

International Telecommunication Union

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**X.1191**

(02/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM  
COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

---

**Functional requirements and architecture for  
IPTV security aspects**

Recommendation ITU-T X.1191



ITU-T X-SERIES RECOMMENDATIONS  
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
<b>IPTV security</b>	<b>X.1180–X.1199</b>
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

*For further details, please refer to the list of ITU-T Recommendations.*

# **Recommendation ITU-T X.1191**

## **Functional requirements and architecture for IPTV security aspects**

### **Summary**

Recommendation ITU-T X.1191 addresses the functional requirements, architecture, and mechanisms dealing with the security aspects of IPTV content, services, networks, terminal devices, and subscribers (end users).

### **Source**

Recommendation ITU-T X.1191 was approved on 20 February 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

### **Keywords**

Authentication, authorization, encryption, IPTV, privacy protection, security, security architecture, scrambling, service and content protection.

## 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 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 2009

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

## CONTENTS

	<b>Page</b>
1 Scope .....	1
2 References.....	1
3 Terms and definitions .....	1
3.1 Terms defined elsewhere .....	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms .....	4
5 Conventions .....	5
6 Security requirements .....	6
6.1 General security requirements .....	6
6.2 Content security requirements .....	6
6.3 Service security requirements.....	8
6.4 Network security requirements.....	10
6.5 Terminal security requirements .....	11
6.6 Subscriber security requirements .....	12
7 Security architecture .....	12
7.1 General security architecture .....	13
7.2 Content protection architecture .....	14
7.3 Service protection architecture .....	17
7.4 Description of functions and functional blocks in IPTV security architectures.....	19
8 Security mechanisms .....	21
8.1 Security mechanisms dealing with content protection .....	21
8.2 Security mechanisms dealing with service protection.....	23
8.3 Security mechanisms dealing with networks protection .....	23
8.4 Security mechanisms dealing with terminal device protection .....	23
8.5 Security mechanisms dealing with subscribers or end users.....	23
Annex A – Subscriber security protection .....	25
A.1 User data protection.....	25
A.2 Parental control, protection of legal minors, access control.....	26
Appendix I – Security threats.....	27
I.1 Security threats model .....	27
Appendix II – Interoperability of SCP .....	30
II.1 Overview of interoperability of SCP .....	30
II.2 Interoperable SCP scenarios.....	30
II.3 Technical areas of SCP interoperability .....	31
II.4 SCP interoperable architectures .....	32
II.5 Scenarios of SCP-B or SCP-IX deployed in TD.....	33

	<b>Page</b>
Appendix III – Example of IPTV content protection process .....	35
Appendix IV – DVB content protection and copy management .....	36
IV.1    Introduction .....	36
IV.2    Definitions .....	36
IV.3    Abbreviations and acronyms .....	37
IV.4    CPCM architecture .....	38
IV.5    CPCM reference model and functional entities.....	39
IV.6    CPCM-authorized domain.....	39
IV.7    CPCM content usage rules .....	40
IV.8    Usage state information metadata .....	40
IV.9    CPCM content .....	40
IV.10   CPCM device.....	40
IV.11   Usage rule and usage state information.....	40
Appendix V – Secure transcodable scheme .....	41
V.1    Overview of the secure transcodable scheme.....	41
Bibliography.....	42

## **Introduction**

IPTV services, content delivered through such services, terminal devices used in processing, and provision of such services require taking into account many security aspects. This Recommendation draws up the requirements, architectural models, functional entities, interfaces, mechanisms, and additional informative background material that describe and address these security aspects.



# Recommendation ITU-T X.1191

## Functional requirements and architecture for IPTV security aspects

### 1 Scope

This Recommendation addresses the functional requirements, architecture, and mechanisms dealing with the security and protection aspects of IPTV content, services, networks, terminal devices, and subscribers. It is anticipated that requirements and relevant functions identified in this Recommendation can be applied appropriately according to the IPTV service and business models which could request different level of security capabilities.

### 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 regularly published. The 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 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture.*

### 3 Terms and definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 access control** [b-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 application** [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

**3.1.3 authentication** [b-ITU-T X.800]: See data origin authentication and peer-entity authentication.

**3.1.4 authorization** [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

**3.1.5 availability** [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

**3.1.6 confidentiality** [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**3.1.7 data origin authentication** [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

**3.1.8 denial of service (DoS)** [b-ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

**3.1.9 digital signature** [b-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.

**3.1.10 elementary stream** [b-ITU-T H.222.0]: A generic term for one of the coded video, coded audio or other coded bit stream in PES packet.

NOTE – PES means a packetized elementary stream.

**3.1.11 functional architecture** [b-ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

**3.1.12 functional entity** [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

**3.1.13 integrity** [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

**3.1.14 key** [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

**3.1.15 key management** [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

**3.1.16 masquerade** [b-ITU-T X.800]: The pretence by an entity to be a different entity.

**3.1.17 network provider** [b-ITU-T Q.1290]: The organization that maintains and operates the network components required for IPTV functionality.

NOTE 1 – A network provider can optionally also act as service provider.

NOTE 2 – Although considered as two separate entities, the service provider and the network provider can optionally be one organizational entity.

**3.1.18 peer-entity authentication** [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

**3.1.19 privacy** [b-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.

**3.1.20 repudiation** [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

**3.1.21 security label** [b-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.

**3.1.22 security policy** [b-ITU-T X.800]: The set of criteria for the provision of security services.

**3.1.23 service provider** [b-ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider can optionally operate a network. A service provider can optionally be a customer of another service provider.

**3.1.24 threat** [b-ITU-T X.800]: A potential violation of security.

## **3.2 Terms defined in this Recommendation**

This Recommendation defines the following terms:

**3.2.1 acquisition:** Process of obtaining content by the end-user.

**3.2.2 content export:** Process of exporting securely the IPTV content from the IPTV terminal to another terminal owned by the user entitled to use it.

**3.2.3 content protection:** Ensuring that an end user can only use the content that he/she already acquired in accordance with the rights granted to him/her by the rights holder; content protection involves protecting contents from illegal copying and distribution, interception, tampering, unauthorized use, etc.

**3.2.4 content tracing:** Process that enables the identification of the (arbitrary) origin of content and/or responsible party (e.g., end user) to facilitate the subsequent investigation in case of unauthorized use of content, e.g., content copying or redistribution.

NOTE – Content-tracing information may be attached to content as either metadata or forensic watermark.

**3.2.5 entitlements:** Referring to the authorization level(s) including conditional access information that can be used by a subscriber to access certain IPTV services in his/her IPTV TD.

**3.2.6 IPTV terminal device (TD) protection:** Ensuring that the TD employed by an end user in the reception of a service can reliably and securely use content, while enforcing the rights of use as granted for such content and in the course of physically and electronically protecting the integrity of TD and confidentiality of the content and critical security parameters (e.g., saved keys) that are not protected.

**3.2.7 linear TV:** A broadcast TV service similar to the classic form of television services provided by cable, terrestrial, and direct-to-the-home satellite operators; here, the program content is transmitted according to a defined schedule and intended for real-time consumption by the end user.

**3.2.8 metadata for watermarking facilitation:** Metadata created to aid subsequent watermarking embedding by downstream devices.

**3.2.9 phishing:** Act of acquiring sensitive or personal information such as username, date of birth, or credit card details by masquerading as a trustworthy entity.

**3.2.10 rights:** Referring to the ability to perform a predefined set of utilization functions for a content item; these utilization functions include permissions (e.g., to view/hear, copy, modify, record, excerpt, sample, keep for a certain period, distribute), restrictions (e.g., play/view/hear for multiple number of times, play/view/hear for certain number of hours), and obligations (e.g., payment, content tracing) that apply to the content and provide the liberty of use as granted to the end user.

**3.2.11 rights expression:** Syntactic embodiment of rights in concrete, formal form.

**3.2.12 SCP end-to-end:** Service and content protection operating mode wherein content is accessed or exchanged by end devices according to the granted rights using a single service and content protection system.

**3.2.13 SCP bridging:** Service and content protection operating mode wherein two or more service and content protection systems are operational on a single device acting as a bridge between these service and content protection systems; content acquired via one service and content protection system can be accessed via another service and content protection system on the bridge according to the granted rights.

**3.2.14 SCP interchange:** A more general service and content protection operating mode involving two or more devices, with each device having one or more operational service and content protection systems; the content acquired by one device through one of its service and content protection systems can be securely transferred to and accessed on another device through a different service and content protection system according to the granted rights.

**3.2.15 scrambling:** Process designed to protect multimedia content; scrambling usually uses encryption technology to protect content.

**3.2.16 scrambling algorithm:** Algorithm used in a scrambling or a descrambling process.

**3.2.17 secure transcodable scheme:** A kind of a security scheme that enables the intermediate network node to perform transcoding without decryption while preserving end-to-end security; this scheme can be executed by combining scalable coding, progressive encryption, and packetizing. The secure transcodable scheme can provide both the confidentiality and message integrity/authentication.

**3.2.18 service protection:** Ensuring that an end user can only acquire a service and the content hosted therein by extension as what he/she is entitled to receive; service protection includes protecting service from unauthorized access as IPTV contents traverse through the IPTV service connections.

**3.2.19 service and content protection:** A combination of service protection and content protection or the system or implementation thereof.

**3.2.20 spoofing:** An activity wherein a forged (spoofed) source (e.g., a person or a computer program) successfully masquerades as a legitimate source by falsifying data and for the purpose of obtaining information and/or obscuring the true source so that the forged source can carry out unauthorized activities such as spreading computer malware (e.g., virus), etc.

**3.2.21 tamper-resistant:** Resistance to tampering by either the personal users/attackers of a product, package, or system with physical/software access to it.

**3.2.22 transcoding:** Process of transforming multimedia content such as images, text, audio, and video from the original format to a different format or quality.

**3.2.23 user privacy protection:** Ensuring that information considered to be private (or confidential) by an end user is kept confidential while remaining subject to mandatory disclosure due to legal processes.

**3.2.24 video signature:** Metadata (or visual feature) for identifying a video content; unlike watermark embedded by manipulating original video contents, video signature is extracted from a video content itself without the risk of quality deterioration.

#### **4 Abbreviations and acronyms**

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, and Accounting
AD	Authorized Domain
CBC	Cipher Block Chaining
CDN	Content Delivery Network
DNG	Delivery Network Gateway
DNGF	Delivery Network Gateway Function
DoS	Denial of Service
ECB	Electric Code Book
ECM	Entitlement Control Message
EMM	Entitlement Management Message
EPG	Electronic Program Guide

HN	Home Network
HN-TD	Home Network Terminal Device
ID	Identifier
IPTV	Internet Protocol Television
MIKEY	Multimedia Internet KEYing
NAT	Network Address Translation
OFB	Output FeedBack
P2P	peer to peer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
REL	Rights Expression Language
SCP	Service and Content Protection
SCP-B	SCP Bridge
SCP-EE	SCP End-to-End
SCP-IX	SCP Interchange
STS	Secure Transcodable Scheme
TD	IPTV-compliant Terminal Device
USB	Universal Serial Bus
VoD	Video on Demand

## 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 Recommendation is to be claimed.

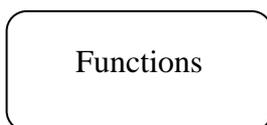
The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

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

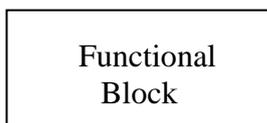
The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the context of IPTV security architecture in this Recommendation:

"**Functions**" are defined as a collection of functionalities. They are represented by the following symbol:



A "**functional block**" is defined as a group of functionalities that has not been further subdivided at the level of detail described in this Recommendation. It is represented by the following symbol:



## 6 Security requirements

### 6.1 General security requirements

- The IPTV architecture is recommended to take into account the influence/impact on performance, quality of service, usability, scalability, and cost constraints on the deployment of security.
- The IPTV architecture can optionally support the content protection of end user-shared content.

### 6.2 Content security requirements

This clause specifies the requirements that individually or collectively deal with content and content protection.

#### *Architecture requirements*

- The IPTV architecture is required to support content protection as defined in clause 3.
- The IPTV architecture is required to support associating content with protection and content management metadata.
- The IPTV architecture is required to support the secure delivery of content protection and content management metadata including usage rights metadata.
- The IPTV architecture is required to support content usage rights metadata that distinguishes between rights of use including rendering (viewing), storage, (re)distribution, and combinations thereof.
- The IPTV architecture is required to support the protection of content distributed simultaneously to a very large number of subscribers (scalability).
- The IPTV architecture is required to support the protection of multicast and/or unicast streaming content.
- The IPTV architecture is required to support securing stored content according to the granted usage right.
- If content tracing is deployed, the IPTV architecture is required to support robust content tracing in an offline (non-real-time) manner (e.g., VoD content).
- The IPTV architecture is prohibited from precluding support for the means of conveyance of content-tracing information (e.g., watermark facilitation metadata).
- The IPTV architecture is prohibited from precluding support for the application of content-tracing technology within the output of TD for the purpose of uniquely identifying a session

(e.g., channel, time/date), TD, and/or network operator. Examples of such content-tracing technology may include visible and invisible information as an option.

