Founding Members of ETSI ISG ECI

ISG ECI: Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions

White Paper

Authors

Bundesministerium für Wirtschaft und Energie (BMWi):	Peter Mann[1]
Deutsche Telekom AG:	Jens Johann[1]
Institut für Rundfunktechnik:	Klaus Illgner[1]
Irdeto BV:	Michiel Willemsen[1]
Kabel Deutschland Vertrieb und Service GmbH:	Christoph Schaaf[2]
KATHREIN-Werke KG:	Georg Schell[1]
Van Baar Beheer BV:	Theo van Aalst[2]

A) 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. 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 (e.g. CI Plus) 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.

All 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

[1] Founding Member

[2] Participant

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.

Some market participants argue that security and standardization is a contradiction in itself. However, it is in consumers' interest that they are able to continue using the CPEs they bought, including the content procured, 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 appropriate security architecture. Further fragmentation of the market for CPEs can only be prevented and competition encouraged by ensuring the exchangeability of CA and DRM systems.

B) Overcoming Market Fragmentation by a Standardization Effort of Committed Partners

The founding members concluded that a standardized system architecture for **general purpose, software-based, embedded,** and **exchangeable CA/DRM systems** 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
- Opening of the market by avoiding “Lock-in” for platform operators, network/service providers, and consumers
- An open entire eco-system fostering market development.

The founding members are convinced that there is a window of opportunity. They have agreed to go for a standardization initiative and to launch an ISG with committed partners in order to develop specifications within 2 years.

C) Market Needs and Use Cases

Any successful standardization has to address existing market needs. It should be based on practical use cases and follow requirements of end-users and of the market players.

Basic Use Cases

In the digital TV business environment, different reasons might occur that require exchanging the CA/DRM system in CPE equipment. The following use cases are applicable to broadcast and as well as to broadband, and hybrid scenarios.

- A digital media content provider may decide to change the CA/DRM system of its CPEs for its customers. Reasons may be
    - Different technical or commercial reasons, such as requirements of enhanced CA/DRM functionalities, higher security levels or higher system performance or in case of a deep hack of the current system
    - Acquisition of new customers in a certain network, which used to access services of a competitor

- A digital media content provider may decide to deliver services to a broad range of retail devices which, based on today's business understanding, may be equipped with different CA/DRM solutions.
- A platform operator may decide to change the CA/DRM system of the CPEs in its platform. Reasons may be
    - Different technical or commercial reasons, such as requirements of enhanced CA/DRM functionalities, higher security levels or higher system performance or in case of a deep hack of the current system
    - Harmonisation of technologies after acquisition of a network
- A CA/DRM vendor acquires a new customer who operates a platform, where a competitor had already established its CA/DRM system, or a CA/DRM vendor takes over another CA/DRM vendor and wants to harmonize the security technologies.
- An end-user has bought a CPE in any shop and connects it to the network of access network provider A. One or more service providers offer their services over this network. The end-user can choose any of these services and download their CA/DRM system, if he/she is registered (including authentication and authorisation) with the corresponding service provider.
  After some time, the same end-user decides to be connected to the network of access network provider B. He/she connects his/her CPE to this network. If his CPE supports the required reception technologies (e.g. DVB-C/C2, -S/S2, -T/T2, Ethernet, xDSL), one or more service providers offer their services over this network. The end-user can choose any of these services and exchange/swap the CA/DRM systems accordingly, if he/she is registered (including authentication and authorisation) with the corresponding service provider.
- A CE manufacturer wants to bring CPEs to the retail market, which supports both FreeTV and PayTV. The CPEs may however be adapted for use with specific PayTV services by software upgrade with consent of the end-user.
- A consumer connects his/her retail TV receiver (with broadband connectivity) to a broadcast service, which the broadcast service provider has chosen to protect. The service provider offers additional service elements via broadband which are protected with the same CA/DRM system. By downloading the appropriate CA/DRM system, the consumer is able to receive that particular service. Now, the service provider offers additional service elements from a business partner by linking to its TV Apps, which e.g. protect content with a different CA/DRM system. By downloading the relevant CA/DRM system in parallel into the CPE the consumer can access the whole service offering.
- Consumers expecting to use services on “their” devices in a given usage context. This specifically includes devices which are not natively broadcast receivers, but also devices receiving video via broadband. Thus, the devices need to support all possible CA/DRM solutions from service / platform providers.

