International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series J

Supplement 8

(04/2021)

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

Embedded common interface (ECI) for exchangeable CA/DRM solutions; Trust environment

ITU-T J-series Recommendations – Supplement 8

Supplement 8 to ITU-T J-series Recommendations

Embedded common interface (ECI) for exchangeable CA/DRM solutions; Trust environment

Summary

Supplement 8 to ITU-T J-series of Recommendations addresses details of a trust environment for the embedded common interface (ECI) for exchangeable conditional access (CA)/digital rights management (DRM) (CA/DRM) solutions and complements ECI-related ITU-T Recommendations covering the ECI Ecosystem.

This ITU-T Supplement is a transposition of ETSI standard ETSI GS ECI 001-6 and is a result of a collaboration between ITU-T SG9 and ETSI ISG ECI.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J Suppl. 8	2020-04-23	9	11.1002/1000/14287
2.0	ITU-T J Suppl. 8	2021-04-28	9	11.1002/1000/14641

Keywords

CA/DRM, trust.

* 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

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Introduction

This ITU-T Supplement is a transposition of the ETSI standard [b-ETSI GS ECI 001-6] and is a result of a collaboration between ITU-T SG9 and ETSI ISG ECI.

The **embedded common interface** (**ECI**) system combines security with interoperability to provide a flexible and future-proof **Content Protection System**. It is an open, standardized system, which allows CA/DRM vendors to implement a wide range of products and consumers to readily switch between vendors on **ECI** compliant **customer premises equipment** (**CPE**s). The openness of the **ECI** system requires specific security elements in a compliant **CPE** to be swappable. In addition to the technical aspects of the standard there exist certain operational and commercial aspects which need to be handled in order for the security of the system, and the trustworthiness for all stakeholders to be provisioned and maintained. These aspects are addressed by creating a **Trust Environment** that consists of a contractual framework, policies, and technical specifications required for creating an **ECI Ecosystem**.

Supplement 8 to ITU-T J-series Recommendations

Embedded common interface (ECI) for exchangeable CA/DRM solutions; Trust environment

1 Scope

This Supplement specifies the basic technical principles and tasks for defining an **ECI** compliant **Trust Environment** intended for establishing an **ECI Ecosystem** as specified in [ITU-T J.1010], [ITU-T J.1011], [ITU-T J.1012] and further ECI-related ITU-T Recommendations. The present document therefore also provides guidance for a party that intends to serve as an **ECI Trust Authority** for an **ECI Ecosystem**.

This Supplement covers specification details in the following clauses: clause 6 addresses the **Trust Environment** and its stakeholders, clause 7 addresses the role of the **ECI Trust Authority**, clause 8 describes the tasks of the **ECI Trust Authority**, and clause 9 deals with critical workflows within the **ECI Ecosystem**. Appendix I gives some additional background information on the security aspects.

2 References

[ITU-T J.1010] Recommendation ITU-T J.1010 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements.*

[ITU-T J.1011] Recommendation ITU-T J.1011 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview*.

[ITU-T J.1012] Recommendation ITU-T J.1012 (2020), *Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation*.

[ITU-T J.1013] Recommendation ITU-T J.1013 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The virtual machine*.

[ITU-T J.1014] Recommendation ITU-T J.1014 (2020), *Embedded common interface for exchangeable CA/DRM solutions; Advanced security – ECI-specific functionalities*.

[ITU-T J.1015] Recommendation ITU-T J.1015 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The advanced security system – Key ladder block*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 advanced security system (AS system): Function of an **embedded common interface (ECI)** compliant **customer premises equipment** (**CPE**), which provides enhanced security functions (hardware and software) for an **ECI Client**.

NOTE – The details are specified in [ITU-T J.1014].

3.2.2 certificate: Data with a complementary secure **Digital Signature** that identifies an **Entity** in an **ECI Ecosystem**.

NOTE – The holder of the secret key of the signature attests to the correctness of the data – authenticates it by signing it with its secret key. Its public key can be used to verify the data.

3.2.3 certificate chains: List of **Certificate**s in an **ECI Ecosystem** that authenticate each other up to and including a **Root Revocation List**.

3.2.4 certificate processing subsystem (CPS): Subsystem of the **ECI Host** that provides **Certificate** verification processing and providing additional robustness against tampering.

