CI Plus ILA Addendum for ECP

THIS CI Plus ILA ADDENDUM FOR ECP ("**Addendum**") is by and between CI Plus LLP ("**CI Plus LLP**"), a United Kingdom limited liability partnership, and the Licensee identified below that signs the Addendum (the "**Named Licensee**").
The Addendum is effective as of the date when it has been signed by both parties (the "**Effective Date**").

BY SUBMITTING A SIGNED COPY OF THIS ADDENDUM TO CI PLUS LLP (BY EMAIL, CERTIFIED OR REGISTERED PRE-PAID MAIL), NAMED LICENSEE CONFIRMS TO HAVE READ AND THAT HE AGREES TO ALL TERMS OF THIS ADDENDUM

CI PLUS LLP: C/O BDO LLP, 31 Chertsey Street, Guildford, Surrey, GU1 4HD. United Kingdom. Registered in England and Wales. Registered No: OC341596	Individual Authorised Signatory: _____ Signed on behalf of CI Plus LLP: Name: Title: Date:
NAMED LICENSEE: Company Name: Address: City: State: Postal Code: Country:	Individual Authorised Signatory: _____ Name: Title: Date:
NAMED LICENSEE'S AGENT (see Section 16.8 of the Agreement): Name: Address: Postal Code:	

WHEREAS, CI Plus LLP and Named Licensee have entered into a CI Plus LLP DEVICE INTERIM LICENSE AGREEMENT ("**Agreement**") and Named Licensee confirms that Licensee is in good standing under such Agreement;

WHEREAS, Licensee wishes to implement the CI Plus ECP Specification (as defined below) and CI Plus LLP is willing to license the use of Licensed Technology (as defined in the Agreement, as amended by this Addendum) and CI Plus Logo to Licensee in respect of the CI Plus ECP Specification, subject to the Agreement and the additional rights and obligations contained in the Agreement (as amended by this Addendum);

WHEREAS, in furtherance of such desire, the parties agree to amend the Agreement as set forth below in this Addendum;

NOW THEREFORE, in consideration of the foregoing promises and the covenants and agreements set forth herein, and other good and valuable consideration, CI Plus LLP and Licensee hereby agree to amend the Agreement as follows:

DEFINITIONS

All capitalized terms not defined in this Addendum shall have the same meaning as set forth in the Agreement, including its Exhibits or the Specifications, or as set forth in the CI Plus ECP Specification.

AMENDMENTS

1.1 The following definitions shall be added to the Agreement:

1.1.1 "**Applicable CI Plus Specification**" means:

(1) For a Standard Device: the CI Plus Standard Specification

(2) For an ECP Device: the CI Plus ECP Specification

1.1.2 "**Applicable Compliance Rules**" means:

(1) For a Standard Device: The Standard Compliance Rules

(2) For an ECP Device: the ECP Compliance Rules

1.1.3 "**Applicable Robustness Checklist**" means:

(1) For a Standard Device: The Standard Robustness Checklist

(2) For an ECP Device: The ECP Robustness Checklist

1.1.4 "**Applicable Robustness Rules**" means:

(1) For a Standard Device: The Standard Robustness Rules

(2) For an ECP Device: The ECP Robustness Rules

1.1.5 "**Applicable Specifications**" means Applicable CI Plus Specification and CI Plus License Specification.

1.1.6 "**CI Plus Standard Specification**" means the specification titled either (i) "CI Plus Specification – Extensions for Implementation Using the Universal Serial Bus" for a Device that provides CI Plus functionality over USB interface or (ii) "CI Plus Specification - Content Security Extensions to the Common Interface" for all other Devices. The applicable CI Plus Specification and version for each Registered Device Type is indicated on the Device Registration form submitted when the Standard Device is registered following commencement of the applicable Device Type registration by CI Plus LLP. The CI Plus Specification is publicly available at no charge at URL http://www.ci-plus.com and may be amended from time to time in accordance with Section 6.3.of the Agreement.

1.1.7 "**CI Plus ECP Specification**" means the version of the specification titled "CI Plus Specification – Extensions for Enhanced Content Protection" effective at

Device registration for each Device. The applicable version for each Registered Device is indicated on the Device Registration form submitted when the ECP Device is registered. The CI Plus ECP Specification is publicly available at no charge at URL http://www.ci-plus.com and may be amended from time to time in accordance with Section 6.3 of the Agreement.

1.1.8 "**CI Plus Logo**" means either the CI Plus Logo or the CI Plus ECP-1 Logo, as applicable, both as more particularly described in the "CI Plus Logo Guidelines" posted at URL as updated from time to time in accordance with the terms of the Agreement.

1.1.9 "**ECP Compliance Rules**" mean the rules, including a list of approved outputs, described in (i) Exhibit D of the Agreement as amended by Exhibit ECP_D of this Addendum and (ii) Exhibit ECP_C of this Addendum hereto which apply to ECP Devices and generally serve to prevent unauthorized distribution or copying of Controlled Content and ECP Controlled Content.

1.1.10 "**ECP Controlled Content**" means 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. **Note:** Audio content is not ECP Controlled Content.

1.1.11 "**ECP Device"** means any ECP Host or ECP Module hereunder.

1.1.12 "**ECP Device Type**" means a Device Type based on the CI Plus ECP Specifications, ECP Compliance Rules and ECP Robustness Rules.

1.1.13 "**ECP Host"** means any Host as defined by the CI Plus ECP Specification.

1.1.14 "**ECP Module"** or **"ECP CICAM"** means any CICAM as defined by the CI Plus ECP Specification.

1.1.15 "**ECP Registered Device**" means a Registered Device that belongs to an ECP Device Type.

1.1.16 **"ECP Robustness Checklist**" means the checklist as defined in Exhibit ECP_G of this Addendum.

1.1.17 "**ECP Robustness Rules**" means the rules described in Exhibit ECP_B of this Addendum which apply to ECP Devices and serve to resist attempts to modify ECP Devices to defeat the security of Controlled Content including ECP Controlled Content provided by the CI Plus ECP Specification or the ECP Compliance Rules.

1.1.18 "**Standard Compliance Rules**" mean the rules, including a list of approved outputs, described in Exhibit C and Exhibit D of the Agreement which apply to Standard Devices and generally serve to prevent unauthorized distribution or copying of Controlled Content that is not ECP Controlled Content.

1.1.19 "**Standard Device"** means any Standard Host or Standard Module hereunder.

1.1.20 "**Standard Device Type"** means a Device Type based on CI Plus Standard Specification, Standard Compliance Rules and Standard Robustness Rules.

1.1.21 "**Standard Host**" means any Host, as defined by the CI Plus Standard Specification, that is not an ECP Host.

1.1.22 "**Standard Module**" or "**Standard CICAM**" means any CICAM as defined by the CI Plus Standard Specification, that is not a ECP CICAM.

1.1.23 "**Standard Robustness Checklist**" means the Checklist as defined in Exhibit G of the Agreement.

1.1.24 "**Standard Robustness Rules**" means the rules described in Exhibit B of the Agreement which apply to Standard Devices and serve to resist attempts to modify Standard Devices to defeat the security of Controlled Content that is not ECP Controlled Content.

1.2 The following definitions of the Agreement shall be amended as follows:

1.2.1 Section 1.11 "**CI Plus Specification**" shall be deleted in its entirety and replaced with the following:

> **1.11 "CI Plus Specification"** means the CI Plus Standard Specification and the CI Plus ECP Specification.

1.2.2 Section 1.13 "**Compliance Rules**" shall be deleted in its entirety and replaced with the following:

> **1.13 "Compliance Rules"** means the Standard Compliance Rules and the ECP Compliance Rules.

1.2.3 Section 1.44 "**Robustness Rules**" shall be deleted in its entirety and replaced with the following:

> **1.44 "Robustness Rules"** means the Standard Robustness Rules and the ECP Robustness Rules.

1.3 Agreement

The following subsections of the Agreement shall be amended or replaced, as applicable, as follows:

1.3.1 Section 10.2 "**Termination by CI Plus LLP of Agreement for Cause**" shall be deleted in its entirety and replaced with the following:

> **"10.2 Termination by CI Plus LLP of Agreement for Cause**. CI Plus LLP may, upon notice to Named Licensee, terminate this Agreement in whole or in part in the event that:
> (a) Named Licensee commits, or
> (b) where a Licensee is an Affiliate of Named Licensee, that Licensee is deemed to have committed (by way of Named Licensee's failure to procure that Affiliate's compliance with the following named Sections),

a material breach of any term, representation, warranty or covenant set forth in Section 2.0, 4.0, 5.0, 8.0, 9.0 or 11.0 of the Agreement hereto and: (i) if the breach is curable, such breach remains uncured forty-five (45) Business Days following the date of Named Licensee's receipt of written notice of such material breach from CI Plus LLP; or (ii) such breach cannot be cured. Termination of the Agreement in whole or in part shall have the effect of De-Registration for all Registered Devices of Standard Device Type and/or ECP Device Type, as required by CI Plus LLP in writing. CI Plus LLP shall not invoke the right of Termination under this Section 10.2 in response to cases of Material Breach which can be identified with a particular Registered Device, where De-Registration and/or Revocation of affected Registered Device alone, as per Section 15.3.1, would be a sufficient or more proportionate remedy."

