ETSI GS ECI 001-1 V1.1.1 (2014-09)

Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 1: Architecture, Definitions and Overview

Disclaimer

This document has been produced and approved by the Embedded Common Interface (ECI) for exchangeable CA/DRM solutions ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/ECI-001-1

Keywords
CA, DRM, swapping

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Embedded Common Interface (ECI) for exchangeable CA/DRM solutions.

The present document is part 1 of a multi-part deliverable covering the Architecture, Definitions and Overview for the Embedded Common Interface for exchangeable CA/DRM solutions specification, as identified below:

Part 1: "Architecture, Definitions and Overview";

Part 2: "Use cases and requirements";

Part 3: "CA/DRM Container, Loader, Interfaces, Revocation";

Part 4: "The Virtual Machine";

Part 5: "The Advanced Security System";

Part 6: "Trust Environment";

Part 7: "Extended Requirements".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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, IPTV or new OTT (over-the-top) 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.

1 Scope

ECI Architecture, Definitions and Overview, as covered by this framework document, 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 solution 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 easier, allowing the end-user to change operator 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 (the present document), in combination with the underlying specifications:

Part 1: Architecture, Definitions and Overview (the present document)

Part 2: Use cases and requirements [1]

Part 3: CA/DRM Container, Loader, Interfaces, Revocation [i.1]

Part 4: The Virtual Machine (VM) [i.2]

Part 5: The Advanced Security System [i.3]

Part 6: Trust Environment [i.4]

Part 7: Extended Requirements [i.5]

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 GS ECI 001-3 [i.1], 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 GS ECI 001-4 [i.2].

GS ECI 001-5 [i.3] specifies an Advanced Security mechanism to protect the key to the content during its travel into the CPE processor chip's content decryption facility.

The present document 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 the present document.

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, GS ECI 001-6 [i.4].

NOTE: Contractual framework (license agreement), compliance and robustness rules, and appropriate certification process are not subject to the standardization work in ISG ECI.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

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

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

NOTE: The following references are intended to become normative references once these Group Specifications are completed.

[i.1] ETSI GS ECI 001-3: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 3: CA/DRM Container, Loader, Interfaces, Revocation".

[i.2] ETSI GS ECI 001-4: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 4: The Virtual Machine".

[i.3] ETSI GS ECI 001-5: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 5: The Advanced Security System".

[i.4] ETSI GS ECI 001-6: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 6: Trust Environment".

[i.5] ETSI GS ECI 001-7: "Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 7: Extended Requirements".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Advanced Security: function of an ECI compliant CPE which provides enhanced security functions (hardware and software) for an **ECI Client**

NOTE: The details are specified in [i.3].

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

ECI Client (Embedded CI Client): implementation of a CA/DRM client which is compliant with the Embedded CI specifications

NOTE: 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.

ECI Client Loader: software module part of the ECI host which allows to download, verify and install new ECI client software in an ECI container of the ECI host

ECI Container (Embedded CI Container): abstract concept which provides an isolated environment comprised of a virtual machine and a single ECI client

ECI Host: hardware and software system of a CPE, which covers **ECI** related functionalities and has interfaces to an **ECI Client**

NOTE: The **ECI Host** is one part of the CPE firmware. The ECI host is responsible to ensure the isolation of each ECI container and provides authenticated loading of ECI clients.

ECI Host Loader: software module which allows to download, verify and install (new) ECI Host software into a CPE

NOTE: In a multi-stage loading configuration this term is used to refer to all security critical loading functions involved in loading the ECI host.

Trust Authority (TA): organization governing all rules and regulations that apply to implementations of **ECI**

NOTE: 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.

