1.0 CI Plus Robustness Checklist for ECP Devices

1.1 Declaration of compliance

Date	
Manufacturer or Brand	
Product Name	
Hardware Model or Software Version	
Company Name	
Company Address	
Print Name or Names	
Signature or signatures	

1.2 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 you 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 you 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 your answer is Exhibit B, then the Licensee shall respond to the questions listed in section 1.11.

If your 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 your answer is Exhibit B, then the Licensee shall respond to the questions listed in section 1.12.

If your 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 your answer is Exhibit B then the Licensee shall respond to the questions listed in section 1.13.

If your 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 your answer is Exhibit B, then the Licensee shall respond to the questions listed in section 1.14.

If your 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.

1.3 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 ◯

1.4 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 ◯

1.5 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 ◯

1.6 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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 you 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.

1.7 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 ◯

1.8 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 ◯

1.9 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 ◯

1.10 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 ◯

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

Yes ◯ No ◯

If you 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 you 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 you 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 you 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 you 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.

1.12 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.

1.13 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.

1.14 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.