- The IPTV architecture is prohibited from precluding the retrieval of all the content-tracing information from the content.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability wherein only authorized user(s) or device(s) is(are) allowed to use the IPTV content even after its(their) transfer to another security system.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to keep identification information such that IPTV content may be identified consistently regardless of which identification schemes are used and to which security system the content is transferred.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to avoid downgrading the level of security when content is transferred to another security system.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability wherein only trusted devices are granted rights.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability so as to provide a secure environment for exchanging service and content protection interoperability data (e.g., authentication information, metadata, key information, etc).
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability such that interoperability is not dependent on specific software or hardware.
- The IPTV architecture is prohibited from requiring the service and content protection mechanism of either side of two interoperating SCP schemes to be specified openly in trying to achieve interoperability.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability that is flexible and extensible to support various business models.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability among multiple security systems using different security mechanisms for the purpose of supporting the seamless time-shifting service (subscribers can store the content and retrieve it later) and place-shifting service (subscribers can view the content anywhere) even with different security mechanisms.
- The IPTV architecture is prohibited from precluding support for service and content protection interoperability to maintain transparency for users.
- The IPTV architecture is prohibited from precluding support for multiple content and service protection mechanisms regardless of specific hardware or software requirements.

#### *Architecture recommendations*

- If IPTV content employs a content-tracing technology, then the tracing technology is recommended to be imperceptible.
- The IPTV architecture is recommended to support robust content tracing in real-time (e.g., broadcast content).
- The IPTV architecture is recommended to support the capability for authenticating and authorizing end users for content sharing services (e.g., content export and content redistribution), if content sharing is supported.

- If the IPTV architecture implementation uses content-tracing technology based on metadata for watermarking facilitation, embedding the relevant metadata in the content elementary stream using provisions for "user data", such as those provided in the specific encoding scheme, is recommended.
- In case one TD or HN-TD within an IPTV-architecture supports multiple content and service protection mechanisms, it is recommended to use one standardized translating function, giving the possibility of linking more than one SCP-system together and translating between them in a consistent way and ensuring the interoperability for any connected TD or HN-TD taking part on this translating mechanism.

#### *Architecture options*

- The IPTV architecture can optionally support the inclusion of content-tracing information. Such content-tracing information can optionally contain the operator ID, content owner ID, TD ID, and other information.

#### *Scrambling algorithm requirements*

- Scrambling algorithms for broadcast stream are required to support the periodic update of the necessary cryptographic keys.
- Scrambling algorithms for IPTV are required to be built using publicly available and standardized cryptographic algorithms.

#### *Scrambling algorithm recommendations*

- Scrambling algorithms for IPTV are recommended to have sufficiently large key entropy to effectively protect the content from crypto-analysis.
- The IPTV architecture is not prohibited from precluding support for widely used scrambling algorithms.
- The IPTV architecture is recommended to refrain from precluding support for multiple scrambling systems.
- Scrambling algorithms for IPTV are recommended to be efficiently implementable for both hardware and/or software implementations.
- Scrambling algorithms for IPTV are recommended to be scalable and future-proof, i.e., cryptographic parameters (e.g., key length, crypto periods, etc.) or cryptographic mode (e.g., CBC, OFB, ECB, etc.).

#### *Scrambling algorithm options*

- Scrambling algorithms for IPTV can optionally apply cryptographic algorithms of varying strength to different content types.

### **6.3 Service security requirements**

This clause specifies the requirements that individually or collectively deal with services and service protection.

#### *Architecture requirements*

- The IPTV architecture is required to support service protection as defined in clause 3.
- The IPTV architecture is prohibited from precluding support to update SCP or the renewal of SCP in the TD from the server side.
- The IPTV architecture is required to support end-user (subscriber) authorization and authentication.
- The IPTV architecture is required to support a mechanism to signal TD to utilize a specified scrambling algorithm based on a standardized framework.

- The IPTV architecture is required to have the ability to use standard key management systems (e.g., MIKEY, EMM/ECM) as required for interoperability.
- The IPTV architecture is required to support the capability to update and query the SCP system concerning the scrambling algorithms for IPTV and any other operator-selected scrambling algorithm on the server side via SCP interfaces.
- The IPTV architecture is required to support SCP mechanisms that are independent of specific content formats.
- The IPTV architecture is required to support a mechanism for providing integrity protection and data origin authentication for sensitive metadata.
- The IPTV architecture is required to support a mechanism for the secure delivery of rights and content access control information to TDs.
- The IPTV architecture is required to support content usage control (e.g., replay).
- The IPTV architecture is required to support different modes of replay, e.g., limit on the number of plays, time-limit on plays, restriction of fast forward or rewind.
- The IPTV architecture is required to support a mechanism to enable maintaining the confidentiality of signalling messages between the SCP server and SCP client.
- The IPTV architecture is required to support a mechanism to enable maintaining the authenticity of signalling messages between the SCP server and SCP client.
- The IPTV architecture is required to support a mechanism to enable maintaining the integrity of signalling messages between the SCP server and SCP client.
- The IPTV architecture is required to support a mechanism to retrieve the SCP parameters securely (e.g., configuration, status) from TD.
- The IPTV architecture is required to support a mechanism to update the SCP parameters securely (e.g., configuration) of TD.
- The IPTV architecture is prohibited from precluding support for the capability to turn on and off the content-tracing function in a programmable manner (e.g., based on time, event, content, or channel).
- If it employs a key management system, such system is required to be designed for scalability, reliability, and interoperability.
- The IPTV architecture is prohibited from precluding support for the installation and operation of multiple service protection solutions without hardware replacements except removable devices (such as USB dongle and SIM cards).
- The IPTV architecture is prohibited from precluding support for an identification mechanism for available service protection solutions that are capable of satisfying the requirement specified for related content protection.
- The IPTV architecture is prohibited from precluding support for an SCP system discovery mechanism such that it may support a discovery method and adapt itself to it whenever a specific content requires a specific service protection system.
- The IPTV architecture is prohibited from precluding support for a mechanism for the selection of an SCP system from the available SCP systems without any hardware replacement except removable devices.
- The IPTV architecture is prohibited from precluding support for secure downloading for an SCP system. The downloaded SCP system can optionally depend on specific service protection requirements.
- If downloadable SCP is deployed, the IPTV architecture is required to perform integrity protection and data origin authentication for the downloaded SCP system.

- If the secure downloading of an application program to TD is supported, the IPTV architecture is required to perform integrity protection and data origin authentication for the downloaded applications.

#### *Architecture recommendations*

- The IPTV architecture is recommended to enable content confidentiality.
- The IPTV architecture is recommended to support multiple scrambling algorithms.
- The IPTV architecture is recommended to support the capability to authenticate and authorize end users for content sharing services (e.g., content export and content redistribution).
- If the IPTV architecture employs a key management system, considering a hierarchical key management scheme is recommended to support scalability.
- If the IPTV architecture employs a key management system that uses a group key management protocol, considering a hierarchical key management and a key management algorithm alternative is recommended to support scalability.
- If the IPTV architecture employs a key management system that uses short term keys, provisioning the media path such that NAT traversal and bandwidth constraints do not limit the key exchange is recommended.
- The IPTV architecture is recommended to support at least the same degree of protection (for purposes of controlling unauthorized access) for content-tracing information as applied to the corresponding traced content.
- The IPTV architecture is recommended to support the joint transmission of content and content-tracing information while retaining the synchronization of content and content-tracing information during transport.
- If the IPTV architecture employs PKI to authenticate TD or service or content provider, considering the multi-level hierarchy of PKI is recommended to support scalability, reliability, and interoperability.
- If the IPTV architecture employs PKI for the IPTV service, using publicly available, standardized certificate format, certificate revocation list, or online certificate status protocol is recommended.
- The IPTV architecture is recommended to support the secure downloading of application programs to TD.
- The IPTV architecture is recommended to support a mechanism for limiting viewing-rights of certain programs to certain groups of subscribers (e.g., block viewing by residents of a specific area (for example, this can optionally be useful for sporting events)).

#### *Architecture options*

- To provide a scalable IPTV service for the user-owned terminal whose resolution is different from that of the user terminal, the IPTV architecture can optionally support the ability of a secure transcodable scheme as defined in clause 3.

## **6.4 Network security requirements**

This clause specifies the requirements that individually or collectively deal with networks or their protection.

#### *Architecture requirements*

- The IPTV architecture is required to support the capability of mitigating a DoS attack.
- The IPTV architecture is required to support the provision of security measures to block illegal or unwanted traffic.

- The IPTV architecture is required to be resistant to attacks on multicast capabilities.
- The multicast architecture is recommended to support the capability to authenticate a peer in the general or overlay (peer to peer) multicast environment.
- The communication link between terminal devices within the home network is required to be protected for content security when carrying a premium, e.g., paid by consumer, content that is not protected.
- The IPTV architecture is required to support DNG authentication by the IPTV management function.
- The IPTV architecture is required to support the authentication of the IPTV management function by DNG.

#### *Architecture recommendations*

- To protect the home network from malicious or unauthorized access, the IPTV architecture is recommended to support the ability of delivery network gateway function (DNGF) to establish a firewall that is remotely configurable and with multiple levels of security and appropriate application-level gateways.
- The IPTV architecture is recommended to support the capability of IPTV management to configure remotely a NAT and an intrusion protection function of DNG.
- The IPTV architecture is recommended to support the capability to remotely configure NAT and intrusion protection function of the DNG by the remote IPTV management function.
- The IPTV architecture is recommended to secure the remote management of TD in case remote management is supported.
- The IPTV architecture is recommended to support the use of content label information to control content delivery.

### **6.5 Terminal security requirements**

This clause specifies the requirements that individually or collectively deal with TDs or their protection.

#### *Architecture requirements*

- The IPTV architecture is required to support TD protection as defined in clause 3.
- The IPTV architecture is required to support TD authentication.
- The IPTV architecture is required to support physical tamper resistance for TD.
- The IPTV architecture is required to support a means of detecting when physical tampering has occurred on the TD.
- If downloadable SCP is deployed, the IPTV architecture is required to support the secure download and installation of the SCP operating code to TDs.
- The IPTV architecture is required to support a secure means of performing security-critical processes in the TD such as key management and media serialization to abort the playback of content in case of security-related malfunction, detection of tampering, or other indication of misuse.
- The IPTV architecture is required to provide physical protection for sensitive security-enabling processes and components involved in the processing transmission and storage of valued content in the TD in the absence of logical protection (such as encryption or serialization watermarks). These processes include descrambling and media serialization.
- The IPTV architecture is required to recognize the need for the physical protection (against probing or tampering of the SCP functions system on the TD) of sensitive security-enabling

processes in the TD including descrambling and media serialization (content tracing) and critical data supporting those processes, as well as for all components involved in the processing, transmission, and storage of any valued content lacking logical protections, such as encryption or content-tracing watermarks.

- The IPTV architecture is prohibited from precluding support for the interchange of content between the TD and other (physical or logical) devices, provided the uses granted for this content include such interchange.
- The IPTV architecture is required to support a mechanism that allows a TD to authenticate the SCP servers.
- The IPTV architecture is prohibited from precluding support of the renewal of SCP in the TD.
- The IPTV architecture is required to support digital or analog output that should be protected as required by the SCP client off-device storage in case digital or analog video/audio output are available on the TD.

#### *Architecture recommendations*

- The IPTV architecture is recommended to provide the content export in TDs enabling the IPTV content to be transferred securely from the IPTV terminal to the other terminal owned by the user entitled to use it.

## **6.6 Subscriber security requirements**

This clause specifies the requirements that individually or collectively deal with subscribers and end users or their protection.

#### *Architecture requirements*

- The IPTV architecture is required to support user privacy protection as defined in clause 3.
- The IPTV architecture is required to allow a subscriber to set an access control mechanism (e.g., using a password) to restrict access to content and/or services.
- The IPTV architecture is required to be capable of indicating why the user has been denied access to content.
- The IPTV architecture is required to support a mechanism that enables a subscriber to request for extensions (e.g., more plays, more playtime) of usage rights associated with specific content instances.

#### *Architecture recommendations*

- The IPTV architecture is recommended to allow the end user (as allowed by rights) to change, i.e., replace, a TD without inherently affecting the rights to consume content.
- The IPTV architecture is recommended to support a mechanism for rating programs according to content.

NOTE – Rating information can be used for access control, e.g., parental control.

## **7 Security architecture**

This clause defines an IPTV security architecture in terms of a general security architecture, a content protection architecture, and a service protection architecture as well as security functional entities to meet the requirements described in the previous clauses.