1.3.2 Section 10.5 "**Survival**" shall be deleted in its entirety and replaced with the following:

"10.5 Survival. Termination or expiration of this Agreement will not relieve either party from fulfilling its obligations that by their terms or nature survive termination or expiration, including, but not limited to Sections 1.0, 2.5 (to the extent that the Named Licensee shall procure its Affiliates' compliance with the other surviving Sections noted in this Section 10.5, 7.0, 9.0, 10.0, 11.0, 12.0, 13.0, 14.0, and 15.0 and 16.0. In addition, Exhibits B, C, D, ECP_B, ECP_C and ECP_D shall survive any termination of this Agreement with respect to products that are both Registered and distributed under this Agreement. For the avoidance of doubt, the warranty, license or obligation to grant a license under Section 7.0 shall survive termination or expiration of this Agreement only in respect of (i) the version of the Specifications in effect at the date of such termination or expiration and (ii) Necessary Claims having a filing date on or before such termination or expiration; provided that the warranty under Section 7.1 shall not survive for a particular Device Type or Licensee, as the case may be, if this Agreement is terminated in accordance with Sections 10.2 or 10.3"

1.4 Device Type

The following subsections of the Agreement shall be amended as follows:

1.4.1 Section 1.2 "**All Licensed Products**" shall be amended by replacing all occurrences of "Device Type" with "Standard Device Type or ECP Device Type".

1.4.2 Section 1.16 "**De-Registration**" shall be amended by replacing all occurrences of "Device Type" with "Standard Device Type or ECP Device Type".

1.4.3 Section 1.29 "**Licensed Product**" shall be amended by replacing all occurrences of "Device Type" with "Standard Device Type or ECP Device Type".

1.4.4 Section 1.39 "**Registered**" shall be amended by replacing all occurrences of "Device Type" with "Standard Device Type or ECP Device Type".

1.4.5 Section 1.40 "**Registered Device**" shall be amended by replacing all occurrences of "Device Type" with "Standard Device Type or ECP Device Type".

1.4.6 Section 1.41 "**Registration**" shall be amended by replacing all occurrences of "Device Type" with "Standard Device Type or ECP Device Type".

1.5 Compliance Rules.

The following subsections of the Agreement shall be amended as follows:

1.5.1 Exhibit C of the Agreement shall be renamed to "Compliance Rules for Standard Host Devices".

1.5.2 Section 1.2 "**All Licensed Products**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.3 Section 1.28 "**Licensed Component**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.4 Section 1.29 "**Licensed Product**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.5 Section 1.41 "**Registration**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.6 Section 1.47 "**Test Partners**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.7 Section 2.4 "**Limitation on All Licenses**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.8 Section 5.2 "**Host Self-Test Registration status**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.9 Section 10.4 "**Effect of termination**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.10 Section 11.2 "**Licensee**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.11 Section 15.3.2.1 "**Criteria for Revocation**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.12 Section 15.3.2.2 "**Criteria for De-Registration**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.13 Section 16.7 "**Product Audit**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.14 Exhibit A "**Device Type**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.5.15 Exhibit B "**Robustness Rules for Standard Devices**" shall be amended by replacing all occurrences of "Compliance Rules" with "Standard Compliance Rules".

1.5.16 Exhibit C "**Compliance Rules for Standard Host Devices**" shall be amended by replacing all occurrences of "Compliance Rules" and "Compliance Rules for Host Devices" with "Compliance Rules for Standard Host Devices".

1.5.17 Exhibit G "**Robustness Checklist for Standard Devices**" shall be amended by replacing all occurrences of "Compliance Rules" with "Standard Compliance Rules".

1.5.18 Exhibit J "**Registration Procedure**" shall be amended by replacing all occurrences of "Compliance Rules" with "Applicable Compliance Rules".

1.6 Robustness Rules.

The following subsections of the Agreement shall be amended as follows:

1.6.1 Exhibit B of the Agreement shall be renamed to "Robustness Rules for Standard Devices".

1.6.2 Section 1.2 "**All Licensed Products**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.3 Section 1.28 "**Licensed Component**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.4 Section 1.29 "**Licensed Product**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.5 Section 1.41 "**Registration**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.6 Section 1.47 "**Test Partners**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.7 Section 2.4 "**Limitation on All Licenses**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.8 Section 5.2 "**Host Self-Test Registration status**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.9 Section 10.4 "**Effect of termination**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.10 Section 11.2 "**Licensee**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.11 Section 15.3.2.1 "**Criteria for Revocation**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.12 Section 15.3.2.2 "**Criteria for De-Registration**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.13 Section 16.6.1 shall be amended by replacing all occurrences of "applicable Robustness Rules" with "Applicable Robustness Rules".

1.6.14 Section 16.7 "**Product Audit**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.15 Exhibit A "**Device Type**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.6.16 Exhibit B "**Robustness Rules**" shall be amended by replacing all occurrences of "Robustness Rules" with "Standard Robustness Rules".

1.6.17 Exhibit C "**Compliance Rules for Standard Host Devices**" shall be amended by replacing all occurrences of "Exhibit B, Robustness Rules" with "Exhibit B, Robustness Rules for Standard Devices".

1.6.18 Exhibit C "**Compliance Rules for Standard Host Devices**" shall be amended by replacing all occurrences of "Robustness Rules" with "Standard Robustness Rules".

1.6.19 Exhibit D "**Compliance Rules for CICAM Devices**" shall be amended by replacing all occurrences of "Exhibit B, Robustness Rules" with "the Applicable Robustness Rules".

1.6.20 Exhibit G "**Robustness Checklist for Standard Devices**" shall be amended by replacing all occurrences of "Robustness Rules" with "Standard Robustness Rules".

1.6.21 Exhibit J "**Registration Procedure**" shall be amended by replacing all occurrences of "Robustness Rules" with "Applicable Robustness Rules".

1.7 CI Plus Specification.

The following subsections of the Agreement shall be amended as follows:

1.7.1 Section 4.0 "**CHANGE OF VERSION**" of Exhibit C "**Compliance Rules for Host Devices**" shall be amended by replacing all occurrences of "CI Plus Specification" with "Applicable CI Plus Specification".

1.7.2 Section 6.0 "**CHANGE OF VERSION**" of Exhibit D "**Compliance Rules for CICAM Devices**" shall be amended by replacing all occurrences of "CI Plus Specification" with "Applicable CI Plus Specification".

1.7.3 Exhibit G "**Robustness Checklist for Standard Devices**" shall be amended by replacing all occurrences of "CI Plus Specification" with "Applicable CI Plus Specification".

1.8 Specifications.

The following subsections of the Agreement shall be amended as follows:

1.8.1 Section 1.2 "**All Licensed Products**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.2 Section 1.28 "**Licensed Component**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.3 Section 1.29 "**Licensed Component**" shall be amended by replacing all occurrences of "applicable Specifications" with "Applicable Specifications".

1.8.4 Section 1.41 "**Registration**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.5 Section 1.47 "**Test Partners**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.6 Section 2.4 "**Limitation on All Licenses**" shall be amended by replacing the first occurrence of "Specifications" with "Applicable Specifications".

1.8.7 Section 5.2 "**Host Self-Test Registration status**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.8 Section 10.4 "**Effect of termination**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.9 Section 11.2 "**Licensee**" shall be amended by replacing all occurrences of "applicable Specifications" and "Specifications" with "Applicable Specifications".

1.8.10 Section 15.3.2.1 "**Criteria for Revocation**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.11 Section 15.3.2.2 "**Criteria for De-Registration**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.12 Section 16.7 "**Product Audit**" shall be amended by replacing all occurrences of all occurrences of "Specifications" with "Applicable Specifications".

1.8.13 Exhibit A "**Device Type**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.8.14 Exhibit B "**Robustness Rules for Standard Devices**" shall be amended by replacing all occurrences of all occurrences of "Specifications" with "Applicable Specifications".

1.8.15 Exhibit G "**Robustness Checklist for Standard Devices**" shall be amended by replacing all occurrences of all occurrences of "Specifications" with "Applicable Specifications".

1.8.16 Exhibit J "**Registration Procedure**" shall be amended by replacing all occurrences of "Specifications" with "Applicable Specifications".

1.9 Robustness Checklist.

The following subsections of the Agreement shall be amended as follows:

1.9.1 Exhibit G of the Agreement shall be renamed to "Robustness Checklist for Standard Devices".

1.9.2 Exhibit G **"Robustness Checklist for Standard Devices"** shall be amended by replacing all occurrences of "Robustness Rules checklist" with "Robustness Checklist for Standard Devices".

1.10 Registration Procedure.

The following subsections of the Agreement shall be amended as follows:

1.10.1 Exhibit J "**Registration Procedure**" shall be amended by replacing:

> "Having completed an agreement with a Test Partner, Licensee may submit a Device and a completed checklist for such Device attached as Exhibit G of this Agreement ("Robustness Checklist") to a Test Partner as a new Device Type for testing."

