



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1195

(02/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

Service and content protection (SCP) interoperability scheme

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2011

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

Recommendation ITU-T X.1195

Service and content protection (SCP) interoperability scheme

Summary

This Recommendation develops a complete set of requirements for interoperable SCP to support interoperability between multiple SCP mechanisms. This includes interoperable SCP scenarios, interoperable SCP architecture and interoperable SCP process.

Keywords

Interoperability, Interoperable SCP, Security, Content Protection, Service Protection.

1195

Table of Contents

1.	Scope	4
2.	References.....	4
3.	Terms and definitions	4
3.1.	Terms defined elsewhere	4
3.2.	Terms defined in this Recommendation.....	5
4.	Abbreviations and acronyms	5
5.	Conventions	6
6.	Introduction	6
6.1	IPTV general architecture and content protection architecture	6
6.2	Overview of the interoperable SCP framework	8
7	Interoperable SCP framework	9
7.1	Interoperable SCP architecture.....	9
7.2	Interworking processes	10
8	Interworking process protocol specification.....	18
8.1	Overview of the protocol message	18
8.2	Authentication protocol	18
8.3	Negotiation protocol	20
8.4	Transmission protocol	22
8.5	Transmission packet format	25
Annex A	Scenarios of SCP-B or SCP-IX deployed in IPTV TD	28
A.1	Definitions of terms used in the diagram	28
A.2	Scenario 1: SCP with SCP-IX	28
A.3	Scenario 2: SCP with optional SCP-B and storage	29
A.4	Scenario 3: SCP with storage and SCP-IX.....	29
Annex B	Basic type and premises of the interworking process protocol	30
B.1	Request type	30
B.2	Response type	30
B.3	Status type	30
B.4	Extension type	31
B.5	Nonce type.....	31
B.6	Canonicalization and digital signature	31
Annex C	Interworking process protocol schema	32
Appendix I	Interoperable SCP types.....	36
I.1	SCP End-to-End (SCP-EE).....	36
I.2	SCP Bridging (SCP-B)	36

Recommendation ITU-T X.1195

Service and content protection (SCP) interoperability scheme

1. Scope

This Recommendation develops a complete set of requirements for the interoperable SCP to support interoperability between multiple SCP mechanisms. This includes interoperable SCP scenarios, interoperable SCP architecture and interoperable SCP process. The Recommendation describes general requirements of the SCP interoperability. This recommendation provides a complete set of requirements for a specific approach and does not include any other legacy approaches to solve SCP interoperability in Recommendation ITU-T X.1191.

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 published regularly.

A reference to a document within this Recommendation does not give it, as a standalone document, the status of a Recommendation.

[ITU-T X.509]	Recommendation ITU-T X.509 (2008), <i>Information Technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks</i>
[ITU-T X.800]	Recommendation ITU-T X.800 (1991), <i>Security Architecture for Open Systems Interconnection for CCITT applications</i>
[ITU-T X.1191]	Recommendation ITU-T X.1191 (2009), <i>Functional requirements and architecture for IPTV security aspects</i>

3. Terms and definitions

3.1. Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 Authentication [ITU-T X.800]:** See Data Origin Authentication and Peer Entity Authentication.
- 3.1.2 Authorization [ITU-T X.800]:** The granting of rights, which includes the granting of access based on access rights.
- 3.1.3 Content Protection [ITU-T X. 1191]:** Ensuring that an end-user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder. Content Protection includes protecting contents from illegal copying and distribution, interception, tampering, unauthorized use, etc.