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)**

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

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 receiver
IP	Internet Protocol
IPTV	TV services delivered via IP protocol
ISO	International Standards Organization
LA	License Agreement
MPEG	Motion Picture Experts Group
OS	Operating System
OSD	On Screen Display
OTT	Over The Top
PIN	Personal Identification Number
ROM	Read Only Memory
SI	Service Information
TA	Trust Authority
TTP	Trusted Third Party
TV	Television
UI	User Interface
VM	Virtual Machine

4 The technical concept of the **ECI** System

4.1 Basic considerations

The present document, in combination with Parts 2 to 5 and 7 of the specifications ([1], [i.1], [i.2], [i.3] and [i.5]), 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 as many **ECI Clients** as its resources can handle, at least two. 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 the present document and specified in [1], [i.1], [i.2] and [i.3], 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 [i.1].

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 [i.2]. The **ECI Container** is specified for CA/DRM functionality only, which is reflected in [i.1]. The interface with the CPE, detailed in [i.1], 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. GS ECI 001-5 [i.3] 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 [i.1] 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 [i.3].

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.

4.2 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**. [i.1] 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 [i.3]. The specific protocols and implementations of proprietary clients are out of scope of the ECI specifications.

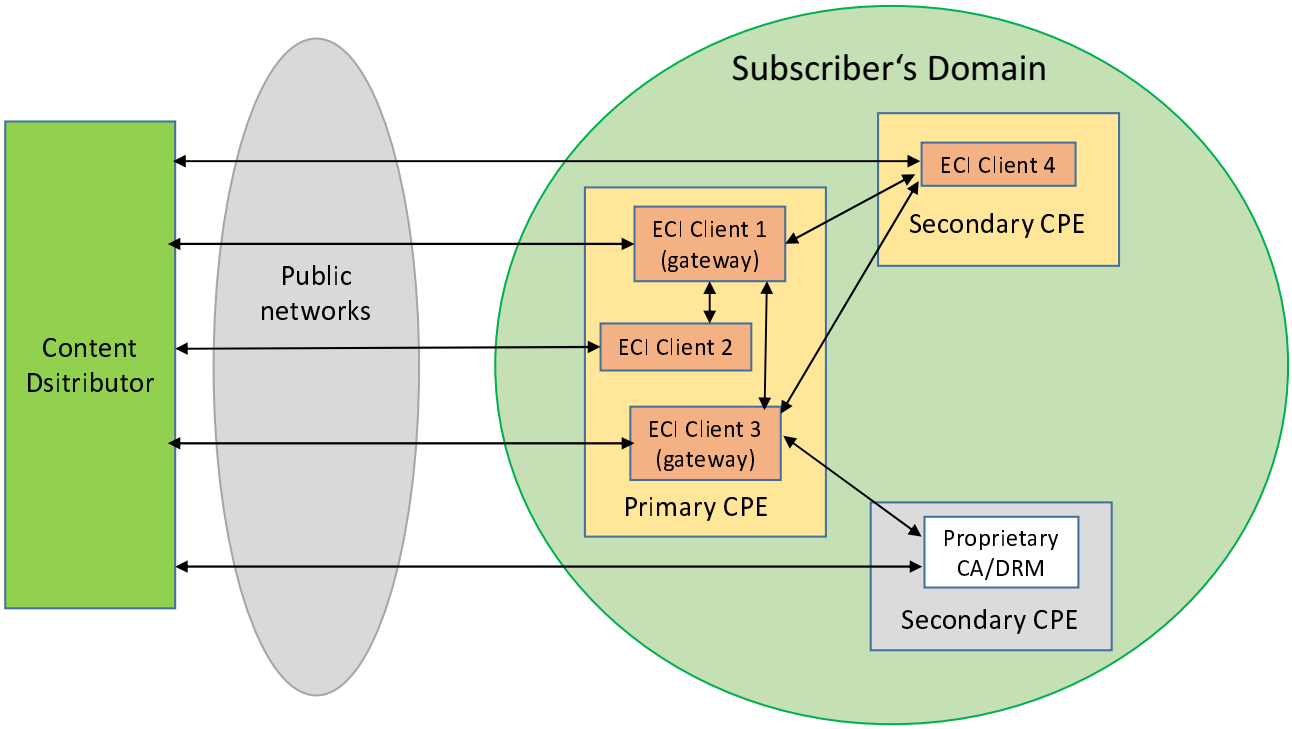


Figure 1: The ECI Clients within a single customer's domain

The ECI specifications define, amongst others, the interface between an **ECI container** and the **ECI Host.** Figure 2 shows the 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**.

