

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

ITU-T

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/>.

© 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	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	1
4	Abbreviations and acronyms	3
5	Conventions	4
6	Overview of ECI Trust Environment	4
	6.1 Introduction	4
	6.2 Trust Environment and ECI Ecosystem	4
	6.3 ECI Certificates and trust	4
	6.4 ECI export groups and trust.....	5
	6.5 Stakeholders of the ECI-Ecosystem	5
7	Role of the ECI Trust Authority	6
	7.1 Introduction	6
	7.2 Prerequisites	6
	7.3 Delegation of responsibility	7
	7.4 Creation and enforcement of mandatory rules and policies	7
	7.5 Ownership of critical components.....	7
	7.6 Responsibility, accountability, and liability	7
8	Tasks of the ECI Trust Authority	8
	8.1 Introduction	8
	8.2 Control and management of Root keys	8
	8.3 Control and management of Root Revocation List	8
	8.4 Definition of the process for creating Certificates	8
	8.5 Definition of the process for revoking Certificates	9
	8.6 Repository for Certificates and Revocation Lists.....	9
	8.7 Creation and management of the technical framework of an ECI ecosystem	9
	8.8 Creation and management of the contractual framework of an ECI ecosystem	9
	8.9 Definition of the certification process	10
	8.10 Conformance of ECI stakeholders.....	10
	8.11 Registering, assigning, and managing Id values and keys	10
	8.12 Creating and updating policies for security and robustness	11
	8.13 Settling disputes between stakeholders	11
	8.14 Updating ECI specification(s) and development of future version	11
	8.15 Point-of-contact for third parties	12

	Page
9 Critical processes and workflows	12
9.1 Introduction	12
9.2 Certification.....	12
9.3 Revocation.....	12
9.4 Key generation and management	12
Appendix I – Additional information on security aspects	13
I.1 Implementing security related processes.....	13
I.2 The concept behind the three Root keys.....	13
Bibliography.....	14

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 (CPEs)**. 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**.

