International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1196

(10/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment

Recommendation ITU-T X.1196

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.1196

Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment

Summary

Recommendation ITU-T X.1196 provides a framework for the downloadable service and content protection (SCP) scheme in the mobile Internet Protocol television (IPTV) environment. It also describes functional architecture and requirements for the downloadable service and content protection (SCP) scheme for roaming in the mobile IPTV environment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1196	2012-10-14	17

Keywords

Downloadable SCP, SCP interoperability, security requirement.

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/.

Table of Contents

Recommendation ITU-T X.1196

Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment

1 Scope

Recommendation ITU-T X.1196 provides a framework for the downloadable service and content protection (SCP) scheme in the mobile Internet Protocol television (IPTV) environment. It also describes the functional architecture and requirements for the downloadable SCP scheme for roaming in the mobile IPTV environment.

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 X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.

[ITU-T X.1193] Recommendation ITU-T X.1193 (2011), *Key management framework for secure Internet protocol television (IPTV) services*.

[ITU-T X.1195] Recommendation ITU-T X.1195 (2011), *Service and content protection interoperability scheme*.

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

[ITU-T Y.1911] Recommendation ITU-T Y.1911 (2010), *IPTV services and nomadism: Scenarios and functional architecture for unicast delivery*.

[IETF RFC 2315] IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 certificate [b-ITU-T X.1252]: A set of security-relevant data issued by a security authority or a trusted third party that, together with security information, is used to provide the integrity and data origin authentication services for the data.

3.1.2 content protection [ITU-T X.1191]: Ensuring that an end user can only use the content that he/she has 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.

3.1.3 key hierarchy [b-NIST SP 800-120]: A tree structure that represents the relationship of different keys. In a key hierarchy, a node represents a key used to derive the keys represented by the descendent nodes. A key can only have one precedent, but may have multiple descendent nodes.

3.1.4 roaming [b-ITU-T Q.1706]: The ability for a user to function in a serving network different from the home network.

NOTE – This is the ability of the users to access services according to their user profile while moving outside of their subscribed home network, i.e., by using an access point of a visited network. This requires the ability of the user to get access to the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators.

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

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

3.1.7 service protection [ITU-T X.1191]: Ensuring that an end user can only acquire a service and the content hosted therein by extension as to 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 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 certificate hierarchy: A tree structure of certificates that represent the relationships of different certificates to allow individuals to verify the validity of a certificate's issuer. In a certificate hierarchy, a node represents a certificate that is issued and signed by the corresponding private key in the certificate that resides at a higher node in the certificate hierarchy. A certificate can only have one precedent, but may have multiple descendent nodes. The validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it.

3.2.2 certificate chain: An ordered list of certificates, containing an end-user subscriber's certificate, intermediate certificates, which represents the intermediate certification authority (CA), and a root certificate, which allows the receiver of the certificate to verify that the certificate of the sender and all intermediates certificates are trustworthy.

3.2.3 coordinator model: A model in which the brokering service provider acts as a negotiator or a connector between the service providers and the end users for the service.

3.2.4 delegator model: A model in which the brokering service provider acts as an intermediary between the service provider and the end user during the entire process of the service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSP Brokering Service Provider

CA Certification Authority

CP Content Protection

CVC Code Verification Certificate

CVS Code Verification Signature

DoS Denial-of-Service

EAP Extensible Authentication Protocol

EK Encryption Key

HN Home Network

IMS IP Multimedia Subsystem

IPTV Internet Protocol Television

NACF Network Access Control Function

NGN Next Generation Network

OAM Operations, Administration and Maintenance

OSP Original Service Provider

RACF Resource Access Control Function

SCF Service Control Function

SCP Service and Content Protection

SP Service Protection

SSL Secure Sockets Layer

TA Trusted Authority

TD Terminal Device

TLS Transport Layer Security

TLV Type/Length/Value

WM Watermark Metadata

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 this Recommendation.

6 Overview

The downloadable SCP system for the mobile environment gives great benefits to both IPTV service providers and IPTV users, in terms of enabling convenient and portable IPTV service. The IPTV service in the mobile environment is different from the existing one in that the former provides more mobility since it is based on a mobile IPTV terminal device (TD), e.g., smartphone. Therefore, in order to provide a downloadable SCP system in the mobile IPTV service, the mobility of a TD and a user shall be taken into account. The downloadable SCP for all IPTV services may be considered as an optional requirement, rather than mandatory.

It may be necessary to use downloadable SCP from an IPTV service provider to a user's TD in the following situations:

- when the new user's TD is attached to the service provider's network;
- when the new user's TD changes its IPTV service provider;
- when the user's TD is replaced; or
- when the user's TD is requested to change the SCP operation code by the service provider (e.g., SCP security update).

If the new user's TD is attached to the service provider's network, and the new TD requires upgrading of SCP codes, three downloadable features should be performed to meet the different environments: upgrading of firmware, service protection (SP) software code, and/or content protection (CP) software code.

If the new service provider uses the same SCP software as the previous service provider, and the removable hardware in the IPTV TD has already been installed with the common SCP software code, it may not be possible for downloadable features to be performed until the new service provider requests the IPTV TD to upgrade the firmware and the SCP software code.

If a user changes the service provider or IPTV service provider, the following steps may be required to access the IPTV service content:

1) upgrade of firmware, if the new service provider requires ownership and use of a dedicated firmware;
2) upgrade of SP software, to adapt the IPTV TD to the SP system used by the IPTV service provider; and
3) upgrade of CP software, to adapt the IPTV TD to the CP system used by the IPTV service provider.

The hardware or software residing in the IPTV TD interacts with downloaded security software on the network side, to permit access to the content being received.

The objectives of a downloadable SCP include the following:

- The IPTV service provider should securely download the SCP software code into IPTV TD, as needed;
- The downloadable SCP should provide integrity and message origin authentication for the downloaded SCP software code, and can optionally perform confidentiality for the downloaded SCP software code; and
- The IPTV service provider should download the software code only after authenticating the legitimacy of IPTV TD.