With:

> "Having completed an agreement with a Test Partner, Licensee may submit a Device and a completed Applicable Robustness Checklist for such Device to a Test Partner as a new Device Type for testing."

1.10.2 Exhibit J "**Registration Procedure**" shall be amended by replacing all occurrences of "Robustness Checklist" with "Applicable Robustness Checklist".

1.11 Host Self-Test Registration status.

The following subsection of the Agreement shall be amended as follows:

1.11.1 Section 5.2 "**Host Self-Test Registration status**" shall be amended to add the following:

> "Notwithstanding the above, a Licensee who otherwise has Host Self-Test Registration status may choose Self-Test Registration for ECP Hosts only if either (i) an ECP Host was one of the two successful Normal Registrations which resulted in the Host Self-Test Registration status being obtained, or (ii) at least one ECP Host has been successfully registered through Normal Registration during the Host Self-Test Registration status period.[Note: A Licensee must complete a minimum of one Normal Registration of an ECP Host in order to be eligible for Host Self-Test Registration status of an ECP Host during a period when Licensee has Host Self-Test Registration status as defined in Section 5.2 of the CI Plus ILA. If the Licensee allows their Host Self-Test Registration status to expire, then Licensee must again complete a minimum of one Normal Registration of an ECP Host to obtain Host Self-Test Registration status for ECP Hosts in a new period of Host Self-Test Registration status.]"

1.12 Scope of Changes.

Section 6.1 of the Agreement "**Scope of Changes**" shall be deleted in its entirety and replaced with the following:

6.1 Scope of Changes.

This Section 6.0 applies to changes in the following (collectively, "Changes"):

6.1.1 Device Type (Exhibit A of the Agreement);
6.1.2 Robustness Rules for Standard Devices (Exhibit B of the Agreement);
6.1.3 Compliance Rules for Standard Host Devices (Exhibit C of the Agreement);
6.1.4 Compliance Rules for CICAM Devices (Exhibit D of the Agreement);
6.1.5 URI Mapping Table (Exhibit E of the Agreement);
6.1.6 Robustness Checklist for Standard Devices (Exhibit G of the Agreement);
6.1.7 Registration Procedure (Exhibit J of the Agreement);
6.1.8 Revocation Procedure (Exhibit L of the Agreement)
6.1.9 Robustness Rules for ECP Devices (Exhibit ECP_B of the Agreement);
6.1.10 Compliance Rules for ECP Host Devices (Exhibit ECP_C of the Agreement);
6.1.11 Additional Compliance Rules for ECP CICAM Devices (Exhibit ECP_D of the Agreement);
6.1.12 URI Mapping Table for ECP (Exhibit ECP_E of the Agreement);
6.1.13 Robustness Checklist for ECP Devices (Exhibit ECP_G of the Agreement); and
6.1.14 Specifications

1.13 Exhibit A – Device Types

Exhibit A of the Agreement shall be amended by adding the following paragraph after the final paragraph:

"For the avoidance of doubt, a Standard Device cannot be considered as a derivative of an ECP Device. Likewise, an ECP Device cannot be considered as a derivative of a Standard Device."

1.14 Exhibits ECP_B – ECP_G

The Agreement shall be amended by adding Exhibits ECP_B – ECP_G of this Addendum as Exhibits ECP_B – ECP_G of the Agreement.

1.15 Miscellaneous.

Section 2.2 of the Agreement "**Commercial Use**" shall be amended to add the following:

"For avoidance of doubt, Licensed Component implementing CI Plus ECP Specification shall not be distributed to Fellow Licensees that has not signed an agreement equivalent to this Agreement"

2.0 CONTINUITY

2.1 The provisions of the Agreement shall, save as amended in this Addendum, continue in full force and effect, and shall be read and construed as one document with this Addendum.

3.0 MISCELLANEOUS

3.1 The provisions of clauses 16.8 (Law & Jurisdiction), 16.12 (Amendments), 16.14 (Severability) and 16.19 (Third Party Rights) of the Agreement shall apply to this Addendum, as if set out in full and so that references in those provisions to "this agreement" shall be construed as references to this Addendum and references to "party" or "parties" shall be construed as references to parties to this Addendum.

LIST OF EXHIBITS

Exhibit ECP_A: [Intentionally left blank]
Exhibit ECP_B: Robustness Rules for ECP Devices version 1.4, issued January 1st, 2021
Exhibit ECP_C: Compliance Rules for ECP Host Devices version 1.2, issued January 1st 2021
Exhibit ECP_D: Additional Compliance Rules for ECP CICAM Devices version 1.0, issued May 31st, 2018
Exhibit ECP_E: URI Mapping Table for ECP version 1.2, issued January 1st 2021
Exhibit ECP_F: [Intentionally left blank]
Exhibit ECP_G: Robustness Checklist for ECP Devices version 1.0, issued May 31st, 2018

Remainder of this page intentionally left blank.

Exhibit ECP_B: Robustness Rules for ECP Devices

Version 1.4

Note: The terms of this Exhibit ECP_B do not apply with respect to Prototypes or Licensed Components.
Note: The terms of this Exhibit ECP_B apply to ECP Host devices and ECP CICAM devices.

1.0 Definitions.

1.1 "Certificates" means the Root certificate, Brand certificate and Device certificate as described in the Specifications.

1.2 "CI Plus 2nd RoT Secret Values" means (i) Device Keys and Protocol Secrets obtained from the CI Plus 2nd Root of Trust and (ii) Content Keys and Intermediate Keys as generated when the CI Plus 2nd Root of Trust is selected.

1.3 "CI Plus 2nd RoT Trust Values" means (i) Certificates obtained from the CI Plus 2nd Root of Trust, (ii) Revocation Information associated with the CI Plus 2nd Root of Trust, (iii) Critical Security Update Version of the software that implements the ECP Protection Functions and (iv) SRM.

1.4 "CI Plus ECP Trusted Boundary" means the set of hardware and software that implements the ECP Protection Functions and the ECP Controlled Content Path, and may implement the Standard Protection Functions. The CI Plus ECP Trusted Boundary only makes use of code which (i) has been authenticated and integrity checked by a Secure Boot, (ii) has been approved by the Manufacturer of the Licensed Product, and (iii) runs in a Trusted Executed Environment. Software running in the Trusted Execution Environment and implementing functions other than the ECP Protection Functions or the ECP Controlled Content Path or Standard Protection Functions is not part of the CI Plus ECP Trusted Boundary.

1.5 "CI Plus RoT Secret Values" means (i) Device Keys and Protocol Secrets obtained from the CI Plus Root of Trust and (ii) Content Keys and Intermediate Keys as generated when the CI Plus Root of Trust is selected.

1.6 "CI Plus RoT Trust Values" means (i) Certificates obtained from the CI Plus Root of Trust, (ii) Revocation Information associated with the CI Plus Root of Trust and (iii) Critical Security Update Version of the software that implements the Standard Protection Functions.

1.7 "Content Keys" means CCK and CIV as described in the Specifications.

1.8 "Device Keys" means MDQ and HDQ as described in the Specifications.

1.9 "ECP Controlled Content Path" means internal non-persistent or transitory transmissions, processing and transformation of ECP Controlled Content for the purpose of immediate display or output as specified in Exhibit ECP_C.

1.10 "ECP Protection Functions" means functions related to the protection of ECP Controlled Content, including but not limited to (i) authentication using CI Plus 2nd Root of Trust credentials, (ii) encryption, (iii) decryption, (iv) revocation as defined in the Specifications and using CI Plus 2nd Root of Trust credentials, (v) enforcement of the ECP Compliance Rules, (vi) maintaining the authenticity of CI Plus 2nd RoT Trust Values, and (vii) maintaining the authenticity and secrecy of CI Plus 2nd RoT Secret Values.

1.11 "Intermediate Keys" means DHX, DHY, DHSK, SEK, SAK, and Kp, as described in the Specifications.

1.12 "Professional Tools" means professional tools or equipment (excluding Circumvention Devices and professional tools or equipment that are made available only on the basis of a non-disclosure agreement), such as chip disassembly systems, or in-circuit emulators or other tools, equipment, methods or techniques not included in the definition of Widely Available Tools and Specialized Tools.

1.13 "Protocol Secrets" means all numerical, algorithmic and implementation secrets in the CI Plus License Specification, and the credentials marked as both 'license constant' and 'keep local' in the CI Plus Specification Version 1.3 Table 5.2.

1.14 "Revocation Information" means the Revocation Signalling Data (RSD) version number, RSD transmission time out, RSD detection on/off state, Root of Trust identification and the service operator identity (as defined in the Specifications) provided by the CA System.

1.15 "Secure Boot" means a boot process whereby each component must authenticate and check the integrity of the component that follows it before transferring control to it. This must continue in an uncircumvented and unbroken chain until (i) all software implemented in the CI Plus ECP Trusted Boundary and (ii) all software affecting ECP Controlled Content security has been loaded in the Trusted Execution Environment. The root of this trust shall be securely provisioned in hardware, e.g. permanently factory burned.

