International Telecommunication Union

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

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/.

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

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

PIN	Personal Identification Number
PVR	Personal Video Recorder
ROM	Read Only Memory
SI	Service Information
STB	Set-Top Box
TA	Trust Authority
TTP	Trusted Third Party
TV	Television
UI	User Interface
VM	Virtual Machine

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 the specification.

In the body of this Recommendation 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 Architecture for exchangeable, embedded CA/DRM solutions

6.1 General remarks

ECI architecture, definitions and overview, as covered by this framework Recommendation, is part of a multi-part standard specifying a system architecture for general purpose, software-based, embedded and exchangeable CA/DRM systems which would be the most appropriate and future-proof solution for overcoming market fragmentation and enabling interoperability. Key benefits of the envisaged approach for content security are:

– Flexibility and scalability due to software-based implementation
– Exchangeability fostering future-proof solutions and enabling innovation
– Applicability to content distributed via broadcast and broadband, including OTT
– Support of multi-screen environment

– Stimulation of the market for platform operators, network/service providers and consumers by avoiding "lock-in"
– The specification of an open eco-system fostering market development.

The ECI system aims at exchangeability of CA and DRM systems in CPEs on all relevant levels and aspects, at lowest possible costs for the consumers and at minimal restrictions for CA or DRM vendors to develop their target products for the PayTV market. The core element of ECI is to specify the interface between the software-based CA/DRM client and the host system. Therefore, amongst others, the ECI has the following functionalities:

– A software container for the CA respectively the DRM kernel – hereafter called ECI client with:
  • standardized interfaces to all relevant functionalities of the CPE
  • a standardized virtual machine (VM) to run upon
– Support of smartcard-less systems as well as use in smartcard-based systems
– Inclusion of a multitude of such software containers in a CPE, each container running on its own instance of the VM
– Installation of the ECI client independently from other CPE software by a secure and standardized loader concept
– Advanced security, also known as chip set security, to support state-of-the-art content protection
– Provisions to leverage hardware-assisted security functionalities
– Methods for the user to discover the right ECI client to download
– Methods for revocation of (parts of) the ECI client's functionality and CPE's functionality
– Suited for classical digital broadcasting, IPTV or modern OTT-based systems.

Although ECI shows some similarity with already deployed solutions, there are substantial differences:

(1) The CA/DRM client module is in software and no longer in hardware. Hence, no costs are incurred at the consumer side to swap a CA or DRM system.
(2) Several parallel ECI clients can be implemented in one and the same CPE, without adding relevant cost.
(3) These clients can run concurrently in the one device.

As a result, a CA or DRM component can be exchanged much more easily, allowing the end user to change operators or get services from a variety of operators on his CPE, without having to exchange expensive modules.

The complete multi-part standard consists of a group of specifications, including a framework specification, in combination with the underlying specifications:

– Part 1: Architecture, definitions and overview [ETSI GS ECI 001-1]
– Part 2: Use cases and requirements [ETSI GS ECI 001-2]
– Part 3: CA/DRM container, loader, interfaces, revocation [b-ETSI GS ECI 001-3]
– Part 4: The virtual machine (VM) [b-ETSI GS ECI 001-4]
– Part 5: The advanced security system [b-ETSI GS ECI 001-5]
– Part 6: Trust environment [b-ETSI GS ECI 001-6]
– Part 7: Extended requirements [b-ETSI GS ECI 001-7]

which together describe a solution allowing replacement of ECI clients at any time by just downloading the ECI clients requested by an end customer. The ECI clients are installed in a

standard software container in the CPE by a separate loader, with separate security algorithms and keys to protect the ECI clients against integrity and substitution attacks independently from all other software in the CPE. The container's interfaces with the CPE are generic and defined in [b-ETSI GS ECI 001-3], enabling the ECI client to interact with the various functions in the CPE and beyond.

The ECI clients run upon a virtual machine instance that is defined in [b-ETSI GS ECI 001-4].

[b-ETSI GS ECI 001-5] specifies an advanced security mechanism to protect the key to the content during its travel into the CPE processor chip's content decryption facility.

This Recommendation addresses an architecture and an overview of the relevant interface specifications for the implementation of interoperable CA/DRM systems in CPEs.

The ECI specification only applies to the reception and further processing of content which is controlled by a conditional access and/or digital rights management system and has been scrambled by the service provider. Content that is not controlled by a conditional access and/or DRM system is not covered by this Recommendation.

The ECI group specification is intended to be used in combination with a contractual framework (license agreement), compliance and robustness rules, and appropriate certification process (see note), under control of a trust authority [b-ETSI GS ECI 001-6]. Note that contractual framework (license agreement), compliance and robustness rules and appropriate certification processes are not subject to the standardization work in ISG ECI.

