

DFAST Technology License Agreement

Exhibit C-1

Robustness Checklist

Notice: This Checklist is intended as an aid to the correct implementation of the Robustness Rules for hardware and software implementations of the Referenced Technology in a Unidirectional Digital Cable Product. This Checklist does not address all aspects of the Referenced Technology and Compliance Rules necessary to create a product that is fully compliant. Failure to perform the tests and analysis necessary to comply fully with the Referenced Technology, Compliance Rules or Robustness Rules could result in a breach of this Agreement and appropriate legal action taken by CableLabs or other parties under the License Agreement.

DATE: _____

MANUFACTURER: _____

PRODUCT NAME: _____

HARDWARE MODEL OR SOFTWARE VERSION: _____

NAME OF TEST ENGINEER COMPLETING CHECKLIST:

TEST ENGINEER: _____

COMPANY NAME: _____

COMPANY ADDRESS: _____

PHONE NUMBER: _____

FAX NUMBER: _____

GENERAL IMPLEMENTATION QUESTIONS

1. Has the Unidirectional Digital Cable 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, analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Referenced Technology or Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized copying?

2. Has the Unidirectional Digital Cable 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?

3. Has the Unidirectional Digital Cable 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 analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Referenced Technology or Compliance Rules?

4. Does the Unidirectional Digital Cable Product have service menus, service functions, or service utilities that can alter or expose the flow of Controlled Content within the device?

If 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.

5. Does the Unidirectional Digital Cable Product have service menus, service function, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Referenced Technology or Compliance Rules?

If 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

encryption features of DFAST (including compliance with the Compliance Rules and the Referenced Technology).

6. Does the Unidirectional Digital Cable Product have any user-accessible buses (as defined in Section 2 of the Robustness Rules)?

If so, is Controlled Content carried on this bus?

If so, then:

identify and describe the bus, and whether the Controlled Content is compressed or uncompressed. If such Data is compressed, then explain in detail how and by what means the data is being re-encrypted as required by Section 2 of the Robustness Rules.

7. Explain in detail how the Unidirectional Digital Cable Product protects the confidentiality of all keys.
8. Explain in detail how the Unidirectional Digital Cable Product protects the confidentiality of the confidential cryptographic algorithms used in DFAST.
9. If the Unidirectional Digital Cable 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 are secure from interception and copying as required in Section 3(a) of the Robustness Rules.
10. Are any DFAST functions implemented in Hardware?

If Yes, complete hardware implementation questions.

11. Are any DFAST functions implemented in Software?

If Yes, complete software implementation questions.

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Unidirectional Digital Cable Product, describe the method by which all Keys are stored in a protected manner.
13. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?
14. In the Unidirectional Digital Cable Product, describe the method used to obfuscate the confidential cryptographic algorithms and Keys used in DFAST and implemented in software.
15. Describe the method in the Unidirectional Digital Cable Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Unidirectional Digital Cable Product) are created and held in a protected manner.
16. Describe the method being used to prevent commonly available debugging or decompiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the DFAST functions implemented in software.
17. Describe the method by which the Unidirectional Digital Cable Product self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3(b)(ii) of the Robustness Rules. Describe what happens when integrity is violated.
18. To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing DFAST functions, and describe the method and results of the test.

HARDWARE IMPLEMENTATION QUESTIONS

19. In the Unidirectional Digital Cable Product, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.
20. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?
21. In the Unidirectional Digital Cable Product, describe how the confidential cryptographic algorithms and Keys used in DFAST have been implemented in silicon circuitry or firmware so that they cannot be read.
22. Describe the method in the Unidirectional Digital Cable Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Unidirectional Digital Cable Product) are created and held in a protected manner.

Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement DFAST functions?

24. In the Unidirectional Digital Cable Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of DFAST (including the Compliance Rules, the Referenced Technology, and the Robustness Rules) damage the Unidirectional Digital Cable Product so as to render the Unidirectional Digital Cable Product unable to receive, decrypt, or decode Controlled Content?

Notice: This checklist does not supersede or supplant the Referenced Technology, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the Referenced Technology, the Robustness Rules and the Compliance Rules that are not reflected here but that must be complied with.