

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1198

(06/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – IPTV security

Virtual machine-based security platform for renewable IPTV service and content protection

Recommendation ITU-T X.1198



International
Telecommunication
Union

Document Sharing Hub

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1198

Virtual machine-based security platform for renewable IPTV service and content protection

Summary

Recommendation ITU-T X.1198 specifies a virtual machine-based security platform for the renewable service and content protection (SCP) system. The virtual machine supports an abstract function of hardware devices. This Recommendation defines a common interface and functional logic in the Internet protocol television (IPTV) terminal device and includes the data structure of SCP client and system components for a terminal device such as an embedded SCP, media client and control client.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1198	2013-06-13	17

Keywords

Conditional access, downloadable security, exchangeable security, renewable security, service protection, terminal device.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

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

© ITU 2013

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	3
6 Overview of a virtual machine platform.....	4
6.1 General architecture of a virtual machine	4
6.2 Requirements for a virtual machine-based security system	5
6.3 Architecture of the SCP virtual machine.....	6
7 Virtual machine-based security platform for the SCP system.....	9
7.1 System architecture	11
7.2 SCP virtual machine	12
7.3 Service and content protection (SCP) client.....	13
7.4 Protection of the SCP client and SVM.....	13
7.5 Security policy.....	14
7.6 System call.....	15
7.7 Event.....	16
Annex A – Data structure of SCP client package	19
A.1 Header of SCP client	19
A.2 Policy data	20
A.3 Code data.....	21
A.4 Signature.....	21
Bibliography.....	22

Downloaded from ITU-T X.1198 2013

Recommendation ITU-T X.1198

Virtual machine-based security platform for renewable IPTV service and content protection

1 Scope

This Recommendation develops a virtual machine-based security platform for renewable service and content protection (SCP) under Internet protocol television (IPTV) services. This includes the virtual machine architecture and the mechanism for organizing virtual machine-related components such as SCP client, terminal client (embedded SCP) and media client. The following items are addressed:

- a) Behaviour of SCP client: An SCP client has its pre-determined legitimate behaviour of execution. An SCP virtual machine (VM) should monitor the behaviour of an SCP client in run-time. This allows the system to prevent malicious code or unintentional code. Moreover, an SCP VM may support a reporting ability in case of illegal situations.
- b) Protection of SCP client: An SCP client code should not be seen by any unauthorized person or device during transmission. In addition, an SCP client code may be converted to an unreadable form even while loading a process.
- c) Integration with embedded SCP: An embedded SCP should obey the policy of the SCP client, including storing and retransmission.
- d) Integration with media client: A media client should deliver every event that has occurred in the device to the SCP VM. Deleting or modifying an event or its parameter is not allowed.

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.1194] Recommendation ITU-T X.1194 (2012), *Algorithm selection scheme for service and content protection descrambling*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 (entity) authentication [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.5 digital signature [b-ITU-T X.800]: Data appended to, or a cryptographic transformation (see cryptography in [b-ITU-T X.800]) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

3.1.6 integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.7 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.8 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.9 process [ITU-T X.1194]: Instance of a computer program that is being executed; contains the program code and its current status.

3.1.10 scrambling algorithm [b-ITU-T X.1191]: Algorithm used in a scrambling or a descrambling process.

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

3.1.12 service protection [b-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.

3.1.13 virtual machine [ITU-T X.1194]: Software implementation of a machine that can execute programs just like a physical machine; supports separated operating systems.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 conditional access: A function served by a conditional access system; often used as an abbreviation for conditional access system.

3.2.2 conditional access system: A component of a service and content protection system the purpose of which is to prevent unauthorized (unentitled) access to a service or to content.

3.2.3 trap: A code or signal function designed to capture errors and reveal where they have occurred.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
CPU	Central Processing Unit
ECM	Entitlement Control Message
EMM	Entitlement Management Message
EPG	Electronic Programme Guide
HAL	Hardware Abstraction Layer
H/W	Hardware

ID	Identity
IDE	Integrated Drive Electronics
I/O	Input/Output
IPTV	Internet Protocol Television
OS	Operating System
OTID	One-Time Identifier
PC	Program Counter
SCP	Service and Content Protection
SCSI	Small Computer System Interface
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
SVM	Secure Virtual Machine
S/W	Software
TLS	Transport Layer Security
UI	User Interface
USB	User Serial Bus
UX	User experience
VM	Virtual Machine
VoD	Video on Demand
XML	extensible Markup Language

5 Conventions

In this Recommendation:

The words "**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 words "**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 words "**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 words "**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.

In the body of this Recommendation and its annex, 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 words in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.