7 Requirements for the downloadable SCP scheme

7.1 General requirements for the downloadable SCP scheme in [ITU-T X.1191]

Requirements for key management described in clause 6.3 of [ITU-T X.1191] are:

- The IPTV architecture is prohibited from precluding support for secure downloading for an SCP system. The downloaded SCP system can optionally depend on specific service protection requirements.
- If downloadable SCP is deployed, the IPTV architecture is required to perform integrity protection and data origin authentication for the downloaded SCP system.
- If the secure downloading of an application program to TD is supported, the IPTV architecture is required to perform integrity protection and data origin authentication for the downloaded applications.

- The IPTV architecture is recommended to support the secure downloading of application programs to TDs.

One requirement for secure downloading of the SCP operation code described in clause 6.5 of [ITU-T X.1191] is:

- If downloadable SCP is deployed, the IPTV architecture is required to support the secure download and installation of the SCP operating code to TDs.

7.2 Functional requirements for the downloadable SCP scheme

- IPTV TD is required to authenticate the downloaded SCP operating code.
- IPTV TD is required to verify that the downloaded SCP operating code has not been altered from the original form in which it was provided by the trusted source.
- IPTV TD is required to verify that the downloaded SCP operating code is appropriate or legitimate. If the downloaded SCP operating code is appropriate, the IPTV TD is required to write the new SCP operating code to a non-volatile storage. Once the file transfer is completed successfully, the IPTV TD is required to restart itself with the new SCP operating code.
- IPTV TD is required to log download failures of the SCP operating code, and can report failures asynchronously to the network manager of the IPTV service provider.
- Where the SCP operating code has been upgraded to meet a new version; the SCP operating code is required to work with the previous version in order to allow a gradual transition of units on to the network.
- The process of the downloadable SCP scheme can optionally provide a capability for IPTV service operators to dictate their own downloadable SCP policies.

The IPTV service provider should generate a code verification certificate (CVC) over the SCP operating code and other relevant attributes for PKCS#7-based digital signature [IETF RFC 2315], [b-ITU-T J.192]:

- to the downloaded SCP operating code. The private key used to generate the digital signature should be bound to a public key certificate that chains up to CVC root CA. The digital signature has to authenticate the message and integrity of the downloaded SCP operating code.
- IPTV TD is required to be able to process a PKCS#7-based digital signature for verifying the authenticity of the downloaded SCP code, and an ITU-T X.509 certificate for identifying the IPTV TD, respectively.
- IPTV TD is required to be able to update a code verification certificate (CVC) Root CA Certificate stored in the IPTV device after the certificate has been validated, if contained in a code file as a type/length/value (TLV).
- IPTV TD is required to be able to replace the manufacturer CA certificate(s) stored in the IPTV device after the certificate has been validated, if contained in a Code File as a TLV.
- IPTV TD is required to be able to update the CVC CA certificate stored in the IPTV TD after the certificate has been validated, if contained in a Code File as a TLV.
- IPTV TD is required to be able to update the service provider root CA certificate stored in the device after the certificate has been validated, if contained in a Code File as a TLV.

8 Security framework for a downloadable SCP system in a roaming environment

This Recommendation develops a downloadable SCP system based on the framework described in [ITU-T Y.1911].

8.1 Overview

In Figures 8-1, 8-2 and 8-3, the next generation network (NGN) operator A acts as a home network and NGN operator B as a visited network.

Figure 8-1 shows a non-roaming example. In this case, the end-user functions connect to the home network and access authentication is performed with the network access control function (NACF) of the home network. After access authentication is completed, the end-user functions negotiate with the service control function (SCF) of the home network in order to set up an IPTV session. The SCF then performs the resource allocation to the transport functions through the resource access control function (RACF) of the home network, and the application functions will then send media data to the end-user functions. In the home network, it is assumed that end-user functions can communicate using the standardized mechanism, the so-called IP multimedia subsystem (IMS)-based or non-IMS-based IPTV session control, defined in IPTV functional architecture [ITU-T Y.1910].

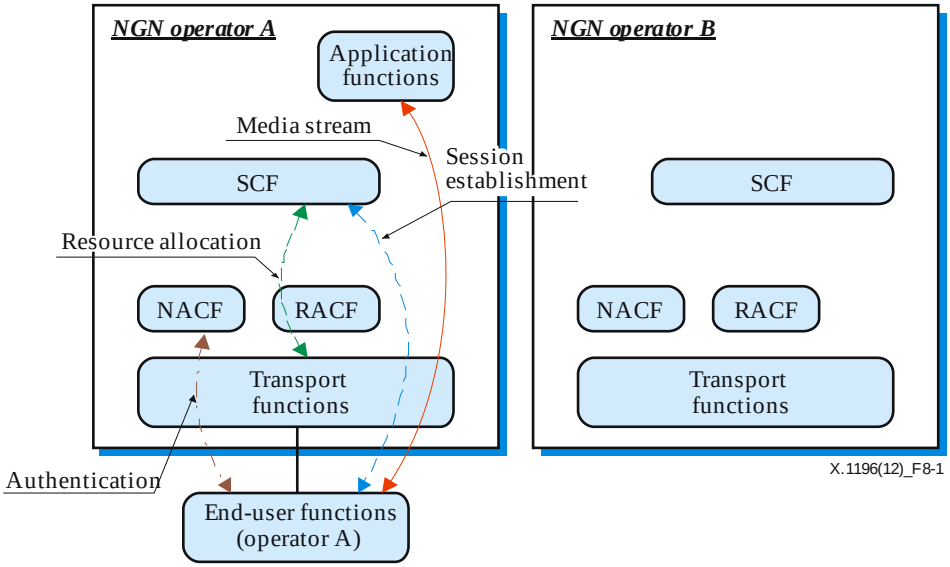


Figure 8-1 – Non-roaming case

Figure 8-2 shows a roaming case where the end-user functions can communicate with the SCF of the visited network. In this case, IMS-based or non-IMS-based session control is used to establish an IPTV session, and it is required to have functional compatibility between the end-user functions provided by the home network and the SCF of the visited network. Since the end-user functions are authenticated by the NACF of the home network through that of the visited network, this NACF-NACF interaction needs to be specified. The session establishment is then performed using an interface between SCF of the home network and that of the visited network. This SCF-SCF interface also needs to be specified. The resource is allocated from the SCF to the transport functions in each network.