- 3.1.4 Rights [ITU-T X.1191]:** One or more legal or business entitlements to use or employ Content, e.g., to view, record, redistribute Content.
- 3.1.5 Rights Expression [ITU-T X.1191]:** The syntactic embodiment of Rights in a concrete form.
- 3.1.6 SCP end-to-end [ITU-T X.1191]:** Service and Content Protection operating mode wherein content is accessed or exchanged by end-devices according to the granted rights using a single Service and Content Protection system.
- 3.1.7 SCP bridging [ITU-T X.1191]:** Service and Content Protection operating mode wherein two or more Service and Content Protection systems are operational on a single device acting as a bridge between these Service and Content Protection systems; content acquired via one Service and Content Protection system can be accessed via another Service and Content Protection system on the bridge according to the granted rights.
- 3.1.8 SCP interchange [ITU-T X.1191]:** A more general Service and Content Protection operating mode involving two or more devices, with each device having one or more operational Service and Content Protection systems; the content acquired by one device through one of its Service and Content Protection systems can be securely transferred to and accessed on another device through a different Service and Content Protection system according to the granted rights.
- 3.1.9 Service [ITU-T X.1191]:** A set of functionality enabled by a provider for end-users; for example, providing IP connectivity with managed quality of service, providing an IPTV Service, providing a content on demand service, etc.
- 3.1.10 Service Protection [ITU-T X.1191]:** Ensuring that an end-user can only acquire a service, and, by extension, the content contained therein, that they are entitled to receive. Service Protection includes protecting service from unauthorized access as IPTV contents traverse through the IPTV service connections.
- 3.1.11 Service and Content Protection [ITU-T X.1191]:** A combination of Service Protection and Content Protection, or a system or implementation thereof.

3.2. Terms defined in this Recommendation

This document defines the following terms:

- 3.2.1 SCP interworking:** General SCP interoperable operation including SCP bridging and SCP interchange

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IPTV	Internet Protocol Television
SCP	Service and Content Protection
SCP-B	SCP Bridging
SCP-EE	SCP End-to-End
SCP-IX	SCP Interchange
TD	Terminal Device
WM	Watermark(ing)

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 document 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 document is to be claimed.

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

In the body of this document and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6. Introduction

In general, two or more SCPs are deployed on a single TD. Content acquired via one SCP system (e.g., from a network) can be accessed via another SCP residing on the same device according to the granted rights. It is necessary to support SCP interoperability among multiple security systems using different security mechanisms for the purpose of supporting the seamless time-shifting service (subscribers can store the content and retrieve it later) and place-shifting service (subscribers can view the content anywhere) even with different security mechanisms.

The objective of this recommendation is to develop a complete set of requirements for the interoperable SCP to support interoperability between multiple SCP mechanisms. This includes interoperable SCP scenarios, interoperable SCP architecture, and interoperable SCP process.

6.1 IPTV general architecture and content protection architecture

The general security architecture for IPTV is depicted in Figure 6-1 below. The general architecture is divided into two primary areas: one considered in-scope for the purpose of considering interoperability based on this document, and the other considered out-of-scope. The first area encompasses End-User, Network Provider, and Service Provider domains, whereas the second area encompasses the Content Provider domain.