1.16 "Secure Storage" means a local and persistent storage that protects data in a form encrypted uniquely for the device. The encryption must be rooted in a securely provisioned, secret, immutable, device-unique value with at least 128 bits of entropy.

1.17 "Specialized Tools" means specialized electronic tools or specialized software tools that are widely available at a reasonable price, EEPROM readers and writers, debuggers, de-compilers, integrated development environments and similar software development products, other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required (Circumvention Devices).

1.18 "Standard Protection Functions" means functions related to the protection of Controlled Content that is not ECP Controlled Content, including but not limited to (i) authentication using CI Plus Root of Trust credentials, (ii) encryption, (iii) decryption, (iv) revocation as defined in the Specifications and using CI Plus Root of Trust credentials, (v) enforcement of the Standard Compliance Rules, (vi) maintaining the authenticity of CI Plus RoT Trust Values, (vii) maintaining the authenticity and secrecy of CI Plus RoT Secret Values and (viii) Overt Watermarking for Controlled Content and for ECP Controlled Content.

1.19 "Trusted Execution Environment" (TEE) means a processing environment on a device that, using hardware enforcement, prevents unauthorized hardware and software from discovering, modifying or interfering with its code and data.

1.20 "Widely Available Tools" means general purpose tools or equipment that are widely available at a reasonable price, such as screw drivers, jumpers, clips, file editors, and soldering irons, other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required (Circumvention Devices).

2.0 Construction.

2.1 Generally. The Licensed Product as shipped shall contain a CI Plus ECP Trusted Boundary.

Software and software updates for the CI Plus ECP Trusted Boundary of the Licensed Product shall remain under control of the Manufacturer of said Licensed Product.

If part of the Standard Protection Functions is implemented outside the CI Plus ECP Trusted Boundary, then Firmware and firmware updates for the Licensed Product shall remain under control of the Manufacturer of said Licensed Product. Under no circumstances shall it be possible for the consumer to add arbitrary binary applications to the Licensed Product except when said application is i) approved by the Manufacturer or ii) application isolation from the Standard Protection Functions is provided.

The ECP Protection Functions and Standard Protection Functions running in a Trusted Execution Environment being part of the CI Plus ECP Trusted Boundary should be isolated from other software running in the Trusted Execution Environment.

2.2 Defeating Functions. Licensed Products shall not include:
(a) switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing; or

(b) Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions; or

(c) special functions or modes of operation (including service menus or remote-control functions);

in each case
(i) by which an ECP Protection Function can be defeated,
(ii) by which a Standard Protection Function can be defeated,
(iii) by which a CI Plus 2nd RoT Trust Value can be modified,
(iv) by which a CI Plus RoT Trust Value can be modified,
(v) by which a CI Plus 2nd RoT Secret Value can be modified or revealed,
(vi) by which a CI Plus RoT Secret Value can be modified or revealed,
(vii) by which ECP Controlled Content can be exposed to unauthorized access, copying, redistribution, or modification of user rights,
(viii) by which Controlled Content can be exposed to unauthorized access, copying, redistribution, or modification of user rights
(ix) by which the protection provided by the CI Plus ECP Trusted Boundary can be defeated,
(x) by which the ECP Compliance Rules can be defeated,
in each case other than as permitted under this License Agreement.

This Section 2.2 does not prohibit the licensed manufacturer from designing and manufacturing its products incorporating means used to analyse or repair products provided that such means do not cause the products to be non-compliant with the ECP Compliance Rules and this Exhibit ECP_B.

2.3 Keep Secret.

When the Licensed Product has to store CI Plus 2nd RoT Secret Values outside the CI Plus ECP Trusted Boundary, the Licensed Product shall make use of a Secure Storage. The Secure Storage shall be designed in a way that prevents CI Plus 2nd RoT Secret Values from being revealed outside of the CI Plus ECP Trusted Boundary. CI Plus 2nd RoT Secret Values in non-encrypted form shall only reside within the CI Plus ECP Trusted Boundary.

2.4 ECP Controlled Content Paths.

Licensed Product shall not make available ECP Controlled Content on outputs other than those specified in the Compliance Rules as defined in Exhibit ECP_C, and within such Licensed Product, both compressed and uncompressed ECP Controlled Content in non-encrypted form shall not be present outside the CI Plus ECP Trusted Boundary.

3.0 Level of Protection.

3.1 The **Trusted Execution Environment** shall be implemented, at a minimum, in a way that it:

- **(i)** Cannot be reasonably foreseen to be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary,
- **(ii)** Can only with difficulty be defeated or circumvented using Professional Tools, and
- **(iii)** Cannot be reasonably foreseen to be defeated or circumvented due to a transition of power state, whether authorized or unauthorized.

3.2 The **Secure Boot process** shall be implemented, at a minimum, in a way that:

- **(i)** It cannot be modified merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary,
- **(ii)** It can only with difficulty be modified using Professional Tools, and
- **(iii)** Compromise for one Device Type cannot be directly exploitable on another Device Type.

3.3 The **CI Plus 2nd RoT Trust Values** shall be protected, at a minimum, in a way that they:

- **(i)** Cannot be modified merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary, and
- **(ii)** Can only with difficulty be modified using Professional Tools.

3.4 The **CI Plus 2nd RoT Secret Values** shall be protected, at a minimum, in a way that they:

- **(i)** Cannot be modified or discovered merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary, and
- **(ii)** Can only with difficulty be modified or discovered using Professional Tools.

3.5 The **Secure Storage** shall be implemented, at a minimum, in a way that it:

- **(i)** Cannot be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary, and

(ii) Can only with difficulty be defeated or circumvented using Professional Tools

3.6 The **CI Plus ECP Trusted Boundary** shall be implemented, at a minimum, in a way that it:

(i) Cannot be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary, and

(ii) Can only with difficulty be defeated or circumvented using Professional Tools

3.7 The **Debug Functions** shall be implemented, at a minimum, in a way that they:

(i) Cannot undergo unauthorized activation merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary, and

(ii) Can undergo unauthorized activation only with difficulty using Professional Tools

3.8 The **ECP Protection Functions** shall be implemented, at a minimum, in a way that they cannot be modified merely by using any hardware or software being part of the Licensed Product but not being part of the CI Plus ECP Trusted Boundary.

3.9 **Controlled Content that is not ECP Controlled Content** shall be protected, at a minimum, under the terms of Exhibit B of the Agreement or may be protected to the same level as defined for ECP Controlled Content in this Exhibit ECP_B.

3.10 The **CI Plus RoT Secret Values** shall be protected, at a minimum, under the terms of Exhibit B of the Agreement or may be protected to the same level as defined for CI Plus 2nd RoT Secret Values in this Exhibit ECP_B.

3.11 The **CI Plus RoT Trust Values** shall be protected, at a minimum, under the terms of Exhibit B of the Agreement or may be protected to the same level as defined for CI Plus 2nd RoT Trust Values in this Exhibit ECP_B.

3.12 The **Standard Protection Functions** shall be implemented, at a minimum, under the terms of Exhibit B of the Agreement or may be implemented as defined for ECP Protection Functions in this Exhibit ECP_B.

3.13 The ECP Robustness Rules as described in this Exhibit ECP_B are applicable to all the CI Plus Interface(s) over which the Host implements CI Plus.

4.0 Advance of Technology.

Although an implementation of a Licensed Product when designed and shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such product to fail to comply with this Exhibit ECP_B ("New Circumstances"). If Licensee has (a) actual Notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as "Notice"), then within eighteen months after Notice Licensee shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with this Exhibit ECP_B in view of the then-current circumstances.

5.0 Documents and Robustness Checklist for ECP Devices.

5.1 Before releasing any Licensed Product, Licensee must assure compliance with this Exhibit ECP_B. A Robustness Checklist for ECP Devices is attached as Exhibit ECP_G for the purpose of assisting Licensee in performing tests covering certain important aspects of this Exhibit ECP_B. Inasmuch as the Robustness Checklist for ECP Devices does not address all elements required for the manufacture of a compliant product, Licensee is strongly advised to carefully review the Specifications, the Agreement, the ECP Compliance Rules and this Exhibit ECP_B so as to evaluate thoroughly the compliance of its Licensed Products.

5.2 Licensee specifically acknowledges and agrees that it must provide copies of the Specifications, the ECP Compliance Rules, this Exhibit ECP_B, and the Robustness Checklist for ECP Devices as defined in Exhibit ECP_G to its responsible supervisors of product design and manufacture in such manner and at such times as to effectively induce compliance with such materials and completion of the ECP Robustness Checklist.

5.3 Licensee specifically acknowledges and agrees that it should prepare a package of records or other necessary materials for independent expert security review. This package must not be submitted for certification but should be prepared prior to Device Registration. This package should contain but not be limited to documentation of the Licensed Product's (i) security analysis, including interpretation of terms "Widely Available Tools", "Specialized Tools", "Professional Tools" and "With difficulty", (ii) implementation security architecture, (iii) detailed design and tests performed.

Remainder of this page intentionally left blank.

Exhibit ECP_C: Compliance Rules for ECP Host Devices
Version 1.2

Note: The terms of this Exhibit ECP_C do not apply with respect to Prototypes or Licensed Components.