6.2 The technical concept of the ECI system

6.2.1 Basic considerations

This Recommendation, in combination with Parts 2 to 5 and 7 of the specifications ([ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4], [b-ETSI GS ECI 001-5] and [b-ETSI GS ECI 001-7]), specifies an architecture allowing downloading, installation, upgrading, removal and replacement of ECI clients at any time, independently from other ECI clients running on the same host, the host CPE's system software or applications running on that host. An ECI host shall be capable to accommodate and to provide the runtime environment for at least two or as many ECI clients as its resources can handle. The ECI clients in a host have to run in parallel, enabling simultaneous decryption or re-encryption of different content streams from different operators.

The technical concept described in this Recommendation and specified in [ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] and [b-ETSI GS ECI 001-5], is applicable to both DVB multicrypt compliant CA systems and common encryption (CENC) compatible DRM systems.

The CPE hosts a special loader only for ECI clients with the necessary security functionality to protect the integrity and authenticity of the ECI clients. This loader can be called and operated at any time to download and verify another ECI client at any time. The loader with its associated security facilities is specified in [b-ETSI GS ECI 001-3].

Concerning this technical concept, each ECI client is installed in a separate software container, with an own virtual machine instance (VM instance), which is specified in [b-ETSI GS ECI 001-4]. The ECI container is specified for CA/DRM functionality only, which is reflected in [b-ETSI GS ECI 001-3]. The interface with the CPE, detailed in [b-ETSI GS ECI 001-3], enables the request and data exchange that is needed for the various CA/DRM functions. These requests and data exchanges may be performed between the ECI client and the host, between two ECI clients in the same host or two ECI clients in different hosts.

TV-centric devices are defined as devices which include MPEG-2 transport stream processing inside the chip-set. ECI requires that those chip-sets implement ECI-compliant advanced security

functionalities. [b-ETSI GS ECI 001-5] specifies provisions to leverage advanced security mechanisms in the chip-set, such as to protect the key associated with the content during its travel into the CPE processor chip's content decryption facility. This advanced security concept allows all ECI clients using the facility, if needed, to operate simultaneously and independently from each other.

Devices for other environments, especially IPTV and tablets, smartphones, etc. typically implement more functionality in software and offer bidirectional IP-communication. This enables specific new types of security enhancement mechanisms. As chip-sets used in those devices include hardware for various processing security functions, ECI requires dedicated hardware-assisted security and robustness functionalities to be implemented in order to achieve ECI-compliance. Therefore, the specification [b-ETSI GS ECI 001-3] includes methods for the ECI client to obtain the relevant parameters of the host's technical capabilities and functionalities, as far as relevant, including possible support of the advanced security as specified in [b-ETSI GS ECI 001-5].

The advanced security functionalities are available simultaneously to any ECI client active in a CPE. ECI clients can also be deployed in platforms with DVB compliant CA systems or with CENC compliant DRM systems running in simulcrypt or multicrypt mode, as long as the server sides of those systems are compliant with the respective DVB/CENC backend standards.

6.2.2 Architectural overview

The ECI allows CA/DRM providers to implement solutions for conditional access (CA) as well as for digital rights management (DRM) within the domain of an individual customer. Figure 1 shows a reference configuration which is fully supported by a complete ECI implementation.

In order to support multi-screen environments within the individual consumer's domain, ECI clients within that domain may communicate with each other, and may make use of a bidirectional network with the provider, depending on the availability of appropriate networks and supporting functionalities in the CA/DRM systems and their ECI clients. [b-ETSI GS ECI 001-3] gives further details.

An ECI client may be implemented in such a way that it is able to operate as a gateway also to non-ECI-conformant clients. The necessary hooks therefore are specified in [b-ETSI GS ECI 001-5]. The specific protocols and implementations of proprietary clients are out of scope of the ECI specifications.