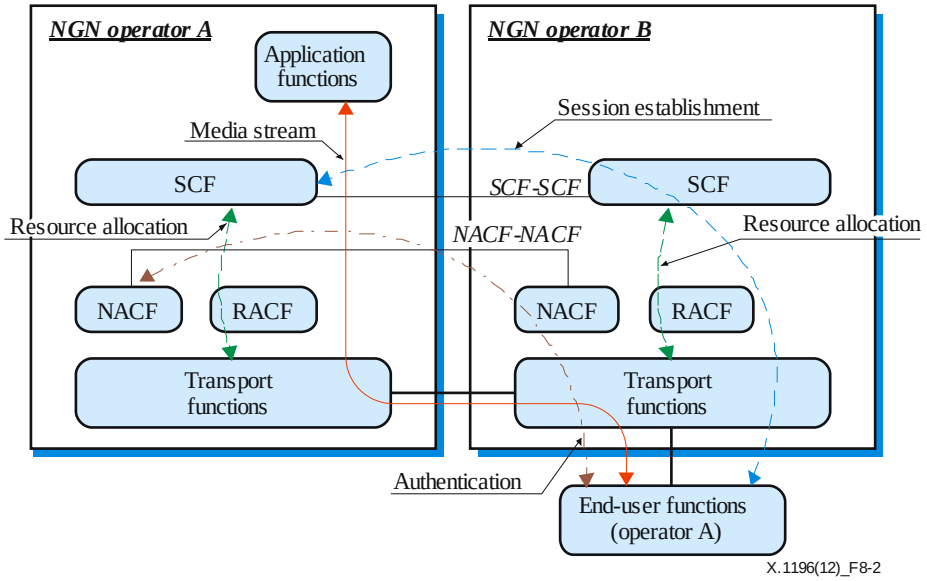


Figure 8-2 – Case of roaming using the service control function (SCF) of the visited network

Figure 8-3 shows a case of roaming when the end-user functions are not capable of communicating with the SCF of the visited network due to lack of compatibility. For example, if the end-user functions support only an IMS-based IPTV session control function, and the SCF of the visited network supports only a non-IMS-based one, there may be incompatibility between them. In this case, the mechanism to exchange the user's policy, including the operator's policy between the NACF of the home network and that of the visited network, needs to be specified. Additionally, the routing mechanism of the session control messages from/to the end-user functions to/from the SCF of the home network needs to be specified. After the end-user functions establish an IPTV session, the SCF of the home network allocates the resource to the transport functions of the home network through the RACF. The RACF of the home network also communicates with that of the visited network, so that the RACF of the visited network can allocate the resource to the transport functions of the visited network. For the realization of this RACF interaction, the specification needs to be defined.

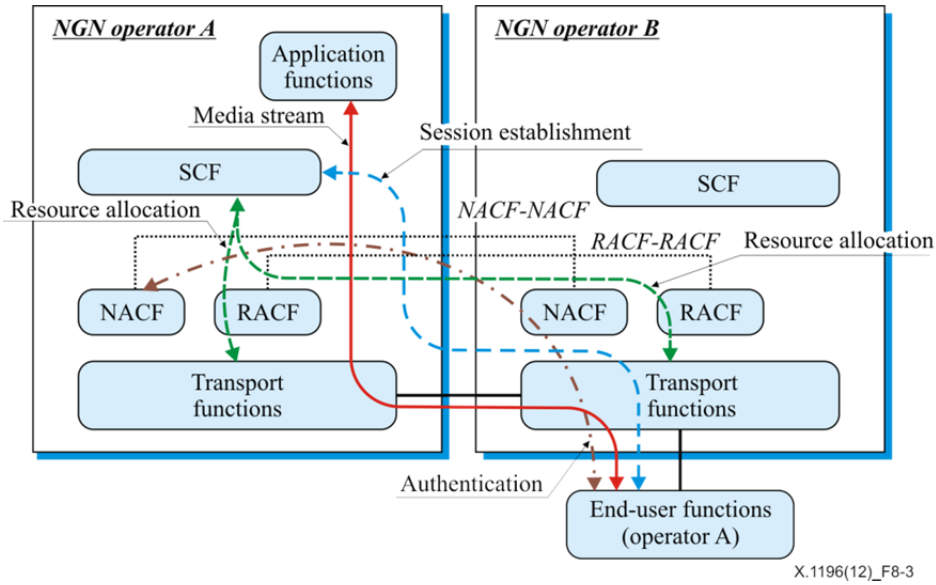


Figure 8-3 – Case of roaming without using service control function (SCF) of the visited network

8.2 Requirements for key management of a downloadable service and content protection (SCP) system architecture in the roaming environment

The requirements for the key management of the downloadable SCP in the roaming environment are as described in clause 7.3.3 of [ITU-T X.1193] as follows:

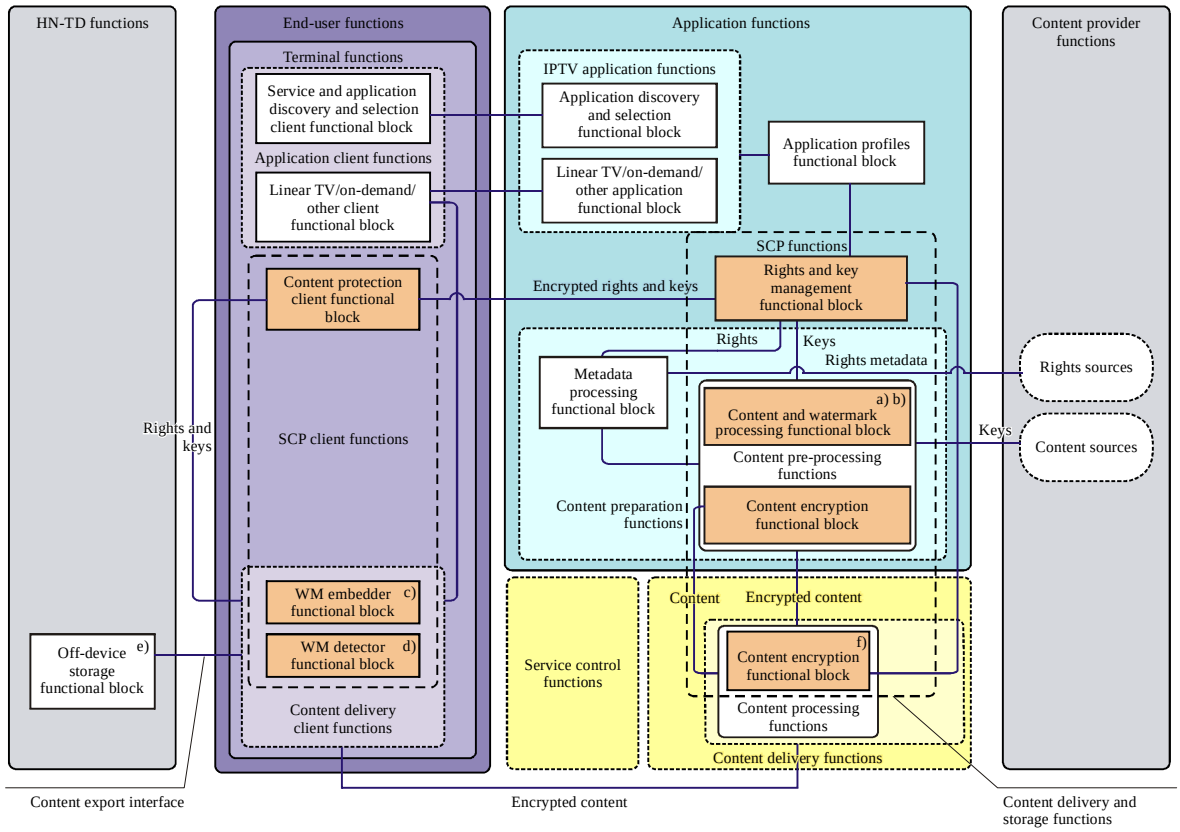
- The key management architecture of a downloadable SCP scheme is required to enable IPTV TD to verify the authenticity (proof of origin and data integrity) and validity (e.g., credentials) of the downloaded SCP client operating code. On successful verification, the IPTV TD is allowed to install and activate the downloaded SCP client operating code.
- The key management architecture of a downloadable SCP scheme is required to support mutual authentication between the SCP Client and the Rights & Key Management function.
- The key management architecture of a downloadable SCP scheme is required to provide a means of proving the validity of the IPTV TD as a trusted environment for SCP software upgrade.
- The key management architecture of a downloadable SCP scheme is required to support confidentiality and integrity for all security sensitive data (especially keys, passwords, and credentials) which are transferred over the network.
- The key management architecture of a downloadable SCP scheme is recommended to provide *key control.*
- The key management architecture of a downloadable SCP scheme is recommended to provide key confirmation.
- The key management architecture of a downloadable SCP scheme is recommended to support post-verification for all integrity-vulnerable information that has been exchanged before a transient integrity key is available.
- The key management architecture of a downloadable SCP scheme is recommended to generate the SCP key for downloading the SCP operating code.
- The key management architecture of a downloadable SCP scheme is recommended to generate an encryption key (EK) for decrypting a downloaded SCP operating code.
- The key management architecture of a downloadable SCP scheme is requested to generate a message integrity checking key for checking the integrity of a downloaded SCP operating code.
- The key management architecture of a secure SCP operating code download is recommended to generate the SCP key for the SCP function.
- The key management architecture of a secure SCP operating code download can optionally use the existing well-known, standardized extensible authentication protocol (EAP) methods for mutual authentication and key agreement.
- If a multicast-based downloadable SCP scheme is deployed, the IPTV TD belonging to the multicast group is recommended to share a group key for multicast-based downloadable SCP with a service provider.
- If a multicast-based downloadable SCP scheme is deployed, the IPTV TD is recommended to have a group key consisting of an encryption key and a message authenticity/integrity key for decrypting the encrypted SCP operating code and checking the validity of the authenticity and integrity of the SCP operating code, respectively.
- If a downloadable SCP scheme is deployed, the IPTV TD is required to have the capability to decrypt the encrypted SCP operating code.
- If a downloadable SCP scheme is deployed, the IPTV TD is required to authenticate the service provider to verify if it is entitled to perform an SCP client software upgrade.

- If a downloadable SCP scheme is deployed, and a handover of the IPTV TD to another service provider occurs, the IPTV TD is required to verify that only an entitled service provider may initiate an upgrade of the IPTV TD (the service provider shall be authenticated by the IPTV TD and authorized to do this).
- If a downloadable SCP scheme is deployed, the service protection or content protection functions shall only be implemented in a trusted execution environment (hardware or virtual machine, i.e., in software). Such an environment shall be tamper-proof, with a secure storage environment for security-sensitive information that these protection systems need to store, and which shall not be revealed outside the IPTV TD.
- If a downloadable SCP scheme is deployed, the service protection and/or content protection clients subsystem in the IPTV TD is required to offer the capability to authenticate the service protection, and/or content protection client software in operation in the IPTV TD, as the authentic software provided by the service protection provider or the content protection provider.
- It is required that the key management architecture of a downloadable SCP scheme for keys/certificates are hard-linked with the IPTV TD relying only on keys/certificates provided by a certificate authority (trusted third party).
- If a downloadable SCP scheme is deployed, upgrading the SCP scheme software on request, or on behalf of the owner of the IPTV TD, shall be possible independently of the currently active SCP scheme or services obtained.

8.3 Architecture and procedure of downloadable service and content protection (SCP) system in the roaming environment

The content protection architecture for IPTV is depicted in Figure 8-4 below. The primary function of the content protection architecture is to delineate the flow and processing of information pertaining to content-usage rights, and the information required to manage and facilitate such rights.

Ultimately, the rights of content-usage originate with the content provider(s); note, however, that such rights may be modified (e.g., narrowed, or perhaps even widened) by the service provider(s) according to their agreements with the content providers, and their operational and business policies. From an operational and typically legal perspective, an end user's access and use of content involve the service provider, and not the content provider. Figure 8-4 illustrates the basic architecture of the downloadable SCP system in the roaming environment.