Licensed Products must comply with the requirements set forth in this Exhibit and be constructed so as to resist attempts at circumvention of these requirements as specified in Exhibit ECP_B.

Licensor may approve from time to time additional outputs and/or content protection technologies on a reasonable and non-discriminatory basis and add such provisions to this Exhibit. The Change Control is indicated in Exhibit K.

1.0 DEFINITIONS

All capitalized terms not defined or modified in this Exhibit shall have the same meaning as set forth in the Exhibit C of the Agreement.

1.1 "**ECP Constrained Image**" means the visual equivalent of not more than 2,073,600 Pixels per frame (e.g. an image with resolution of 1920 horizontal pixels by 1080 vertical pixels for a 16:9 aspect ratio). An ECP Constrained Image can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

1.2 "**Image Constraint Trigger**" or "**ICT**" means the field or bits, as described in the CI Plus Specification, used to trigger the output of a "ECP Constrained Image" in the Output of Licensed Products.

2.0 OUTPUTS

Refer to Exhibit E for URI interpretation when outputting Controlled Content that is not ECP Controlled Content under this Section 2.0.
Refer to Exhibit ECP_E for URI interpretation when outputting ECP Controlled Content under this Section 2.0.

2.1 General. For output of Controlled Content that is not ECP Controlled Content, Licensed Product shall be compliant with the compliance rules defined in Section 2.0 of Exhibit C. Licensed Product shall not output ECP Controlled Content to any output, except as permitted in this Section 2.0. For purposes of this Exhibit ECP_C, an output shall be deemed to include, but not be limited to, any transmissions to any internal copying, recording, or storage device, but shall not include internal non-persistent or transitory transmissions that otherwise satisfy the ECP Robustness Rules.

For avoidance of doubt: Licensed Products are permitted to implement the instructions provided by the URI bits by ensuring that either:

i) ECP Controlled Content is only sent to an output or to storage when this offers adequate protection in the context of this Exhibit, e.g. depending on the state of the URI bits, resolution or other parameters, or:
ii) ECP Controlled Content is not sent to an output or storage.

Licensees are recommended to consider how such behaviour is adequately communicated to the end-user.

2.2 Digital Outputs. Licensed Product with any digital outputs shall only output ECP Controlled Content as permitted by this Section 2.2.

2.2.1 Interface with HDCP. Licensed Product may output ECP Controlled Content to any wired or wireless interface including HDMI, Wi-Fi, Ethernet and USB output in digital form where such output is protected by HDCP 1.X or HDCP 2.X (collectively, "HDCP"), as permitted in accordance with Exhibit ECP_E, licensed by Digital Content Protection LLC, and where HDCP is always active on that interface.
Licensed Product must pass all validly received HDCP SRM, if any, from CICAM to HDCP function.
Capitalized terms used in this Section, but not otherwise defined in this Exhibit ECP_C or the Agreement, shall have the meaning set forth in the HDCP Specification, HDCP License Agreement or the HDCP Addendum to HDCP License Agreement.
The Licensed products shall not deliberately interfere with SRM that may have been received directly from RF broadcast and shall make reasonable efforts to avoid such interference.

2.2.2 DTCP-IP. Licensed Product may pass ECP Controlled Content in digital form where such output is protected by DTCP-IP, as permitted by Exhibit ECP_E.

- Capitalized terms used in this Section, but not otherwise defined in this Exhibit ECP_C or the Agreement, shall have the meaning set forth in the DTCP specification or the DTCP Adopter Agreement.

- When so outputting or passing such content to a DTCP-IP output, the Licensed Product is required to:

  i) map EMI settings from CI Plus URI to the DTCP Encryption Mode Indicator; and
  ii) map URI settings APS, ICT, RCT and DOT as defined in the CI Plus Specification into DTCP Analogue Protection System (APS) signalling, DTCP Image Constraint Token (ICT), DTCP Encryption Plus Non-assertion (EPN), and DTCP Digital Only Token (DOT) signalling in accordance with section 5.7 of the CI Plus Specification Version 1.3.

- Licensed Product must pass all validly received DTCP-IP SRM, if any, from CICAM to DTCP-IP function.

- The Licensed products shall not deliberately interfere with SRM that may have been received directly from RF broadcast and shall make reasonable efforts to avoid such interference.

3.0 COPYING, RECORDING, AND STORAGE OF ECP CONTROLLED CONTENT

3.1 General. Licensed Products, including, without limitation, Licensed Products with inherent or integrated copying, recording or storage capability, shall not copy, record, or store Controlled Content that is not ECP Controlled Content, except as permitted in Section 3.0 of Exhibit C of the Agreement. Licensed Products, including, without limitation, Licensed Products with inherent or integrated copying, recording or storage capability, shall not copy, record, or store ECP Controlled Content, except as permitted in Section 3.0 of Exhibit C of the Agreement and as further constrained below.

3.2 Copy Never. Licensed Products, including, without limitation, such a device with integrated recording capability such as a so-called "personal video recorder", shall not copy ECP Controlled Content that is designated in the EMI bits as never to be copied ("copy never") except as permitted in Section 3.2 of Exhibit C of the Agreement and by the following:

3.2.1 Storage: Without further authorisation, a Secure Storage Licensed Product may, if the ECI bits are set to values other than b101 and b111, store ECP Controlled Content, including for the purpose of pausing, as to which Copy Never control has been asserted for the duration up to the Retention Limit from initial transmission and obliterate or render unusable the stored content after stated period of time (e.g. frame-by-frame, minute-by-minute, megabyte by megabyte, etc.), but in no event shall such unit of data exceed one minute of a Program.

3.2.2 Title Diversity: ECP Controlled Content that has been stored/paused, shall be stored in a manner which is encrypted in a manner that provides no less security than 128-bit Advanced Encryption Standard ("AES"). The stored ECP Controlled Content shall be securely bound to the Licensed Product doing the recording so that it is not removable in a usable form therefrom and is not itself subject to further temporary or other recording within the Licensed Product before it is rendered unusable. The manner of encryption shall be changed at the start of every recording (e.g. by changing the encryption key).

3.3 Removable Storage

Refer to Exhibit ECP_E for URI interpretation when recording ECP Controlled Content under this Section 3.3.

3.3.1 A Secure Storage Licensed Product may use a user accessible digital interface to store ECP Controlled Content on a Secure Storage Product, if: (a) the ECP Controlled Content is encrypted across the interface, and in storage, with an encryption algorithm that provides no less security than 128-bit Advanced Encryption Standard ("AES"); (b) the ECP Controlled Content is uniquely cryptographically associated with the original Secure Storage Licensed Product connected to the Secure Storage Product, such that ECP Controlled Content is unusable to any other product or device; (c) the interface and Secure Storage Product, or the system architecture, provides protection from a "disk cloning attack"; (d) no key information is stored on the Secure Storage Product unless encrypted with security no less than AES (128 bit); and (e) the Move, storage and copying of ECP Controlled Content otherwise meets the criteria set forth in the Exhibit ECP_B and this Exhibit.

3.4 No Waiver. Licensee acknowledges that the provisions of this Section 3.0 are not a waiver or license of any copyright interest or an admission of the existence or non-existence of a copyright interest.

4.0 CHANGE OF VERSION

Refer to Section 4.0 of Exhibit C of the Agreement.

5.0 CHANGE OF CI PLUS INTERFACE

Refer to Section 5.0 of Exhibit C of the Agreement.

Remainder of this page intentionally left blank.

Exhibit ECP_D: Additional Compliance Rules for ECP CICAM Devices
Version 1.0

Note: The terms of this Exhibit ECP_D do not apply with respect to Prototypes or Licensed Components.

Licensed CICAM Products shall comply with the requirements set forth in this Exhibit and Exhibit D and be constructed so as to resist attempts at circumvention of these requirements as specified in Exhibit ECP_B.

1.0 DEFINITIONS

There are no new definitions added by this Exhibit.

2.0 CI PLUS SPECIFIC REQUIREMENTS

2.1 ECI bit signalling. The Licensed Product may use the ECI bits with other values than 0b000. The Licensed module shall only set the ECI bits based on explicit signalling by the network operator. This implies the module shall not have a default value or be hardwired to set the ECI bits.

Remainder of this page intentionally left blank.

