transforms IPTV-KM-CF21/22 may be considered as identical to IPTV-KM-CF31/32 (this results in a 3 layer hierarchy as opposed to the 4 layer model).	

Whilst the present document does not mandate any specific implementation of the cryptographic transforms the boundary conditions below may be considered for analysing the candidate implementations. In addition where the use of IPTV in the NGN may require keys or algorithms to be transported across international borders the design of the transforms should take due account of any restrictions on the movement of cryptographic goods and services.

IPTV-KM-CF21: used to compute SSEK from SEK, SEK-id and URK where the transform has the following properties:

- Input 1: Bit string of length |SEK|;
- Input 2: Bit string of length |SEK-id|;
- Input 3: Bit string of length |URK|;
- Output: Bit string of length |SSEK|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output, provided that Input 3 is unknown (even if the details of the algorithms are known).

IPTV-KM-CF22: used to compute SEK from SSEK, SEK-id and URK where the transform has the following properties:

- Input 1: Bit string of length |SSEK|;
- Input 2: Bit string of length |URK|;
- Input 3: Bit string of length |SEK-id|;

- Output 1: Bit string of length |SEK|;
- Output 2: Boolean.

The algorithm should be designed such that it is difficult to find for a fixed Input 2 a value for Input 1 and Input 3 that results in Output 2 assuming the value "FALSE", provided that Input 2 is unknown (even if the details of the algorithms are known). Moreover, it should be difficult to derive (parts of) Input 2 from the observation of various matching values of other inputs and outputs (known plain text attack).

The hierarchy and deployment of the transforms is shown in figure 6.1.

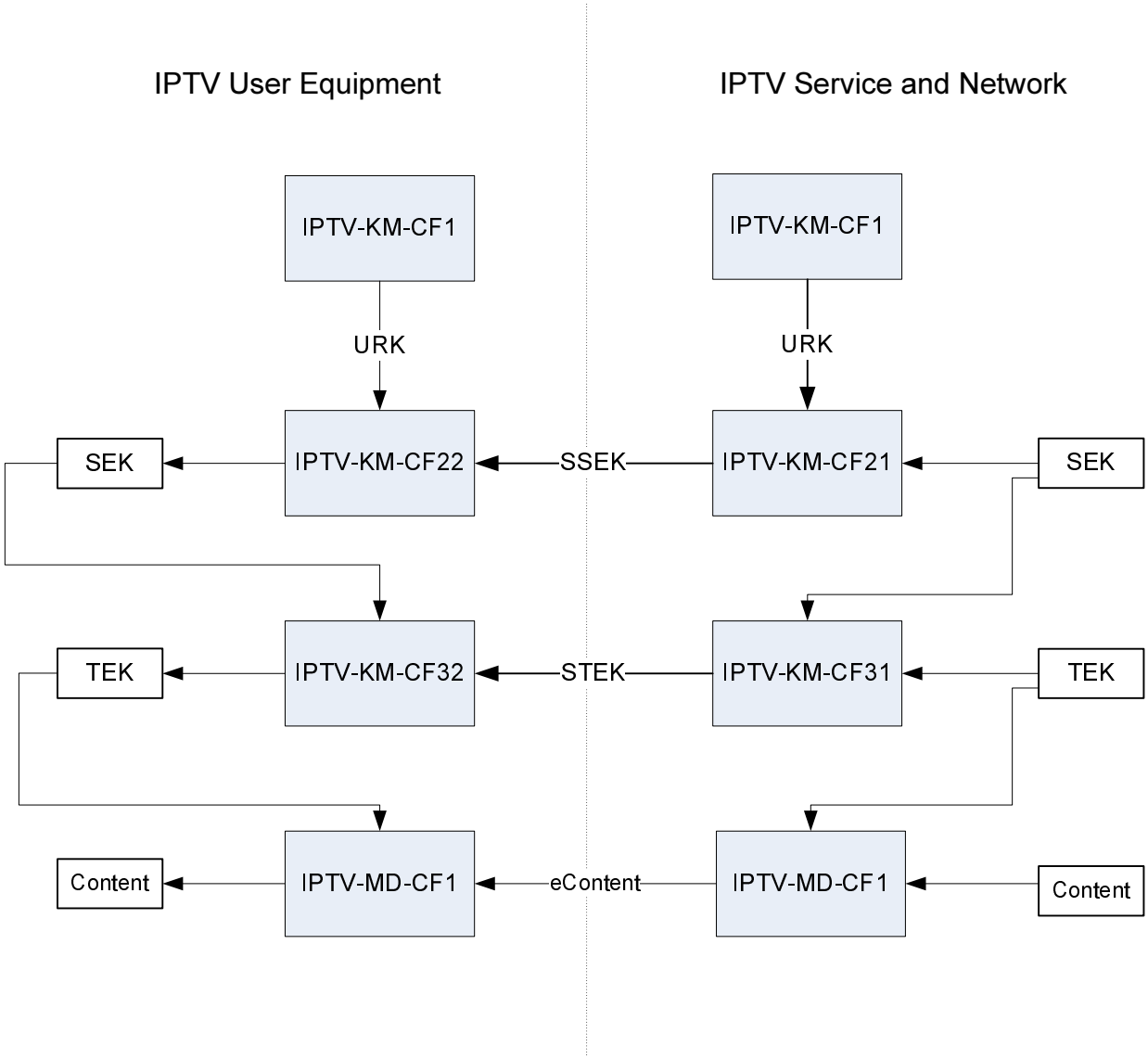


Figure 6.1: Generic IPTV key management and distribution architecture

6.2 Detailed model description

6.2.1 URK generation and delivery

The URK is intended to allow for the protection of delivery of either a group session key (multicast) or a traffic encryption key (unicast). The URK is not intended to be transferred but is to be derived at the UE and in the network.

The URK may be generated at each IPTV service invocation, or may be generated when the user registers to the NGN.

6.2.2 SEK generation and delivery

The SEK is designed to allow multicast delivery of the TEK and is delivered to each IPTV subscriber for a specific IPTV session. The SEK is associated to a specific IPTV subscriber group (see figure 6.2).

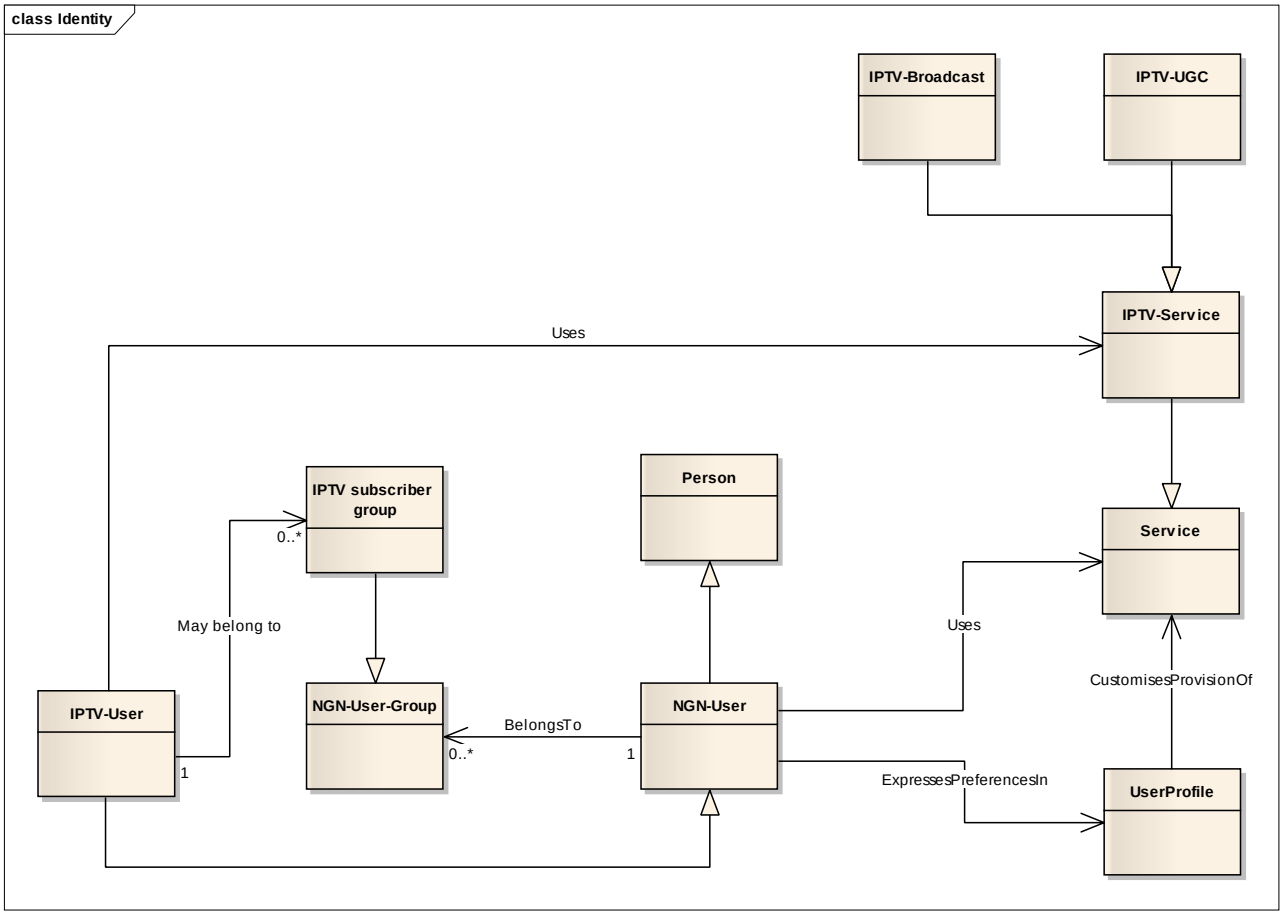


Figure 6.2: IPTV user as member of IPTV subscriber group

The SEK should be pushed from the IPTV service to the UE.

6.2.3 TEK generation and delivery

The TEK is used to give confidentiality protection of the IPTV media stream. The TEK is shared by all receiving IPTV users per programme or per channel.

As there is a risk of an attacker storing the encrypted media and the decryption key (TEK) for distribution via an alternative channel it is recommended to change the TEK periodically in the course of media delivery.

The following information flow is used to inform the receiving IPTV user of the new TEK value and the time at which it will become valid for a particular channel (identified by the iptv:uri defined in TS 184 009 [i.40]) and programme.

IPTV_Generic_TEK_Provide (TEK, [ValidFrom], [ValidTo], [ChannelId], [ProgrammeId], etc.).

NOTE: The convention of [element] indicates the element is optional.

Whilst in normal operation the TEK is pushed to the UE there may be instances where the UE will request the TEK. The following information flow is defined for such cases:

IPTV_Generic_TEK_Request ([IPTV_user_id], [ChannelId], [ProgrammeId]).

It is reasonable to anticipate that there will be misalignment of the "validFrom" and "validTo" information elements and as such it is expected that each UE will retain multiple variants of the TEK as follows:

- **TEK-old:** the version of TEK that the UE believes has been replaced by an updated TEK delivery.
- **TEK-current:** the version of TEK that the UE believes is valid for the current transmission.
- **TEK-future:** the version of TEK that the UE has received in preparation for a later change of active TEK.

7 Candidate Key Hierarchies for Service Protection

7.1 4-Layers Key Hierarchy

The security of multicast IPTV provides different challenges compared to the security of services delivered over point-to-point services. In addition to the normal threat of eavesdropping, there is also the threat that it may not be assumed that valid subscribers have any interest in maintaining the privacy and confidentiality of the communications, and they may therefore conspire to circumvent the security solution (for example one subscriber may publish the decryption keys enabling non-subscribers to view the multicast content). Countering this threat requires the decryption keys to be updated frequently in a manner that may not be predicted by subscribers while making efficient use of the transport network. This may require the use of at least four levels of key hierarchy. The frequency of the update of the lowest level key (e.g. TEKs in figure 7.1) is chosen so that it is not worthwhile to extract and publish the key (i.e. on the Internet) before the next update i.e. this may mean once per second.

Figure 7.1 illustrates the 4-layers key hierarchy for multicast service protection; it consists of the bootstrapping layer, key management layer, key stream layer and the traffic protection layer. The 4-layers key hierarchy can also be used for unicast service protection. Alternatively a 3-layers key hierarchy as described in clause 7.2 can be used.

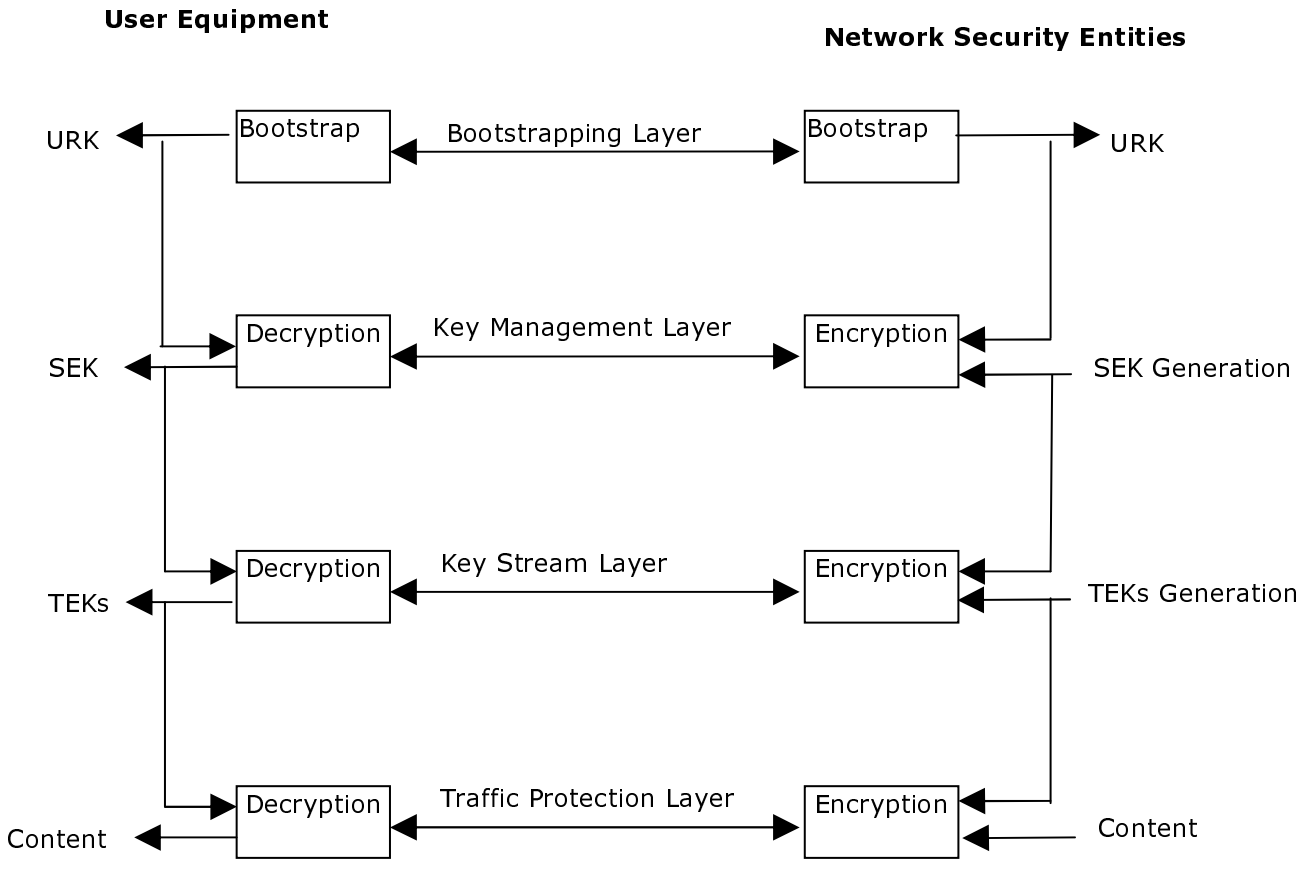


Figure 7.1: 4-Layers IPTV service protection key hierarchy

7.1.1 Bootstrapping Layer

This layer is used to establish the shared User Root Key (URK) between UE and network key management function. The URK is specific to each user, and it is used by Key Management Layer to protect the delivery of Service Encryption Key (SEK).

For UEs which support GBA mechanism defined in TS 133 220 [i.11], the GBA mechanisms should be used to established the URK between Key Management Function and UICC or the UE. If the UICC is capable of handling the GBA_U features defined in TS 133 220 [i.11], the URK should be established between the Key Management Function and the UICC (using GBA-U), and the key Ks_int_NAF should be used as the URK; in case the UICC does not support GBA_U, the URK is established between the Key Management Function and the GBA-capable UE (using GBA-ME), and the key Ks_ NAF should be used as the URK.

7.1.2 Key Management Layer

This layer is used to securely deliver the SEK between key management function and UE by encrypting the SEK with URK.

The SEK is used by Key Stream Layer to protect the delivery of Traffic Encryption Keys (TEKs).

7.1.3 Key Stream Layer

This layer is used to securely deliver TEKs by encrypting the TEKs with SEK.

The TEKs are used by Traffic Protection Layer to encrypt and decrypt the content. TEKs are distributed along with the corresponding content.

7.1.4 Traffic Protection Layer

This layer is used to handle the encryption/decryption of content using TEKs by network security entities and UE.

7.2 3-Layers Key Hierarchy

The 3-layers key hierarchy can be an alternative to the 4-layers key hierarchy in case of unicast IPTV.

The security of unicast IPTV (i.e. CoD) provides different challenges compared to the security of multicast services. The threat of conspiring users circumventing the security solution does not exist. Therefore less complex security solutions can be employed for protecting unicast services than in the multicast service case described in clause 7.1. These considerations lead to three levels of key hierarchy.

Figure 7.2 illustrates the 3-layers key hierarchy for unicast service protection; it consists of the bootstrapping layer, key stream layer and the traffic protection layer. The 3-layers key hierarchy is less complex because it does not require the mechanism of periodical update of decryption keys.

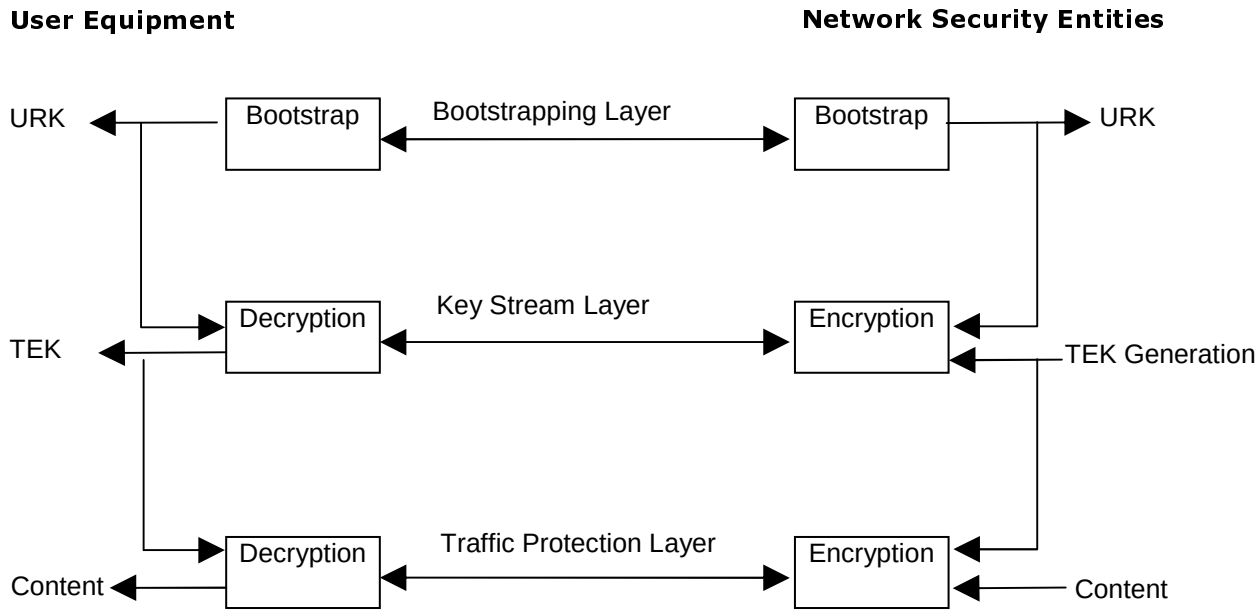


Figure 7.2: 3-Layers IPTV service protection key hierarchy

7.2.1 Bootstrapping Layer

This layer is used to establish the shared User Root Key (URK) between UE and network key management function. The URK is specific to each user, and it is used by the Key Stream Layer to protect the delivery of Traffic Encryption Key (TEK).

For UEs which support GBA mechanism defined in TS 133 220 [i.11], the GBA mechanisms should be used to established the URK between Key Management Function and UICC or the UE. If the UICC is capable of handling the GBA_U features defined in TS 133 220 [i.11], the URK should be established between the Key Management Function and the UICC (using GBA-U), and the key Ks_int_NAF should be used as the URK; in case the UICC does not support GBA_U, the URK is established between the Key Management Function and the GBA-capable UE (using GBA-ME), and the key Ks_ NAF should be used as the URK.

7.2.2 Key Stream Layer

This layer is used to securely deliver TEK by encrypting the TEK with URK.

The TEK is used by the Traffic Protection Layer to encrypt and decrypt the content.

7.2.3 Traffic Protection Layer

This layer is used to handle the encryption/decryption of content using the TEK by network security entities and UE.

8 Candidate Security Models for Service Protection

8.1 Mapping of 4-Layers Key Hierarchy to Security Model

This clause provides service protection model for both multicast and unicast services based on the 4-Layers Key Hierarchy as described in clause 7.1. In order to simplify the model, functional entities that are not tightly related to service protection are not listed in figure 8.1.

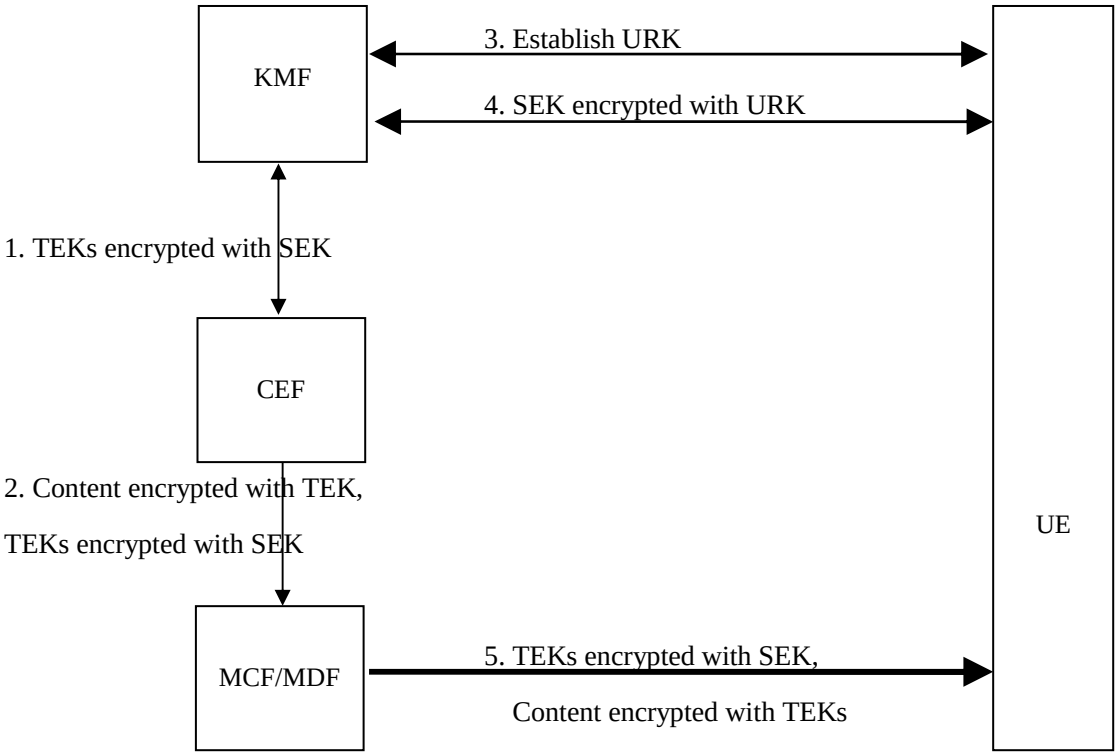


Figure 8.1: IPTV service protection model based on 4-Layers Key Hierarchy

Figure 8.1 illustrates the model for service protection, it contains the following operations:

1) CEF encrypts the content and interacts with KMF to acquire TEKs encrypted with SEK.

2) The CEF transfers the TEKs encrypted with SEK and content encrypted with TEKs to MCF/MDF.

3) UE and KMF execute bootstrapping procedures to establish a shared User Root Key (URK).