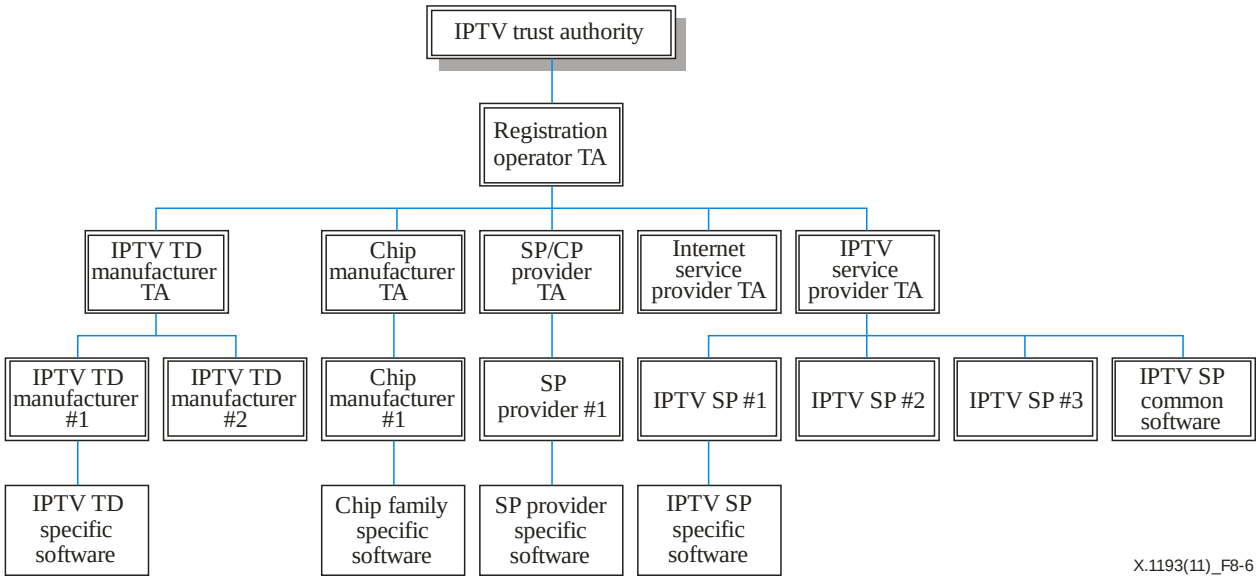


a) Optional watermark metadata generation to facilitate downstream watermark embedding.
b) Optional watermark embedder to individuate content to networks, servers, and unicast deliveries.
c) Optional watermark embedder to individuate multi-cast content instances.
d) Optional detector for copy protection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

Figure 8-4 – IPTV content protection architecture

The key management described in clause 8.3 of [ITU-T X.1193] can be used as the downloadable SCP scheme in the roaming environment.

Figure 8-5 illustrates the trust hierarchy model for the key management of the downloadable SCP scheme in the roaming environment.



TA	Trust authority
IPTV	Internet protocol television
SP provider	Service protection provider
CP provider	Content protection provider
TD	Terminal device
SP	Service provider

Figure 8-5 – Trust hierarchy

The upgrade of an SCP code starts between the end-user function on the IPTV TD side and the NACF on the operator side, after authentication is completed. Downloading of the SCP code is performed between the right and key management function on the home network side, and with the SCP client on the IPTV TD side.

It is assumed that the NACF function in the visited network forwards the messages from the NACF function in the home network, that is, all message exchanges are transparent to the NACF in the visited network.

The following steps will upgrade the SCP software:

- The right and key management function on the home network side initiates remote management connection with the IPTV TD in the visited network.
- During connection establishment, mutual authentication is performed between the key management function on the home network side, and with the IPTV TD in the visited network.
- The right and key management function in the home network side instructs the IPTV TD to download the CP software.
- The IPTV TD performs the requested download of the SCP software package, which contains the CP image and a signature from the SCP owner.
- Only when the SCP software can be verified as authentic, can the installation of the firmware into the IPTV TD be allowed.

9 Security framework for a downloadable service and content protection (SCP) system in the broker environment

9.1 Overview

For a web-based IPTV service brokering, there can be two types of brokering models depending on their role within the service. However, for the end user, it may appear the same regardless of the type of brokering service providers and the actual service procedures.

In the delegator model, the brokering service provider acts as an intermediary between the service provider and the end user throughout the entire service process. This model is often applied when the original service provider has its own middleware, or service platform, so that it does not support end users without the devices with proper intermediate transaction function. Therefore, the brokering service provider (BSP) needs to translate or convert all requests and responses, including related contents. Since the BSP brokers all transactions between the end user and the original service provider, end-users request or respond only to the brokering service providers as shown in Figure 9-1. In this model, the brokering service provider is in charge of the entire service transaction and can manage either the charging or the operations, administration and maintenance (OAM) for the entire service.

