CI Plus ECP Specification v1.0 (2017-03)

Technical Specification

CI Plus Specification.
Enhanced Content Protection.

CI Plus LLP
31 Chertsey Street,
Guildford,
Surrey,
GU1 4HD,
UK

A company registered in England and Wales
Registered Number: OC341596

Copyright Notification

All rights reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owners.

© 2017 CI Plus LLP

Contents

1 Scope 4
2 References 4
3 Definitions, symbols and abbreviations 4
3.1 Definitions 4
3.2 Abbreviations 5
3.3 Use of Words 5
4 Command Interface 6
4.1 Mandatory Resources 6
4.2 Optional Functionalities 6
4.3 Content Control 6
4.3.1 ECP CC System 6
4.3.2 Keys on the credentials layer 6
4.3.3 Authentication 7
4.3.4 Content Key Calculation 7
4.3.5 URI 7
5 ECP Certificate Chain 8
5.1 Introduction 8
5.2 Certificate Management Architecture 8
5.3 Certificate Formats 9
5.3.1 version 9
5.3.2 serial number 9
5.3.3 signature 9
5.3.4 issuer 10
5.3.5 validity 10
5.3.6 subject 10
5.3.7 subjectPublicKeyInfo 10
5.3.8 issuerUniqueID and subjectUniqueID 10
5.3.9 extensions 10
5.3.9.1 Subject Key Identifier 10
5.3.9.2 Authority Key Identifier 10
5.3.9.3 Key usage 10
5.3.9.4 Basic Constraints 10
5.3.9.5 Scrambler capabilities 10
5.3.9.6 CI Plus Info 11
5.3.9.7 CICAM brand identifier 11
5.3.10 signatureAlgorithm 11
5.3.11 signatureValue 11
5.4 Certificate Verification 11
Annex A (normative): Random Number Generator 12
History 13

© 2017 CI Plus LLP

1 Scope

A CI Plus Security Level is a definition of robustness for CI Plus devices. While CI Plus devices may exceed the robustness requirements for a specific CI Plus Security Level, that latter establishes the minimum bar that must be met by a CI Plus device in order to consume content requiring the defined protection level.

CI Plus defined the CI Plus Standard Security Level designed to meet the security standard for consumption of SD and HD content.

The CI Plus ECP Compliance and Robustness Rules [4] introduce the ECP Security Level, designed to meet the security standards for content requiring ECP.

This specification provides the description of a CI Plus LLP implementation based on the CI Plus 1.4 specification [2] in order to realise a device compliant with CI Plus ECP Security Level.

This specification is intended to be used in combination with the appropriate certification process, and subject to conformance by the manufacturers to the CI Plus ECP Compliance and Robustness Rules [4].

2 References

[1] CI Plus Specification V1.3.2 (2015-03): "Content Security Extensions to the Common Interface".

[2] CI Plus Specification V1.4.2 (2016-05): "Content Security Extensions to the Common Interface".

[3] Bluebook A165 (2017-01): "Digital Video Broadcasting (DVB); Extensions to the CI Plus Specification
https://www.dvb.org/resources/public/standards/a165_dvb_ci_plus_1_4_jan_2017.pdf

[4] CI Plus ECP Compliance and Robustness Rules

[5] RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (version 3). https://www.ietf.org/rfc/rfc5280.txt

[6] RSA PKCS#1 v2.1: June 14, 2002. RSA Cryptography Standard, RSA security inc.

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[7] NIST Special Publication 800-90A Revision 1 (June 2015): Recommendation for Random Number Generation Using Deterministic Random Bit Generators

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply in addition to those defined in CI Plus Specification 1.3 [1] and CI Plus Specification 1.4 [2]:

ECP Host: A Host that implements the present document and that conforms to the CI Plus ECP Compliance and Robustness Rules [4].

ECP CICAM: A CICAM that implements the present document and conforms to the CI Plus ECP Compliance and Robustness Rules [4].

ECP Device: An ECP Host or an ECP CICAM.

ECP Security Level: The definition of robustness for CI Plus ECP devices.

Enhanced Content Protection: Content protection measures over and beyond those generally considered sufficient to protect HD content.