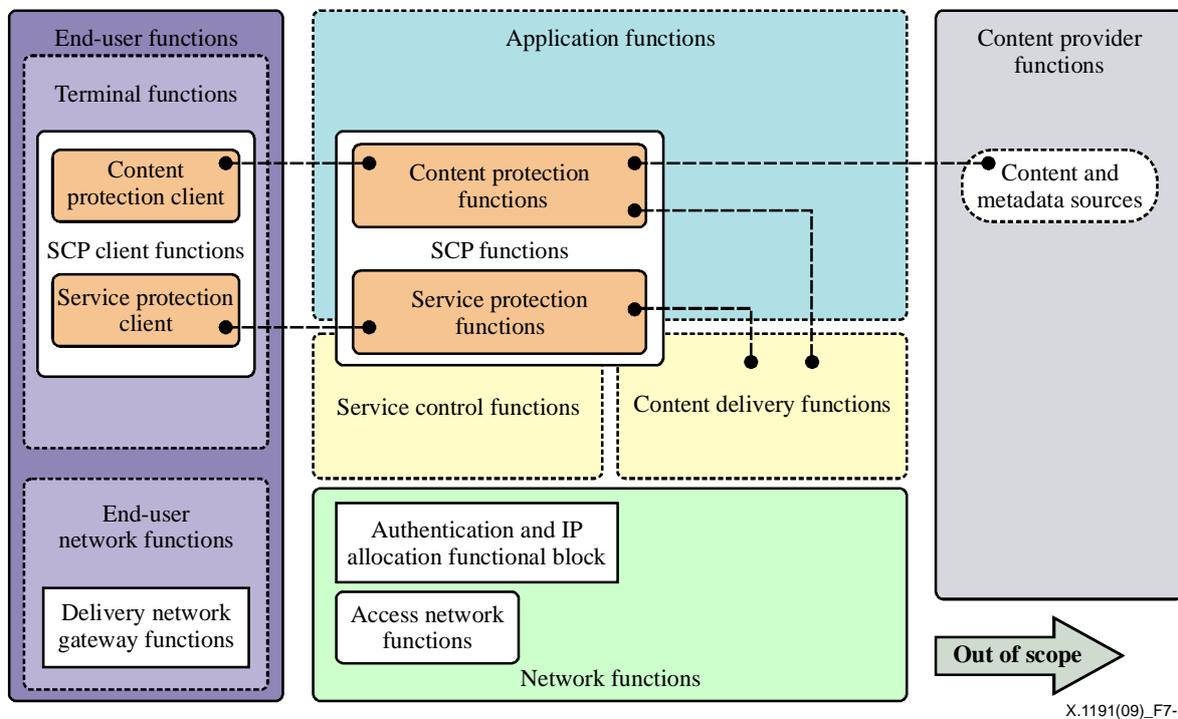
The IPTV security architecture described below is assumed and intended to be used in the context of the IPTV functional domains and IPTV functional architecture framework as defined by clauses 6 and 8 of [ITU-T Y.1910], respectively.

## 7.1 General security architecture

A general security architecture for IPTV is depicted in Figure 7-1 below. This general architecture is divided into two primary areas – one is considered to be within the scope based on the purpose of this Recommendation, and the other is deemed to be beyond the scope. The first area encompasses the end user, network provider, and service provider domains, whereas the second area covers the content provider domain.

In the second area, all security aspects within the content provider domain and interconnection between content providers and service providers are subject to private agreements between the stakeholders operating in these domains. Thus, they are considered to be beyond the scope of this Recommendation.

Although the content provider domain and the interconnection between the content and service provider domains are considered out of the scope in the present context, the content provider domain is included in the following figures and descriptions for the purpose of completeness. As such, any statement made herein concerning these domains is required to be considered informative or explanatory in nature.



NOTE 1 – The content protection functions and service protection functions in this figure are the most important parts of the IPTV security architecture. Detailed discussions of these functions can be found in Figure 7-2 (*Content protection architecture*) and Figure 7-3 (*Service protection architecture*).

NOTE 2 – For the IPTV architecture, some functions and functional blocks without a direct relationship with IPTV security are omitted in this figure to simplify it.

**Figure 7-1 – IPTV general security architecture**

The general security architecture is divided roughly into four functional areas as follows:

- Content provider functions (technically beyond the scope)  
The content provider(s) is (are) assumed to provide access to content to service providers that have established relationship(s) with the content provider(s). In some cases, a content provider itself may serve as a service provider; in such a case, this relationship is considered to be internal.

In providing service providers with access to content, a content provider may use standard or private mechanisms to control and enable access to content; note, however, that such mechanisms are considered to be beyond the scope of this Recommendation and subject solely to a private agreement between stakeholders.

- Service and content protection (SCP) functions (overlap with certain parts in the application functions, service control functions, and content delivery functions)

SCP functions play a central role in the IPTV general security architecture particularly in the service provider domain. Specifically, service protection functions enable the protection of the service infrastructure as well as control of access to services and content hosted therein. On the other hand, content protection functions enable controlling the use of services and content according to licensed uses. The specific functions and functional blocks of SCP functions are dispersed in three sub-areas: application functions, service control functions, and content delivery functions.

A service provider is obligated by the licence(s) from content providers to make content available only under certain conditions of use, e.g., one-time viewing but no recording, one-time recording with multiple viewing, one-time recording with the transfer of recording rights, etc. The primary purpose of the content protection aspects of the SCP functions is to allow a service provider to satisfy such obligations in an objectively verifiable manner.

The primary purpose of the service protection aspects of the SCP functions is to prevent unauthorized access to service resources and information considered confidential by entities in various domains: service, network, terminal device, and end user (subscriber).

A secondary purpose of the service protection aspects of the SCP functions is to protect the service infrastructure from damage due to both the intentional and/or accidental misuse of resource.

The detailed functional blocks of the content protection functions and service protection functions are depicted in Figure 7-2 (*Content protection architecture*) and Figure 7-3 (*Service protection architecture*), respectively.

- Network functions

Security functions dealing with the network domain focus on authenticating entities and authorizing access to the network(s) through which IPTV services are or will be delivered. A secondary function is to protect the integrity of the network itself – physically, electronically, and operationally (e.g., by detecting and thwarting denial of service attacks on the access or bearer network).

- End-user functions

Aspects of security applying to the end user (subscriber) include the protection of integrity of the TD operating on subscriber premises as well as protection of end-user privacy.

Under certain circumstances, a DNG between a TD and a network domain could be considered to be within the end-user domain and subject to end-user security measures.

Finally, it is recommended that the integrity mechanisms be applied to assure the integrity of content received by a TD and subsequently redistributed to other devices within or beyond the home network. (This results in an overlap between end-user security aspects and content security aspects.)

More detailed descriptions of the functions and functional blocks shown in Figure 7-1 are provided in clause 7.4.1.

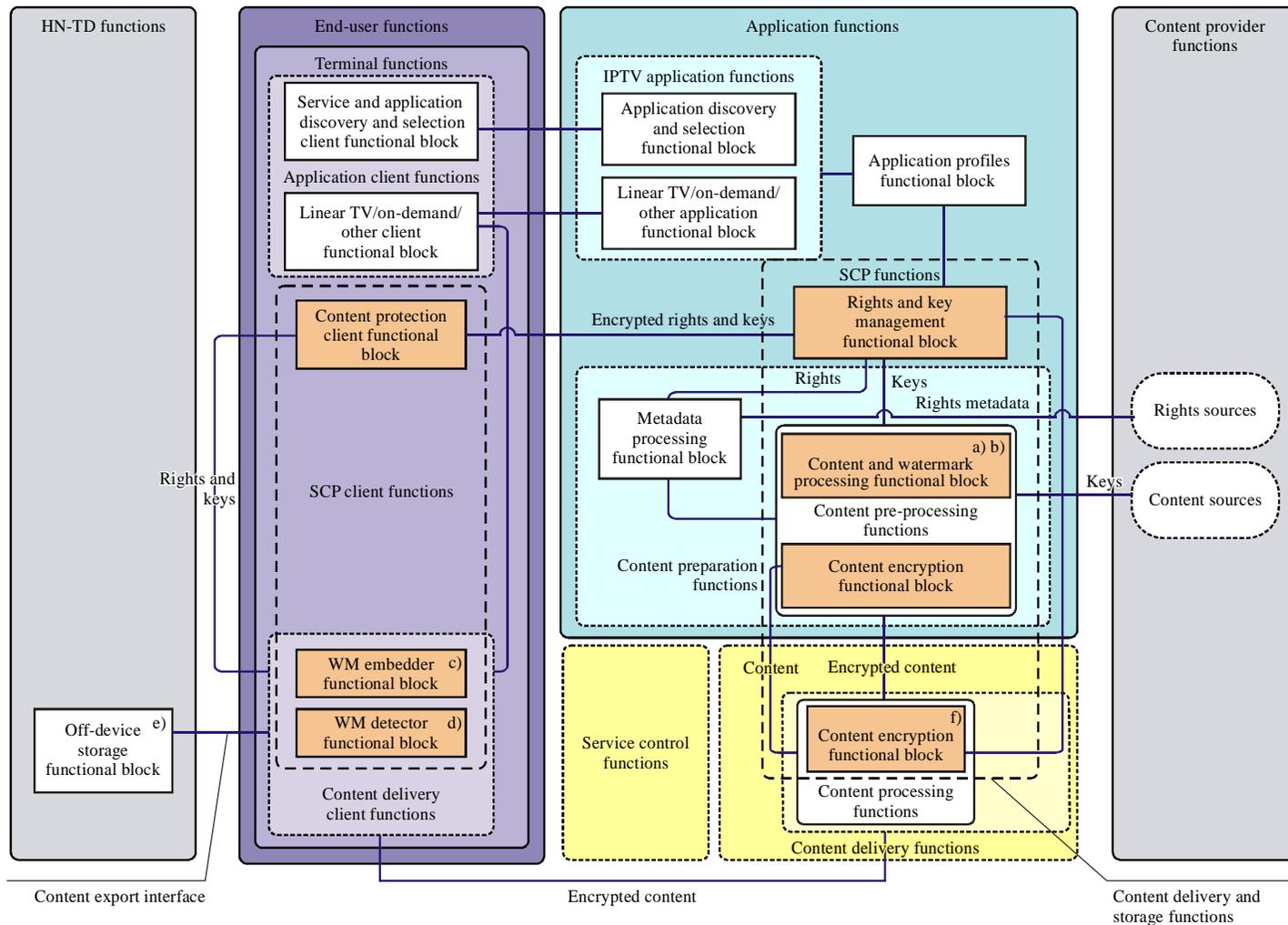
## **7.2 Content protection architecture**

A content protection architecture for IPTV is depicted in Figure 7-2 below.

The primary function of the content protection architecture is to delineate the flow and processing

of information dealing with the content usage rights and information required to manage and facilitate such rights.

Ultimately, the rights to content use originate with the content provider(s); note, however, that such rights may be modified (e.g., narrowed or even widened) by service provider(s) according to its (their) agreements with content providers and operational and business policies.



- <sup>a)</sup> Optional watermark metadata generation to facilitate downstream watermark embedding.
- <sup>b)</sup> Optional watermark embedder to individuate content to networks, servers, and unicast deliveries.
- <sup>c)</sup> Optional watermark embedder to individuate multi-cast content instances.
- <sup>d)</sup> Optional detector for copy protection watermarks.
- <sup>e)</sup> Optional off-device storage: a storage device inside HN-TD.
- <sup>f)</sup> The content encryption functional block located in content delivery and storage functions is optional.

X.1191(09)\_F7-2

NOTE – The content protection functional blocks in this figure consist of content protection functions and content protection client functions.

**Figure 7-2 – IPTV content protection architecture**

The content protection architecture shown above consists of functions residing primarily in two functional areas:

- Service and content protection functions (overlap with application functions and content delivery functions)

Content and its associated rights are collected from content providers, aggregated, and processed for delivery to the end user, where the overall process is managed by several functions such as content preparation functions using data describing an end user's rights and related conditions.

Content, rights, and keys (used to grant access to content and enable its use) information are organized into a form appropriate for the specific application, e.g., linear TV viewing. Rights and key information are delivered to the content protection client functional block in the terminal device as entitlement (e.g., EMM) by the right & key management functional block; content is processed to insert content-tracing (e.g., watermarking) metadata as an option and subsequently encrypted in the content preparation functions prior to delivery. In some cases (e.g., real-time IP services), content can also be encrypted by the content delivery functions as an option.

In the context of the IPTV content protection architecture (as opposed to the IPTV service protection architecture to be described later), the focus is primarily on the management, processing, and delivery of rights and keys as opposed to the encryption of this information or the content subject to these rights.

- End-user functions

The terminal functions operating in the end-user domain are responsible for enforcing content usage rules associated with rights information (also known as content protection metadata). This functional entity interprets content rights and keys obtained from the right & key management functional block and then acts on the interpretation to control how the content is processed and exposed to the end user, either through integrated presentation devices (e.g., display or audio rendering system) or through physical interconnections to external devices.