Exhibit ECP_E: URI Mapping Table for ECP
Version 1.2

Input to ECP Host										Internal Retention Limit	Output of content to devices downstream of the ECP Host					
											Digital Output					
	Use case	CA controlled *1	URI *2								HDCP 2.2.or greater		HDCP less than version 2.2		DTCP *5	
			EMI		ECI			ICT			Allowed export	Image constraint	Allowed export	Image constraint	Allowed export	Image constraint
Copy Never	a	1	1	1	0	0	0	0		Note *6						
	b	1	1	1	0	0	0	1								
	c	1	1	1	0	0	1	0		Note *3	Yes	None	Yes	None	Yes	None
	d	1	1	1	0	0	1	1			Yes	None	Yes	None	Yes	None
	e	1	1	1	0	1	0	0			Yes	None	Yes	None	Yes	None
	f	1	1	1	0	1	0	1			Yes	None	Yes	2,074k	Yes	2,074k
	g	1	1	1	0	1	1	0			Yes	None	Yes	None	Yes	None
	h	1	1	1	0	1	1	1			Yes	None	Yes	2,074k	Yes	2,074k
	i	1	1	1	1	0	0	0			Yes	None	Yes	None	No	-
	j	1	1	1	1	0	0	1			Yes	None	Yes	2,074k	No	-
	k	1	1	1	1	0	1	0		Note *4	Yes	None	Yes	None	No	-
	l	1	1	1	1	0	1	1			Yes	None	Yes	2,074k	No	-
	m	1	1	1	1	1	0	0		Note *3	Yes *7	None	No	-	No	-
	n	1	1	1	1	1	0	1			Yes *7	None	No	-	No	-
	o	1	1	1	1	1	1	0		Note *4	Yes *7	None	No	-	No	-
	p	1	1	1	1	1	1	1			Yes *7	None	No	-	No	-

Notes:

1	"CA controlled" means that there are CA descriptors in the CA_PMT and the selected service is processed by the authenticated CICAM
2	All other URI fields shall be interpreted and mapped as per Exhibit E
3	In these cases, the internal Retention Limit shall be interpreted as specified in Exhibit E
4	In these cases, no internal retention is allowed for the ECP Controlled Content
5	Refer to Exhibit E for the mapping of URI to DTCP
6	These cases are not ECP Controlled Content. Refer to Exhibit E
7	In this case, the requirement for HDCP 2.2 or greater shall be enforced on downstream link protection devices setting the HDCP Type to Type 1 Content Stream

Exhibit ECP_G: Robustness Checklist for ECP Devices
Version 1.0

Disclaimer

The Robustness Checklist for ECP Devices is intended as an aid to the correct implementation of the ECP Robustness Rules (Exhibit ECP_B) for implementations of the Applicable Specifications in a Licensed Product. It does not supersede or supplant the Applicable Specifications, ECP Compliance Rules, or ECP Robustness Rules. The Licensee is advised that there are elements of the Applicable Specifications, the ECP Compliance Rules and the ECP Robustness Rules that are not reflected here but that must be complied with.

This Robustness Checklist for ECP Devices shall be completed at each Registration of an ECP Device Type.

Failure to comply with the Applicable Specifications, ECP Compliance Rules and ECP Robustness Rules could result in a breach of the Agreement and legal action taken by the CI Plus LLP or other parties under the Agreement.

1.0 Introduction

In section 2.1 a declaration of compliance is presented. Signing the declaration shall be viewed as a self-declaration of compliance of an ECP Device and that all the following sections are answered truthfully and honestly.

In section 2.0 a checklist for compliance with the Applicable Specifications, ECP Compliance Rules and ECP Robustness Rules is presented. The "CI Plus Robustness Checklist for ECP Devices" may help Licensee validate the implementation against the Applicable Specifications, ECP Compliance Rules and ECP Robustness Rules.

A completed CI Plus Robustness Checklist for ECP Devices shall be provided for the Registration of a new ECP Device Type for a specific brand.

Important: Do not complete this exhibit when submitting the Addendum.

2.0 CI Plus Robustness Checklist for ECP Devices

2.1 Declaration of compliance

Date: _____

Manufacturer / Brand: _____

Product Name: _____

Hardware Model or Software Version: _____

Company Name: _____

Company Address: _____

Print Name(s): _____

Signature(s): _____

2.2 Questions related to general construction of a Licensed product

Question GEN.1.a: (for Hosts only) Have you read the Compliance Rules in Exhibit C and Exhibit ECP_C and the ECP Robustness Rules in Exhibit ECP_B?

Yes / No (please note the versions)

Question GEN.1.b: (for CICAM only) Have you read the Compliance Rules in Exhibit D and Exhibit ECP_D and the ECP Robustness Rules in Exhibit ECP_B?

Yes / No (please note the versions)

Question GEN.2: Does the ECP Device implement the countermeasures in the document *CI Plus ECP Robustness Considerations, Attacks and Countermeasures* where appropriate?

Yes / No

If answered 'No', please describe what you have done to ensure the robustness of the ECP Device against attacks.

Question GEN.3: Has the Licensee prepared a package of records or other necessary materials, as recommended in section 5.3 of Exhibit ECP_B, for independent expert security review?

Yes / No

If answered 'Yes', please describe the content of this package.

Question GEN.4: Will you be able to provide a package of records or other necessary material within 30 calendar days (as required by section 16.7 of the Agreement)?

Yes / No

Question GEN.5.a: (for Hosts only) Does the ECP Device meet the Compliance Rules as defined in Exhibit ECP_C?

Yes / No

Question GEN.5.b: (for CICAM only) Does the ECP Device meet the Compliance Rules as defined in Exhibit D and Exhibit ECP_D?

Yes / No

Question GEN.6: Does the ECP Device contain a CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 2.1)?

Yes / No

Question GEN.7: Is all software and are all software updates for the CI Plus ECP Trusted Boundary of the ECP Device under control of the Manufacturer of said ECP Device (refer to Exhibit ECP_B section 2.1)?

Yes / No

Question GEN.8: Has the ECP Device been designed such that the ECP Protection Functions running in a Trusted Execution Environment being part of the CI Plus ECP Trusted Boundary are isolated from other software not being part of the CI Plus ECP Trusted Boundary but running in the Trusted Execution Environment. (refer to Exhibit ECP_B section 2.1)?

Yes / No

Question GEN.9: Does the ECP Device protect Controlled Content that is not ECP Controlled Content under the terms of Exhibit B or as defined for ECP Controlled in Exhibit ECP_B?

❑ **Exhibit B** ❑ **Exhibit ECP_B**

If answer is Exhibit B then the Licensee shall respond to the questions listed in section 2.11

If answer is Exhibit ECP_B then any question related to ECP Controlled Content shall be interpreted as also applicable to Controlled Content.

Question GEN.10: Does the ECP Device implement the Standard Protection Functions under the terms of Exhibit B or as defined for ECP Protection Functions in Exhibit ECP_B?

❑ **Exhibit B** ❑ **Exhibit ECP_B**

If answer is Exhibit B then the Licensee shall respond to the questions listed in section 2.12

If answer is Exhibit ECP_B then any question related to ECP Protection Functions shall be interpreted as also applicable to Standard Protection Functions.

Question GEN.11: Does the ECP Device protect the CI Plus RoT Secret Values under the terms of Exhibit B of the Agreement or as defined for CI Plus 2nd RoT Secret Values in Exhibit ECP_B (refer to section 3.10 of Exhibit ECP_B)

❑ **Exhibit B** ❑ **Exhibit ECP_B**

If answer is Exhibit B then the Licensee shall respond to the questions listed in section 2.13.

If answer is Exhibit ECP_B then any question related to CI Plus 2nd RoT Secret Values shall be interpreted as also applicable to CI Plus RoT Secret Values.

Question GEN.12: Does the ECP Device protect the CI Plus RoT Trust Values under the terms of Exhibit B of the Agreement or as defined for CI Plus 2nd RoT Trust Values in Exhibit ECP_B (refer to section 3.11 of Exhibit ECP_B)

❑ **Exhibit B** ❑ **Exhibit ECP_B**

If answer is Exhibit B then the Licensee shall respond to the questions listed in section 2.14.

If answer is Exhibit ECP_B then any question related to CI Plus 2nd RoT Trust Values shall be interpreted as also applicable to CI Plus RoT Trust Values.

Question GEN.13: Describe the method of provisioning Keys and Production Credentials during the production of the Licensed Product. Include any preparation steps.

2.3 Questions related to CI Plus ECP Trusted Boundary

Question TB.1: Do you consider all hardware and software implementing the ECP Protection Functions (as defined in Exhibit ECP_B clause 1.10) as being part of the CI Plus ECP Trusted Boundary of the ECP Device?

Yes / No

Question TB.2: Do you consider all hardware and software implementing the ECP Controlled Content Path (as defined in Exhibit ECP_B section 1.9) as being part of the CI Plus ECP Trusted Boundary of the ECP Device?

Yes / No

Question TB.3: Is all code in the CI Plus ECP Trusted Boundary of the ECP Device authenticated and integrity checked before execution (refer to Exhibit ECP_B section 1.4)?

Yes / No

Question TB.4: Can only code approved by you (as the Licensee) be executed in the CI Plus ECP Trusted Boundary of the ECP Device (refer to Exhibit ECP_B section 1.4)?

Yes / No

Question TB.5: Is all code in the CI Plus ECP Trusted Boundary of the ECP Device executed in a Trusted Execution Environment (refer to Exhibit ECP_B section 1.4)?