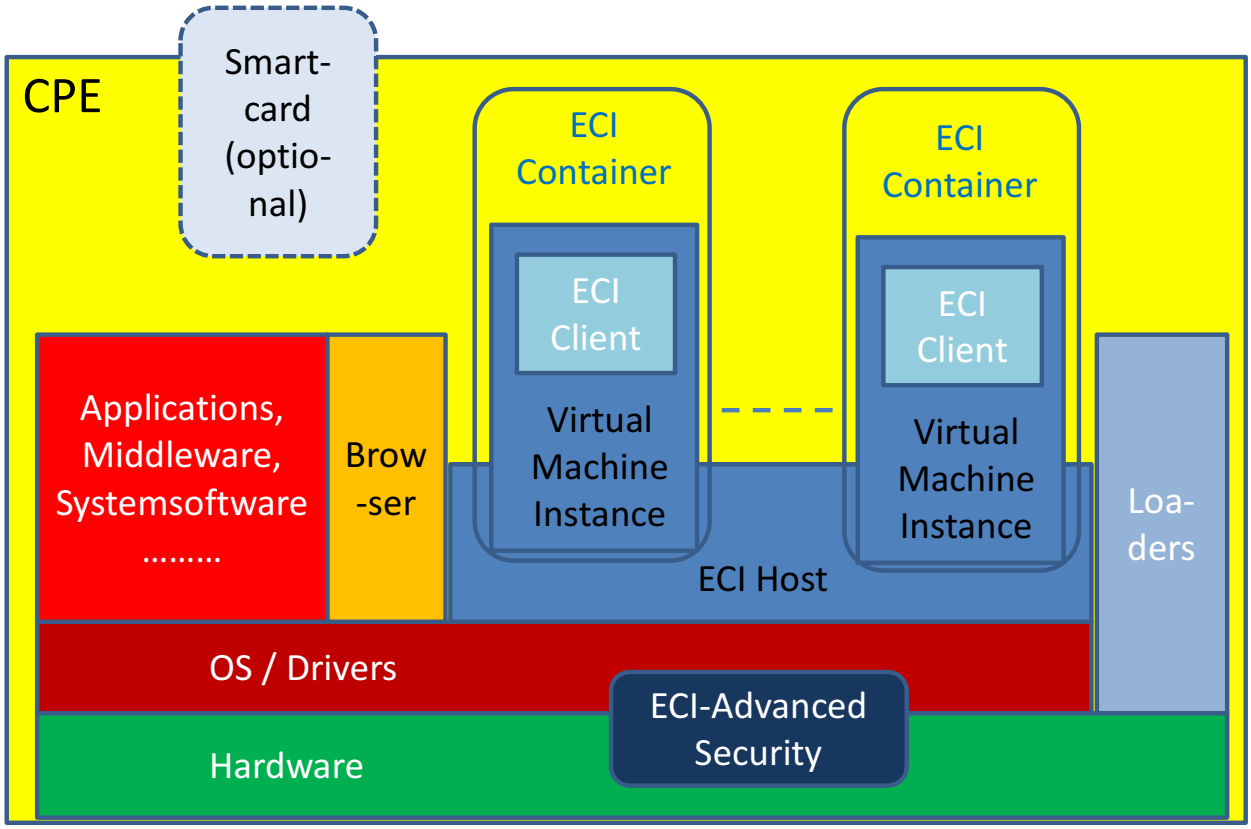


Figure 2: Block diagram of a CPE with embedded ECI Clients, each with their own ECI Container and Virtual Machine instance

First of all the concept is based on a hierarchical loader concept 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 isolated against 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 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 [i.1].

