



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1193

(10/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

Key management framework for secure Internet protocol television (IPTV) services

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Recommendation ITU-T X.1193

Key management framework for secure Internet protocol television (IPTV) services

Summary

This Recommendation describes requirements and architecture for key management, including key hierarchy for unicast and multicast IPTV services in the IPTV context. It also specifies key management for downloadable service and content protection (SCP) if deployed. This Recommendation does not include any other key management architecture and mechanisms in Recommendation ITU-T X.1191.

Keywords

Authentication, Authorization, Content Protection, Encryption, Rights Management, Scrambling, Security, Service Protection

.....

Table of Contents

1	Scope	1
2	References.....	1
3	Definitions.....	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	4
4	Abbreviations and acronyms	5
5	Conventions	6
6	Introduction.....	7
6.1	IPTV general architecture and content protection architecture	7
6.2	IPTV general architecture and content protection architecture	7
6.3	Reference model of group key management	9
6.4	Grouping of TDs	10
7	Requirements for the key management scheme.....	10
7.1	Requirements for key management described in ITU-T X.1191	10
7.2	General requirements for key management.....	11
7.3	Functional requirements for key management	12
7.3.1	<i>Functional key management requirements for unicast IPTV service</i>	<i>12</i>
7.3.2	<i>Functional key management requirements for multicast IPTV service</i>	<i>13</i>
7.3.3	<i>Functional key management requirements for the downloadable SCP scheme</i>	<i>13</i>
7.3.4	<i>Functional key management requirements for the user possessing multiple IPTV terminals (N-screens).....</i>	<i>15</i>
8.1	Key management scheme for unicast-based IPTV service.....	15
8.1.1	<i>Overview</i>	<i>15</i>
8.1.2	<i>Bootstrapping layer</i>	<i>16</i>
8.1.3	<i>Key stream layer</i>	<i>16</i>
8.1.4	<i>Traffic protection layer</i>	<i>16</i>
8.1.5	<i>Procedure of key management for the multicast IPTV service</i>	<i>16</i>
8.2	Key management scheme for multicast IPTV service.....	17
8.2.1	<i>Overview</i>	<i>17</i>
8.2.2	<i>Bootstrapping layer</i>	<i>17</i>
8.2.3	<i>Key management layer</i>	<i>18</i>
8.2.4	<i>Key stream layer</i>	<i>18</i>
8.2.5	<i>Traffic protection layer</i>	<i>18</i>
8.2.6	<i>Procedure of key management for the multicast IPTV service</i>	<i>18</i>
8.3	Key management scheme for a downloadable SCP scheme	18
8.3.1	<i>Introduction</i>	<i>18</i>
8.3.2	<i>Interactive key management for a downloadable SCP scheme</i>	<i>18</i>
8.3.3	<i>Trust Authority-based key management for the downloadable SCP scheme.....</i>	<i>21</i>
APPENDIX I	Multimedia Internet Keying.....	37
I.1	Overview of MIKEY	37
I.2	Protocol operation	38
I.2.1	<i>Pre-shared key</i>	<i>38</i>
I.2.2	<i>Public key encryption</i>	<i>38</i>
I.2.3	<i>Diffie-Hellman key exchange.....</i>	<i>39</i>
APPENDIX II	Extensible authentication protocol.....	40
II.1	EAP-AKA	40
II.2	EAP-PSK.....	40

II.3 EAP-TLS 41

II.4 EAP-FAST 41

II.5 EAP-IKEv2 42

II.6 EAP-TTLS.....42

II.7 PEAP 42

Bibliography.....44

.....

Recommendation ITU-T X.1193

Key management framework for secure Internet protocol television (IPTV) services

1 Scope

This Recommendation describes the requirements and architecture for key management, including key hierarchy for unicast and multicast IPTV services in the IPTV context. It also specifies the key management for downloadable SCP if deployed. This Recommendation does not include any other key management architecture and mechanisms in Recommendation ITU-T X.1191.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly.

A reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.509]	Recommendation ITU-T X.509 (2005) ISO/IEC 9594-8:2005, <i>Information technology –Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.</i>
[ITU-T X.800]	Recommendation ITU-T X.800 (1991), <i>Security architecture for Open Systems Interconnection for CCITT applications.</i>
[ITU-T X.805]	Recommendation ITU-T X.805 (2003), <i>Security architecture for systems providing end-to-end communications.</i>
[ITU-T X.1191]	Recommendation ITU-T X.1191 (2009), <i>Functional requirements and architecture for IPTV security aspects.</i>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 access control** [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
- 3.1.2 authentication** [ITU-T X.800]: See Data Origin Authentication and Peer-Entity Authentication.
- 3.1.3 authorization** [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.
- 3.1.4 accessibility** [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.
- 3.1.5 acquisition** [ITU-T X.1191]: The process of obtaining content by the end user.