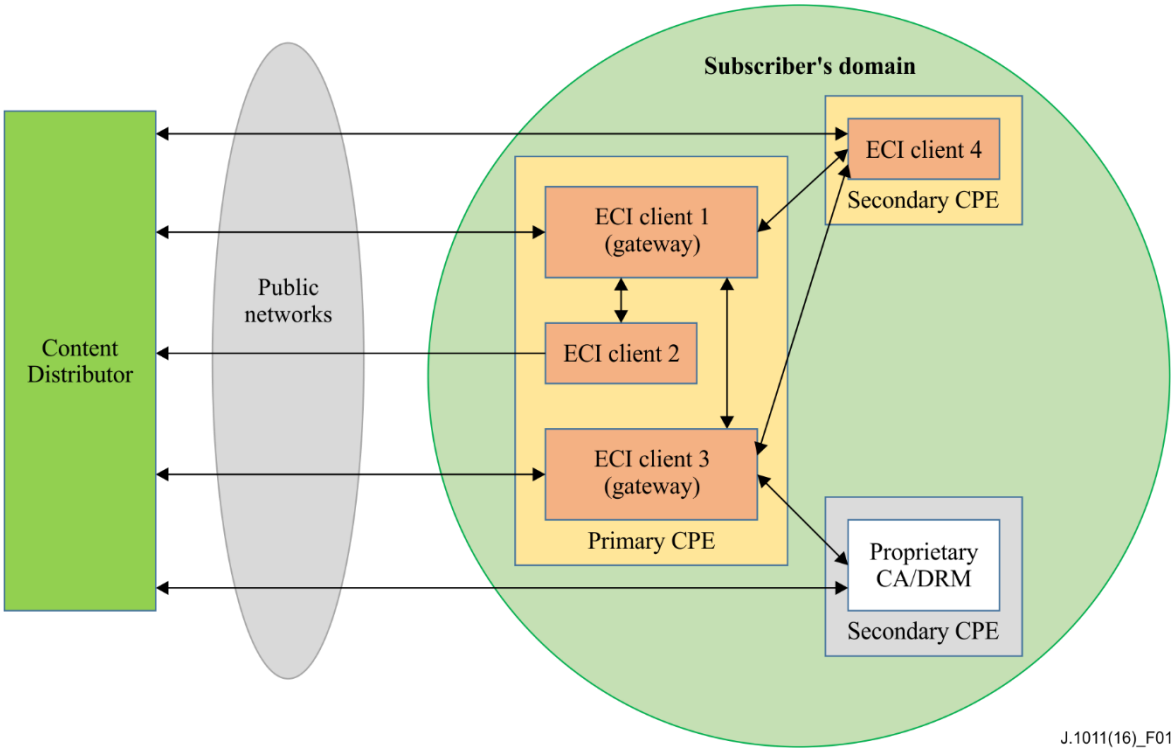


Figure 1 – The ECI clients within a single customer's domain

The ECI specifications define, amongst others, the interface between an ECI container and the ECI host. Figure 2 shows a block diagram of a CPE with ECI containers and the other functions in the ECI host that the ECI containers communicate with or may communicate with. Some of these functions are optional. During the installation of an ECI client and during launch of an ECI client, the host specifies which relevant functions it has available to the ECI client.

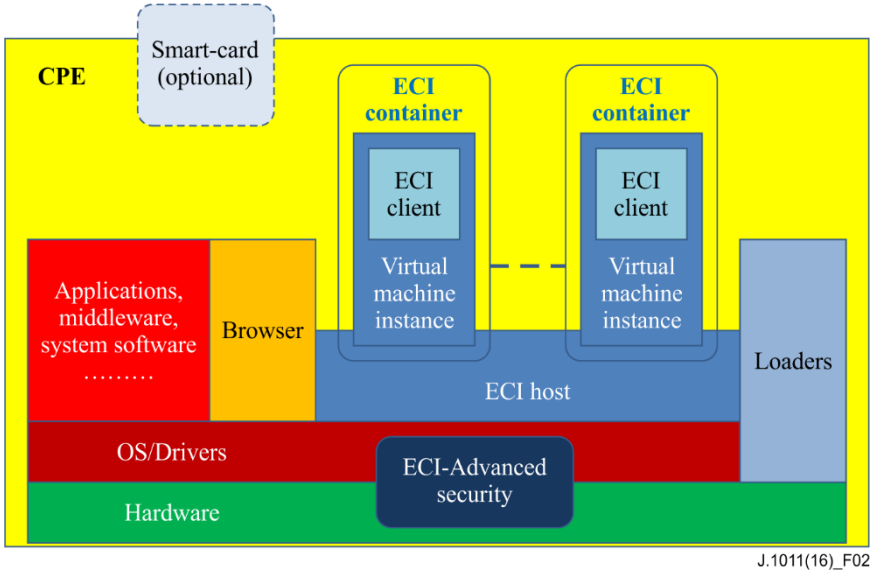


Figure 2 – Block diagram of a CPE with embedded ECI clients, each with their own ECI container and virtual machine instance

First of all the concept is based on a hierarchical loader concept (see Figure 3) consisting of a chip-based loader, the system software loader and the ECI client loader.

The ECI host loader loads the ECI host software. This includes besides other elements the virtual machine, access to advanced security components and the ECI client loader. An ECI host can load multiple ECI clients into separate virtual machine instances, which run independently and are isolated from each other.