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.

4.3 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 ranging from iDTVs, STBs, PVRs, IPTV, tablets, smartphones, etc. Those 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 [i.1], [i.2] and [i.3].

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 those devices include hardware for various security processing functions, ECI requires dedicated hardware-assisted security and robustness functionalities to be implemented in the chip-sets. [i.1], [i.2] and [i.3] specify the necessary mechanisms to leverage those functionalities.

4.4 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 APIs and establishes also 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).

4.5 A minimum User Interface and Display functionality

For communications with the user, a minimum UI and OSD facility shall be available to the **ECI containers**. This is specified in [i.1]. 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 PIN. Details are specified in [i.1] as well.

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

4.6 The Virtual Machine

The **ECI Client** runs upon a standardized **Virtual Machine (VM**). This component is specified in [i.2]. 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.

4.7 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 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 [i.3] supports different simultaneous Control Word streams and different **ECI Clients** that are simultaneously requesting its services. Furthermore the **Advanced Security** facility plays a key roll 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 [i.1], [i.2] and [i.3].

The availability of **Advanced Security** in the CPE is communicated to the **ECI Client** during its installation and during its launch.

4.8 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 GS ECI 001-5 [i.3] the necessary interfaces between the ECI host and the ECI client are defined.

4.9 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 (the present document) and [i.1], [i.2], [i.3] and possibly [i.4].

The **ECI Loader** with the related security facilities is specified in [i.1].