NOTE – For content with accessibility features, this means that the content will be available in a form that can be used by the end user.
- 3.1.6 conditional access** [ITU-T X.1191]: The function served by a conditional access system; often used as an abbreviation for conditional access system.

- 3.1.7 conditional access system** [ITU-T X.1191]: A component of a service and content protection system, the purpose of which is to prevent unauthorized (unentitled) access to a service or to content.
- 3.1.8 confidentiality** [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- 3.1.9 content protection** [ITU-T X.1191]: Ensuring that an end user can only use the content that they have already acquired, in accordance with the rights that they have been granted by the rights holder. Content protection includes protecting contents from illegal copying and distribution, interception, tampering, unauthorized use, etc.
- 3.1.10 data origin authentication** [ITU-T X.800]: The corroboration that the source of data received is as claimed.
- 3.1.11 denial of service** [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.
- 3.1.12 digital rights management** [ITU-T X.1191]: A synonym for service and content protection or content protection, depending upon the context of use.

NOTE – In this Recommendation, the terms “service” and “content protection” are used instead of digital rights management.

- 3.1.13 digital signature** [ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography) of a data unit, that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient.
- 3.1.14 entitlements** [ITU-T X.1191]: Rights granted to a subscriber by a contract with an IPTV service provider.
- 3.1.15 forward secrecy** [b-NIST SP 800-120]: A compromise of long-term private or pre-shared secret keys does not enable an adversary to compute the *MK* generated in previous EAP executions.
- 3.1.16 group controller and key server** [IETF RFC 3740]: Entity and functions that are responsible for issuing and managing cryptographic keys used by a multicast group.
- 3.1.17 implicit key authentication** [b-NIST SP 800-120]: A property of key establishment protocols that provides assurance to one protocol participant that the other protocol participant is the only other party that could possibly be in possession of the correct established key.
- 3.1.18 initiator** [b-IETF RFC 3830]: The initiator of the key management protocol, not necessarily the initiator of the communication.
- 3.1.19 integrity** [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.
- 3.2.20 key** [ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.
- 3.2.21 key confirmation** [b-NIST SP 800-120]: A procedure to provide assurance to one party (the key confirmation recipient) that another party (the key confirmation provider) actually derived the correct secret keying material as a result of a key establishment.
- 3.2.22 key derivation** [b-NIST SP 800-120]: The process that derives keys from another key or from a secret output value, called shared secret, obtained through a key establishment procedure.

- 3.2.23 key establishment** [b-NIST SP 800-120]: A procedure, conducted by two or more participants, which culminates in the derivation of keying material by all participants (see keying material). Key establishment can be based on pre-shared keys or on public key-based schemes.
- 3.2.24 key hierarchy** [b-NIST SP 800-120]: A tree structure that represents the relationship of different keys. In a key hierarchy, a node represents a key used to derive the keys represented by the descendent nodes. A key can only have one precedent, but may have multiple descendent nodes.
- 3.2.25 key management** [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.
- 3.1.26 keying material** [b-NIST SP 800-120]: The output of a key derivation function, a segment of which, with the required length, can be used as a cryptographic key.
- 3.1.27 key transport** [b-NIST SP 800-120]: A procedure to deliver a key from one entity to another entity in a protected manner. In this Recommendation, key transport refers to key delivery from the EAP server to another entity, for example, to an authenticator.
- 3.1.28 masquerade** [ITU-T X.800]: The pretense by an entity to be a different entity.
- 3.1.29 peer-entity authentication** [ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.
- 3.1.30 policy server** [b-IETF RFC 3740]: Entity and functions that are responsible for creating and managing security policies specific to a multicast group.
- 3.1.31 privacy** [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- 3.1.32 repudiation** [ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.
- 3.1.33 responder** [b-IETF RFC3830]: The responder in the key management protocol.
- 3.1.34 rights** [ITU-T X.1191]: One or more legal or business entitlements to use or employ content, e.g. to view, record, redistribute content.
- 3.1.35 rights expression** [ITU-T X.1191]: The syntactic embodiment of rights in a concrete form.
- 3.1.36 security label** [ITU-T X.800]: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- NOTE – The marking and/or binding may be explicit or implicit.
- 3.1.37 security policy** [ITU-T X.800]: The set of criteria for the provision of security services.
- 3.1.38 scrambling algorithm** [ITU-T X.1191]: An algorithm used in a scrambling (encryption) or descrambling (decryption) process.
- 3.1.39 security association** [b-IETF RFC 3740]: A set of policy and cryptographic keys that provide security service to network traffic that corresponds to that policy.
- 3.1.40 service** [ITU-T X.1191]: A set of functionality enabled by a provider for end users; for example, providing IP connectivity with managed quality of service, providing an IPTV service, providing a content-on-demand service, etc.
- 3.1.41 service protection** [ITU-T X.1191]: Ensuring that an end user can only acquire a service and, by extension, the content contained therein, that they are entitled to receive. Service