3.2.5 content protection system: Systems that employs cryptographic techniques to manage access to content and services in an **ECI Ecosystem**.

NOTE – The term may be interchanged frequently with the alternate service protection system. Typical systems of this sort are either conditional access systems, or digital rights management systems.

3.2.6 customer premises equipment (CPE): Media receiver which has implemented **embedded common interface (ECI)**, allowing the user to access digital media services.

3.2.7 CPE manufacturer: Company that manufactures **embedded common interface (ECI)** compliant **customer premises equipment** (**CPE**s).

3.2.8 digital signature: Data (byte sequence) in an **ECI Ecosystem**, decrypted with the public key of the signatory of another piece of data, can be used to verify the integrity of that other piece of data by making a digest (hash) of the other piece of data and comparing it to the decrypted data.

3.2.9 embedded common interface (ECI): Architecture and the system specified in the ETSI ISG "Embedded CI", which allows the development and implementation of software-based swappable **ECI Client**s in customer premises equipment (**CPE**) and thus provides interoperability of **CPE** devices with respect to **ECI**.

3.2.10 ECI chip manufacturer: Company providing systems on a chip that implement **embedded common interface** (**ECI**) specified chipset functionality.

3.2.11 ECI client: Implementation of a conditional access (CA)/digital rights management (DRM) (CA/DRM) client which is compliant with the embedded common interface (CI) specifications.

NOTE – It is the software module in a **customer premises equipment** (**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.

3.2.12 ECI ecosystem: Real-world instantiation of a **Trust Environment** consisting of a **Trust Authority** (**TA**) and several platforms and **Embedded Common Interface (ECI)** compliant **customer premises equipment** (**CPE**s) in a commercial operation in the field.

3.2.13 ECI host: Hardware and software system of a **customer premises equipment (CPE)**, which covers **embedded common interface (ECI)** related functionalities and has interfaces to an **ECI Client**.

NOTE – The **ECI Host** is one part of the **CPE** firmware.

3.2.14 ECI host image: File(s) with software and initialization data for an embedded common interface (ECI) environment.

NOTE – An **ECI Host Image** may consist of a number of **ECI Host Image** files.

3.2.15 ECI trust authority (TA): Organization governing all rules and regulations that apply to implementations of **embedded common interface (ECI)** and manages the interoperability and coexistence of conditional access (CA) and digital rights management (DRM) systems within the **ECI** ecosystem.

3.2.16 entity, entities: Organization(s) (e.g., **Manufacturer**, **Operator** or **Security Vendor**) or real-world item(s) (e.g., **ECI Host**, **Platform Operation** or **ECI Client**) identified by an ID in a **Certificate**.

3.2.17 manufacturer: **Entity** which develops and sells **customer premises equipment** (**CPEs**), which accommodate an implementation of the **ECI** system and allow **ECI Host**s and **ECI Client**s to be installed per software download.

3.2.18 operator: Organization that provides **Platform Operation**s that is enlisted with the **embedded common interface trust authority** (**ECI TA**) for signing the **ECI** ecosystem.

NOTE – An **Operator** may operate multiple **Platform Operations**.

3.2.19 platform operation (PO): Specific instance of a technical **Service** delivery operation having a single **ECI** identity with respect to security.

3.2.20 revocation list (RL): List of **Certificates** in an **ECI Ecosystem** that have been revoked and therefore should no longer be used.

3.2.21 root: Public key or **Certificate** containing a public key that serves as the basis for authenticating a chain of **Certificate**s in an **ECI Ecosystem**.

3.2.22 root certificate: Trusted **Certificate** that is the single origin of a chain of **certificate**s in an **ECI Ecosystem**.

3.2.23 security vendor: Company providing **embedded common interface** (**ECI)** security systems including **ECI Client**s for **Operator**s of **ECI Platform Operation**s.

3.2.24 service: Content that is provided by a **Platform Operation** in an **ECI Ecosystem**.

NOTE – In the context of **ECI** only protected content is considered.

3.2.25 trust authority (TA): Organization governing all rules and regulations that apply to a certain implementation of **ECI** and targeting a certain market.

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 **ECI ecosystem** that it is governing.

3.2.26 trust environment: Collection of rules and related process that constitutes the basis for an **ECI ecosystem**.

