DCI Digital Cinema Initiatives, LLC

Memorandum of Information Regarding the Secure Silicon Requirement of the DCI Digital Cinema System Specification (DCSS)

Approved 10 May 2018
Digital Cinema Initiatives, LLC, Member Representatives Committee

In conjunction with publishing the DCI Compliance Test Plan (CTP) test for Media Block (MB) secure silicon requirements,[1] DCI anticipates there may be questions or concerns as to where to source such single chip integrated circuits (IC). This memo is a guide to NIST site information that lists qualified ICs, and other methods to meet DCSS and CTP secure silicon requirements.

This URL is to the NIST Cryptographic Module (CM) site, which also explains the concepts of "active," "historical," and "revoked" status:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules

To find CMs that meet the DCI secure silicon mandate, click the "search our database of validated modules" link, which takes you to the URL:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

- To search, click "advanced" search type, then fill in by standard "FIPS 140-2", algorithm "DRBG" (needed for RSA key pair generation), embodiment "single-chip", level "3" then click "Search".
- As of 10 May 2018, there are 24 active and 18 historical CM entries that appear. (Note that not all ICs are able to meet MB secure silicon functionality requirements.)
- "Active" validation status is not required (*i.e.*, a "historical" listing is acceptable), however, it is DCI's understanding that if the CM doesn't use "Approved" algorithms for the functions it performs (*e.g.*, generate RSA key pairs, process KDMs, etc.), it won't pass FIPS evaluation, failing the MB.

To verify the CTP requirement, a DCI CTP test entity will use the FIPS single-chip CM documentation (received from the MB supplier), look up the chip on the NIST site, and the IC description and published FIPS security policy information will indicate whether "level 3" physical security exists.

Secure silicon solutions are also available outside of NIST-evaluated CMs, as many semiconductor suppliers offer single chip ICs capable of meeting the DCI requirement. For example, the ISO/IEC 19790 "Security Requirements for Cryptographic Modules" standard evaluates and lists CMs (albeit to criteria different from FIPS 140-2).[2] Non-FIPS rated IC solutions can be evaluated by a NIST accredited FIPS 140-2 laboratory for compliance to FIPS 140-2 level 3 physical security, and provide an attestation that a particular IC solution meets DCI requirements.

DCI suggests that Media Block suppliers work with FIPS experts to review various secure silicon sourcing options and find an appropriate solution. DCI makes no endorsements.

[1] Requirements include meeting FIPS 140-2 "physical security" at level 3. See DCSS section 9.5.2.2 "Physical Security of Sensitive Data."
[2] This is an international standard similar to FIPS 140-2. See: https://www.iso.org/standard/52906.html