**Amendment 1-2009 to SMPTE 430-1-2006**

**SMPTE STANDARD**

# D-Cinema Operations — Key Delivery Message — Amendment 1

## Background

Since publication of SMPTE 430-1 D-Cinema Operations Key Delivery Message, four issues and one note have been identified:

In Section 5.1, the MessageType value defined is legitimate but not of the expected form.

In Section 5.2.1, the structure and content of the Recipient element should be more explicitly defined.

In Section 5.2.5.3, the prose (normative) and XML schema (normative) for DeviceList disagree on minimum number of elements. XML should be corrected to match prose.

In Sections 5.2.6 and 5.2.7, ContentKeysNotValidBefore and ContentKeysNotValidAfter time notation should be defined more rigorously.

In Annex A, clarify informative note about number of keys per KDM.

Amendment of the specification will encourage correct, interoperable implementation.

## Amendment

Upon approval of this amendment, SMPTE 430-1 shall be revised according to the following:

The following informative note shall be added after the normative text in Section 5.1 (page 6):

> Informative Note: The MessageType value "http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type" is legal and correct, but, in the event a future revision of the KDM specification requires a revision to the MessageType value, the MessageType value should follow the pattern http://www.smpte-ra.org/430-1/2006/KDM and match the target namespace of the schema.

The normative text in Section 5.2.1 (page 7), which currently reads:

> The Recipient field shall identify the intended certificate/subject of this KDM. The public key identified in this certificate is used to encrypt the keys found in the AuthenticatedPrivate portion of the KDM message. An X.509 certificate is identified by the name of the Certificate Authority (CA) that issued it, called IssuerName, and the unique serial number assigned by the CA, called SerialNumber. To aid in routing of KDMs, the X.509 SubjectName that is found in the certificate shall also be placed in the Recipient element. The Distinguished Name value in the X509IssuerName element shall be compliant with RFC 2253 [RFC2253].

shall be replaced in its entirety by:

Approved
January 9, 2009

> The Recipient element identifies the intended certificate of this KDM. The public key identified in this certificate is used to encrypt keys and other information in the AuthenticatedPrivate element of the KDM. To uniquely identify the certificate, the Recipient element shall contain two elements - X509IssuerSerial and X509SubjectName. The X509IssuerSerial element identifies the name of the Certificate Authority (CA) that issued the certificate, called X509IssuerName, and the unique serial number assigned by the CA, called X509SerialNumber.
>
> The X509SubjectName element shall contain the X.509 subject distinguished name found in the certificate. The X.509 distinguished name values in X509IssuerName and X509SubjectName elements shall be compliant with RFC2253 [RFC2253].

In the normative XML schema in Annex C (page 17), the XML statement which currently reads:

```
<xs:element name="CertificateThumbprint" type="ds:DigestValueType" minOccurs="0"
maxOccurs="unbounded"/>
```

shall be replaced by:

```
<xs:element name="CertificateThumbprint" type="ds:DigestValueType" minOccurs="1"
maxOccurs="unbounded"/>
```

The normative text in Section 5.2.6 (page 9), which currently reads:

> The time shall be in the form of a Universal Coordinated Time timestamp as specified in RFC 3339. Timestamps shall not include fractional seconds.

shall be replaced by:

> The time shall be 25 characters in the form of a Universal Coordinated Time timestamp as specified in RFC 3339 [Time] section 5.6 date-time. Timestamps shall not include fractional seconds (RFC 3339 time-secfrac). Timestamps shall not use 'Z' ('Zulu') time zone offset notation.

The normative text in Section 5.2.7 (page 10), which currently reads:

> The time shall be in the form of a Universal Coordinated Time timestampas specified in RFC 3339. Timestamps shall not include fractional seconds.

shall be replaced by:

> The time shall be 25 characters in the form of a Universal Coordinated Time timestamp as specified in RFC 3339 [Time] section 5.6 date-time. Timestamps shall not include fractional seconds (RFC 3339 time-secfrac). Timestamps shall not use 'Z' ('Zulu') time zone offset notation.

The informative text in Annex A (page 14), which currently reads:

> This allows a single message to contain all the keys needed to decrypt media that uses multiple keys. However, a rights owner could choose to deliver each content decryption key in a separate KDM.

shall be replaced by:

> This allows a single message to contain all the keys needed to decrypt media that uses multiple keys.