DCI Digital Cinema Initiatives, LLC

DCI Memorandum on NIST Standards Transitions and "Non-FIPS Mode"

Approved 1 July 2020
Digital Cinema Initiatives, LLC, Member Representatives Committee

On December 19, 2019, DCI issued a memorandum informing the d-cinema industry of NIST's announcements regarding the transition to the FIPS 140-3 standard.[1] The key dates of this transition are (1) the start of Media Block (MB) submissions for FIPS 140-3 testing by CMVP labs on September 22, 2020, and (2) the end of MB submissions for FIPS 140-2 testing by CMVP labs on September 22, 2021.

In addition to this transition, there are two other NIST standard changes impacting MB designs:

- **SP800-90B** is effective November 8, 2020, for all new submissions (or any security relevant revalidation submissions) for FIPS 140-2 or FIPS 140-3 cryptographic module validation by a Cryptographic Module Validation Program (CMVP) test lab.[2]

- **SP800-56Br2** is effective January 1, 2021. FIPS 140-2 and 140-3 validated modules that are not compliant to any applicable requirement will be moved onto the historical listing by CMVP.[3]

While DCI's customary practice is to maintain compliance to all NIST/FIPS requirements, it is our position that (1) the security impacts of the above standards changes are minimal, and (2) equipment manufacturers should focus on the FIPS 140-2 to FIPS 140-3 transition and not be additionally impacted by the SP800-90B and SP800-56Br2 effective dates.

DCI therefore elects to allow MB designs to defer SP800-90B and SP800-56Br2 standards changes for FIPS 140-2 validated modules. Compliance is required for FIPS 140-3 designs.

FIPS expertise has counseled DCI that so-called "non-FIPS mode" methods and design work-arounds may be available with respect to SP800-90B and SP800-56Br2. However, DCI is not providing any specific guidance on non-FIPS mode. Instead, MB suppliers should seek guidance from their FIPS compliance laboratory partners regarding MB design requirements and work-around options in this area.

[1] See: https://www.dcimovies.com/FIPS/DCI_Memo_on_FIPS-140-3_2019-12-19.pdf

[2] See: NIST Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf , and
FIPS 140-2 Implementation Guidance 7.18 Entropy Estimation and Compliance with SP 800-90B: https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402IG.pdf

[3] See: NIST Special Publication 800-56B Revision 2: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf , and NIST Special Publication 131A Revision 2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf . Additionally, be advised that the CMVP will not accept modules submissions with non-56Brev2 compliant implementations in Approved Mode after January 1, 2021.