**Exhibit ECP_B: Enhanced Content Protection (ECP) Robustness Rules**

**Version 1.1**

*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 Host devices and 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 Trusted Boundary" means the set of hardware and software that implements the Protection Functions and the ECP Controlled Content Path. The CI Plus 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, (iii) runs in a Trusted Executed Environment. Software running in the Trusted Execution Environment and implementing functions other than the Protection Functions or the ECP Controlled Content Path is not part of the CI Plus Trusted Boundary.

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

**1.4** "Device Keys" means MDQ, HDQ and SIV as described in the Specifications.

**1.5** "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.

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

**1.7** "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, equipments, methods or techniques not included in the definition of Widely Available Tools and Specialized Tools.

**1.8** "Protection Functions" means functions related to the protection of ECP Controlled Content, including but not limited to (i) authentication, (ii) encryption, (iii) decryption, (iv) revocation as defined in the Specifications, (v) enforcement of the Compliance Rules as defined in Exhibit ECP_C, (vi) maintaining the authenticity of Trust Values, and (vii) maintaining the authenticity and secrecy of Secret Values.

**1.9** "Protocol Secrets" means all numerical, algorithmic and implementation secrets related to CI Plus protocol execution as described in the Specifications. This includes the credentials marked as both 'license constant' and 'keep local' in the CI Plus Specification Version 1.3 Table 5.2.

**1.10** "Revocation Information" means the Revocation Signalling Data (RSD) version number and the service operator identity as defined in the Specifications.

**1.11** "Secret Value" means a value that Licensed Products must resist attempts to reveal. Secret Values minimally include (i) Device Keys, (ii) Content Keys, (iii) Intermediate Keys, and (iv) Protocol Secrets.

**1.12** "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

implementing the Protection Functions and (ii) all software affecting ECP Controlled Content security have been loaded in the Trusted Execution Environment. The root of this trust shall be securely provisioned in hardware, e.g. permanently factory burned.

**1.13** "Secure Storage" means a local and persistent storage which 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.

**1.14** "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).

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

**1.16** "Trust Value" means a value that Licensed Products must resist attempts to modify or set. Trust Values minimally include (i) Certificates, (ii) Revocation Information, (iii) Critical Security Update Version, and (iv) SRM.

**1.17** "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 meet the Compliance Rules as defined in Exhibit C and Exhibit ECP_C and shall contain a CI Plus Trusted Boundary.

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

The Licensed Product should make use of the CI Plus Trusted Boundary to isolate Protection Functions from general purpose software.

**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 a Protection Function can be defeated, (ii) by which a Trust Value can be modified, (iii) by which a Secret Value can be modified or revealed, (iv) by which ECP Controlled Content can be exposed to unauthorized access, copying, redistribution, or modification of user rights, or (v) by which the protection provided by the CI Plus Trusted Boundary 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 Compliance Rules as defined in Exhibit C and Exhibit ECP_C and this Exhibit ECP_B.

**2.3 Keep Secret.**

When the Licensed Product has to store Secret Values outside the CI Plus Trusted Boundary, the Licensed Product shall make use of a Secure Storage.
The Secure Storage shall be designed in a way that prevents Secret Values from being revealed outside of the CI Plus Trusted Boundary. Secret Values in non-encrypted form shall only reside within the CI Plus 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 C and 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 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 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 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 **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 Trusted Boundary, and
- **(ii)** Can only with difficulty be modified using Professional Tools.

**3.4** The **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 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 Trusted Boundary, and

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

**3.6** **The CI Plus 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 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 Trusted Boundary, and

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

**3.8** The **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 Trusted Boundary.

**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 ECP Robustness Checklist**.

**5.1** Before releasing any Licensed Product, Licensee must assure compliance with this Exhibit ECP_B. An ECP Robustness Checklist 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 ECP Robustness Checklist does not address all elements required for the manufacture of a compliant product, Licensee is strongly advised to carefully review the Specifications, CI Plus License Documentation, the Compliance Rules as defined in Exhibit C and Exhibit ECP_C 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 Compliance Rules as defined in Exhibit C and Exhibit ECP_C, this Exhibit ECP_B, and the ECP Robustness Checklist 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: Additional Compliance Rules for ECP Host Devices**
**Version 1.0**

*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

**1.1** "**ECP Constrained Image**" means the visual equivalent of not more than 1,958,400 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** "**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.

**1.3** "**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 and Exhibit ECP_E for URI interpretation when outputting ECP Controlled Content under this Section 2.0.

**2.1** **General**. Licensed Product shall be compliant with the compliance rules defined in 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 these ECP Compliance Rules and 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** **Analogue Audio outputs**. Licensed Product with any analogue audio outputs shall only output the audio portion of ECP Controlled Content as permitted by this Section 2.2.