4) SEK encrypted with URK is transferred from KMF to UE, then the UE use the URK to decrypt the SEK.

5) TEKs encrypted with SEK and content encrypted with TEKs are delivered from MCF/MDF to UE.

   For multicast service protection, the TEKs may be frequently updated, e.g. once per second. This will make it expensive or infeasible for the user to disclose the TEKs enabling non-subscribers user to view the content.

6) UE decrypts the TEKs using the SEK, and decrypts the content using the TEKs.

8.2 Mapping of 3-Layers Key Hierarchy to Security Model

This clause provides service protection model based on the 3-Layers Key Hierarchy as described in clause 7.2. In order to simplify the model, functional entities that are not tightly related to service protection are not listed in figure 8.2.

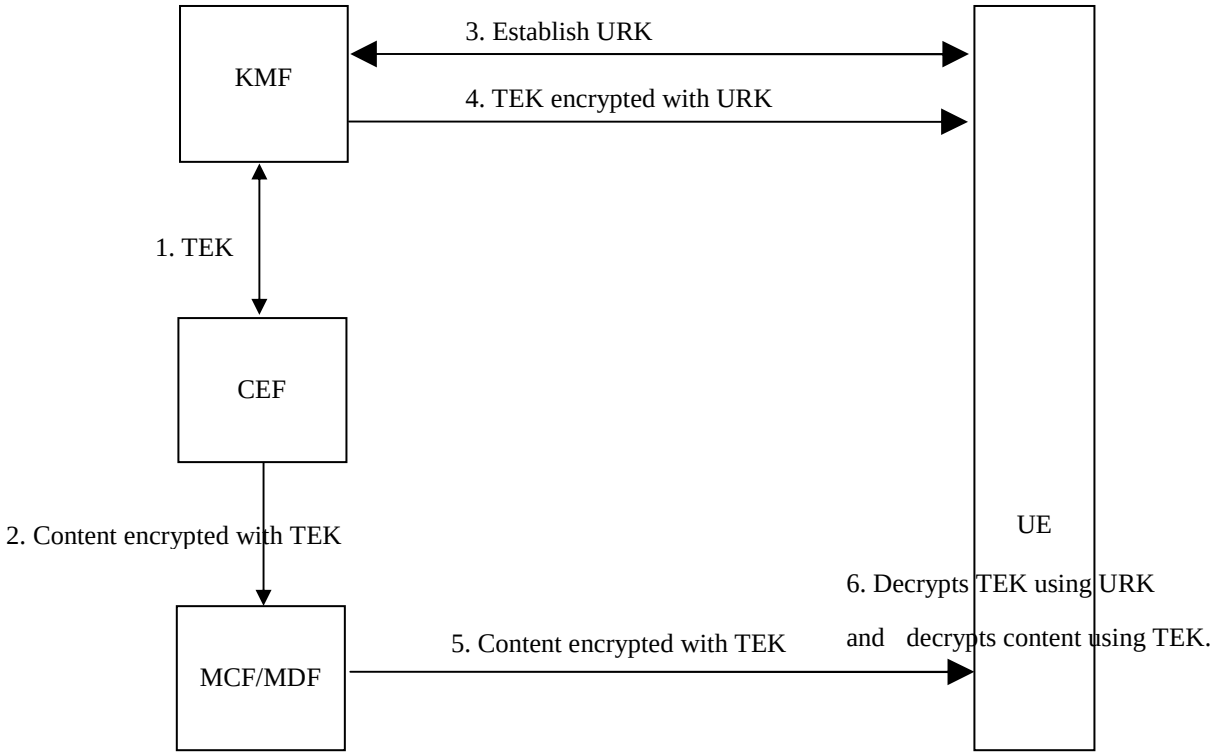


Figure 8.2: IPTV service protection model based on 3-Layers Key Hierarchy

Figure 8.2 illustrates the model for service protection, it contains the following operations:

1) The CEF transfers the TEK to KMF.
2) The CEF transfers the Content encrypted with TEK to MCF/MDF.
3) The UE and the KMF execute bootstrapping procedures to establish a shared User Root Key (URK).
4) The TEK encrypted with URK is transferred from the KMF to UE.
5) The content encrypted with TEK is delivered from the MCF/MDF to the UE.
6) The UE decrypts the TEK using the URK, and decrypts the content using the TEK.

9 Candidate Solutions for Service Protection

9.1 Service Protection Solution One

The service protection solution one is based on the 4-layer key hierarchies and the corresponding service protection model.

9.1.1 Functional Architecture Overview

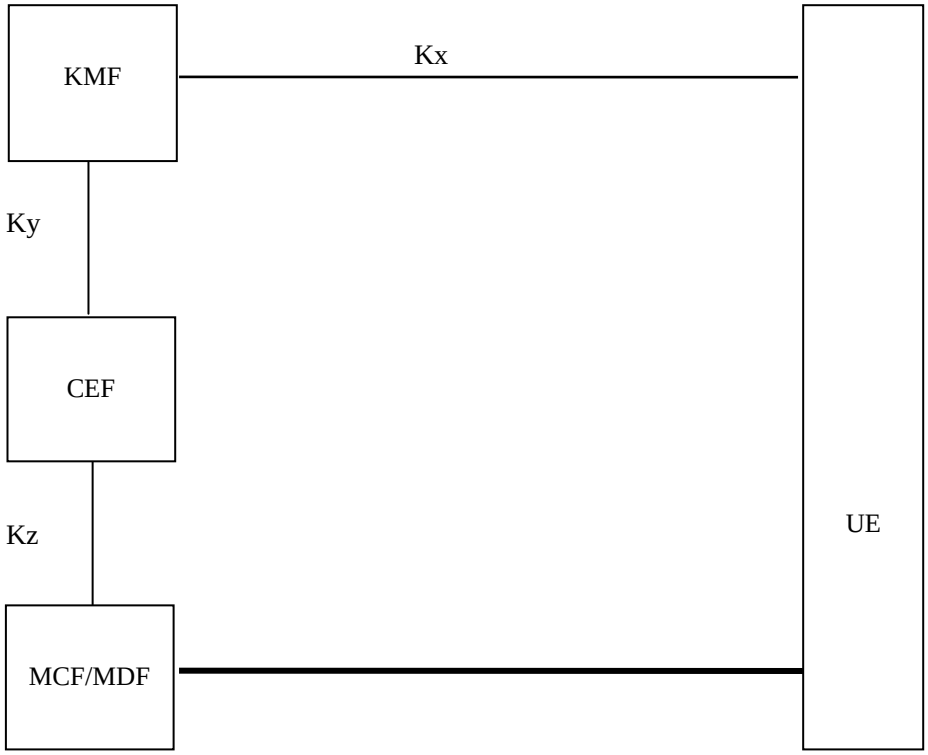


Figure 9.1: Functional architecture for service protection

The service protection architecture illustrated above is based on the IPTV service architecture defined in TS 182 027 [i.5] and TS 182 028 [i.6].

9.1.2 Reference Points

9.1.2.1 KMF - UE (Kx)

This reference point between KMF and UE is used for the delivery of SEK to UE.

9.1.2.2 KMF - CEF (Ky)

This reference point between KMF and CEF is used for the delivery of SEK to CEF.

9.1.2.3 CEF - MDF (Kz)

This reference point between CEF and MDF is used for the transmission of the encrypted content and the encrypted TEKs to MF.

NOTE 1: In case the CEF is co-loated with MDF, this interface is not required.

NOTE 2: Whether the controlling interface between CEF to MCF is required is FFS.

9.1.3 Solution Description

The service protection procedures comprise 2 major steps:

- Service protection deployment steps, the procedures are used to encrypt the content and deliver it to MCF/MDF.
- Key providing steps, the procedures are used to provide keys to each user.

9.1.3.1 Procedures for service protection deployment

Figure 9.2 depicts the typical procedures for security deployment.

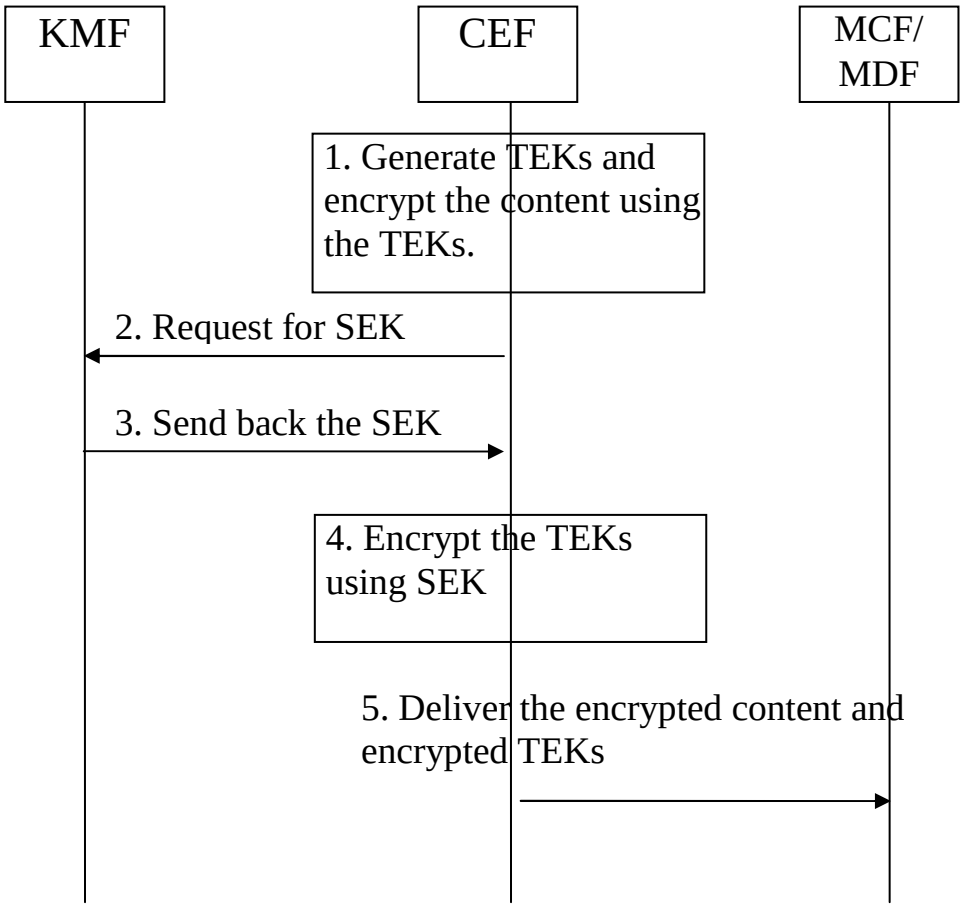


Figure 9.2: Procedures for security deployment

1) CEF generates TEKs and encrypts the content using the TEKs.
2) CEF initiates a request to KMF to request for the corresponding SEK, which includes the content ID or service ID.
3) KMF generates the SEK corresponding to the content ID or service ID, and then sends the SEK back to CEF.
4) The CEF encrypts the TEKs using the SEK.
5) The CEF then delivers the encrypted content and the encrypted TEKs to MCF/MDF.

Then MCF/MDF delivers the content and the encrypted TEKs to the desired UEs for the corresponding service.

9.1.3.2 Procedures for key providing

Figure 9.3 depicts the typical steps for key providing.

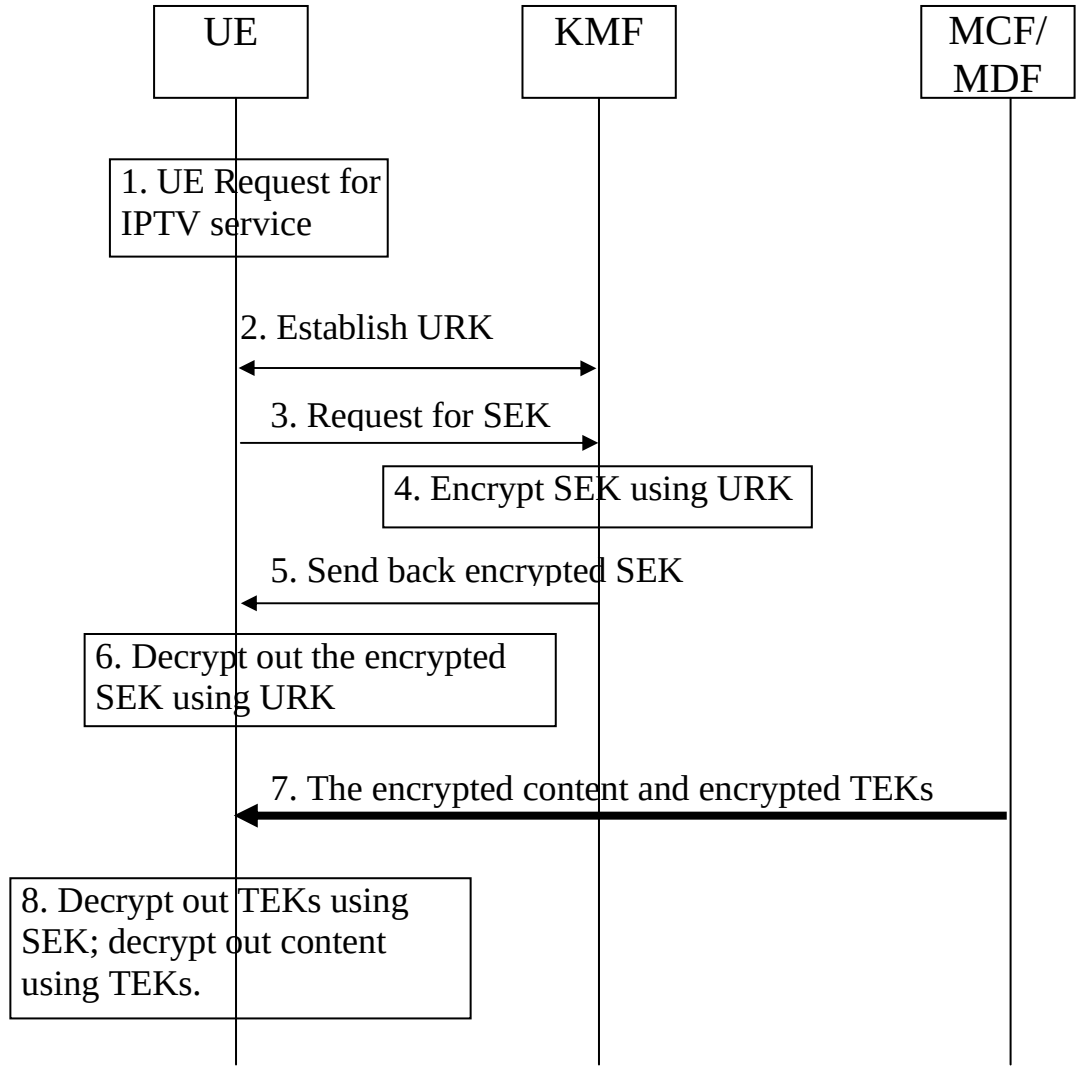


Figure 9.3: Procedures for key providing

1) The UE request for an IPTV service e.g. BC service, which uses service protection.

2) UE establishes the shared URK with KMF, e.g. using GBA mechanism.

3) UE initiates a request to KMF to get the corresponding SEK, which carries the content ID or service ID.

4) KMF retrieves the SEK corresponding to the content ID or service ID, and then encrypts the SEK using the URK.

5) KMF sends back the SEK to UE.

6) UE decrypts out the encrypted SEK using the URK.

7) UE receives the encrypted content and the encrypted TEKs.

8) UE decrypts out the TEKs using the SEK, and then decrypts the content using the TEKs.

Then the user can consume the content, and other users who are not authorized to the service are unable to decrypt out the content.

9.2 OMA BCAST 1.0 as candidate solution

IPTV service protection using a 4-layer model addresses both unicast and multicast.

OMA BCAST 1.0 service protection, as specified in [i.8], is a 4-layer model allowing two key management profiles: the Smartcard Profile and the DRM Profile. OMA BCAST 1.0 interoperability has been validated through successful testfests.

The SmartCard Profile (SCP) is a key management system based on symmetric key model. It uses either 3GPP MBMS security model relying on the (U)SIM on UICC or 3GPP BCMCS security model relying on R-UIM/CSIM.

The DRM Profile is key management system based on the Public Key Infrastructure provided by OMA DRM v2.0.

In order to ensure maximum interoperability, OMA BCAST1.0 defines a common layer for traffic encryption and allows the other layers of key management to be implemented using either the SmartCard Profile or the DRM Profile.

An OMA BCAST Terminal MAY implement Service Protection and MAY implement Content Protection, as shown in table 9.1.

Table 9.1: Service Protection and Content Protection in OMA BCAST Terminals

	BCAST Terminal
Service Protection	OPTIONAL
Content Protection	OPTIONAL

Table 9.2 summarizes the possible scenarios which are focused on mobile terminals only.

Table 9.2

	OMA BCAST Profile		
Non-Cellular or cellular terminals with or without Smartcard	DRM	SCP	Type of Protection
Non-Cellular Terminal WITHOUT SC	MANDATORY	N/A	SP
Non-Cellular Terminal WITH SC	MANDATORY	N/A	SP
Cellular Terminal WITHOUT SC	MANDATORY	N/A	SP
Cellular Terminal WITH SC	OPTIONAL	MANDATORY	SP
Non-Cellular Terminal WITHOUT SC	MANDATORY	N/A	CP
Non-Cellular Terminal WITH SC	MANDATORY	N/A	CP
Cellular Terminal WITHOUT SC	MANDATORY	N/A	CP
Cellular Terminal WITH SC	OPTIONAL	OPTIONAL	CP

NOTE: This consideration has to be widened to address TISPAN [fixed] terminal purposes.

Mobile device is normally linked to one specific user. On the other side, fixed devices like Set Top Boxes or Media PCs are considered being more shared devices, since used by potentially all members of the whole household and over more friends visiting that household. It depends therefore on the use-case, which profile (SCP or DRM) is the better choice for the IPTV protection.

9.2.1 OMA BCAST Functional Architecture and TISPAN IPTV

This clause gives an overview of OMA BCAST functional architecture and provide a mapping between OMA BCAST and TISPAN IPTV logical entities.

- BCAST Functional Architecture Overview.

Figure 9.4 is extracted from Mobile Broadcast Services Architecture document [i.42].

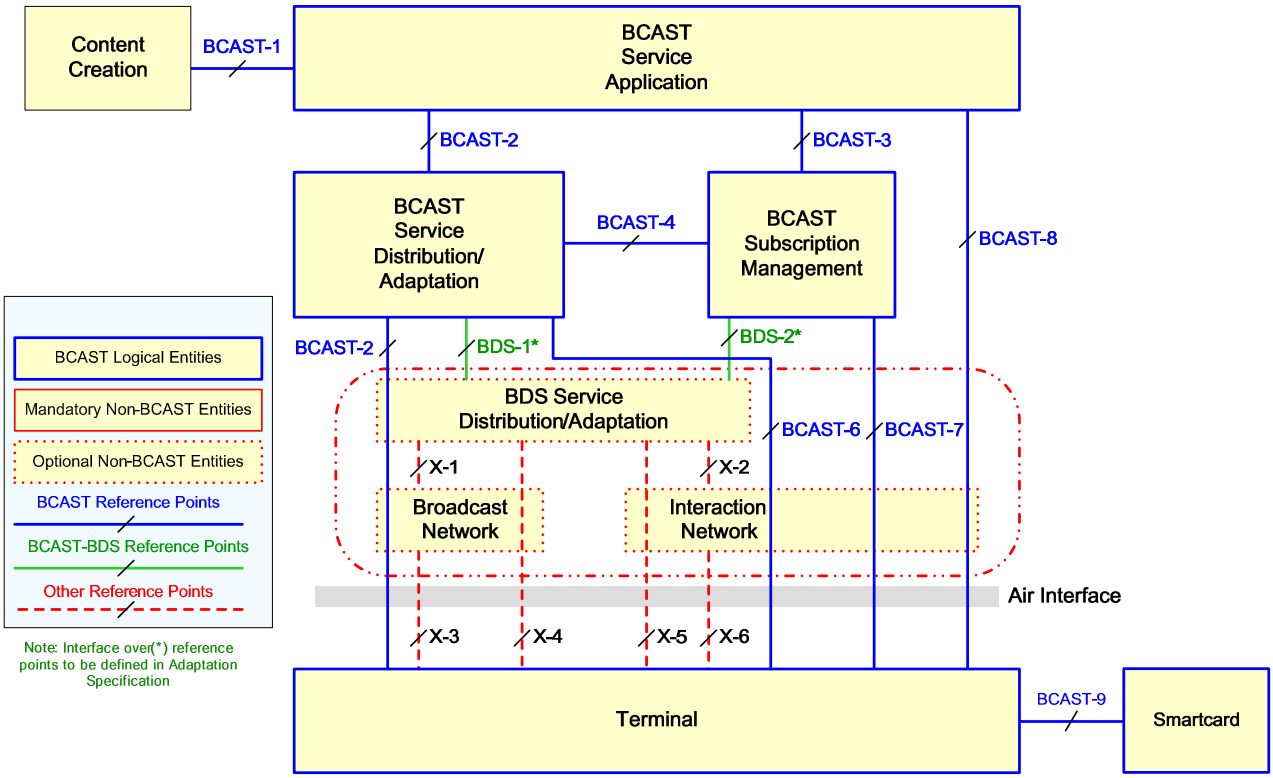


Figure 9.4: BCAST Functional Architecture Diagram

Table 9.3: Descriptions of Logical Entities

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 BCAST 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.

- Mapping between TISPAN IPTV and OMA BCAST logical entities.

The mapping results from the comparison between IPTV architecture and OMA BCAST Service Protection Functional Architecture described in figure 9.4.

Table 9.4: Mapping between TISPAN IPTV and OMA BCAST logical entities

IPTV entities			BCAST entities		
High level entity	**Name**	**Function**	**High level entity**	**Name**	**Function**
Application and IPTV service functions	SDF	Generates and provides service attachment information; provides personalized service discovery	BSD/A	SG (access fragment, SDP)	This fragments are used by the terminal to retrieve the content and associated streams in the broadcast or unicast network. Typically the SDP contains multicast address to retrieve the content.
Application and IPTV service functions	SSF	Provides the service selection information; provides service selection presentation information	BSD/A	SG (service, content, schedule fragments, purchase fragments… displayed to user)	These fragments are used for the selection by the user of content. Information in these fragments are displayed to the user.
Application and IPTV service functions	SCF	Service authorisation; Credit limit and credit control.	BSM	SP-M for service protection function	Service Protection Management Component (SP-M) in the BSM is responsible for the registration of Terminal and the authentication/authorization of User; Generation of Key messages.
Media Delivery, distribution and storage	MCF		BSD/A	FD and FA	
Media Delivery, distribution and storage	MDF	Handling media flows delivery; May additionally process, encode or transcode (if required) media to different required media formats (e.g. TV resolution depending on terminals capabilities or user preferences); May perform content protection functionalities (e.g. content encryption).	BSD/A	FD and FA	The File Delivery Component (FD) in the network is responsible for the delivery, aggregation, and adaptation of a file or a bundle of files; 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. 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 and additional information; If the content protection is done by BCAST, the FA may cooperate with the Content Protection function to encrypt the file.
Application and IPTV service functions	UPSF	The UPSF holds the IMS user profile and possibly IPTV specific profile data	BSM	Equivalent to HSS for Smartcard profile	
Transport functions	Transport control function			BDS Service Distribution/Adaptation; Broadcast Network; Interaction Network	
Transport functions	Transport processing function			BDS Service Distribution/ Adaptation; Broadcast Network; Interaction Network	

Figure 9.5 shows the mapping of logical entities within architecture overview.

