

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1192

(05/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

Functional requirements and mechanisms for the secure transcoding of IPTV

Recommendation ITU-T X.1192



International
Telecommunication
Union

Document Sharing Hub

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
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1192

Functional requirements and mechanisms for the secure transcoding of IPTV

Summary

Recommendation ITU-T X.1192 deals with the functional requirements, architecture, and mechanisms that pertain to the security of transcoding protected IPTV content. Generic security of IPTV content is not discussed in this Recommendation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1192	2011-05-29	17

Keywords

Secure transcoding.

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 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 2012

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	4
5	Conventions	4
6	Overview	5
	6.1 Transcoding	5
	6.2 General transcoding architecture with protection.....	6
7	Security threats	7
	7.1 General security threats	7
	7.2 Security threats in transcoding	8
8	Security requirements for the secure transcoding of protected content.....	9
	8.1 General security requirements	9
	8.2 Security requirements for secure transcoding	10
9	Secure transcodable mechanism	11
	9.1 Overview of the secure transcodable mechanism	11
	9.2 Security components of the secure transcodable mechanism.....	11
	Appendix I – Reference points for secure transcoding in IPTV	22
	I.1 Transcoding reference points	22
	I.2 Types of transcoders.....	23
	I.3 Security requirements for the transcoding reference points	23

Recommendation ITU-T X.1192

Functional requirements and mechanisms for the secure transcoding of IPTV

1 Scope

This Recommendation deals with the functional requirements, architecture, and mechanisms that pertain to the security of transcoding protected IPTV content. Generic security of IPTV content is not discussed in this Recommendation. In particular, since unprotected IPTV content can be open to any user, the security of transcoding unprotected IPTV content is not discussed in this Recommendation.

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 H.234] Recommendation ITU-T H.234 (2002), *Encryption key management and authentication system for audiovisual services*.
- [ITU-T H.235.6] Recommendation ITU-T H.235.6 (2005), *H.323 security: Voice encryption profile with native H.235/H.245 key management*.
- [ITU-T H.264] Recommendation ITU-T H.264 (2007), *Advanced video coding for generic audiovisual services*.
- [ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T T.807] Recommendation ITU-T T.807 (2006) | ISO/IEC 15444-8:2007, *Information technology – JPEG 2000 image coding system: Secure JPEG 2000*.
- [ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.
- [ITU-T Y.1910] Recommendation ITU-T X.1910 (2008), *IPTV functional architecture*.
- [ISO/IEC 14496-2] ISO/IEC 14496-2:2004, *Information technology – Coding of audiovisual objects – Part 2: Visual*.

Document Sharing Hub

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 base layer [ITU-T H.264]: A *bitstream subset* that contains all the *NAL units* with the *nal_unit_type syntax element* equal to 1 and 5 of the *bitstream* and does not contain any *NAL unit* with the *nal_unit_type syntax element* equal to 14, 15, or 20 and conforms to one or more of the profiles specified in Annex A of [ITU-T H.264].

3.1.2 bitstream [ITU-T H.264]: A sequence of bits that forms the representation of *coded pictures* and associated data forming one or more *coded video sequences*. Bitstream is a collective term used to refer either to a *NAL unit stream* or a *byte stream*.

3.1.3 content protection [ITU-T X.1191]: Ensuring that an end user can only use the content 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.

3.1.4 decoder [ITU-T H.264]: An embodiment of a *decoding* process.

3.1.5 encoder [ITU-T H.264]: An embodiment of an *encoding* process.

3.1.6 instantaneous decoding refresh (IDR) picture: A *coded picture* in which all *slices* are *I* or *SI* *slices* that causes the *decoding process* to mark all *reference pictures* as "unused for reference" immediately after decoding the IDR picture. After the decoding of an IDR picture all following *coded pictures* in *decoding order* can be decoded without *inter prediction* from any *picture* decoded prior to the IDR picture. The first *picture* of each *coded video sequence* is an IDR picture.

3.1.7 intra prediction [ITU-T H.264]: A *prediction* derived from the decoded samples of the same decoded slice.

3.1.8 layer [ITU-T H.264]: One of a set of syntactical structures in a non-branching hierarchical relationship. Higher layers contain lower layers. The coding layers are the *coded video sequence*, *picture*, *slice*, and *macroblock* layers.