protection includes protecting service from unauthorized access as IPTV contents traverse through the IPTV service connections.

3.1.42 service and content protection [ITU-T X.1191]: A combination of service protection and content protection, or a system or implementation thereof.

3.1.43 terminal device protection [ITU-T X.1191]: Ensuring that a terminal device employed by an end user in the reception of a service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters (e.g. saved keys) not otherwise protected.

3.1.44 threat [ITU-T X.800]: A potential violation of security.

3.2 Terms defined in this Recommendation

This document defines the following terms:

3.2.1 authentication proxy: A server, residing on the IPTV service provider's side, which is responsible for managing a secure downloadable SCP message exchange with SM on the IPTV terminal's side. It authenticates a security module (SM) and acts as proxy for downloadable SCP services. The authentication proxy plays the role of sub-function of the right and key management function.

3.2.2 authentication server: A server that performs the secure downloadable SCP function with SM on the terminal side in the IPTV context.

3.2.3 content key: A key used to protect the IPTV data stream(s).

3.2.4 Key confirmation: A procedure for proving to one entity that another entity establishes the correct secret keying material as a result of key establishment.

3.2.5 key hierarchy: A tree structure that represents the relationship of different keys. In a key hierarchy, a node represents a key used to derive the keys represented by the descendent nodes. A key can only have one precedent but may have multiple descendent nodes.

3.2.6 master key (MK): A key derived from authentication and key management between SM and AP or Authentication server for the secure downloadable SCP.

3.2.7 multicast IPTV service: An IPTV service provided to a sub-group of IPTV users so that content stream is delivered simultaneously to all TDs belonging to the sub-group when transmitted by the SCP function.

3.2.8 multicast-based downloadable SCP scheme: A downloadable SCP scheme that can download the SCP operating code to multiple TDs belonging simultaneously to SLAG.

3.2.9 rekey: A process to change the SCP key so as to limit the amount of data encrypted with the same SCP key.

3.2.10 pairwise master key (PMK): A key derived from the master key shared by SM and AP for the secure downloadable SCP.

3.2.11 pre-shared key (PSK): A key shared in advance by SM and AP or authentication server for the secure downloadable SCP.

3.2.12 security module: A hardware or software module with tamper resistance to perform the download SCP protocol, generate and store keys, and store SCP client data and code. The security module acts as a sub-function of the SCP client on the IPTV terminal.

- 3.2.13 SCP client code:** The software code that performs the SCP client function. It can be downloaded to IPTV TD if the downloadable SCP is deployed.
- 3.2.14 sub-local area group (SLAG):** A multicast group consisting of many TDs that reside in the same physical area or belong to the same logical area.
- 3.2.15 unicast-based downloadable SCP:** A downloadable SCP scheme that can download SCP operating code to a single TD.
- 3.2.16 unicast IPTV service:** A service provided to a single TD so that content stream is delivered to a single TD in the IPTV context when transmitted by the SCP function.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, and Accounting
ACS	Auto-Configuration Server
AES	Advanced Encryption Standard
AP	Authentication Proxy
CAS	Conditional Access System
CDN	Content Delivery Network
CEF	Content Encryption Function
CGK	CK Generation Key
CK	Content Encrypting Key
CM	Counter Mode
CP	Content Protection; Content Provider
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
CS	Crypto Session
CSB	Crypto Session Bundle
DH	Diffie-Hellman
DoS	Denial of Service
DRM	Digital Rights Management
EMM	Entitlement Management Message
ECM	Entitlement Control Message
GCKS	Group Controller and Key Server
HDD	Hard Disk Drive
ID	Identifier
IPTV	Internet Protocol Television
ISP	Internet Service Provider
KMF	Key Management Function