In those cases wherein TD transmits protected content to an external device (e.g., display output), the content rights may be translated into other forms; the content to which such usage applies may be further processed to insert client-side content-tracing information (e.g., watermarks) as an option or re-encrypt content to execute downstream access control.

More detailed descriptions of the architectural blocks shown in Figure 7-2 are provided in clause 7.4.

In Figure 7-2, the content export interface is a logical interface connecting IPTV TD and HN-TD. HN-TD may consume content itself or export content to other HN-TDs. The content delivery client functions may adjust the corresponding security label to ensure that only the authorized HN-TD system can consume and export content.

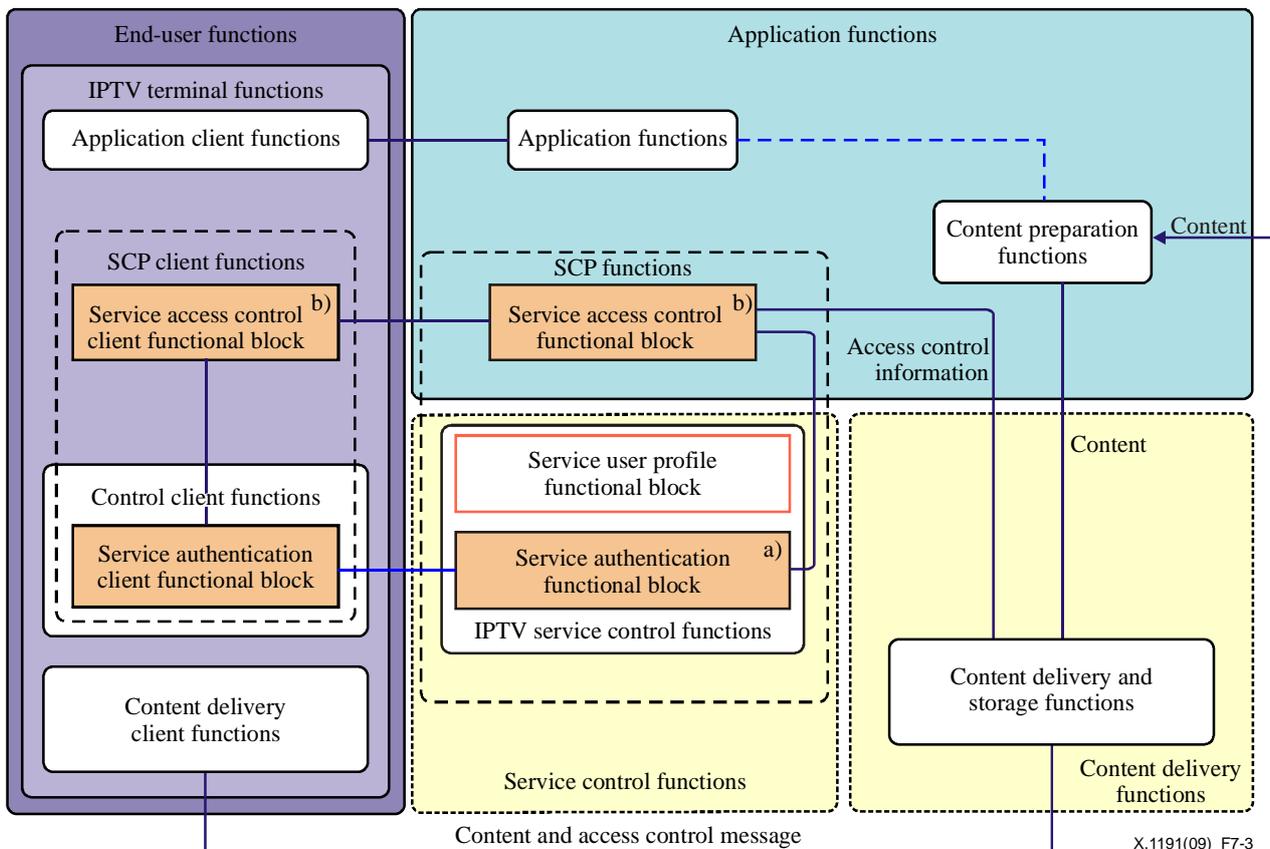
### **7.3 Service protection architecture**

For the managed services involving protected content, a typical case is that wherein the end user (subscriber) and TD must be authenticated and authorized following successful authentication to access the service(s) and content hosted therein.

Depending on the circumstances, authentication and authorization functions may be performed separately on TD and end user(s). In other cases, additional devices in end-user premises such as a delivery network gateway and other end-user devices may require authentication before service access is authorized.

The combination of authentication and authorization can be used for controlling access to both IPTV service and to TD for purposes of service and content acquisition prior to use.

A service protection architecture for IPTV is depicted in Figure 7-3 below.



<sup>a)</sup> Authentication: It identifies a subscriber name and ID with the assigned privilege.

<sup>b)</sup> Service access control: To protect a service from the illegally unauthorized access.

NOTE – The service protection functional blocks in this figure consist of service protection functions and service protection client functions.

**Figure 7-3 – IPTV service protection architecture**

The primary functions of the service protection architecture include:

- Subscriber and TD authentication:
  - This function is responsible for authenticating subscribers and TDs.
  - Subscriber authentication: Process of the authenticity of the user
  - TD authentication: Process of the authenticity of the TD
- In cases wherein X.509 base certificates are used as credentials for authentication, a revocation function is required.
- Server authentication:
  - In TD, a function for authenticating the server for mutual authentication
- Service access control:
  - Function for restricting acquisition of and access to services by authorized users using security mechanisms such as scrambling and encryption

More detailed descriptions of the architectural blocks shown in Figure 7-3 are provided in clause 7.4.

## 7.4 Description of functions and functional blocks in IPTV security architectures

This clause provides more descriptive details of the functions and functional blocks depicted in the architectural models found in clause 7.1 (*General security architecture*), clause 7.2 (*Content protection architecture*), and clause 7.3 (*Service protection architecture*) above. These functions and functional blocks are defined only in general descriptive terms and divided into three parts corresponding to each of these three clauses.

### 7.4.1 General architecture functions and functional blocks

**Access network functions:** Provide for the collection and aggregation of control and data traffic originating in the network(s); enable QoS/QoE including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, and traffic shaping.

NOTE 1 – These functions are independent of the service and content protection functions from the point of view of IPTV service and content protection.

**Application functions:** Divided between the server (service provider) side and client (end-user premises) side; consist of functional components that prepare, originate, receive, and process service-level IPTV applications such as linear TV, VoD, and related content, e.g., accessibility information, interactive applications, etc.

**Authentication & IP allocation functional block:** Provides the functionality to authenticate the delivery network gateway functional block connecting to the network functions as well as the allocation of IP address to the IPTV terminal functions.

**Content protection functions:** Provide mechanisms that enable the enforcement of content usage policies including aggregation, distribution, and management of rights and keys, optional generation and insertion (embedding) of content-tracing information (e.g., watermarks), and content encryption (under the control of service protection functions).

NOTE 2 – The specific functional blocks making up the content protection functions are discussed further in clauses 7.2 and 7.4.2.

**Content protection client functions:** Interact with the server-side content protection functions to enforce content usage policies.

**Content provider functions:** Deliver content and content rights and key metadata to service providers.

**Delivery network gateway functions:** Provide for connectivity between the terminal device and delivery network; manage local (end-user premises) IP connectivity, obtain IP address(es), and IP configuration for the TD.

NOTE 3 – These functions are independent of service and content protection functions from the point of view of IPTV service and content protection.

**Service protection functions:** Provide mechanisms for performing authentication and authorization for and controlling access to IPTV services and content contained therein, including control of and direct implementation of control signal and content interchange encryption either independently of or in conjunction with the content protection functions.

NOTE 4 – These functions are independent of the service and content protection functions from the point of view of IPTV service and content protection.

NOTE 5 – The specific functional blocks making up the service protection functions are discussed further in clauses 7.3 and 7.4.3.

**Service protection client functions:** Interact with the service protection functions on the server side to perform service access control and other protection functions.

**Terminal functions:** Provide service protection and content protection clients for decrypting and enforcing service and content usage policies according to usage rights metadata; performing link-layer encryption and SCP translation (interchange) as required for further downstream content output or redistribution and internal (or external) content storage including support for secure (tamper-resistant) media processing pipelines, local secret (e.g., key) storage, security software renewability, authentication and verification of the downloaded software assets, and protection of locally stored and interchanged user data subject to end-user privacy considerations.

#### 7.4.2 Content protection architecture functions and functional blocks

**Application client functions:** Primary point of coordination and control of interaction between the end user and service(s) provided by the IPTV application functions; for standard applications such as linear TV viewing, providing for primary user interface and operating paradigm through which the end user obtains a service.

- **Application discovery and selection client functional block:** Permits the end user and/or terminal device to discover the existence and selection of applications and application services available from the service provider(s).

**IPTV application functions:** Logical entities that embody the point of origination for some IPTV services such as linear TV, VoD, etc.; responsible for orchestrating all service provider facilities to enable the existence of some service(s) operationally.

- **Application discovery & selection functional block:** Interacts with application discovery and selection client functional block above to enable the end user and/or terminal device to discover the existence and selection of applications and application services.

**Application profile functional block:** Stores and manages configuration information on applications and services both of a global nature and of an end user (subscriber)-specific nature; typically used to permit application server(s) to customize services and content for the end user, will frequently interact with or implement (internally) various accounting systems.

**Content preparation functions:** Perform various types of content pre-processing prior to delivery such as content-tracing (e.g., watermark) analysis and metadata generation, content and content metadata multiplexing, and content encryption.

- **Content and watermark processing functional block:** Optional processing step(s) that analyse(s) content to produce content-tracing (e.g., watermark) metadata for use in subsequent downstream processing, particularly a process of individuating (identified with information by the associating source) such metadata.
- **Metadata processing functional block:** Manages and processes the program-related metadata and usage rights information delivered by the content provider.
- **Content encryption functional block:** Performs the encryption of (scrambles) protected content to facilitate access control and confidentiality of such content during the content delivery process; content can be encrypted in real time or pre-encrypted offline (content encryption can optionally support the secure transcoding without decryption).

NOTE 1 – The encryption of the content can be implemented in content preparation functions within the application layer. In some cases, it can also be implemented in content delivery functions as an option.

**Rights and key management functional block:** Correlates rights and keys with content and manages their distribution to the content protection client functional block in the terminal device.

**Content protection client functional block:** Obtains or receives the rights and keys using this information to control content decryption and enforce usage rules; this functional block needs to be tamper-resistant.

**Content delivery functions:** Perform cache and storage functionalities and deliver the content according to the request from the end-user functions; the content delivery functions can optionally process (e.g., encode, encrypt) the content.

**Content delivery client functions:** Responsible for the content reception in the IPTV terminal functions; perform content media decryption, demultiplexing, decoding, and subsequent presentation and storage processing on content (these functions also need to have the capability of being tamper-resistant).

- **Watermark detector functional block:** If present, detects the use of watermark(s) in content received from the service provider(s) to verify or implement the desired content usage rules in the terminal device or downstream interfaces from the terminal device.
- **Watermark embedder functional block:** If present, performs the individuation of content instance for presentation and subsequent storage or redistribution.

**Rights sources:** Originating content metadata dealing with content usage rights.

**Content sources:** Originating content to be aggregated, processed, and subsequently delivered to end users by means of service applications such as linear TV, VoD, etc.

**Off-device storage functional block:** Post-receipt content storage mechanisms that are physically external to the TD and whose storage and content use is not managed by the TD.

NOTE 2 – If external storage exists, and its use is under the control of TD at all times, then it may be considered to be on-device storage via an authorized, protected interface depending on the applicable terminal device compliance and robustness rules.

### 7.4.3 Service protection architecture functions and functional blocks

**Service access control functional block:** Mainly responsible for service access control; uses security mechanisms such as scrambling and encryption are used by this functional block to prevent users from accessing or acquiring the services without permission.

**Service access control client functional block:** Performs service protection-related tasks on the client as defined by the service access control functional block on the server side.

**Service authentication functional block:** Performs authentication to verify the authenticity of user and/or TD; it also supports the authentication requests that come from the TD to verify the server.

**Service authentication client functional block:** Besides performing subscriber authentication-related tasks on the client side, it also includes the function of verifying the authenticity of the server side of service protection for mutual authentication.

## 8 Security mechanisms

This Recommendation does not define any specific security mechanism or solution; instead, it describes in general terms certain security mechanisms that may be considered for purposes of defining or implementing mechanisms that address security requirements, security architectural functional entities, and security threats.

The set of security mechanisms described below does not comprehensively address all the security requirements documented above.

### 8.1 Security mechanisms dealing with content protection

Content security mechanisms include a set of functions operating between content sources and TDs to ensure that content can be distributed (or transmitted) securely by a network and can be acquired, consumed, exported, stored, and redistributed (or retransmitted) securely by an end user.

