DRAFT ISDCF Doc5 - Guideline Formulations for Interop and SMPTE KDMs

Last revised 03 November 2011

Actual DCI-compliant systems are now starting to appear in the field. Some KDM providers have been sending KDMs containing ContentAuthenticator to be used with Interop content. This will not work on a DCI-compliant system. When ContentAuthenticator is present (as discussed many times in ISDCF) the DCI-compliant system will use DCI-compliant DCP checking, which requires a SMPTE ST 429-2-compliant DCP.

There are four existing formulations of SMPTE 430-1 KDM:

1. "Transitional 1" -- No ContentAuthenticator element, DeviceList contains only the recipient's certificate thumbprint (DEPRECATED).

2. Modified "Transitional 1" -- No ContentAuthenticator element, DeviceList contains only DCI "assume trust" certificate thumbprint.

3. "DCI any" -- ContentAuthenticator element is present, DeviceList contains only DCI "assume trust" certificate thumbprint.

4. "DCI specific" -- ContentAuthenticator element is present, DeviceList contains one or more valid remote SPB or projector SPB thumbprints.

*The DCI "assume trust" thumbprint is the Base-64 encoded SHA-1 digest of a zero-length input, i.e., "2jmj7l5rSw0yVb/vlWAYkK/YBwk="

Note: Role of Certificate that Signs the KDM and CPL:
The KDM shall be signed using a leaf certificate with a SubjectName having the CS role exclusively. (See ST 420-2 for more information about certificate roles). DCI recommends the use of CPL signature in those cases where the CPL references encrypted track files (See DCSS 5.2.3 "Packaging Concepts".) The rationale for KDM interpretation presented above explains why this is a desirable practice. It should be noted however that DCI does not require that a player reject a CPL that is not signed, even in the case where the CPL references encrypted track files.

The KDMs must be paired with content as follows:

a) A "DCI" KDM, whether "any" or "specific", must be used only with SMPTE 429-2 content.

b) "Transitional 1" KDMs must be used only with Interop content. This formulation is DEPRECATED and WILL NOT WORK on most DCI-compliant systems. KDM providers are strongly encouraged to move to Modified "Transitional 1" KDMs for Interop content.

c) Modified "Transitional 1" KDMs may be used with Interop or SMPTE 429-2 content.

Recommended logic for allowing Interop playback on a DCI-compliant device:

1. DCI compliance is tested by executing the test procedures using the reference test material. All of the KDMs in the reference test material contain an instance of the ContentAuthenticator element.

2. It is now common industry practice to eliminate the ContentAuthenticator from the KDM when making a KDM for Interop content (per ISDCF participants).

Considering (1) and (2) above, if an implementation a) *enables* DCI-compliant DCP checking when ContentAuthenticator is *present* in the KDM and b) *disables* DCI-compliant DCP checking when ContentAuthenticator is *not present* in the KDM, then the implementation will both pass the DCI CTP *and* play Interop content.

Rationale for using ContentAuthenticator as a flag for allowing Interop: When ContentAuthenticator is not present in the KDM it is possible to alter the Composition in ways that would still allow playout. Given this vulnerability, there is little use in trying to enforce strict checking on the Composition in that case. Content owners that want to ensure that altered Compositions will not play must require that ContentAuthenticator be present in all KDMs.