3.2.27 trusted third party (TTP): External company that fulfils operational roles and tasks of the **Trust Authority** and on its behalf, such as issuing **certificate**s.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

API	Application Program Interface
AS	Advanced Security
CA	Conditional Access
CA/DRM	Conditional Access/Digital Rights Management
CI	Common Interface
COBIT	Control Objectives for Information and Related Technologies
CPE	Customer Premises Equipment
CPS	Certificate Processing Subsystem
DRM	Digital Rights Management
ECI	Embedded Common Interface

ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
HSM	Hardware Security Module
OEM	Original Equipment Manufacturer
PO	Platform Operation
TA	Trust Authority
TTP	Trusted Third Party

5 Conventions

The use of terms in bold and starting with capital characters in the present document shows that those terms are defined with an ECI specific meaning, which may deviate from the common use of those terms.

6 Overview of ECI Trust Environment

6.1 Introduction

The **ECI**-related ITU-T Recommendations [ITU-T J.1010], [ITU-T J.1011], [ITU-T J.1012], [ITU-T J.1013], [ITU-T J.1014], [ITU-T J.1015], associated by [b-ITU-T J-Suppl.9] and [b-ITU-T J-Suppl.7], provide significant freedom for making technical implementations, enabling ecosystems to make their own choices on how to implement certain features. In addition, the openness of the **ECI** system allows for certain components to be interchangeable. These properties require mutual trust between parties participating in the system and compliance to a common set of rules. These rules are collected in a **Trust Environment** and created and maintained by an **ECI Trust Authority** (**TA**).

The **Trust Environment** is defined by the **Trust Authority** and consists of the contractual framework, policies, and technical specification required for creating a real-world **ECI Ecosystem**. The **TA** is a legal entity that governs all rules and regulations for a specific **Trust Environment** and enforces them through legal and technical means**.** In addition, the **Trust Authority** serves as trusted **Root** for the chain of **Certificate**s used to authenticate **Entities** of the ecosystem.

6.2 Trust Environment and ECI Ecosystem

The **Trust Environment** is a formal construct that combines all mandatory aspects described in the present document as well as the other **ECI** specifications. The **Trust Environment** is therefore the sum of all technical and contractual aspects needed for creating a real-world ecosystem.

The **ECI Ecosystem** is the real-world instantiation of a **Trust Environment**. An ecosystem is always created on the basis of a **Trust Environment**. However, the concrete shape of the ecosystem is also affected by regulatory, legal, and economic factors that are outside of the scope of the present document.

6.3 ECI Certificates and trust

Within the **ECI Ecosystem**, trust is established and managed through the use of **ECI** specific **Certificate**s and **Certificate Chains** as defined in [ITU-T J.1012]. This allows all parties involved with an **ECI Ecosystem**, from key stakeholders to end users, to verify that each certified **Entity** has been directly or indirectly certified by the **Trust Authority**. Examples that illustrate the possibilities and properties of the certificate system and show how such a process may be implemented can be found in [b-ITU-T J-Suppl.9].

6.4 ECI export groups and trust

A unique feature within the **ECI Ecosystem** is the ability to securely transfer purchased content between **ECI Client**s, as long as certain technical and contractual prerequisites are met. The technical basis for this process is a special application program interface (API) and **Certificate**s as specified in clause 9.7 of [ITU-T J.1012]. But since the transfer of protected content from one **ECI Client** to another implies a transfer of responsibility and liability between stakeholders, it is recommended that the **Trust Authority** provides the necessary rules and requirements within the **Trust Environment** to facilitate the creation of export groups between different stakeholders.

6.5 Stakeholders of the ECI-Ecosystem

6.5.1 Definition

A stakeholder of an **ECI Ecosystem** is any legal entity that commits itself to the contractual framework of the ecosystem by entering a contractual relationship with the **Trust Authority**. In addition to the contractual relationship with the **TA**, stakeholders may also have relationships with each other. Any relationship of a stakeholder with a third party outside of the ecosystem (e.g., subcontractors) is subject to the contractual framework of the **ECI Ecosystem**.

The following key stakeholders exist in an **ECI Ecosystem**:

- Platform **Operator**/**Service** Provider
- **CPE Manufacturer**
- **Security Vendor** (creates **ECI Client**s)
- **ECI Chip Manufacturer**

The present document focuses on the key stakeholders of an **ECI Ecosystem**. In addition, other stakeholders such as independent original equipment manufacturers (OEMs) or suppliers of subsystems may play an active role in an **ECI Ecosystem**.