When loading an ECI client into the system a virtual machine instance is being created in which the ECI client is loaded. This VM instance acts as a sandbox between the ECI client and the host. The interface between the ECI client and the VM instance is the key interface which the Group Specification (GS) is specifying. The interface specifies in addition the information flow/protocol between multiple instances of such an ECI client and to other functionality inside the CPE, like advanced security, display, etc. Note that the other ECI client needs not necessarily to be in the same ECI host. This interface and communication protocol is specified in [b-ETSI GS ECI 001-3].

The ECI host itself depends on the manufacturer implementation. It interfaces to the OS and the driver layer and provides all functionalities defined by the ECI client interface specification. The ECI-host is not specified by ECI, but it needs to be certified by the TA in order to ensure compliance with the ECI client interface specification.

6.2.3 Mandatory functionality of ECI compliant devices

ECI addresses a range of usage scenarios (see Figure 1). Hence, ECI has to deal with a broad range of devices such as iDTVs, STBs, personal video recorders (PVRs), IPTV, tablets, smartphones, etc. These devices vary in their capabilities while ECI provides a harmonized security framework. ECI distinguishes TV-centric devices from devices for other environments, including but not limited to IPTV and tablets.

TV-centric devices are defined as devices which include MPEG-2 transport stream processing inside the chip-set. ECI requires that those chip-sets implement ECI-compliant advanced security functionalities. TV-centric ECI compliant CPEs shall be compliant with the functions as given in the specifications [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] and [b-ETSI GS ECI 001-5].

Devices for other environments especially IPTV, computers and tablets typically implement more functionality in software and connect to a bidirectional IP-communication. This enables different types of security mechanisms. As chip-sets used in these devices include hardware for various security processing functions, ECI requires dedicated hardware-assisted security and robustness functionalities to be implemented in the chip-sets. [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] and [b-ETSI GS ECI 001-5] specify the necessary mechanisms to leverage those functionalities.

6.2.4 Necessary interfaces between ECI host and ECI client

The ECI container is a technical concept combining the VM and the ECI client with the objective to isolate and to shield the VM and the ECI client from the rest of the CPE. The virtual machine is a functionality of the ECI host. By loading an ECI client the ECI host creates a virtual machine instance. The virtual machine provides the necessary interfaces to the ECI client and connects them to the ECI host. The ECI specification defines the interface between the VM and the ECI client, see also Figure 2 for a high level architecture on an ECI compliant device. The interface provides certain application programming interfaces (APIs) and also establishes a secure communication channel.

The following list highlights important software interfaces:

– Interface for capability information to ECI client from ECI host and vice versa
– Interface to the processing of input and outputs signals of the CPE
– Interface to the advanced security hardware/drivers block
– Interface to loader functionalities
– Interface to support user interaction

– Interface to encryption and decryption functionality
– Interface to the optional smartcard reader
– Interface to specific security functionalities like fingerprinting and watermarking
– Interface to local storage

All interfaces of the ECI client are provided by means of the virtual machine.

There are in addition communication protocols on top of the interfaces allowing a secure communication. In particular a protocol to established communication between ECI clients, regardless if internal or external, is being specified.

The CPE can be connected to any type of network and several networks concurrently, both unidirectional or bidirectional. It does not always need to be connected to any network (downloaded/stored content).

6.2.5 A minimum user interface and display functionality

For communications with the user, a minimum user interface (UI) and on screen display (OSD) facility shall be available to the ECI containers. This is specified in [b-ETSI GS ECI 001-3]. It is used to display messages for the user that have been generated by or sent using the CA/DRM system. Also, it is used to allow the user entering inputs, such as a personal identification number (PIN). Details are specified in [b-ETSI GS ECI 001-3] as well.

The user interacts locally with the CA/DRM system through the ECI client.

6.2.6 The virtual machine

The ECI client runs upon a standardized virtual machine (VM). This component is specified in [b-ETSI GS ECI 001-4]. Each installed ECI client shall have its own instance of the VM. The VM instance provides a secured environment for executing conditional access kernel or digital rights management client applications. APIs are provided by the VM, where resources of the ECI host environment can be accessed in a standardized way.

6.2.7 The advanced security facility

ECI defines minimum necessary security functionalities required to build a secure content protection system. ECI requires enhancements based on hardware-elements. In TV-centric devices this is delivered by TV-specific dedicated advanced security functions. It specifies what is usually referred to as a "key ladder block" in systems on chip (SoCs). An essential task of the advanced security facility is to protect the content protection keys during its transmission from the ECI client to the content decryption facility in a CPE or the transfer of protected content from one ECI client to another ECI client (see Figure 1). The advanced security system as specified in [b-ETSI GS ECI 001-5] supports different simultaneous control word streams and different ECI clients that are simultaneously requesting its services. Furthermore the advanced security facility plays a key role to verify the download of the software for the host and the ECI clients.