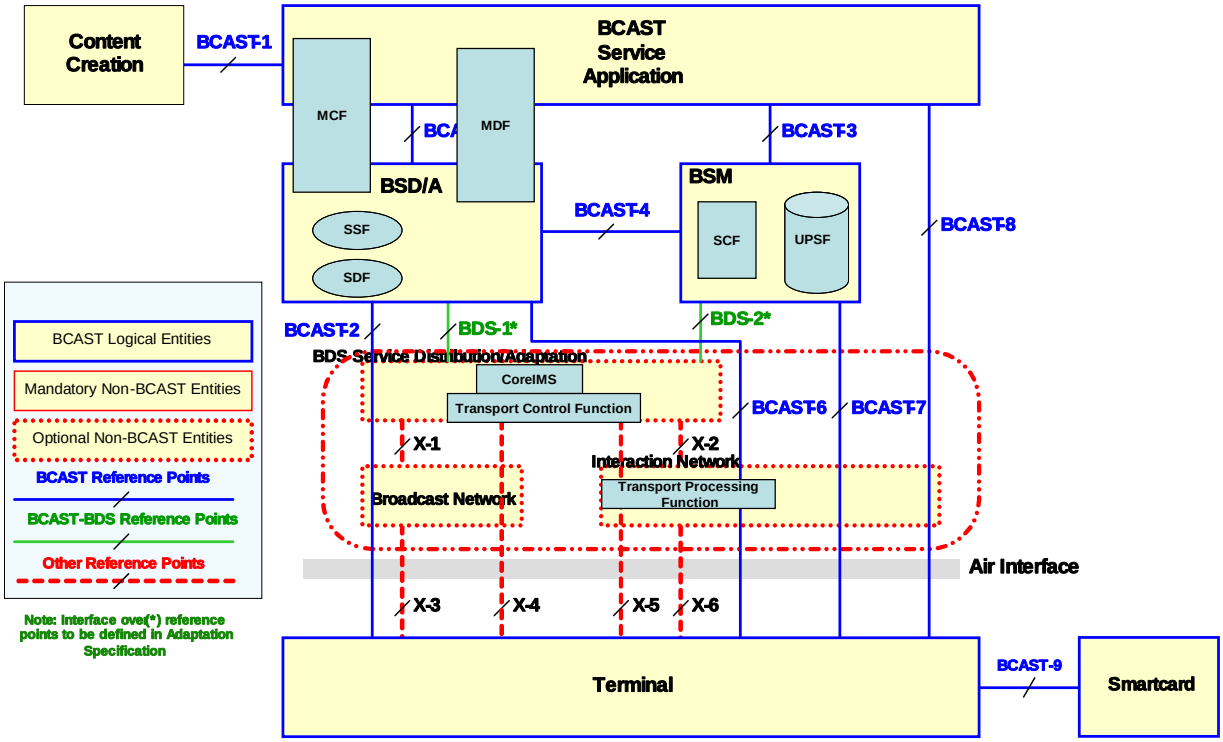


Figure 9.5: Mapping between IPTV and OMA BCAST logical entities within architecture overview

- OMA BCAST mechanisms addressed in TS 183 063 [i.7].

Some OMA BCAST mechanisms are already addressed by TS 183 063 [i.7]. Clauses of TS 183 063 [i.7] related to OMA BCAST are the following:

- Clause 6.3.1.5: procedure for retrieving OMB BCAST service selection.
- Clause 10: procedure using FLUTE for IMS-based IPTV, where the clause applies when using OMA BCAST multicast delivery for service provider and guide discover.
- Clause J.2: Integration of non SIP AS service discovery function based on OMA BCAST ESG.
- Clause L.1.2: Mapping of OMA BCAST ESG delivery descriptors to XML schema for service attachment.

9.2.2 OMA BCAST Service and Content Protection

- OMA BCAST Service Protection / Content Protection.

OMA BCAST specifies both Service Protection and Content Protection systems to address various business models. Broadcast content could be protected by means of OMA BCAST Service Protection **and/or** Content Protection. OMA BCAST may be used to provide Service Protection only. In the absence of any subsequent Content Protection, the content is freely available once it is securely delivered.

OMA BCAST defined for the Smartcard Profile new MIKEY EXTension payload that may be included in LTKM or STKM. This payload is referred as "EXT BCAST for LTKM" or "EXT BCAST for STKM", and is used to transport additional information governing the use of keys carried within LTKM or STKM.

EXT BCAST payload contains Management data, one of the fields corresponds to the "security_policy_extension" (SPE) associated to the key, e.g. the key SEK for LTKM or the key TEK for STKM. OMA BCAST describes the semantics of the different SPE values for LTKM and STKM. A SPE value is specific for Service Protection **OR** Content Protection.

Remark: in OMA BCAST, the term "LIVE" refers to Service Protection, and the term "PLAYBACK" refers to Content Protection.

EXT BCAST payload is described in Service and Content Protection for Mobile Broadcast Services specification [i.8], clause 6.6.4.2:

- BCAST Service Protection Functional Architecture Overview is described in OMA Mobile Broadcast Service Architecture specification [i.14].
- Mapping between TISPAN IPTV and OMA BCAST Smartcard Profile key management entities.

The mapping results from the comparison between IPTV service protection model based on 4-Layers Key Hierarchy described in clause 8.1 and OMA BCAST Service Protection Functional Architecture described in figure 9.5.

Table 9.5: Mapping between TISPAN IPTV and OMA BCAST Smartcard Profile Service Protection entities

IPTV entities			BCAST entities		
High level entity	**Name**	**Function**	**High level entity**	**Name**	**Function**
	KMF	KMF execute bootstrapping procedures to establish a shared User Root Key; encrypted with URK is transferred from KMF to UE	BSM	SP-M	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 Smartcard.
	CEF	CEF encrypts the content and interacts with KMF to acquire TEKs encrypted with SEK; CEF transfers the TEKs encrypted with SEK and content encrypted with TEKs to MCF/MDF; TEKs encrypted with SEK and content encrypted with TEKs are delivered from MCF/MDF	BSD/A	SP-Encryption; SP Key distribution	• 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 Service Protection Key Distribution Component (SP-KD) in the BSD/A is responsible for the distribution over the broadcast channel of the STKM, generation of TEK and the optional generation of STKM.
	MCF/MDF		BSD/A		
Transport functions	Transport control function			BDS Service Distribution/Adaptation; Broadcast Network; Interaction Network	
Transport functions	Transport processing function			BDS Service Distribution/Adaptation; Broadcast Network; Interaction Network	

- OMA BCAST Smartcard Profile advantages compared to MBMS

OMA BCAST Smartcard Profile relies on MBMS and also contains additional features that could be useful for TISPAN IPTV Service Protection.

- OMA BCAST supports MBMS

  OMA BCAST Smartcard Profile relies on MBMS and also contains additional features. OMA BCAST Smartcard Profile supports MBMS.

- DVB Simulcrypt support

BCAST Subscription Management that support service or content protection supports Interface SP-4. Interface SP-4 may support DVB Simulcryt. The description of DVB Simultcrypt support is described in clause 13.1 of Service and Content Protection for Mobile Broadcast Services specification [i.8].

- ISIM and IMPI

  OMA BCAST Smartcard Profile relies on GBA with USIM application or ISIM application on UICC while MBMS relies only on GBA with USIM application on UICC.

  TISPAN IMS AKA relies on ISIM on UICC

  The private user identity, the IMPI, used in MBMS is derived from the IMSI of the USIM application. With OMA BCAST, the user identity, the IMPI, would correspond to the IMPI of the IMS subscription, i.e. the IMPI of the ISIM on UICC.

- Parental Control/ Pay Per View / Pay Per Time

  Parental Control and Pay Per Time are services supported by TISPAN IMS based IPTV subsystems. Pay Per View signalling flows and Parental Control procedure are described in TS 182 027 [i.5] "IPTV functions supported by the IMS subsystem". The support of Parental Control service is mandated by TS 181 016 [i.3] "NGN Services and IPTV" for TISPAN R2 and R3. Pay Per View is mandated by TS 181 016 [i.3] for TISPAN R3.

  Parental Control, Pay Per View and Pay Per Time services are addressed by OMA BCAST Smartcard Profile while they are not addressed by MBMS.

- Video on Demand and Content on Demand

  Video on Demand and Content on Demand are covered by OMA BCAST while they are not addressed by MBMS.

- Key Validity Data

  The Key Validity Data for the Service Encryption Key and Program Encryption Key is coded on 32 bits within OMA BCAST Smartcard Profile (maximum key lifetime is 132 days) while the Key Validity Data is coded on 16 bits in MBMS (maximum key lifetime is 7 days).

- Service Guide

  Service guide is a features proposed by OMA BCAST Smartcard Profile that does not exist in MBMS.

  TS 183 063 [i.7] "IMS-based IPTV stage 3 specification" contains clause on "Procedures using Flute for IMS-based IPTV" (clause 10). This clause applies when using OMA BCAST multicast delivery for service provider and guide discovery.

- TS increment

  In MBMS for each STKM sent the TS field is increased, even if this STKM carries the same TEK as the previous STKM message. For OMA BCAST BCAST Smartcard Profile the server may resend the same STKM, containing the same TEK, without increasing the TS field. This avoids the need for generating new STKMs within the same crypto period. This is an improvement to the MBMS since BSM handling needs less processing for building subsequent authenticated STKM with the same key material included.

- Secure Channel

  The OMA BCAST Smartcard Profile defines the possibility to use a secure channel. The secure channel performs mutual authentication between the smartcard and the terminal, and protects the exchanges between the Smartcard and the Terminal. The keys decrypted by the Smartcard are sent to the terminal protected in integrity and confidentiality.

  MBMS does not describe possible usage of secure channel.

- Choice of the encryption level

  In OMA BCAST, there is the choice of the level of encryption, IPSEC, SRTP, ISMACryp. For MBMS, SRTP is the only level of encryption that is used to protect the content.

  For IPSEC the encryption is made at the lower level in the IP stack, at IP level. The encryption is removed at the IP level of the stack and the content is transmitted in clear from the IP level to the application level through the stack, passing through a lot of software layers for which secure execution depends on implementation.

  For SRTP, the encryption is made at the transport level RTP of the stack. The encryption is removed in the IP stack and the content is transmitted in clear to the application level, passing through some software layer.

  For ISMACryp, the encryption is made at the application level. The content is transmitted from the stack to the application in encrypted form and the encryption is removed in the application itself. This allows the use of non-secure IP stack. This allows also a decryption either in software or in hardware in a dedicated chipset used for video decompression. This latter implementation increases significantly the security level within the terminal.

- Conclusion on usage of OMA BCAST Smartcard Profile for TISPAN IPTV Service Protection.

Some OMA BCAST mechanisms are already addressed by TS 183 063 [i.7] as described in clause 9.2.1 of the present document.

TISPAN could also adopt OMA BCAST Smartcard Profile Service Protection and associated Key Management to perform TISPAN IPTV Service Protection.

9.2.2A OMA BCAST Smart Card Profile adaptation to MPEG-2 TS

In OMA BCAST, content streams are sent in UDP/RTP packets and may be encrypted at different layers:

- IP layer using IPSEC;
- RTP layer using SRTP; or
- at applicative layer using ISMACrypt.

In TISPAN IPTV:

- When the RTP transport is used for the transport of the content, one of the encryption protocol defined in OMA BCAST can be used and the STKM can be transported over UDP/RTP as defined in OMA BCAST.
- When the content is transported in MPEG2 TS encapsulated in UDP/RTP the STKM may be transported in the MPEG2 TS and the following adaptation of OMA BCAST Smartcard profile applies.

STKM Transport in MPEG-2 TS

In OMA BCAST, the audio and video streams are transported in RTP multicast packets on the IP stack integrated in the broadcast bearer. This bearer depends on the technology used. For example, in case of DVB-H, the IP stack is transported in the MPEG2 TS of the DVB-H bearer.

In case of TISPAN IPTV, audio and video streams may be transported in MPEG2 TS on the IP network.

To guarantee the synchronization of the delivery of keys used to encrypt the content and the encrypted content itself, an adaptation of STKM message to the MPEG2 TS is defined in this section. This is especially important when the Quality of Service is not guarantee as for unmanaged networks.

OMA BCAST has defined short term key messages (STKM) to vehicle the content key (TEK) on MIKEY messages from the server to the terminal or the Smartcard using RTP protocol in multicast mode.

In the context of systems where the services are transported in a MPEG2 Transport stream (TS), messages dedicated to the conditional access system like the ECM are transported in the MPEG2 TS in specific packets identified by the CA_PID.

The PID of the ECM packet associated to a program is retrieved in the PMT of this program in the CA-descriptor (Descriptor-tag = 0x09).

In case of OMA BCAST SCP, the following adaptation is defined to permit the broadcast of TEK in the MPEG2 TS in ECM defined by DVB.

Signalling of ECM in PMT for OMA BCAST SCP:

- the CA-descriptor retrieved in the PMT contains the following data for OMA BCAST SCP;
- the CA-system-ID associated to OMA BCAST SCP (OMA BCAST 1.0 (U)SIM Smartcard Profile using 3GPP GBA_U) and defined by DVB (http://www.dvbservices.com/identifiers/ca_system_id);
- and the CA-PID associated to the ECM.

The STKM can be transported in the associated CA-PID in private section.

Integration of ECM in private section of the CA packet:

- ECMs are integrated in PES packets with the stream-id set to "1111 0000".

These PES packets are encoded as private section as defined in MPEG2 TS specification 13818-1 [i.25].

The table_id for the ECM is given in ETR 289 [i.43] and can be 0x80 or 0x81 the last bit is the toggle bit indicating that the section has been changed.

To ensure that TEK are present when the corresponding encrypted content is broadcasted, the TEK will be broadcasted in advance during the previous crypto period. When the user zaps to a new channel, to ensure that the Smartcard is able to compute the TEK without waiting for the next crypto period, the ECM containing the current TEK will be broadcasted during the crypto period corresponding of its use in the encrypted content. The ECM will then contain the current and the next TEK during a crypto period.

The MIKEY message defined in OMA BCAST SCP is integrated in the CA_data_bytes defined in ETR 289 [i.43] as follows:

Table 9.6: CA_message_section

Syntax	No. of bits	Identifier
CA_message_section() {		
table_id	8	uimsbf
section_syntax_indicator	1	bslbf
DVB_reserved	1	bslbf
ISO_reserved	2	bslbf
CA_section_length	12	uimsbf
for(i=0; I<N; i++) {		
CA_data_byte	8	bslbf
}		
}		

All the fields except CA_data_bytes are defined in ETR 289 [i.43]. CA_data_bytes contain the MIKEY message defined in OMA BCAST specification for the STKM of the Smartcard profile for the TEK_n and the TEK_{n+1}.

Table 9.7: CA_data_bytes for TEK_n and the TEK_{n+1}

Common HDR (TEK_n)
EXT MBMS (TEK_n)
EXT BCAST (TEK_n)
TS (TEK_n)
KEMAC (TEK_n)
Common HDR (TEK_{n+1})
EXT MBMS (TEK_{n+1})
EXT BCAST(TEK_{n+1})
TS (TEK_{n+1})
KEMAC (TEK_{n+1})

The payloads depicted in table 9.7 are defined in OMA-TS-BCAST_SvcCntProtection [i.8].

The terminal filters the ECM using the toggle bit and send the corresponding STKMs to the smartcard when the toggle bit has changed or when the user zaps to another channel.

The terminal sends the STKMs contained in the ECM separately using the AUTHENTICATE Command as defined in OMA BCAST specification.

The terminal sends the STKM corresponding to the TEK_n only once to avoid a replay detection error in the Smartcard.

The STKM corresponding to the TEK_n could be sent before the STKM corresponding to the TEK_{n+1} to avoid a playback processing in the Smartcard.

This adaptation minimizes the impact on the standard OMA BCAST terminal and Smartcard.

Example of ECM processing

Figure 9.5A shows which STKM are transmitted to the Smartcard by the terminal with an example.

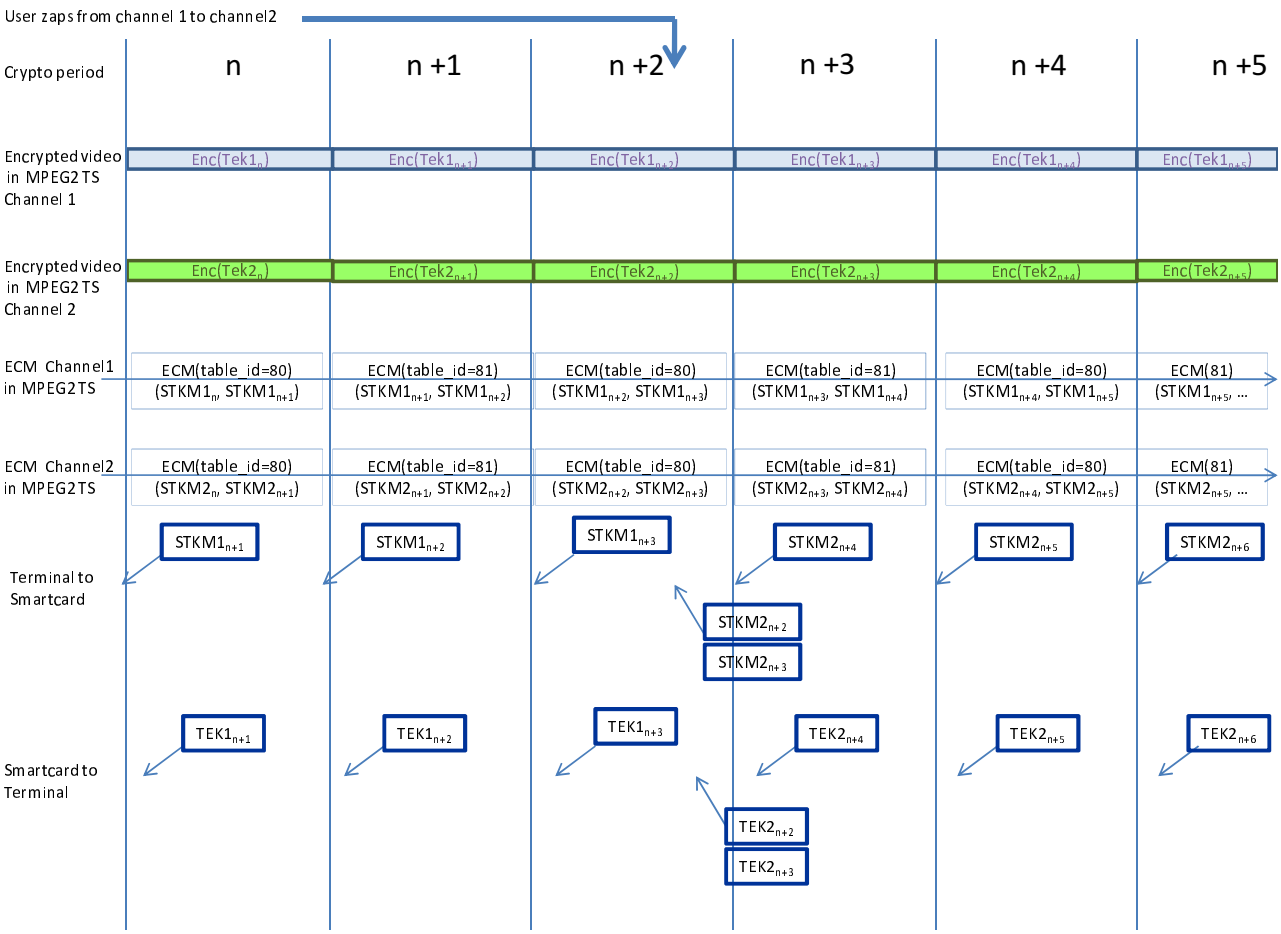


Figure 9.5A: Example of ECM Processing

STKM and MPEG-2 TS encryption

In case the content is transported in MPEG2 TS, the encryption algorithm used is defined by the Scrambling Descriptor of the program signalled in the PMT. The possible values for this scrambling descriptor are defined in the DVB bluebook A125 [i.44].

The key used for the encryption is signalled in the TS header in the transport_scrambling_control field if the TS payload is scrambled at TS level, or in the PES header in the PES_scrambling_control field if the TS payload is scrambled at PES level.

Two keys may be used, the odd key or the even key.

In the STKM of the OMA BCAST Smartcard profile , a TEK_ID in the EXT-MBMS extension is used to identified the content key.

When the TEK_ID has an even value, the key transported in the KEMAC corresponds to the even key, and when the TEK_ID has an odd value, the key transported in the KEMAC corresponds to the odd key.

An odd key returned by the smartcard will replace the previous odd key stored in the terminal, and the even key returned by the smartcard will replace the previous even key stored in the terminal. Only two keys, an even and odd keys are present in the terminal and used to decrypt the content.

9.2.3 OMA BCAST DRM-Profile as a candidate solution

OMA BCAST DRM-Profile can be used with TISPAN IMS-based IPTV as well as with NGN-integrated IPTV.

9.2.3.1 Functional Architecture Overview

For IPTV with OMA BCAST DRM-Profile service protection but also content protection can be realized.

OMA BCAST DRM-Profile is based on the 4-layer Key Management Model. Keys (TEKs) are applied to the actual content (Layer 4) following different mechanisms depending on the actual encryption method used. For the DRM Profile, within the STKM (Short Term Key Messages), the TEK is encrypted with a PEK (Program Encryption Key), and the PEK is also carried in the STKM, encrypted with the SEK. STKMs contain extension of content IDs for the program or service. Devices use this ID to identify which Long Term Key Message (LTKM) contains the necessary keys to use for decryption of Short Term Key messages. The Rights Encryption Key (REK) is used to protect the LTKM delivery. REK and meta-data are delivered as a result of the registration phase.

NOTE: Long Term Key messages (LTKMs) are stored within the secure storage entity, and are never exposed outside of the secure storage.

Encryption is carried out using the AES algorithm with 128 Bit symmetric keys (TEKs). TEKs may be a part of IPSec SAs, Master Key at SRTP or Access Units (AUs) at ISMACrypt.

Transmission of LTKMs can be done in two different ways:

- via broadcast over OMA BCAST broadcast channel; or
- via an interactivity channel.

When delivering ROs to devices that have access to an interactive channel such devices use standard OMA DRM 2.0 mechanisms and acquire ROs for broadcast content via the interactive channel using the DRM 2.0 ROAP protocol.

When delivering Ro to devices over the broadcast channel a method is described for securely delivering BCROs (Broadcast Rights Objects) to groups of devices at the same time. Valuable portions of ROs are protected by group or unit keys, and when necessary, broadcast encryption can be used to allow messages to be decrypted only by arbitrary sets of devices within a larger group.

OMA BCAST DRM Profile uses OMA DRMv2.0 for the registrations and rights management over the interactive channel and specifies a set of protocols for use in broadcast and out-of-band channels.

The OMA DRM Profile uses PKI-based mechanism. The device stores private/public key pair, the public key is certified by a certificate authority. At registration the Rights Issuer proofs the certificates validity and after successful check generated REK, protects it with UEs Public Key and sends it so to the UE.

The registration protocol is based on ROAP (Rights Object Acquisition Protocol). ROAP is based on XML basics.

The ROAP supports the 4-pass registration protocol (used for the registration), 2-pass Rights Object Acquisition Protocol (to pull the rights objects) and 1-pass Rights Object Acquisition Protocol (to push the rights objects).

