# CI Plus ECP Specification v1.1 (2017-11)

*Technical Specification*

## CI Plus Specification.
## Extensions for Enhanced Content Protection.

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

A company registered in England and Wales
Registered Number: OC341596

# Contents

# 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, it 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 ILA Addendum for ECP [4] introduces enhanced security protection measures, designed to meet the security standards for content requiring Enhanced Content Protection (ECP). This specification builds upon the CI Plus 1.4 specification [2] to define the requirements for a device suitable for receiving such content.

This specification is intended to be used in combination with the appropriate certification process, and subject to conformance by the manufacturers to the ILA Addendum for ECP [4].

# 2 References

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

[2] CI Plus Specification V1.4.3 (2017-10): “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 ILA Addendum for ECP

[5] 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 achieves the ECP Security Level.

**ECP CICAM**: A CICAM that implements the present document and achieves the ECP Security Level.

**ECP Controlled Content:** video content that has been received over and is interpreted by the CI Plus interface with the Encryption Mode Indicator (“EMI”) bits set to one, one (1,1) and with the ECP Control Info (“ECI”) bits set to values other than b000.

**ECP Device**: An ECP Host or an ECP CICAM.

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

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations defined in CI Plus Specification 1.3 [1] and CI Plus Specification 1.4 [2] apply.

## 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)*.

# 4 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.

An ECP Device shall implement version 5 of the URI as specified in Bluebook A165 [3] which defines fields (ECI and ICT) applicable to ECP Controlled Content. Refer to the CI Plus ILA Addendum for ECP [4] for the compliance rules.

# 5 Root of Trust Support

This chapter specifies the support of the Roots of Trust for devices compliant with the present document.

An ECP CICAM shall support both the CI Plus 2nd Root of Trust defined in chapter 6 of CI Plus 1.4 Specification [2] and the CI Plus Root of Trust defined in CI Plus Specification 1.3 [1].

An ECP Host shall support both the CI Plus 2nd Root of Trust defined in chapter 6 of CI Plus 1.4 Specification [2] and the CI Plus Root of Trust defined in CI Plus Specification 1.3 [1].

The CI Plus 2nd Root of Trust Device Certificate shall indicate support of the ECP Security Level, as defined in clause 6.3.3.9.8 of CI Plus 1.4 Specification [2].

An ECP CICAM may choose to not descramble content that requires ECP when the Host supports only the Standard Security Level.

# 6 Random Number Generator

An ECP Device shall generate the random values listed in Table A.1 of CI Plus Specification 1.3 [2] by use of a PRNG as defined in NIST 800-90A Revision 1[5].

# 7 Optional Functionalities

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

# History

| Document history | | |
|---|---|---|
| **Version** | **Date** | **Description** |
| 1.0 | 31/03/2017 | Publication |
| 1.1 | 17/10/2017 | Reference to CI Plus 2nd Root of Trust as now defined in CI Plus 1.4 Specification [2] |