Devices for other environments especially IPTV, computers and tablets typically implement more functionality in software and connect to a bidirectional IP-communication. ECI specifies the same advanced security concepts and mechanisms but will map them differently on the devices security architectures [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] and [b-ETSI GS ECI 001-5].

The availability of advanced security in the CPE is communicated to the ECI client during its installation and during its launch.

6.2.8 Re-scrambling

Protected content, which is been received by an ECI compliant CPE may not be consumed immediately. The following functionalities are available with ECI compliant devices:

– Local storage:
  - under control of the CPE
  - under control of a CA- or DRM client
– Gateway:
  - delivery of a protected content element to an external device under control of a DRM client
  - delivery of a protected content element to another ECI client either inside the same CPE or running on another ECI compliant CPE.

To support these functionalities the ECI compliant device is able to re-scramble content. The ECI system does not specify the transport mechanisms nor the available DRM functionalities for storage or delivery of protected content to other devices. In [b-ETSI GS ECI 001-5], the necessary interfaces between the ECI host and the ECI client are defined.

6.2.9 The ECI loader functionalities

An ECI compliant CPE shall provide loader functionalities, allowing loading and installation, as well as integrity and anti-substitution protection of the relevant software modules of the ECI system.

Initially, the loader integrated into the chip loads the system software loader. This embedded loader is to ensure that only a certified system software loader can be installed and launched. The system software loader includes the ECI host loader and thus the system software loader needs to be signed by the trust authority. The system software loader may include loaders for other system software which is not relevant for ECI functionalities and has no relationship to the security related elements of the system. The ECI host software includes the ECI client loader, which then upon request can load the ECI client.

During its installation in its ECI container as well as during its launch, the ECI client is informed by the ECI host about its facilities, such as recording facilities, HD facilities, a smart card reader, fingerprinting and watermarking facilities and networks, as well as compliance with the framework specification (this Recommendation) and [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] and [b-ETSI GS ECI 001-5] and possibly [b-ETSI GS ECI 001-6].

The ECI loader with the related security facilities is specified in [b-ETSI GS ECI 001-3].