A special case in this context is the user who is considered a part of the **ECI Ecosystem** without being a stakeholder due to not being in a contractual relationship with the **Trust Authority**.

In addition to these stakeholders, which exist within an **ECI Ecosystem,** there also exist external parties that are not considered stakeholders but can still have influence on the **ECI Ecosystem**. Examples of such third parties are:

- Content owners and their representatives
- Regulatory bodies
- Consumer rights organizations

6.5.2 Obligations of the stakeholders

All stakeholders of an **ECI Ecosystem** are bound by the contractual framework and the compliance and robustness rules the **Trust Authority** established for that ecosystem. In general, all stakeholders that create certified **Entities** (see also clause 7.4.3) that are used within an **ECI Ecosystem**, such as **ECI Clients**, have to make sure that their **Entities** are created and certified, and can be updated or revoked in accordance with the compliance and robustness rules as described in [ITU-T J.1012] and [ITU-T J.1014].

In addition to the obligation to provide **ECI** compliant **Entities** this includes specific obligations for each key stakeholder:

- Platform **Operator**: The platform **Operator** has to make sure that only valid **ECI Clients** are deployed and used, and that outdated or malicious **ECI Clients** are revoked according to the compliance and robustness rules. This includes ensuring its **Platform Operation** secret keys are managed in a secure manner.

- **CPE Manufacturer**: The **CPE Manufacturer** has to make sure that the **CPE**, the **ECI** virtual machine, and the **ECI Host** provided for it are **ECI** compliant and necessary updates are provided in a timely manner. This includes ensuring that any hardware related components and their integration in a **CPE** are compliant to the robustness rules.
- **Security Vendor**: The **Security Vendor** has to make sure that **ECI Clients** are created and can be revoked according to the compliance and robustness rules.
- **ECI Chip Manufacturer**: The **ECI Chip Manufacturer** has to ensure that any hardware is compliant to the robustness rules.

It is important that all stakeholders cover the entire lifecycle of their respective **Entities**, including the maintenance (e.g., updates) of their respective components. This is especially important for hard-to-update components such as the **Advance Security System** in a **CPE**.

6.5.3 Liabilities of the stakeholders

The various aspects concerning obligations, certification, and compliance outlined in the present document imply that the contractual framework of the **ECI Ecosystem** contains rules concerning the liability of the respective stakeholders as well as how liability is handled or passed on between stakeholders when they interact. It is recommended that the **Trust Authority** should add sufficient provisions to the contractual framework to adequately cover the topic of liability within the ecosystem. The details for handling liability are a business decision and therefore outside the scope of the present document.

7 Role of the ECI Trust Authority

7.1 Introduction

The primary role of the **ECI Trust Authority** is to serve as the head and legal representative of an **ECI Ecosystem**. More than one **ECI Ecosystem** may exist but only one **TA** needs to exist within any given **ECI Ecosystem**. The **Trust Authority**'s purpose is to facilitate the creation, operation, and future development of an **ECI Ecosystem** by providing and enforcing the necessary contractual framework, policies, compliance and robustness rules, and certification regime required. The **TA**'s goal is to maintain a secure and stable **ECI Ecosystem** that benefits its stakeholders. The **Trust Authority** needs to retain the control over the ecosystem necessary to fulfil its purpose.

7.2 Prerequisites

For an **ECI Ecosystem** to function properly the **Trust Authority** has to fulfil certain prerequisites:

- The **Trust Authority** needs to be impartial towards all stakeholders of its ecosystem and treat all stakeholders equally and fairly. This is especially important when enforcing conformance to the specification and the contractual framework.
- The **Trust Authority** needs to be an appropriate representation of the markets the ecosystem wants to address. It is important that the **TA** is able to balance the relevant market requirements.
- In case a **Trust Authority** assumes full or partial liability for certain aspects of the ecosystem, it needs to make sure it has the required financial resources.
- The **Trust Authority** needs to have an appropriate legal form and governance that enables it to fulfil its role.
- The **Trust Authority** needs to be a trustworthy business partner towards all stakeholders and third parties that interact with the ecosystem.
- The **Trust Authority** needs to be a reliable and responsive party and handle the certification or revocation of **ECI Entities** in a timely manner.

