DCI Digital Cinema Initiatives, LLC

2015 Update to FIPS 140-3 Transition
October 21, 2015

Background:
In March 2009 and November 2010 DCI posted informational bulletins to its website regarding National Institute of Standards and Technology (NIST) security developments that were anticipated to impact the digital cinema community and our reliance on FIPS 140-2 for implementation guidance and compliance testing. Some of these NIST developments have had an impact on the DCI Specification:

- New rules regarding RSA key usage resulted in the need for two certificates in Media Blocks.
- The deprecated Random Number Generator (RNG) used for content integrity checks will be supplemented by having the KDM carry the Message Integrity Code (MIC) key.

FIPS 140-3 Transition:
In 2005 NIST began a process to transition from FIPS 140-2 to a newer FIPS 140-3 set of requirements. Following developments, DCI issued the above informational bulletins to advise the D-Cinema community about the probable impact of the transition to FIPS 140-3, which would begin upon U.S. government ratification.

The FIPS 140-3 transition process timetable, though still visible (as of the date of this posting) on the NIST website (http://csrc.nist.gov/groups/ST/FIPS140_3/), has been stalled since the fall of 2012. On August 15, 2015, NIST issued a request for public comment regarding replacing the transition to FIPS 140-3 with an ISO/IEC alternative standard: ISO/IEC 19790:2012 "*Security Requirements for Cryptographic Modules*," to be used as the U.S. Federal Standard for cryptographic modules (see the same NIST website).

DCI has not undertaken a detailed review of the implications of this potential NIST direction, however it believes that the D-Cinema community's security interests would be maintained under either the proposed FIPS 140-3 or the ISO/IEC alternative (as well as with the FIPS 140-2 status quo).

This bulletin is issued as an informational update, and supports our continuing goal of keeping the industry informed concerning developments that may impact D-Cinema.