

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series J

Supplement 7

(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; Guidelines for the implementation of ECI

ITU-T J-series Recommendations – Supplement 7

ITU-T

Supplement 7 to ITU-T J-series Recommendations

Embedded common interface (ECI) for exchangeable CA/DRM solutions; Guidelines for the implementation of ECI

Summary

Supplement 7 to ITU-T J-series Recommendations serves as a guidance document, which contains performance parameters and values as well as use cases for the embedded common interface (ECI) for exchangeable CA/DRM solutions and complements ECI-related ITU-T Recommendations covering the ECI Ecosystem.

This ITU-T Supplement is a transposition of ETSI Group Report ETSI GR ECI 004 and is a result of a collaboration between ITU-T SG9 and ETSI ISG ECI. A minor amendment was introduced with a new clause 6.4.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T J Suppl. 7	2020-04-23	9	11.1002/1000/14286
2.0	ITU-T J Suppl. 7	2021-04-28	9	11.1002/1000/14639

Keywords

CA/DRM, guide.

* 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/>.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Supplement	2
4	Abbreviations and acronyms	4
5	Conventions	5
6	Guidelines for the implementation of an ECI compliant CPE	5
	6.1 Introduction	5
	6.2 The relevance of the ECI Implementation Guidelines for ECI Eco- Systems.....	5
	6.3 Performance requirements for ECI Clients and ECI Hosts	5
	6.4 Parameters required for the operation of ECI Clients and ECI Hosts in an ECI Ecosystem	8
	6.5 Performance requirements for the ECI Virtual Machine	8
	6.6 Performance requirements for the Advanced Security System	9
7	Use cases and scenarios associated with an ECI Ecosystem	10
	7.1 Introduction	10
	7.2 Management of protected content	10
	7.3 Implementation of a Secure Authenticated Channel (SAC) between two ECI Clients	11
	7.4 Mechanism for future update or extension of API messages	11
	7.5 Mechanism for future extension of content properties.....	11
	7.6 Watermarking	12
	7.7 Update mechanism for RL.....	12
	7.8 Uninstallation of an ECI Client	12
	Appendix I – General VM computing performance	14
	I.1 Performance values	14
	Bibliography.....	15

Introduction

This ITU-T Supplement is a transposition of the ETSI Group Report [b-ETSI GR ECI 004] and is a result of a collaboration between ITU-T SG9 and ETSI ISG ECI. A minor amendment was introduced with a new clause 6.4.

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 services. This includes the distribution of HD and UHD content to various types of customer premises equipment (CPE) in order to protect business models of content owners and **Service** providers, including Broadcasters and PayTV operators.

Existing CA/DRM technologies limit the freedom of many players in digital multimedia content markets. Due to technological progress, innovative, software-based CA/DRM solutions become feasible. Maximizing interoperability while maintaining a high level of security, these solutions promise to meet upcoming demands in the market, allow for new businesses, and broaden consumer choice with respect to content consumption via broadcast and broadband connections.

An **ECI Ecosystem**, compliant with [ITU-T J.1010], [ITU-T J.1011], [ITU-T J.1012], [ITU-T J.1013], [ITU-T J.1014] and [ITU-T J.1015], as well as [b-ITU-T J Suppl.8] and [b-ITU-T J Suppl.9], addresses important attributes, such as enabling a high level of system security, flexibility and scalability due to software-based implementation, as well as exchangeability fostering a future-proof solution and enabling innovation. Further aspects are applicability to content distributed via different types of networks, including classical digital broadcasting, IPTV and OTT **Services**. The **ECI** system specification of an open eco-system, fostering market development, provides the basis for exchangeability of CA and DRM systems in **CPEs**, at lowest possible costs for the consumers and with minimal restrictions for CA or DRM vendors to develop their target products for the PayTV market.

Complementing [ITU-T J.1010]], [ITU-T J.1011], [ITU-T J.1012], [ITU-T J.1013], [ITU-T J.1014] and [ITU-T J.1015], as well as [b-ITU-T J- Suppl.8] and [b-ITU-T J Suppl.9], the present Supplement gives further guidance and addresses beside necessary performance requirements a number of use cases and scenarios, which on one side make use of the **ECI Ecosystem** and on the other extend its possibilities.