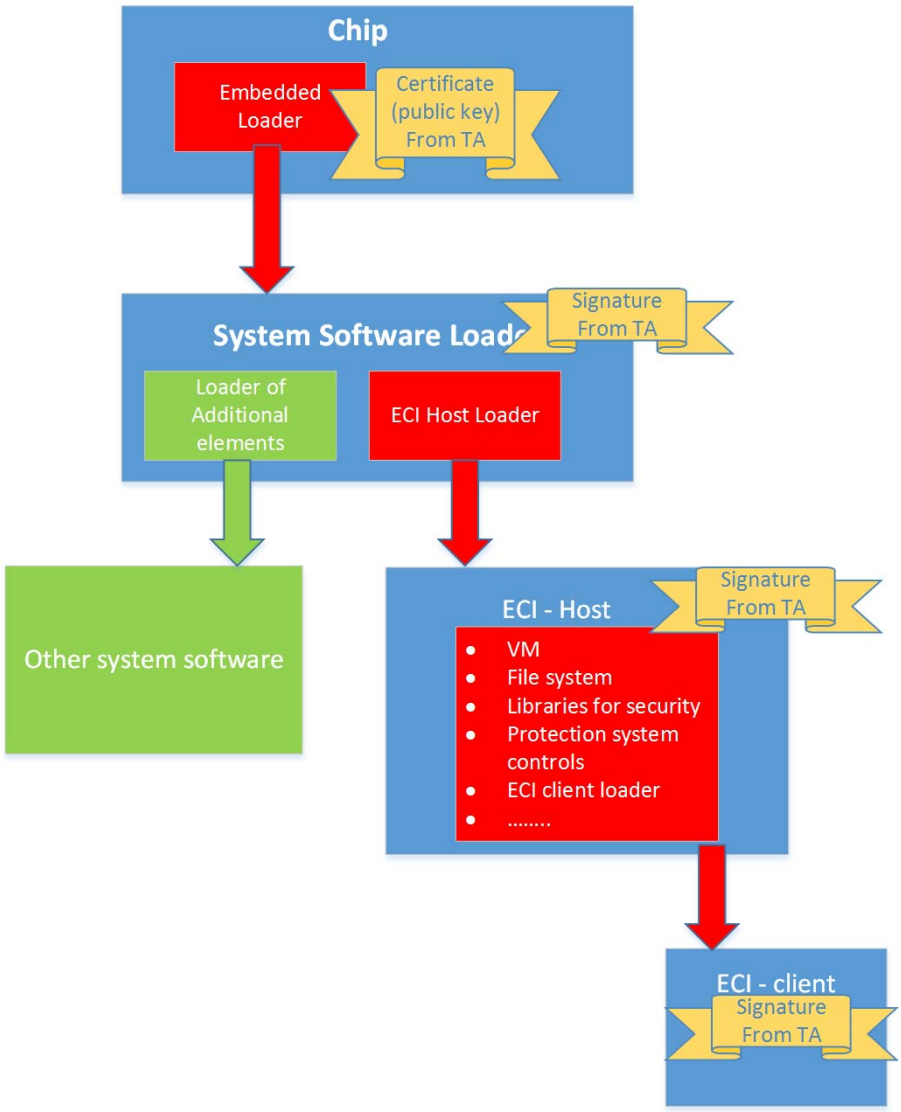


Figure 3: Hierarchical Loader Concept

4.10 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 of the functionality of the relevant CA or DRM system and out of the scope of the present document.

The revocation process is specified in [i.1].

5 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 GS ECI 001-6 [i.4], are essential in order to fully understand how **ECI** works.

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 who 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 exists 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.

5.1 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 those interactions between those 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.