D) Expected Basic Needs

Reflecting the use cases above and end customer expectations concerning CA/DRM solutions in retail CPEs, which have been reported by consumer organizations, the specification is expected

- to enable interoperability of the CA/DRM functionalities of retail CPE devices.
- to enable that CA/DRM functionalities can be replaced by software download. It is expected that such a change runs smoothly and that no significant cost is associated with such a change.
- to ensure that the security of swappable CA/DRM solutions is comparable to solutions existing in the market, allowing to access to all types of offered pay-services. The solution is expected to be available for all devices operated in a personal environment.
- to support a user friendly user interface, which allows the configuration of the device according to consumer expectations based on the provided functionalities of the CPE.

The development of system requirements is subject to the ISG ECI and shall reflect the interest of all relevant market partners. However, the above listed expectations are regarded as essential criteria for a software-based exchangeable CA/DRM architecture.

E) The Technical Concept

In order to facilitate the understanding of the technical concept as described in this document, the following terms were defined and they will be re-used in the subsequent chapters.

Terms:

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

Embedded CI client (**ECI client**) is the implementation of a CA/DRM client, which is compliant with the **Embedded CI** specifications.

CA/DRM client is a software module, which provides all means to receive and decrypt content and to manage the usage rights.

Embedded CI container (**ECI container**) is the framework which provides the interfaces and hooks for an **ECI client** to connect to the CPE and in which the **ECI client** is being executed.

Structure and Elements of a Standard

Concerning the conceptual description, it is proposed, that the complete standard consists of a group of specifications with a Framework specification (F), in combination with further underlying specifications:

(A): ECI Requirements

(B): The ECI Container: including Loader and all Interfaces and Resources

(C): The Virtual Machine (VM)

(D): The Advanced Security System

(E): Trust Environment

which together describe a solution allowing replacement of ECI clients at any time by just downloading the ECI clients in question. The ECI clients will be 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 to be defined in specification (B), and enable the ECI client to interact with the various functions in the CPE and beyond.

The ECI client runs upon a virtual machine instance that is to be defined in specification (C).

Specification (D) will specify an Advanced Security mechanism to protect the key to 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 even simultaneously. The ECI container has methods to its disposal to deny access to content in the case the CPE does not support this Advanced Security.

The technical solution will be applicable to CA and DRM systems. Further, it allows the implementation of a multitude of ECI clients in a single CPE, each with its own Virtual Machine instance. The ECI clients in a CPE will be able to run simultaneously, and simultaneously use the Advanced Security facility, if available.

The number of ECI clients embedded in a single CPE is only limited by the available resources in the CPE.

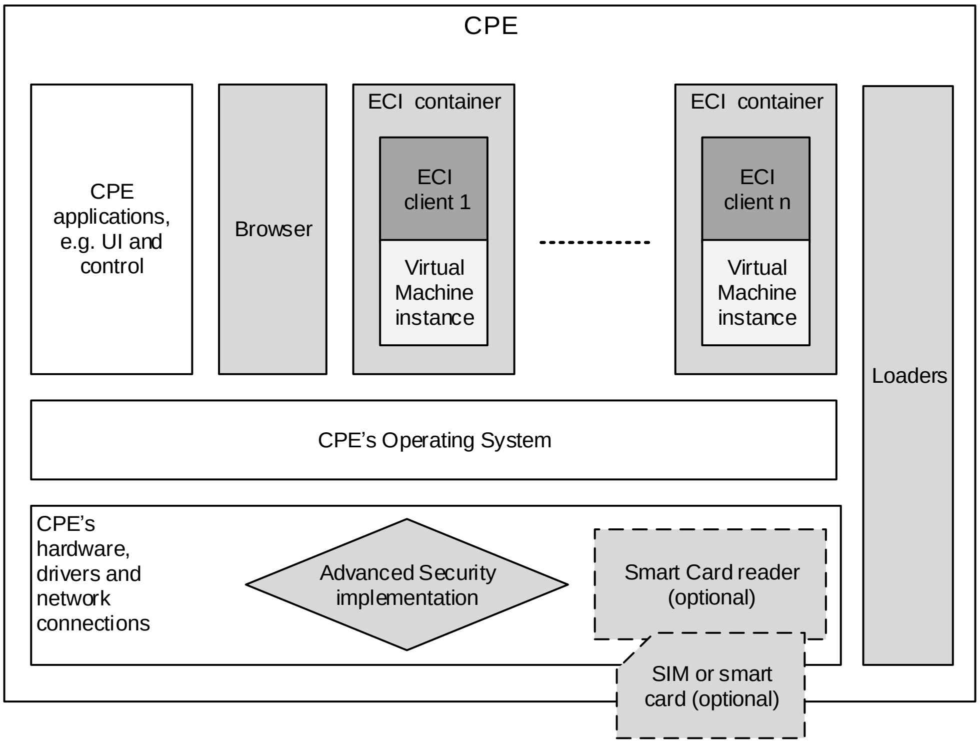
Upon its installation, the ECI clients will be notified by the CPE about the content delivery paths the CPE has found. Also, they will be notified about the relevant facilities in the CPE, such as Advanced Security, recording facilities and HD outputs. The ECI clients are expected to check possible set restrictions regarding the use as set by the operator or content distributor, if any, and notify the user. This will be specified in (B).