Content security mechanisms can be applied to content distribution, content acquisition, content consumption, content storage, content export, and content redistribution. The following mechanisms can be used to meet the requirements of IPTV content and service protection (all of them are optional):

### **8.1.1 Content encryption**

In many cases, contents may be encrypted to prevent their illegal use during delivery.

### **8.1.2 Content tracing and identification**

Content tracing serves to identify and trace the origin (source) of the content and/or the responsible party (e.g., end user) to facilitate subsequent investigation in case of unauthorized content access and usage.

Content-tracing information may be attached to content either as metadata or as forensic watermark. Content-tracing watermarks are typically designed to be robust and imperceptible to protect against their intentional or inadvertent removal.

Facilitation of content identification by a video signature technology is recommended.

### **8.1.3 Watermarking**

Watermarking refers to the process of adding information to content through the alteration of certain content features. This is a field of study known as *steganography*.

Watermarking is preferable for many applications due to the difficulty in removing this information from content. In an IPTV service, watermarking may refer to the inclusion of hidden information directly in a video or an audio stream of multiplexed content. Ideally, watermarks are invisible and/or inaudible to human perception but will successfully survive conversion among media formats.

### **8.1.4 Content labelling**

Content labelling is the process of inserting or associating metadata with content describing the nature of the content as well as content aspects and characteristics with content. Content labelled with such metadata may be sorted, filtered, or categorized more easily by intermediate devices in the content delivery chain.

Some regions, administrations, or specific deployments of IPTV may require the presence of certain types of content labels such as rating information to permit some degree of end-user (subscriber) control over access of content considered inappropriate or harmful.

### **8.1.5 Secure transcodable scheme**

A secure transcodable scheme (STS) refers to a kind of a security scheme enabling the intermediate network node to perform transcoding without decryption while preserving end-to-end security. This scheme can be achieved by combining scalable coding, progressive encryption, and packetizing.

For STS, there are three entities: a sender, an intermediate network node, and a user with an IPTV terminal. A sender performs a secure transcodable function to produce scalable encrypted packets from the video and adds the unencrypted header to send the information; an intermediate network node reads the unencrypted header and uses the information to truncate or discard the adequate packets according to the desired transcoding operation, with the IPTV terminal decrypting the encrypted packets and decoding the plain-text packet to produce the video. The detailed description is given in Appendix V.

NOTE – This clause is not intended to define or describe the additional mechanisms for STS. This topic is required to be discussed further in other Recommendations.

## **8.2 Security mechanisms dealing with service protection**

Service security mechanisms include authentication and authorization. Implementations of specific access control mechanisms such as encryption and decryption systems may also be included.

### **8.2.1 Service authentication**

In the case of managed services for which an end user (subscriber) has a direct relationship with a certain service provider, the service provider will typically require the terminal device and/or the end user (subscriber) to be authenticated in a secure manner before service can be rendered; in a such case, authentication involves producing and presenting in a secure manner credentials/information that can be correlated with the service provider's subscriber database to verify the authenticity of the terminal device and/or the end-user for the purpose of service delivering.

### **8.2.2 Service authorization**

Following end-user (subscriber) and/or terminal device authentication for the purpose of service delivering, a service authorization mechanism is used to authorize and grant access to specific services and content hosted therein according to the service and subscriber provisioning.

### **8.2.3 Service access control**

In most (if not all) cases, a service protection system will contain mechanisms that can or do perform encryption (scrambling) and decryption (descrambling) of both service control signalling traffic and content traffic. Typically, two-way service control traffic will be encrypted in both directions – both from server to client and from client to server. On the other hand, content streams will typically be encrypted only from server (service provider) to client (terminal device). Nevertheless, there are usage scenarios wherein a content stream may be uploaded from a client to a server, in which case such content may be encrypted on a terminal device for uploading purposes (e.g., to ensure that only an authenticated, authorized service provider can access the uploaded content).

## **8.3 Security mechanisms dealing with networks protection**

This Recommendation does not define or describe any mechanism dealing with network security. In general, the implementations of core, access, bearer, and delivery networks are expected to enable implementing whatever mechanisms are believed to be required to protect the operational integrity of the network, including denial of service (DoS) detection and prevention, for example. Generally, security mechanisms employed by IPTV service providers and TDs will be transparent to these networks, provided these security mechanisms operate at or above the payload data elements provided by network layers.

## **8.4 Security mechanisms dealing with terminal device protection**

Terminal device security mechanisms include a wide range of functionality including secure and tamper-resistant secrets data storage, service authentication, service authorization, control signal encryption and decryption, content decryption, content rights metadata decoding, content usage enforcement, watermark detection and embedding, programmatic content authentication and verification, service and content protection bridging and interchange, digital output port (interface) encryption, media path tamper resistance, pluggable and renewable security processors and components, both hardware- and software-based, etc.

## **8.5 Security mechanisms dealing with subscribers or end users**

Subscriber or end-user security mechanisms are primarily related to the collection, storage, and transmission of information that may be subject to privacy considerations or end-user confidentiality. As such, these mechanisms may be divided between the point of collection, the

terminal device, and the service provider possibly harvesting, maintaining, and reusing this information. Consequently, descriptions and definitions of these mechanisms are expected to be included in clauses describing the service and terminal device security.

Currently, this Recommendation does not define the subscriber or end-user security mechanisms. Future work on this Recommendation is expected to discuss these topics further.

Additional information on subscriber security is provided in Annex A.

## Annex A

### Subscriber security protection

(This annex forms an integral part of this Recommendation)

#### A.1 User data protection

When implementing IPTV services among general users, giving sufficient consideration to security, the protection of subscriber data is essential.

The subscriber data may also include tracked data information such as channel number before and after the channel change, time of change and user information for the EPG service, package identification, time of play, etc. The above-mentioned data are personal and confidential in nature. Protecting all of these subscriber data from abuse requires the IPTV service provider to consider the user privacy protection issues.

- The IPTV service can optionally handle the minimum subscriber's personal data necessary for delivering the IPTV services.
- The IPTV service can optionally explain the intended use of the subscriber's personal data and obtain consent from the subscriber before collecting the information required to deliver the IPTV services.
- The IPTV service can optionally destroy the subscriber's personal data that becomes unnecessary for the continuity of IPTV services.
- When the service provider administers the subscriber's personal data, the IPTV service can optionally store the collected data under strict security.

There are many possible ways by which a subscriber's personal data can be leaked: There may be leaks from the service company, leaks from the network, and leaks from the home, e.g., through terminal devices. Here, we present methods of protecting the subscriber's personal data for each of these leak routes.

To prevent the leak of the subscriber data, the IPTV service provider is recommended to pay careful attention to the following:

- Classify the subscriber's personal data into that which requires control and that which does not
- Securely administer the subscriber's personal data requiring control
- Ensure that the subscriber's personal data requiring control is not used for purposes other than the intended one.

IPTV service providers are recommended to pay careful attention to the points below in relation to the services and transactions involving the handling of the subscriber's personal data:

- Classify the subscriber's personal data into that which requires control and that which does not
- Use encrypted communication channels for the transmission of the subscriber's personal data requiring control.

IPTV service providers sometimes store the subscriber's personal data in terminal devices to enhance service efficiency. In such cases, they are recommended to pay careful attention to the points below. Furthermore, security is recommended to be considered when exchanging TDs.

- Ensure that no third party can easily read the subscriber's personal data stored inside the TD.
- The IPTV service provider can optionally control access to the subscriber's personal data stored in the TD.

- Ensure that the subscriber's personal data stored in the TDs can be completely deleted by a subscriber or a service provider.
- TDs are required to ideally be protected against attack by computer malware, e.g., viruses and spyware, in the near future.

## **A.2 Parental control, protection of legal minors, access control**

In the IPTV platform, a mechanism for the protection of legal minors can be used to restrict the IPTV content that can be accessed by legal minors. In a typical usage pattern, a terminal device for IPTV services is shared in a home by multiple people, including legal minors. For terminal devices, the IPTV service provider is recommended to:

- Ensure that parental ratings can be set for content as necessary.
- Ensure that terminal devices can be operated in accordance with parental ratings.
- Ensure that terminal devices are capable of changing parental rating settings.
- Ensure that terminal devices are capable of password-based controls so that only the guardians of legal minors can change parental ratings.
- Ensure that content ratings can be set for different age groups.
- Ensure that subscriber privileges can be allocated for different age groups.
- Ensure that authorization can be made in terminal devices for legal minors viewing a particular channel or content, e.g., using a PIN challenge.
- Ensure that guardians who are not in proximity of legal minors can remotely monitor and receive content for legal minors from the network copy storage.

Note that the conditions of each administration or region in relation to third-party organizations for eliminating harmful content may be necessary, since this is related to the control of content flow and access. One may assume that the original content-creator gives appropriate consideration to the simultaneous retransmission of broadcasting at the time of producing the content; hence, the need to give sufficient attention to transmission delays and distribution cost increases.

# Appendix I

## Security threats

(This appendix does not form an integral part of this Recommendation)

This appendix describes a set of identified security threats addressed by some requirements or mechanisms of this Recommendation.

The security threat model and other fundamental materials have been addressed according to the following ITU-T Recommendations:

- [b-ITU-T X.800] defines the general security-related architectural elements that can be applied appropriately under the circumstances wherein the protection of communication between open systems is required.
- [b-ITU-T X.805] defines the network security architecture for providing end-to-end network security.

Parties interested in security considerations related to IPTV are encouraged to read these base security Recommendations; the reader of this Recommendation is assumed to be aware of the information presented in such Recommendations.

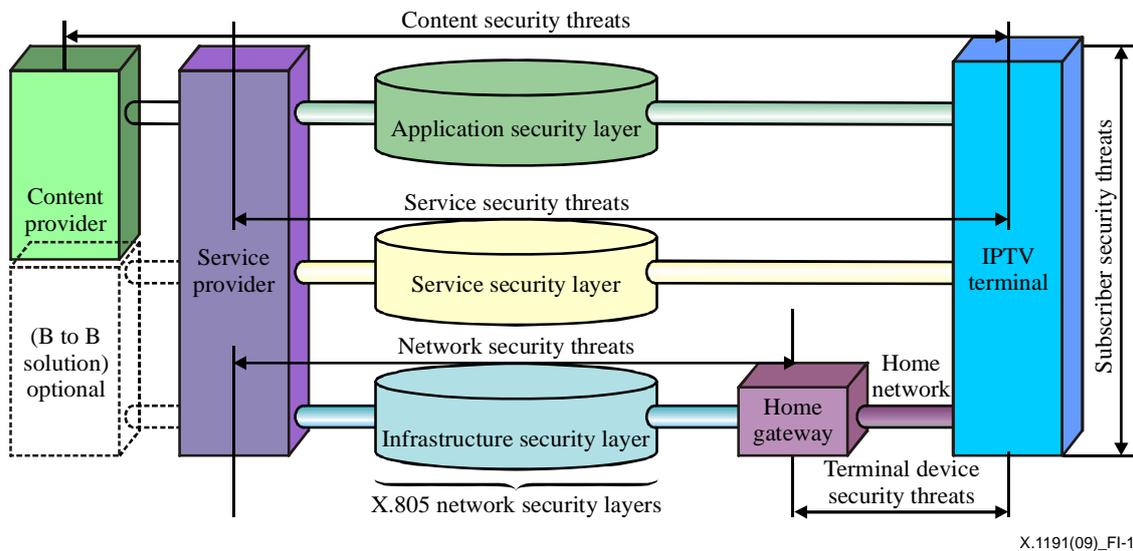
[b-ITU-T X.800] and [b-ITU-T X.805] identify the following security threats to the networks (also serving as security threats to service and content application applicable to IPTV):

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal, or loss of information and/or other resources
- Disclosure of information
- Interruption of services

### I.1 Security threats model

Security threats to IPTV can be classified into the following types: content security threats, service security threats, network security threats, terminal device security threats, and subscriber security threats.

Figure I.1 illustrates the security threats model, which shows the relationships among each of these threats.



**Figure I.1 – Security threats model**

### I.1.1 Content security threat

**Content assets:** Assets that belong to a content provider and/or a service provider can be consumed by the end user via the TD.

Content assets that need to be protected include: linear TV content, VoD content, push VoD content, PVR content, downloaded applications, etc.

The following are the content threats:

- Interception: A breach of confidentiality of the digit content through the illegal monitoring of service networks
- Unauthorized viewing
- Unauthorized reproduction or redistribution

### I.1.2 Service security threat

**Service assets:** Assets belonging to a service provider; they include media servers, SCP servers, and operational information such as service logs and billing information at the very least.

The following are the service threats:

- Copyrights infringement of programs provided by the IPTV service platform to subscribers
- Masquerading/spoofing the IPTV service provider
- Malicious threats targeting the IPTV servers (SCP servers, media servers, etc.): may include hacking aimed at security leaks in the application software or communication protocol, denial of service attack, etc.
- Theft (often uses malicious programs such as Trojan horse) of the subscribers' information (e.g., identifier information, billing information, subscription information).

