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

ITU-T

International Telecommunication Union

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/.

Table of Contents

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*.

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.

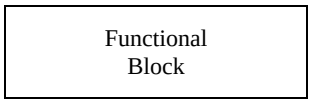
The keywords "**is recommended**" indicate a specification that is recommended but not absolutely required. In other words, this specification does not need to be present to claim conformance.

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.

The keywords "**can optionally**" indicate an optional specification that 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 that the feature can be optionally enabled by the network operator/service provider. Rather, it means that the vendor may optionally provide the feature and still claim conformance to the specification.

In the context of the secure transcodable architecture in this Recommendation:

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 Overview

6.1 Transcoding

Given the increasing popularity of various types of terminal devices, transcoding has become a very important operation. Transcoding is the ability of a network node to transform given digital content from one format or quality to another. Several types of transcoding are possible depending on the parameters of the compressed bitstream modified during the transcoding process. They include:

- quality (i.e., bit rate) transcoding;
- spatial resolution transcoding;
- frame rate transcoding;
- format transcoding (e.g., MPEG-4 bitstream to ITU-T H.264 bitstream);
- and/or their combinations.

Among the aforesaid classes of transcoding, format transcoding is not discussed in this Recommendation.

A generic IPTV service architecture is shown in Figure 6-1. In this figure, the head-end is the sender of content encoded in Code1, and user TD (STB) is the receiver of the content, assuming that the receiver can properly operate in Code1.

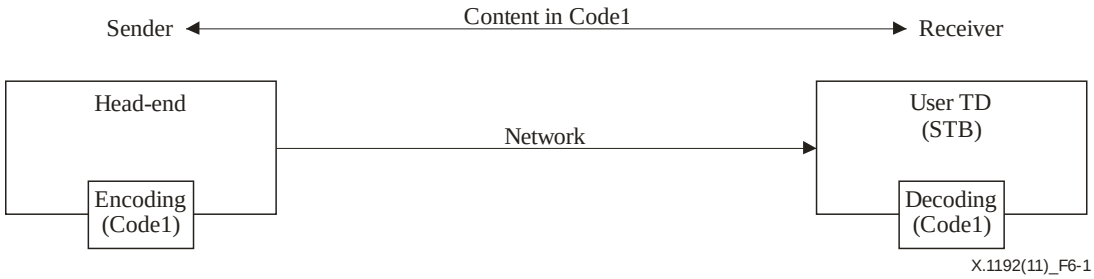


Figure 6-1 – IPTV service architecture

Note, however, that there are many situations wherein the receiver cannot properly operate in Code1. To ensure the proper operation of the receiver, transcoding of the content is required.

Transcoding generally takes place at an interim network node located between the head-end and the user terminal device. The purpose of transcoding may include but is not limited to the following:

- *To overcome network limits*: Reduce the time and bandwidth required to transmit content over low-bandwidth access, i.e., from wired to wireless.

- *To resolve the mismatch between content formats*: Content encoded in one format may not be suitable for display in the user terminal device for various reasons (for example, the format is simply not supported by the user terminal device, or the format is too big to be displayed in the user terminal).
- *To overcome computational constraint*: A user terminal device may not have enough computing and/or power resources to display the content in the original format.
- *To overcome the mismatch between SCPs*: The content protection of one SCP domain may not be supported by a device from another SCP domain.

An example of transcoding architecture is shown in Figure 6-2. In this example, the head-end is the sender of the original content encoded in Code1, and user TD (STB) is the transcoder; the user device (PDA) is the receiver of the transformed content encoded in Code2. Since the receiver can only properly operate on content encoded in Code2, the transcoder translated the original content into Code2 format.

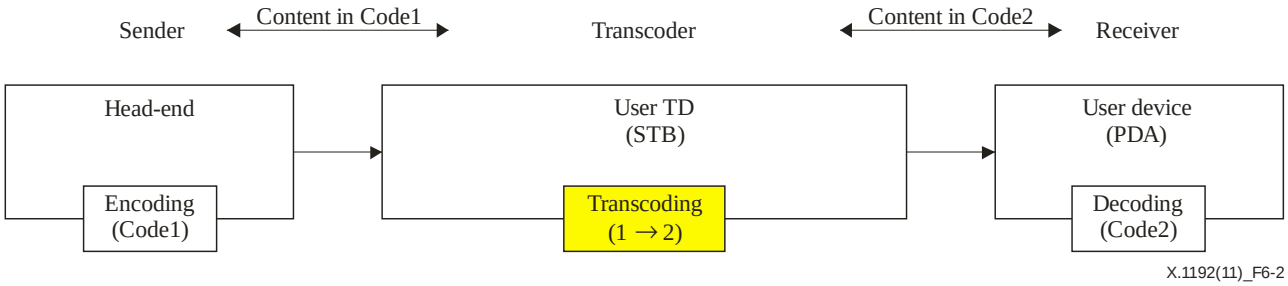


Figure 6-2 – Transcoding architecture

6.2 General transcoding architecture with protection

In general, valuable IPTV contents are protected using SCP. Since the content is intended only for the receiver, content should be protected before, during, and after transcoding.

Figure 6-3 shows a traditional architecture wherein transcoding and SCP occur at the same time. As shown in the figure, the decryption and the re-encryption functions are unnecessarily required before and after transcoding, using the same key entitled to the receiver. If the three entities are in the same service domain, only one SCP can be used. Note, however, that the transcoder should decrypt and re-encrypt content because viewing the content for transcoding is required.

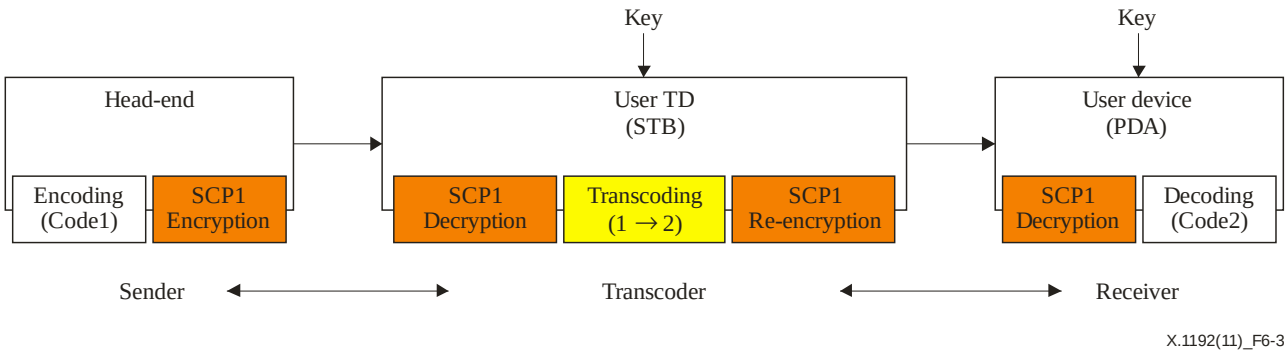


Figure 6-3 – Transcoding architecture with single protection

A more complicated situation is depicted in Figure 6-4. In this figure, a transcoder is located in a public place to serve multiple nearby receivers. This is a similar approach to the wireless LAN "hot-spot" services. First of all, if the transcoder supports several SCPs, a receiver from one SCP domain (SCP2) can benefit from the transcoder to access the content from another SCP domain (SCP1). However, to support multiple receivers (from different SCP domains), the transcoder

should possess the keys and decrypt the content prior to transcoding and re-encrypt the content after the transcoding.