© 2017 CI Plus LLP

In this document:

- any reference to Host shall be interpreted as an ECP Host unless otherwise explicitly mentioned
- any reference to CICAM shall be interpreted as an ECP CICAM unless otherwise explicitly mentioned

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply in addition to those defined in CI Plus Specification 1.3 [1] and CI Plus Specification 1.4 [2]:

ECP	Enhanced Content Protection
PKI	Public Key Infrastructure

3.3 Use of Words

The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the specification and from which no deviation is permitted *(shall* equals *is required to).*

The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required *(should* equals *is recommended that).*

The word *may* is used to indicate a course of action permissible within the limits of the specification *(may* equals *is permitted to).*

© 2017 CI Plus LLP

4 Command Interface

This section defines the mandatory and optional resources for an ECP Device.

4.1 Mandatory Resources

An ECP Device shall implement all the mandatory resources as specified in the CI Plus 1.4 Specification [2] except where otherwise specified in the present document.

4.2 Optional Functionalities

An ECP Device may implement optional functionalities as specified in the CI Plus 1.4 Specification [2].

4.3 Content Control

4.3.1 ECP CC System

The ECP Security Level uses a dedicated PKI referred to as the ECP CC System.

CC system ID 1 is allocated for the Standard Security Level as defined in CI Plus Specification 1.3 [1].

CC system ID 2 is allocated for the ECP Security Level as defined in the present document and is called ECP CC System ID.

During the Authentication protocol, the Host shall advertise the ECP CC System ID using the method defined in clause 11.3.1.2 of CI Plus Specification 1.3 [1].

The Table 11.34 of CI Plus Specification 1.3 [1] shall then be replaced by Table 4.1:

Table 4.1: Host Capability Evaluation

Step	Action	APDU	Content
1	CICAM requests the Host's CC system ID bitmask	cc_open_req	
2	Host sends its CC system ID bitmask	cc_open_cnf	cc_system_id_bitmask: • bit 0 set indicates support for CI Plus Standard Security Level • bit 1 set indicates support for CI Plus ECP Security Level

The Host shall not advertise the support of ECP CC System for a session of the Content Control resource with resource identifier 0x008C1001 or 0x008C1002. The CICAM shall select the ECP CC System when the Host advertises it.

The CICAM shall inform the Host of the selection of the ECP CC System as described in clause 20 of BlueBook A165 [3].

4.3.2 Keys on the credentials layer

An ECP Device is provisioned with a pair of public (MDP/HDP) and private (MDQ/HDQ) keys dedicated to the ECP CC System.

An ECP Device may be provisioned as well with a pair of public and private keys dedicated to the Standard CC System.

NOTE: The ECP CC System public and private keys are different from the Standard CC System public and private keys.

There is a unique certificate chain for both CICAM and Host known as the ECP Certificate Chain which is described in chapter 5 of the present document.

The ECP Certificate Chain is independent from the Standard Certificate Chain defined in CI Plus Specification 1.3 [1] for the Standard Security Level.

© 2017 CI Plus LLP

When the ECP CC System is selected, the constants (DH_p, DH_g, DH_q) involved in operations on the authentication layer are ECP specific and are different from the constants used for the Standard CC System.

4.3.3 Authentication

During the execution of the Authentication protocol, Host and CICAM shall generate random values listed in table A.1 by use of a PRNG as defined in Annex A of the present document.

Annex A of the present Specification supersedes and replaces Annex A of the CI Plus Specification 1.3 [1].

4.3.4 Content Key Calculation

During the Content Key calculation, the CICAM shall generate Kp using a nonce generated by use of a PRNG as defined in Annex A of the present document.

4.3.5 URI

When the ECP CC System is selected:

- The Host shall support version 5 of the URI as defined in clause 19 of BlueBook A165 [3].
- The support of previous URI versions is not required.
- The CICAM shall always select URI version 5.

© 2017 CI Plus LLP

5 ECP Certificate Chain

5.1 Introduction

With the introduction of the ECP Security Level, CI Plus LLP defines in this chapter a new certificate chain (the ECP certificate chain) independent from the Standard certificate chain defined in CI Plus Specification 1.3 [1] for the Standard Security Level.

