From: Michael Karagosian
Subject: **[ISDCF] NIST and DCI**
Date: October 2, 2010 9:14:22 PM PDT
To: isdcf@lists.isdcf.com

The issue of a looming problem between NIST and the DCI specification is regularly highlighted in ISDCF meetings, but I doubt many people are familiar with the specifics. There are multiple issues presented by NIST that complicate matters. Currently, the DCI specification requires products to comply to the FIPS 140-2 specification. NIST plans to transition to a revised specification, FIPS 140-3, in the 2011-2012 timeframe. DCI has not taken action as yet in regards to this planned transition. However, a surprise was introduced in January of this year when NIST changed Annex A of FIPS 140-2, the NIST specification for which DCI currently requires compliance. The transition period for this revision is taking place right now, in this calendar year. NIST says that after December 31 of 2010, it will no longer accept test results from products that comply with the older version of FIPS 140-2.

There are some notable exceptions to this deadline that benefit the digital cinema community. But one very significant issue remains regarding dual use of the asymmetrical key-pair in the media block, for which the December 31 deadline is still intact. The primary use of the media block key-pair is to encrypt and decrypt the KDM. But the DCI spec calls for other uses of this key-pair, as well. The dilemma presented by FIPS 140-2 is discussed in my report in the September issue of the SMPTE Journal, which is online at http://mkpe.com/report/.

To summarize the problem: SMPTE 430-5, one of the standards that establishes the DCI-compliant Security Log, requires that the media block certificate (public key) be used to digitally sign the media block security logs. This behavior is mandated by the DCI specification, in addition to other DCI-specified uses. The older version of FIPS 140-2 allows this multi use of the media block key-pair through its normative reference to FIPS 186-2. However, the newer FIPS 186-3 forbids the multi-use case. FIPS 140-2 Annex A was updated in January 2010 to now require conformance with FIPS 186-3. Further, a NIST discussion paper on their website requires compliance to FIPS 186-3 after December 31, 2010.

Below is the relevant text taken from SMPTE 430-5, FIPS 186-3, and the NIST discussion paper:

* From SMPTE 430-5 Security Log Event Class and Constraints, Section 6.2:
"Each Signature shall be signed with the Digital Cinema Certificate of the Security Device that generates the Log Record or sequence of Log Records."
(A copy of SMPTE 430-5 can be purchased from the SMPTE web site at http://store.smpte.org/product-p/smpte%200430-5-2008.htm.) Note that the other uses mandated in the DCI spec of the media block's Digital Cinema Certificate is to create the KDM and to establish a TLS session between media block and projector.

* From FIPS 186-3, page 11 (http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf):
"However, a key pair used for digital signature generation and verification as specified in this Standard shall not be used for any other purpose."

* From NIST DISCUSSION PAPER: The Transitioning of Cryptographic Algorithms and Key Sizes (http://csrc.nist.gov/groups/ST/key_mgmt/documents/Transitioning_CryptoAlgos_070209.pdf):
"New implementations designed to conform to FIPS 186-2 may be tested by the labs until December 31, 2010, after which only implementations claiming conformance to FIPS 186-3 will be tested for validation."

If no action is taken by DCI, the result will be that the DCI specification will be in conflict with itself after December 31. The DCI spec will call for compliance to FIPS 140-2, which will no longer allow the media block key-pair applications that are also required by the DCI specification, including the KDM as it is defined today.

The least disruptive action that will solve this problem is to privately publish the earlier version of FIPS 140-2, call it XYZ 140-2. This, plus private publication of supporting standards such as a re-published XYZ 186-2, will allow digital cinema products to continue to be manufactured, and for KDMs to be produced, without change. Since the NIST standards are public documents, paid for by US taxpayers, re-publication under a different name will not violate copyrights. Further, testing agencies will not be conflicted in testing for compliance to a privately published XYZ 140-2. In contrast, if asked to test to FIPS 140-2, the same testing agencies are required by NIST to test to the latest version.

This particular solution could remain stable for quite some time. It solves an important issue that DCI is now facing: that of reliance on standards from an agency whose scope of responsibilities does not include the motion picture industry. Complaints by the motion picture industry to NIST fall on deaf ears, as NIST's scope is to support security standards for US government agencies. In turn, the US government equipment updates required by NIST are paid for by US tax dollars. Digital cinema upgrades will not be paid for by US tax dollars. Decoupling from NIST, while embracing its past work, would be an important move to ensure stability for the digital cinema format.

Other solutions no doubt exist. What I described is the solution I favor. I invite others to propose their own. In particular, I invite DCI members to speak up. The most harmful action to take at this point is to take no action.

Best,
Michael