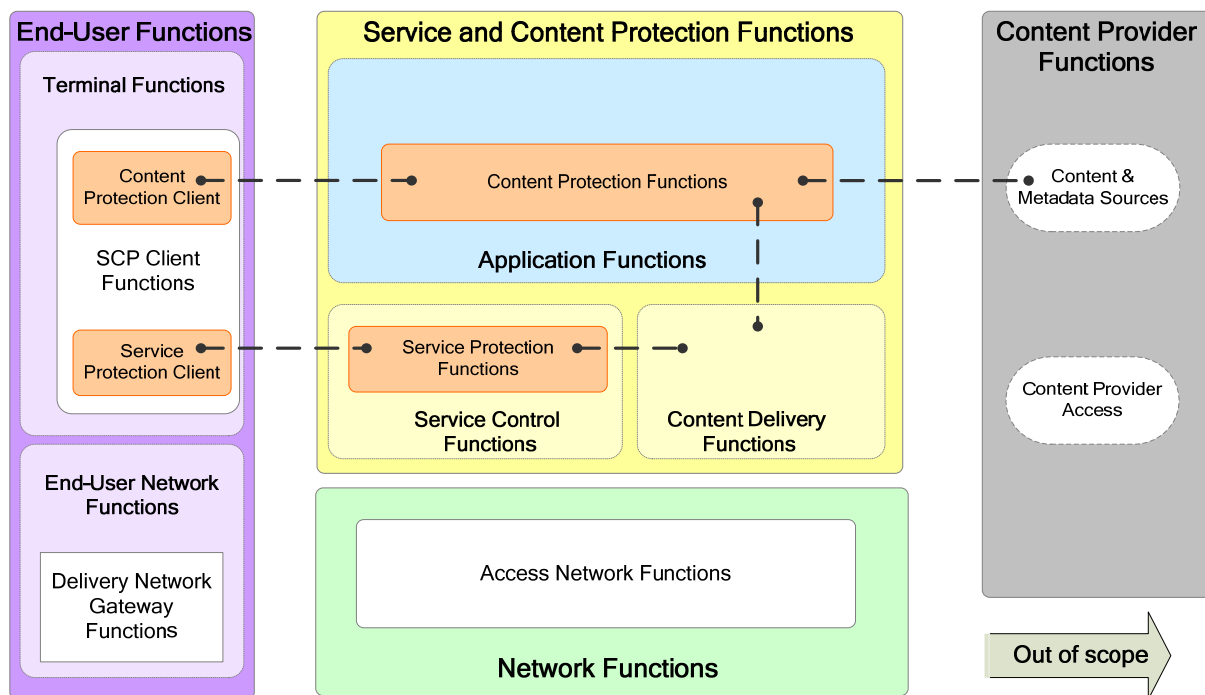
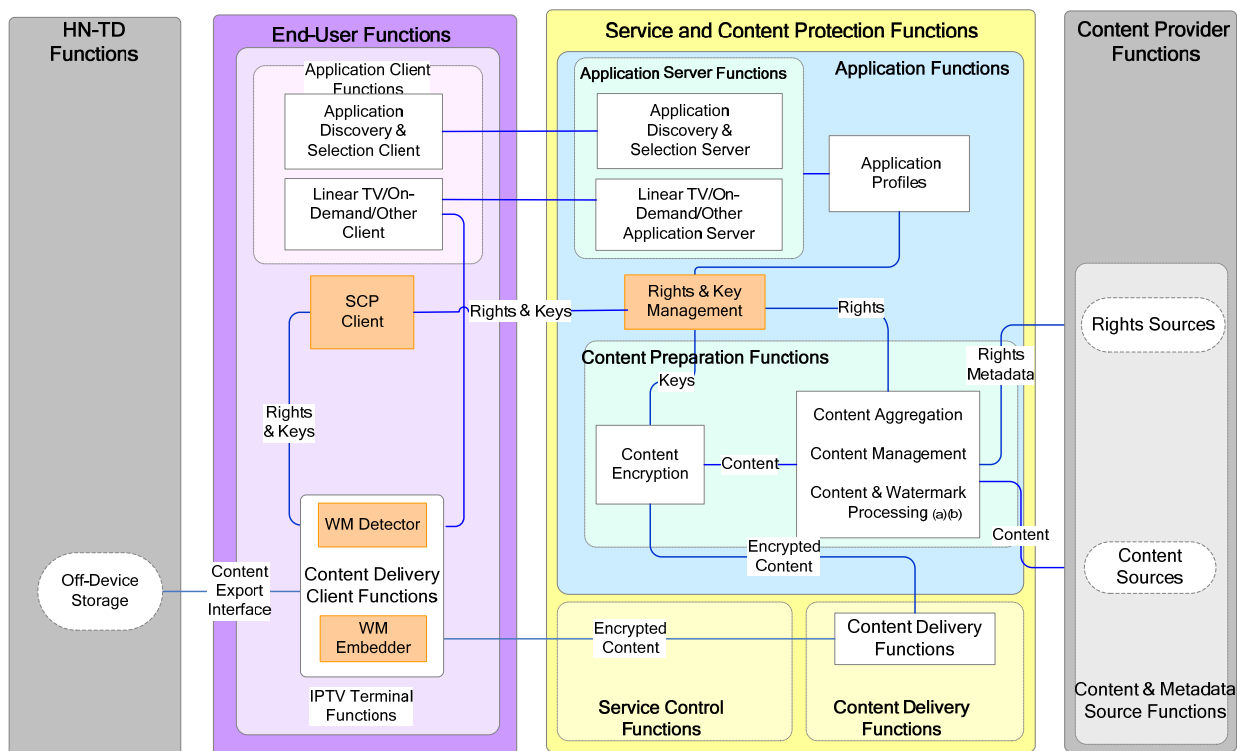


Figure 6-1 - IPTV general security architecture

The content protection architecture for IPTV is depicted in Figure 6-2 below.

The primary function of the content protection architecture is to delineate the flow and process of information related to content usage rights and information required to manage and facilitate such rights.