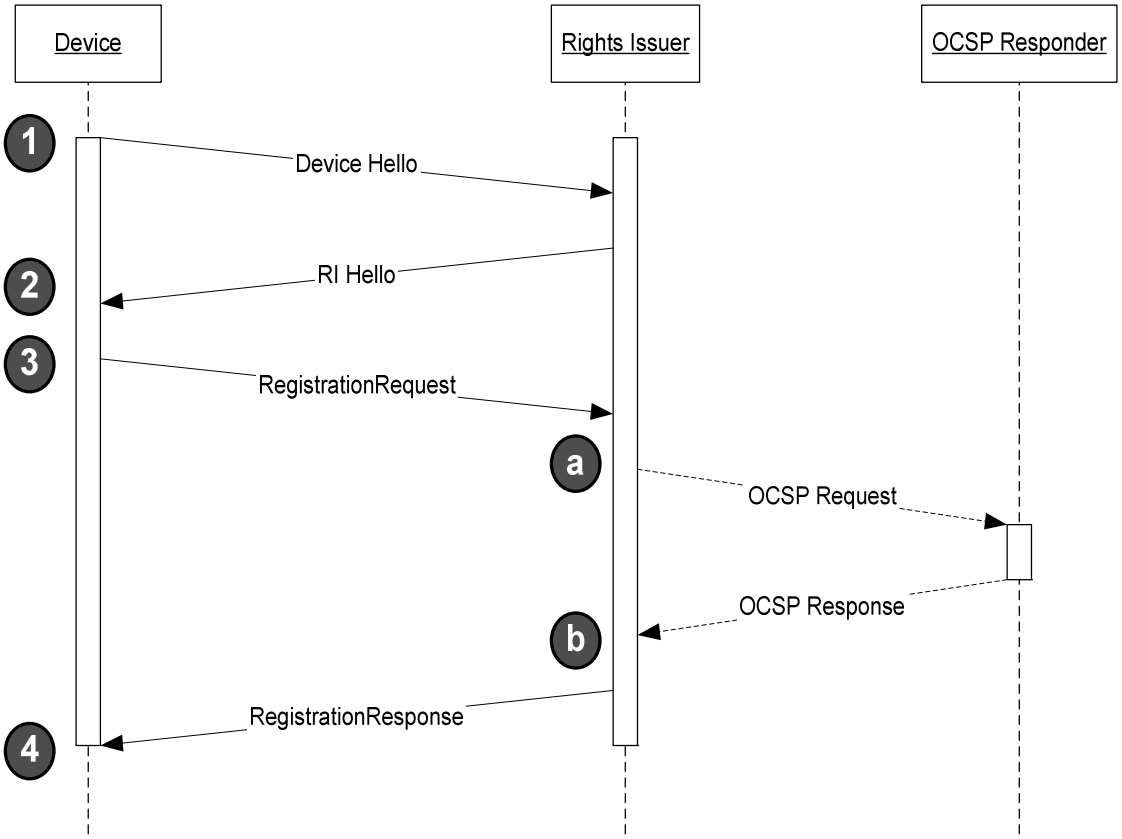


Figure 9.6: 4-pass registration protocol

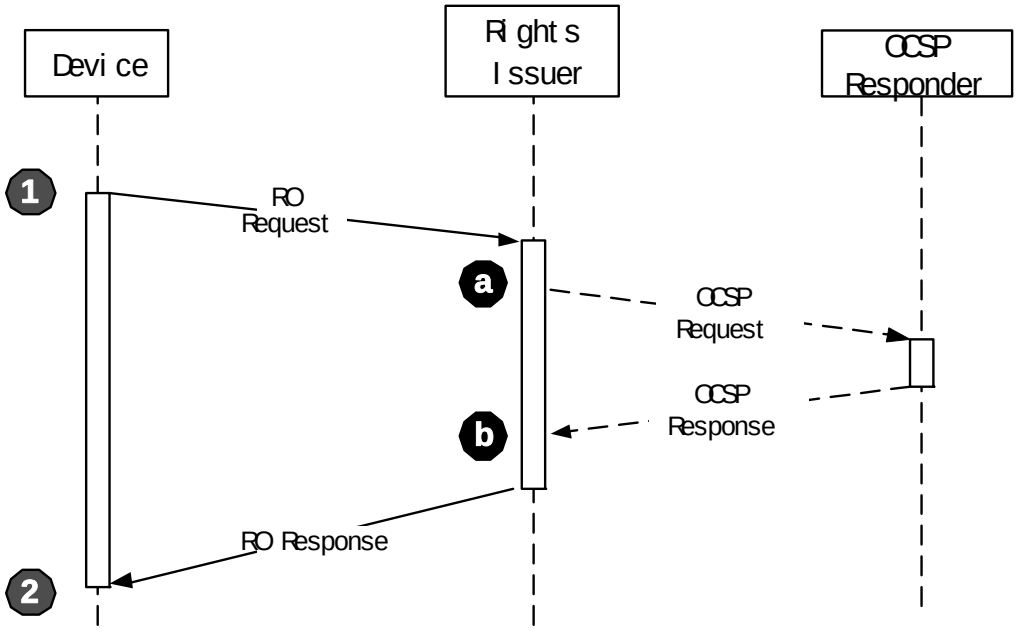


Figure 9.7: 2-pass Rights Object Acquisition Protocol

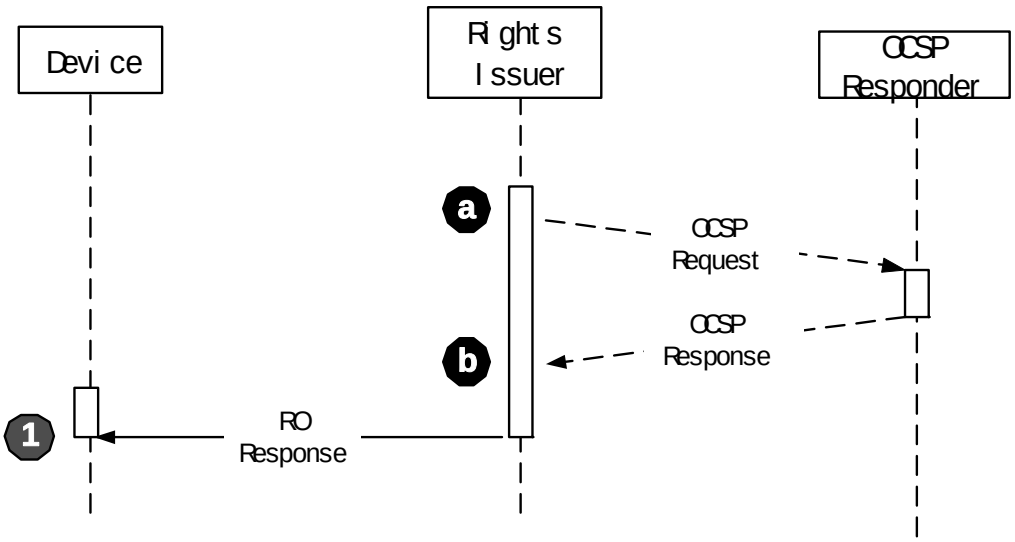


Figure 9.8: 1-pass Rights Object Acquisition Protocol

Within TISPAN OMA BCAST DRM-Profile could be integrated in a platform, similar to an architecture which uses a registrar functionality for the initial registration and the delivery of LTKMs. This platform is shown in figure 9.9.

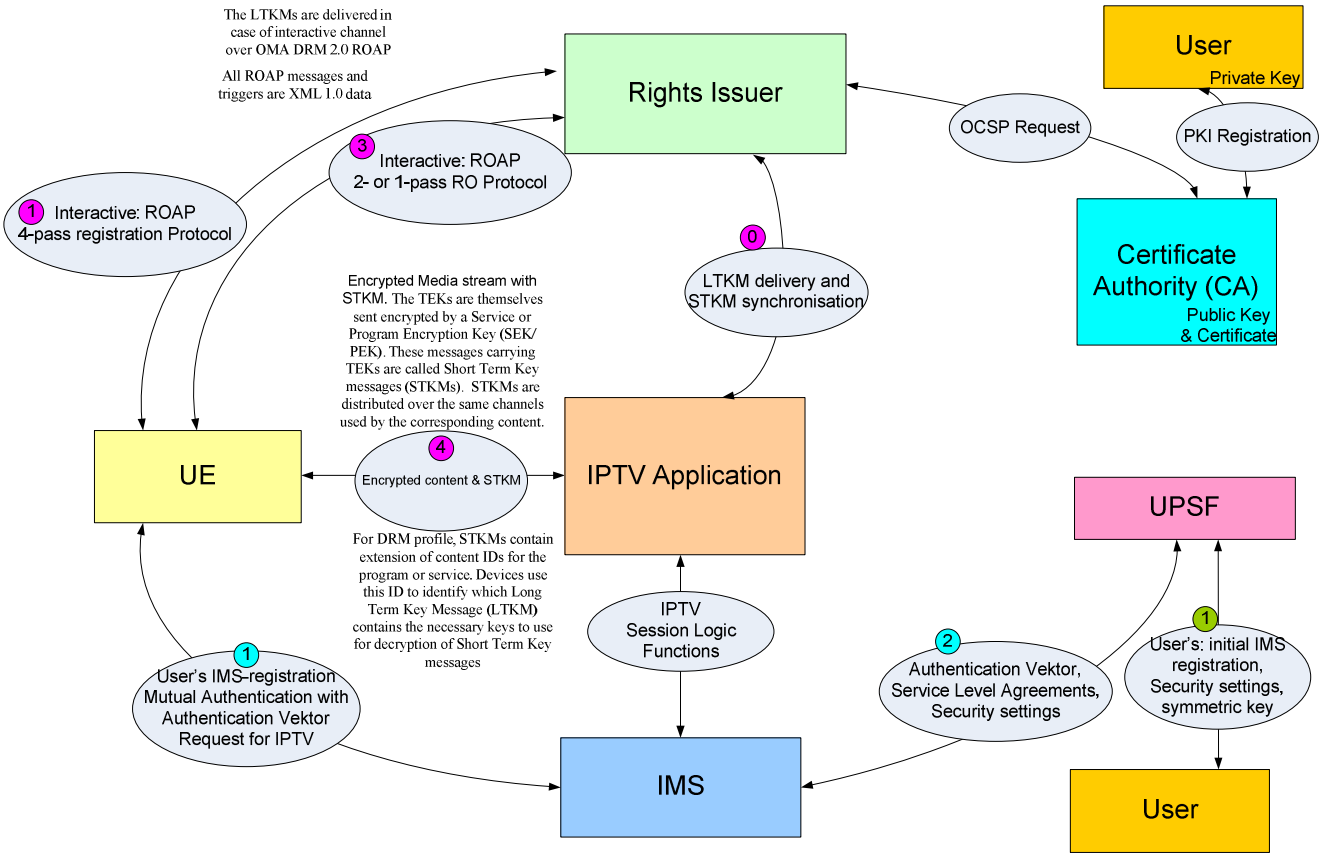


Figure 9.9: Proposed platform for OMA BCAST DRM-Profile and TISPAN IPTV

9.3 Service Protection using DVB Simulcrypt approach

Following the DVB simulcrypt approach as defined in [i.9], service media and data are encrypted only once even if several Service Protection solutions are deployed in parallel. This avoids the duplication of streams over the delivery network.

Service media and data are encrypted using one TEK at a time. This TEK is protected by the SEK of each Service Protection solution. For example for 2 different Service Protection solutions the TEK is protected by SEK_1 provided by $SKMF_1$ and the same TEK is protected by SEK_2 provided by $SKMF_2$.

9.3.1 Functional Architecture Overview

The security models provided in clause 8 applies. The only particularity is that several instances of SKMF can work in parallel. So interfaces between SKMF and UE or SMF remain unchanged. The difference come from the need to have a common TEK for all SKMF instances. This applies to both 4-layer and 3-layer key hierarchies.

Figure 9.10 shows an example for 2 Service Protection solutions with a 4-layer key hierarchy.

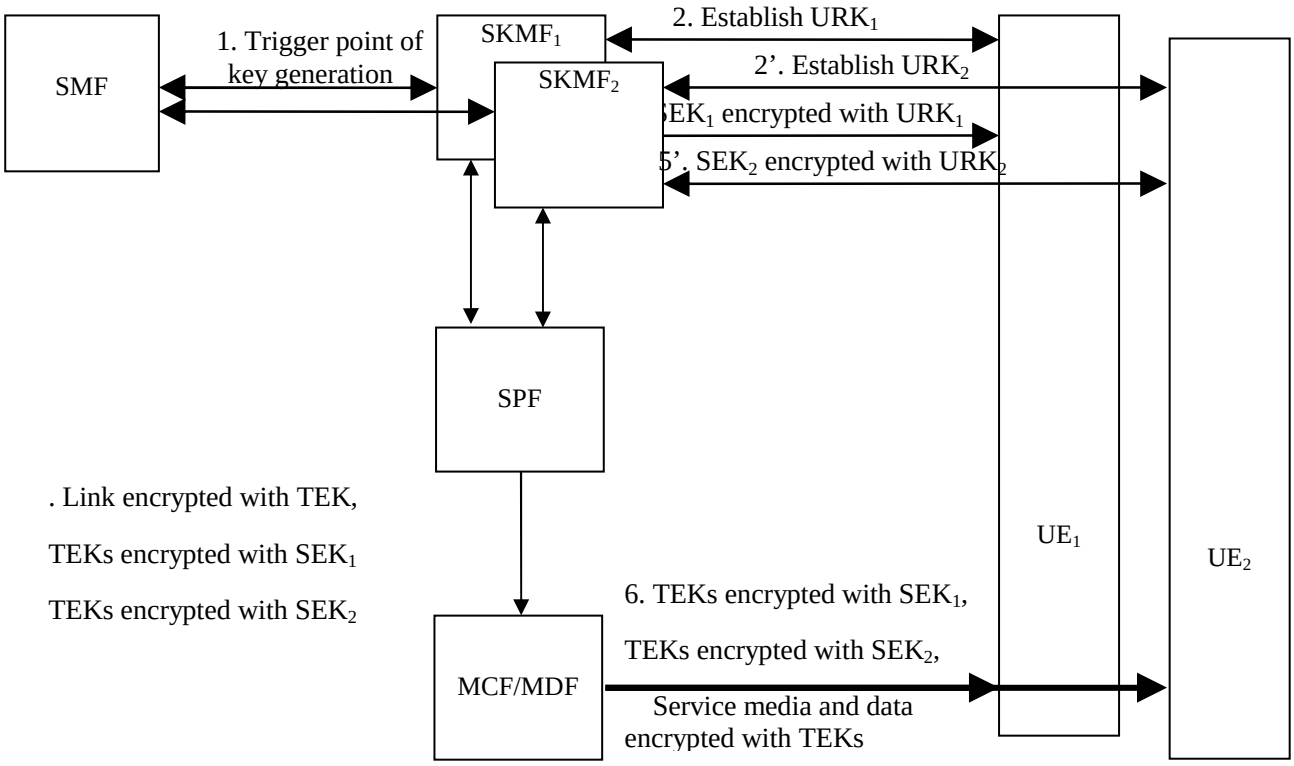


Figure 9.10: Simulcrypt model based on 4-layer key hierarchy

In this example UE_1 negotiates URK_1 with $SKMF_1$, obtains SEK_1 using URK_1, then TEK using SEK_1, then can decrypt the service media or data.

Similarly UE_2 negotiates URK_2 with $SKMF_2$, obtains SEK_2 using URK_2, then TEK using SEK_2, then can decrypt the service media or data.

9.3.2 Solution Description

The simplest way to have a common TEK is to make it generated by the SPF.

The SPF generate TEK.

The SPF asks each $SKMF_n$ to return TEK protected by SEK_n.

9.4 MBMS as candidate solution for IPTV Service Protection

3GPP's MBMS as described in [i.10] uses a 4-layer key management model and addresses so both, unicast download, and multicast live-streaming services.

MBMS is based on a symmetric key model using currently on the UE side smartcards for security processing and credential storage.

NOTE: MBMS as candidate solution (as proposed within the present document) currently only applies to IMS-based IPTV. Since MBMS was originally designed independently from IMS, it should also work for integrated IPTV. Investigating whether MBMS can also be candidate for integrated IPTV should be for further study.

MBMS is based on Generic Bootstrapping architecture [i.11]. As such it provides bootstrapping of IPTV-application security to mutually authenticate the subscriber and the IPTV-Service using the AKA protocol and provides also confidentiality and data integrity of multimedia live-stream and unicast download during the content delivery.

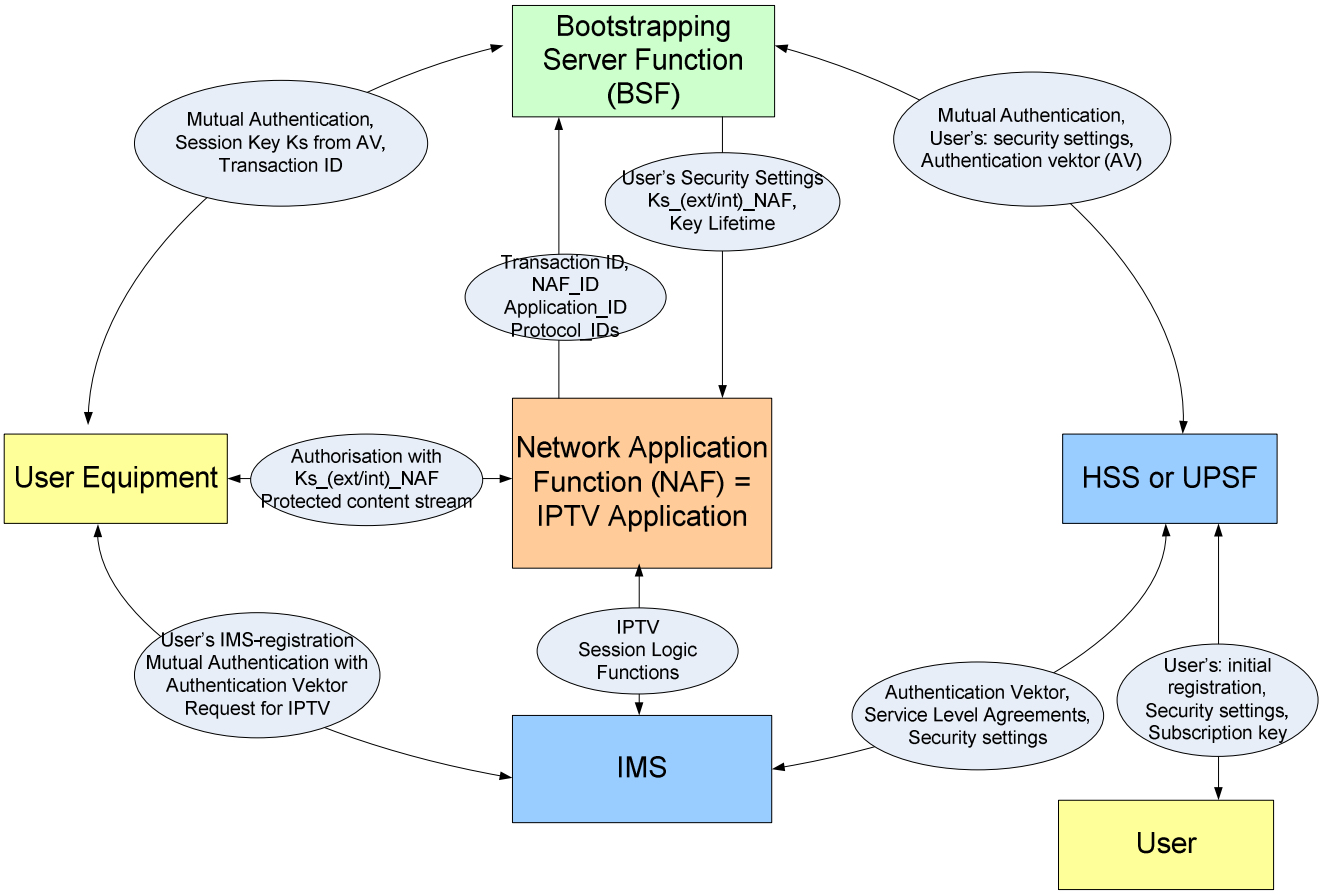


Figure 9.11: Functional Entities and Data Flow Diagram

- At user request for the IPTV-Service, the IPTV-server responses the UE to authenticate at the Bootstrapping Server Function (BSF).
- On behalf of the following UE's requests to the BSF, the BSF contacts the Home Subscriber Server (HSS at 3GPP) or User Profile Server Function (UPSF at ETSI TISPAN) to pull from it user's security settings together with corresponding credentials.
- Subsequently session derivation key Ks and IPTV Bootstrapping Transaction ID (B-TID) for the IPTV consumption are generated.
- BSF sends B-TID to the UE.
- The UE takes now the B-TID (its current pseudonym user-name) and requests with it again the IPTV-Server for the IPTV-Service.
- The IPTV-Server contacts now the BSF with the B-TID and its NAF-ID and (after successful authentication) gets from it the final session Key Ks_(ext/int)_NAF which is associated to the B-TID and the NAF_ID (Ks_(ext/int)_NAF is also derived from the Session Key generated previously between the UE and the BSF).

- Henceforth the UE and IPTV-Server are able to derive all the other keys to protect the E2E confidentiality and data integrity between them for all subsequent IPTV-applications belonging to this session.

In 3GPP there is also a specification for IMS-based PSS and MBMS User Service (as described in [i.13]). The IMS-based PSS and MBMS User Service specification using MBMS protection has big similarities with ETSI TISPAN IMS-based IPTV (see figure 7.2). It is therefore a very good candidate for ETSI TISPAN IMS-based IPTV R3 protection, giving the chance to implement point-to-point confidentiality and data integrity between the IPTV-application and the UE with only minor architecture adaptations. Over more IMS-based MBMS as well as IMS-based ETSI TISPAN IPTV are based on IMS and use it for the IPTV session logic (for session initiation, session maintenance and session termination). Also due to the fact that both mobile and fixed network provider use IMS as trusted platform, IMS-based IPTV combined with MBMS seems to be an excellent candidate for Mixed Mobile Convergence IPTV.

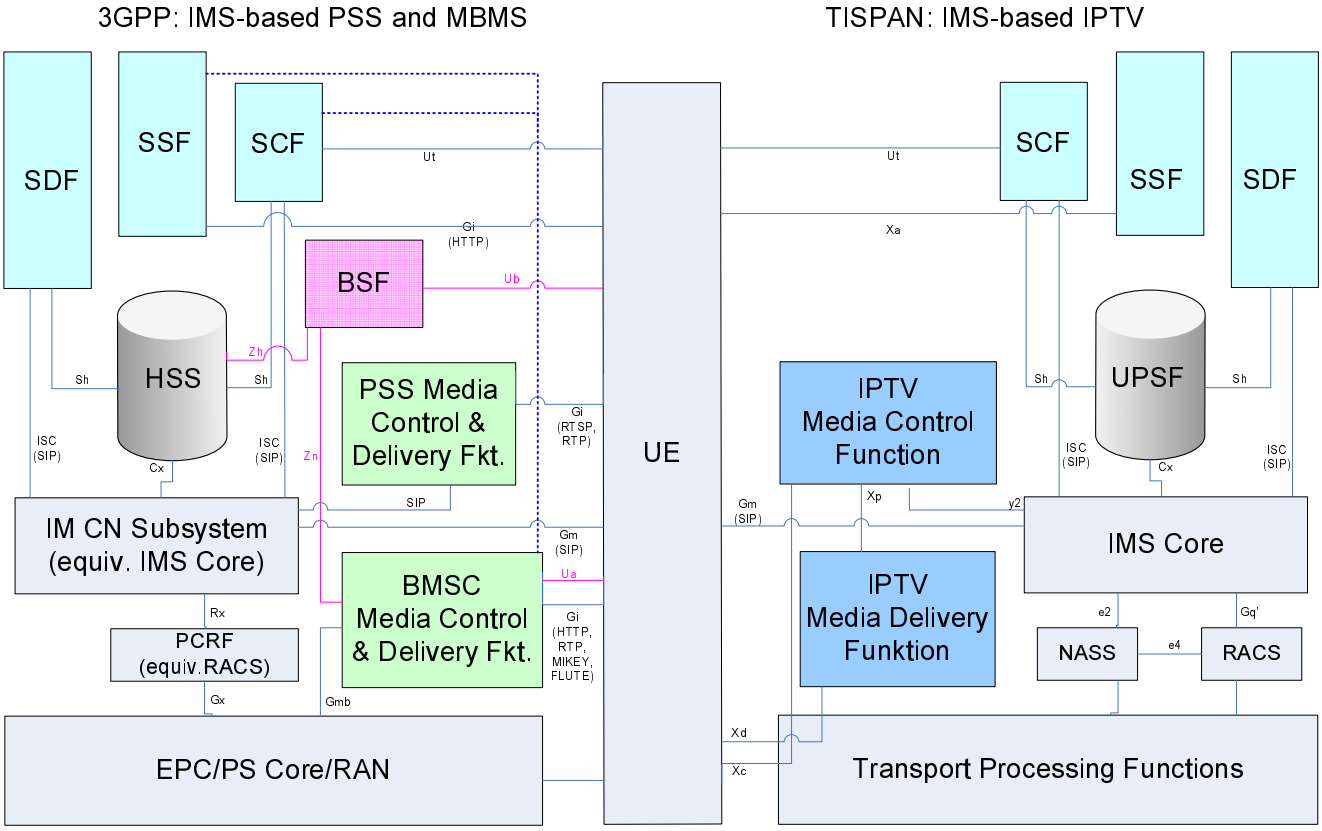


Figure 9.12: Comparison IMS-based PSS and MBMS User Service with ETSI TISPAN IMS-based IPTV

NOTE: Anyhow, since there are functional entities which overlap to a certain amount with functional entities of ETSI TISPAN IMS-based IPTV R3 MBMS cannot be used as a whole. Therefore the proposal is to use only the protection parts of MBMS (and BM-SC) and adapt it to ETSI TISPAN IMS-Based IPTV purposes.

9.4.1 Summary of MBMS as candidate solution

1) With MBMS service protection for IMS-based ETSI TISPAN IPTV R3 can be specified.

2) MBMS is based on 4-layer key management method and therefore capable to perform Multicast live-stream encryption and data integrity during multicast delivery.

3) MBMS as the protection system for IMS-based IPTV is an already available 3GPP specification [i.10] implementing protection mechanism for multicast and broadcast multimedia live-streaming services as well as for unicast download multimedia services.

4) MBMS is already accepted at OMA BCast specification for live-streaming multimedia service and is included in the "SmartCard" profile specification.

5) MBMS could be integrated already with minor adaptations into ETSI TISPAN IMS-based IPTV architecture.

6) The most of the Procedures and Protocols from TS 126 237 [i.13] could be easily adapted into ETSI TISPAN IMS-based IPTV stage 3 specifications [i.13].

7) IMS-based MBMS and IMS-based IPTV have the same session control logic for IPTV and are therefore excellent candidates for fixed-mobile-convergent IPTV [i.13].