Yes / No

2.4 Questions related to ECP Protection Functions

Question PF.1: Can you specifically confirm that the set of hardware and software that implements **authentication** using CI Plus 2nd Root of Trust credentials is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

Question PF.2: Can you specifically confirm that the set of hardware and software that implements **encryption relating to the protection of ECP Controlled Content** is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

Question PF.3: Can you specifically confirm that the set of hardware and software that implements **decryption relating to the protection of ECP Controlled Content** is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

Question PF.4: (for CICAM only) Can you specifically confirm that the set of hardware and software that implements **revocation** as defined in the Specifications and using CI Plus 2nd Root of Trust credentials is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

Question PF.5: (for Host only) Can you specifically confirm that the set of hardware and software that implements **enforcement of the Compliance Rules as defined in Exhibit ECP_C** is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

Question PF.6: Can you specifically confirm that the set of hardware and software that **maintains the authenticity of CI Plus 2nd RoT Trust Values** is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

Question PF.7: Can you specifically confirm that the set of hardware and software that **maintains the authenticity and secrecy of CI Plus 2nd RoT Secret Values** is part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 1.10)?

Yes / No

2.5 Questions related to software implementation of ECP Protection Functions

Question SWPF.1: Can you confirm that all the software implementing the ECP Protection Functions is loaded into a Trusted Execution Environment by a Secure Boot process (refer to Exhibit ECP_B section 1.15)?

Yes / No

Question SWPF.2: Can you confirm that the Secure Boot process enforces that each component authenticates and checks the integrity of the component that follows it before transferring control to it (refer to Exhibit ECP_B section 1.15)?

Yes / No

Question SWPF.3: Is the root of trust of such Secure Boot process provisioned in hardware (refer to Exhibit ECP_B section 1.15)?

Yes / No

Question SWPF.4: Can you confirm that the Trusted Execution Environment(s) implementing the ECP Protection Functions uses hardware enforcement to prevent unauthorized software and/or hardware from discovering, modifying or interfering with its code and data (refer to Exhibit ECP_B section 1.19)?

Yes / No

2.6 Questions related to protection against Defeating Functions

Question DF.1: Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which an **ECP Protection Function** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to defeat any ECP Protection Function.

Question DF.2: Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which an **ECP Protection Function** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered ‘No’, please describe how every such JTAG port, emulator interface or test point is protected from being used to defeat any ECP Protection Function.

Question DF.3: Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which an **ECP Protection Function** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered ‘No’, please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to defeat any ECP Protection Function.

Question DF.4: Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which a **Standard Protection Function** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to defeat any Standard Protection Function.

Question DF.5: Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which a **Standard Protection Function** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to defeat any Standard Protection Function.

Question DF.6: Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which a **Standard Protection Function** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered ‘No’, please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to defeat any Standard Protection Function.

Question DF.7: Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which a **CI Plus 2nd RoT Trust Value** can be modified (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered ‘No’, please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to modify any CI Plus 2nd RoT Trust Value.

Question DF.8: Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which a **CI Plus 2nd RoT Trust Value** can be modified (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered ‘No’, please describe how every such JTAG port, emulator interface or test point is protected from being used to modify any CI Plus 2nd RoT Trust Value.

Question DF.9: Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which a **CI Plus 2nd RoT Trust Value** can be modified (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to modify any CI Plus 2nd RoT Trust Value.

Question DF.10: Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which a **CI Plus 2nd RoT Secret Value** can be modified or revealed (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to modify or reveal any CI Plus 2nd RoT Secret Value.

Question DF.11: Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which a **CI Plus 2nd RoT Secret Value** can be modified or revealed (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to modify or reveal any CI Plus 2nd RoT Secret Value.

Question DF.12: Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which a **CI Plus 2nd RoT Secret Value** can be modified or revealed (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to modify or reveal any CI Plus 2nd RoT Secret Value.

Question DF.13: (for Host only) Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which **ECP Controlled Content** can be exposed to unauthorized access, copying, redistribution, or modification of user rights (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to expose any ECP Controlled Content to unauthorized access, copying, redistribution, or modification of user rights.

Question DF.14: (for Host only) Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which **ECP Controlled Content** can be exposed to unauthorized access, copying, redistribution, or modification of user rights (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to expose any ECP Controlled Content to unauthorized access, copying, redistribution, or modification of user rights.

Question DF.15: (for Host only) Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which **ECP Controlled Content** can be exposed to unauthorized access, copying, redistribution, or modification of user rights (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to expose any ECP Controlled Content to unauthorized access, copying, redistribution, or modification of user rights.

Question DF.16: Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which the protection provided by the **CI Plus ECP Trusted Boundary** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to defeat the protection provided by the CI Plus ECP Trusted Boundary.

Question DF.17: Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which the protection provided by the **CI Plus ECP Trusted Boundary** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to defeat the protection provided by the CI Plus ECP Trusted Boundary.

Question DF.18: Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which the protection provided by the **CI Plus ECP Trusted Boundary** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to defeat the protection provided by the CI Plus ECP Trusted Boundary.

Question DF.19: (for Hosts only) Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which the **Compliance Rules as defined in Exhibit ECP_C** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to defeat the Compliance Rules as defined in Exhibit ECP_C.

Question DF.20: (for Hosts only) Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which the **Compliance Rules as defined in Exhibit ECP_C** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to defeat the Compliance Rules as defined in Exhibit ECP_C.

Question DF.21: (for Hosts only) Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which the **Compliance Rules as defined in Exhibit ECP_C** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to defeat the Compliance Rules as defined in Exhibit ECP_C.

Question DF.22: (for CICAMs only) Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which the **Compliance Rules as defined Exhibit D and Exhibit ECP_D** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to defeat the Compliance Rules as defined Exhibit D and Exhibit ECP_D.

Question DF.23: (for CICAMs only) Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which the **Compliance Rules as defined Exhibit D and Exhibit ECP_D** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to defeat the Compliance Rules as defined Exhibit D and Exhibit ECP_D.

Question DF.24: (for CICAMs only) Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which the **Compliance Rules as defined Exhibit D and Exhibit ECP_D** can be defeated (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to defeat the Compliance Rules as defined Exhibit D and Exhibit ECP_D.

2.7 Questions related to Secure Storage

Question SS.1: If the ECP Device stores any CI Plus 2nd RoT Secret Value outside of the CI Plus ECP Trusted Boundary, does it use Secure Storage (refer to Exhibit ECP_B section 2.3)?

Yes / No / Not Applicable

Question SS.2: If the ECP Device stores any CI Plus 2nd RoT Secret Value outside of the CI Plus ECP Trusted Boundary, is Secure Storage designed in a way that prevents CI Plus 2nd RoT Secret Values from being revealed outside of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 2.3)?

Yes / No / Not Applicable

Question SS.3: Do all CI Plus 2nd RoT Secret Values in non-encrypted form reside only within the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 2.3)?

Yes / No

Question SS.4: If the ECP Device stores any CI Plus 2nd RoT Secret Value outside of the CI Plus ECP Trusted Boundary, is Secure Storage of the ECP Device encrypted with a securely provisioned, secret, immutable, device-unique key of at least 128 bits of entropy (refer to Exhibit ECP_B section 1.16)?

Yes / No / Not Applicable

2.8 Questions related to ECP Controlled Content Paths

Question CCP.1: (for Hosts only) Can you confirm that all the software affecting the ECP Controlled Content security has been loaded in a Trusted Execution Environment by a Secure Boot process (refer to Exhibit ECP_B section 1.15)?

Yes / No

Question CCP.2: (for Hosts only) Can you confirm that the Secure Boot process enforces that each component authenticates and checks the integrity of the component that follows it before transferring control to it (refer to Exhibit ECP_B section 1.15)?

Yes / No

Question CCP.3: (for Hosts only) Is the root of trust of such Secure Boot process provisioned in hardware (refer to Exhibit ECP_B section 1.15)?

Yes / No

Question CCP.4: (for Hosts only) Can you confirm that the Trusted Execution Environment(s) implementing all code and data affecting ECP

Controlled Content security in the ECP Device uses hardware enforcement to prevent unauthorized software and/or hardware from discovering, modifying or interfering with its code and data (refer to Exhibit ECP_B section 1.19)?

Yes / No

Question CCP.5: (for Hosts only) Can you confirm the ECP Device does not make available ECP Controlled Content on outputs other than those specified in the Compliance Rules as defined in Exhibit ECP_C (refer to Exhibit ECP_B section 2.4)?

Yes / No

Question CCP.6: (for Hosts only) Can you confirm that ECP Controlled Content in non-encrypted form is not present outside the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 2.4)?

Yes / No

Question CCP.7: (for Hosts only) Can you confirm that all internal non-persistent or transitory transmissions, processing and transformation of ECP Controlled Content is part of the ECP Controlled Content Path of the ECP Device (refer to Exhibit ECP_B section 1.9)?

Yes / No

2.9 Questions related to ECP Level of Protection

Question LP.1: Is the Trusted Execution Environment that is part of the CI Plus ECP Trusted Boundary of the ECP Device implemented, at a minimum, in a way that it cannot be reasonably foreseen to be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.1)?

Yes / No

Question LP.2: Is the Trusted Execution Environment that is part of the CI Plus ECP Trusted Boundary of the ECP Device implemented, at a minimum, in a way that it can

only with difficulty be defeated or circumvented using Professional Tools (refer to Exhibit ECP_B section 3.1)?