Supplement 7 to ITU-T J-series Recommendations

Embedded common interface (ECI) for exchangeable CA/DRM solutions; Guidelines for the implementation of ECI

1 Scope

This Supplement serves as a guidance document for the **ECI Ecosystem** as specified in [ITU-T J.1012], [ITU-T J.1013], [ITU-T J.1014] and], as well as [b-ITU-T J Suppl.8] and [b-ITU-T J-Suppl.9], including specification of the architecture of the **ECI** system as defined in [ITU-T J.1011] and specification of the requirements as defined in **ECI** ITU-T Recommendation [ITU-T J.1010]. A major advantage and innovation of the **ECI Ecosystem**, compared with currently deployed systems, is a fully software-based client container architecture, backed by a standardized advanced security hardware and secure software functionality for the loading and exchanging of CA/DRM client systems in **CPEs**. **ECI** compliant solutions do not require any detachable hardware modules in **CPEs**. Software containers provide a secure ("Sandbox") environment for either CA or DRM kernels, hereafter named as **ECI Clients**, together with their individual **Virtual Machine Instances**. The download process is embedded in a secure and trusted environment, providing a trust hierarchy for installation and exchange of **ECI Host** and **ECI Clients** and thus enabling an efficient protection against integrity- and substitution attacks. For this reason, the **ECI Ecosystem** integrates an advanced security mechanism.

This Supplement covers implementation guidance details in the following clauses:

- Clause 6 contains performance requirements and parameters for the **ECI Host**, the **ECI Client**, the Virtual Machine and for the **Advanced Security System**.
- Clause 7 deals with use cases and applications based on the **ECI Ecosystem**, which either complement the **ECI** ITU-T Recommendations or address given scenarios in more detail.

This Supplement has the objective to make available to **ECI** implementers as much as possible of the common understanding captured during the work developing 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] and [ITU-T J.1015] as well as [b-ITU-T J Suppl.8] and [b-ITU-T J Suppl.9]. The present Supplement was prepared with the intention to provide know-how complementary to the content of these **ECI**-related ITU-T Recommendations themselves and about the environment in which an **ECI Ecosystem** will be operated. It is planned to extend this guideline by further guidance and background information gained during the implementation and operation of **ECI** compliant ecosystems.

2 References

- | | |
|----------------|--|
| [ITU-T J.1010] | Recommendation ITU-T J.1010 (2016), <i>Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements</i> . |
| [ITU-T J.1011] | Recommendation ITU-T J.1011 (2016), <i>Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview</i> . |
| [ITU-T J.1012] | Recommendation ITU-T J.1012 (2020), <i>Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation</i> . |
| [ITU-T J.1013] | Recommendation ITU-T J.1013 (2020), <i>Embedded common interface for exchangeable CA/DRM solutions; The virtual machine</i> . |

- [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 **ECI** compliant **CPE**, which provides enhanced security functions (hardware and software) for an **ECI Client**.

NOTE – The details are specified in [ITU-T J.1014] and [ITU-T J.1015].

3.2.2 AS slot: Resources of the Advanced Security block provided exclusively to an **ECI Client** by the **ECI Host**.

3.2.3 AS slot session: Resources and computing in an **AS slot** related to the de-cryption or re-encryption of a content element.

3.2.4 certificate: Data structure as defined in clause 5 of [ITU-T J.1012] 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.

3.2.5 CPE: **ECI** compliant customer premises equipment.

NOTE – A **CPE** can be a stationary device (e.g., SetTopBox or iDTV) or any kind of mobile or portable device, which is able to process digital media content within an **ECI Ecosystem**.

3.2.6 CPE manufacturer: Company that manufactures **ECI** compliant **CPEs**.

3.2.7 ECI (embedded CI): 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 **CPEs** with respect to **ECI**.

3.2.8 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.

3.2.9 ECI client image: File with software as VM code, and initialization data required by the **ECI Client Loader**.

3.2.10 ECI client loader: Software module part of the **ECI Host** which allows downloading, verifying and installing new **ECI Client Images** in an **ECI Host**.

3.2.11 ECI ecosystem: Commercial operation consisting of a **TA** and several platforms and **ECI** compliant **CPEs** in the field.