MAC	Message Authentication Code
MCF	Media Control Function
MDF	Media Distribution Function
MIKEY	Multimedia Internet Keying
MK	Master Key
PC	Personal Computer
PK	Public-Key
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PSK	Pre-Shared Key
QoS	Quality of service
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
SA	Security Association
SCK	SCP KeySDP Session Description Protocol
SIP	Session Initiation Protocol
SLAG	Sub Local Area Group
SM	Security Module
SP	Service Protection; Service Provider
SRTP	Secure RTP
TA	Trust Authority
TD	Terminal Device
TTP	Third-party Trust Provider
VoD	Video on Demand
WM	Watermark(ing)

5 Conventions

In this Recommendation:

The keywords “**is required to**” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “**is recommended**” indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords “**is prohibited from**” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “**can optionally**” indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network

operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 Introduction

6.1 IPTV general architecture and content protection architecture

IPTV services are classified into two typical types: a unicast-based service and a multicast-based service. According to the number of senders, a multicast-based service is classified into two types: a 1-to-N service and an M-to-N service. In a 1-to-N multicast-based service, only one sender can transmit a message to multiple TDs, while in an M-to-N multicast-based service, many senders can transmit a message to many TDs. Key management is the process of distributing the keys needed to provide secure IPTV services. To provide various cryptographic keys, key management together with authentication playing a critical role in providing secure IPTV services.

This Recommendation describes the set of requirements and architecture, including key hierarchy, for unicast and multicast IPTV services in the IPTV context. It also includes key management for the downloadable SCP.

6.2 IPTV general architecture and content protection architecture

The general security architecture for IPTV is illustrated in Figure 6-1 below. This general architecture is divided into two primary areas: one considered in-scope for the purpose of considering interoperability based on this document, and another considered out-of-scope. The first area encompasses the End-User, Network Provider, and Service Provider domains, whereas the second area covers the Content Provider domain.