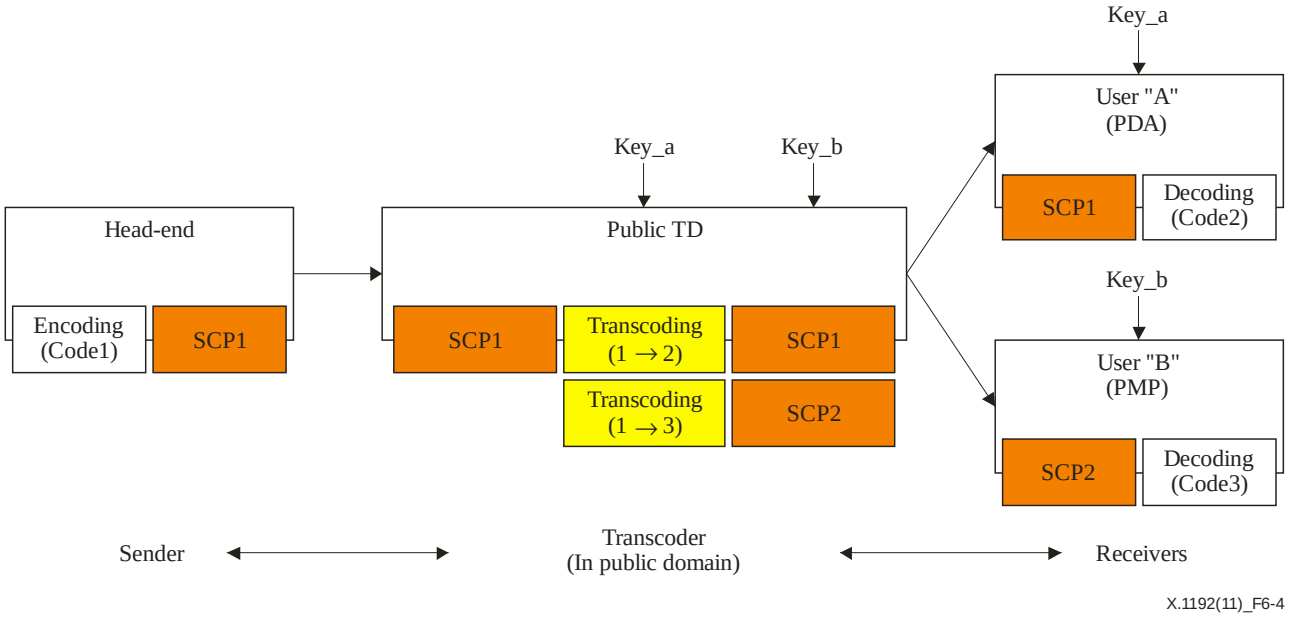


Figure 6-4 – Transcoding architecture with multiple protections

The transcoding architecture with multiple protections is not discussed in this Recommendation, since the intermediate node cannot transcode the protected content from one SCP domain to another SCP domain without keys and decryption.

7 Security threats

7.1 General security threats

The base security threat model and the other fundamental materials for general IPTV service have been addressed in [ITU-T X.1191].

[ITU-T X.1191] classified security threats to IPTV into the following types: content security threat, service security threat, network security threat, terminal device security threat, and subscriber security threat:

Content security threats

- interception,
- unauthorized viewing,
- unauthorized reproduction or redistribution.

Service security threats

- copyrights infringement of programs provided by the IPTV service platform to subscribers,
- masquerading/spoofing the IPTV service provider,
- malicious threats targeting IPTV servers (SCP servers, media servers, etc.),
- theft of subscribers' information.

Network security threats

- intentional threats targeting network equipment or resources,
- security threats to the multicast technique used in the IPTV bearer network,
- malicious attacks (such as DoS, hacking) on nodes in the content distribution network.

Terminal device security threats

- illegally accessing clear content by tampering with device hardware or software,
- illegally accessing keys or other secret information in devices using software cracking or hardware tampering,
- device malfunction by hardware method,
- downloading, running and storing in terminal devices of unauthorized applications (such as software programs),
- 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.

Subscriber security threat

- subscriber security requires that a mechanism ensuring content security and a mechanism guaranteeing service security cooperate with each other, because the IPTV service includes a service wherein content security and service security cooperate with each other.

7.2 Security threats in transcoding

In addition to the threats described in [ITU-T X.1191], additional security threats to IPTV due to the transcoding scheme are specified hereafter.

To be able to transcode, the transcoder generally needs to view the content even if the transcoder itself is not supposed to view it. Therefore, if the content is protected by SCP, SCP should allow the transcoder to access the content and key altogether.

Therefore, the transcoder would be vulnerable to possible attacks such as eavesdropping and content theft. Even possibly untrustworthy transcoders need to possess the encryption/decryption key, which raises security concerns. Examples are as follows:

- Videoconferencing or surveillance may leak their content to an unwanted eavesdropper who has tampered with the transcoder and managed to dump memory during transcoding.
- An illegitimate user may override the transcoding function of the transcoder to strip off any protection. The collected unprotected content may be redistributed to other users through the network (e.g., in P2P networks).

7.2.1 Content security threats

- **Interception/eavesdropping**: This threat is the most identifiable threat in transcoding protected content. Since the content is handled in unprotected form, the transcoder is most vulnerable to interception and/or eavesdropping attack(s), especially when the content is valuable.
- **Unauthorized viewing/redistribution**: A forged transcoder may employ an interface designed to tap into the transcoder while the transcoder handles the content in unprotected form. Through the interface, the owner of the transcoder could obtain content reserved only for the receiver. A legitimate viewer may intentionally employ such a forged transcoder to obtain the unprotected content to redistribute it through the Internet (for example, using P2P).

7.2.2 Service security threats

- **Masquerading service provider**: Without proper TD-side authentication against the service provider, a forged transcoder may play the role of service provider. Therefore, the content received from the transcoder may include (1) spam messages, (2) forged metadata, and (3) forged overlay images. Because those contents are not coming from a legitimate service provider, the content may be harmful to the receiver.
- **Privacy**: While obtaining transcoded content from a service provider through a forged transcoder, a receiver may leak its personal, subscription, and billing information.
- **Threat against IPTV service provider elements**: To obtain transcoded content from a service provider, the receiver may communicate with the service provider through a forged transcoder, which in turn collects the service provisioning information to exploit a further attack against service-provider elements such as AAA servers, media servers, etc. This may lead to a type of denial-of-service attack.

7.2.3 Network security threats

Apart from the network security threats of general IPTV services previously addressed in [ITU-T X.1191], there are no additional security threats related to the network.