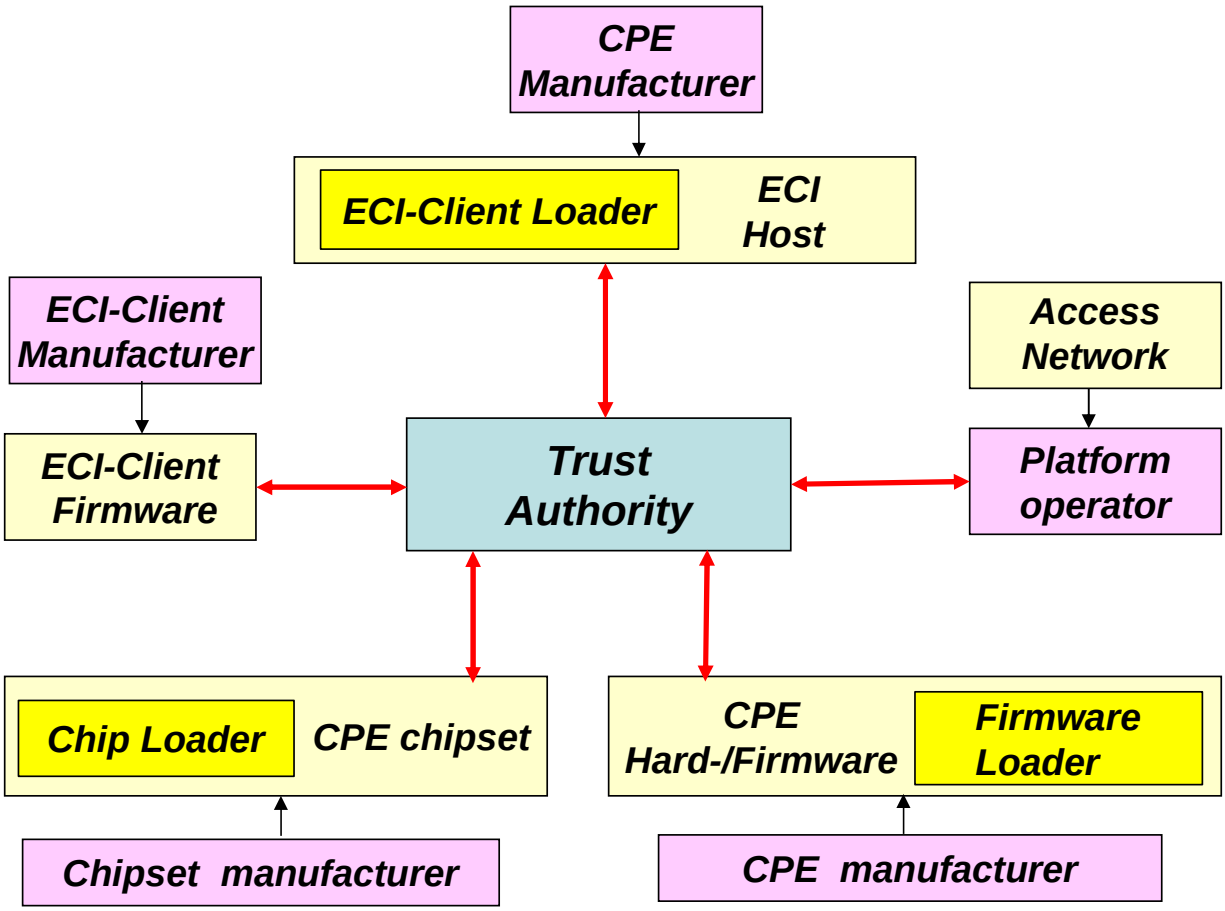


Figure 4: Necessary Trust Management between Trust Authority (TA) and the relevant market participants

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 compliance and robustness regime and certification procedures in order to provide the environment for the establishment of ECI systems.

4) Remedies

In case 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 has included SoC ("System on Chip") 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

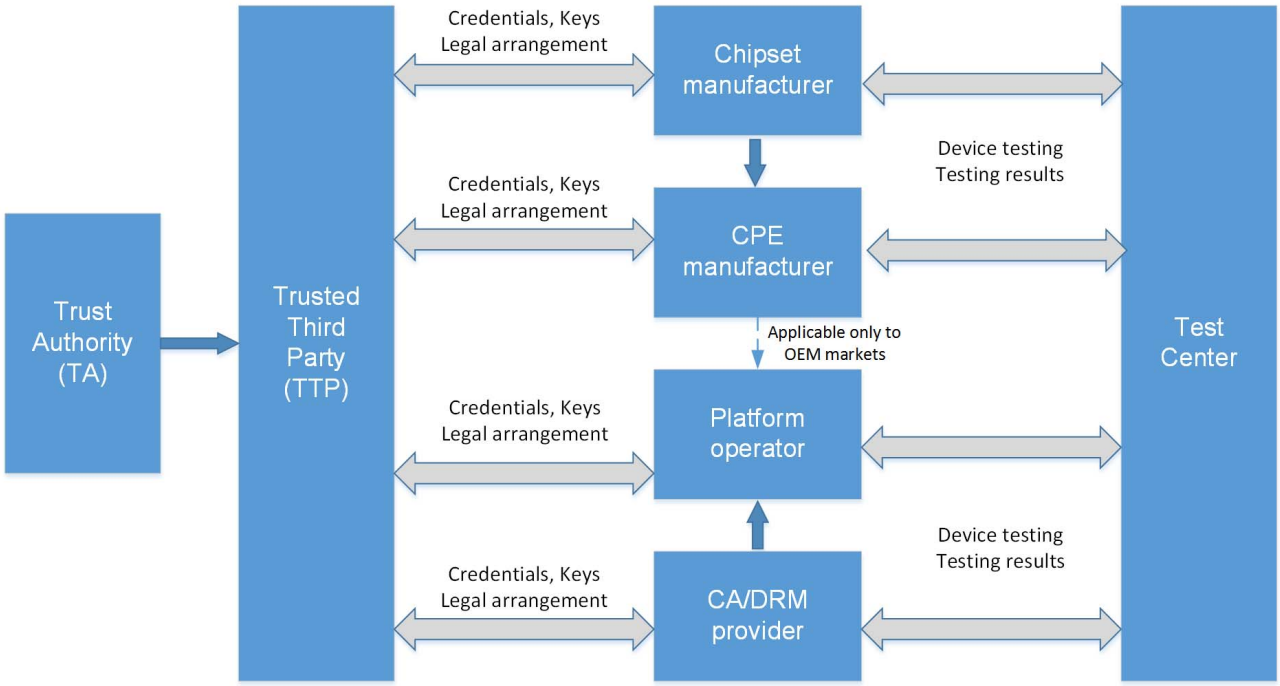
The CPE firmware has manifold interactions with the ECI Client and all relevant CPE hardware interfaces. Security is ensured by detailed specifications and appropriate compliance and robustness rules.