A Host implementing the ECP Security Level shall be provisioned with the certificates and private key (HDQ) for the ECP CC System and may be provisioned with the certificates and private key for the Standard CC System.

A CICAM implementing the ECP Security Level shall be provisioned with the certificates and private key (HDP) for the ECP CC System and may be provisioned with the certificates and private key for the Standard CC System.

5.2 Certificate Management Architecture

The CI Plus ECP trust hierarchy is organized as a tree structure with a single ECP Root of Trust (ECP-ROT). There is only one tree for all participants in CI Plus ECP, see Figure 5.1.

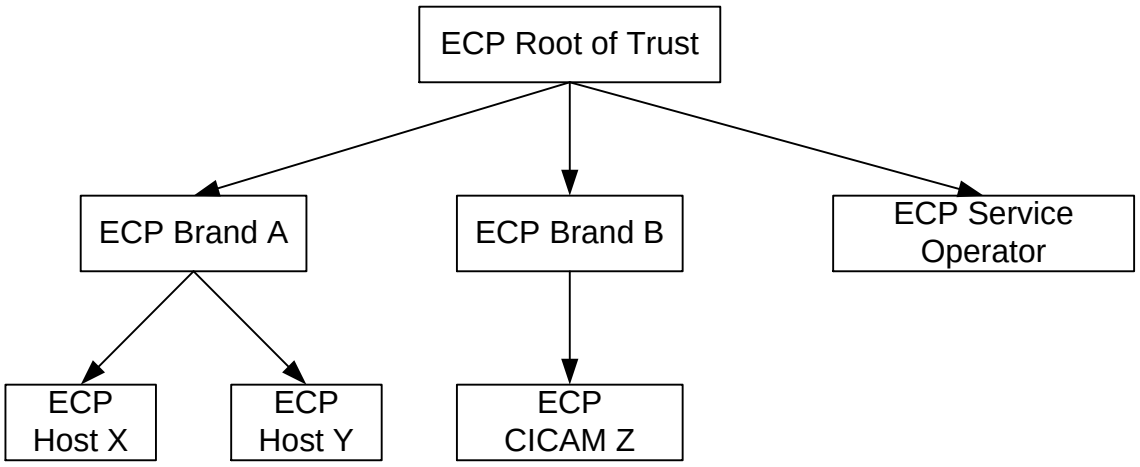

Figure 5.1: Certificate Hierarchy Tree

There are four different types of certificates.

- ECP Root certificate
  - issued by the ECP ROT
  - self-signed
  - only one root certificate exists for all of CI Plus ECP
- ECP Brand certificate
  - issued by the ECP ROT
  - signed with the private key of the ECP root certificate
  - one certificate of this type exists for each brand (or manufacturer)
- ECP Device certificate
  - issued by the ECP ROT
  - signed with the private key of the ECP brand certificate
  - each single ECP device has a unique device certificate

© 2017 CI Plus LLP

- ECP Service operator certificate
  - issued by the ECP ROT
  - signed with the private key of the ECP root certificate
  - one certificate of this type exists for each service operator

Each ECP certificate contains a public key (MDP/HDP) for which there is a corresponding private key (MDQ/HDQ).

Each Host and CICAM shall integrate the following certificate related information at manufacturing time:

- the CI Plus ECP root certificate
- the ECP brand certificate
- the ECP device certificate
- the private key corresponding to the ECP device certificate (MDQ or HDQ, see Table 5.2 of CI Plus Specification 1.3 [1])

Unlike other certificates, the service operator certificate does not have to be integrated into the Host or CICAM at time of manufacturing.

5.3 Certificate Formats

As defined in CI Plus Specification 1.3 [1] clause 9.3 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.1 version

As defined in CI Plus Specification 1.3 [1] clause 9.3.1.

5.3.2 serial number

As defined in CI Plus Specification 1.3 [1] clause 9.3.2.

5.3.3 signature

All certificates use RSASSA-PSS signatures as defined in PKCS1v2.1 [6], section 8.1.1.

