DCI Digital Cinema Initiatives, LLC

DCI Memorandum on RNG Revocation and Related NIST and FIPS Developments

Approved 16 March 2017 and 11 May 2018
Digital Cinema Initiatives, LLC, Member Representatives Committee

On March 23, 2018, DCI posted revisions to the Compliance Test Plan (CTP) that include new "secure silicon" requirements. Following the "stage 2" 120 day window, these requirements will be enforced as of July 21, 2018. In order to further smooth the transition, DCI is extending the below exclusion and grandfathering clauses to include all secure processing block (SPB) devices, which the Digital Cinema System Specification now requires to employ secure silicon.

On January 1, 2016, the Random Number Generator (RNG) used by the D-Cinema industry for content integrity validation became disallowed under NIST requirements for FIPS-mode Cryptographic Module (CM) operation. Additionally, the RNG historically used for Media Block (MB) RSA key generation has also been revoked.[1] As a result, all existing MBs have been moved from the NIST "Active Validation" list to the "Historical Validation" list.[2]

In addition to the above RNG disallowance, there are many other reasons that CMs get moved to the Historical Validation list. A recent "five year sunset" policy change at NIST in fact makes this an automatic process if any CM has not been reexamined by a FIPS lab within the previous five years.[3] NIST has provided guidelines as a function of "change scenarios" (i.e., what changed with the module or NIST requirements) which CM vendors can follow to get back onto the Active Validation list. There are five change scenarios defined in NIST document "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program" (IG), section G.8 "Revalidation Requirements".[4]

It is DCI's position that the D-Cinema industry need not be directly impacted by the Historical listing due to the disallowed RNGs. Until otherwise noticed, DCI does not require any action on the part of MB vendors or exhibition regarding MB purchase and use decisions with respect to legacy MBs that use the revoked RNGs.[5] However, there are related factors that encourage software upgrades for legacy MBs.

In particular, the recently published SMPTE KDM and DCert standards revisions enable the KDM to carry the new "MIC" and "Aux Data" key types. Many legacy MBs are candidates for software upgrades that would enable them to process the revised KDM and use these new key types. It is anticipated that some of these MBs can be simultaneously upgraded to eliminate the revoked RNGs and replace them with a NIST "Approved" Digital Random Bit Generator (DRBG).

DCI wishes to encourage the upgrading of existing MBs to replace the disallowed RNGs with an approved DRBG, and be able to accept and process the revised KDM. Additionally, by working with a FIPS lab to initiate a NIST IG "scenario 3" procedure, the upgraded MB can be reinstated to the NIST Active Validation list.

---

[1] These two RNGs are specified under FIPS 186-2 and ANSI X9.31 respectively.
[2] See: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
[3] See: http://csrc.nist.gov/groups/STM/cmvp/notices.html
[4] See: http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf
[5] DCI's requirement that new MB designs be validated as fully FIPS compliant does not change.

DCI requires that a MB that receives hardware or software upgrades undergo Compliance Test Plan (CTP) reexamination.[6] In particular, the CTP provides for "Confidence Retesting," which can reduce the reexamination burden for software upgrades. However, the current policy does not allow Confidence Retesting if a "device performs in a manner that would fail the CTP," and states "such device shall be required to complete a full CTP retest to become compliant."

DCI has recognized that the CTP Confidence Retesting prohibition for any non-compliant MB deficiencies may be problematic as a result of two errata:

- FIPS 140-2 single chip cryptographic module secure silicon (posted August 30, 2012). [7]
- Self-generated RSA key establishment (posted April 28, 2016). [8]

CTP tests for both will soon be posted, and following the CTP notification window, after 120 days enforcement will commence. This Enforcement Date is referred to below as "EDate."

Once the above CTP tests are in effect, a legacy MB that undergoes a software upgrade for any purpose will not pass CTP testing if the MB does not meet the secure silicon or RSA key establishment requirements. Since these are manifested in MB hardware designs, DCI has defined the following situations for which a MB may be excused from these CTP tests:

1. MBs that are listed on the DCI Compliant Equipment List, or are in the CTP test process with a licensed CTP test lab as of EDate.
2. MBs that are nearly completed design, but not yet in the CTP test process can qualify for exclusion *provided* the vendor applies for "nearly completed proof-of-design status" verification from a licensed CTP test lab before EDate. CTP testing may thereafter commence at any time *for that design*.

To meet the "for that design" constraint, the vendor must supply proof of a completely frozen physical and electrical hardware design, as codified by a licensed DCI CTP test lab. The exclusion will be allowed thereafter only against that codified design. MB designs that qualify for the above exclusions will be grandfathered going forward; there will be no exclusions otherwise for MBs entering the CTP test process after EDate.

DCI hopes this process will extend the working life of MB designs by providing a path for software upgrades to meet the latest NIST/FIPS requirements and D-Cinema functionality.

[6] See: http://www.dcimovies.com/compliance_test_plan/DCI-Test-Policy%202011-0726v2.pdf
[7] See errata #95 and #96 at: http://www.dcimovies.com/archives/spec_v1_2_No_Errata_Incorporated/errata_1-96_aug30/DCI-Errata_90-96_v1-2_08-30-2012.html
[8] See errata #24 at: http://www.dcimovies.com/errata/v1_2_with-errata-8-12/DCI-Errata_24_APRIL-28-2016_v1-2_08-30-2012.pdf