7.2.4 Terminal device security threats

Apart from the terminal device security threats of general IPTV services previously addressed in [ITU-T X.1191], there are no additional security threats related to the terminal device.

7.2.5 Subscriber security threats

Apart from the subscriber security threats of general IPTV services as previously addressed in [ITU-T X.1191], there is no additional security threat related to the subscriber.

8 Security requirements for the secure transcoding of protected content

8.1 General security requirements

The security requirement for general IPTV service has been addressed in [ITU-T X.1191]. [ITU-T X.1191] classified the security requirements for general IPTV service into the following types: content security requirements, service security requirements, network security requirements, terminal device security requirements and subscriber security requirements. Parties interested in security requirements related to general IPTV service are encouraged to read [ITU-T X.1191].

In addition to the requirements described in [ITU-T X.1191], additional security requirements for the transcoding scheme are specified hereafter.

- Transcodable encryption is recommended to be efficient so that there is no delay in the transmission or access operations of transcodable media such as SVC (Scalable Video Coding) and MPEG FGS, etc.
- For efficiency, transcodable encryption is recommended to support partial encryption and lightweight encryption.
- Transcodable encryption is recommended to be compression-friendly so that it has little or no impact on the data compression ratio.
- Transcodable encryption is recommended to be compliant with standard decoders. To support format compliance, any standard decoder is recommended to support decoding the encrypted media without decryption.
- Transcodable encryption is recommended to support error tolerance so that it has little or no impact on other bits after decryption from a single bit error that occurs in the encrypted bitstream during transmission.

- Transcodable encryption is recommended to prohibit decoding error or visual distortion at the decoder as a consequence of bit error during transmission.

8.2 Security requirements for secure transcoding

8.2.1 Content security requirements

- Transcodable encryption is required to enable content confidentiality from one end to the other.
- To provide end-to-end security, transcodable encryption is required to support the intermediate network node to perform transcoding of protected content without decryption.
- The intermediate network node performing transcoding is prohibited from illegally acquiring a content-encrypted key.
- The transcodable encryption is recommended to use publicly standardized cryptographic algorithms.
- Transcodable encryption is recommended to prevent illegal users from predicting the encrypted area.
- Transcodable encryption is recommended to support perceptual security as defined in clause 3.
- Transcodable encryption is recommended to support the capability of preventing replacement attacks, which replace some of the encrypted data with certain values and reduce the encrypted video's perceptual security.
- If the transcodable encryption employs a key management system, then it is recommended that it be designed for scalability.

8.2.2 Service security requirements

- Transcodable encryption is recommended to support many types of terminals with different frame rates, qualities, and image sizes (i.e., spatial resolution).
- Transcodable encryption is recommended to support flexibility of the security level by adjusting the encryption area and/or encryption algorithm with regard to device capability, network conditions, etc. Network conditions can include network bandwidth, delay, packet loss, etc.
- The transcodable encryption is required to support the protection of content transcoded to any other image size (i.e., spatial resolution), frame rate, and quality by an intermediate node during network transmission.
- The secure transcodable scheme is required to support a mechanism to allow the TD to authenticate the intermediate node performing transcoding as well as SCP servers.
- The secure transcodable scheme is required to support a mechanism to allow intermediate nodes performing transcoding to authenticate the SCP servers.

8.2.3 Network security requirements

Apart from the network security requirements of general IPTV services addressed in [ITU-T X.1191], there are no additional network-related security requirements.

8.2.4 Terminal device security requirements

Apart from the terminal device security requirements of general IPTV services previously addressed in [ITU-T X.1191], there are no additional terminal device-related security requirements.

8.2.5 Subscriber security requirements

Apart from the subscriber security requirements of general IPTV services addressed in [ITU-T X.1191], there are no additional subscriber-related security requirements.

9 Secure transcodable mechanism

This clause provides the mechanism of the secure transcodable scheme. The mechanism of generic security of IPTV content and service is not discussed in this Recommendation. The security mechanism for the general IPTV service has been addressed in [ITU-T X.1191].

9.1 Overview of the secure transcodable mechanism

The secure transcodable mechanism is based on scalable content encoded by scalability-supporting video compression algorithms such as MPEG4 FGS, ITU-T H.264/SVC, etc. Studying scalability-supporting video compression algorithms such as MPEG4 FGS and ITU-T H.264/SVC before specifying the secure transcodable scheme is helpful. The algorithm and architecture for MPEG4 FGS and ITU-T H.264/SVC have been well-defined in [ISO/IEC 14496-2] and [ITU-T H.264], respectively. For reference, there is another codec, JPEG2000, to support video scalability. JPEG2000 is a still image-based compression algorithm, and a transcodable security architecture has been defined in the JPEG2000 Recommendation, [ITU-T T.807].

This mechanism ensures the end-to-end security of scalable content while dynamically transcoding the protected content without decryption according to the network conditions or end devices' capabilities; the former can include network bandwidth, delay, packet loss, etc., and the latter can include computing power, memory size, etc. It includes the overall procedure for creating secure transcodable content, transcoding secure content, and providing secure IPTV services for end users.

9.2 Security components of the secure transcodable mechanism

The security components of the secure transcodable mechanism are shown in Figure 9-1. The functionality of each component of the secure transcodable mechanism is shown in Table 9-1.