Specification (B) will also include methods to revoke rights to access content, for example in the case of a CA system that has been compromised, or in the case where the content owner does not wish specific content versions, e.g. a version in high definition, being released by a certain CA system.

The roles of Trusted Authorities and Trusted Third Parties generating and distributing keys and certificates are needed as described in section F of this paper.

Conceptual Description

a) CPE Architecture


CPE
CPE applications, e.g. UI and control
Browser
ECI container
ECI client 1
Virtual Machine instance

ECI container
ECI client n
Virtual Machine instance
Loaders
CPE's Operating System
CPE's hardware, drivers and network connections
Advanced Security implementation
Smart Card reader (optional)
SIM or smart card (optional)

The figure shows the block diagram of a CPE with n ≥ 2 embedded ECI clients, each with their own Virtual Machine instance. The shaded areas are subject of this document and the planned specifications (B), (C) and (D). Optional elements are indicated by dotted lines.

b) Key Elements of the Architecture

The ECI container and its interfaces

The ECI container has standardized interfaces with the various possible functions in the CPE (see (B) for detailed specifications), such as:

- Payload processing capabilities regardless of the transport protocol
- Recording and play-back facilities
- Inputs and outputs
- A browser, for which a minimum is specified in (B), see also here below
- A possible smart card (a smart card or similar, as well as the reader are optional)
- The content selection and decryption facilities.

The possibility to use watermarking and fingerprinting should be considered.

The ECI container is expected to be limited to the functionalities required to host compatible ECI clients. The CPE can be connected to any number of networks, both unidirectional and bidirectional. It does not always need to be connected to any network.

A Minimum Browser

For communications with the user, a minimum browsing facility is expected to be available to the ECI clients. This will be specified in (B). It is used to display messages for the user that have been generated by or sent using the ECI system. As it is capable to be used in broadcast only environments it needs appropriate access to APIs connecting to broadcast and IPTV services. Also, it is used to have the user enter inputs, such as a PIN.

The Virtual Machine (VM)

The ECI clients run upon a standardized VM. This will be specified in (C). Each installed ECI client is expected to have its own instance of the VM.

The Advanced Security facility

Advanced Security protects the Control Word during its travel from the ECI client environment to the content decryption facility in a CPE. For broadcasting reception devices (set-top-boxes or integrated digital TV receivers) the availability of advanced security facilities, as will be specified in (D), is mandatory. For other devices, capable to present video, such as tablets or Smart Phones, advanced security facilities are optional. In case advanced security facilities are not available in a device the access to video may be further restricted, depending on the signaling provided by the content rights owner.

The Loader

The CPE is expected to include a separate loader for the ECI clients, allowing loading, verification and installation, as well as integrity and anti-substitution protection during the ECI client's lifetime, independently from

- All other software in the CPE;
- Any other ECI clients or related facility.