The fields of the RSASSA-PSS-params shall have values as defined in Table 5.1:

Table 5.1: Certificate Signature Algorithm

Parameter	Value
hashAlgorithm	SHA-256
maskGenAlgorithm	MGF1 using SHA-256
saltLength	32 bytes
trailerField	one byte: 0xbc

The corresponding ASN.1 object identifiers are:

```
id-RSASSA-PSS OBJECT IDENTIFIER ::= { pkcs-1 10 }

pkcs-1 OBJECT IDENTIFIER ::= {
       iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }


rSASSA-PSS-Default-Params RSASSA-PSS-Params ::= {
       sha256Identifier, mgf1SHA256Identifier, 32, 1}

sha256Identifier AlgorithmIdentifier ::= { id-sha256, NULL }

id-sha256 OBJECT IDENTIFIER ::= {
       joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
       csor(3) nistalgorithm(4) hashalgs(2) 1 }
```

© 2017 CI Plus LLP

```
mgf1SHA256Identifier AlgorithmIdentifier ::= { id-mgf1, sha256Identifier }
```

5.3.4 issuer

As defined in CI Plus Specification 1.3 [1] clause 9.3.4 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.5 validity

As defined in CI Plus Specification 1.3 [1] clause 9.3.5 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.6 subject

As defined in CI Plus Specification 1.3 [1] clause 9.3.6 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.7 subjectPublicKeyInfo

As defined in CI Plus Specification 1.3 [1] clause 9.3.7 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.8 issuerUniqueID and subjectUniqueID

As defined in CI Plus Specification 1.3 [1] clause 9.3.8 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.9 extensions

As defined in CI Plus Specification 1.3 [1] clause 9.3.9 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.9.1 Subject Key Identifier

As defined in CI Plus Specification 1.3 [1] clause 9.3.9.1 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.9.2 Authority Key Identifier

As defined in CI Plus Specification 1.3 [1] clause 9.3.9.2 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.9.3 Key usage

As defined in CI Plus Specification 1.3 [1] clause 9.3.9.3 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.9.4 Basic Constraints

As defined in CI Plus Specification 1.3 [1] clause 9.3.9.4 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

5.3.9.5 Scrambler capabilities

Scrambler capabilities is a private extension for CI Plus. It shall be present in each device certificate and marked as critical. The ASN.1 definition is defined as

```
id-pe-scramblerCapabilities OBJECT IDENTIFIER ::= { id-pe 25 }
id-pe ::= {
   iso(1) identified-organization(3) dod(6) internet(1) security(5)
   mechanisms(5) pkix(7) 1 }

ScramblerCapabilities ::= SEQUENCE {
```

© 2017 CI Plus LLP

```
capability   INTEGER (0..MAX),
version      INTEGER (0..MAX) }
```

The following values are supported for capability:

Table 5.2: Capabilities Supported

Value	Meaning
0	Reserved
1	AES
all others	reserved for future use

5.3.9.6 CI Plus Info

As defined in CI Plus Specification 1.3 [1] clause 9.3.9.6.

5.3.9.7 CICAM brand identifier

As defined in CI Plus Specification 1.3 [1] clause 9.3.9.7.

5.3.10 signatureAlgorithm

This field is as defined in section 5.3.3 signature.

5.3.11 signatureValue

As defined in CI Plus Specification 1.3 [1] clause 9.3.11.

5.4 Certificate Verification

As defined in CI Plus Specification 1.3 [1] clause 9.4 except that reference to RFC3280 shall be replaced by reference to RFC5280 [5].

© 2017 CI Plus LLP

Annex A (normative): Random Number Generator

The Host and CICAM random number generator shall adhere to NIST 800-90A Revision 1[7] and shall be used to generate the following random numbers:

Table A.1: random numbers

Field	Length (bits)	Comment
DHX	2048	Diffie Hellman exponent "x"
DHY	2048	Diffie Hellman exponent "y"
Kp	256	CICAM's key precursor to Host for CCK
Ns_Host	64	Host's challenge to CICAM for SAC
Ns_Module	64	CICAM's challenge to CICAM for SAC
Auth_nonce	256	nonce in authentication protocol

© 2017 CI Plus LLP

History

Document history		
Version	**Date**	**Description**
1.0	31/03/2017	Publication

© 2017 CI Plus LLP