Yes / No

Question LP.3: Is the Trusted Execution Environment that is part of the CI Plus ECP Trusted Boundary of the ECP Device implemented, at a minimum, in a way that it cannot be reasonably foreseen to be defeated or circumvented due to a transition of power state, whether authorized or unauthorized (refer to Exhibit ECP_B section 3.1)?

Yes / No

Question LP.4: Is the Secure Boot process of the ECP Device implemented, at a minimum, in a way that it cannot be modified merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.2)?

Yes / No

Question LP.5: Is the Secure Boot process of the ECP Device implemented, at a minimum, in a way that it can only with difficulty be modified using Professional Tools (refer to Exhibit ECP_B section 3.2)?

Yes / No

Question LP.6: Is the Secure Boot process of the ECP Device implemented, at a minimum, in a way that compromise for one Device Type cannot be directly exploitable on another Device Type (refer to Exhibit ECP_B section 3.2)?

Yes / No

Question LP.7: Are all CI Plus 2nd RoT Trust Values of the ECP Device protected, at a minimum, in a way that they cannot be modified merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.3)?

Yes / No

Question LP.8: Are all CI Plus 2nd RoT Trust Values of the ECP Device protected, at a minimum, in a way that they can only with difficulty be modified using Professional Tools (refer to Exhibit ECP_B section 3.3)?

Yes / No

Question LP.9: Are all CI Plus 2nd RoT Secret Values of the ECP Device protected, at a minimum, in a way that they cannot be modified or discovered merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.4)?

Yes / No

Question LP.10: Are all CI Plus 2nd RoT Secret Values of the ECP Device protected, at a minimum, in a way that they can only with difficulty be modified or discovered using Professional Tools (refer to Exhibit ECP_B section 3.4)?

Yes / No

Question LP.11: Is the Secure Storage of the ECP Device implemented, at a minimum, in a way that it cannot be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.5)?

Yes / No / Not Applicable

Question LP.12: Is the Secure Storage of the ECP Device implemented, at a minimum, in a way that it can only with difficulty be defeated or circumvented using Professional Tools (refer to Exhibit ECP_B section 3.5)?

Yes / No / Not Applicable

Question LP.13: Is the CI Plus ECP Trusted Boundary of the ECP Device implemented, at a minimum, in a way that it cannot be defeated or circumvented merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.6)?

Yes / No

Question LP.14: Is the CI Plus ECP Trusted Boundary of the ECP Device implemented, at a minimum, in a way that it can only with difficulty be defeated or circumvented using Professional Tools (refer to Exhibit ECP_B section 3.6)?

Yes / No

Question LP.15: Are all Debug Functions of the ECP Device implemented, at a minimum, in a way that they cannot undergo unauthorized activation merely by using Widely Available Tools or Specialized Tools, or any software or hardware being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.7)?

Yes / No

Question LP.16: Are all Debug Functions of the ECP Device implemented, at a minimum, in a way that they can undergo unauthorized activation only with difficulty using Professional Tools (refer to Exhibit ECP_B section 3.7)?

Yes / No

Question LP.17: Are all ECP Protection Functions of the ECP Device implemented, at a minimum, in a way that they cannot be modified merely by using any hardware or software being part of the ECP Device but not being part of the CI Plus ECP Trusted Boundary (refer to Exhibit ECP_B section 3.8)?

Yes / No

2.10 Questions related to the PRNG

Question PRNG.1: Does the Pseudo Random Number Generator of the ECP Device comply with NIST 800-90A Revision 1 when generating the random values listed in Table A.1 of CI Plus Specification 1.3? For

example, the compliance can be verified by using the tests specified in the NIST SP 800-22 Revision 1a publication.

Yes / No

2.11 Questions related to the protection of Controlled Content that is not ECP Controlled Content

In this section, any reference to Controlled Content shall be understood as referring to Controlled Content that is not ECP Controlled Content.

The questions in this section can be skipped if the ECP Device protects the Controlled Content as defined for ECP Controlled Content in Exhibit ECP_B.

The questions in this section apply when the Controlled Content is protected under the terms of Exhibit B (Licensee answered Exhibit B to question GEN.9).

Question CC.1: Does the ECP Device have any User Accessible Bus (as defined in Section 2.0 of the Robustness Rules Exhibit B)?

Yes / No

If answered 'Yes', is Controlled Content carried on this bus?

Yes / No

If answered ‘Yes’, then identify and describe the bus, and whether the Controlled Content is compressed or uncompressed. If such Data is present, then explain in detail how and by what means the data is being protected as required by Section 2.0 of the Robustness Rules Exhibit B.

Question CC.2: Does the ECP Device have any User Accessible Bus that supports Direct Memory Access?

Yes / No

If answered ‘Yes”, then explain why Controlled Content, Keys and Production Credentials cannot be disclosed, revealed, replaced, or modified using Direct Memory Access.

Question CC.3: If the ECP Device delivers Controlled Content from one part of the product to another, whether among software modules, integrated circuits or otherwise or a combination thereof, explain how the portions of the product that perform authentication and decryption and the MPEG (or similar) decoder have been designed, associated and integrated with each other so that Controlled Content is secure from interception and copying as required in Section 3.0(a) of the Robustness Rules Exhibit B.

Question CC.4: (for Host only) Can you confirm the ECP Device does not contain any switches, buttons, jumpers, specific traces (electrical connections) that can be cut, or software equivalents of any of the foregoing by which **Controlled Content** can be exposed to unauthorized access, copying, redistribution, or modification of user rights (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such switch, button, jumper, specific trace, or software equivalent is protected from being used to expose any Controlled Content to unauthorized access, copying, redistribution, or modification of user rights.

Question CC.5: (for Host only) Can you confirm the ECP Device does not contain any Debug Functions such as active JTAG ports, active emulator interfaces or active test points to probe security functions by which **Controlled Content** can be exposed to unauthorized access, copying, redistribution, or modification of user rights (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such JTAG port, emulator interface or test point is protected from being used to expose any Controlled Content to unauthorized access, copying, redistribution, or modification of user rights.

Question CC.6: (for Host only) Can you confirm the ECP Device does not contain any special functions or modes of operation (including service menus or remote-control functions) by which **Controlled Content** can be exposed to unauthorized access, copying, redistribution, or modification of user rights (refer to Exhibit ECP_B section 2.2)?

Yes / No

If answered 'No', please describe how every such special function or mode of operation (including service menus or remote-control functions) is protected from being used to expose any Controlled Content to unauthorized access, copying, redistribution, or modification of user rights.

2.12 Questions related to Standard Protection Functions implemented under the terms of Exhibit B

The questions in this section can be skipped if the ECP Device implements the Standard Protection Functions as defined for ECP Protection Functions in Exhibit ECP_B.

The questions in this section apply when the ECP Device implements the Standard Protection Functions under the terms of Exhibit B (Licensee answered Exhibit B to question GEN.10).

Question SPF.1: Is all software and are all software updates of the ECP Device under control of the Manufacturer of said ECP Device (refer to Exhibit ECP_B section 2.1)?

Question SPF.2: Describe the method by which the ECP Device self-checks the integrity of the firmware or hardware components in such manner that modifications will cause failure of authorization or decryption as described in Section 3.0(b)(ii) of the Exhibit B. Describe what happens when integrity is violated.

Question SPF.3: Describe the method by which the ECP Device checks the authenticity and integrity of firmware updates in such manner that unauthorized firmware updates will be rejected.

Question SPF.4: If applicable, describe the method by which the ECP Device protects stored Controlled Content for the purpose of PVR or PauseTV.

Question SPF.5: (for CICAM only) In the ECP Device, describe the method by which the Certificate Revocation Lists (CRL and CWL) are protected from replacement and change.

2.13 Questions related to CI Plus RoT Secret Values protected under the terms of Exhibit B

The questions in this section can be skipped if the ECP Device protects the CI Plus RoT Secret Values as defined for CI Plus 2nd RoT Secret Values in Exhibit ECP_B.

The questions in this section apply when the ECP Device protects the CI Plus RoT Secret Values under the terms of Exhibit B (Licensee answered Exhibit B to question GEN.11).

Question SV.1: In the ECP Device, describe the method by which the confidentiality of the CI Plus RoT Key(s) is preserved when stored in firmware and / or hardware.

Question SV.2: In the ECP Device, describe the method by which the authenticity of the CI Plus RoT Production Credentials is preserved when stored in firmware and / or hardware.

Question SV.3: In the ECP Device, describe the method by which the CI Plus RoT intermediate cryptographic values (e.g. values created during the process of authentication between host and module) are created and held in a protected manner.

2.14 Questions related to CI Plus RoT Trust Values protected under the terms of Exhibit B

The questions in this section can be skipped if the ECP Device protects the CI Plus RoT Trust Values as defined for CI Plus 2nd RoT Trust Values in Exhibit ECP_B.

The questions in this section apply when the ECP Device protects the CI Plus RoT Trust Values under the terms of Exhibit B (Licensee answered Exhibit B to question GEN.12).

Question TV.1: In the ECP Device, describe the method by which the authenticity of the CI Plus RoT Trust Values is preserved when stored in firmware and / or hardware.

Remainder of this page intentionally left blank.