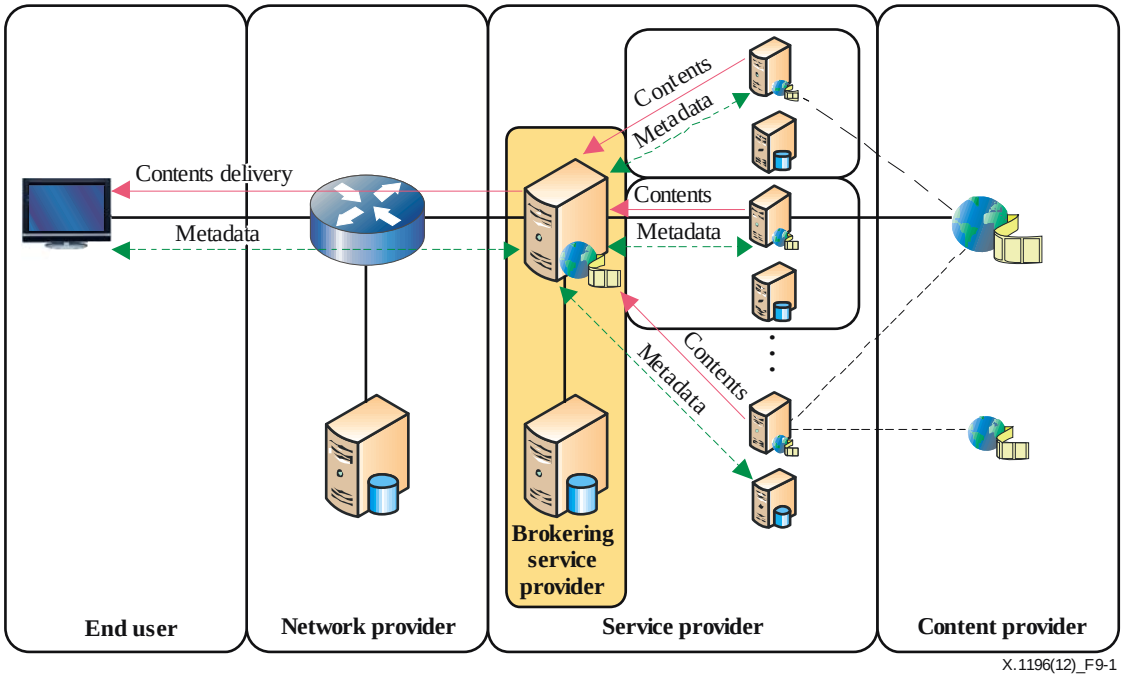


Figure 9-1 – Overview of the delegator model

In the coordinator model, the brokering service provider acts as a negotiator or a connector between the service providers and the end users for the service. It brokers only for their connection, which is until the end user's selection is made. Then the transactions for the requested service are done directly between the end user and the original service provider, as shown in Figure 9-2.

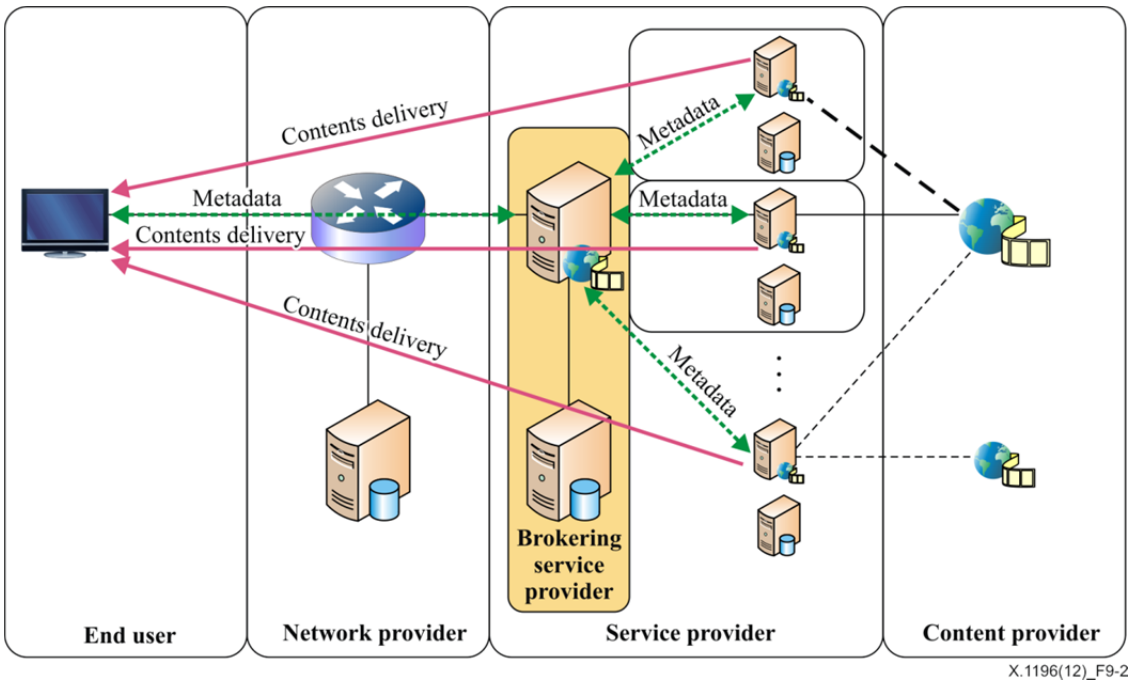


Figure 9-2 – Overview of the coordinator model

9.2 Security requirements for a web-based IPTV brokering service

This clause describes security requirements for a web-based IPTV brokering service.

Web-based IPTV brokering service should be configured to protect against various threats which are described in Appendix I of [ITU-T X.1191]. In general, security requirements specified in [ITU-T X.1191] can also be applied.

Figure 9-3 describes three components consisting of an end user, a brokering service provider, an original service provider and relevant SCP models for the web-based IPTV brokering service:

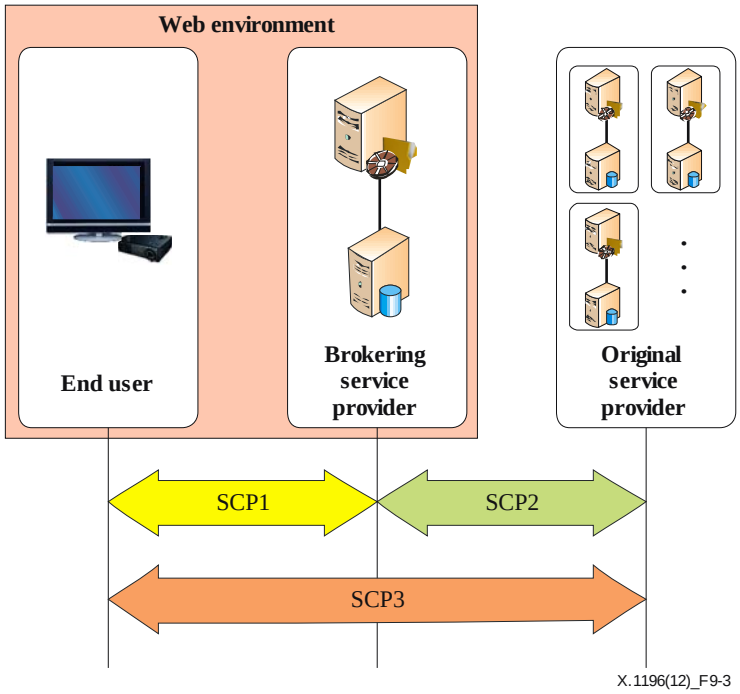


Figure 9-3 – SCP model for web-based IPTV brokering service

Security requirements of the web-based IPTV brokering service are grouped into four categories: general security requirements, security requirements between the end user and the brokering service provider, security requirements between a brokering service provider and an original service provider, and security requirements between an end user and an original service provider (only in the coordinator model).