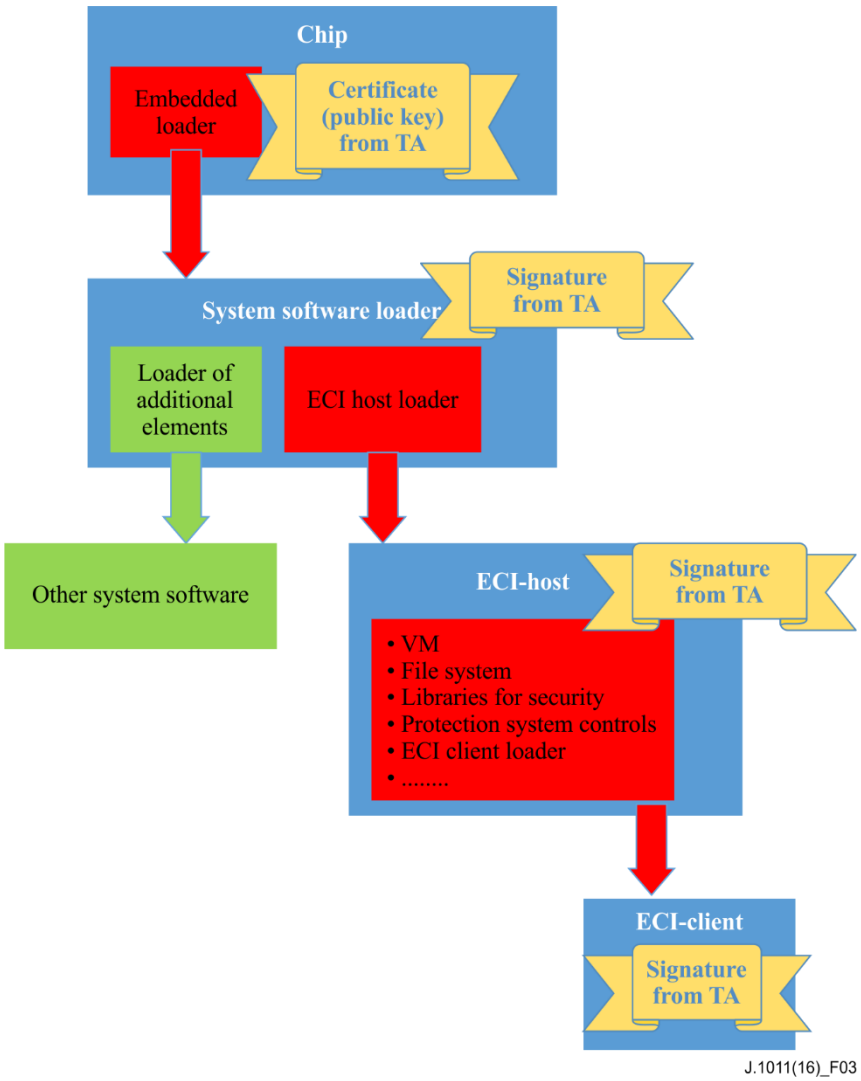


Figure 3 – Hierarchical loader concept

6.2.10 Revocation

The trust authority may decide to put a CPE, a range of CPEs, a type of CPEs or all CPEs from a specific manufacturer on a black list. The content provider or operator may revoke these concerned CPE or CPEs from their service distribution point. The methods used allow other operators and content distributors to continue their services to these CPEs if they wish to do so.

Revocation can block all services from the operator or content provider to the CPE(s) concerned, or to a subset of services. This is subject to the functionality of the relevant CA or DRM system and out of the scope of the present Recommendation.

The revocation process is specified in [b-ETSI GS ECI 001-3].

7 Trust environment

In order to be able to establish a system based on embedded CI, a trust environment has to be set up. Details about the trust environment are out of scope of the ECI specifications. However, the principles, which are specified in [b-ETSI GS ECI 001-6], are essential in order to fully understand how ECI works.

The trust authority (TA) is an organization governing all rules and regulations that apply to implementations of the ECI architecture**.** 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. This includes:

– CPE manufacturers
– CA/DRM (ECI client) manufacturers
– Chipset manufacturers, whose components include unchangeable secure processor keys and certificates, which are necessary for interaction between host and the compliant CA/DRM system
– Platform operators; the platform operator is the party that controls all necessary elements of a CA/DRM system. Platform operators are for example service providers or network operators
– Application providers, if applicable

A trusted third party (TTP) is a technical service provider, which issues certificates and keys to compliant manufacturers of the relevant components of an ECI system. The trust of these keys and certificates is assured by the TA, which holds the root of trust.

Trust authority and trusted third party form the basis for the chain of trust and thus have to be involved in the entire processes ranging from production (chips and CPEs), over operations (secure ECI client download and activation) to control measures (e.g., revocation).

The trust authority as a legal entity ensures the functioning of the trust environment via a contractual framework also called license agreement, under which the various parties involved can assume their responsibilities and liabilities. Under the license agreement trust authority/trusted third party are generating and issuing key pairs, certificates, test credentials and operator IDs, etc.

One TA establishes trust between all market participants. A second TA cannot exist to establish trust "a second time" for the same environment. However, there could be multiple TAs, e.g., per country or per region, segments, eco-systems.

If multiple TAs exist in parallel there is a need that TA A and TA B trust each other as a prerequisite that devices registered in TA A can be used in the domain of TA B.

7.1 Necessary operational workflows

This clause gives a first overview of the necessary operational workflows, which serve the needs of the different market participants in order to implement a business based on the ECI technology. Furthermore the indicated workflows are based on the essential technical elements which are necessary for implementation of an ECI system. Figure 4 shows these interactions between technical components and the relevant market participants.

Remark: The description is generic and is not intended to reflect any existing proprietary solution or any actual running standardization activity.

