DCI Memorandum on Compliance Test Plan (CTP) Confidence Retesting

Approved 13 October 2021
Digital Cinema Initiatives, LLC, Member Representatives Committee

On 11 May 2018, DCI reissued the "DCI Memorandum on RNG Revocation and Related NIST and FIPS Developments," which included certain exclusions for the Compliance Test Plan (CTP) reexamination related to Confidence Retesting.[1] While this memo remains in effect, it is primarily directed to NIST/FIPS requirements. The following is directed exclusively to Confidence Retesting exclusions and adds a third exclusion item.

DCI requires that a Secure Processing Block (SPB) that receives hardware or software upgrades undergo Compliance Test Plan (CTP) reexamination.[2] Additionally, the CTP provides for Confidence Retesting, which can reduce the reexamination burden for software upgrades. However, Confidence Retesting is not allowed if a "device performs in a manner that would fail the CTP," in which case "such device shall be required to complete a full CTP retest to become compliant."

DCI has recognized that the CTP Confidence Retesting prohibition for non-compliant SPB deficiencies may be problematic because of the following:

- Secure silicon integrated circuit requirements of DCSS section 9.5.2.2, which were changed by erratum on August 30, 2012.[3]
- Self-generated RSA key pair establishment per DCSS section 9.5.1, which was changed by erratum on April 28, 2016.[4]
- New and evolving NIST/FIPS requirements for SP800-90B and SP800-56Br2 compliance.[5]

In the 1 July 2020 memo "DCI Memorandum on NIST Standards Transitions and 'Non-FIPS Mode'," DCI established that the requirements of the NIST standards of the last bullet above could be deferred for FIPS 140-2 validated modules.[6]

The following clarifies the deferments with respect to the CTP:

> To minimize barriers to upgrades, SPB devices that are already listed on the Compliant Equipment page of the DCI website may be excused from CTP tests associated with the bullets above for purposes of a Confidence Retest, provided the devices are compliant to the associated DCSS requirements in place when originally CTP certified.[7]

Since implementations of the above are largely manifested in hardware, DCI views the security risks as low from allowing legacy designs to remain in place. These steps will help extend the life of existing products.

---

[1] See: https://www.dcimovies.com/announcements/DCI-Memo-on-RNG-Revocation_20180511.pdf. The exclusions on page 2 of the 11 May 2018 memorandum are repeated in the first two bullets above.
[2] See: https://www.dcimovies.com/compliance_test_plan/DCI-Test-Policy%202011-0726v2.pdf
[3] See: https://www.dcimovies.com/archives/spec_v1_2_No_Errata_Incorporated/errata_1-96_aug30/DCI-Errata_90-96_v1-2_08-30-2012.html, erratum #96.
[4] See: https://www.dcimovies.com/errata/v1_2_with-errata-8-12/DCI-Errata_24_APRIL-28-2016_v1-2_08-30-2012.pdf, erratum #24.
[5] See: https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips140-2/FIPS1402IG.pdf for requirements timing.
[6] See: https://www.dcimovies.com/FIPS/DCI_Memo_on_NIST_Standards_transitions_and_Non-FIPS_mode_2020-07-01.pdf
[7] Exclusions associated with the last bullet do not exclude the mandate for SPB devices to be FIPS certified.