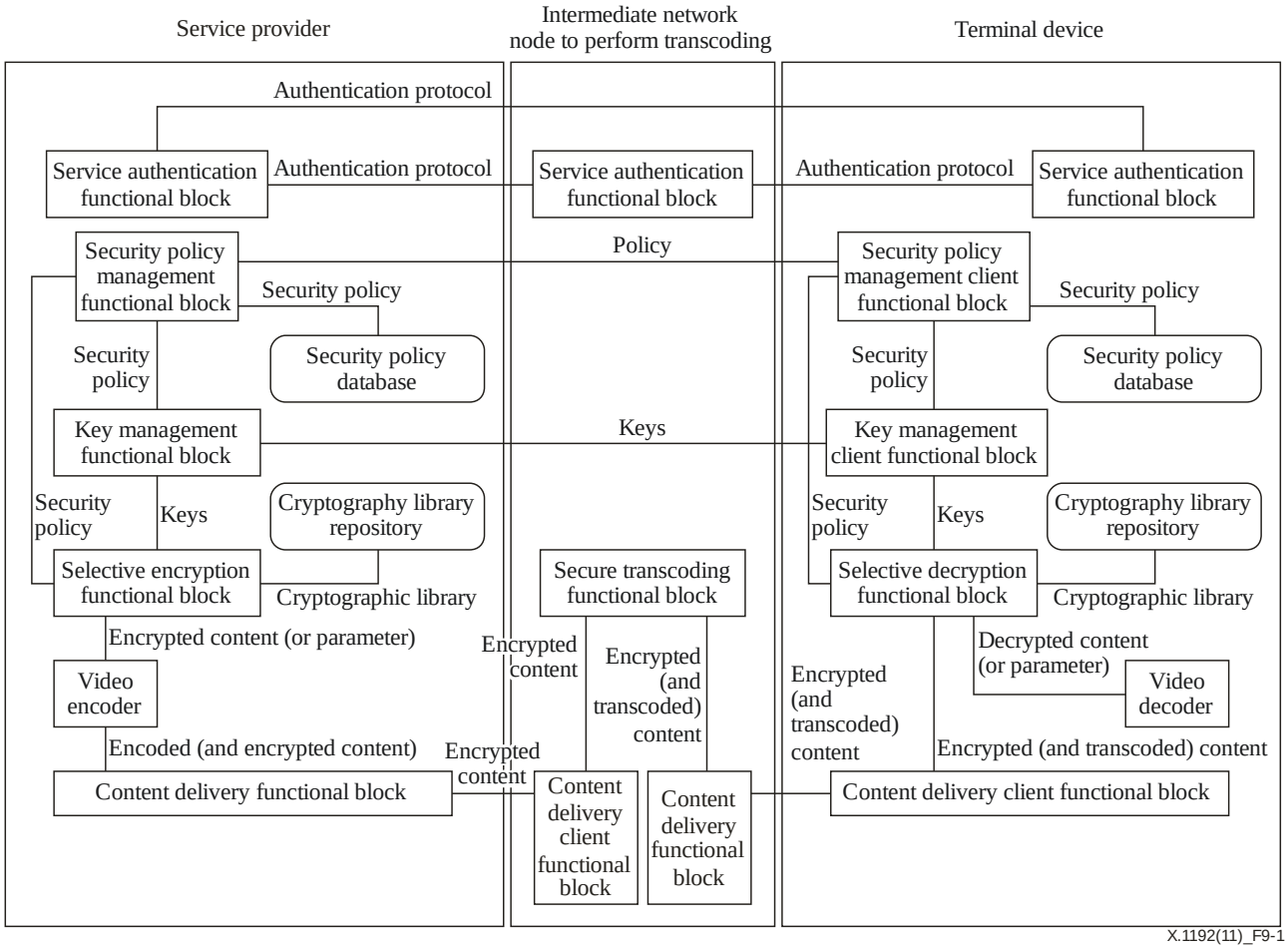


Figure 9-1 – Security components of the secure transcoding mechanism

The process of the secure transcoding mechanism is as follows:

The selective encryption functional block at the service provider creates secure transcodable content in cooperation with the video encoder. The selective encryption functional block should be controlled by policies configured by the service provider. The security policy-management functional block manages the security policy, including the encryption type, encryption method, encryption layer, parameter set, etc. Such policies are generally stored and managed in the policy database. The encryption key is provided by the key management functional block, and the cryptographic library is provided by the cryptographic library repository. The information of the selected security policy and key is transmitted to the terminal device through a particular channel. The structure of the policy database and the key management mechanism are described in clauses 9.2.5 and 9.2.4, respectively. The encrypted content is delivered to the intermediate network node to perform transcoding through the content-delivery functional block. The service authentication functional block provides the functionality to authenticate the server, intermediate node to perform transcoding, and TDs. In the service provider, the service authentication functional block is responsible for authenticating subscribers and TDs.

Selectively encrypted content is transcoded without decryption and re-encoding by a secure transcoder in particular device(s); secure transcoding may be performed at any place such as the head-end, interim node, end device, and other elements that participate in IPTV services. The transcoded data is then transmitted to the user device through the content delivery functional block.

Afterward, the selective decryption functional block in the terminal device decrypts the transcoded secure content by using the decryption key and security policy provided by service provider.

Table 9-1 – Functionalities of the security components of the secure transcoding mechanism

Components		Description
Content provider	Content sources	Originates content to be aggregated, processed, and subsequently delivered to end users by means of service applications such as linear TV, VoD, etc.
Service provider	Key management functional block	Correlates keys with content and manages their distribution to the terminal device in accordance with a security policy
	Security policy management functional block	Manages security policy including encryption type, encryption method, encryption layer, parameter set, etc.; the security policy is configured by the service provider
	Cryptography library repository	Provides a cryptographic library related to the protection of transcodable content
	Security policy database	Provides security policy including encryption type, encryption method, encryption layer, parameter set, etc.
	Selective encryption functional block	Creates secure transcodable content using an in-compression and/or a post-compression selective encryption approach
	Video encoder	Combines any hardware or software enabling video compression that is a combination of spatial compression and temporal motion compression
	Content delivery functional block	Combines any hardware or software to provide video-related services such as video streaming, VoD, etc., to clients
	Service authentication functional block	Provides the functionality to authenticate the server, intermediate node to perform transcoding, and TDs NOTE – This function is independent of the service and content protections from the point of view of IPTV transcodable security
Intermediate node to perform transcoding	Secure transcoder	Transcodes the encrypted content by extracting some parts of bitstreams or truncating specific parts from the encrypted content without decoding, decryption, and re-encoding
	Content delivery client functional block	Combines any hardware or software to receive the IPTV content
	Content delivery functional block	Combines any hardware or software to provide video-related services such as video streaming, VoD, etc. to clients
	Service authentication functional block	Provides the functionality to authenticate the server, intermediate node to perform transcoding, and TDs NOTE – This function is independent of the service and content protections from the point of view of IPTV transcodable security

Table 9-1 – Functionalities of the security components of the secure transcoding mechanism

Components		Description
Terminal device	Selective decryption functional block	Decrypts the transcoded secure content; if the content is encrypted using an in-compression-based approach, decryption is performed in the process of decoding; if the content is encrypted using a post-compression-based approach, decryption is performed before decoding
	Key management client functional block	Obtains or receives keys using this information to control content decryption
	Security policy management functional block	Manages security policy, including encryption type, encryption method, encryption layer, parameter set, etc.; the security policy is received from the service provider
	Cryptography library repository	Provides cryptographic library related to the protection of transcodable content
	Security policy database	Provision of security policy including encryption type, encryption method, encryption layer, parameter set, etc.
	Video decoder	Reverse-processes an encoder via any combination of hardware or software so that the original video can be reproduced
	Service authentication functional block	Provides the functionality to authenticate the server, intermediate node to perform transcoding, and TDs NOTE – This function is independent of the service and content protections from the point of view of IPTV transcodable security
	Content delivery client functional block	Receives the IPTV content and routes video signals to the video decoder via any combination of hardware or software

9.2.1 Creation process of secure transcodable content

In the secure transcoding mechanism, once the original content is encoded with a specific protection mechanism (i.e., selective encryption), the content can be reconstructed with respect to spatial scalability, temporal scalability, and quality scalability without decryption, decoding, and re-encoding. Accordingly, prior to creating the secure transcodable content, it is required to determine not only which parts are to be encrypted but also when to encrypt.

The key element in creating secure transcodable content is that any information needed in transcoding with respect to three different scalabilities must not be encrypted when executing selective encryption. Selective encryption for the creation of secure transcodable content can be classified into two types:

- *In-compression selective encryption:* Selective encryption is performed in the process of encoding. The parameters to be encrypted could be Intra-Prediction Mode (IPM), Texture sign, Motion Vector Difference (MVD), etc. The primary advantage of this method is format compliance so that a standard decoder is able to decode the encrypted bitstream without decrypting and subsequently reproducing distorted video. Moreover, it is compression-friendly since it has very little or no impact on data compression efficiency.