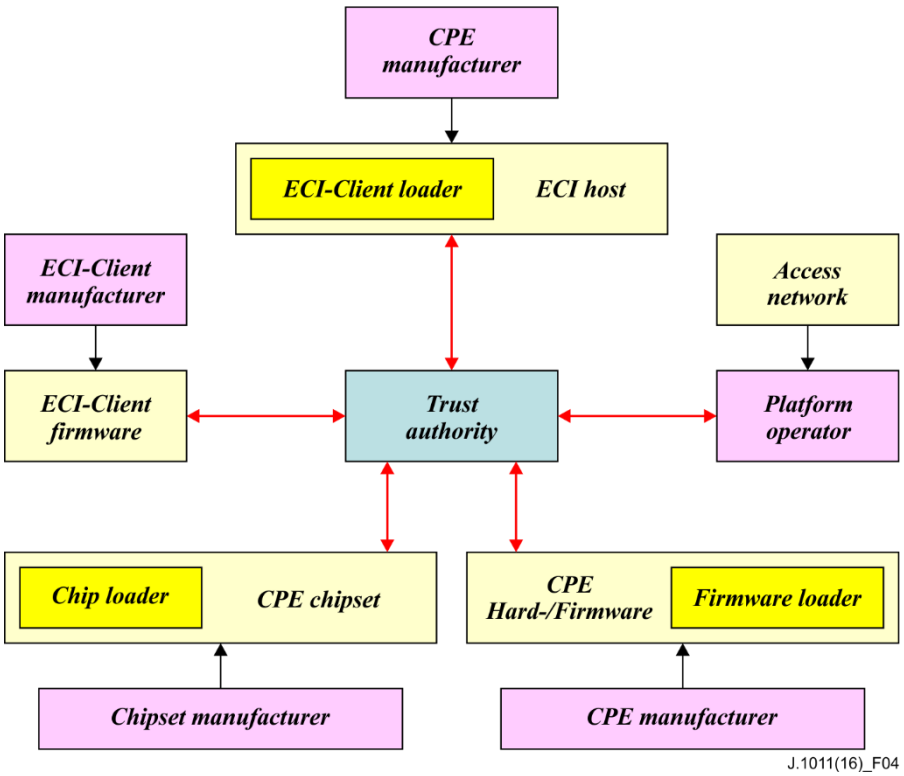


Figure 4 – Necessary trust management between trust authority (TA) and the relevant market participants

The operational and related contractual issues (see red arrows in Figure 4) for the trust environment are:

1) Integrity

Integrity means the requirement that one market participant is able to verify whether a hardware/software component provided by another market participant has not been modified by any unauthorized party and is fulfilling the specifications and robustness rules. This requirement can be fulfilled by suitable credentials and signatures and testing procedures based on test credentials provided by the trust authority/trusted third party.

2) Authenticity

Authenticity means that any hardware/software component which originates from a TA contract partner of the trust authority and which has passed the necessary verification and certification steps can clearly be associated with the contract partner and thereby distinguished from any cloned component. Authenticity of any relevant hardware/software component is proven by any ECI system.

3) Contractual Framework

The contractual framework established by the trust authority as a legal entity shall encompass a compliance and robustness regime and certification procedures in order to provide the environment for the establishment of ECI systems.

4) Remedies

In the case where hardware/software components of an ECI system are no longer compliant, the trust authority establishes procedures for the provider of that component, targeting to re-establish the integrity of the eco-system in a reasonable timeframe.

Essential technical components (yellow boxes in Figure 4) are:

1) CPE chipset

   The CPE chipset is the main component within CPE hardware which usually includes "system on chip" (SoC) due to existing requirements of platform operators and content providers. Furthermore usually the chip loader is included in the CPE chip.

2) CPE hardware

   The secure CPE chipset implementation, prevention of any unauthorized access to storage elements (Flash, ROM) and protection of interfaces are essential issues.

3) Different loaders

   The chip loader downloads different additional loaders, depending on the hardware/software configuration of the CPE.

4) CPE firmware

   The CPE firmware has manifold interactions with the ECI client and all relevant CPE hardware interfaces. Security is ensured by detailed specifications and appropriate compliance and robustness rules.

5) ECI client

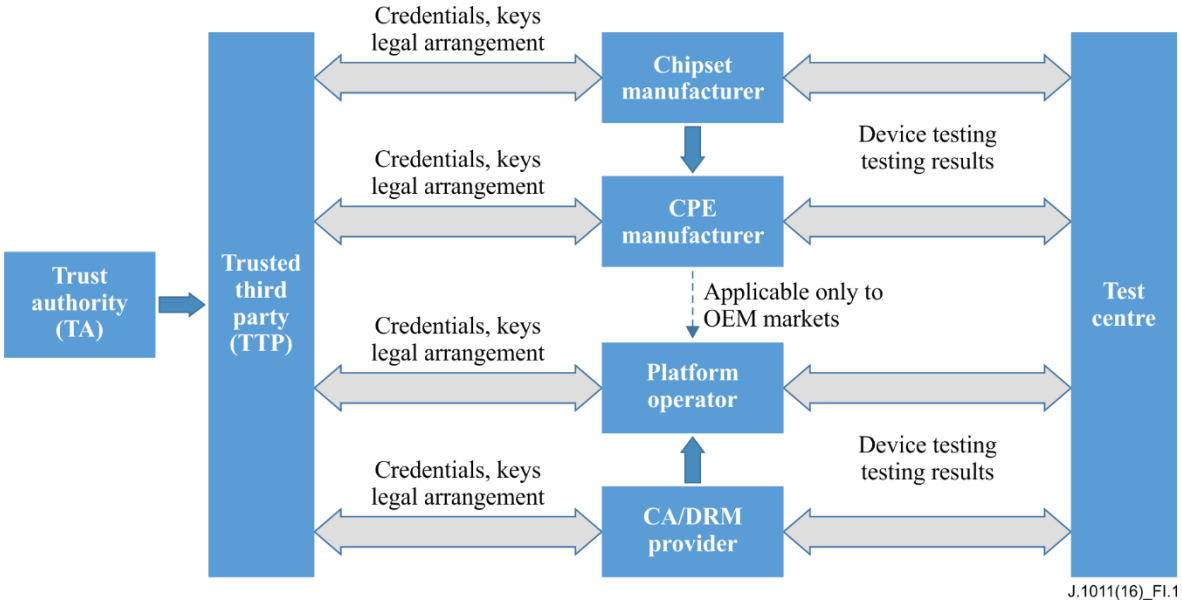
   The ECI client extracts all CA and DRM related information delivered by the frontends of the CPE and initiates the corresponding settings within the CPE device (descrambler, interfaces), which obviously needs close and secure interaction with the CPE firmware.