During its installation in its ECI container, the ECI client is informed by the CPE about its facilities, such as recording facilities, HD facilities and networks, and compliance with the planned framework specification (F) and (B), (C) and possibly (D). Should the facilities not match the minimum needs of the ECI client, then the ECI client will inform the user by displaying a message using the browser, and send a message to the loader, enabling the loader to at least isolate the image file of the ECI client, or delete it. The ECI client will also inform the user about restricted functionality in case the ECI client's requirements regarding the CPE functionality are only partly fulfilled. This will be further detailed in (B).

The loader with the related security facilities will be specified in (B).

Revocation

Revocation may affect clients as well as the host. Means to revoke include technical elements and contractual obligations. Revocation of a single CPE or a range of CPEs should be possible. This will also be specified in (B). It is advised to revoke the ECI client on head end level.

F) Trust Management

Overview

In a vertical market with a proprietary CA/DRM system the CA/DRM vendor controls all aspects of security and the associated compliance and robustness rules. This makes an exchange of the CA/DRM system very difficult. In a horizontal market with a possibility of downloading/exchanging CA/DRM systems this control function for security and trust has to be assumed by a neutral party, a Trust Authority (TA). A TA has to serve the needs of a variety of market actors, in particular CA/DRM vendors, platform operators and CPE manufacturers. It plays a key role in case of a CA/DRM system exchange. It has to issue secure keys and certificates and to take care that the compliance and robustness rules of the systems in use can be applied appropriately and security of operation is always guaranteed. ECI is based on such a concept for neutral management of security and trust, which is described hereafter.

Organization and Workflows

Based on analysis of several standardization efforts it is commonly accepted that two elements are necessary to manage trust in such a scenario:

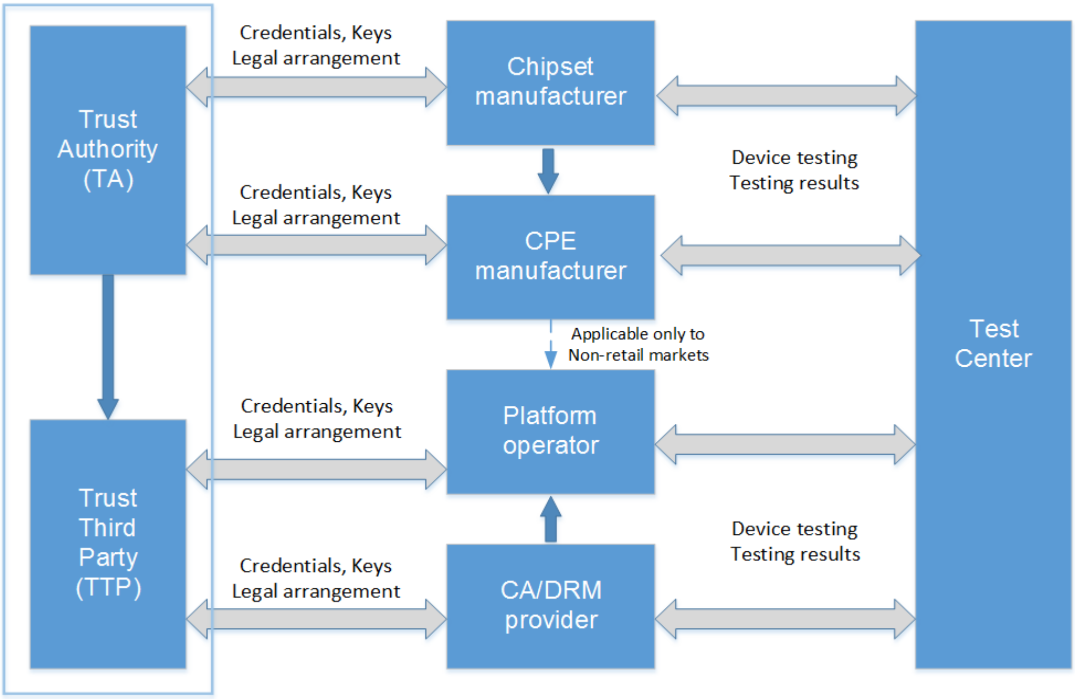
- **Trust Authority (TA)** as an organization governing all rules and regulations that apply to implementations of the ECI architecture. The Trust Authority has to be a legal entity to be able to achieve legal claims. The Trust Authority needs to be impartial to all players in the downloadable CA/DRM ecosystem. This includes:
    - Manufacturers of ECI compliant host systems (CPE manufacturers)
    - CA/DRM manufacturers (their ECI clients)
    - Chipset manufacturers, whose components include unchangeable Secure Processor keys and certificates, which are necessary for interaction between host and the compliant ECI client.
    - Platform operators; the platform operator is the party who controls all necessary elements of an ECI client. The role of a Platform operator can be taken for example by service providers and / or network operators.