### I.1.3 Network security threat

**Network assets:** Assets that belong to the network provider; they could include physical equipment (e.g., routers, switches) and network resources (e.g., bandwidth, multicast services, etc.).

The following are the network threats:

- Intentional threats targeting network equipment or resources (bandwidth): malicious attacks to the bearer network such as denial of service.

- Security threats to the multicast technique used in the IPTV bearer network, e.g., masquerading/spoofing multicast TV sources or illegitimate multicast group members.
- Malicious attacks (such as DoS, hacking) on nodes in the content distribution network.

#### I.1.4 Terminal device security threat

**Terminal assets:** Assets that belong to a terminal device that can be used by the end user to process and store content and other relevant information for the IPTV service.

The following are the terminal threats:

- Illegally accessing clear content by tampering device hardware or software; for example, clear contents can be copied by bus data interception or SCP software cracking.
- Illegally accessing keys or other secret information in devices using software cracking or hardware tampering; attackers can tamper the device memory or analyse the data flow to obtain the keys and other secrets (content key exposure results in content leak, and device key leak leads to device impersonation).
- Device malfunction by hardware method such as control of the device clock system to disable the functions of the SCP systems or by software method such as the installation of viruses to deplete the device resources.
- Unauthorized applications (such as software programs) were downloaded, run, and stored in terminal devices.
- Failure of terminal equipment (hardware and software) caused by malicious codes/viruses from the network.
- Unauthenticated terminal devices connecting to the home network.
- Unauthorized use by subscribers.

#### I.1.5 Subscriber security threat

**Subscriber assets:** Assets that belong to a subscriber; they can consist of information on the subscriber, subscriber household, their IPTV transactions, etc.

Subscriber security requires that a mechanism realizing content security and a mechanism realizing service security work in cooperation with each other, because the IPTV service includes a service wherein content security and service security work in cooperation with each other.

Examples of subscriber threats are listed in Table I.1.

**Table I.1 – Subscriber security categories**

	Subscriber security		
	Example of service	Sample threats	Example of protection mechanism
<b>Content security</b>	Linear TV, VoD service	Illegal copy	TD identification (service protection, content protection)
<b>Service security</b>	Bidirectional service	Phishing	Personal identification (protection of personal data, PIN/password)
	Parental	Spoofing	Personal identification (PIN/password, authentication)
<b>Network security</b>	Not specified	Eavesdropping	Subscriber line identification Encryption data, multicast join control
<b>Terminal device security</b>	P2P service	Illegal copy	Content protection (P2P)

## Appendix II

### Interoperability of SCP

(This appendix does not form an integral part of this Recommendation)

#### II.1 Overview of interoperability of SCP

There are several scenarios of interoperable SCP: SCP-EE, SCP-B, and SCP-IX. The interoperable SCP can be applied to either the service provider domain or end-user domain. This appendix focuses only on the terminal side.

#### II.2 Interoperable SCP scenarios

Interoperable SCP scenarios are classified into at least three modes: SCP end-to-end (SCP-EE), SCP bridging (SCP-B), and SCP interchange (SCP-IX).

##### 1) SCP end-to-end (SCP-EE)

**SCP-EE:** Using a single SCP, two or more devices exchange and access content according to the granted rights. This mode is the simplest mode to implement, since only a single SCP is used.

##### 2) SCP bridging (SCP-B)

**SCP-B:** On a single TD, two or more SCPs are deployed. Content acquired via one SCP system (e.g., from a network) can be accessed via another SCP residing on the same device according to the granted rights.

##### 3) SCP interchange (SCP-IX)

**SCP-IX:** This case is characterized by two or more devices, with each device having one or more deployed SCPs. Content acquired by one device through one of its SCPs can be securely transferred to and accessed on another device through a different SCP, according to the granted rights.

Figure II.1 illustrates a model of the case described above.

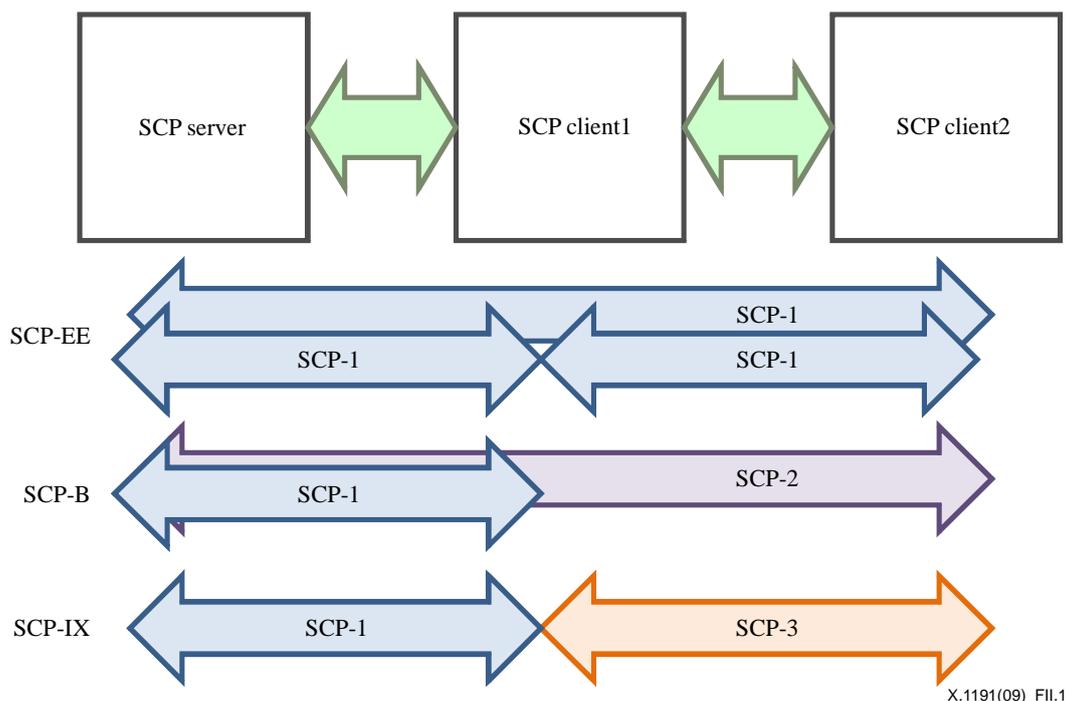


Figure II.1 – SCP interoperability mode

### **II.3 Technical areas of SCP interoperability**

The following areas represent the key interoperability elements required in SCP-EE, SCP-B, and SCP-IX modes:

#### **1) Authentication of devices, users, and SCPs**

Before content can be exchanged between entities, the identifier of the terminal device and possibly its user(s) must be established securely. Moreover, since content providers may not trust specific SCPs, authenticating the receiving SCP(s) or implementation levels before exchanging content should be possible. Such authentication should have a sound cryptographic basis and may employ various well-known digital signature techniques. Public key cryptography in particular provides a sound mechanism for digital signatures in authentication protocols.

#### **2) Rights expression exchange**

Different SCPs use different rights expression languages or license formats. For SCP-B and SCP-IX modes to function, a means of common rights expression is required. This could take the form of a common rights expression language (REL) or a rights expression translator. Another possible rights expression exchange mechanism is license negotiation.

#### **3) Common encryption algorithms for content exchange**

For content to pass securely from the control of one SCP to another or within the same SCP but on different physical devices, content encryption is required. This renders the content unusable except for entities possessing the appropriate key or keys necessary for decryption to occur. There are many different types of encryption algorithms (e.g., block ciphers, stream ciphers, public key-based, etc.), but those using symmetric keys generally tend to be best suited for high-speed content exchange. For interoperability purposes, a small number of commonly agreed upon algorithms must be chosen. Ideally, one default algorithm should also be specified.

#### **4) Key management and/or exchange for common encryption algorithms**

Before secure content exchange can take place, the keys to be used in specific instances need to be exchanged or commonly generated by the authenticated entities. Key management is usually the most difficult part to implement in a security system. Techniques such as public key cryptography have simplified device key distribution but require a public key infrastructure (PKI) to establish and maintain the validity of these keys. Such infrastructure could be sanctioned and maintained by a license authority responsible for content protection (as opposed to general network security).

#### **5) Secure download of the SCP client**

Ideally, any TD would be able to exchange content obtained (legitimately) through other devices and/or using any SCP according to the granted rights (i.e., SCP-IX mode). Note, however, that pre-loading at the manufacture time every TD with every SCP system demanded by market forces is hardly practical; hence the need for a secure mechanism for downloading and executing a selected SCP system onto a terminal device. Elements such as secure boot loaders and secure download protocols play a part in this area of interoperability.

NOTE – When SCP interoperability is deployed in the devices and end systems, IPTV devices should have a trusted architecture to support the interoperability of content security.

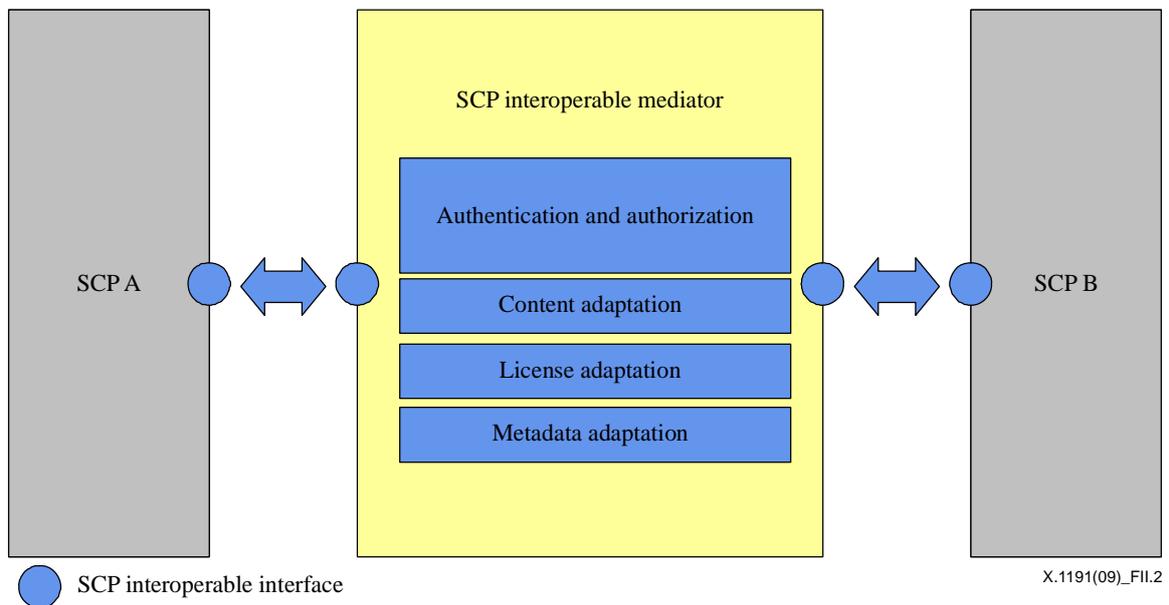
#### **6) Secure rights export**

To export digital rights securely, the IPTV SCP client should check whether usage rights are permitted to export targeting the SCP system. Digital rights may have rights expressions that enable the target SCP system to export rights. In this case, the IPTV SCP client should check these rights expressions and authorize proper target SCP systems to export digital rights.

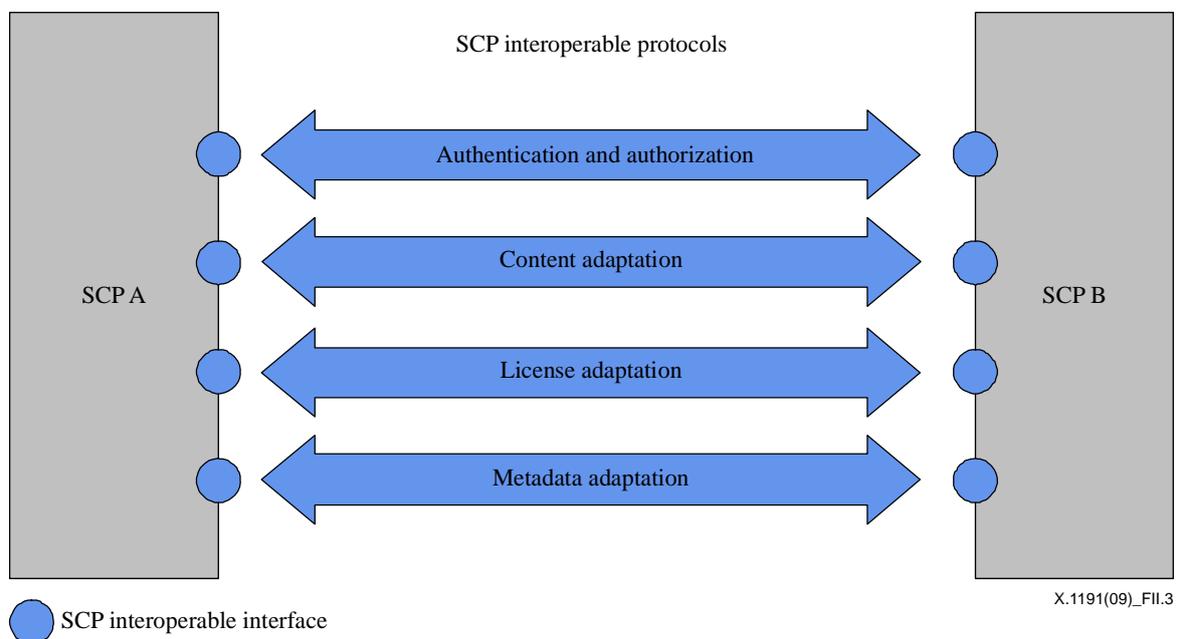
## II.4 SCP interoperable architectures

Two kinds of possible SCP interoperable architectures can be considered; one is based on mediator-based interoperability architecture, which uses a mediator system located in the middle of two SCP systems to process interoperable transmission. The other one is a standard protocol-based architecture using standard interfaces and protocols to transform protected digital content and associate information between two different SCP systems.