This method does not need to concern itself with information referenced by a transcoder to extract a subset of scalability; that is because in this approach, selective encryption involves performing encryption before writing scalable information to the bitstream. The weakness of this method is that modifications in both encoder and decoder are required. Figure 9-2 shows the structure of in-compression selective encryption.

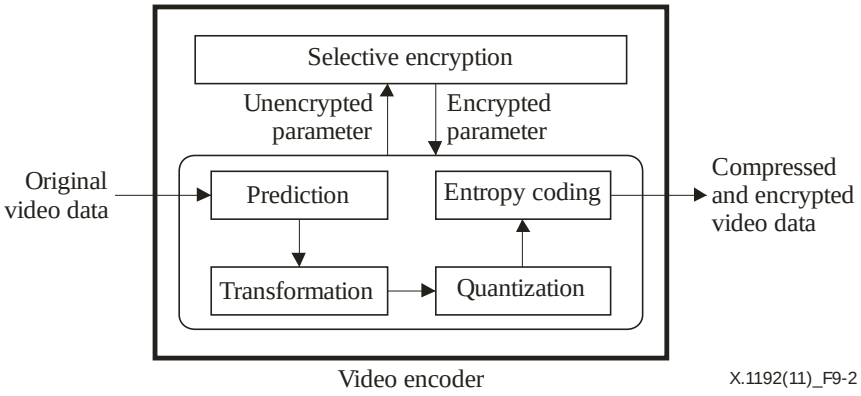


Figure 9-2 – In-compression selective encryption approach

- *Post-compression selective encryption:* Selective encryption starts after encoding. In the case of SVC, the encryption procedures are carried out at the network abstract layer (NAL) level. NAL is the smallest unit that can define spatial, temporal, and quality scalabilities. The NAL unit to be encrypted could be any or all of them such as instantaneous decoding refresh picture (IDR), sequence parameter set (SPS), picture parameter set (PPS), etc. Note, however, that the parameters or data applied to selective encryption might not be limited to these parts described above. The multiple parts can be simultaneously used for encryption according to the application requirements and user's service demands.

  Figure 9-3 shows the post-compression selective encryption approach. The primary advantage of this method is to separate encryption functions from encoding; thus, it does not need any modification to the encoder and decoder. This approach is generally compression-friendly, but non-format-compliant.

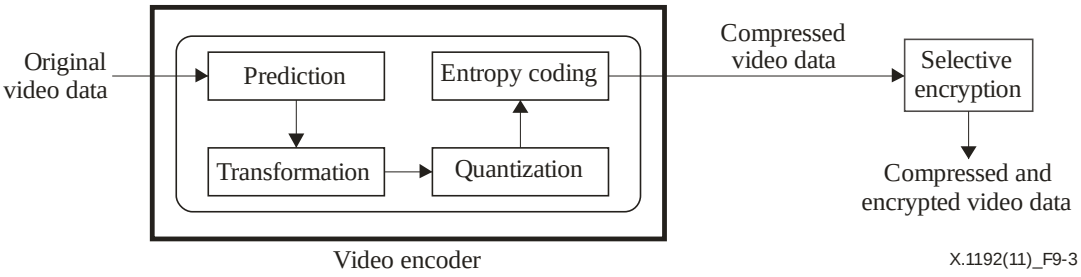


Figure 9-3 – Post-compression selective encryption approach

In this approach, the information referenced by a transcoder to extract a subset of quality (or spatial or temporal) layers should not be encrypted. Such information might be scalable layer information in the NAL header of SVC, etc. Figure 9-4 shows the NAL unit structure in SVC. The scalability information is written in the NAL unit header extension. Dependency_id, Temporal_id, and Quality_id in Figure 9-4 indicate spatial, temporal, and quality layer information, respectively.

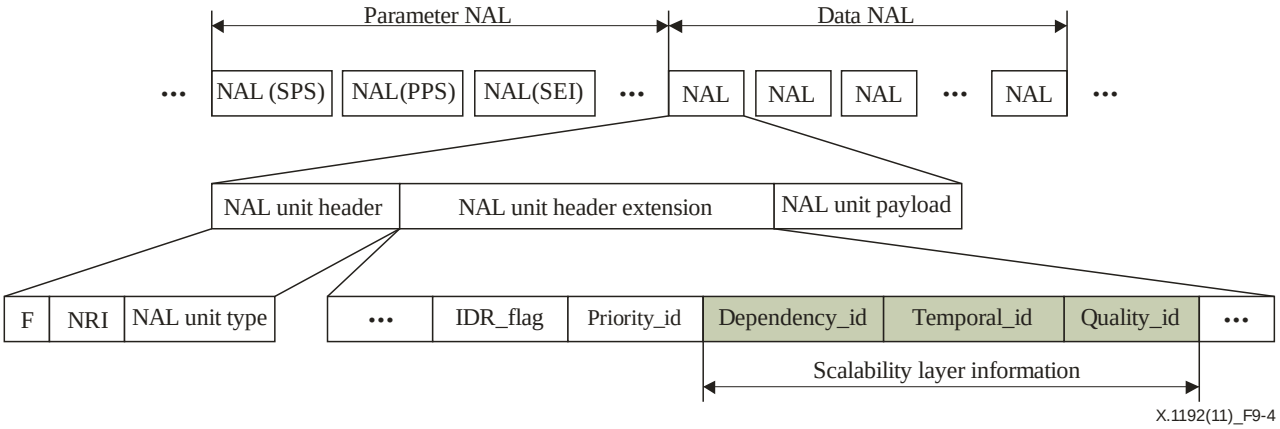


Figure 9-4 – NAL unit structure

- *Hybrid-type selective encryption*: This is a 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. This method could be applied to the reuse/retransmission of protected media in a secure manner. In-compression selective encryption in general is suitable for real-time media transmission because it is compression-friendly and format-compliant, but it may not be suitable for non-real time reuse (e.g., record the received real-time media at the local storage such as set-top-box, personal video recorder (PVR), etc., and copy it to another user device and play it) because it is not secure enough from the replacement attack compared to post-compression encryption.

  In case of post-compression selective encryption, it is suitable for non-real-time reuse and retransmission because it is safe from the replacement attack compared to in-compression encryption. Thus, additional encryption (post-compression encryption) can be performed to the locally stored media encrypted by the in-compression method for securely reusing the recorded media.

  Figure 9-5 shows the hybrid-type selective encryption approach.