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.

Annex A (informative): Implementation of a ECI-compliant Trust System

This informative annex A 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 in clause 5.1 shows those interactions between those technical components and the relevant market participants.



NOTE: Trusted Third Party (TTP) and Test Center are contract partners of the Trust Authority (TA) for certification and key issuing process.

Figure A.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 get operative all required keys and other relevant security related material and information when connecting CPEs to providers of choice, as far as allowed conform 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 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 & liabilities, testing & certification, implementation guidelines, etc.

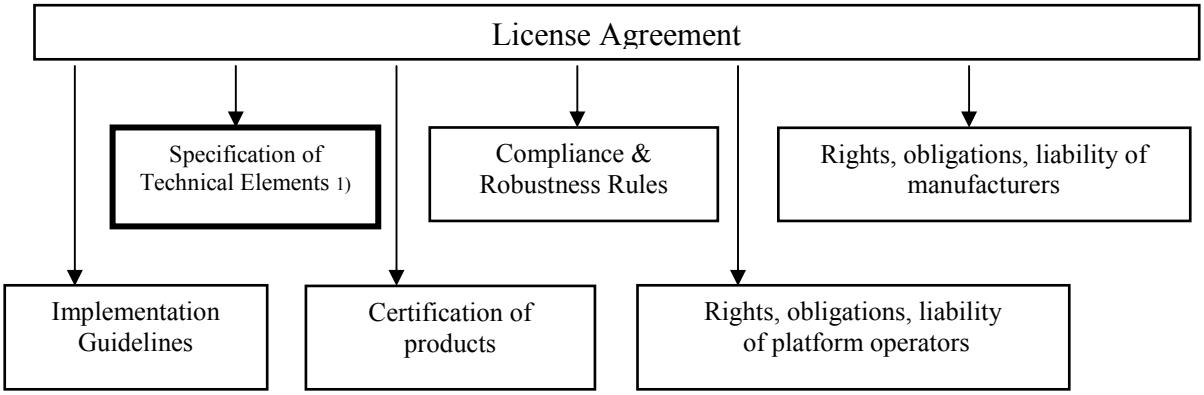


Figure A.2: Components of License Agreement

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

Annex B (informative): Bibliography

ETSI ISG ECI: "Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions, White paper".

CENELEC EN 50221 (1997-02): "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications".

ETSI TS 101 699 (V1.1.1) (1999-11): "Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification".

CI Plus Specification (V1.3.1) (2011-09): "Content Security Extensions to the Common Interface".

NOTE: Available from http://www.CI Plus.com/data/CI Plus_specification_V1.3.1.pdf.

Recommendation ITU-T H.222.0 (2006)/ISO/IEC 13818-1:2007: "Information technology -- Generic coding of moving pictures and associated audio information: Systems".

ETSI EN 300 468 (V1.13.1) (2012-08): "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

ETSI TS 103 205: "Digital Video Broadcasting (DVB); Extensions to the CI Plus™ Specification".

NOTE: Available from http://www.dvb.org.

ETSI TS 103 162 (V1.1.1) (2010-10): "Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification".

ISO 7816: "Information Technology Identification Card Integrated Circuit Cards with contacts".

History

Document history		
V1.1.1	September 2014	Publication