**2.2.1** **Analogue Audio Output**. The Licensed Product may pass the audio portion of ECP Controlled Content to mono, stereo and multichannel Analogue Audio Output.

**2.3** **Digital Outputs**. Licensed Product with any digital outputs shall only output ECP Controlled Content as permitted by this Section 2.3.

**2.3.1** **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, 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 Addendum, shall have the meaning set forth in the HDCP Specification 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 make reasonable efforts to avoid such interference.

**2.3.2** **S/PDIF with SCMS.** Licensed Product may pass the audio portion of ECP Controlled Content to an output, in digital compressed or uncompressed form over S/PDIF, including TOS-link or coax interfaces, where the output has SCMS active and on. Licensed product shall provide a category code in conjunction to the L-bit and may choose a category code from the list defined in IEC60958-3, section 5.3.2.2.4, table 7

**2.3.3** **Other digital audio output**. Licensed Product may pass the audio portion of ECP Controlled Content over any digital audio output, without any content protection in a compressed or uncompressed format with the constraint of encoding at 48kHz, 16 bits or less.

**2.3.4** **DTCP-IP**. Licensed Product may pass ECP Controlled Content in digital form where such output is protected by DTCP-IP.

- Capitalized terms used in this Section, but not otherwise defined in this Exhibit ECP_C or the Addendum, 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 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 ECP Controlled Content, except as permitted in the Section 3.0 of Exhibit C of the Agreement and as further constrained below.

**3.2** **Mere Buffer for Display**. Licensed Products may store ECP Controlled Content temporarily for the sole purpose of enabling the immediate display of ECP Controlled Content, provided that (a) such storage does not persist after the content has been displayed, and (b) the data is not stored in a way that supports copying, recording, or storage of such data for other purposes, (c) the buffering is limited to a maximum of 10 seconds of video data.

**3.3** **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 or by the following:

**3.3.1** **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.

**3.3.2** **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 there from 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).

**3.3.3** **Playback Control**. Notwithstanding Section 3.3.1, Secure Storage Licensed Product may store ECP Controlled Content as to which Copy Never control has been asserted in such a way that it can only be played back with authorisation from CICAM in accordance with Section 5.10 of CI Plus Specification Version 1.3.

**3.4** **Removable Storage**

Refer to Exhibit E and Exhibit ECP_E for URI interpretation when recording ECP Controlled Content under this Section 3.4.

**3.4.1** 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.

**Remainder of this page intentionally left blank.**

**Exhibit ECP_E: URI Mapping Table Extension for ECP**
**Version 1.0**

| Input to ECP Host | | | | | | | | | Internal Retention limit | Output of content to Devices downstream of the ECP Host | | | | | | Non ECP Controlled Content | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | Digital Output | | | | | | | | |
| | | | | | | | | | | HDCP 2.2.or greater | | HDCP Less than version 2.2 | | DTCP | | | | |
| | Use case | CA controlled *1 | URI *2 EMI | | ECI | | | ICT | | Allowed Export | Image constraint | Allowed Export | Image constraint | Allowed Export | Image constraint | ECP Controlled Content | | |
| Copy Never | a | 1 | 1 | 1 | 0 | 0 | 0 | 0 | Note *3 | Yes | None | Yes | None | Yes | None | | All Digital outputs | |
| | b | 1 | 1 | 1 | 0 | 0 | 0 | 1 | | Yes | None | Yes | None | Yes | None | | | |
| | c | 1 | 1 | 1 | 0 | 0 | 1 | 0 | | 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 | 1,959k | Yes | 1,959k | | | |
| | 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 | 1,959k | Yes | 1,959k | | | |
| | i | 1 | 1 | 1 | 1 | 0 | 0 | 0 | | Yes | None | Yes | None | No | - | | HDCP only | |
| | j | 1 | 1 | 1 | 1 | 0 | 0 | 1 | | Yes | None | Yes | 1,959k | No | - | | | No retention |
| | 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 | 1,959k | No | - | | | |
| | m | 1 | 1 | 1 | 1 | 1 | 0 | 0 | Note *3 | Yes | None | No | - | No | - | | HDCP 2.2 only | |
| | n | 1 | 1 | 1 | 1 | 1 | 0 | 1 | | Yes | None | No | - | No | - | | | |
| | o | 1 | 1 | 1 | 1 | 1 | 1 | 0 | Note *4 | Yes | None | No | - | No | - | | | No retention |
| | p | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | Yes | 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 this case, the Internal Retention limit shall be interpreted as specified in Exhibit E.

4 In this case, no Internal Retention is allowed for the ECP Controlled Content.