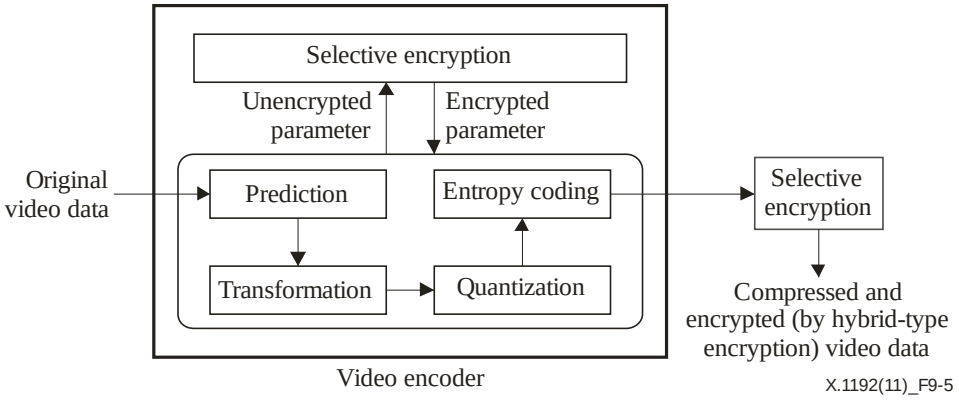


Figure 9-5 – Hybrid-type selective encryption approach

9.2.2 Secure transcoding process with protection

Basically, the original content is generated by encoding raw data according to a specific video compression algorithm (i.e., codec). For that reason, to provide consistent and transparent content protection over (re)distribution with the required level of security, the original content must be adaptively encrypted by reflecting the encoding rules and data structure of a video compression algorithm. Moreover, for the security requirements described in clause 8 and specific application conditions, the secure transcoding process is required to support an extraction function as follows:

- *Extraction (security-aware content transformation)* can be defined as a technique of extracting some parts of bitstreams or truncating specific parts from the encrypted content without decoding, decryption, and re-encoding, so that security can be maintained with no compromise in this function.

Figure 9-6 shows the illustration of secure transcoding with protection in the case of SVC. In this mechanism, the secure transcoder only performs the extraction of bitstreams from encrypted content; it has no rights to access original contents.

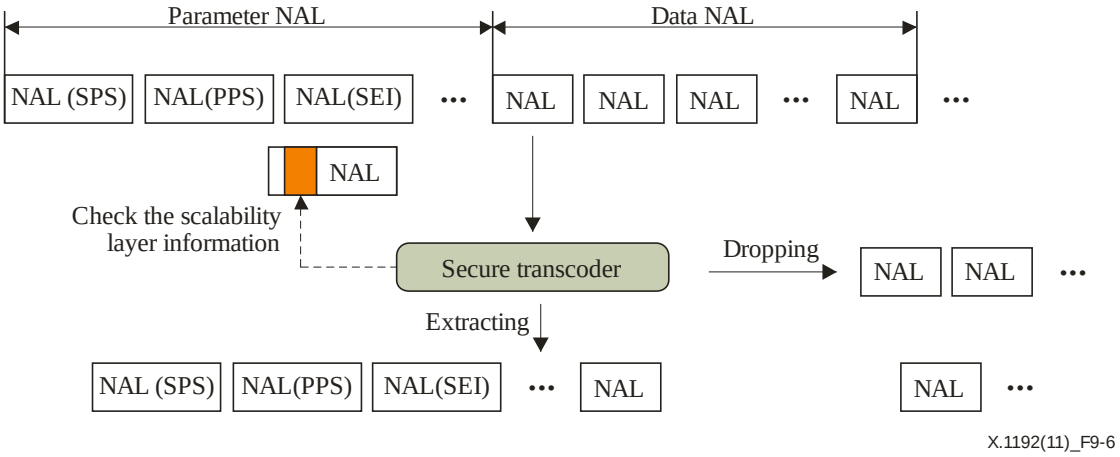


Figure 9-6 – Illustration of secure transcoding with protection

9.2.3 Decryption process

The selective decryption functional block in the user device decrypts the transcoded secure content by using the security policy information and key received from the service provider. In the case of in-compression encrypted data, decryption is performed in the process of decoding.

Figure 9-7 shows the in-compression selective decryption approach. The parameters to be decrypted could be IPM, Texture sign, MVD, etc. The information of the encryption method and encryption parameter of the received content is included in the security policy data. This approach is format-compliant, such that a decoder with no access rights to the content is able to decode the encrypted bitstream without decryption and subsequently reproduce the distorted video.

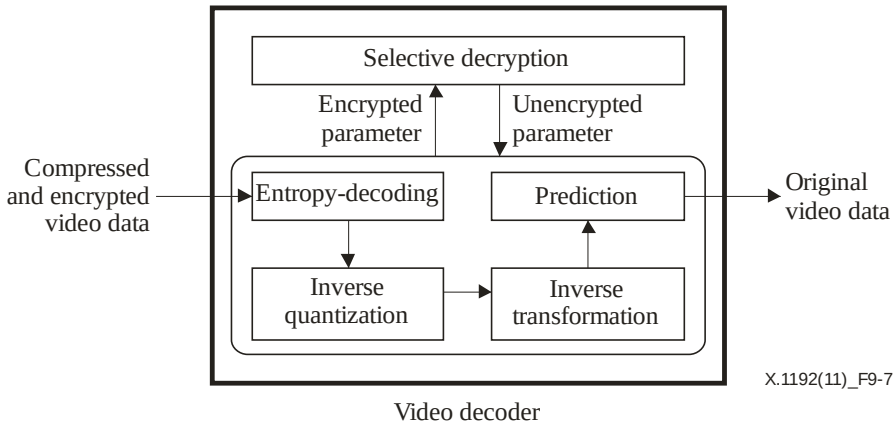


Figure 9-7 – In-compression selective decryption approach

In case of post-compression encrypted data, decryption is performed before decoding. In the case of SVC, the decryption process of the post-compression encrypted data is carried out at the NAL level. The NAL unit to be decrypted could be any or all of them such as IDR, SPS, PPS, etc. The information of the encryption method and encryption data of the received content are included in the security policy data.

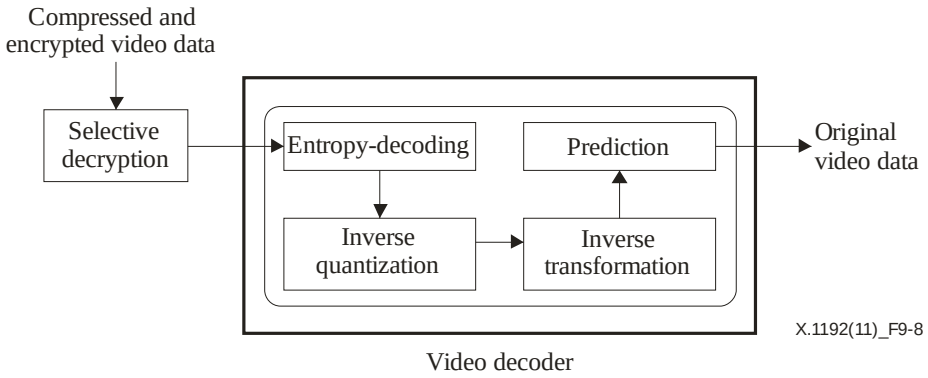


Figure 9-8 – Post-compression selective decryption approach

9.2.4 Key management process

Key management is defined as the generation, exchange, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy [ITU-T X.800].

