CI Plus Robustness Certification Checklist

Date: _____

Licensee / Brand: _____

Product Name: _____

Hardware Model or Software Version: _____

Company Name: _____

Company Address: _____

Phone Number: _____

Fax Number: _____

Print Name(s): _____

Signature(s): _____

1. General design and implementation questions

Question 1.1: Have you read the Compliance Rules and the Robustness Rules?

☐ Yes
☐ No (if yes, which version and date)

Question 1.2: Has the Licensed Product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies, analogue protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specifications or Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized copying?

☐ Yes
☐ No

Question 1.3: Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of Controlled Content or expose it to unauthorized copying?

☐ Yes
☐ No

Question 1.4: Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analogue protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specifications or Compliance Rules?

☐ Yes
☐ No

Question 1.5: Does the Licensed Product have service menus, service functions, or service utilities that can alter or expose the flow of Controlled Content within the device?

☐ Yes
☐ No

If answered 'Yes', please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to expose or misdirect Controlled Content.

Question 1.6: Does the Licensed Product have service menus, service functions, or service utilities that can turn off any analogue protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specifications, the Compliance Rules, or the Robustness Rules?

☐ Yes
☐ No

If answered 'Yes', please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the Compliance Rules and the Robustness Rules.

Question 1.7: Does the Licensed Product have any User Accessible Buses (as defined in Section 2.0 of the Robustness Rules)?

☐ Yes
☐ No

If answered ‘Yes’, are 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.

Question 1.8: Does the Licensed Product have User Accessible Buses that support 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.

Remainder of this page intentionally left blank.

Question 1.9: If the Licensed Product 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.

Question 1.10: To assure correct operation of the Pseudo Random Number Generator (see Annex A of the CI Plus Specification) verify its behaviour by performing the tests specified in the NIST SP 800-22 publication.

☐ Pass
☐ Fail

Question 1.11: Describe the method by which the Licensed Product 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 Robustness Rules. Describe what happens when integrity is violated.

Question 1.12: Describe the method by which the Licensed Product checks the authenticity and integrity of firmware updates in such manner that unauthorized firmware updates will be rejected.

Question 1.13: If applicable, describe the method by which the Licensed Product protects stored Controlled Content for the purpose of PVR or PauseTV.

Question 1.14: Describe the method of provisioning Keys and Production Credentials during the production of the Licensed Product. Include any preparation steps.

Question 1.15: (for Hosts only): does the product have any user accessible menus that change the version the Host back to an earlier version of the CI Plus Specification than the version of the CI Plus Specification used for this Registration?

☐ Yes
☐ No

Question 1.16: (for Hosts only): does the product contain one or more options that change the behavior of any CI Plus Resource to that of a higher version of the CI Plus Specification than the version of the CI Plus Specification used for the Registration?

☐ Yes
☐ No

If answered Yes: List each Resource that can be changed to a higher version and confirm that the Host is compliant to the applicable specifications for every (combination of) settings of all such options.

Remainder of this page intentionally left blank.

2. Design and implementation questions

Question 2.1: In the Licensed Product, describe the method by which the confidentiality of the Key(s) is protected when stored in firmware and / or hardware.

Question 2.2: In the Licensed Product, describe the method by which the authenticity of the Production Credentials is protected when stored in firmware and / or hardware.

Question 2.3: In the Licensed Product, describe the method by which the intermediate cryptographic values (e.g., values created during the process of authentication between Host and Module, or devices within a Licensed Product) are created and held in a protected manner.

Question 2.4: In the Licensed CICAM Product, describe the method by which the Certificate Revocation Lists (CRL and CWL) are protected from replacement and change.

Question 2.5: In the Licensed Product, describe the method being used to prevent commonly available debugging or decompiling tools (incl. JTAG and I^2C) from being used to single-step, decompile, or examine the operation of the CI Plus functions implemented in software and/or hardware.

3. Anti-tampering questions

Question 3.1: To assure that integrity self-checking is being performed, perform a test to reassure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing CI Plus functions, and describe the method and results of the test.

☐ Pass
☐ Fail

Question 3.2: In the Licensed Product, does the removal or replacement of hardware elements or modules that implement CI Plus functions render the Licensed Product unable to receive, decrypt, or decode Controlled Content? For example, a DIP package FLASH memory chip can be easily be removed and replaced by another FLASH memory. The replaced FLASH memory may contain software-code that circumvents the Compliance Rules and Robustness Rules.

☐ Yes
☐ No

If answered 'No', describe the means used to prevent such attempts.

Question 3.3: If applicable, specify the tamper resistance properties of security epoxies used by the Licensed Product in order to meet the required level of robustness as defined by the Robustness Rules.