7.3 Delegation of responsibility

It is not required that the **Trust Authority** itself implements every process or operational aspect of the tasks outlined in the present document. The **TA** may outsource any task or role, partially or fully to a third party (also called a **Trusted Third Party**), as long as it serves the purpose of the **ECI Ecosystem** and the third party is contractually bound to the **Trust Environment**. However, the **Trust Authority** needs to remain accountable to the stakeholders of the ecosystem regarding the correct implementation of outsourced tasks.

7.4 Creation and enforcement of mandatory rules and policies

7.4.1 Introduction

The **Trust Authority**'s role as head of an **ECI Ecosystem** means that it is the **TA**'s responsibility to create all rules and policies, both contractual and technical ones, which are required for a working, real-world **ECI Ecosystem**. Two key aspects of this responsibility are the handling of conformance and certification related tasks, both of which are essential parts of the security of an ecosystem.

7.4.2 Conformance

Stakeholders of an **ECI Ecosystem** expect a constant level of quality and functionality from all other entities in the same ecosystem. This basic assumption is a fundamental requirement for an ecosystem with exchangeable components as it requires all **Entities** to correctly implement a mandatory set of functions, such as those defined for ECI in [ITU-T J.1012]. The **Trust Authority** is responsible for enforcing conformance and compliance with the **ECI Ecosystem**, especially for critical aspects such as the robustness requirements for security components as defined in [ITU-T J.1014] and [ITU-T J.1015]. Possible measures include the inclusion of adequate provisions in the contractual framework for the **TA** to use, such as penalties and liability.

7.4.3 Certification

The **ECI** specification uses the terms "certification" and "certify" as a mandatory requirement for an **Entity** to be allowed to partake in the ecosystem as defined in clause 5 of [ITU-T J.1012]. The idea of having each technical component certified before it can be used is to ensure a high level of quality and security, as well as conformance to the specification and contractual obligations. The **Trust Authority** is responsible for specifying and enforcing the requirements and processes related to certification.

NOTE – The description of the certification process used in [ITU-T J.1012] allows the implementation of different business models.

7.5 Ownership of critical components

The **Trust Authority**'s role as head of an **ECI Ecosystem** also includes it being the owner of critical components such as the **Root** keys as described in [ITU-T J.1012] which, together with the **Root Revocation List,** are essential and security critical components of the **ECI** system. Due to the criticality of such components for the ecosystem the **TA** needs to remain their owner.

7.6 Responsibility, accountability, and liability

The **Trust Authority** is responsible and accountable for the correct implementation of all tasks and the correct fulfilment of all roles described in the present document, as well as any additional tasks and roles required to create and to manage an **ECI Ecosystem**. The **TA** may outsource aspects of these tasks and roles to third parties whereby they become responsible for that specific task or role. The contractual framework should define how accountability and liability are handled within the **ECI Ecosystem**.

8 Tasks of the ECI Trust Authority

8.1 Introduction

This clause describes the most important tasks that the **ECI Trust Authority** needs to fulfil in order to have a working **ECI Ecosystem**. All tasks are based on the role of the **TA** within an ecosystem. Additional informative guidelines on how these tasks may be fulfilled can be found in clause 9 and Appendix I.

8.2 Control and management of Root keys

The security of the **ECI** system is centred on the concept of **Certificate**s and signatures for verifying the integrity and authenticity of key components as described in clause 5 of [ITU-T J.1012]. For this to work, a reliable trust anchor is required. The technical incarnation of this trust anchor is an **ECI Root Certificate** with the corresponding **Root** keys. In addition, a legal entity needs to exist that serves as owner and custodian of the **Root** keys.

In an **ECI Ecosystem** the **Root** keys needs to be owned by the **Trust Authority**. The technical aspects, such as handling of the key material, may be outsourced to a third party (such as a professional certification authority) but the **Trust Authority** needs to retain control over the use of the **Root** keys.

NOTE – Specific care is recommended for the implementation of the secrecy of the "spare" root keys as described in clause I.2.

8.3 Control and management of Root Revocation List

The security of the **ECI** system is centred on the concept of **Certificate**s and signatures for verifying the integrity and authenticity of key components. For this to work, a revocation mechanism is required that allows compromised keys or other certified entities to be made invalid. **ECI** employs a system of **Revocation List**s to provide such a mechanism as described in clauses 5 and 8 of [ITU-T J.1012]. For this system to work, a legal entity needs to exist that ultimately decides which entities are placed on a **Revocation List**.