9.2.1 General requirements

- The IPTV architecture of an IPTV brokering service is required to support content protection and service protection.
- The IPTV architecture of an IPTV brokering service is required to use publicly available and standardized cryptographic algorithms.
- The IPTV architecture of an IPTV brokering service is prohibited from precluding support for service and content protection interoperability wherein only authorized user(s), device(s), server(s) is(are) allowed to use authorized IPTV content, even after its (their) transfer to another SCP system.
- The IPTV architecture of an IPTV brokering service 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 SCP system.
- The IPTV architecture of an IPTV brokering service is prohibited from requiring the service and content protection mechanism of either side of the two interoperating SCP schemes.
- The IPTV architecture of an IPTV brokering service is prohibited from precluding support for service and content protection interoperability that is flexible and extensible, to support various business models.
- The IPTV architecture of an IPTV brokering service is required to have the ability to use standard key management systems.
- The IPTV architecture of the IPTV brokering service is recommended to support secure payment for the premium IPTV contents delivered from the brokering service provider.
- The IPTV architecture of the IPTV brokering service is required to provide protection of personally identifiable information about an end user.
- The IPTV architecture of an IPTV brokering service is required to support mechanisms for secure key management for a downloadable SCP scheme in the brokering service.
- The IPTV architecture of an IPTV brokering service is required to support the capability to protect against network-based attacks, and to mitigate a denial-of-service (DoS) attack.
- The IPTV architecture of an IPTV brokering service is required to support confidentiality and integrity of sensitive information (e.g., purchase list, payment information, and authentication information).

9.2.2 Security requirements between the end user and the brokering service provider

This clause specifies the security that deals individually, or collectively, with the service between end users and brokering service providers. In addition, it considers web-based environments.

- The IPTV architecture of an IPTV brokering service is required to support the protection of content distributed simultaneously to a large number of subscribers (scalability).
- The IPTV architecture of an IPTV brokering service provider is required to provide mechanisms for service and content protection to fit a web browser, and/or proper Internet applications of end users.
- The IPTV architecture of an IPTV brokering service is prohibited from precluding support for service and content protection interoperability, in order to support mobility of users.

- The IPTV architecture of an IPTV brokering service is prohibited from precluding support to update SCP, or the renewal of SCP, in the TD from a brokering service provider.
- The IPTV architecture of an IPTV brokering service is required to support end-user authorization and authentication.
- The IPTV architecture of an IPTV brokering service is required to provide confidentiality and integrity for contents delivered from a brokering service provider to an end user.
- The IPTV architecture of an IPTV brokering service is required to support a mechanism for providing integrity protection and data origin authentication for sensitive metadata.
- The IPTV architecture of an IPTV brokering service is recommended to support confidentiality, integrity, and data origin authentication, through a transport layer protection protocol (e.g., secure sockets layer/transport layer security (SSL/TLS)).
- The IPTV architecture of an IPTV brokering service is required to provide confidentiality and integrity of contents delivered from a brokering service provider to an end user.
- The IPTV architecture of an IPTV brokering service is required to provide availability of a brokering service provider 's system at the web level.
- The IPTV architecture of an IPTV brokering service is required to support the secure delivery of content protection and content management metadata, including usage rights metadata.

9.2.3 Security requirements between a brokering service provider and an original service provider

This clause specifies the security that individually or collectively deals with the service of a brokering service provider and an original service provider. Security requirements described in [ITU-T X.1191] should be applied. However, the following specific security requirements shall be applied:

- In the case of a delegator model, the IPTV architecture of a brokering service provider is required to provide collecting contents or metadata securely from one or more original service providers.
- In the case of a delegator model, the IPTV architecture of a brokering service provider is required to support mechanisms for providing contents and metadata transformation securely.
- The IPTV architecture of an IPTV brokering service is required to provide data source authentication of metadata and contents delivered from an original service provider or a brokering service provider.
- The IPTV architecture of an IPTV brokering service is required to have a security service level agreement with the original service provider.

9.2.4 Security requirements between an end user and an original service provider (only in a coordinator model)

This clause specifies the security that deals individually, or collectively, with the service of an end user and an original service provider in a coordinator model.

- The IPTV architecture of an IPTV brokering service is required to support end-to-end confidentiality of meta-data and contents.
- In the case of a coordinator model, the IPTV architecture of the brokering service provider is required to collect metadata securely from one or more original service providers.
- The IPTV architecture of a brokering service provider is required to provide metadata transformation securely between web environments and the original IPTV environment.

- The IPTV architecture of an IPTV brokering service is required to support SCP mechanisms that can be operated regardless of specific formats of content.
- The IPTV architecture of an IPTV brokering service is recommended to protect the wireless access point and the entry point that are deployed in the end user 's premise.

9.3 Security requirement for a downloadable SCP system in a broker environment

9.3.1 General security requirements for downloadable SCP system in broker environment

Figure 9-4 describes a framework for a downloadable SCP system with a trusted authority (TA) in a broker environment. It is composed of four elements: an end-user, a brokering service provider, an original service provider and a trusted authority. An end-user can download a SCP operating code from the brokering service provider or the original service provider depending on the brokering model. In the case of the coordinator model, the end-user is able to download a SCP operating code from original service provider. In case of the delegator model, an end-user is not able to download a SCP operating code from the original service provider as shown in Figure 9-5.