8) Since MBMS is based on Generic Bootstrapping architecture, it has the following advantages:

   a) It uses Bootstrapping Server Function (BSF) as a kind of trusted third party registrar for the IPTV user and for the IPTV service provider. Only the BSF communicates with the back-end databases HSS or UPSF. Otherwise a huge amount of IPTV-Application Servers have to communicate with HSS and UPSF. This is not a good security.

   b) IPTV-Servers are Network Application Functions which can be deployed anywhere in the NGN network: in the visited, as well as in the home or third party network.

   c) Through MBMS IPTV-Sessions are well authenticated and authorised, the Media during delivery is confidentiality and data integrity protected.

   d) Through MBMS and GBA the IPTV-service provider may flexibly create program packages, offer them to the customers and perform powerfully conditional access.

   e) MBMS Key Management System is an interactive system between the IPTV-user and the IPTV-Application.

   f) MBMS implements privacy concerning the user identities: for each established session the BSF creates with the B_TID a user-name pseudonym.

   g) Through slight modification open framework for service protection can be implemented, so that MBMS-Protection for IMS-based IPTV is open for a variety of proprietary CA-Systems.

   h) Additionally, for encryption purposes encryption tool box could be specified, where the customer had the choice to choose between different encryption mechanisms.

Because MBMS is the most flexible, scaleable and most accepted solution under the current available standardised IPTV-Protection mechanisms, and is the best candidate for FMC-IPTV and is over more the candidate solution specified in most details, we propose to take MBMS as a candidate for the Technical Specification TS 187 003 [i.4] for ETSI TISPAN IMS-based IPTV Release 3.

NOTE: This proposal is conditional on the following limitations/issues with MBMS being addressed either in 3GPP or TISPAN.

1) The IPTV architecture allows more than one implementation, and not just MBMS.

2) In MBMS, the Key Management Server is the Bootstrapping Server Function (BSF) in 3GPP Generic Bootstrapping Architecture. However, the referenced 3GPP specifications mandate that a physical UICC is present. This may not be possible for all set top boxes for IPTV services. TISPAN has to investigate possible solutions for UICC-less environments.

3) The need for multiple users on a set to box and the binding of these identities to authentication is not covered in MBMS and the current UICC specifications.

4) There may be more threats introduced as a result of a shared device in the home compared with MBMS, which assumes a personally owned device and can these be countered e.g. protected channel.

5) MSK distribution in MBMS is "point to point" (p-t-p) initiated by request from the end user. With p-t-p, it is trivial to generate acknowledgements if needed (In the mobile device switched off, flat battery out of coverage) MNO it is understood that point to multipoint (p-t-m) is being considered for TISPAN IPTV. Handing acknowledgements is far more complex for p-t-m delivery, but then maybe fixed operators can assume the device is commented at all times so this may not be an issue. A compromise may be to use p-t-m with "staggered" acknowledgments and then p-t-p to catch the stragglers.

6) IPTV in the fixed network may require a means to support service transfer from device to device and the ability of a 3rd device to act as a controller. In this context, the controller device acts as an Attribute Authority where the IPTV service acts as the Source of Authority (SoA). This may require changes to the MBMS security Architecture.

7) MBMS was originally designed independent from IMS, and therefore should work for integrated IPTV also. We need to investigate whether MBMS can also be candidate for integrated IPTV.

NOTE: For the adaptation purposes of MBMS to TISPAN IMS-based IPTV R3, see informal annex A.

9.5 User Authentication and Service Authorization and any Content Protection (UA, SA and any CP) as candidate solution

This clause proposes to consider a Service Protection solution, as defined in TISPAN, based on the combination of the following 3 mechanisms:

- user authentication and service authorization, based on existing solution referenced in TISPAN, i.e. GBA, HTTP digest and NASS Bundle Authentication, as described in [i.4];
- service confidentiality and service integrity, based on existing solution in TISPAN, i.e. TLS, as described in [i.4];
- and any content protection applied to IPTV content.

Depending on the requirements and the level of security to be provided, one, two or the three mechanisms are combined.

This solution will be called User Authentication and Service Authorization and any Content Protection, in short "UA, SA and CP" in the present document. The proposed solution is similar to the solution adopted in Open IPTV Forum. However in Open IPTV Forum, the content protection solutions are restricted to a limited set of solutions, specifically specified.

9.5.1 Open IPTV Authentication, Content and Service Protection Specification

Open IPTV Forum (OIPF) Content and Service Protection (CSP) [i.15] supports two approaches:

1) a terminal-centric approach that is Marlin-based, that uses OMA file formats (PDCF, DCF) and the Marlin IPMP file format for protection of files, and that supports AES or DVB-CSA encryption, the ECM from IEC 62455 [i.24] for MPEG-2 transport stream protection; and

2) a gateway-centric approach that is based on a secure authenticated channel between a gateway device, the CSPG and the OITF (CND in TISPAN words). The CSP Gateway (CSPG) functional entity supports a framework enabling alternatives to the Marlin based content and service protection solution. Two solutions have been defined in [i.15]: a CI+ based gateway centric approach and a DTCP-IP based gateway approach.

This clause only takes in account the two following content protection solutions:

- Terminal centric approach based on Marlin. It is based on the Marlin DRM protocol and architecture [i.16], [i.17], [i.18], [i.19] and [i.20].
- Gateway centric approach based on CI+. In OIPF this solution describes a deployment where the Content Protection Client is embedded in a CI+ CAM module, inserted in the OITF. In TISPAN, this solution should be extended to embedded Content Protection Client CSPG in the OITF (CND in TISPAN words).

The last solution Gateway centric approach based on DTCP-IP defines an architecture where the content protection solution is in the IMS Gateway (CNG in TISPAN words) and where the IPTV protocol for protected content between this IMS Gateway and the network is out of scope of the specification and not described. Therefore this solution is not taken in account in this clause.

Both solutions foresee an integrated mechanism for both, the service protection and the content protection, and The protection of the service (as defined within TISPAN specs) is delegated to the protection of the content, and so its scope is larger than the simple transport of the streams/files from the network server to the customer device. Hence the specification defines mainly the behaviour of the OIPF elements and their interfaces to the content protection system, complying with the various Marlin specification and use-cases for the first solution, and with [i.25] for the second solution. Figures 9.13 and 9.14 show at high level the OIPF content protection architecture for the terminal-centric approach where the CSP is integrated into the OITF (CND in TISPAN words), or for CI+ based gateway centric approach, where the CSPG is integrated into a CI+ CAM module inserted in the OITF. The selected content protection solution impacts on the customer device (OITF in the picture), and to the IPTV Provider Network (CSP-T/CSP-G Server, in the picture). Moreover the OIPF specification defines an interface for the communication between the OITF and the Providers Network (UNIS-CSP-T/UNIS-CSP-G).

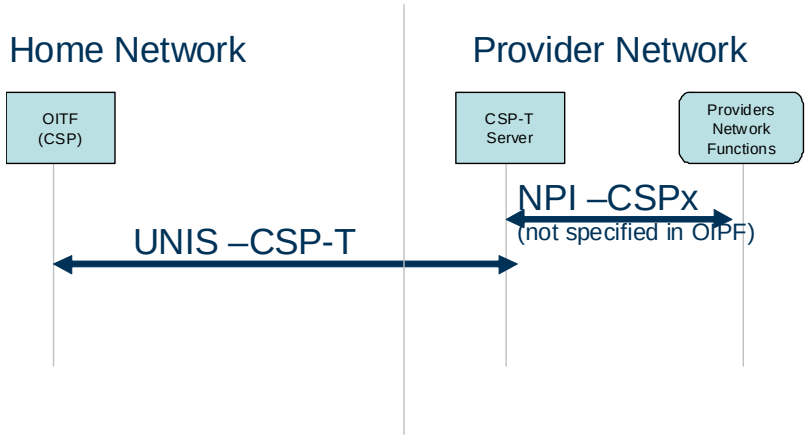


Figure 9.13: OIPF CSP Terminal Centric Approach general architecture

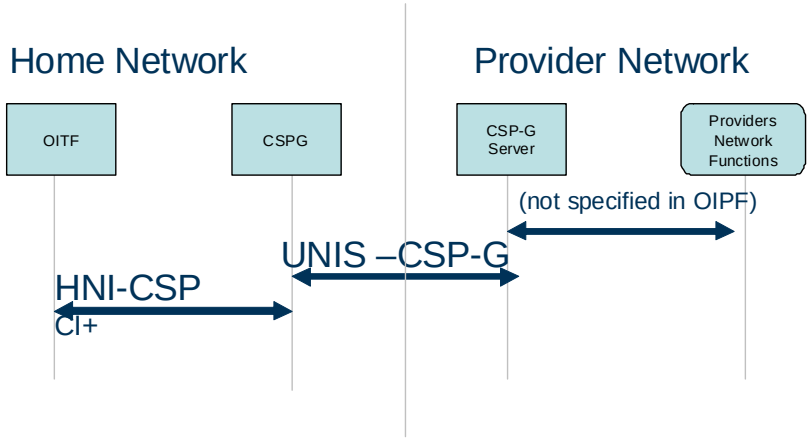


Figure 9.14: OIPF CSP Gateway Centric Approach general architecture

The functional entities in figure 9.14 are described below:

- CSP/CSP-G consists of Content Protection Client Function.
- CSP-T/CSP-G Server consists of the Content Protection Server Function.
- Providers Network Function is the function in the Providers Network that interacts with the CSP-T/CSP-G Server.

The full description of OIPF content protection solutions is available in the volume 7 of the OIPF specification release 1 [i.15].

OIPF additionally specify the users access authentication mechanisms to the IPTV service (strictly speaking, the Service Protection is limited to the authentication and authorization of the user). To be note that, given such objectives, the OIPF security architecture does not define or manage any specific key hierarchy, leaving that aspects to the DRM (i.e. Marlin) mechanisms. The general authentication architecture is based on the Service Access and Authentication (SAA) element.

The Open IPTV Terminal Function (OITF) contacts the IPTV Service Function via HTTP requests. It is up to the service provider to select SSL/TLS protocol for further protection. The Service Access Authentication (SAA) is responsible to perform the actual authentication of the user (the SAA could be collocated with the Service Function) and the communication among the three elements is based on the HTTP redirect messages.

The following authentication mechanisms are supported:

- No authentication.
- HTTP authentication: this can be basic or digest authentication [i.23]. Optionally SSL/TLS can be used to protect the basic authentication process.
- Network based authentication, similar to the TISPAN Nass Bundled Authentication (NBA).
- Web based authentication, where it is described a possible authentication mechanism based on HTML forms.
- GBA based authentication based on the TS 133 220 [i.11]. It is assumed that the UICC is present in the customer device. Note that the GBA is used only for the authentication of the customer; the shared keys generated at the end of the AKA process are not used for the protection of the delivery of the content.
- SAML web-based SSO authentication based on the usage of SAML [i.21], [i.22] token to realize a Single Sign On behaviour (the initial authentication can be based on one of the other listed mechanisms).

The **requested service** decides what security (service protection) is needed for the service delivery: authentication needed or not, confidentiality needed (TLS/SSL) or not.

The **SAA** decides what authentication mechanisms it uses and what security is needed for the performed authentication: TLS/SSL or not.

9.5.2 OIPF SAA and CSP solutions integration into TISPAN NGN

To sum up, the OIPF content and service protection architecture is based on the following:

- The protection of the content and its delivery (and so also the service protection in TISPAN specs) is based on the usage of a content protection mechanism (either Marlin or a proprietary CAS protection for CI+ based approach).
- The actual service protection is limited to the initial user authentication and authorization.

Given the fact that the integration of a specific content protection solution is out of the scope of TISPAN (but anyway network procedures such as for example Marlin registration, Marlin de-registration, Marlin License acquisition have to be integrated at the application level with a minimal impact to the IPTV architecture), the integration of the OIPF security architecture into the TISPAN NGN can be simply realized by integrating the authentication mechanisms defined in the OIPF specifications at the application layer (IPTV server). To be noted that in the "managed model", the OIPF IPTV architecture is actually the TISPAN IMS-based IPTV, and so the main authentication mechanism should be based on the GBA or Digest authentication (for UICC-less customers).

The following picture shows the mapping of the OIPF content and service protection for the managed model into the TISPAN IMS IPTV architecture (in blue colour the new elements).

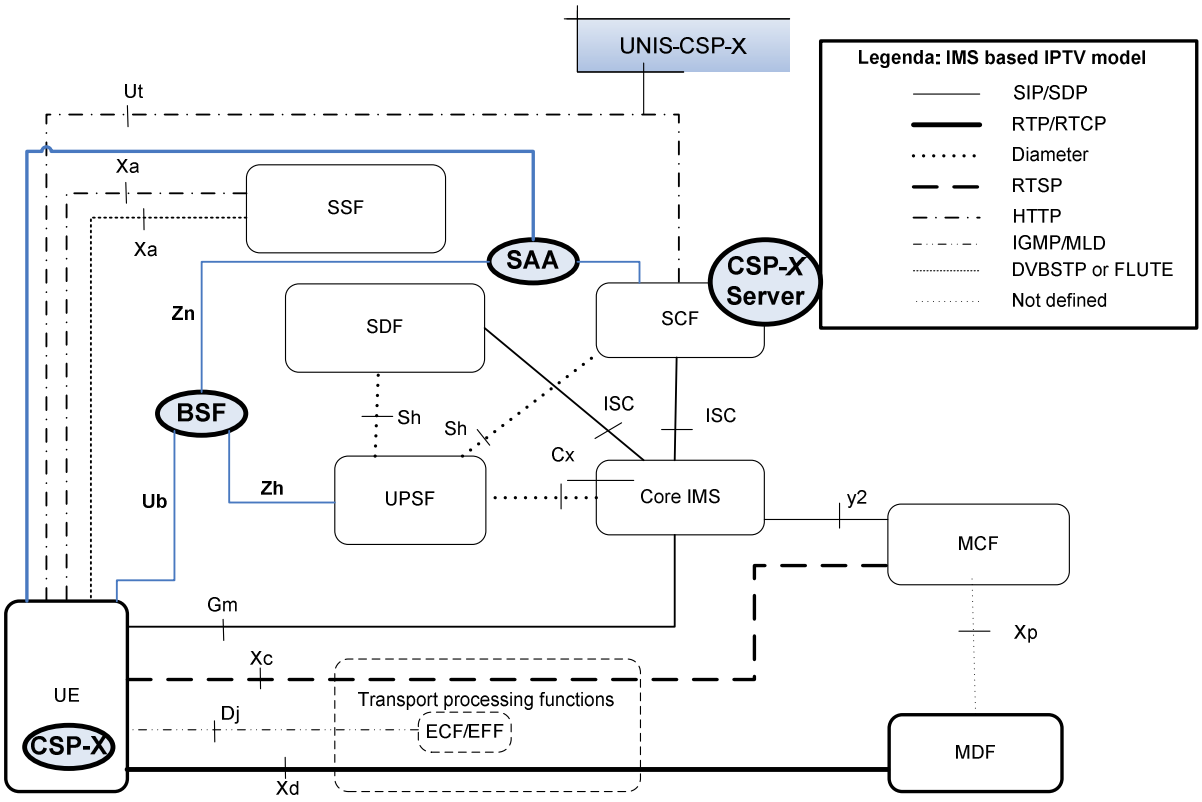


Figure 9.15: TISPAN IMS IPTV and OIPF authentication architecture

As showed in figure 9.15, the OIPF content and service protection specification impacts (in blue colour) on the TISPAN architecture as follow:

- The CPN and CND have to comply to the OIPF specification. The CSP-X (client) (CSP or CSP-G CI+) can be placed in the CPN within the CND (e.g. IPTV STB).
- The CSP-*X* (CSP-T or CSPG) server functions can be placed e.g. within the IPTV Service Control Function.
- The UNIS-CSP-*X* (communication between the CND and the Content Protection Server Service Function) can be mapped to the Ut or Xa or a new reference point to be defined; This interface should remain open.
- Authentication procedures between the CND, the Service Function and SAA at the application level are OIPF specific (e.g. SAML web-based SSO). The IMS authentication over Gm is already defined in the TISPAN architecture.
- In order to use the GBA, it is necessary to include in the TISPAN architecture the Bootstrap Server Function (BFS). The BSF interacts to the SAA for the authentication of the customers.

10 Gap Analysis and Selection of Possible Solutions for Service Protection

10.1 TISPAN IPTV Security Requirements

Table 10.1

General IPTV Sec Arc requirements	OMA BCAST (9.2)	Simulcrypt (9.3)	MBMS (9.4)	UA, SA and any CP (9.5)
Support 3-layer key layer model	YES	YES	YES	If supported by the Content Protection Solution
Support 4-layer key layer model	YES	YES (DVB)	YES (broadcast)	If supported by the Content Protection Solution
Common IPTV Security Requirements (14)	(13/14)	Oos	(8/14)	(14/14) but depends on the content protection solution
IPTV Service Protection Requirements (7)	(5/7)	(2/7)	(4/7)	(7/7) but depends on the content protection solution
Non-IMS-based IPTV Security Requirements (9)	(6/9)	Oos	(1/9)	(9/9) but depends on the content protection solution
Availability and DoS Protection Requirements (3)	oos	Oos	Oos	Oos
Other Assessment Requirements				
NOTE 1: "-> MBMS" means that in the case of OMA BCAST the MBMS solution is applied. NOTE 2: "(x/y)" means X over Y requirements are fulfilled.				

10.1.1 Common IPTV Security Requirements

OMA BCAST corresponds to Smartcard Profile and DRM Profile. SCP refers to OMA BCAST Smartcard Profile.

For OMA BCAST solution, more details are provided for SCP in order to facilitate comparison with MBMS.

Table 10.2

	OMA BCAST (9.2)	Simulcrypt	MBMS (9.4)	UA, SA and any CP (9.5)
R-IPTV-C-1	- Yes OMA BCAST address all kind of users	oos	YES MBMS addresses users and not group of users	Yes User Authentication
R-IPTV-C-2	- Yes There is unique and non-forgeable user identity. For SCP, the user identity is IMPI from ISIM or IMPI derived from IMSI of USIM	oos	YES IMPI is IMPI derived form IMSI of USIM	Yes User Authentication when using non forgeable identity. If not it may be combined with content protection using non forgeable identity

	OMA BCAST (9.2)	Simulcrypt	MBMS (9.4)	UA, SA and any CP (9.5)
R-IPTV-C-3	- Yes There could be one subscription identified by a SEK/PEK and distributed to several users. Same subscription but sent separately to the users	oos	- Yes There could be one subscription identified by a MSK and distributed to several users	Yes User Authentication Subscriptions can be managed in the network and/or with Content Protection
R-IPTV-C-4	- Yes SCP: GBA for exchange of credentials that are used to send the LTKM DRM: public/private key stored on the terminal are used to secure the delivery of REK key used to protect the LTKM	oos	YES GBA used to compute MRK and MUK keys. MUK key is user key used to send the MSK messages	Yes User Authentication when using non forgeable identity. If not it may be combined with content protection using non forgeable identity
R-IPTV-C-5	- Yes Each user is authorized through the SEK/PEK received within the LTKM	oos	YES Each user is authorized through MSK received within MSK message protected by means of MUK key	Yes User Authentication and Service Authorization Subscriptions can be managed in the network and/or with Content Protection
R-IPTV-C-6	- Yes SCP: At this time not a notion of groups but can assign unique and non forgeable identities to user: IMPI	oos	- (No notion of groups)	Yes User Authentication when using non forgeable identity. If not it may be combined with content protection using non forgeable identity Group can be managed in the network and/or with the Content Protection solution
R-IPTV-C-7	- Yes SCP: At this time not a notion of groups but all subscribers are authenticate using the credentials exchanged during GBA procedure	oos	- (No notion of groups)	Yes User Authentication Group can be managed in the network and/or with the Content Protection solution
R-IPTV-C-8	- Yes SCP: At this time not a notion of groups but all subscribers are uniquely authorized	oos	- (No notion of groups)	Yes User Authentication, Service Authorization and optionally Content Protection. Group can be managed in the network and/or Content Protection

	OMA BCAST (9.2)	Simulcrypt	MBMS (9.4)	UA, SA and any CP (9.5)
R-IPTV-C-9	- Yes The user device is uniquely identified through the IMEI or more generally Terminal_ID when the secure channel is established between Terminal and card	oos	- (per user not device)	Yes, according content protection solution in use, which usually has a device specific non forgeable ID
R-IPTV-C-10	- Yes Authorization to IPTV service is given to user; but using the secure channel verification that a trustable terminal is used is verified when the Secure channel is established	oos	- (per user not device)	Yes, according content protection solution in use, which usually has a device specific ID
R-IPTV-C-11	- Yes SCP: Unique identity to IPTV session are defined by Key Domain ID/ SEK/PEK ID (MSK ID Key group). Verification of rights is done by the Card and then the user and not the device. DRM: per	oos	- (per user not device)	Yes, according content protection solution in use, which identifies the session
R-IPTV-C-12	- Yes SCP: Service provider is defined through the Key domain ID. The credentials exchanged during the GBA procedure ensure the verification, integrity and authentication	oos	YES	Yes, according content protection solution in use which identifies the service providers
R-IPTV-C-13	- (Not addressed)	oos	- Not addressed	Yes User Authentication and Service Authorisation RTSP Session can be controlled through RTSP Session Id delivered in authenticated (and possibly protected) SIP or HTTP Session
R-IPTV-C-14	- Yes Identity is associated to the service using the SEK/PEK key group, but using also the KV, the authorisation can be reduced to a content (PEK instead of SEK in this case)	oos	- (Not addressed)	Yes, according content protection solution in use which identifies the content

10.1.2 IPTV Service Protection Requirements

Table 10.3

	OMA BCAST (9.2)	Simulcrypt (9.3)	MBMS (9.4)	UA, SA and any CP (9.5)
R-IPTV-CN-1	- Yes Delivery of SEK/PEK with corresponding rights (token-based, pay per view, pay per time, etc.) in LTKM	YES(Another spec from DVB)	- Yes Delivery of MSK	Yes Content Protection Key/right/license distribution and TLS establishment depends on previous User authentication and authorization
R-IPTV-CN-2	- Yes LTKM are protected against unauthorized access using the SMK (SCP: derived during GBA procedure). The message are encrypted and signed	oos	-Yes MSK messages are protected by means of MUK user key	Yes Service Authorization, TLS and Content Protection
R-IPTV-CN-3	- Yes Communication between service and user is protected using the SMK for LTKM and using SRK for all other communication	oos	- Yes Communication is protected using MUK key and MSK key	Yes User authentication and TLS
R-IPTV-CN-4	- Yes This is ensured by the Key validity data. There is also a Key lifetime that the terminal can use to erase TEK but this is not very useful as TEK are updated often	oos	- Yes There are key lifetime	Yes User Authentication, Service Authorization and TLS can be sufficient in some cases for connected services, content protection can be used in addition in all cases on ITPV content
R-IPTV-CN-5	- Yes OMA BCAST can support DVB Simulcrypt by means of SP-4 interface	YES	- MBMS does not support DVB Simulcrypt	Yes Any Content Protection Solution is supported
R-IPTV-CN-6		oos		Yes User authentication and TLS can be combined with almost any Content Protection Solution
R-IPTV-CN-7		oos		Yes

10.1.3 Non-IMS-based IPTV Security Requirements

Table 10.4

	OMA BCAST (9.2)	Simulcrypt (9.3)	MBMS(9.4)	UA, SA and any CP (9.5)
R-IPTV-NIMS-1	- Yes The link to an IPTV session is done using the SEK/PEK received by the user	oos	-Yes (per session) The link to an IPTV session is done using the MSK received by the user	Yes User authentication
R-IPTV-NIMS-2	- Yes The link to an IPTV session is done using the SEK/PEK received by the user	oos	Yes The link to an IPTV session is done using the MSK received by the user	Yes User authentication
R-IPTV-NIMS-3	- Yes The IPTV service are identified through the SEK/PEK ID and this identification is used to provide the keys (TEKs). Only authorized users are able to consume the IPTV service	oos	- Yes The IPTV service are identified through the MSK ID and this identification is used to provide the keys (TEKs). Only authorized users are able to consume the IPTV service	Yes The IPTV services are identified through the content protection solution and this identification is used to provide the keys to access the IPTV service. Only authorized users are able to consume the IPTV service Metadata delivery can be protected with TLS
R-IPTV-NIMS-4	- Yes The IPTV service are identified through the SEK/PEK ID and this identification is used to provide the keys (TEKs). Only authorized users are able to consume the IPTV service	oos	- Yes The IPTV service are identified through the MSK ID and this identification is used to provide the keys (MTKs). Only authorized users are able to consume the IPTV service	Yes The IPTV services are identified through the content protection solution and this identification is used to provide the keys to access the IPTV service. Only authorized users are able to consume the IPTV service
R-IPTV-NIMS-5	- Yes The IPTV service are identified through the SEK/PEK ID and this identification is used to provide the keys (TEKs). Only authorized users are able to consume the IPTV service	oos	- Yes The IPTV service are identified through the MSK ID and this identification is used to provide the keys (MTKs). Only authorized users are able to consume the IPTV service	Yes The IPTV services are identified through the content protection solution and this identification is used to provide the keys to access the IPTV service. Only authorized users are able to consume the IPTV service

	OMA BCAST (9.2)	Simulcrypt (9.3)	MBMS(9.4)	UA, SA and any CP (9.5)
R-IPTV-NIMS-6	- Yes The IPTV service are identified through the SEK/PEK ID and this identification is used to provide the keys (TEKs). Only authorized users are able to consume the IPTV service	oos	- Yes The IPTV service are identified through the MSK ID and this identification is used to provide the keys (MTKs). Only authorized users are able to consume the IPTV service	Yes The IPTV services are identified through the content protection solution and this identification is used to provide the keys to access the IPTV service. Only authorized users are able to consume the IPTV service
R-IPTV-NIMS-7	-	oos	-	Yes User Authentication and Service Authorization
R-IPTV-NIMS-8	-	oos	-	Yes User Authentication and Service Authorization
R-IPTV-NIMS-9	-	oos	-	Yes TLS established after User Authentication

10.1.4 Availability and DoS Protection Requirements

Table 10.5

	OMA BCAST (9.2)	Simulcrypt (9.3)	MBMS (9.4)	UA, SA and any CP (9.5)
R-IPTV-AD-1	No (oos is provided by the network itself)			
R-IPTV-AD-2				
R-IPTV-AD-3				

10.1.5 Other Assessment Requirements

10.1.5.1 Ability to address legacy IPTV head end and interworking to deployed equipment

For most of already deployed IPTV solutions based on MPEG-2 TS over UDP or RTP, a part of the above requirements are covered by the content protection solution generally known as a CAS (conditional Access System). In order to leverage on existing IPTV Head Ends and allow smooth migration to TISPAN deployment the following assessment needs to be considered:

- Ability of Service Protection solution to be applied on a service delivering IPTV content over MPEG-2 Transport Streams over UDP or RTP and protected by encrypting Transport Stream Packets with the DVB-CSA algorithm complying with protection system signalling as specified in. [i.25].