In an **ECI Ecosystem** the content of the **Root Revocation List** needs to be defined by the **Trust Authority.** Therefore, the **TA** needs to take responsibility for its content and remain accountable to the stakeholders within the ecosystem. The **Revocation List** related processes and rules are subject to the contractual framework between the stakeholders that has been established by the **TA**.

The technical aspects, such as handling of the **Revocation List** and the key material needed to create it, may be outsourced to a third party (such as a professional certification authority) but the **Trust Authority** needs to retain the final authority on the decision of placing an **Entity** on the **Root Revocation List**.

NOTE – The **Root Revocation List** defined in [ITU-T J.1012] implies the minimal version of every child **Certificate** and **Revocation List** thereof.

8.4 Definition of the process for creating Certificates

Every **Entity** in an **ECI Ecosystem** needs to have a valid **Certificate** before it can be used by any other **ECI** compliant device within the same ecosystem as defined in clause 5 of [ITU-T J.1012]. It is therefore important that the process for creating **Certificate**s for **Entities** is fully defined. Therefore, the **Trust Authority** needs to define the processes, rules, and requirements for creating **Certificate**s.

Important key aspects of **Certificate** creation that need to be defined are:

- What are the prerequisites that need to be fulfilled before a **Certificate** can be created.
- What is the specific process for creating **Certificate**s.
- Who is allowed to create **Certificate**s for specific **Entities**.
- How and on initiative of whom is this process started.
- Who is responsible for the creation and handling of the secret key associated with a **Certificate**.
- How security sensitive data (e.g., secret keys) is handled and authenticated.

Additional guidance on the correct implementation of this task can be found in clauses 9 and I.1.

8.5 Definition of the process for revoking Certificates

In order to uphold the security of an **ECI Ecosystem** it needs to be possible to revoke any **Entity** if the need arises as defined in clauses 5 and 8 of [ITU-T J.1012]. It is therefore important that the process for revoking **Certificate**s for **Entities** is fully defined. Consequently, the **Trust Authority** needs to define the processes, rules, and requirements for revoking **Certificate**s.

Important key aspects of **Certificate** creation that need to be defined are:

- What are the prerequisites that need to be fulfilled before a **Certificate** can be revoked.
- What is the specific process for revoking **Certificate**s.
- Who is allowed to revoke **Certificate**s for specific **Entities**.
- How and by whom can this process be started.

Additional guidance on the correct implementation of this task can be found in clauses 9 and I.1.

8.6 Repository for Certificates and Revocation Lists

To facilitate the **Certificate** based security mechanisms in **ECI**, the **Trust Authority** should provide a repository containing all relevant **Certificate**s and **Revocation List**s. Access to this repository or specific items within the repository is subject to the rules and policies of the specific ecosystem but should be as unrestricted as possible. The aim of the repository should be to reduce the complexity and delay for retrieving specific **Certificate**s or **Revocation List**s.

NOTE – **Certificate**s and **Revocation List**s both contain only public (i.e., non-secret) information.

8.7 Creation and management of the technical framework of an ECI ecosystem

As the head of an ecosystem, the **ECI Trust Authority** decides which current versions of the relevant specifications, as well as which additional requirements such as performance or robustness requirements, are mandatory and enforced within that specific **ECI Ecosystem**. Guidelines on the selection of specific performance values can be found in [b-ITU-T J-Sup.7]. As part of this task the **TA** also decides which old specifications are to be deprecated within the **ECI Ecosystem**.

NOTE – This task concerns mandating a specific version within a single ecosystem.

8.8 Creation and management of the contractual framework of an ECI ecosystem

As the legal entity that represents the **ECI Ecosystem**, the **Trust Authority** is responsible for managing all legal and contractual aspects related to the ecosystem. The **Trust Authority** needs to create all legally binding agreements in such a way that it is able to enforce conformance and compliance within the **Trust Environment** as described in clause 8.10. This is important as all trust within the **ECI Ecosystem** is based on the ability of all stakeholders and **Entity**'s to reliably verify the authenticity of **ECI** compliant components through the means of **ECI Certificate**s as defined in

[ITU-T J.1012]. The **TA**'s ability to enforce conformance and compliance is crucial for the creation of a **Trust Environment**.