The two possible architectures are shown in Figures II.2 and II.3.



**Figure II.2 – Mediator-based SCP interoperable architecture**



**Figure II.3 – Standard protocol-based SCP interoperable architecture**

## Function block description

- **Content adaptation:** Content adaptation is responsible for converting cryptographic algorithm. The several predefined standard encryption algorithms given will facilitate these processes.
- **License adaptation:** License adaptation is responsible for converting a license. Any temporal or standard license known to both parties should maintain almost the same permission behaviours (media assets and consumption permission pair) as defined by the original license. A set of right mapping (rights expression mapping and semantic mapping) may be included in the license adaptation. Moreover, license adaptation may be responsible for repackaging the right information and securely delivering it to native SCP clients.
- **Metadata adaptation:** Metadata adaptation is responsible for converting metadata information. The temporal or standard metadata known to both parties should maintain the same information as what the original metadata had. A set of metadata mapping (syntax and semantic mapping) may be included in the metadata adaptation. In addition, metadata adaptation may be responsible for repackaging metadata information and securely delivering it to the other SCP party.
- **Authentication and authorization:** Each SCP party should judge whether the other party is a proper target for achieving SCP interoperability. It is usually accompanied by the mutual authentication process as a preliminary step between two SCP parties.

**Exceptional case:** If SCP A and SCP B are located within the same device, or in case of a dedicated secure communication channel between two SCPs, the content adaptation process may not require interoperable processing.

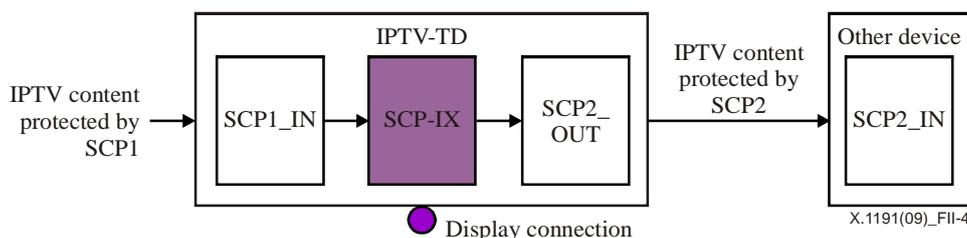
## II.5 Scenarios of SCP-B or SCP-IX deployed in TD

This clause describes three possible scenarios requiring SCP interchange between service security and content security.

### II.5.1 Definitions of terms used in the diagram

- SCP\_IN: Input port through which IPTV content protected by SCP comes in
- SCP\_OUT: Out port through which IPTV content protected by SCP goes out

### II.5.2 Scenario 1: SCP with SCP-IX

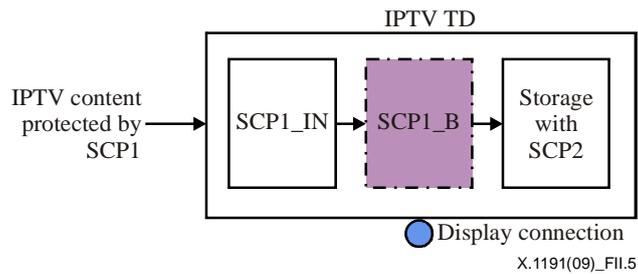


**Figure II.4 – SCP with SCP-IX**

IPTV TD (terminal device) in this case has SCP with SCP-IX to support interoperability between the IPTV TD without storage that adopts only specific service security and the external device with storage having specific content protection only.

To support secure and flexible connectivity to any kind of external device adopting various content protection mechanisms, IPTV TD should have SCP-IX rather than case-to-case implementation for security connection between two devices.

### II.5.3 Scenario 2: SCP with optional SCP-B and storage



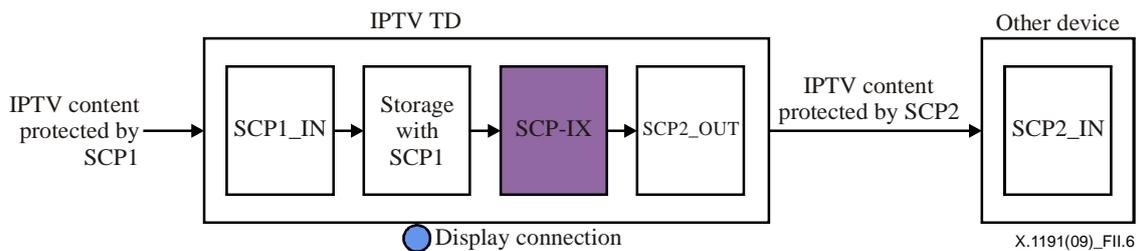
**Figure II.5 – SCP with optional SCP-B and storage**

IPTV TD in this case has SCP with SCP-B to support interoperability between service protection and content protection on a single device.

The manufacturer of IPTV TD may adopt the proprietary content protection mechanism for internal storage. In such a case, SCP\_B is not necessary, and SCP1 may be used by the storage.

To support flexible connectivity to any kind of internal storage that adopts various content protection mechanisms, IPTV TD is recommended to have SCP\_B rather than the case-to-case implementation for security connection between service protection and content protection.

### II.5.4 Scenario 3: SCP with storage and SCP-IX



**Figure II.6 – SCP with storage and SCP-IX**

In this case, IPTV TD has SCP with storage and SCP-IX to support interoperability between the internal content protection mechanism and the external one.

To support flexible connectivity to any kind of external storage that adopts various content protection mechanisms, IPTV TD is recommended to have SCP-IX rather than the case-to-case implementation for security connection between the internal content protection mechanism and the external one.

## Appendix III

### Example of IPTV content protection process

(This appendix does not form an integral part of this Recommendation)

The following describes a sample process of VoD application for content protection:

- *Subscriber authentication phase*
  - A subscriber selects a VoD application through the "service and application discovery and selection client functional block."
  - The "IPTV application functions" will send the request upon receipt to the "application profile functional block" to verify this subscriber. If successful, the authorization information pertinent to this subscriber will be cached in the "application profile functional block" for query.
- *Content selection phase*
  - The subscriber can select the specific media content using information from the ECG, and the "VoD application functional block" will deliver the selected content location information (URL) to the TD.
  - The "VoD client functional block" in the TD receives the content location for transmission to the "content delivery client functions."
- *Encrypted content delivery phase*
  - The "content delivery client functions" apply for the media content (encrypted) using the content location information; they also apply for the rights and keys associated with this content from the "content protection client functional block."
- *Rights and keys distribution phase*
  - If it does not have the rights and keys, the "content protection client functional block" will request for such information from the "rights & keys management functional block" in the IPTV service provider.
  - The "rights & keys management functional block" will apply for authorization information associated with this subscriber with the "application profile functional block" to check whether the subscriber has a right to consume this content using information.
  - If successful, the right and key for the selected contents will be delivered to the "content protection client functional block."
  - Upon receipt, the "content protection client functional block" will transfer the key and right to "content delivery client functions" to decrypt the contents and to control their usage.

## Appendix IV

### DVB content protection and copy management

(This appendix does not form an integral part of this Recommendation)

This appendix provides an outline of the set of DVB content protection and copy management (DVB-CPCM) specifications, which were developed in ETSI.

DVB-CPCM is an example of a fully standardized system for the protection of television and other content within a home network and beyond. DVB-CPCM can acquire content from an ITU-defined (or other) IPTV service protection mechanism and maintain IPTV content protection throughout the content lifecycle from acquisition to consumption including the storage, processing, and export of protected content to other IPTV security mechanisms while maintaining correct authorized usage.

#### IV.1 Introduction

DVB CPCM is a system for content protection and copy management of commercial and free-to-air digital content delivered to consumer products and home networks. CPCM manages content usage from acquisition into the CPCM system up to final consumption or export from the CPCM system, in accordance with the particular usage rules of such content. CPCM is intended for use in protecting all types of content, e.g., audio, video, and associated applications and data. CPCM provides specifications to facilitate the interoperability of such content after acquisition into CPCM by networked consumer devices for both home networking and remote access. The specification is made up of parts, some of which specify signalling and actions required for technical compliance and other parts explaining the rationale behind the specification including implementation guidelines. A reference model provides the framework for the CPCM system and serves as the foundation on which the remaining specification elements are built.

#### IV.2 Definitions

This appendix defines the following terms in addition to those in the main body:

**IV.2.1 acquire:** Involves receiving and ingesting content from outside the CPCM system into the CPCM system.

**IV.2.2 acquisition point (AP):** Abstract CPCM functional entity wherein content acquisition takes place.

**IV.2.3 acquisition:** Receipt and ingestion of content outside the CPCM system into the CPCM system.

**IV.2.4 authorized domain (AD):** A distinguishable set of DVB CPCM-compliant devices that are owned, rented, or controlled by members of a single household; a household is considered the social unit consisting of all individuals who live together as occupants of the same domicile (it makes no assumptions regarding the physical locations of the devices owned, rented, or controlled by the members of the household).

**IV.2.5 authorized usage:** The permitted usage of CPCM content; consists of a set of usage rule assertions applied to such content.

**IV.2.6 consume:** Involves tangibly rendering content or outputting content restricted from inhibiting any other usage.

**IV.2.7 consumption point (CP):** Abstract CPCM functional entity wherein consumption is executed.

**IV.2.8 consumption:** Tangible rendition of content or device output containing a transformation or a signal intended to inhibit usage other than the immediate conversion of the content to sound and image.

**IV.2.9 content item:** A discrete instance of content with finite duration, e.g., program/event or incomplete segment thereof.

**IV.2.10 content license:** A securely maintained and communicated data structure containing the information necessary to manage the security of a CPCM content item.

**IV.2.11 content:** Data to be protected by the CPCM system; this generally refers to audiovisual content including optional accompanying data such as subtitles, images/graphics, animations, web pages, text, games, software (both source code and object code), scripts, or any other information to be delivered to and consumed by a user.

**IV.2.12 copy:** A CPCM-managed process wherein a new stored content item is created from acquired content or from an existing stored content item.

**IV.2.13 CPCM device:** Device that hosts one or more CPCM instances.

**IV.2.14 CPCM system:** The set of all compliant-CPCM devices.

**IV.2.15 device application:** Any non-CPCM functionality within a CPCM device.

**IV.2.16 export point (EP):** Abstract CPCM functional entity wherein CPCM content leaves the CPCM system.

**IV.2.17 export:** Release of CPCM content from explicit protection and management by the CPCM system to a controlled CPS, a trusted CPS, or an untrusted space.

**IV.2.18 move:** Process of making a copy wherein the original is then removed, erased, or rendered no longer accessible.

**IV.2.19 output:** Device interface or CPS used to transmit CPCM content, consumed content, or exported content.

**IV.2.20 processing entity (PE):** Abstract CPCM functional entity where CPCM content is processed.

**IV.2.21 processing:** A CPCM-compliant operation on encrypted or unencrypted content aside from consumption or export, e.g., CPCM content undergoes a permitted transformation from its original form to create new transformed CPCM content, or information such as audio volume levels or still images are extracted from the content.

**IV.2.22 usage state information (USI):** CPCM content metadata that signals authorized usage for each CPCM content item.

**IV.2.23 view:** Consume.

NOTE – This also includes listen for audio-only content.

**IV.2.24 viewing:** Consumption.

NOTE – This also includes listening for audio-only content.