10.1.5.2 OMA BCAST solution

Ability to support already deployed service protection solutions:

OMA BCAST solution addresses service protection and/or content protection and can take into account already deployed service protections by means of SP-4 Interface that can support DVB Simulcrypt. MBMS does not support DVB Simulcrypt.

Equipment without smart card:

OMA BCAST DRM Profile provides solution for equipments without presence of a smart card. MBMS solution requires the presence of a UICC.

OMA BCAST Smartcard Profile supports MBMS.

10.1.5.3 UA, SA and any CP

By definition this solution authorizes any content protection solution, including DVB-Simulcrypt compliant deployments.

10.2 Comparisons between OMA BCAST Smartcard Profile and MBMS solutions

- **OMA BCAST supports MBMS**

  OMA BCAST Smartcard Profile relies on MBMS and also contains additional features. OMA BCAST supports MBMS smart cards.

- **DVB Simulcrypt support**

  BCAST Subscription Management that support service or content protection supports Interface SP-4. Interface SP-4 may support DVB Simulcrypt. The description of DVB Simultcrypt support is described in clause 13.1 of Service and Content Protection for Mobile Broadcast Services specification [i.8].

- **ISIM and IMPI**

  OMA BCAST Smartcard Profile relies on GBA with USIM application or ISIM application on UICC while MBMS relies only on GBA with USIM application on UICC.

  TISPAN IMS AKA relies on ISIM on UICC.

  The private user identity, the IMPI, used in MBMS is derived from the IMSI of the USIM application. With OMA BCAST, the user identity, the IMPI, would correspond to the IMPI of the IMS subscription, i.e. the IMPI of the ISIM on UICC.

- **Parental Control/ Pay Per View / Pay Per Time**

  Parental Control and Pay Per Time are services supported by TISPAN IMS based IPTV subsystems. Pay Per View signalling flows and Parental Control procedure are described in TS 182 027 [i.5] "IPTV functions supported by the IMS subsystem". The support of Parental Control service is mandated by TS 181 016 [i.3] "NGN Services and IPTV" for TISPAN R2 and R3. Pay Per View is mandated by TS 181 016 [i.3] for TISPAN R3.

  Parental Control, Pay Per View and Pay Per Time services are addressed by OMA BCAST while they are not addressed by MBMS.

- **Video on Demand and Content on Demand**

  Video on Demand and Content on Demand are covered by OMA BCAST while they are not addressed by MBMS.

- **Key Validity Data**

  The Key Validity Data for the Service Encryption Key and Program Encryption Key is coded on 32 bits within OMA BCAST Smartcard Profile (maximum key lifetime is 132 days) while the Key Validity Data is coded on 16 bits in MBMS (maximum key lifetime is 7 days).

- **TS increment**

  In MBMS for each STKM sent the TS field is increased, even if this STKM carries the same TEK as the previous STKM message. For OMA BCAST BCAST Smartcard Profile the server may resend the same STKM, containing the same TEK, without increasing the TS field. This avoids the need for generating new STKMs within the same crypto period. This is an improvement to the MBMS since BSM handling needs less processing for building subsequent authenticated STKM with the same key material included.

- **Secure Channel**

  The OMA BCAST Smartcard Profile defines the possibility to use a secure channel. The secure channel performs mutual authentication between the smartcard and the terminal, and protects the exchanges between the Smartcard and the Terminal. The keys decrypted by the Smartcard are sent to the terminal protected in integrity and confidentiality.

  MBMS does not describe possible usage of secure channel.

- **Terminals without presence of smartcard**

  In OMA BCAST, the scenario of UICC-less terminal is covered by means of the DRM profile.

  The DRM Profile is based on the Public Key Infrastructure provided by OMA DRM v2.0.

  MBMS addresses terminals containing a UICC.

- **Choice of the encryption level**

  In OMA BCAST, there is the choice of the level of encryption, IPSEC, SRTP, ISMACryp. For MBMS, SRTP is the only level of encryption that is used to protect the content.

  For IPSEC the encryption is made at the lower level in the IP stack, at IP level. The encryption is removed at the IP level of the stack and the content is transmitted in clear from the IP level to the application level through the stack, passing through a lot of software layers for which secure execution depends on implementation.

  For SRTP, the encryption is made at the transport level RTP of the stack. The encryption is removed in the IP stack and the content is transmitted in clear to the application level, passing through some software layer.

  For ISMACryp, the encryption is made at the application level. The content is transmitted from the stack to the application in encrypted form and the encryption is removed in the application itself. This allows the use of non-secure IP stack. This allows also a decryption either in software or in hardware in a dedicated chipset used for video decompression. This latter implementation increases significantly the security level within the terminal.

- **Service Guide**

  Service guide is a features proposed by OMA BCAST Smartcard Profile that does not exist in MBMS.

  TS 183 063 [i.7] "IMS-based IPTV stage 3 specification" contains clause on "Procedures using Flute for IMS-based IPTV" (clause 10). This clause applies when using OMA BCAST multicast delivery for service provider and guide discovery.

10.3 Pros and Cons considering DRM and SmartCard Profile

The use of a smartcard has advantages in terms of security. The SmartCard Profile provides a higher level of security than the DRM Profile due to the mandatory presence of the smart card, which is a an independent operator distributed tamper resistant device. Some actors of broadcast chain value, e.g. content creators and content providers, have very strong requirements in term of security to ensure that their content will be protected. Moreover, broadcast systems bring new security threats due to the fact that the users can be interested in hacking their own equipment, and the fact that one hacked user equipment compromises the whole system.

On the other side the Smartcard Profile may hamper the flexible use of the IPTV application within a household. To be able to guarantee secure access to all members, each of them ought to have a smartcard. In some scenarios it may be hardly acceptable for the provider to provision and to maintain such an amount of smartcards.

NOTE: The following smartcard-less use case is based on HTTPS (SSL or TLS) and describes a secure access to an IPTV Application using e.g. a STB as a shared device. It also differentiates between device (based on PKI) and user authentication:

1) OMA BCAST DRM-Profile protected device (e.g. STB) has its Private/Public key pair, the private key stored in a secure environment of the STB, the public key with a valid certificate (e.g. X.509).

2) Initial registration takes place between the Subscriber and the NGN/IPTV-Provider. NGN/IPTV-Provider proves the authenticity of the public key.

3) The user also subscribes to a specific IPTV Program with his IPTV-Source of Authority (SoA), in terms of OMA BCAST, the Rights Issuer. He gets from his SoA its public key with a valid certificate. This certificate can be easily validated by the user.

4) As soon as the user switches on his STB, the user's device registers as a valid device in the NGN/IPTV-Network.

5) As next, the user connects to his SoA and requests for his IPTV program.

6) He gets back the response from his SoA. In this response the SoA's public key (with certificate) is included and can be proofed by the user.

7) The user validates the certificates and generates a NONCE.

8) User encrypts NONCE with the SoA's Public Key and sends a new request with this encrypted NONCE to the IPTV Source of Authority.

9) Between the user and the SoA a secure channel is established.

10) SoA requests now a user-name and password authentication from the user. To avoid the thread of eavesdropping within the shared device (e.g. STB or PC), the user either has a list with transaction IDs, or he gets a transaction ID as an SMS over his mobile.

11) He types now his user-name and the transaction ID and transfers it to the IPTV Source-of-Authority.

12) After successful authentication the 4 phase ROAP takes place. SoA generates the Rights Encryption Key (REK) and sends it across the protected Channel to the user.

Summary: Good level of security is combined with the flexibility of one device serving as a shared device, enabling multiple users to access the IPTV without the need of a smartcard.

Using Smartcards in shared device environment like STB or Media PC may cause the following problems:

IPTV session keys may be copied/inserted on an exposed UICC-IPTV set top box interface. Although the session keys used in IPTV applications may have a quite limited scope, the requirements to protect keys (crossing the UICC-ME interface) may, in some specific use cases, be higher for IPTV devices than for personally purchased devices, due to:

1) The unguarded, unattended nature of the IPTV devices.

2) IPTV devices may have a gateway capability, so a compromise may increase the impact of key exposure over the UICC-ME interface for specific use cases.

However, there are mechanisms to prevent key exposure on UICC-IPTV set top box interface:

- The ETSI/3GPP secure channel specifications (TS 102 484 [i.29], TS 133 110 [i.30]), which require a shared secret or other type of credential, may be used to protect the UICC-IPTV set top box interface if required.

- Physical security mechanisms may be used to protect the UICC-IPTV set top box interface if required and these mechanisms can have more strength on an IPTV set top box than on a personally purchased consumer device.

11 Coexistence and Interoperability Analysis

11.1 Coexistence of pre-existing non-TISPAN IPTV protection solutions

11.1.1 DVB Simulcrypt

Many legacy IPTV solutions are deployed today where content is protected by scrambling at MPEG-2 TS packet level. According to DVB Simulcrypt [i.9] different overlying key management systems can be found generally referred to as CAS or DRM systems. These CAS/DRM solutions are likely to respond to Content Protection according to TISPAN definition. Consequently the framework for the integration of content protection solutions as introduced in clause 11.3 is likely to enable these non-TISPAN solutions.

11.1.2 OMA BCAST

OMA BCAST allows two key management profiles: the Smartcard Profile and the DRM Profile.

The Smartcard Profile relies on MBMS and also contains additional features. OMA BCAST Smartcard Profile supports MBMS.

OMA BCAST Subscription Management that support service or content protection supports Interface SP-4. Interface SP-4 may support DVB Simulcrypt, allowing the deployment of several service protection solutions in parallel and that could be already deployed on the field.

The description of DVB Simulcrypt support is described in clause 13.1 of Service and Content Protection for Mobile Broadcast Services specification [i.8].

11.1.3 UA SA and any CP

Any content protection solution, including DVB-Simulcrypt compliant deployments, and probably even other Service Protection Solution can be used with User Authentication, Service Authorization and optionally Service Confidentiality and Integrity as defined in [i.4].

11.2 Interoperability of service protection with content protection

NOTE: the intention of the clause is to demonstrate the service protection is open to interoperate/integrate with the content protection mechanism.

11.2.1 MPEG-2 Transport Stream Protection

TISPAN IPTV Architecture supports delivering a protected MPEG-2 Transport Stream complying with protection system signalling as specified in [i.25].

Where a TISPAN selected Service Protection solution is used for protection of MPEG-2 TS media over RTP or UDP, it should support that the MPEG_2 TS is additionally protected at TS packet level as specified in [i.25].

When TISPAN will consider Content Protection solutions, it should include content protection solutions for protection of MPEG-2 Transport Stream complying with protection system signalling as specified in [i.25].

11.2.2 OMA BCAST

OMA BCAST specification addresses service protection and content protection.

The OMA BCAST service protection could be used without the content protection.

OMA BCAST allows the integration of any content protection mechanism:

- In case that the content protection to be integrated is OMA BCAST content protection, then no additional security layer is required to address content protection since the same key hierarchy and messages would be used for both OMA BCAST service protection and content protection. OMA BCAST content protection information is added to the messages sent by the server to the user for OMA BCAST service protection.
- In case that the content protection to be integrated is not OMA BCAST content protection, then a second security layer is required. In this case, the content protection is provided using a separate set of security mechanisms.

11.3 Service Protection Model reusing UPSF/PDBF, BSF and NAFs

This clause provides service protection model reusing UPSF/PDBF, BSF, and NAFs, being capable of integration of a variety of different key management systems into the IPTV security architecture.

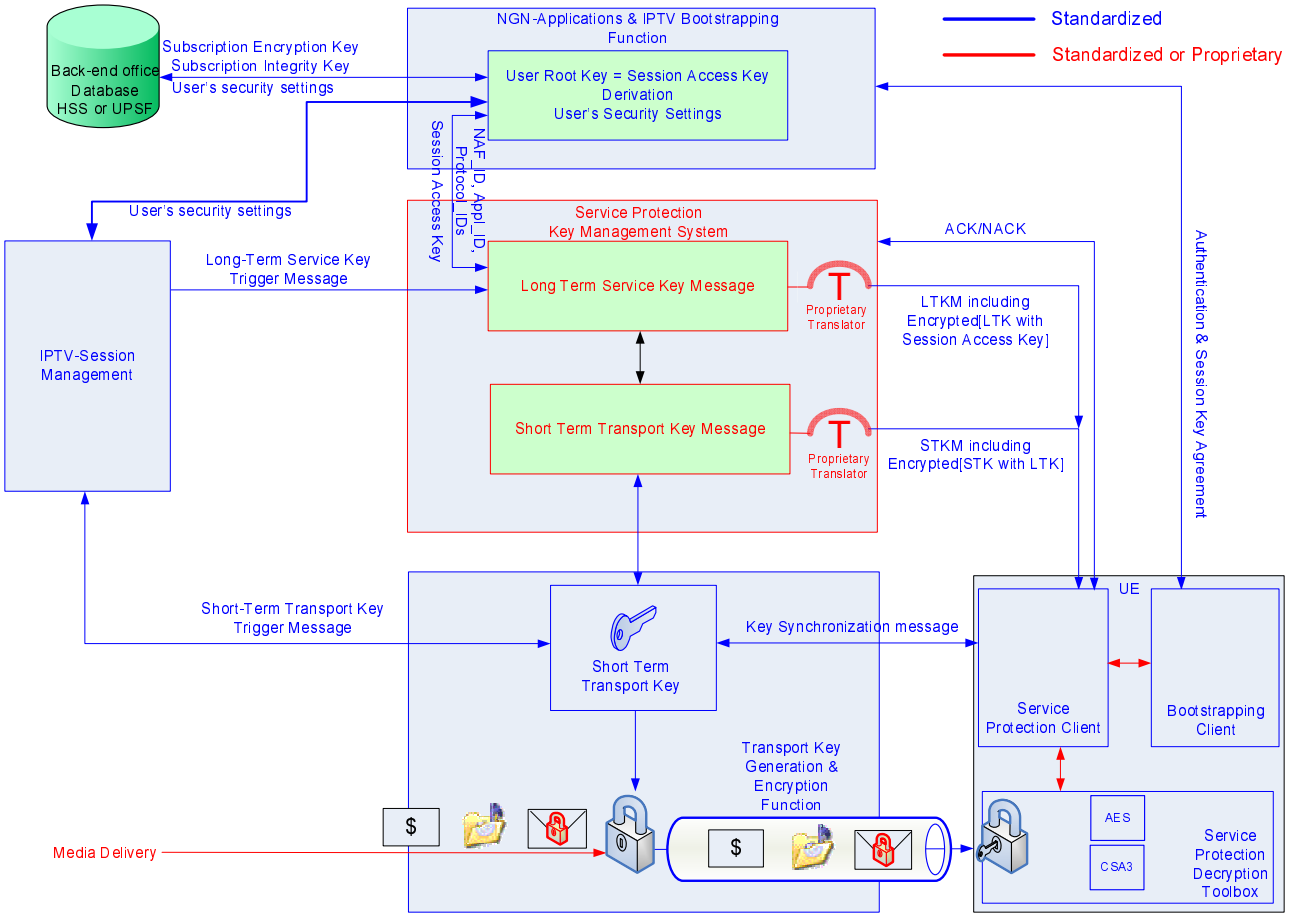


Figure 11.1: Service Protection Reusing UPSF/PDBF, BSF and NAFs

NOTE 1: All red lines describes possibly proprietary entities, protocols and formats; all blue lines describe open standardized entities, protocols and formats.

NOTE 2: Content protected by a content protection system (e.g. DRM, CAS) along with service information (e.g. meta-data, multicast UserID, content provider ID, parameters that affect service provider billing) is tunnelled through the service protection to provide e.g. general privacy of use of the service as illustrated in figure 11.1.

NOTE 3: CSA3 is designed to work at the IP level, whereas CSA1, CSA2 are designed for mpeg2 transport stream only.

Preconditions for the following consideration is the completed contract between the IMS-subscriber and IMS-end-user. As result, the IMS and IPTV-user possesses a subscriber key which will then be used in the IPTV-bootstrapping process. The subscriber key as well as the IPTV-user's security settings (including service profiles) are permanently stored in the back-office database, HSS or UPSF.

The open framework for the service protection consists of 4 parts:

1) NGN-Applications and IPTV Bootstrapping Function

   NGN-Applications and IPTV-Bootstrapping Function is fully standardized.

   NGN-Applications and IPTV Bootstrapping Function acts as a kind third party registrar for the IPTV-session. Its role is:

   a) To authenticate the user for the IPTV-session, to pull his service and security settings (with UE's encryption capabilities), and to generate session reference key (e.g. Ks) as well as IPTV-transaction ID, which serves for the duration of the IPTV-session as user's pseudonym user-name. To be able to create a session reference key, the NGN-Applications and IPTV Bootstrapping Function securely (ensuring mutual authentication, data confidentiality and data integrity) communicates with the Back-end office Database (HSS or UPSF) and pulls from there the user's credentials which are based on user's subscription key.

   b) To generate a session access key (e.g. Ks_ext/int_NAF) for the specific - from user requested - IPTV-session. The session access key is created based on the user's service and security settings (stored in the back-end-office), IPTV-transaction ID, the ID of the Service Protection Key Management System and the Service ID of the requested IPTV-service. The session access key is used for the access of the user to the IPTV-application and the protection of keys necessary for the confidentiality and data integrity delivery of the IPTV-service. To be able to generate a session access key the NGN and IPTV-registrar is contacted by the Service Protection Key Management System (see next bullet).

2) Service Protection Key Management System

   Service Protection Key Management System may be fully standardized or proprietary system.

   Service Protection Key Management System is responsible:

   a) For user's access authentication to the IPTV-service and for the subsequent establishment of a protected link between the IPTV-application server and the UE. To be able to do it, it generates the Long Term Service Key associated with the IPTV-Program (e.g. MSK= MBMS Service Key) the user wants to use and protects it with the session access key, obtained from the NGN and IPTV-registrar.

   b) For the generation of the Long Term Service Keys Messages (containing the protected service key), according to the received Long Term Service Key Trigger Message.

   c) For the generation of Short Term Transport Key Messages, (containing the protected transport key) according to the announced and received Short Term Transport Key Trigger Message got from the Transport Key Generation and Encryption Function.

   d) For secure delivery of the service key and the transport key to the authorized customer with his UE. Since all user equipment (also unauthorized) will get access to the content if they possessed the transport key, only the authorized users equipment is able to obtain the transport key, which encrypts the content delivered during the session. In the case of a multicast content stream all customers get point-to-multipoint the transport key encrypted with service key. But only the customer who is able to use the service key is now able to decrypt the transport key which is necessary for the content decryption. To ensure that only the authorized user's equipment gets the service key, the Service Protection Key Management System pushes now to each single authorized customer (point-to-point) also the service key, but encrypted with the customer's session access key. Now, only the authorized user's equipment can decrypt the service key (because only he possesses the session access key), then decrypt the transport key and use the obtained transport key to decrypt the content.

   e) In case of a proprietary system, for the translation of the possibly proprietary Long Term Service Key Messages Syntax and Semantic and Short Term Transport Key Messages Syntax and Semantic to standardised Long Term Service Keys Messages Syntax and Semantic and Short Term Transport Key Messages Syntax and Semantic.

f) For the delivery of the Long Term Service Keys Messages and the Short Term Transport Key Messages to the user's device.

3) Transport Key Generation and Content Encryption Function

This entity is responsible for:

a) to encrypt the content that was received from the content provider for submission to the CPE. The encryption algorithm used is selected by the service provider;

b) for the Transport Key Generation and its delivery to the Service Protection Key Management System and the Content Encryption Function;

c) synchronization of the key messages sent to the customer and the corresponding encrypted media packages.

4) User Equipment

User Equipment contains the necessary client parts that interact with the network functions.

Contains the following client parts:

a) IPTV bootstrapping client, which is responsible for the initiation of registration and authentication with the service providers IPTV service.

b) Service protection client, which allows the client to obtain the necessary keys needed to be able to decrypt content received from the IPTV service provider.

c) Content Decryption Toolbox, which contains a set of decryption algorithms that ensures that the UE is interoperable with the IPTV service providers it can be used with.

12 Recommendations

12.1 OMA BCAST

OMA BCAST with its two key management profiles, Smartcard Profile and DRM Profile, is a candidate solution that fulfils TISPAN IPTV Service Protection requirements, both at services level and security level. OMA BCAST solution addresses service protection and/or content protection and can take into account already deployed service protections by means of SP-4 Interface that can support DVB Simulcrypt.

OMA BCAST should be incorporated in TS 187 003 [i.4] as solution for TISPAN IPTV Service Protection.

12.2 UA SA and any CP

In simple and maybe early deployment of IMS IPTV, Service Protection as defined in TISPAN, can be ensured using User Authentication and Service Authorization based on user authentication as already defined in TISPAN and optional service confidentiality use, with combination of any Content Protection solution.

Consequently, it should be explicitly stated in clause 9, Security Architectures for IPTV, of TS 187 003 [i.4], that a possible solution can be ensured with the NGN security architecture as defined in clause 4 of TS 187 003 [i.4] in conjunction with any content protection solution.

Annex A (informative): Service Protection using MBMS Approach

A.1 Introduction

MBMS Service protection guarantees that only authorised users get access to ETSI TISPAN IPTV service. Through MBMS protection the authenticity of the customer and the service provider is proofed in context of an IPTV session establishment. Over more it protects the confidentiality and data integrity of the data sent during the established IPTV session based on the subscriber keys and derived session keys.

MBMS is based on GBA architecture offering scalability to the operators and data privacy to the customer.

In context of 3GPP specifications, GBA based Service Protection for Multimedia Broadcast and Multicast services is already specified in TS 133 246 [i.10] and could easily be adopted as service protection mechanism to the IPTV R3 architecture.