Copyright International Telecommunication Union/ITU Telecommunication Sector

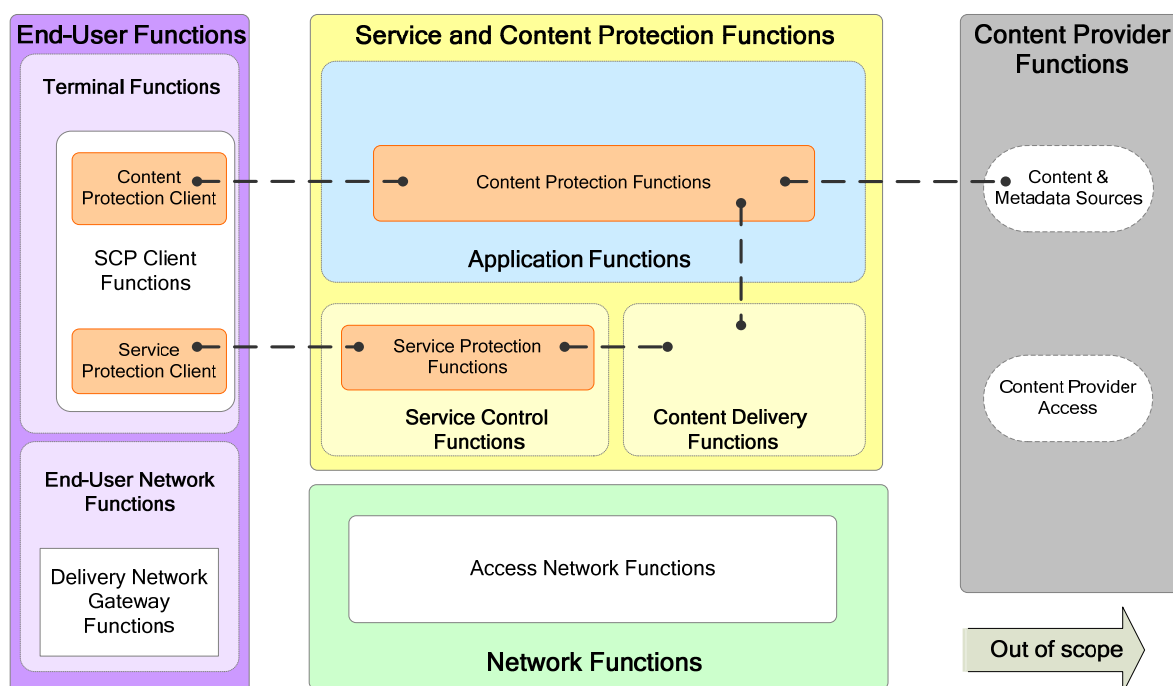
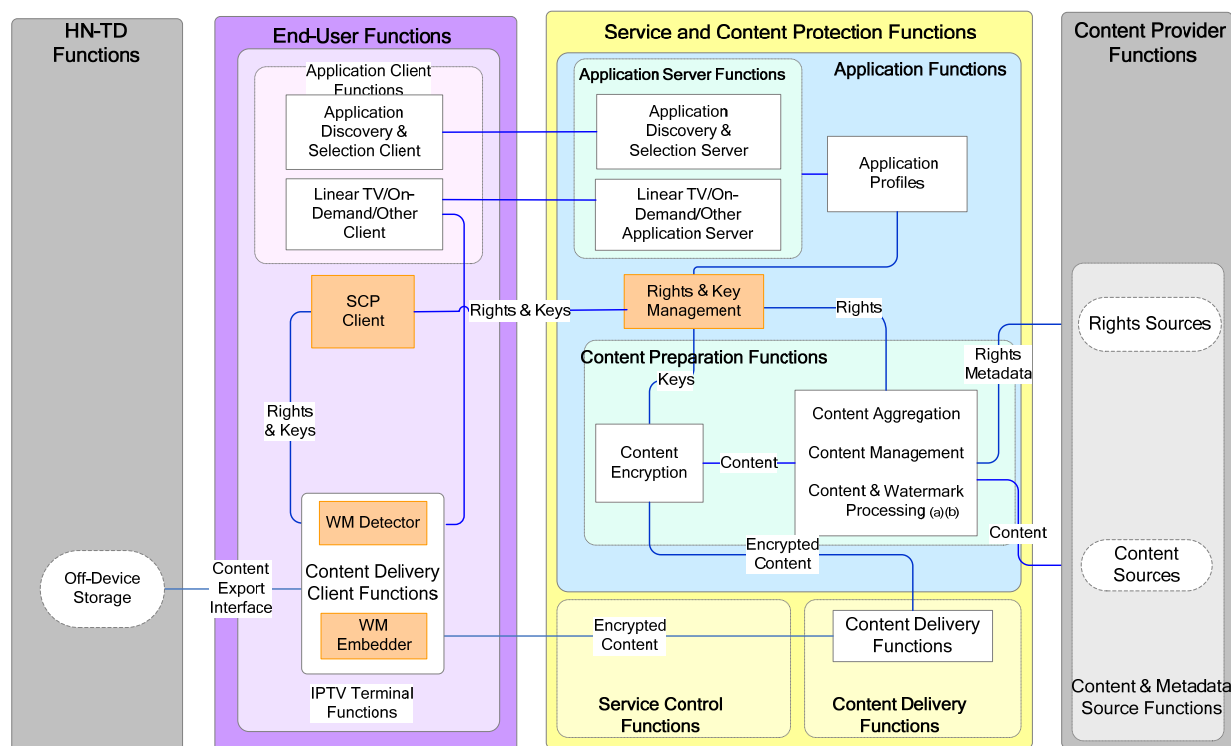


Figure 6-1 – IPTV general security architecture

Content protection architecture for IPTV is depicted in Figure 6-2 below. The primary function of content protection architecture is to delineate the flow and processing of information pertaining to content usage rights, and information required to manage and facilitate such rights.

Ultimately, the rights of content-use originate with the content provider(s); but it should be noted that such rights may be modified (e.g., restricted, or perhaps even expanded) by service provider(s), according to their agreements with content providers and their operational and business policies. From an operational and typical legal perspective, an end user's access and use of content involve the service provider, and not the content provider.



- (a) Optional Watermark Metadata Generation to facilitate downstream watermark embedding
 (b) Optional Watermark embedder to individuate content to networks, servers, and unicast deliveries
 (c) Optional Watermark embedder to individuate multi-cast content instances
 (d) Optional Off-Device Storage: a storage device inside HN-TD.
 (e) Optional Detector for copy protection watermarks

Note: objects in gray color are out scope of IPTV security architecture

Figure 6-2 – IPTV content protection architecture

6.3 Reference model of group key management

The IPTV terminal can be classified into several groups: a group for the multicast IPTV service and a group for the secure downloadable SCP service, etc. This clause only describes the conceptual reference model for group key management. There are four entities: a policy server, a group controller key server (GCKS), a sender, and a receiver. GCKS is an entity responsible for issuing and managing the cryptographic keys used for a specific group; and the Policy Server is an entity responsible for creating and managing security policies for managing groups.