Therefore, the **TA** needs to create and manage the contractual framework that governs the **Trust Environment**. A very important part of the contractual framework is the liability and the penalties for breach of contract. It is crucial for all stakeholders to be aware of their contractual obligations and to commit to them fully prior to entering the ecosystem and to uphold them when entering **ECI** related contracts, e.g., **CPE Manufacturer** and chip vendor.

The actual creating of contracts or legal documents and the management of contracts may be outsourced as long as it does not compromise the **TA**'s ability to effectively fulfil its role as head of the ecosystem. The **Trust Authority** needs to remain in control of and accountable for the correct handling of all legal and contractual matters.

8.9 Definition of the certification process

It is up to the **Trust Authority** to specify and enforce the requirements and processes related to certification (see also clause 7.4.3) as the details of this process are out of scope for the **ECI** specification. Therefore, the **Trust Authority** needs to create a certification regime covering contractual and technical aspects, that aims to provide the necessary level of quality, and ultimately trust, within the ecosystem. The certification process itself can take many different forms, such as self-certification or certification by an authorized third party. The **Trust Authority** may commission external companies for auditing or certifying **ECI Entities**.

The Trust authority needs to ensure an adequate emphasis on prevention of security breaches, as opposed to relying on liability of participants, specifically for **ECI Entities** that are hard to maintain once deployed. This specifically holds for hardware-based elements in the **Advanced Security System** of the **ECI CPE**.

8.10 Conformance of ECI stakeholders

As head of the **ECI Ecosystem** the **Trust Authority** is responsible for enforcing the conformance to the **ECI** specifications referenced in clause 2 by all stakeholders as well as their conformance with the contractual framework. In order to do so, the **TA** has the ability to sanction non-conformance through contractual and technical means (e.g., by revoking nonconforming **Entities**). Sanctioning nonconforming stakeholders is an important task as it provides stability to a system that has many independent players. The **TA** should always take adequate steps when enforcing rules.

Enforcing conformance within the ecosystem is crucial for an **ECI** system to work as it is a fundamental requirement for enabling exchangeable **ECI Client**s as described in [ITU-T J.1012]. This also includes fulfilling performance and use case requirements as discussed in [b-ITU T J-Sup.7]. An important aspect of this is that all stakeholders are treated equal with regard to their obligations (e.g., correct implementation of features). The goal of the conformance regime is to have a constant level of security across all **Entities** within the ecosystem.

8.11 Registering, assigning, and managing Id values and keys

The **Trust Authority** serves as the central registrar for registering and managing the necessary Id values and keys defined in [ITU-T J.1012] within an **ECI Ecosystem**. As such, the **TA** is responsible for keeping accurate and consistent records and for providing information to stakeholders wherever it is required within the ecosystem.

The values and keys are:

- **Manufacturer** Id
- CPE type, model, and Id
- Chipset Id

- Chipset Public Key

In addition to Id values the **TA** also needs to maintain a register of the Chipset Public Keys of specific **CPE**s and provide them to **Operator**s. This register also needs to contain a list of individual compromised **CPE**s and their respective Chipset Public Keys that is accessible to **Operator**s. The register may be protected to maintain a certain level of privacy.

8.12 Creating and updating policies for security and robustness

The **Trust Authority** needs to create and update all mandatory policies for security and robustness as described in [ITU-T J.1014], as well as their validation. These policies need to be complementary to the current **ECI** Recommendations [ITU-T J.1010] to [ITU-T J.1015], associated by [b-ITU-T J-Suppl.9] and [b-ITU-T J-Suppl.7], and apply to all stakeholders and **Entities** in an ecosystem. The goal of these policies should be to enable the **ECI Ecosystem** to fulfil the current requirements for **Content Protection System**s in specific markets. In addition to internal aspects, policies can also include external input such as content security requirements expressed by content owners.

Examples for such policies include:

- Robustness requirements and their validation.
- Policies regarding creating and management of cryptographic material by the stakeholders.
- Disclosure rules for security incidents.
- Definition of responsibilities of specific stakeholders.

The **Trust Authority** also needs to take attempts at circumvention of security measures into account when creating the policies.