A.2 Key Architecture

A.2.1 Four-layered key management system

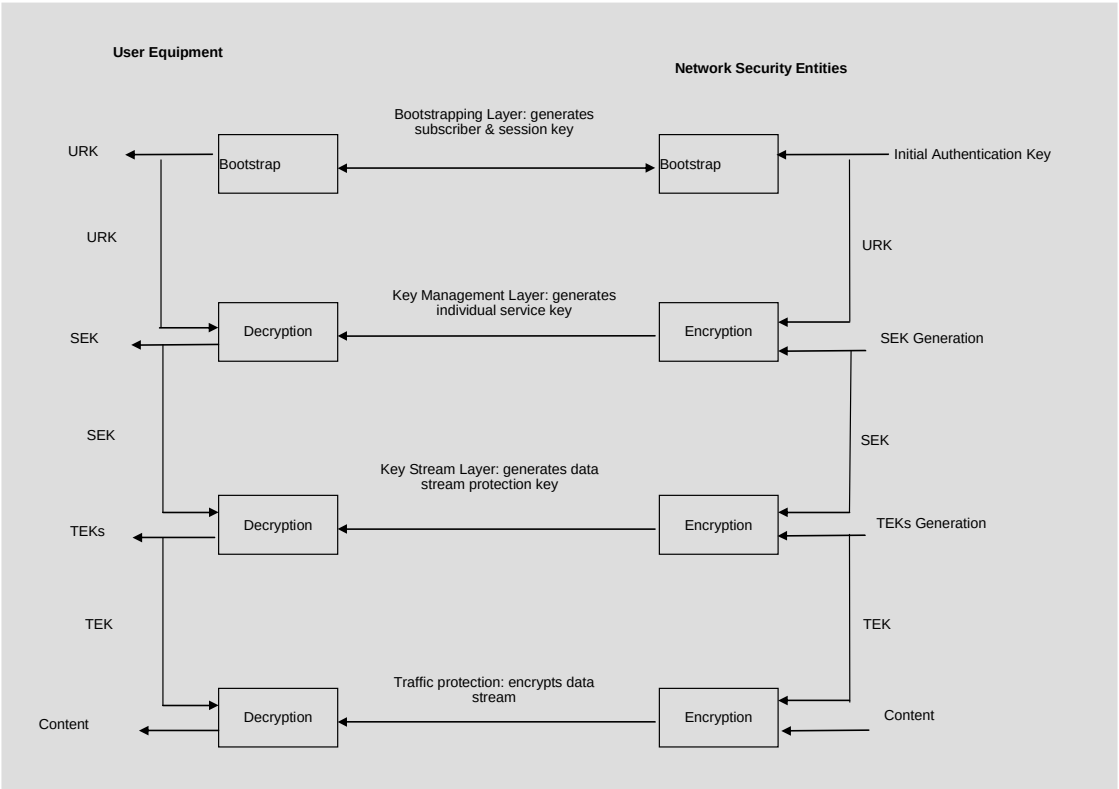


Figure A.1: Key management model

Layer 1 is the place for the subscription, service registration and the bootstrapping of authorised service session.

Layer 2 is responsible for the Service Key Distribution over broadcast or interactive channel.

Layer 3 is responsible for the Traffic Key Distribution over broadcast or interactive channel.

Layer 4 is responsible for the encryption of the unprotected data with the Traffic Key, its delivery over the broadcast channel and their decryption with the Traffic Key Distribution.

A.2.2 Root Key and the Layer 1 subscriber management key

In our consideration we assume, that IMS- and IPTV-service providers have trusted relationship. Then, the layer 1 root key is the user's subscriber key agreed with the IMS-provider and be trusted by the IPTV-provider. The root key is then used for the derivation of all another keys in the subsequent Layers. These are the session key (being still in layer 1) used for the IPTV service, Long-term-key belonging exclusively to a special user (Layer 2) and eventually the Short-term-keys (Layer 3) with which the traffic is eventually encrypted and decrypted (Layer 4). The key derivation procedure is described in the figure 7.1.

The meaning of the keys is:

- The subscriber key authenticates the customer gaining access to the IMS-services.
- The IPTV-session key authenticates the customer for the access to the IPTV. With the session key the customer is authorised to use the IPTV-service.
- Long-term keys protect the data integrity and confidentiality of the short-term key's delivery to the customer in case of multicast. In case of unicast the long-term key protects the data integrity and confidentiality of the unicast data stream itself.
- Short-term keys protect the data integrity and confidentiality of the multicast data stream.

In case of multicast we need all 4 Layer, in case of unicast only the Long-term-key is needed (and therefore only 3 layers), because we do not need to address customer group.

A.2.3 Key architecture within ETSI-TISPAN Security architecture

The GBA/GAA-based 4-layered key management architecture fits into TISPAN Security Architecture as follows:

The root key, as proposed in 1.2 is agreed between the IMS-Provider and the customer and stored in UPSF (HSS). From there all NGN-applications are able to use it for authentication purposes.

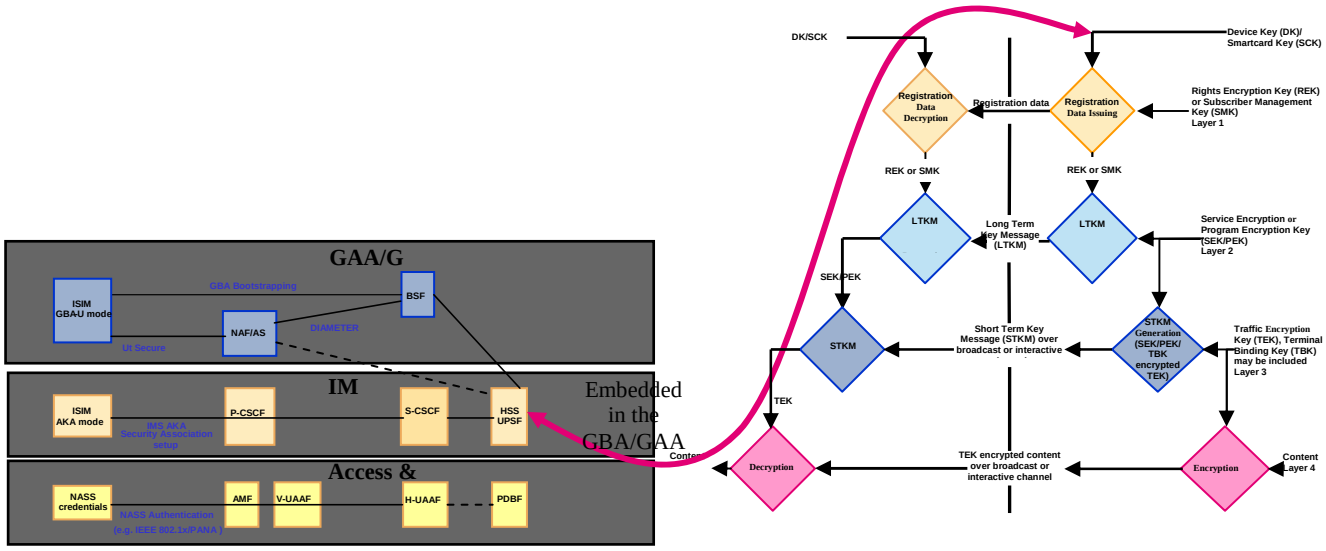


Figure A.2: 4-layered key architecture integrated in TISPAN NGN Security Architecture

A.3 MBMS-Architecture

We propose the use of MBMS architecture based on GBA for the IPTV protection purposes.

A.3.1 MBMS and GBA

GBA provides bootstrapping of application security to authenticate the subscriber using the AKA protocol. This infrastructure could be used to enable application functions in the network and on the user side to establish shared keys.

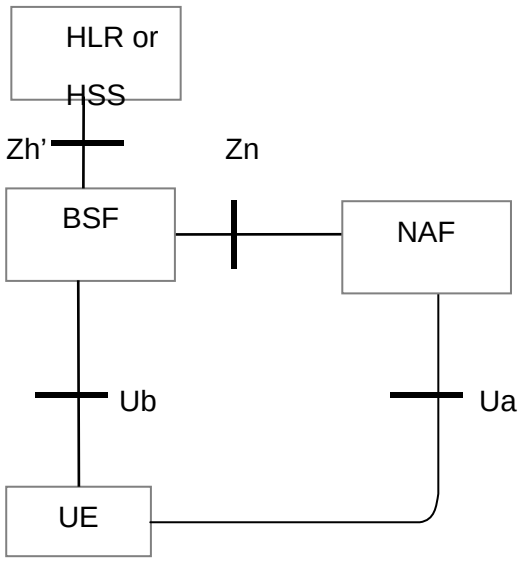


Figure A.3: GBA-Architecture - Functional Entities and Reference Points

Core GBA functional elements are the Bootstrapping Service Function (BSF) and the Network Application Function (NAF). In order to establish a valid session for the customer, the BSF communicates with Home Location Register (HLR) or Home Subscriber Server (HSS); it pulls there the User's subscriber Key, on behalf of the UE's request. In case of TISPAN, the subscriber key will be pulled from the UPSF, which has in case of IPTV the same functionality as HSS.

For detailed description of GBA Network Elements, please see clause 4.2 (Network Elements) in TS 133 220 [i.11].

A.3.1.1 Bootstrapping server function (BSF)

The BSF can be seen as a Registrar (a kind of trusted third party trusted by the customer as well as by the NAF and HSS), registering the user for the IPTV-Service. It is designed on the one side for secure communication between the HSS database storing the persistent user profiles and credentials, agreed at subscription contract. On the other side it communicates securely with the NAF, which is in our case the IPTV server. The BSF hides user's origin identity with a transaction ID, which is subsequently used by the user for the establishment of the IPTV session. As such the BSF protects user's privacy.

Core requirements for the BSF as described in TS 133 220 [i.11]:

1) BSF and UE mutually authenticate using the AKA.

2) BSF and UE agree on session keys, that are afterwards applied between UE and a Network Application Function.

3) BSF restricts the applicability of the key material to a specific NAF (IPTV service).

4) Lifetime of the key material is set according to the local policy of the BSF.

5) BSF is able to acquire the GBA User Security Settings (GUSS) from the HSS.

6) BSF is able to keep a list, which assigns NAFs to NAF Groups. This list is used to select if any and which application-specific USS within GUSS is valid for a certain NAF.

7) Upon successful authentication BSF generates a transaction ID (G_TID) with witch the user authenticates in the next step at the NAF.

A.3.1.2 Network application function (NAF)

The following core requirements describes the functionality of the NAF:

1) NAF is able to locate and securely communicate with the subscriber's BSF.

2) NAF is able to acquire a shared key material established between UE and the BSF during the run of the application-specific protocol.

3) NAF is able to acquire zero or more application-specific USSs (User Security Settings) from the HSS via the BSF.

4) NAF is able to set the local validity condition of the shared key material according to the local policy.

5) NAF is able to check lifetime and local validity condition of the shared key material.

A.3.1.3 Home Subscriber Server (HSS)

The following core requirements describes the functionality of the HSS

1) HSS provides the only persistent storage for GUSS (GBA User Security Settings).

2) GUSS is defined in such a way that interworking of different operators for standardised application profile is possible.

3) GUSS is be defined in such a way that profiles for operator specific applications and extensions to existing application profiles are supported without need for standardisation or these elements.

A.3.1.4 UE

The required functionalities from the UE are:

1) The support of HTTP Digest AKA protocol.

2) The capability of both a USIM and an ISIM in bootstrapping.

3) The capability to select either a USIM or an ISIM for bootstrapping if all of them are present.

4) The capability to derive new key material to be used with the protocol over Ua interface from CK and IK.

5) Support of NAF-specific application protocol (see TS 133 221 [i.31]).

A.3.1.5 Bootstrapping architecture and reference points

In this clause we describe only reference points important for the use of MBMS with TISPAN IPTV. For complete information see TS 133 220 [i.11], clause 4.2.

A.3.1.5.1 Reference point Ub

The reference point Ub is between the UE and the BSF. Reference point Ub provides mutual authentication between the UE and the BSF. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure.

The HTTP Digest AKA protocol, which is specified in RFC 3310 [i.32], is used on the reference point Ub. It is based on the AKA TS 133 102 [i.33] protocol. The interface to the USIM is as specified in TS 133 102 [i.33] and to the ISIM is as specified in TS 131 103 [i.34].

A.3.1.5.2 Reference point Ua

The reference point Ua carries the application protocol, which is secured using the key material agreed between UE and BSF as a result of the run of HTTP Digest AKA over reference point Ub.

A.3.2 BM-SC as NAF

Within MBMS architecture, the Broadcast Multicast Service Centre (BM-SC) is responsible for distribution and protection of Multicast Media Streams to the customer. It is a part of the MBMS architecture.

Within the GBA architecture BM-SC gets the role of the Network Application Function (NAF).

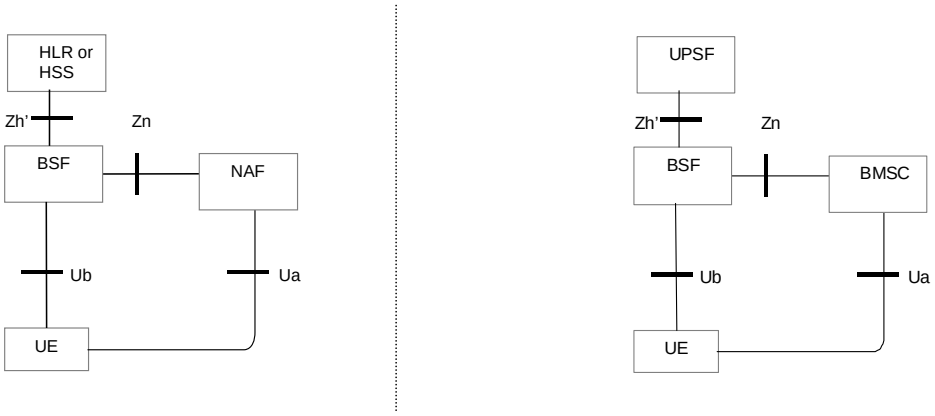


Figure A.4: BM-SC' role in GBA

A.3.3 BM-SC Network Components

This clause has only informational character. This is due to the fact that all here in the clause described functional entities have very similar functionalities to ETSI TISPAN IPTV R3 functional entities but none of them is identical to functional entities described in TISPAN IMS-based IPTV. This is simply because MBMS has been designed for mobile networks. To adopt one-to-one all functional entities of BM-SC to TISPAN IPTV is therefore not possible.

To adopt the protection mechanism, we therefore propose to adopt only the BM-SC Security Function for ETSI TISPAN.

For more detailed information about BM-SC see TS 123 246 [i.12].

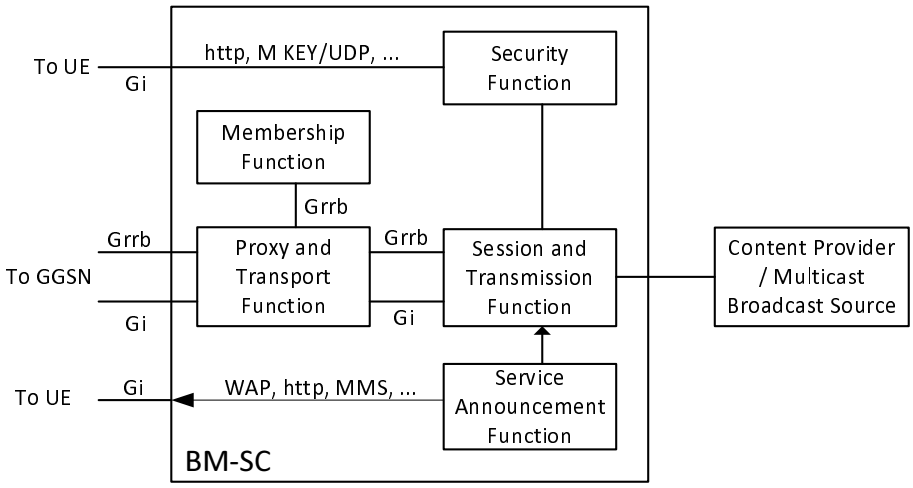


Figure A.5: BM-SC and its network components

A.3.3.1 Membership function

Membership Function:

1) Provides authorization for UEs who is requesting to activate an MBMS service.

2) Maintains subscription data of MBMS service users.

3) May generate charging records for MBMS service users.

4) May also provide membership management etc. In this case it does also have a Gi interface.

The membership function has functionalities which can be found in ETSI TISPAN IPTV R3 in the Service Control Function (SCF) and the Service Membership Function (SMF) but does not match totally. Over more, it has peculiarities which are related only to mobile environment.

A.3.3.2 Session and transmission function

Session and transmission function:

1) Maintains session transmissions and retransmissions.

2) It makes the sessions identifiable.

3) Provides the bearer layer with transport associated parameters (QoS).

4) It initiates and terminates the bearer resources.

5) Responsible for error detection and correction.

6) Should be able to authenticate and authorize external sources and accept content from them.

7) Is user service level function and triggers bearer level functions when MBMS sessions are scheduled.

The Session and transmission function has functionalities which can be found in ETSI TISPAN IPTV R3 in the Service Control Function (SCF) but do not match totally. Over more, it has peculiarities which are related only to mobile environment.

A.3.3.3 Proxy and Transport Function

MBMS bearer service is a function with the following functionalities:

1) Responsible for the signalling over Gmb, e.g. between MB-SC Membership Function and BM-SC Session and Transmission function.

2) Is able to generate charging records for content provider charging of transmitted data.

3) May be divided into function managing control plane and transport function managing the multicast payload.

The Proxy and Transport function has functionalities which can be found in ETSI TISPAN IPTV R3 in the Media Delivery Function (MDF), the Media Control Function (MCF) and the Service Membership Function (SMF) but do not match totally. Over more, it has peculiarities which are related only to mobile environment.

A.3.3.4 Service Announcement Function

Service Announcement Function is a function with the following functionalities:

1) Provision of service announcements for MC and BC.

2) Provision of media description such as type of video and audio decoding.

3) Provide UE with MBMS session description (e.g. MC service ID).

The Service Announcement Function has functionalities which can be found in ETSI TISPAN IPTV R3 in the Service Selection Function (SSF) and the Service Discovery Function (SDF) but do not match totally.

A.3.3.5 MBMS Security Function

MBMS Security Function is the only function which can be adopted in ETSI TISPAN's IPTV R3 architecture. And ETSI TISPAN does not have Security Function yet. We therefore propose the use of MBMS Security Function and its adaptation to IMS-Based IPTV R3 part, as described in clause 4.

MBMS Security Function provides UE with integrity and/or confidentiality protection of MBMS data. It controls access to the MBMS-data by distributing keys only to authorized UEs.

In terms of service protection, MBMS is responsible for:

1) Establishing shared secret with the UE using GBA.

2) Authenticating the UE with HTTP digest authentication.

3) Registering and De-registering UEs for MBMS Service.

4) Generating the keys necessary for MBMS security using MIKEY.

5) Distributing the keys necessary for MBMS security using MIKEY.

6) Applying the appropriate protection to data transmission.

A.3.3.6 Protocol stack used by MBMS User Services

For more information see TS 126 346 [i.35] MBMS Protocol and Codecs. The grey-shaded protocols and functions are outside of the scope of TS 126 346 [i.35]. MBMS security functions and the usage of HTTP-digest and SRTP are defined in TS 133 246 [i.10].

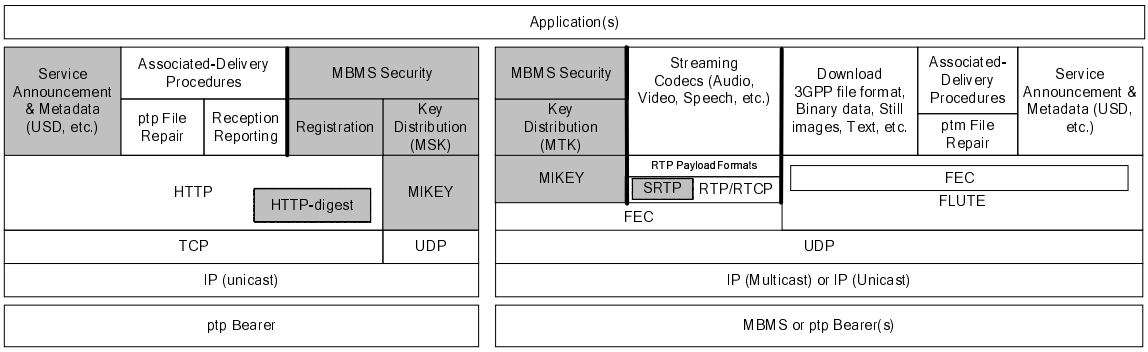


Figure A.6: Protocol stack used by MBMS user services

For IPTV R3 of ETSI TISPAN its bearer has to be adapted to the MBMS architecture.

The multicast media stream is delivered through the RTP (Real Time Protocol). The control stream is transported through the RTCP (Real Time Control Protocol). The SRTP as described in the table provides confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP) as described in the RFC 3711 [i.36]. According to the RFC 3711 [i.36] SRTCP uses by default the same master key (and master salt) as SRTP.

A.4 Service protection of TISPAN IMS-based IPTV using MBMS

A.4.1 Using MBMS security function for IMS-based IPTV-Service Protection

A.4.1.1 MBMS and BM-SC scope

The MBMS Security Mechanism is specified in TS 133 246 [i.10].

MBMS defines service protection system for Multimedia Broadcast and Multicast services, with the following security mechanism:

1) Protected access to the Multicast and Broadcast service.

2) Granting the authenticity of the communicating peers.

3) Data Integrity Protection.

4) Confidentiality Protection of Data streams.

As such it fits into the ETSI TISPAN requirements for IPTV service protection.

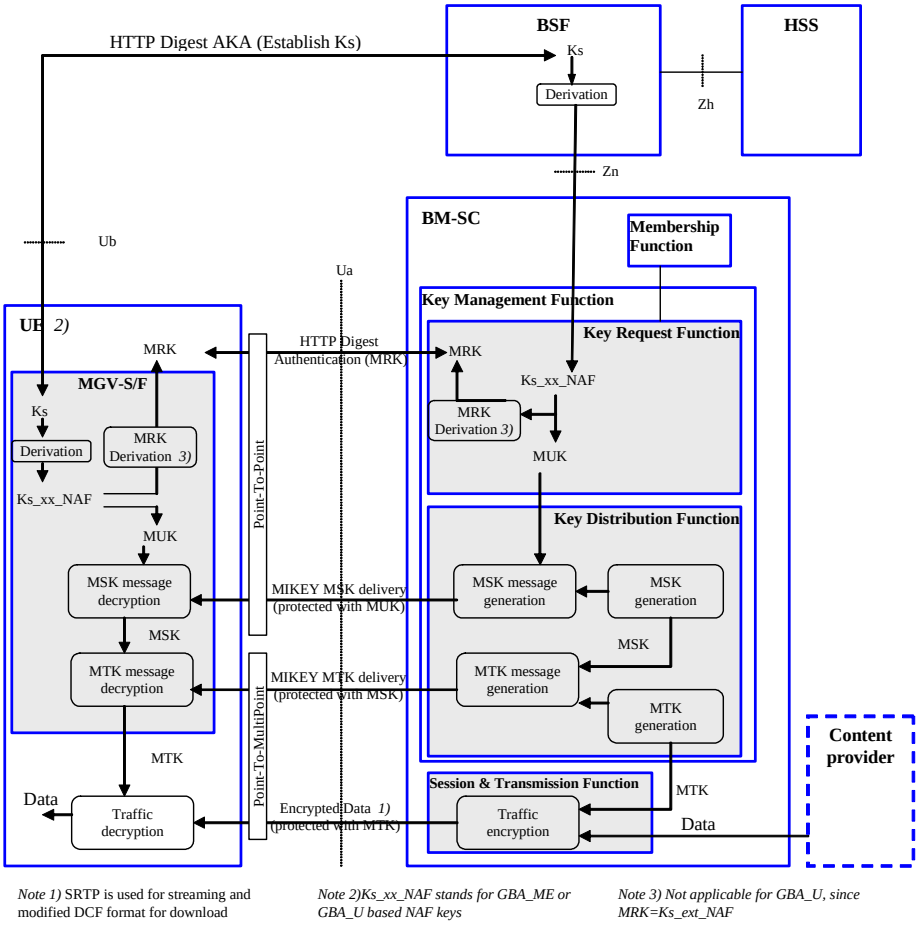


Figure A.7: MBMS Security Architecture

BM-SC is a source of MBMS data and is BM-SC responsible for:

1) establishing shared secrets with the UE using GBA;
2) authenticating the UE with HTTP digest authentication mechanism;
3) registering and de-registering UEs for MBMS User Services;
4) generating and distributing the keys necessary for MBMS security to the UEs with MIKEY protocol;
5) applying the appropriate protection to data that is transmitted as part of a MBMS User Service;
6) BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish MBMS bearer with the GGSN.

NOTE: Only the bullet 6 seems to be different to IPTV R3, where the bearer is established through the MCF and MDF.

A.4.1.2 Functional entities in BM-SC and their matching to ETSI TISPAN

BM-SC as source of MBMS Data consists of the following functional entities:

1) Key Management function;
2) Membership Function; and
3) Session and Transmission Function.

A.4.1.2.1 Key Management Function

Key Management Function consists of the:

- Key Request Function; and
- Key Distribution Function.

The **Key Request Function** is responsible for:

1) Bootstrapping initiation.
2) Bootstrapping re-negotiation.
3) HTTP digest authentication.
4) MRK derivation.
5) MBMS User Service Registration procedure.
6) MBMS User Service Deregistration procedure.
7) MSK request procedure.

During the Bootstrapping initiation and re-negotiation the Key Request Function retrieves GBA keys from the BSF. In the next step the user authenticates and authorises through HTTP digest authentication at the BM-SC at the MBMS-application itself. During this authentication the user uses the shared secret Ks, agreed with the BSF in a previous step for the derivation of the request key (MRK=MBMS Request Key), with which the user eventually requests access to MBMS. With MRK the user gains access to the MBMS service. With MRK the subsequent key, the MBMS User Key (MUK) can be derived. MUK is then used for the encryption of the MBMS Service Key MSK, which is performed in the Key Distribution Function.