- One or more Certificate Authorities, which can issue certificates and keys to compliant manufacturers of the relevant components of the CA/DRM system, under appropriate conditions and under a contract with the TA. Those authorities who manage the credentials are usually denominated as **Trusted Third Party (TTP).**
  The trust of these certificates chains back to the TA, which holds the root of trust.
  A Trusted Third Party is a technical service provider and may be easily replaced within a CA/DRM eco-system.

Trust Authority (TA) and Trusted Third Party (TTP) 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).

TA and TTPs ensure the functioning of the contractual framework (see next section), under which the various parties involved can assume their responsibilities and liabilities. Under a License Agreement (LA) from the TA the TTPs are generating and issuing key pairs, certificates, test credentials and Operator IDs. They are also signing software (e.g. loaders). The following picture gives an indication of some of the steps involved (not complete). The actions may vary in the various processes and depending on the particular contractual framework.

The TA is also issuing the compliance and robustness rules which the CPEs have to fulfill. The technical specification has to provide the necessary hooks for generating compliance and robustness rules.


Trust Authority (TA)
Trust Third Party (TTP)
Credentials, Keys Legal arrangement
Credentials, Keys Legal arrangement
Credentials, Keys Legal arrangement
Credentials, Keys Legal arrangement
Chipset manufacturer
CPE manufacturer
Applicable only to Non-retail markets
Platform operator
CA/DRM provider
Device testing Testing results
Device testing Testing results
Test Center

General workflow overview; Trusted Third Party (TTP) and Test Center are contract partners of the Trust Authority (TA) for certification and key issuing process

Contractual Framework

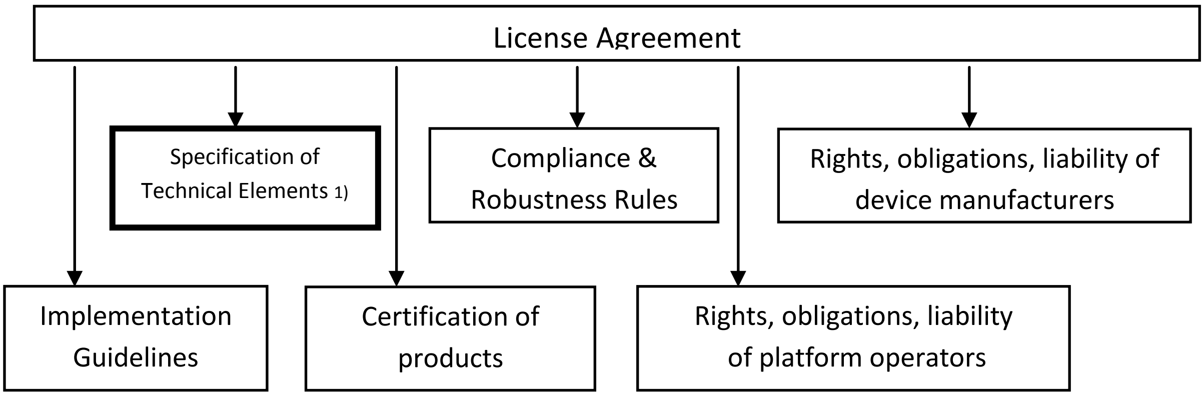
The present paragraph is presented for information purposes and represents only a view on the necessities for a contractual framework to operate SW-based exchangeable CA/DRM solutions in a secure environment.

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 in accordance with the relevant usage rules. Similarly, the LA 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.


License Agreement
Specification of Technical Elements 1)
Compliance & Robustness Rules
Rights, obligations, liability of device manufacturers
Implementation Guidelines
Certification of products
Rights, obligations, liability of platform operators

Components of License Agreement

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

***