Appendix I

Implementation of an ECI-compliant trust system

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

Appendix I gives a first overview of the necessary operational workflows, which serve the needs of the different market participants in order to implement a business based on the ECI technology. Figure I.1 shows an overview of the general workflow. Furthermore the indicated workflows are based on the essential technical elements which are necessary for implementation of an ECI system. Figure 4 in clause 7.1 shows the interactions between technical components and the relevant market participants.



NOTE – Trusted third party (TTP) and test centre are contract partners of the trust authority (TA) for certification and key issuing process.

Figure I.1 – General workflow overview

Legal/Contractual framework

Secure trust management can only be carried out under a clearly defined legal and contractual framework, in which the license agreement (LA) constitutes the core element. The TA provides license agreements to anyone seeking to implement the specification(s), be they CPE manufacturers, CA/DRM system vendors, chip manufacturers, other technology providers, platform operators, etc.

Therefore the license agreement is the essential instrument for the TA to create, maintain and make available to the horizontal market a secure but user friendly method to receive and make operative all required keys and other relevant security related material and information when connecting CPEs to providers of choice, that conform to the relevant usage rules. Similarly, the license agreement framework enables the TA to take proper care of revocation of all security material when a consumer is disconnected by the provider, as far as is technically and economically possible.

The license agreement enables the coordinated and consistent application of the other elements of the contractual framework such as the technical specification, compliance and robustness rules, obligations and liabilities, testing and certification, implementation guidelines, etc.

Figure I.2 shows components of the license agreement.

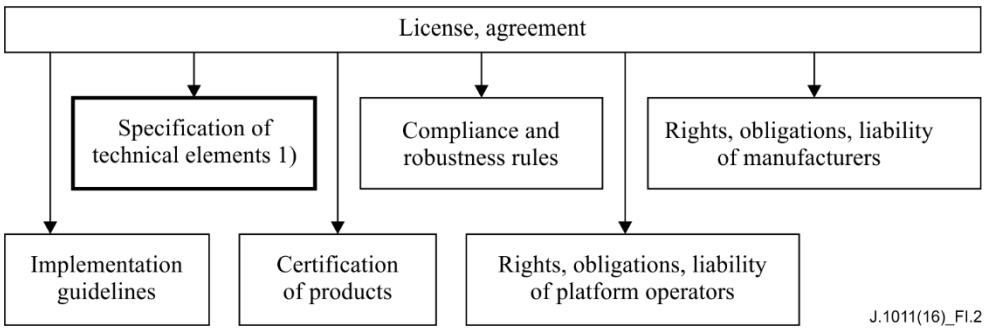


Figure I.2 – Components of the license agreement

These specifications will be developed in the ETSI ISG ECI as Group Specifications.

Bibliography

[b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006) | ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.

[b-CENELEC EN 50221] CENELEC EN 50221 (1997), *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications.*

[b-CI Plus Specification] CI Plus Specification (V1.3.1) (2011), *Content Security Extensions to the Common Interface*.

[b-ETSI EN 300 468] ETSI EN 300 468 V1.13.1 (2012), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*.

[b-ETSI ISG ECI] ETSI ISG ECI White Paper (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*. www.etsi.org/deliver/etsi.../ECI/.../gs_ECI00101v010101p.pdf

[b-ETSI TS 101 699] ETSI TS 101 699 V1.1.1 (1999), *Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification*. http://webstore.ansi.org/RecordDetail.aspx?sku=ETSI+TS+101+699-v1.1.1-1999-11

[b-ETSI TS 103 162] ETSI TS 103 162 V1.1.1 (2010), *Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification*.

[b-ETSI TS 103 205] ETSI TS 103 205 V1.1.1 (2014), *Digital Video Broadcasting (DVB); Extensions to the CI PlusTM Specification*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017