The **Key Distribution Function** is responsible for:

1) Generation of the MBMS Service Key (MSK), used for the encryption of the MBMS Transport Key.
2) Generation and delivery of the MSK message to the UE in point-to-point manner.
3) Generation of the MBMS Transport Key (MTK), used for the data stream encryption.
4) Encryption of the MTK with the MSK.
5) Generation and delivery of the MTK message to chosen UEs, members of the multicast group. Within this message, the MTK is encrypted with MSK. This delivery happens in point-to-multipoint manner.

A.4.1.2.2 Session and Transmission Function

For more information see TS 126 346 [i.35].

Session transmission function is responsible for:

1) Traffic Encryption.
2) Session generation.
3) Scheduling of session transmissions and retransmissions.
4) Identification of sessions.
5) QoS of Transmission.
6) Triggering of bearer level functions.

The traffic encryption of the Session and Transmission Function in ETSI TISPAN's IPTV is performed through the Service Encryption.

NOTE 1: Better: "transport protection"?) Function.

NOTE 2: The other functionalities of session and transmission function could be covered best with the SCF and the MCF.

A.4.2 Using MBMS as IPTV R3 Protection Mechanism

A.4.2.1 General Overview

In short, the following steps are necessary to get access to the IPTV service:

1) perform authentication at IMS layer;

2) request IPTV-service;

3) derive session key for this service;

4) authorize at the IPTV-service level;

5) get individual customer long term service key for protected delivery of IPTV program-specific short term transport key;

6) get program-specific short term transport key;

7) encrypt and decrypt the multicast media stream.

These steps are shown in figure A.8.

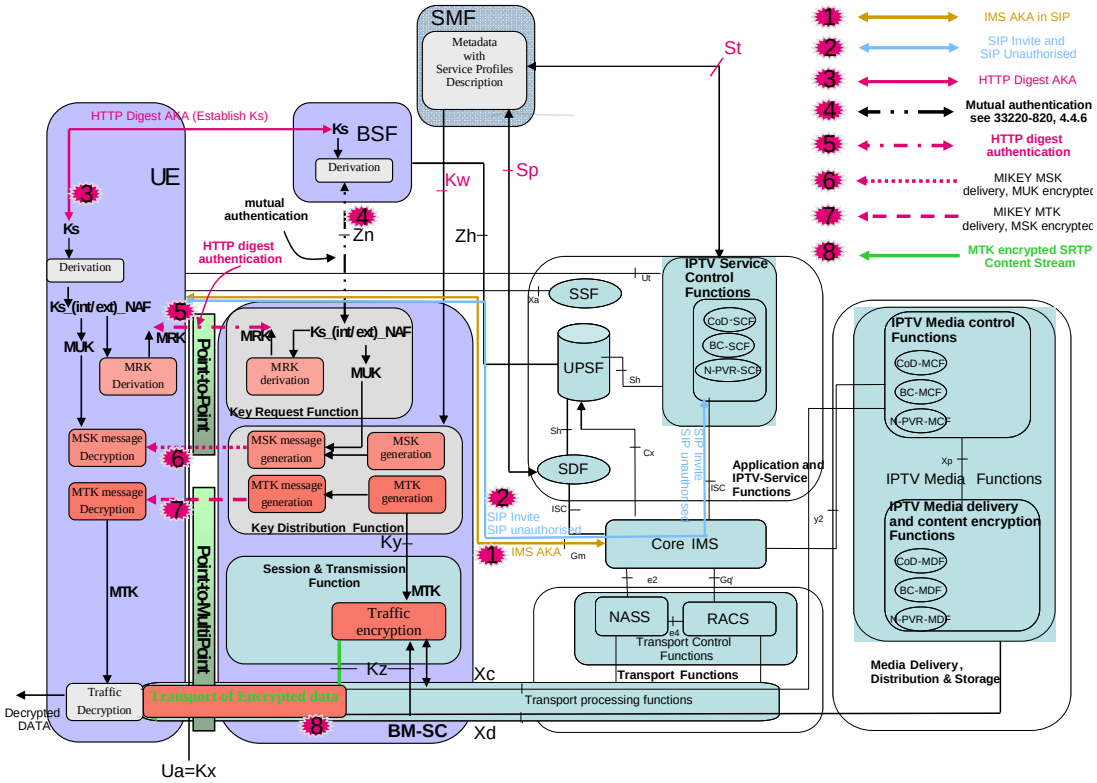


Figure A.8: MBMS and ETSI TISPAN IMS-based IPTV combined for Multicast IPTV service protection

Communication between the UE and the IPTV-Application performing service protection:

1) UE and the IMS core perform mutual authentication with IMS AKA.

2) UE sends SIP Invite to the SCF over Core IMS. SCF makes a look up at the user profiles in the SMF, sees that the user is not authorised and sends SIP Unauthorised back to the user over Core IMS.

3) UE authenticates with HTTP Digest AKA at the BSF and derives session key Ks necessary for the authorization at the IPTV-Service and gets from BSF a B_TID (Bootstrapping Transaction ID) for the subsequent communication with the NAF=BM-SC. With B_TID UE requests once again the NAF=BM-SC for the IPTV-Service.

4) With B_TID NAF=BM-SC requests BSF for UE's credentials. BSF proofs if NAF_BM-SC is authorised to make the request. Mutual authentication takes place between NAF=BM-SC and BSF (for further mutual authentication details see 33220-820, 4.4.6). As result, NAF=BM-SC gets from the BSF Ks_(int/ext)_NAF and UE's GUSS (UE's user profiles).

5) UE authorizes at the NAF= BM-SC (the IPTV service itself) with HTTP Digest Authentication.

6) BM-SC generates through MIKEY the long term service key (MSK) related to specific customer and sends it within the MSK Message to the customer in point-to-point manner.

7) BM-SC generates through MIKEY the short term transport key (MTK) and sends it to customers in point-to-multipoint manner.

8) The Media stream will be encrypted by the session and transmission function and distributed to the customer with SRTP. The Customer uses his MUK which is derived from the Session Key Ks to decrypt his MSK and subsequently his MSK to decrypt the MTK. With the MTK the customer is able to decrypt the encrypted SRTP stream.

A.4.2.2 Service Protection Processes for ETSI TISPAN IMS-based IPTV R3 described in detail

If MBMS User Service information indicates via User Service Discovery / Announcement procedures to the UE that the service is protected, the user registers to the MBMS User Service. Registration is required to ensure that the UE receives the necessary MSK updates.

Step 1: UE and the IMS core perform mutual authentication with IMS AKA. For further details see TS 133 203 [i.41] (Access Security for IP-based Services).

Step 2: SDF and SSF perform service announcement. For IPTV-service, pull or push, UE contacts the Session Control Function with SIP "Invite" over Core IMS. SCF makes a look up at the user profiles in the SMF, sees that the user is not authorised and sends "SIP unauthorised" back to the user over Core IMS:

Alternative 1: In case SCF (and SMF) does not have UE credentials in a running session available, it requests UE to authenticate with "SIP unauthorized" with BSF. In this case, for the further communication the UE uses the Gm interface. The SCF waits for UE's answer (using SIP) to obtain a B_TID to be able to request BSF for user's credentials (The communication between the SCF and BSF is described in step 4).

Alternative 2: In case SCF (as SMF) does not have UE credentials in a running session available, it requests UE to authenticate with "SIP Notify" with BSF. In this case, for the further communication the UE uses the Ut interface. Then, it waits for UE's answer (using HTTP) to obtain a B_TID to be able to request BSF for user's credentials (communication between the SCF and BSF is described in step 4).

Step 3: Establishment of the first stage User Root Key, the Ks between UE and BSF:

1) Getting SIP "Unauthorised" from SCF, UE request now an authentication with BSF (which takes the role of a registrar for NGN-services). If BSF does not have UE's credentials available, it requests UE's Profiles (GUSS=GBA User Security Settings) with UE's Authentication Vector (AV) from UPSF (HSS).

NOTE 1: The BSF recognises from the structure of the "username" parameter (see clause B.4 in TS 133 220 [i.11]) whether a TMPI or an IMPI was sent. If a TMPI was sent the BSF looks up the corresponding IMPI in its local database. If the BSF does not find an IMPI corresponding to the received TMPI it returns an appropriate error message to the UE. The UE then deletes the TMPI and retries the request using the IMPI.

2) The AV is the basis for the mutual authentication.

3) Upon successful mutual authentication UE and BSF have now the authentication vector (AV) with the attributes RAND||AUTN||XRES||CK||IK.

4) Ks=CK|IK is established between the UE and BSF as shared secret.

5) BSF sends to UE OK with the Bootstrapping Transaction ID ((B-TID) which functions now as the user-name for the IPTV access) together with the key lifetime of the agreed key Ks.

6) Both the UE and the BSF now use the Ks to derive the key material Ks_(int/ext)_NAF.

In case of GBA_ME, Ks_NAF is computed as KS_NAF = KDF (Ks, "gba_me", RAND, IMPI, NAF_Id), where KDF is the Key Derivation Function as specified in annex B of TS 133 220 [i.11]. For KDF to be consistent, prerequisites have to be fulfilled, as specified in clause 4.5.2 of TS 133 220 [i.11].

In case of GBA_U, Ks_ext_NAF is computed as KS_ext_NAF = KDF (Ks, "gba_me", RAND, IMPI, NAF_Id), and Ks_int_NAF is computed as Ks_int_NAF = Ks_int_NAF = KDF(Ks, "gba-u", RAND, IMPI, NAF_Id), where KDF is the key derivation function as specified in annex B of TS 133 220 [i.11].

7) The UE and the BSF store Ks with associated B-TID until the lifetime of Ks has expired.

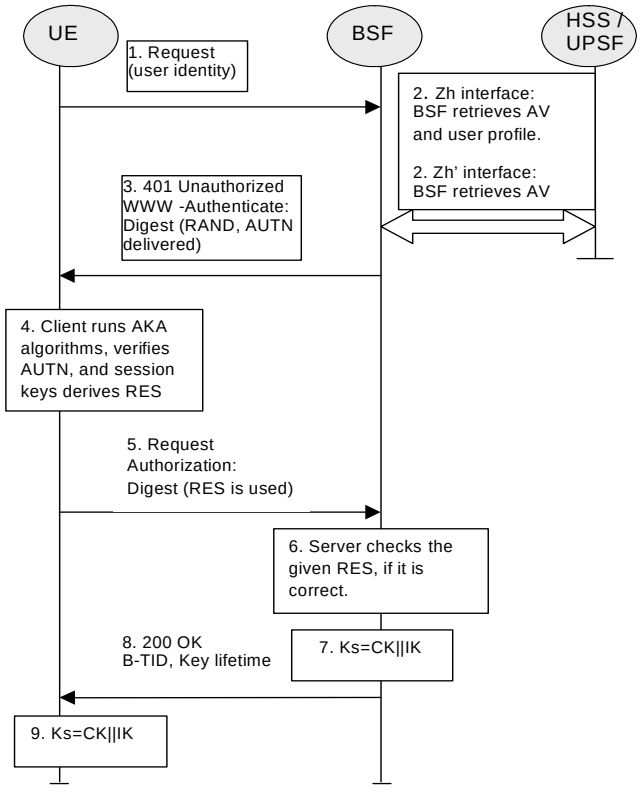


Figure A.9: Ks agreement between UE and BSF

Step 4: NAF=BM-SC (and with it the IPTV-Application) requests UE's credentials from the BSF. Both parts NAF=BM-SC and BSF authenticate mutually.

NOTE 2: The IPTV-application itself consists of the entities SCF, SMF, and BM-SC. If embedded in the Generic Bootstrapping Architecture the IPTV-application functions as the NAF.

NOTE 3: The link between them is protected either through a trusted link if in the same security domain or though IPSec or TLS, if in different security domains (see TS 133 220 [i.11], clause 4.4.6).

1) Having got the B-TID, UE again starts communication with the IPTV application over the reference point Gm and supplies the B-TID to the SCF (e.g. over "SIP notify"). SCF forwards the job to the SMF and the SMF forwards the B-TID to the Key Request Function of the BM-SC. The Key Request Function in BM-SC in now able to retrieve the corresponding keys from the BSF.

2) Key request function in BM-SC starts communication over reference point Zn with BSF:

   a) It requests key material corresponding to the B-TID (supplied by the UE).

   b) Key Request Function requests IPTV-specific USSs from BSF which the request received from UE may access.

3) With the key material request, the Key Request Function (which is within the GBA the NAF) supplies a NAF-Id (which includes the SCF's FQDN that the UE has used to access this NAF and the Ua security protocol identifier). The BSF is able to verify that this NAF (in the function of the IPTV application) is authorized to use that FQDN.

4) With NAF_Id and B-TID, the BSF creates a session key Ks_(int/ext)_NAF which is linked to the NAFs identity and supplies it to the Key Request Function, as well as the bootstrapping time and the lifetime of that key (and some more attributes belonging to user security settings, USS).

5) Key Request Function stores the Ks_(int/ext)_NAF, Bootstrapping time, lifetime during the entire session. The purpose of the bootstrapping is now fulfilled as it enabled UE and the IPTV-Application (BM-SC with session and transmission function) to use reference point Ua in a secure way.

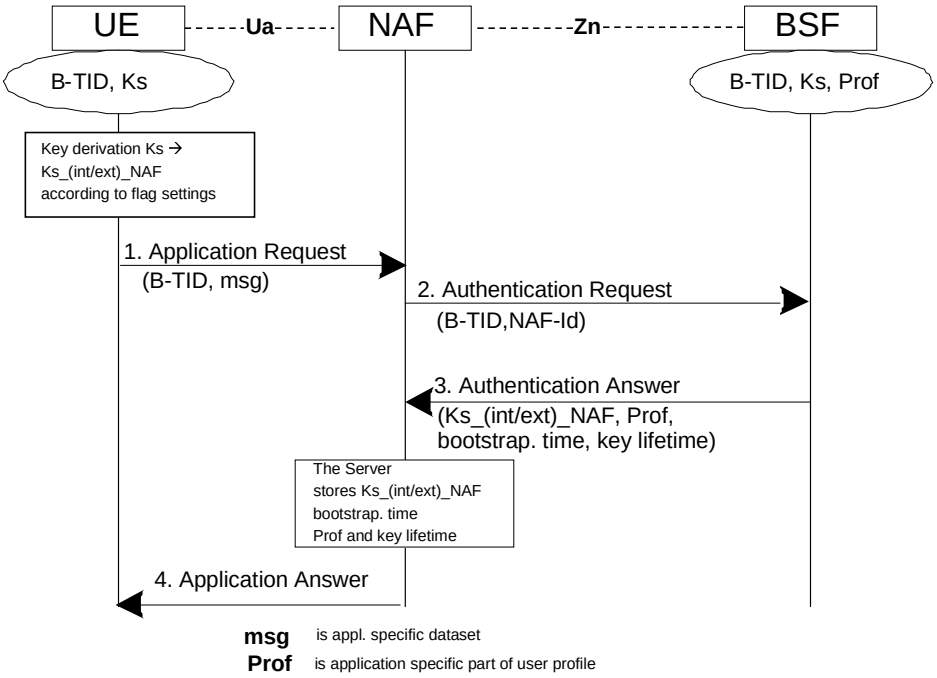


Figure A.10: Ks_(int/ext)_NAF establishment between NAF=BM-SC and BSF

Step 5: UE's authentication and authorisation at the IPTV-Application with HTTP Digest AKA and the use of MUK (MBMS User Key).

As next, the UE authenticates for the IPTV-Application at the MB-SC. First, he uses Ks previously agreed with BSF for the derivation of Ks_(int/ext)_NAF with the B-TID and NAF_Id. As next he derives MBMS Request Key (MRK). (BM-SC possesses the same key material sent from BSF and is able to authenticate the UE for the IPTV-usage.)

1) HTTP Digest AKA (see RFC 2617 [i.23]) is performed between the UE and BM-SC.

2) The purpose of the MRK (MBMS Request Key) is to authenticate the UE to the BM-SC and vice versa when performing UE's access to BM-SC.

3) Two methods can be used for the MRK derivation in case of the UE: GBA_ME (using SIM/GBA-unaware UICC), GBA_U (using GBA-aware UICC).

4) In case of GBA_ME the MRK is Ks_NAF in case of GBA_U the MRK is Ks_ext_NAF (concerning the key format see TS 124 109 [i.37]).

5) Additionally to RFC 2617 [i.23] the following adaptations apply to HTTP digest:

   a) the B-TID as specified in TS 133 220 [i.11] is used as username;

   b) MRK (MBMS Request Key) is used as password.

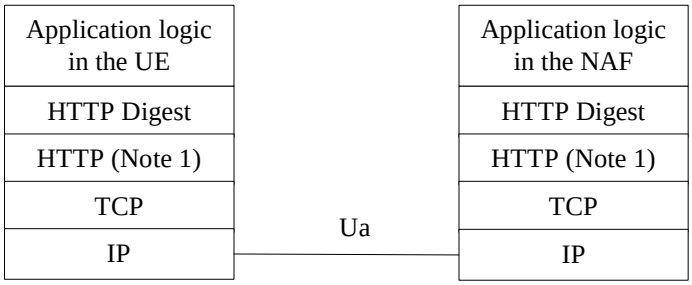


Figure A.11: The protocol stack of the Ua interface when HTTP Digest authentication is used

As a result of a GBA_U run, the BM-SC will share a key Ks_ext_NAF with the UE and share a key Ks_int_NAF with the UICC.

In case the UICC supports MBMS then this key Ks_int_NAF is used by the BM-SC and the UICC as the key **MUK** (MBMS User Key) to protect MSK (MBMS Service Key) deliveries to the UICC. The key Ks_ext_NAF is used as the key MRK (MBMS Request Key) within the protocols.

In case the UICC does not support MBMS then the key Ks_int_NAF can not be used for ME based key management, but the key Ks_ext_NAF is used as **MUK** and the key MRK is derived from the key Ks_ext_NAF by the BM-SC and the ME as specified in TS 133 246 [i.10], annex F.

A run of GBA_ME or 2G GBA results in the BM-SC sharing a key Ks_NAF with the UE. Both the BM-SC and the UE use the key Ks_NAF as MUK. The key MRK is derived from the key Ks_NAF by the BM-SC and the UE as specified in TS 133 246 [i.10], annex F. The key MUK is used to protect MSK deliveries to the ME (see TS 133 246 [i.10], clause 6.2). The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within clause 6.2.

The MUK and MRK are identified by the combination of B-TID and NAF-ID (without the Ua security protocol identifier) in the UE and by B-TID in the BM-SC, where B-TID and NAF-ID are defined as specified in TS 133 220 [i.11].

Step 6 and 7: Generation of MBMS Service Key (MSK) and MBMS Transport Key.

For detailed information see TS 133 246 [i.10], clauses 6.3.2.2, 6.3.2.3 and 6.5.

When a UE detects that it needs the MSK(s) for a specific MBMS User Service, the UE should try to get the MSKs that will be used to protect the data transmitted as part of this MBMS User Service.

UE request for MSK

The MSK is generated by the Key Distribution Function.

MSKs is carried in MIKEY messages. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

BM-SC delivers MSK to the user.

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.2, 6.4.3 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the UE on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5. MIKEY is used with pre-shared keys as described in RFC 3830 [i.38].

As MIKEY is used in a key transport mode, the key derivation function as defined in section 4.1.4 of RFC 3830 [i.38] is used for MIKEY internal keys and MIKEY internal salt. The pre-shared key used for transmission of MSK is the MUK, and the pre-shared key used for transmission of MTK is the MSK.

Once the MSK is in place in the UE, the UE can make use of the MTK messages sent by the BM-SC over MBMS bearer. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret.

With MTK the Multicast media stream is encrypted. Only users being able to use the right MTK are able to decrypt the Multicast media stream.

Step 8: The session and encryption function uses MTK to encrypt the SRTP media stream and forwards encrypted media stream to the UE.

A.5 GBA and ETSI TISPAN NGN Architecture

MBMS is based on GBA. Therefore it is necessary to analyse how GBA fits into TISPAN NGN functional architecture.

Concerning the functionalities the GBA Architecture fits with the majority of its functional elements to ETSI TISPAN functional Architecture.

Functional entities with nearly the same functionalities are:

- NAF (GBA) and Application Server (ETSI TISPAN).
- HSS (GBA) and UPSF (ETSI TISPAN) as Subscriber Database.
- SLF (GBA) connected to BSF and SLF (TIPSPAN) connected to I/S-CSCF.
- UE as User Equipment.

Different or missing functional Entities:

Bootstrapping Server Function (BSF) at TISPAN NGN Architecture.

Reference Points:

Looking at the both architectures, the Reference Points between the functional entities are completely different. The different Reference Points are:

TISPAN:

Sh: AS - UPSF.

Cx: UPSF - I/S-CSCF.

ISC: AS - I/S-CSCF.

Dx: SLF - I/S-CSCF.

Dh: AS - SLF.

GBA:

Ua: UE - NAF.

Ub: UE - BSF.

Zn: BSF - NAF.

Zh: BSF - HSS.

Dz: BSF - SLF.

Adaptation of GBA to ETSI TISPAN NGN Architecture.

From their logical model, the adaptation of the GBA architecture to ETSI TISPAN NGN architecture would require to add BSF as functional entity and extend the following functional entities with additional reference points as follows:

Ua: UE - NAF=AS.

Ub: UE - BSF.

Zn: BSF - NAF=AS.

Zh: BSF - HSS=UPSF.

Dz: BSF - SLF.

The SLF in GBA (see TS 133 220 [i.11], V8.20, page 16):

- is queried by the BSF in conjunction with the Zh interface operation to get the name of the HSS containing the required subscriber specific data;
- is accessed via the Dz interface by the BSF.

The SLF is not required in a single HSS environment. Use of SLF is not required when BSF are configured/managed to use pre-defined HSS.

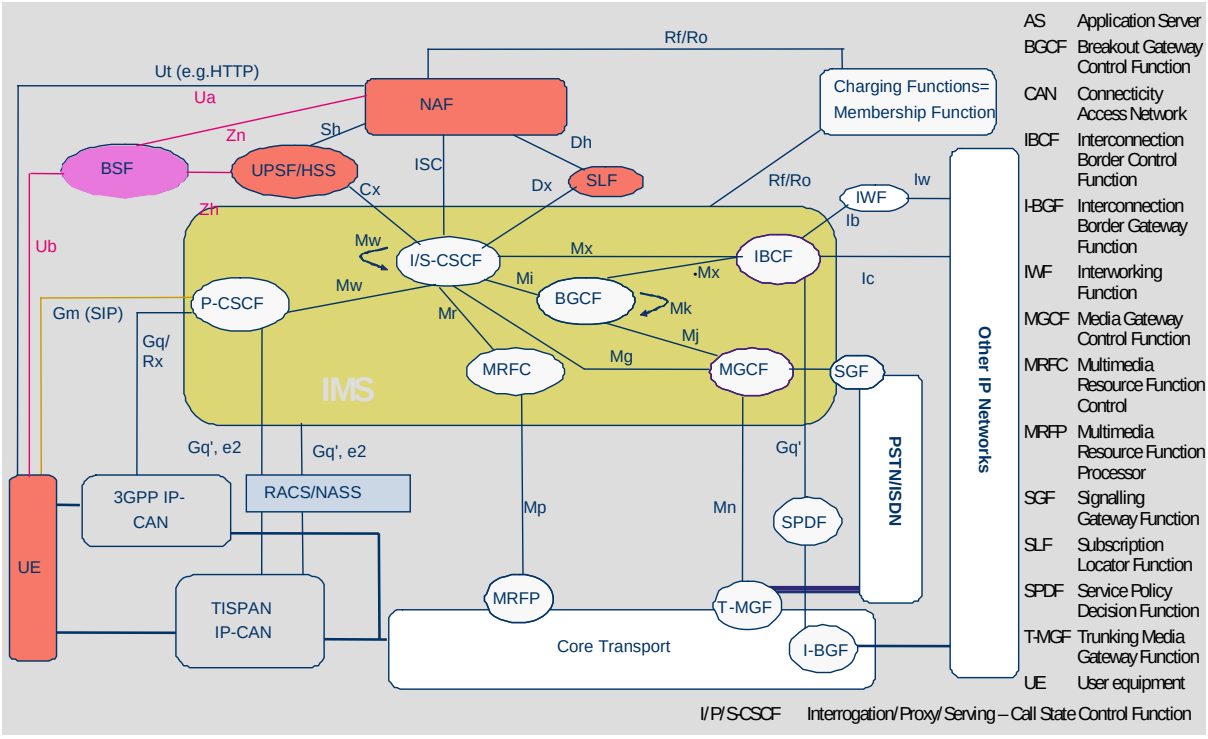


Figure A.12: GBA Architecture adapted to ETSI TISPAN NGN Functional Architecture

The red coloured entities in figure A.12 are the once with very similar functionalities at both, 3GPP and TISPAN.

The pink coloured entity, the BSF, is present only at the GBA.

History

Document history		
V3.1.1	February 2011	Publication