The function of a GCKS, a policy server, and a sender could be part of the rights and key management function in Figure 6-2; and the function of a sender could be part of the SCP client function in Figure 6-2.

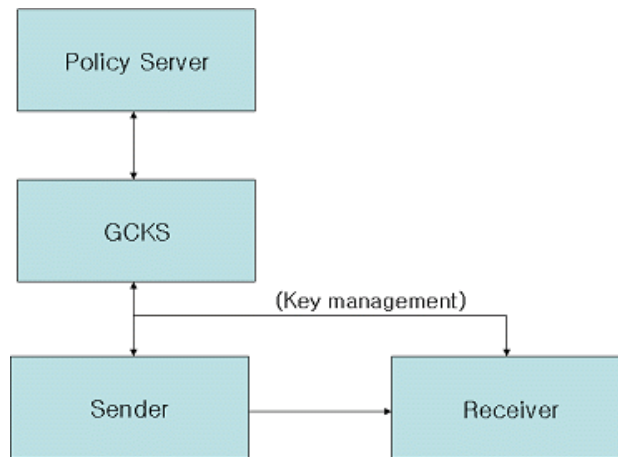


Figure 6-3 – Reference model for group key management

6.4 Grouping of TDs

Any TD may be classified into a sub-local area group. SLAG (Sub-Local Area Group) is a group consisting of many TDs that reside in the same physical area, or belong to a logical area. The communication between the IPTV service provider and all TDs in SLAG is assumed to be multicast-based communication.

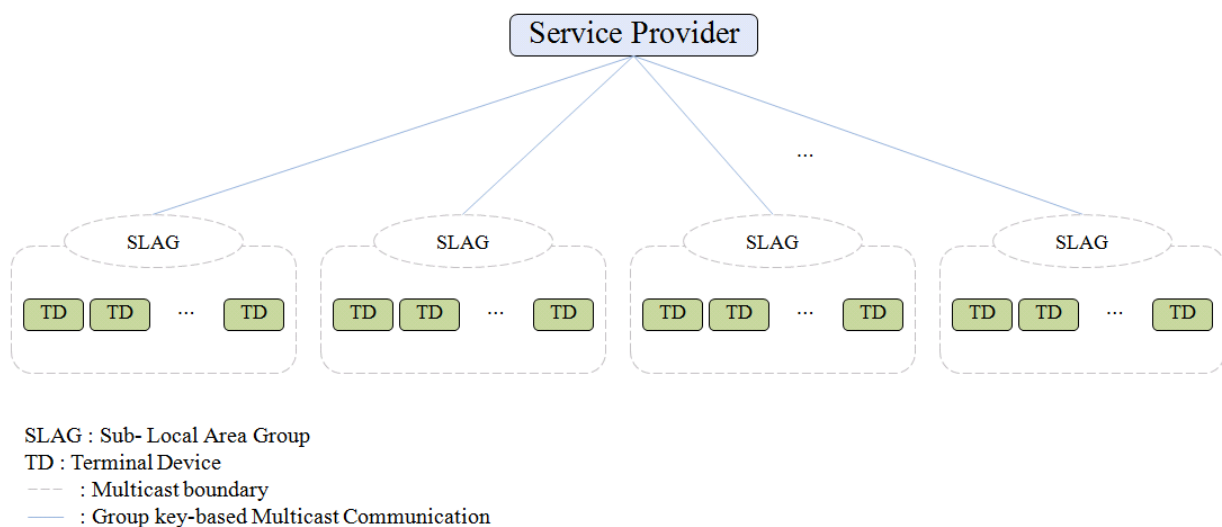


Figure 6-4 – Configuration of SLAG

7 Requirements for the key management scheme

7.1 Requirements for key management described in ITU-T X.1191

In Recommendation ITU-T X.1191, key management is defined as the generation, storage, distribution, deletion, archiving, and application of keys, in accordance with a security policy outlined in clause 3.1.15. In clause 6.3, concerning service security requirements, the following key management requirements are described:

- The IPTV architecture is required to have the ability to use standard key management systems (e.g. MIKE, EMM/ECM) as required for interoperability.
- If the IPTV architecture employs a key management system, then it is required to be designed for scalability, reliability, and interoperability.