In the secure transcodable mechanism, it is possible to invoke, create, distribute, and maintain the keys with respect to an individual layer for guaranteeing the layered access control to the protected content.

With such consideration, general mechanisms in [ITU-T H.234] and [ITU-T H.235.6] can be used to provide an effective, efficient key management mechanism.

9.2.5 Security policy

This clause describes the need for a security policy, a suitably defined configuration example of security policy data, and its agreement process in the selective encryption approach. The concepts are then applied to the secure transcodable systems.

9.2.5.1 Need for a security policy

The secure transcodable mechanism is concerned primarily with the encoding rule, encryption method, parts to be encrypted, cryptographic algorithm, key management protocol, and content distribution.

The need for a security policy regarding the secure transcodable mechanism is classified into two classes:

- There is a need to consider a set of factors that influence the performance of secure transcodable systems before creating secure transcodable content.
- Operational consistency is also important between the service provider and terminal device, since two entities must abide by a single rule for maintaining the persistent protection of the content throughout all processes of the secure transcodable mechanism.

Accordingly, it is required that the system provider offer a well-defined configuration of the factors in the form of a security policy to support stable quality and consistency of services.

9.2.5.2 Security policy database

The security policy database is the conceptual repository for managing all security-relevant information especially needed by the secure transcodable systems. This concept does not suggest any form for the storage of information or its implementation. Note, however, that each service provider must contain the necessary security-relevant information to enable it to enforce an appropriate security policy in any operation of selective encryption and decryption. Such a system requires the distribution of security policy data to the entities (i.e., terminal devices) subject to this security policy administered by the service provider.

Table 9-2 shows a possible configuration of the security policy database.

- The "encryption method" field defines three different kinds of selective encryption approaches – *ISE, PSE,* and *HSE* – as introduced in clause 9.2.1.
- The "encryption type" field defines the parts to be encrypted by the pre-defined encryption method.
- In the "encryption layer" field, the layer indices representing a *start* layer and an *end* layer – which are allowed to encrypt their parts – are specified in (*EL_start, EL_end*) form.
- The "cryptographic parameter set" consists of three sub-fields: encryption algorithm, key size, and key lifetime. Each of them can be specified by simple characters or numbers.

Note, however, that the configuration and structure of security-relevant information in the security policy database may vary according to the service provider's administrative rules, application characteristics, or user's service demands.

Table 9-2 – Illustration of security policy data

Field	Items
Encryption method	– *ISE*: In-compression selective encryption – *PSE*: Post-compression selective encryption – *HSE:* Hybrid-type selective encryption
Encryption type	In-compression selective encryption – *I_type1*: IPM encryption – *I_type2*: Texture sign encryption – *I_type3*: MVD encryption – *I_type4*: Texture sign + MVD encryption Post-compression selective encryption – *P_type1*: SPS encryption – *P_type2*: SPS+PPS encryption – *P_type3*: SPS+PPS+Payload encryption Hybrid-type selective encryption – *Any of the combination types above is applicable.*

Table 9-2 – Illustration of security policy data

Field		Items
Encryption layer		(*EL_start, EL_end*)
Cryptographic parameter set	Encryption algorithm	*3DES, SEED, CSA, CSA3, AES, etc.*
	Key size	*64, 128, 168, 192, 256 bits, etc.*
	Key lifetime	Time in seconds

In this context, Figure 9-9 shows the security policy data transmitted from the head-end device to the end device. In this data, *id00001* represents content identity. In-compression selective encryption is used as an encryption method; only texture sign bits (*I_type2*) of base layer {*0, 0*} are selected as the parts to be concealed. An encryption algorithm is denoted by *AES* (*192bits*), and the keys can be valid for *10,000* seconds.

{id00001, ISE, I_type2, {0, 0}, CP_set{AES, 192, 10000}…}

Figure 9-9 – Security policy data transmitted to the end device

9.2.5.3 Security policy process

The process of security policy agreement consists of two parts: security policy generation and transmission. To assign newly-defined security policy data to the selective encryption process, the selective encryption functional block requires the creation or retrieval of security-relevant information in the form of security policy data from the security policy management functional block or security policy database. Furthermore, this security policy data generated at the service provider may be transmitted to the terminal device to provide the selective decryption functional block with a guide to the selective decryption process.

Figure 9-10 shows two entities including functional blocks related to the security policy, and describes the order of executing the security policy agreement process.

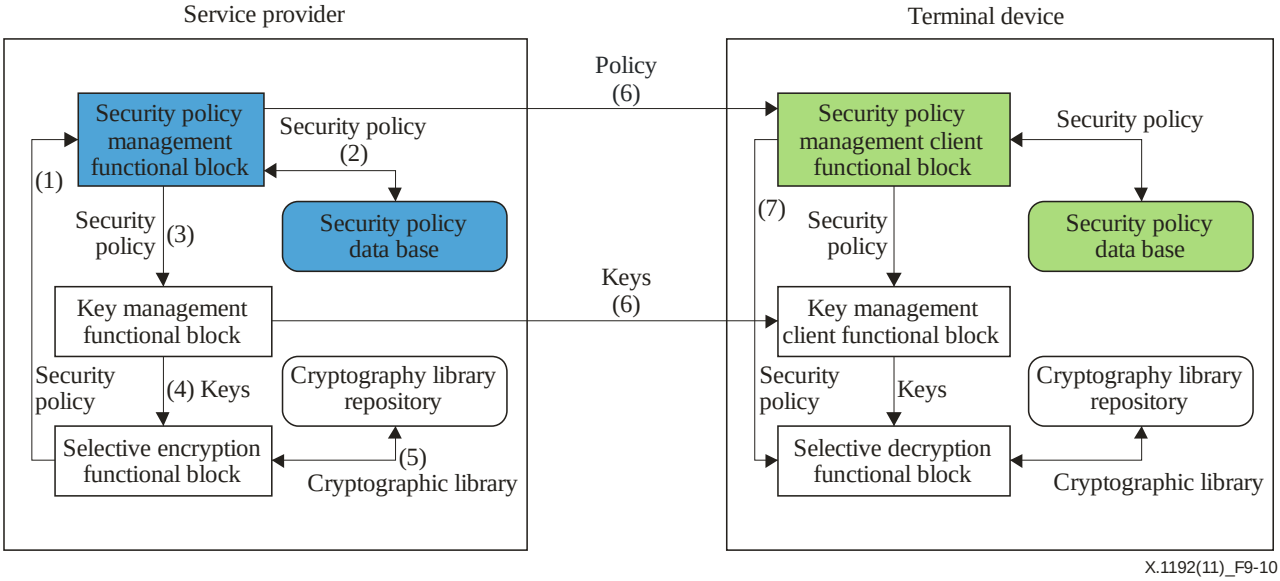


Figure 9-10 – Security policy agreement in the secure transcodable mechanism

The major operations in the security policy agreement are as follows:

1) The selective encryption functional block requests the creation of new security policy data or retrieval of pre-defined security policy data prior to creating secure transcodable content.
2) The security policy management functional block then generates or retrieves a security policy data suitable for a specific content according to a request type submitted by the selective encryption functional block.
3) After interpreting the given security policy data, the key management functional block produces a set of encryption keys with particular bits and lifetime.
4) The selective encryption functional block receives the security policy data and keys.
5) According to the security policy data, this functional block encrypts the content in cooperation with the cryptography library repository.
6) Next, the security policy data and decryption keys are transmitted to the terminal device through a communication channel. The information can be stored and managed in the security policy database and key management client functional block of the terminal device, respectively, for a particular purpose.
7) The selective decryption functional block will use the security policy data to decrypt the received content according to the security policy data provided by the service provider entity.

