DRAFT ISDCF Doc5 - Guideline for SMPTE KDMs and Certificates Behaviors

Last revised 16 July 2012

1 SMPTE KDM Formulations

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 five existing formulations of SMPTE ST 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. “Multiple Modified Transitional 1” -- No `ContentAuthenticator` element, `DeviceList` contains two or more valid remote SPB or projector SPB certificate thumbprints.
4. "DCI any" -- `ContentAuthenticator` element is present, `DeviceList` contains only DCI "assume trust" certificate thumbprint.
5. "DCI specific" -- `ContentAuthenticator` element is present, `DeviceList` contains one or more valid remote SPB or projector SPB certificate thumbprint(s).

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:
The KDM shall be signed using a leaf certificate with a SubjectName having zero to many role(s) (See SMPTE ST 430-2 for more information about certificate roles). DCI requires the use of CPL signature in those cases where the CPL references encrypted track files (See DCI Specification v1.2, section 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 - except in the special case where the `ContentAuthenticator` element is present in the KDM.

The above SMPTE KDMs must be paired with content as follows:

a) A "DCI" KDM, whether "any" or "specific", must be used only with SMPTE ST 429-2 content. A "DCI any" KDM is for single remote SPB (or single projector SPB) setup only, while a "DCI specific" KDM is for single or for multiple remote SPB (or projector SPB) setup.

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" (for single remote SBP or projector SPB setup only) or “Multiple Modified Transitional 1” KDMs (required for multiple remote SPB or multiple projector SPB setup) for Interop content.

c) “Modified Transitional 1" and “Multiple Modified Transitional 1” KDMs may be used with Interop or SMPTE ST 429-2 content.

2 Recommended Logic for Allowing Interop Content 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 (with the exception of the checks listed in section 3 below) 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 content playback: 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 who want to ensure that altered Compositions will not play must require that the SMPTE DCP be used and that the `ContentAuthenticator` element be present in all KDMs.

3 Required Checks

The checks listed in the paragraphs 3.1 and 3.2 shall always be enforced (for all content types – Interop or SMPTE), whether the KDM `ContentAuthenticator` element is present or not.

3.1 KDM Checks

- **KDM Format:** A SMPTE KDM shall comply with SMPTE ST 430-1:2006 and ST 430-1-A1:2009. A SMPTE KDM failing such compliance shall NOT allow playback.
- **KDM `DeviceList` Element**: `DeviceList` element check failure shall result in playback rejection in ALL cases. Also, the certificates referenced by the KDM `DeviceList` element shall successfully pass the applicable validation rules identified in Annex A. Failure to pass identified certificate validation rules shall make the KDM un-usable to allow playback in ALL cases.

  Note: The usage of a “Modified Transitional 1” KDM or of a “DCI any” KDM shall NOT allow playback on a multiple remote SPB (or multiple projector SPB) configuration. To allow playback on multiple remote SPB (or multiple projector SPB) setup, either a “Multiple Modified Transitional 1” KDM or a “DCI specific” KDM shall be used.

- **KDM Validity Time Window**: Playback outside of the KDM time window (defined by the `ContentKeysNotValidBefore` and `ContentKeysNotValidAfter` elements) shall be forbidden in ALL cases – unless the playback started within the time window, then it can be extended up to 6 hours beyond the time window as allowed by the DCI Specification v1.2.

- **KDM Signature:** a KDM with an incorrect signature shall NOT allow playback. Also, the certificates used in the KDM signing chain shall successfully pass the applicable validation rules identified in Annex A. Failure to pass identified certificate validation rules shall make the KDM un-usable to allow playback in ALL cases.

3.2 CPL Checks

- **CPL `Id`:** The CPL `Id` shall be checked against the KDM `CompositionPlaylistId` element's value in ALL cases. Failure to match the KDM `CompositionPlaylistId` shall result in playback rejection in ALL cases. The CPL id shall also be checked against the CompositionPlaylistId value located in all the KDM's `CipherData` structure(s). Failure to match all the CompositionPlaylistId value(s) located in the KDM's `CipherData` structure(s) shall result in playback rejection in ALL cases.
- **CPL Signature:**
  - In the case of a KDM with the `ContentAuthenticator` element present, a failed CPL Signature failure shall always result in playback rejection. In such case, the certificates used in the CPL signing chain shall successfully pass the applicable validation rules identified in Annex A. Failure to pass identified certificate validation rules shall result in playback rejection as well.
  - In the case of a KDM without `ContentAuthenticator`, a CPL signature shall NOT result in playback rejection. It is recommended that a CPL signature failure be logged in such cases, while the playback shall NOT be forbidden because of this failure. In such case, the certificates used in the CPL signing chain do not have to pass the applicable validation rules identified in Annex A. Failure to pass identified certificate validation rules shall NOT result in playback rejection.

4 Authoritative KDM

Security Managers may be faced with the case of having multiple "valid" KDMs ingested at the same time, each targeting the same CPL. For a given CPL (and at a given time), a "valid" KDM is defined as a KDM that successfully passes all the KDM checks identified in section 3.1 - meaning that it would allow playback on the connected equipment.

