

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
IPTV security	X.1180–X.1199
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

Page

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

Copyright International Telecommunication Union/ITU

	Page
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.

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

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.

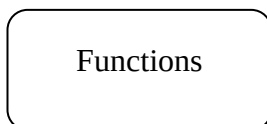
The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

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.

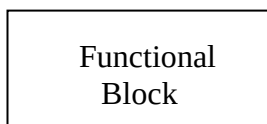
The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service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