Ultimately, rights of content use originate with content provider(s); however, such rights may be modified (e.g., narrowed, or perhaps even widened) by service provider(s) according to their agreements with content providers and their operational and business policies. From an operational and typical legal perspective, an end-user's access and use of content is with the service provider, and not with a content provider.



- (a) Optional Watermark Metadata Generation to facilitate downstream watermark embedding
- (b) Optional Watermark embedder to individuate content to networks, servers, and uni-cast deliveries
- (c) Optional Watermark embedder to individuate multi-cast content instances
- (d) Optional Off-Device Storage: a storage device inside HN-TD.
- (e) Optional Detector for copy protection watermarks

Note: objects in grey color are out scope of IPTV security architecture

Figure 6-2 - IPTV content protection architecture

6.2 Overview of the interoperable SCP framework

IPTV Terminal Device can have two different SCPs, one for IPTV service and the other for PVR function. And in general, SCPs have their own proprietary protected content format, encryption scheme, rights expression languages, and metadata description language and protection policies.

If a content which is provided from a certain IPTV service provider and protected by SCP₁, is about to be stored on the PVR storage with SCP₂'s protection mechanism for later use, protection scheme for the content needs to be changed from SCP₁ to SCP₂ while storing. For the seamless conversion, it needs proprietary or standard protocol between SCP₁ and SCP₂. Interoperable SCP framework is a recommended standard to provide interoperable conversion environment based on SCP interworking process between two different SCPs.

Comprehensive overview of Interoperable SCP framework for IPTV TD is depicted in Figure 6-3.

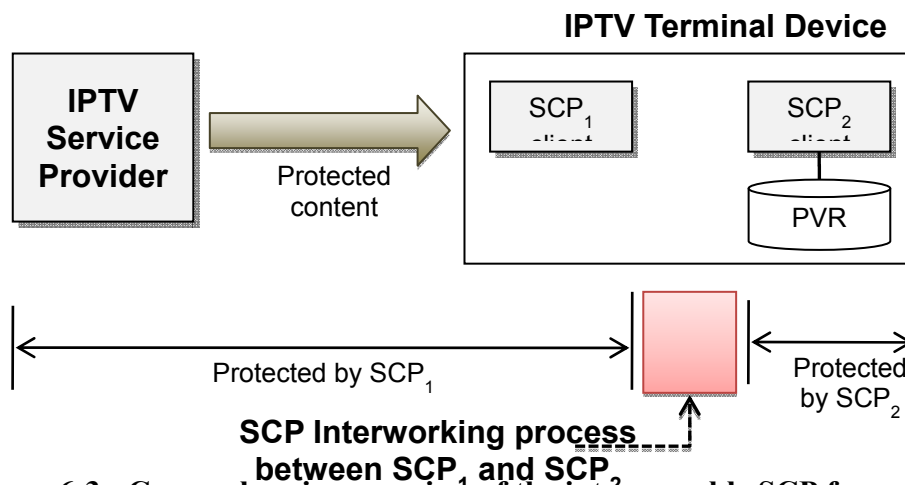


Figure 6-3 - Comprehensive overview of the interoperable SCP framework

An open protocol that is specified in this document can be introduced for the interoperable SCP framework, or a legacy scheme may take on this role.

7 Interoperable SCP framework

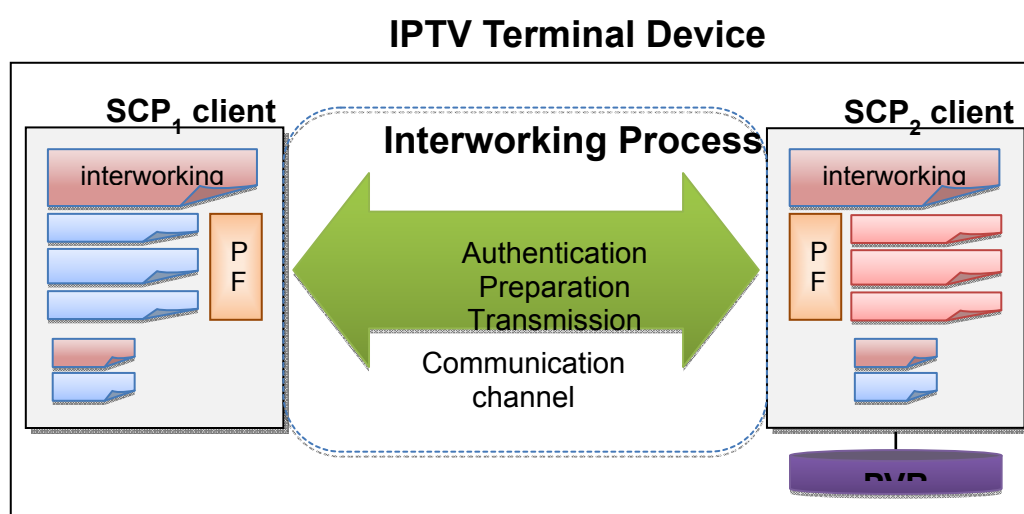
7.1 Interoperable SCP architecture

The interoperable SCP architecture consists of two SCP clients having would-be transferable content and related information and interworking process as in Figure 7-1.

Basically, the interworking process is a set of procedures wherein two SCP clients mutually authenticate, process preparation works for the transmission, and transmit interworking data (i.e., content, metadata, and usage rights) from SCP₁ to SCP₂ through a secure communication channel.

Rules and policies supervise the interworking process. Each SCP has its own rules and policies for the interchange of content. Rules and policies may be provided by the IPTV service provider, PVR provider or SCP providers, etc.

Detailed explanation will be described in the following subclauses.



PFs:Preparation functions

Figure 7-1 - Interoperable SCP architecture

7.1.1 Interworking policy

For the interworking process, there can be rules, restrictions and/or policies from IPTV service provider and/or SCP provider such as ‘blacklisted SCPs’, ‘viewing of the stored content is limited to 1 week’, ‘interworking is allowed only to the SCPs with certificate from specified authority’, etc.

The interworking policy is differentiated from usage rights. Usage rights is a metadata described usage permission or condition of the content itself. On the other hand, the interworking policy is the criteria to determine whether a SCP₁ client starts the interworking or not against the SCP₂.

7.1.2 Preparation functions

Preparation functions in the SCP client are behaviours to adapt or convert content, metadata and usage rights from SCP₁ client to SCP₂ client. Detail functions of the preparation functions are described in the subclause 7.2.4.

7.1.3 SCP clients

SCP clients that take part in the interworking process are responsible for sending or receiving content, metadata and usage rights through the converting process, which is done by the preparation functions.

It has the interworking policy and preparation functions for the interworking process. SCP₁ client has the content, metadata and usage rights to be sent to opponent SCP₂ client. And SCP₂ client has also those ones received from SCP₁.

7.1.4 Communication channel

Communication channel is a secure authenticated channel. It is for data transmission between SCP₁ client and SCP₂ one. The channel is required to be accessible only after passing the mutual authentication process between two SCP parties.

The communication channel is usually protected by secure mechanism.

7.1.5 Interworking process

Interworking process comprises of three sub processes which are authentication, preparation and transmission. Details of the interworking process are explained at subclause 7.2

7.2 Interworking processes

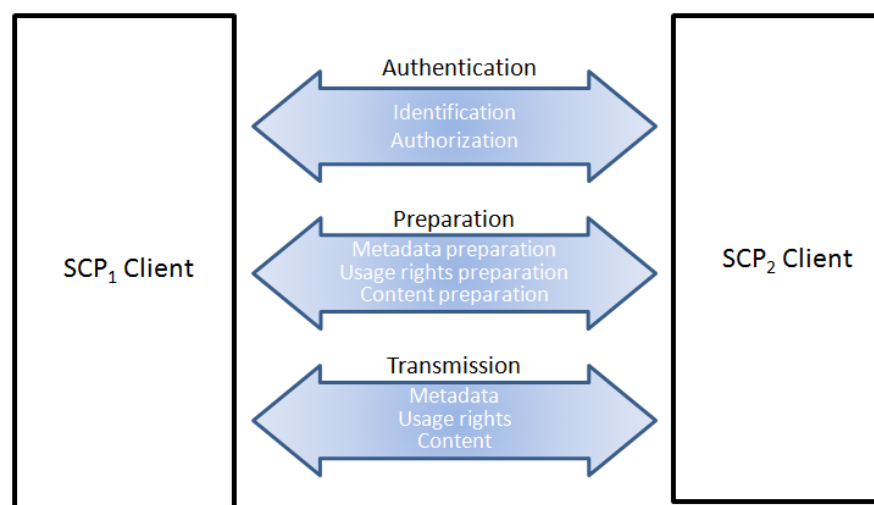


Figure 7-2 - Interworking process

7.2.1 Overview

Interworking process comprises of three sub processes which are authentication, preparation and transmission.

7.2.2 Authentication

Each SCP party is required to judge whether the other party is a proper target for achieving SCP interworking. It is a preliminary step before data conversion and transmission, and usually accompanied by the mutual authentication process.

All SCP clients are required to be identified by corresponding SCP with unique identifier for later authorization process on the interworking process. This step includes verifying authenticity of the identifier by cryptographic mechanism.

To improve efficiency of the verifying process, some registration function is involved in this step.

All identified SCP clients are required to be authorized by the corresponding SCP with the identifier for further interworking process. Even though an SCP client is identified and verified properly, it can be rejected in the authorization process if the SCP client does not meet the requirements described in the interworking policy. The interworking policy can be managed in the form of whitelist or blacklist.

7.2.2.1 Authentication protocol

The SCP interworking process always needs mutual authentication to confirm that both sender and receiver are secure parties. Authentication is recommended to use well-known and proven technology for secure processing. X.509 certificate technology is required to be used as authentication method. It provides very useful infrastructure to exchange secure data and guarantee trustworthy validation of the participants' authenticity. Various authentication schemes based on the X.509 certificate such as SSL/TLS can be used as authentication protocol. Figure 7-3 describes the authentication process of the interworking process.

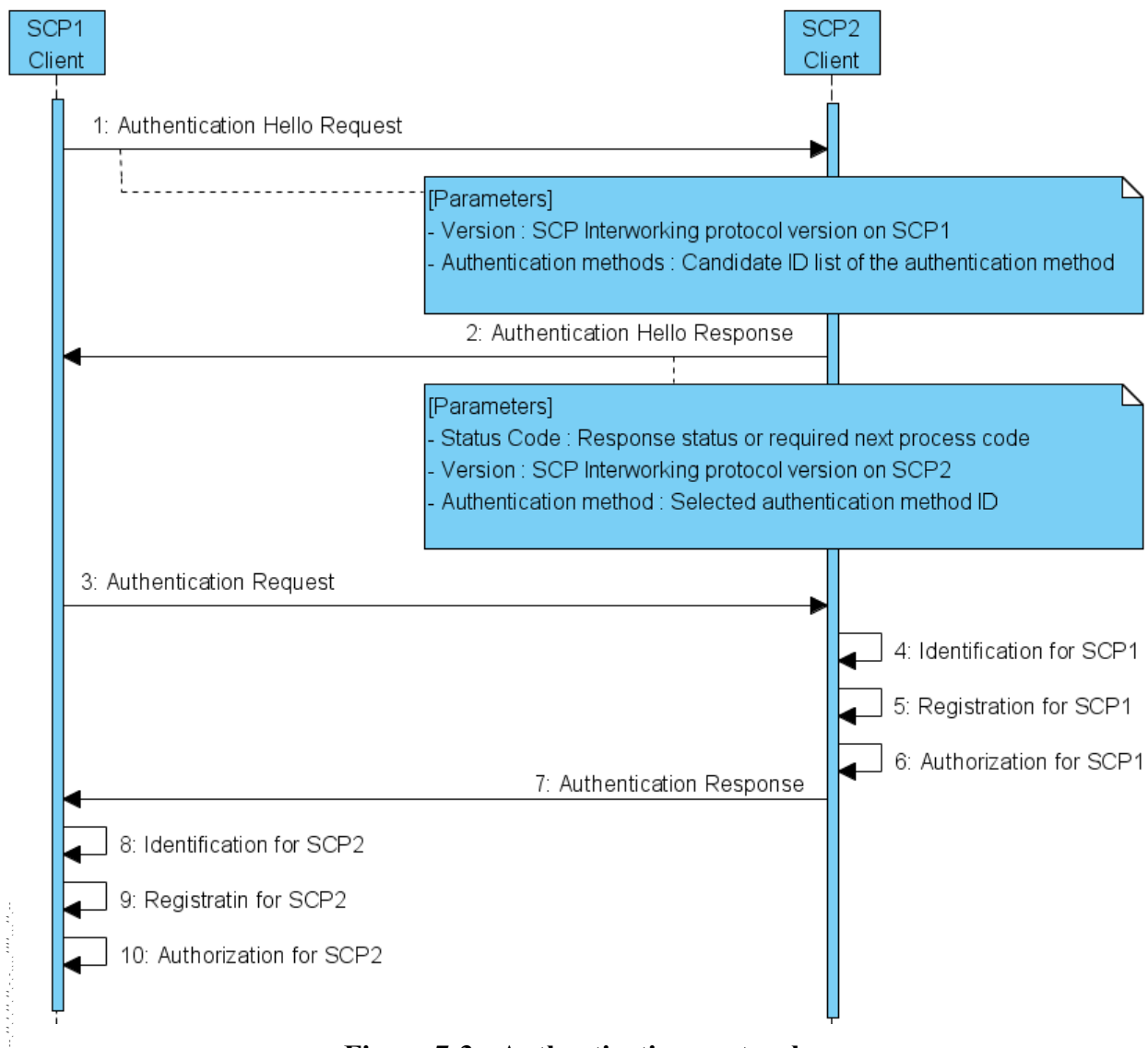


Figure 7-3 - Authentication protocol

First, as indicated in the figure above, the SCP₁ and SCP₂ Client agree authentication method each other by exchanging Hello messages. Then two parties do mutual authentication process with agreed method. The processing sequences are:

1. SCP₁ Client sends Authentication Hello Request message to SCP₂ to start protocol with the following parameters
 - Version: SCP Interworking protocol version number on SCP₁.
 - Authentication methods : Candidate ID list of the authentication methods
2. SCP₂ Client sends Authentication Hello Response message to SCP₁ Client with the following parameters
 - Status Code: Return value.
 - Version: SCP Interworking protocol version number on SCP₂
 - Authentication type: Selected authentication type ID

3. SCP₁ Client starts authentication process with agreed method
4. Identification for SCP₁: SCP₂ Client verifies SCP₁'s authenticity with its ID.
5. Registration for SCP₁: SCP₂ Client registers SCP₁'s ID. It is used when SCP₁'s ID is not registered. ID is an encoded subjectPublicKeyInfo component of the X.509 digital certificate, which is digested with SHA256 and encoded with based 64. Appendix N shows an example how to get this value with the openssl tool.
6. Authorization for SCP₁: SCP₂ Client decides if it allows further processing with SCP₁ by its interworking policy.
7. SCP₂ Client responses authentication process with the agreed method
8. Identification for SCP₂: SCP₁ Client verifies SCP₂'s authenticity with its ID.
9. Registration for SCP₂: SCP₁ Client registers SCP₂'s ID. It used when SCP₂'s ID is not registered. ID is an encoded subjectPublicKeyInfo component of the X.509 digital certificate, which is digested with SHA256 and encoded with based 64. Appendix N shows an example how to get this value with the openssl tool.
10. Authorization for SCP₂: SCP₁ Client decides if it allows further processing with SCP₂ by its interworking policy.

SSL/TLS or proprietary authentication schemes are able to be used as mutual authentication method (steps 3 ~ 7). During the authentication process, it is assumed that the X.509 digital certificates of the SCP₁ and SCP₂ clients are sent to each other based on the agreed authentication method. A proprietary authentication scheme based on the X.509 certificate is introduced in Appendix L.

7.2.3 Preparation

Each SCP party needs to convert the content protection scheme, expression way of the metadata and usage rights before they are transmitted. It is a preliminary step before data transmission and is usually accompanied by exchanging some information on each SCP's preferences, e.g. usage rights or metadata format, bit rates and resolution etc.

7.2.3.1 Content preparation

Content preparation is responsible for converting cryptographic algorithm for content protection. Several predefined standard encryption algorithms are able to be considered.

If the communication channel for data transmission is well-protected, content can be transmitted with plain text.

Bit rates or resolution of the content can be changed after exchanging information between 2 SCPs in this step.

7.2.3.2 Usage rights preparation

Usage rights preparation is responsible for converting expression way of usage rights. Some standard or preferred expression ways of usage rights known to both parties are used for converting.

The converted usage rights are required to maintain the same semantics defined in the original usage rights.

The standard expression ways are the predefined ones that every IPTV TD compliant SCPs have to know. And the preferred expression way can be determined after exchanging information between 2 SCPs in this step.