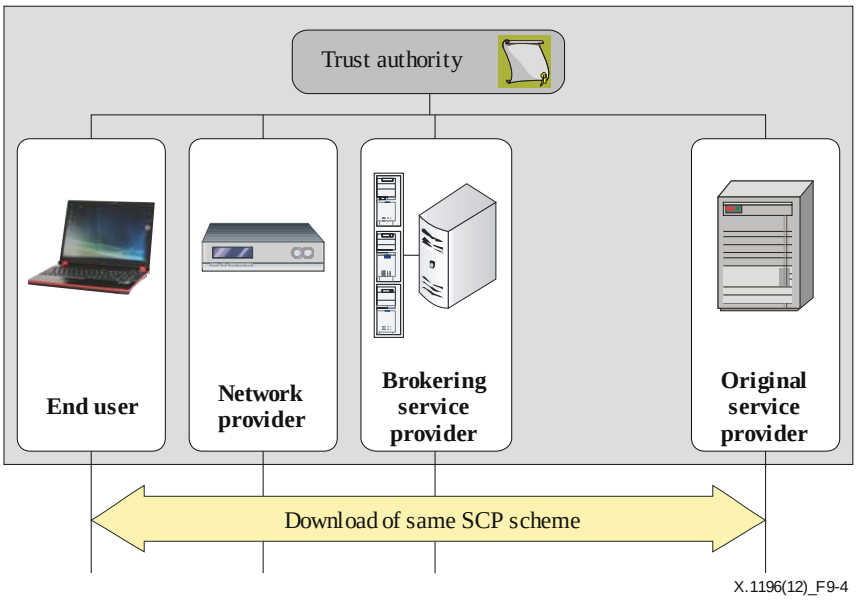


Figure 9-4 – Downloadable SCP system with TA in broker environment (coordinator model)

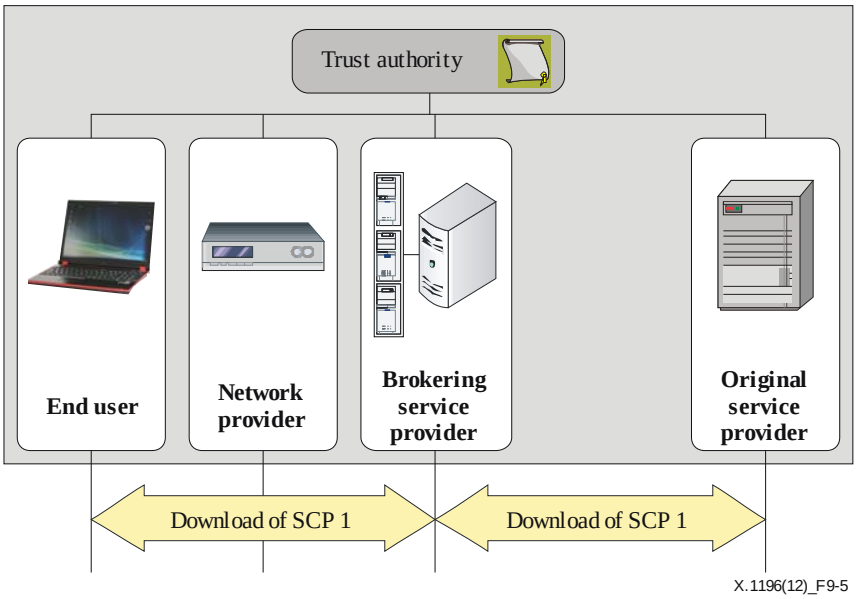


Figure 9-5 – Downloadable SCP system with TA in broker environment (delegator model)

This clause describes general security requirements for the downloadable SCP system in the broker environment.

- A downloadable SCP system can optionally run the SCP operating code on the virtual machine in the end-user system, where the virtual machine is software implementation of a machine (i.e., a computer) that executes programs like a physical machine.
- A downloadable SCP system is required to provide support for integrity, mutual authentication and non-repudiation for the downloaded SCP operating code.
- A downloadable SCP system is required to provide error processing.
- A downloadable SCP system is prohibited from updating and modifying the SCP code while SCP function is running in the end-user system.

9.3.2 Security requirements for secure download of the SCP operating code

The security requirements for downloadable SCP system may depend on the two types of brokering models.

- Regardless of the brokering model, it is recommended to use the key management scheme described in clause 8.3 of [ITU-T X.1193] for downloading the SCP operating code.
- Regardless of the brokering model, it is recommended to use the SCP interoperability scheme described in [ITU-T X.1195] for downloading the SCP operating code.
- IPTV TD in the end user is required to authenticate the downloaded SCP operating code.
- IPTV TD in the end user is required to verify that the downloaded SCP operating code has not been altered from the original form in which it was provided by the trusted source.
- IPTV TD in the end user is required to verify that the downloaded SCP operating code is appropriate for itself. If the downloaded SCP operating code is appropriate, the IPTV TD is required to write the new SCP operating code to non-volatile storage. Once the file transfer is completed successfully, the IPTV TD is required to restart itself with the new SCP operating code.

- IPTV TD in the end user is required to log download failures of the SCP operating code, and can report failures asynchronously to the network manager of the IPTV service provider.
- Where the SCP operating code has been upgraded to meet a new version, the SCP operating code is required to work with the previous version in order to allow a gradual transition of units on to the network.
- The process of the downloadable SCP scheme can optionally provide a capability for IPTV service operators to dictate their own downloadable SCP policies.
- The IPTV service provider should generate a code verification certificate (CVC) over the SCP operating code and other relevant attributes for PKCS#7-based digital signature to the downloaded SCP operating code. The private key used to generate the digital signature should be bound to a public key certificate that chains up to CVC root CA. The digital signature is to authenticate the message and integrity of the downloaded SCP operating code.
- IPTV TD in the end user is required to be able to process a PKCS#7-based digital signature for verifying the authenticity of the downloaded SCP code, and an ITU-T X.509 certificate for identifying the IPTV TD, respectively.
- IPTV TD in the end user is required to be able to update a code verification certificate (CVC) root CA certificate stored in the IPTV device after the certificate has been validated, if contained in a Code File as a TLV.
- IPTV TD in the end user is required to be able to replace the manufacturer CA certificate(s) stored in the IPTV device after the certificate has been validated, if contained in a code file as a TLV.
- IPTV TD in the end user is required to be able to update the CVC CA certificate stored in the IPTV TD after the certificate has been validated, if contained in a code file as a TLV.
- IPTV TD in the end user is required to be able to update the service provider root CA certificate stored in the device after the certificate has been validated, if contained in a code file as a TLV.

Bibliography

[b-ITU-T J.192] Recommendation ITU-T J.192 (2005), *A residential gateway to support the delivery of cable data services*.

[b-ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[b-ITUT X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-NIST SP 800-120] NIST Special Publication 800-120, *Recommendation for EAP methods used in wireless network access authentication*.

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, 2013