8.13 Settling disputes between stakeholders

The **Trust Authority** should serve as arbiter for any internal conflict between stakeholders of the ecosystem. This role is important as it might involve sensitive information or trade secrets of stakeholders. The contractual framework should already contain rules or provisions for handling disputes between stakeholders. In general, the **Trust Authority** should always aim to keep the ecosystem stable and to settle disputes in such a manner that benefits the ecosystem as a whole.

8.14 Updating ECI specification(s) and development of future version

As there may exist more than one such ecosystem, and therefore more than one **TA**, it is important that any future development represents a cooperative effort of all currently active **TA**s. Any update to the specification should be driven by market requirements to ensure the applicability of the new version.

Updates or new versions of the **ECI** specification should take at least the following aspects into account:

- The introduction of new features.
- The backwards compatibility to previous versions of the specification.
- How future proof current and new features are.
- Whether a new version is worthwhile taking into consideration the effort it takes to upgrade to it.

The task of creating a new version of a specification may be outsourced to a third party, such as a group of technical experts or a standardization body.

NOTE – This task is different because it is not limited to a specific ecosystem.

8.15 Point-of-contact for third parties

The **Trust Authority** represents the ecosystem outwardly and serves as point-of-contact for external parties such as companies interested in joining the ecosystem or content owners interested in information about the security of the ecosystem. The **TA** also represents the ecosystem during any communication directed at the general public, such as advertisement of the standard or the ecosystem. The **Trust Authority** should therefore include specific rules in its contractual framework to regulate how stakeholders communicate with third parties or the public.

9 Critical processes and workflows

9.1 Introduction

This clause aims to provide pointers to additional resources for guidance on implementing critical processes within an **ECI Ecosystem**. General guidelines on security aspects can also be found in Appendix I.

9.2 Certification

The basic requirements for defining the process of creating **ECI Certificate**s are described in clause 8.4. A more detailed example of such a workflow can be found in clause 13 of [b-ITU-T J-Suppl.9].

9.3 Revocation

The basic requirements for defining the process of creating **ECI Revocation List**s are described in clause 8.5. A more detailed example of such a workflow can be found in clause 13 of [b-ITU-T J-Suppl.9].

9.4 Key generation and management

Secure generation and management of cryptographic keys is a complex topic and any specific process needs to take the environment and market into account, in which a specific solution is intended to operate. This is especially important for fixed keys, such as the Chipset Public Key, which are impossible to replace.

Some general guidelines and considerations for how to address this issue can be found in [ITU-T J.1014] and [ITU-T J.1015], as well as some of the external sources referenced therein.

Appendix I

Additional information on security aspects

I.1 Implementing security related processes

It is assumed that the **ECI Trust Authority** models its internal policies and processes based on established international best practices and standards, such as ITIL, COBIT, ISO 27001 or ISO 9001. Any creation, management, or handling of crypto graphical material, especially the private **Root** keys, should involve technical components that are designed and certified for this purpose, such as hardware security modules (HSMs). All employees tasked with the handling of security critical components, especially the private **Root** keys, should be specifically trained for their tasks.

It is strongly recommended that the initial system and their related processes are audited by an external security company before the **Trust Authority** goes operational.

I.2 The concept behind the three Root keys

The **ECI** specifications require three independent **Root** keys to exist at any given point in time. Any new device is required to include the three **Root Certificate**s of the currently valid **Root** keys. Only one **Root** key is in active use at any given point in time with the other two remaining dormant.

The idea behind this is to prevent a catastrophic system failure in case the current **Root** key is lost or compromised. By having three independent keys available in every device, the **Trust Authority** is able to switch from the lost or compromised key to one of the two remaining **Root** keys and resume normal operation.

In order for this to work, it is important for the **Trust Authority** to store these keys separate from each other and in such a way that loss or compromise of the current **Root** key does not affect the other two **Root** keys.

Bibliography

[b-ITU-T J-Suppl.7]	ITU-T J-series Recommendations – Supplement 7 (2020), *Embedded common interface for exchangeable CA/DRM solutions; Guidelines for the implementation of ECI.*
[b-ITU-T J-Suppl.9]	ITU-T J-series Recommendations – Supplement 9 (2020), *Embedded common interface for exchangeable CA/DRM solutions; System validation*.
[b-ETSI GS ECI 001-6]	ETSI GS ECI 001-6 (2018), *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment*.

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, 2021