3.1.9 motion vector [ITU-T H.264]: A two-dimensional vector used for *inter prediction* that provides an offset from the coordinates in the *decoded picture* to the coordinates in a *reference picture*.

3.1.10 NAL unit [ITU-T H.264]: A *syntax structure* containing an indication of the type of data to follow and *bytes* containing that data in the form of an *RBSP* interspersed as necessary with *emulation prevention bytes*.

3.1.11 picture parameter set [ITU-T H.264]: A *syntax structure* containing *syntax elements* that apply to zero or more entire *coded pictures* as determined by the *pic_parameter_set_id syntax element* found in each *slice* header.

3.1.12 residual [ITU-T H.264]: The decoded difference between a *prediction* of a sample or data element and its decoded value.

3.1.13 secure transcodable scheme [ITU-T X.1191]: A kind of a security scheme enabling the intermediate network node to perform the transcoding without decryption while preserving an 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.

3.1.14 sequence parameter set [ITU-T H.264]: A *syntax structure* containing *syntax elements* that apply to zero or more entire *coded video sequences* as determined by the content of a *seq_parameter_set_id syntax element* found in the *picture parameter set* referred to by the *pic_parameter_set_id syntax element* found in each *slice header*.

3.1.15 service protection [ITU-T X.1191]: 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.

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

3.1.17 transcoding [ITU-T X.1191]: Process of transforming multimedia content such as images, text, audio, and video from the original format to a different format or quality.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 entropy coding: Lossless data compression scheme that is independent of the specific characteristics of the medium. One of the main types of entropy coding creates and assigns a unique prefix code to each unique symbol that occurs in the input. The entropy encoders then compress data by replacing each fixed-length input symbol with the corresponding variable-length prefix codeword.

3.2.2 entropy decoding: Inverse process of *entropy coding*.

3.2.3 hybrid-type selective encryption: Combination of post-compression and in-compression selective encryption. In this approach, selective encryption is carried out at two points, during and after encoding, for better content security.

3.2.4 in-compression selective encryption: Selective encryption performed during the encoding process.

3.2.5 intra-prediction mode: Direction mode of *intra-prediction*.

3.2.6 inverse quantization: Inverse process of *quantization*.

3.2.7 inverse transformation: Inverse process of *transformation*.

3.2.8 motion vector difference (MVD): Difference between a previous motion vector and a current motion vector.

3.2.9 perceptual security: Security technique for measuring the visual degradation of a ciphered image (or video) with respect to its plain image (or video). It assumes that the ciphered image (or video) can be decoded without decryption.

3.2.10 post-compression selective encryption: Selective encryption performed after encoding.

3.2.11 prediction: Use of a predictor to provide an estimate of the sample value or data element currently being encoded.

3.2.12 predictor: Combination of specified values or previously encoded sample values or data elements used in the encoding process of subsequent sample values or data elements.

3.2.13 quantization: Loose compression technique applied by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible.

3.2.14 texture sign: Sign of residual data generated by the intra-prediction process.

3.2.15 transformation: Scalar quantity considered to be in a frequency domain associated with a particular one-dimensional or two-dimensional frequency index in a transform part of the encoding process.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, and Accounting
FGS	Fine Granularity Scalability
HSE	Hybrid-type Selective Encryption
IDR	Instantaneous Decoding Refresh
IPM	Intra-Prediction Mode
ISF	In-compression Selective Encryption
LAN	Local Area Network
MPEG	Moving Picture Experts Group
MVD	Motion Vector Difference
NAL	Network Abstract Layer
P2P	Peer-to-Peer
PPS	Picture Parameter Set
PSE	Post-compression Selective Encryption
SCP	Service and Content Protection
SEI	Supplemental Enhancement Information
SPS	Sequence Parameter Set
STB	Set-Top Box
STS	Secure Transcodable Scheme
SVC	Scalable Video Coding
TD	IPTV-compliant Terminal Device
TV	Television
VoD	Video-on-Demand

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a specification that 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 specification that is recommended but not absolutely required. In other words, this specification does not need to be present to claim conformance.

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