Appendix I

Reference points for secure transcoding in IPTV

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

I.1 Transcoding reference points

In the context of IPTV architecture, transcoding will appear as a "functional block". In the IPTV architecture, transcoding belongs to the content delivery and storage function. In Figure I.1, several places where transcoding may occur are indicated in rectangular boxes (▭). Note that Figure I.1 does not provide an exhaustive list of all possible reference points; but serves as an illustration of how transcoding may be integrated in the deployment of the IPTV services. Therefore, the transcoding functional block of the reference points indicated in Figure I.1 maps the various functional entities required to provide the IPTV services.

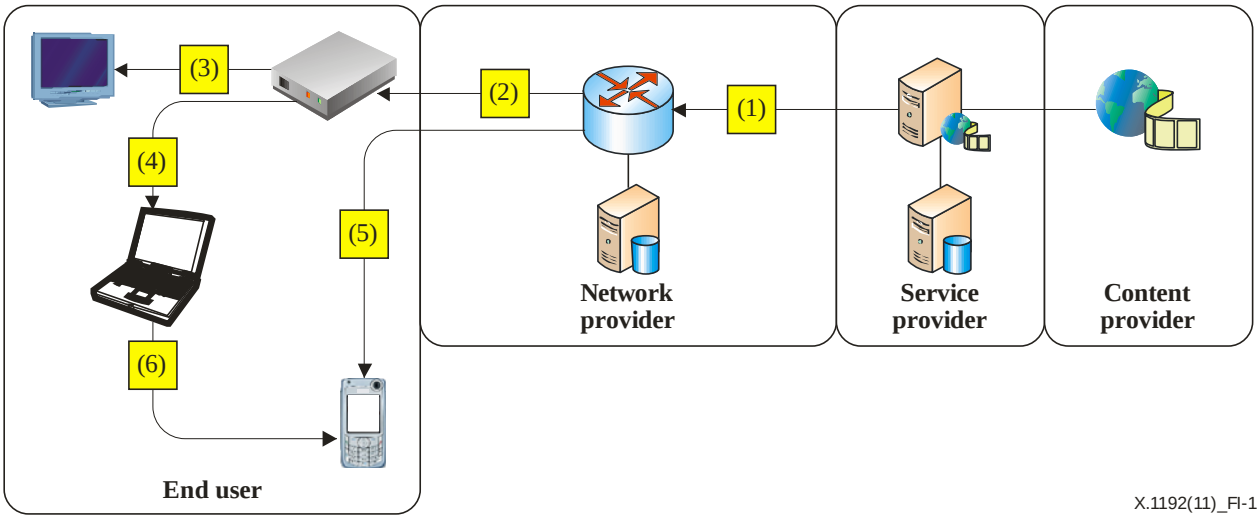


Figure I.1 – Sample transcoding reference points in IPTV domains

Table I.1 – Description of the transcoding reference points

Reference point	Description
(1)	Reference point between the service provider and an interim network entity (e.g., video hub office [ITU-T Y.1910]). The service provider may perform transcoding to reduce the time and bandwidth required to transmit content over a network with limited bandwidth
(2)	Reference point between an interim network entity (e.g., VHO) and the end user's terminal device (e.g., the set-top box (STB)). VHO may perform transcoding to reduce the time and bandwidth required to transmit content over a network with limited bandwidth
(3)	Reference point between the end user's terminal device (e.g., set-top box) and the TV set. STB may perform transcoding before it sends the video signal to the TV set
(4)	Reference point between an end-user's terminal device and the laptop (or PC). STB may perform transcoding before it sends the video signal to the laptop

Table I.1 – Description of the transcoding reference points

Reference point	Description
(5)	Reference point between an interim network entity (e.g., VHO [ITU-T Y.1910]) and the end user's mobile terminal device (e.g., PDA). VHO may perform transcoding to meet the capacity of TD and reduce the time and bandwidth required to transmit content over a network with limited bandwidth
(6)	Reference point between the end user's terminal device (e.g., set-top box) and the end user's mobile terminal device (e.g., PDA). The laptop may perform transcoding to meet the capacity of TD

I.2 Types of transcoders

Transcoding generally takes place at an interim network node located between the head-end and the user terminal device. Therefore, the role of the interim network node can be categorized into two types.

Table I.2 – Transcoder types

Type	Description
Visible transcoder	An interim network node that is authorized to view the content and transcode the content at the same time
Invisible transcoder	An interim network node that is NOT authorized to view the content but is authorized to transcode the content

I.3 Security requirements for the transcoding reference points

Since the transcoder acts differently according to its type, the security requirements for the transcoding reference points are described separately in Table I.3. However, as the transcoding reference points in Table I.1 do not represent an exhaustive list of all possible reference points, the security requirements in Table I.3 are not the complete listing. In Table I.3, when the use case of the transcoder type in the reference point is rarely used, it is marked as "N/A".

Table I.3 – Security requirements

Reference point	Transcoder type	Security requirement
(1)	Visible	The original content should be available only to the service provider. The transcoded content should be available only to the interim network entity (e.g., the video hub office [ITU-T Y.1910])
	Invisible	N/A
(2)	Visible	The original content should be available only to the interim network entity (e.g., VHO). The transcoded content should be available only to the end user's terminal device (e.g., set-top box)
	Invisible	N/A

Table I.3 – Security requirements

Reference point	Transcoder type	Security requirement
(3)	Visible	The original content should be available only to the end user's terminal device (e.g., set-top box). The transcoded content should be available only to the TV set
	Invisible	The original content should be available only to the interim network entity (e.g., VHO). The transcoded content should be available only to the TV set
(4)	Visible	The original content should be available only to the end user's terminal device (e.g., set-top box). The transcoded content should be available only to the laptop (or PC)
	Invisible	The original content should be available only to the interim network entity (e.g., VHO). The transcoded content should be available only to the laptop (or PC)
(5)	Visible	The original content should be available only to the interim network entity (e.g., VHO). The transcoded content should be available only to the end user's mobile terminal device (e.g., PDA).
	Invisible	N/A
(6)	Visible	The original content should be available only to the laptop (or PC). The transcoded content should be available only to the end user's mobile terminal device (e.g., PDA)
	Invisible	The original content should be available only to the interim network entity (e.g., VHO). The transcoded content should be available only to the end user's mobile terminal device (e.g., PDA)

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
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012