Therefore at any instant in time for a particular CPL, Security Managers shall select one and only one KDM out of potentially many. This single KDM shall be referred to as the "Authoritative KDM". Security Managers shall follow the following precedence rules in order to select such "Authoritative KDM":

1) If at a given time (prior to Pre-Show operation – as defined by the DCI specification v1.2) there is only one KDM that is "valid" for a given CPL, that KDM shall be the Authoritative KDM.
2) If at a given time (prior to Pre-Show operation) there are multiple "valid" KDMs, the KDM with the latest (i.e., most recent) `IssueDate` (at the time Pre-Show operation is performed) shall be the Authoritative KDM.

   Note: In the unlikely (but possible) case of two or more KDM candidates having equal `IssueDate` values, the system behavior is undefined.
3) If a new "valid" KDM is ingested after or during Pre-Show operation, it shall NOT be taken into account for the Authoritative KDM selection - if it is ingested before Pre-Show operation, it shall be taken into account for the Authoritative KDM selection.

5 `ContentAuthenticator` Element

In ALL cases (for SMPTE contents), the KDM `ContentAuthenticator` field (if present) shall reference only the CPL signer certificate (the Leaf certificate) and NOT any other certificate of the CPL signer chain.

Background: The CPL signer certificate is the only certificate that must comply with both SMPTE and DCI requirements. DCI Specification v1.2 requires in section 9.4.3.5 that "*For encrypted content, validation shall be by cross checking that the associated KDM's `ContentAuthenticator` element matches a certificate thumbprint of one of the certificates in the CPL's signer chain (see item 1 above), and that such certificate indicate only a "Content Signer" (CS) role*". And per its definition in SMPTE ST 430-2, the CS role can only be carried by a Leaf certificate.

6 Self-Signed Certificates

Root certificates are self-signed CA certificate, and they shall NOT be used to sign a CPL, a KDM or a PKL.

A self-signed SMPTE certificate can be used to sign a CPL, KDM or PKL only:

- If it complies with SMPTE ST 430-2:2006, taking into account the applicable rules identified in Annex A
- If in its BasicConstraint field, the CA attribute is false, and the PathLenConstraint is absent (or zero)
- If the DigitalSignature flag is true in its KeyUsage.
- And, only in the case of SMPTE CPL signing, if it carries the CS role only.

Such self-signed certificate shall NOT be considered a ”Root certificate”.

Note: Using such self-signed certificate is allowed, while it is not recommended. In fact, this would make the signing chain length equal to one. SMPTE ST 430-2 explains that a minimum chain length of three certificates is recommended - however, playback shall not be forbidden because of a chain length shorter than three.

ANNEX A: SMPTE Certificates Validation Contexts

SMPTE ST 430-2 defines certificate validation rules. These rules are numbered from 1 to 19, and they are referenced in the first column of the table below. Each one of the following columns defines one certificate validation context, each context being independent from the others.

When a check has to be enforced, the validation rules identified below shall be enforced as part of the check for all certificates involved in this check (e.g. KDM `DeviceList` element check requires checking all Remote SPB certificates listed in this `DeviceList` element). If a validation rule is flagged as N/A or Best Effort in the table below, the rule shall not be enforced in the corresponding context.

If a certificate is failing one or more of the validation rule(s) below as part of a check that shall not be enforced (e.g. CPL signature check when `ContentAuthenticator` element is absent), this certificate validation failure shall not result in playback rejection.

	Interop CPL signing chain (with SMPTE Certificate)	Interop PKL signing chain (with SMPTE Certificate)	SMPTE CPL signing chain	SMPTE PKL signing chain	SMPTE KDM signing chain	Remote SPB certificate chain	Secure Log signing chain	SMPTE FLM signing chain	KDM recipient certificate chain
Rule #1: DER	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #2: Version	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #3: Unrecognized Extensions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #4: Required Fields	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #5: PathLenConstraint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #6: KeyUsage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #7: ON	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #8: Leaf Certificate Role	0 to many role(s)	0 to many role(s)	One role: CS only	0 to many role(s)	0 to many role(s)	1 to many role(s): Req: LD	1 to many role(s): Req: SM or LS	0 to many role(s)	1 to many role(s): Req: SM
Rule #9: Desired Time	CPL IssueDate	PKL IssueDate	CPL IssueDate	PKL IssueDate	KDM IssueDate and current time	Current time	Log creation date	FLM IssueDate	Current time
Rule #10: Signature Algorithm	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #11: RSA Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #12: Revoked Keys/Certificates	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes
Rule #13: DnQualifier	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #14: AuthorityKeyId	Yes	Yes	Yes	Yes	Yes	Best Effort	Yes	Yes	Yes
Rule #15: Signature Value	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #16: Minimum Chain Length	1 (*)	1 (*)	1 (*)	1 (*)	1 (*)	1 (*)	1 (*)	1 (*)	1 (*)
Rule #17: Issuer	Yes	Yes	Yes	Yes	Yes	Best Effort	Yes	Yes	Yes
Rule #18: Validity Dates	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule #19: Trusted Root	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes

(*) Note: A minimum chain length of 1 is allowed. However, a minimum chain length of three certificates is highly recommended in ALL cases.