### **IV.3 Abbreviations and acronyms**

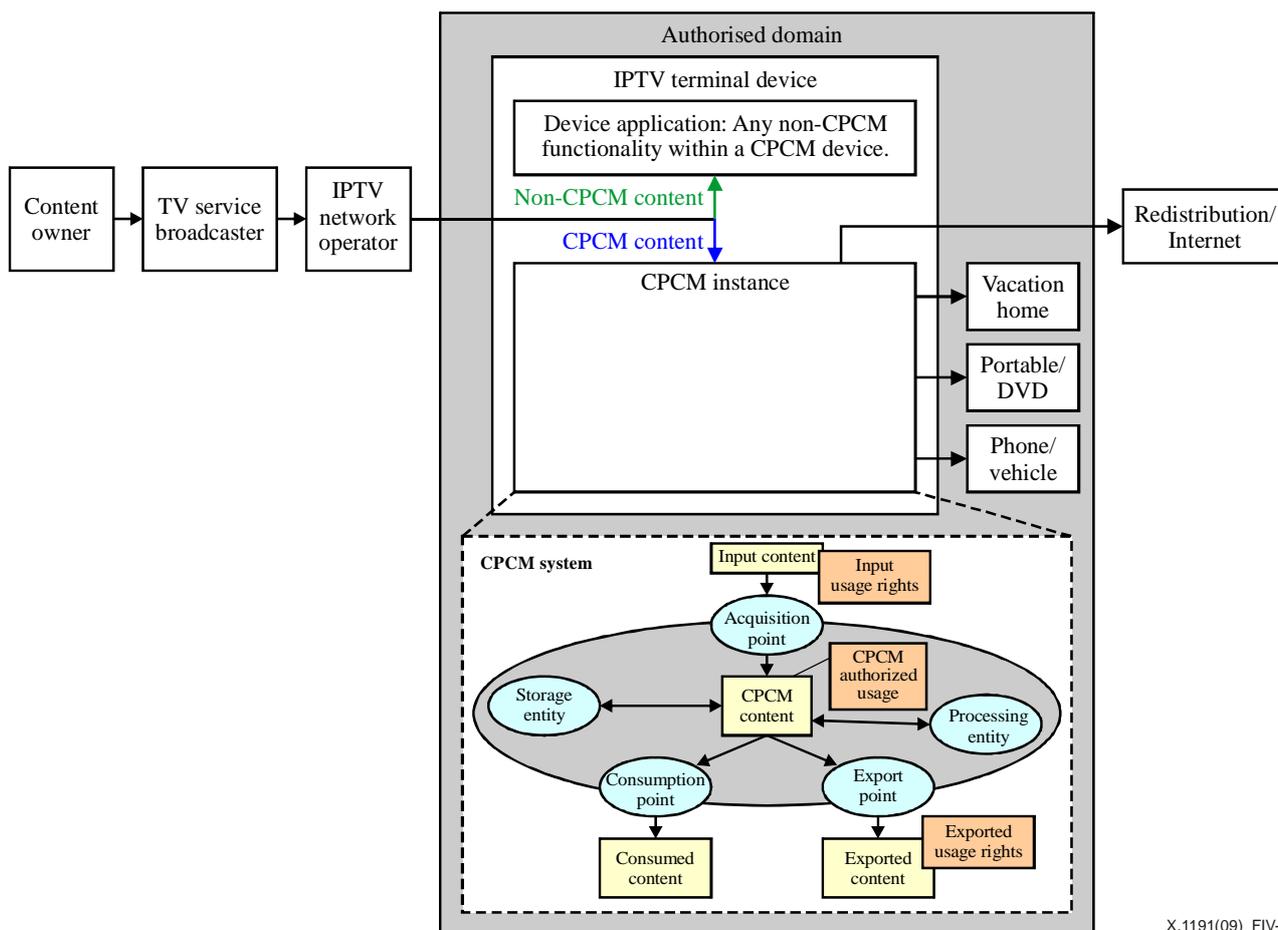
This appendix uses the following abbreviations in addition to those in the main body:

AP	Acquisition Point
APECS	Acquisition, Processing, Export, Consumption, Storage
CL	Content License
CP	Consumption Point

CPCM	Content Protection and Copy Management
CPE	Customer Premises Equipment
CPS	Content Protection System
DVB	Digital Video Broadcasting
EP	Export Point
PE	Processing Entity
SE	Storage Entity
USI	Usage State Information

#### IV.4 CPCM architecture

At the heart of CPCM is the "authorized domain", a collection of devices belonging to a household even when they are away from home. The AD concept recognizes that tying content to a single set top box (TD) and an attached TV display is not enough in the age of networked entertainment. CPCM takes content from a trusted source such as an IPTV SCP system as an embodiment or a part of the TD and protects the received content stream or file, managing how it can be viewed, moved, and copied. As the basic CPCM content management model, input content enters the CPCM system to become CPCM content. CPCM content is managed and protected within the CPCM system; it leaves the CPCM system when it is consumed by the user or exported to another system.



X.1191(09)\_FIV-1

Figure IV.1 – Content flow in a CPCM environment

CPCM supports a variety of uses for content on a home network; it can also manage access to content from remote locations such as a laptop on a broadband Internet connection. Using CPCM, service providers can signal to device manufacturers the permissible scenarios for each type of content. This extends many of today's protection methods such as those embodied in IPTV SCP technologies, wherein content is typically restricted to a single point-to-point interconnection cable between the content source device (such as a set top box) and the digital display device.

CPCM goes beyond such localized protection, giving broadcasters, network operators, and content owners the option to allow access by a household member from a remote location, such as a hotel, during a business trip or a vacation.

CPCM can also allow users to copy content to portable devices and removable storage such as a DVD. As long as the playback device belongs to the same authorized domain, the device will be able to play back the content even when it is disconnected from the home and the original service provider. CPCM content does not require any online authorization from a service provider to add or remove devices to/from the authorized domain.

The CPCM content protection system is not a standalone entity; it is incorporated/overlaid into the overall end-to-end IPTV SCP distribution system. As such, it coexists with rather than replaces an IPTV SCP system. In any TD, the CPCM instance is optional; if it is not present, however, it will not be granted access to any CPCM-protected content. Still, the TD does not need to implement all CPCM elements. Only those that are useful to the TD are required to perform the functionality it needs. For example, a simple device may only implement CPCM acquisition and consumption functionalities if it has no CPCM storage or export requirements.

#### **IV.5 CPCM reference model and functional entities**

The CPCM reference model defines the set of five abstract content management functions covering all relevant content usage scenarios in the consumer environment: acquisition, storage, processing, consumption, and export. These functions map to the five CPCM functional entities: acquisition point, storage entity, processing entity, consumption point, and export point. Figure VI.1 shows a view of the CPCM system in terms of the set of abstract functional entities.

Thus, the input content entering the CPCM system does so through its acquisition at an acquisition point by a CPCM device implementing such an acquisition point to become CPCM content. CPCM content can be stored or processed by the corresponding functional entities (storage entity, processing entity) implemented on a CPCM device. CPCM content leaves the CPCM system when it is consumed at a consumption point or exported at an export point. Again, these functional entities can be implemented inside any CPCM device.

#### **IV.6 CPCM-authorized domain**

CPCM devices can be logically grouped into authorized domains. If all those devices belong to one household, then they would constitute that household's authorized domain (AD). Thus, the authorized domain provides a destination for content that maps to the bounds of a single household. Generally, AD can be viewed as the logical grouping of all CPCM devices belonging to one household, devices located in the main domicile, devices located at another domicile (e.g., holiday home), portable handheld devices that are only connected intermittently with the above-mentioned stationary devices, or devices fitted to the vehicles(s) belonging to that household. AD is designed to be an autonomous logical group of devices; it does not require any external administration. Note, however, that there may be cases wherein AD is linked to a particular service provider that may offer to administer AD as part of its service provision to the consumer.

#### **IV.7 CPCM content usage rules**

The authorized usage for any item of CPCM content is the set of usage assertions expressed in the CPCM usage rules tied to the content. The CPCM usage rules may be set by the content or service provider or mapped from the form of delivery (e.g., free-to-air broadcast). The extent at which storage, consumption, and export operations can be performed may be subject to the content's authorized usage. CPCM defines a common set of usage rules any content provider can select from and derive the desired authorized usage for the content within the CPCM system accordingly. The set of CPCM usage rules is designed to be flexible enough to cover all applicable content protection and management models, as well as concise enough to maintain clear and relatively simple content usage models for the consumer.

#### **IV.8 Usage state information metadata**

The authorized usage of a content item is coded as CPCM content metadata called usage state information (USI). CPCM content is managed and protected according to the USI applied to each content item. Apart from the compliant USI state transitions carried out implicitly by the CPCM system, entities holding legitimate authorization over content within the CPCM system can execute other changes to a content item's USI state after acquisition in the CPCM system.

#### **IV.9 CPCM content**

"Content" generally refers to audiovisual content plus optional accompanying data such as subtitles, images/graphics, animations, web pages, text, games, software (both source code and object code), scripts, or any other information to be delivered to and consumed by a user. CPCM content is content protected and managed by and in conformity with the CPCM system. A content item is a discrete instance of content with finite duration. Each CPCM content item is accompanied by a content license carrying the associated USI together with more CPCM metadata. The CPCM system can handle the content license and content item itself in different ways, depending on the target functionality and/or usage rules enforcement as required by USI.

#### **IV.10 CPCM device**

A CPCM device is a device that implements any CPCM functionality in a compliant manner. The implementation of the CPCM functionality is referred to as a CPCM instance. A CPCM device is a device that hosts one or more CPCM instances. It can also contain other non-CPCM compliant functions in addition to its CPCM functionality. CPCM content handling is performed only by the CPCM instance inside the device. The non-CPCM part of the device has no access to CPCM content. The CPCM device can also host the non-CPCM secure functionality for the secure acquisition of content from other protection systems or secure export (or possibly consumption) of CPCM content.

#### **IV.11 Usage rule and usage state information**

A usage rule in CPCM is a particular operation or behaviour of the content to be controlled within the scope of the CPCM system. The complete set of usage rule assertions for a particular CPCM content item is referred to as the authorized usage of such CPCM content item. A content item's authorized usage is expressed by its coding in usage state information (USI), the CPCM content metadata that signals the authorized usage for that particular content.

## Appendix V

### Secure transcodable scheme

(This appendix does not form an integral part of this Recommendation)

#### V.1 Overview of the secure transcodable scheme

The transcoding of content has attracted a lot of attention due to the increasing popularity of various types of devices such as PDA, non-PC devices, cellular phones, and smart mobile terminal. Transcoding refers to a process of transforming multimedia content such as images, text, audio, and video from original format to a different format or quality.

Transcoding seeks to reduce the download delay of multimedia content over low-bandwidth access links such as modem links and wireless access links, and resolve the mismatch between the encoding format supported by a client device and that employed by a multimedia content provider. It also allows the computational constraint terminal to display the content encoded based on the transcoding capability.

There are three entities for the secure transcodable scheme: a sender, an intermediate network node, and a user with an IPTV terminal. The transcoding function resides in an intermediate network node placed between the content provider and the client device. There are two kinds of transcoding architectures: traditional transcoding architecture and secure transcoding architecture.

In traditional transcoding architecture, a transcoding proxy is used as an intermediate network node between the content server and the client device. A sender encrypts the content with adequate compression and sends the encrypted content to the intermediate network node called transcoding proxy. The transcoding proxy decrypts the encrypted content with decompression. It then changes the size of content or its format with new compression and finally re-encrypts the transcoding data for transmission to the client device. The client device decrypts the encrypted content and decompresses the content using new compression algorithm. Note, however, that a security problem occurs in the transcoding proxy, i.e., once the content has been decrypted in the transcoding proxy and before it is encrypted, the unencrypted content resides in the transcoding proxy. In other words, an observer can access the unencrypted content through eavesdropping. Such unencrypted content weakens the end-to-end security guarantee of the privacy, wherein only the sender and the legitimate client are supposed to access the content in unencrypted state.

To address the security problem, secure transcoding architecture was suggested. A secure transcodable scheme is a kind of a security scheme that enables the intermediate network node to perform transcoding without decryption while preserving end-to-end security. This scheme can be executed by combining scalable coding, progressive encryption, and packetizing. A sender performs a secure transcodable function to produce scalable encrypted packets from the video and adds the unencrypted header to send the information; an intermediate network node reads the unencrypted header and uses the information to truncate or discard the adequate packets according to the desired transcoding operation, with the IPTV terminal decrypting the encrypted packets and decoding the plain-text packet to produce the video.

## Bibliography

- [b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006) | ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.
- [b-ITU-T H.622.1] Recommendation ITU-T H.622.1 (2008), *Architecture and functional requirements for home networks supporting IPTV services*.
- [b-ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operator's networks*.
- [b-ITU-T Q.1290] Recommendation ITU-T Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks*.
- [b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for open systems interconnection for CCITT applications*.
- [b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.
- [b-ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services*.
- [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [b-ETSI TS 102 825] ETSI TS 102 825 (all parts), *Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM)*.  
<<http://pda.etsi.org/pda/AQuery.asp>>
- [b-ATIS 0800001] ATIS 08000001, *IPTV DRM Interoperability Requirements, ATIS-IIF*, April 2007.  
<<https://www.atis.org/docstore/product.aspx?id=21212>>
- [b-ATIS 0800006] ATIS 08000006, *IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification*, February, 2007.  
<<https://www.atis.org/docstore/product.aspx?id=22663>>



## SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
<b>Series X</b>	<b>Data networks, open system communications and security</b>
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems