

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1011

(09/2016)

SERIES J: CABLE NETWORKS AND TRANSMISSION
OF TELEVISION, SOUND PROGRAMME AND OTHER
MULTIMEDIA SIGNALS

Conditional access and protection – Exchangeable
embedded conditional access and digital rights
management solutions

Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview

Recommendation ITU-T J.1011



International
Telecommunication
Union

Document Sharing Hub

Recommendation ITU-T J.1011

Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview

Summary

Recommendation ITU-T J.1011 specifies an architecture for exchangeable, embedded conditional access/digital rights management or CA/DRM solutions, enabling consumer premises equipment (CPE), which are capable of receiving broadcast and broadband content, to download CA/DRM clients under a trusted environment. By utilizing a downloadable multi-CA/DRM service, entitled consumers can consume broadcast and broadband content, which is controlled by digital rights management (DRM) and/or CA systems, even though a CPE does not have a required content-related CA/DRM client available, by downloading it from a trusted source into various types of CPEs including set-top boxes (STBs), smart TVs, PCs, smart phones and/or smart tablets.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J.1011	2016-09-02	9	11.1002/1000/12773

Keywords

CA/DRM, exchangeable embedded common interface, retail CPE.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 2017

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.....	1
4	Abbreviations and acronyms	2
5	Conventions	3
6	Architecture for exchangeable, embedded CA/DRM solutions	3
	6.1 General remarks.....	3
	6.2 The technical concept of the ECI system	5
7	Trust environment.....	11
	7.1 Necessary operational workflows.....	12
	Appendix I – Implementation of an ECI-compliant trust system	15
	Bibliography.....	17

Copyright International Telecommunication Union/ITU Telecommunication Sector
 Provided by IHS Markit under license with ITU-T
 No reproduction or networking permitted without license from IHS
 Full document details: ITU-T J.1011 2016

Introduction

Service and content protection realized by conditional access (CA) and digital rights management (DRM) are essential in the rapidly developing area of digital broadcast and broadband, including content, services, networks and customer premises equipment (CPE), to protect business models of content owners, network operators and PayTV operators. While conceptually CA focuses on mechanisms to access protected content distributed by a service provider over a network, DRM originally describes type and extent of the usage rights, according to the subscriber's contract.

PayTV operators have established digital TV platforms, which implement standards for basic functions, extended with proprietary elements. Most CA and DRM systems used for classical digital broadcasting, Internet protocol television (IPTV) or new over-the-top (OTT) services capture consumer premises equipment (CPE) by binding it with proprietary security related elements. As a result, consumer premises equipment configured for use in network or platform A cannot be used in network or platform B or vice versa. Thus, the consumer electronics market for digital TV is still fragmented, as specifications differ not only per country, but also per platform. Detachable CA/DRM modules only offer a partial solution; the modules are again proprietary to the CA/DRM system, they are not cheap either and they are used primarily for cable or satellite TV and are not usable in modern-type equipment such as tablets due to lack of appropriate physical interfaces.

Currently implemented solutions, whether embedded or as detachable hardware, result in "lock-in" effects. This seriously restricts the freedom of many players in digital multimedia content markets. Due to technological advances, innovative, software-based CA/DRM solutions become feasible. Maximizing interoperability while maintaining a high level of security, they promise to meet upcoming demands in the market, allow for new businesses, and broaden consumer choice.

It is in consumers' interest that they are able to continue using the CPEs they bought e.g., after a move or a change of network provider or even utilize devices for services of different commercial video portals. This can only be achieved by interoperability of CPEs regarding CA and DRM, based on an appropriate security architecture. Further fragmentation of the market for CPEs can only be prevented and competition encouraged by ensuring a consumer-friendly and context-sensitive exchangeability of CA and DRM systems.

Recommendation ITU-T J.1011

Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview

1 Scope

The object of this Recommendation is to specify functional entities of an architecture for an exchangeable, embedded common interface, in order to download any necessary CA/DRM system to CPE. The download process is operated under a trusted environment and enables the consumption of protected content delivered via broadcast and/or broadband connections with various types of terminal equipment in line with the acquired content rights of the end user. This Recommendation is one in a series of Recommendations, specifying the whole embedded common interface (ECI) eco-system.

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.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1 (2014), *Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview*.

[ETSI GS ECI 001-2] ETSI GS ECI 001-2 (2014), *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 advanced security: Function of an ECI compliant CPE which provides enhanced security functions (hardware and software) for an ECI client. Note that the details are specified in [b-ETSI GS ECI 001-5].

3.2.2 ECI (embedded CI): The architecture and the system specified in the ETSI ISG "embedded CI", which allows the development and implementation of software-based swappable ECI clients in customer premises equipment (CPE) and thus provides interoperability of CPE devices with respect to ECI.

3.2.3 ECI client (embedded CI client): Implementation of a CA/DRM client which is compliant with the embedded CI specifications. Note that it is the software module in a CPE which provides all means to receive, in a protected manner and to control execution of a consumer's entitlements and rights concerning the content that is distributed by a content distributor or operator. It also

receives the conditions under which a right or an entitlement can be used by the consumer and the keys to decrypt the various messages and content.

3.2.4 ECI client loader: Software module part of the ECI host which allows downloading, verification and installation of new ECI client software in an ECI container of the ECI host.

3.2.5 ECI container (embedded CI container): Abstract concept which provides an isolated environment comprised of a virtual machine and a single ECI client.

3.2.6 ECI host: Hardware and software system of a CPE, which covers ECI related functionalities and has interfaces to an ECI client. Note that the ECI host is one part of the CPE firmware. The ECI host is responsible for ensuring the isolation of each ECI container and provides authenticated loading of ECI clients.

3.2.7 ECI host loader: Software module which allows downloading, verification and installation of (new) ECI host software into a CPE. Note that in a multi-stage loading configuration this term is used to refer to all security critical loading functions involved in loading the ECI host.

3.2.8 trust authority (TA): Organization governing all rules and regulations that apply to implementations of ECI. Note that the trust authority has to be a legal entity to be able to achieve legal claims. The trust authority needs to be impartial to all players in the downloadable CA/DRM ecosystem.

3.2.9 trusted third party (TTP): Technical service provider which issues certificates and keys to compliant manufacturers of the relevant components of an ECI-system under control of the trust authority (TA).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CA	Conditional Access
CENC	Common Encryption
CI	Common Interface
CPE	Customer Premises Equipment
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
ECI	Embedded Common Interface
HD	High Definition
HTTP	Hypertext Transfer Protocol
iDTV	integrated Digital TV
IP	Internet Protocol
IPTV	Internet Protocol Television
LA	License Agreement
MPEG	Motion Picture Experts Group
OS	Operating System
OSD	On Screen Display
OTT	Over-The-Top