

DCI Informational Bulletin**NIST Standards Evolution & FIPS 140-2 to FIPS 140-3 Transition**

11 November 2010

As has been well socialized in the d-cinema community, the National Institute of Standards and Technology (NIST) has announced changes in two areas that will impact SMPTE standards as well as the DCI Digital Cinema System Specification (DCSS):

- Changes in approved NIST algorithms and usage
- The transition from FIPS 140-2 to FIPS 140-3

This informational bulletin provides guidance on affected DCI requirements.

NIST Algorithm and Usage Changes

Three pending NIST changes have been identified that impact d-cinema specifications:

1. Phase out of the current random number generation method by the end of 2015
2. Use of SHA-1 for signature generation disallowed beyond December 2013
3. Multiple RSA key usage is disallowed beyond December 2010

The above are referenced by FIPS 140 requirements, and the changes will apply to both FIPS 140-2 and 140-3. DCI intends to modify the DCSS so that it references FIPS 140 requirements and SMPTE standards, rather than state explicit cryptographic algorithms or methods. In some instances FIPS provides options; so to assure interoperability, it will be important for a single method to be selected. DCI will work with the current SMPTE NIST Study Group to address such needs and align SMPTE standards with NIST requirements. The first two items above will be addressed in this fashion.

Regarding the third item, the Media Block ¹ private key is currently used for two functions:

- KDM decryption and TLS server session establishment – “RSA Encrypt”
- Security log signing and TLS client session establishment ² – “RSA Sign”

The new NIST prohibition means that for new Media Block designs different key pairs must be used for the RSA encrypt and RSA Sign functions.³

The current process is fully compliant until the retirement of FIPS 186-2, which is as yet unannounced. Additionally, DCI has investigated formal requirements and concluded that the dual key use prohibition will not be enforceable by the FIPS certification process in the short term. However, to eliminate uncertainty and meet long term requirements, DCI will publish DCSS errata to:

1. Remove explicit algorithm requirements and reference FIPS 140 standards,
2. Require that a second digital cinema compliant certificate be added to Media Blocks for purposes of RSA Sign functions.

The DCI Compliance Test Plan (CTP) will be updated to follow the above.⁴

¹ “Media block” refers to the Image Media Block as defined in the DCSS.

² TLS server example is SMS → SM; TLS client example is SM → remote SPB.

³ Such key pairs are associated with device digital certificates.

⁴ DCI has published a memo to its web site discussing CTP change requirements.

DCI recommends that new Media Block designs and devices undergoing upgrades begin to include the RSA Sign certificate as soon as possible, separating certificate usage according to the above “encrypt” and “sign” functional split. The DCSS will mandate that the RSA Sign certificate be bound to the RSA Encrypt certificate. Options for doing this appear to be: ⁵

- Placement of the RSA Encrypt certificate thumbprint or serial number into the RSA Sign certificate’s CommonName field (or other appropriate field).
- Have the RSA Sign certificate be part of the RSA Encrypt certificate chain: Root / Parent CA → Intermediate Cert(s) ⁶ → RSA Sign Cert → RSA Encrypt Cert
- Have security log records carry the RSA Encrypt certificate thumbprint.

Security log reports which have been signed by either single or dual certificate devices can be validated by recipients having manufacturer root certificates, as always.

To align with new NIST requirements, DCI requests that the SMPTE NIST Study Group provide timely standards change and transition recommendations to address:

- Implementation decisions per the above options for the new RSA Sign certificate
- Random number generation alternative(s)
- Retirement of SHA-1 for signature generation ⁷

The affected SMPTE standards have already been identified,⁸ and NIST has provided approved alternatives to the methods / algorithms being retired or phased out.

Transition to FIPS 140-3

Ratification of the FIPS 140-3 standard is expected in Q1 of 2011, which will be followed by a NIST designated transition period. It is anticipated there will be an approximate 6 month overlap period during which in-process 140-2 validations can be completed, and 140-3 validations can be started, after which 140-2 conformance testing will terminate. Equipment suppliers should solicit NIST sources for timing and transition details.

Following FIPS guidelines, once a device has been FIPS 140 certified, it maintains its FIPS certificate indefinitely, *so long as its design (hardware or software) remains unchanged*. Therefore, continued production of such devices will continue to meet DCSS requirements. Should a device undergo a design change, FIPS 140 guidelines dictate the extent that recertification is required. Thus, during the transition period, a new or modified device will undergo either FIPS 140-2 or FIPS 140-3 conformance testing as a function of when it is submitted for FIPS review.⁹

Once the FIPS 140-3 standard is ratified, the DCSS will be updated to reflect the requirements for both 140-2 and 140-3. Prior to the beginning of FIPS 140-3 conformance testing the DCI Compliance Test Plan (CTP) will also be updated to provide for DCI compliance testing of either FIPS 140-2 or FIPS 140-3 certified devices.

⁵ There may be other solutions; the approach must be standardized.

⁶ Intermediate certificates are supplier specific and out of scope

⁷ SHA-1 remains permitted for non-digital signature applications (i.e., HMAC, RBGs, key derivation functions, and hash-only applications) and legacy digital signature verification.

⁸ See “SMPTE Standards Transition Issues for NIST/FIPS Requirements v1.1” report from Taehyun Kim of DRM inside

⁹ Depending upon modification timing, a FIPS 140-2 module may need to move to FIPS 140-3 requirements for recertification.