

REVISION TO DCI *DIGITAL CINEMA SYSTEM SPECIFICATION* *COMPLIANCE TEST PLAN, VERSION 1.2*

CTP Revision items continue to be evaluated and will be posted after agreement by the DCI membership that the specific CTP Revision needs to modify the DCI Digital Cinema System Specification, Compliance Test Plan, Version 1.2. Suggested CTP Revision issues may be emailed to dci.info@dcimovies.com. Please include "CTP Revision" in the subject line.

DCI DCSS CTP v1.2 REVISION

25 SEPTEMBER 2015

Revision Date	Revision Stage Type	CTP v1.2 Page No.	Sections Affected	Problem Description	Revision Description
September 25, 2015	1	346	9.5.2 LE Key Generation, item 2a	Item 2a references FIPS 140-2 area 1 ("cryptographic module specification") for key generation. With the DCSS erratum changing area 1 from FIPS level 3 to level 2, the key generation requirements being evaluated by this item need to be re-directed to area 7 "Cryptographic Key Management," which maintains level 3 constraints.	Replace text as indicated below.

Current CTP 1.2 Text – Section 9.5.2 – Procedure Test 2a:

- a. Link Encryptor (LE) keys are 112 bits in length for TDES or 128 bits in length for AES, and that those keys are generated according to the requirements of the [DCI-DCSS-1-2], Section 9.7.6 and [FIPS-140-2] level 3 "cryptographic module specification" specifications (per the requirements of [DCI-DCSS-1-2], Section 9.5.2.5).

Revised CTP 1.2 Text – Section 9.5.2 – Procedure Test 2a:

- a. Link Encryptor (LE) keys are 112 bits in length for TDES or 128 bits in length for AES, and that those keys are generated according to the requirements of the [DCI-DCSS-1-2], Section 9.7.6 and [FIPS-140-2] level 3 "cryptographic key management" area 7 requirements (per the requirements of [DCI-DCSS-1-2], Section 9.5.2.5).