SMPTE 430-7-2008

SMPTE STANDARD

D-Cinema Security — Facility List Message

Table of Contents

Page

3 Barker Avenue, White Plains, NY 10601
(914) 761-1100

Approved
October 28, 2008

Foreword

SMPTE (the Society of Motion Picture and Television Engineers) is an internationally-recognized standards developing organization. Headquartered and incorporated in the United States of America, SMPTE has members in over 80 countries on six continents. SMPTE's Engineering Documents, including Standards, Recommended Practices and Engineering Guidelines, are prepared by SMPTE's Technology Committees. Participation in these Committees is open to all with a bona fide interest in their work. SMPTE cooperates closely with other standards-developing organizations, including ISO, IEC and ITU.

SMPTE Engineering Documents are drafted in accordance with the rules given in Part XIII of its Administrative Practices.

SMPTE Standard 430-7 was prepared by Technology Committee DC28.

Intellectual Property

At the time of publication no notice had been received by SMPTE claiming patent rights essential to the implementation of this Standard. However, attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. SMPTE shall not be held responsible for identifying any or all such patent rights.

1 Scope

This specification defines a “Facility List Message” (FLM) for use in Digital Cinema (D-Cinema) systems. The FLM has been designed to deliver digital certificate information between exhibition sites (facilities), KDM distributors, and/or content owners. The FLM carries three classes of information:

- Identification and useful information pertaining to the exhibition complex (FacilityInfo),
- Optionally, descriptive information about the device (DeviceDescription)
- The digital cinema certificate(s) (KeyInfo) information of the device

The FLM is based on the D-Cinema generic Extra-Theater Message (ETM) format specified in SMPTE 430-3. It uses XML to represent the D-Cinema Digital Certificate information specified in SMPTE 430-2, and provides security using standardized XML encryption and signature primitives. The FLM message uses X.509 digital certificates, constrained for the digital cinema application in SMPTE 430-2, to provide authentication and trust.

Note: The brackets convention “[…]” as used herein denotes either a normative or informative reference.

2 Conformance Notation

Normative text is text that describes elements of the design that are indispensable or contains the conformance language keywords: "shall", "should", or "may". Informative text is text that is potentially helpful to the user, but not indispensable, and can be removed, changed, or added editorially without affecting interoperability. Informative text does not contain any conformance keywords.

All text in this document is, by default, normative, except: the Introduction, any section explicitly labeled as "Informative" or individual paragraphs that start with "Note:”

The keywords "shall" and "shall not" indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

The keywords, "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

The keywords "may" and "need not" indicate courses of action permissible within the limits of the document.

The keyword “reserved” indicates a provision that is not defined at this time, shall not be used, and may be defined in the future. The keyword “forbidden” indicates “reserved” and in addition indicates that the provision will never be defined in the future.

A conformant implementation according to this document is one that includes all mandatory provisions ("shall") and, if implemented, all recommended provisions ("should") as described. A conformant implementation need not implement optional provisions ("may") and need not implement them as described.

Unless otherwise specified, the order of precedence of the types of normative information in this document shall be as follows. Normative prose shall be the authoritative definition. Tables shall be next, followed by formal languages, then figures, and then any other language forms.

3 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent edition of the standards indicated below.

[CountryCode] ISO 3166, Codes for the Representation of Names of Countries, 1993. See: http://www.iso.org/iso/en/prods-services/iso3166ma/index.html

[CountryDialingCode] ITU-T, List of ITU-T Recommendation E.164 assigned country codes, October 2006. See http://www.itu.int/pub/T-SP-E.164D-2006/en

[Data Types] SMPTE 433-2008, D-Cinema — XML Data Types

[DateTime] IETF RFC 3339, Date and Time on the Internet: Timestamps. G. Klyne and C. Newman. July 2002. See: http://www.ietf.org/rfc/rfc3339.txt

[Email] IETF RFC 822, Standard for the Format of ARPA Internet Messages, D.H. Crocker, August 1982. See http://www.ietf.org/rfc/rfc0822.txt

[ETM] SMPTE 430-3-2006, D-Cinema Operations — Generic Extra Theater Message Format

[URI] IETF RFC 2396, Uniform Resource Identifiers (URI): Generic Syntax. T. Berners-Lee, R. Fielding, and L. Masinter. August 1998. See http://www.ietf.org/rfc/rfc2396.txt

[UUID] "A Universally Unique Identifier (UUID) URN Namespace" July 2005. See: http://www.ietf.org/rfc/rfc4122.txt

[KeyInfo] "The KeyInfo Element." See http://www.w3.org/TR/xmldsig-core/#sec-KeyInfo

[XML] World Wide Web Consortium (W3C) (2004, February 4). *Extensible Markup Language (XML) 1.0 (Third Edition)*

[XML Schema] World Wide Web Consortium (W3C) (2004, October 28). *XML Schema Part 1: Structures (Second Edition)*

[XML Schema] World Wide Web Consortium (W3C) (2004, October 28). *XML Schema Part 2: Datatypes (Second Edition)*

4 Glossary

The following paragraphs define the acronyms used in this document:

Base64:	A printable encoding of binary data. See [Base64].
ETM:	Extra Theater Message [See SMPTE 430-3]
FLM:	Facility List Message
IETF:	Internet Engineering Task Force standards group.
IP:	Internet Protocol. An IETF standard.
ISO:	International Standards Organization
KDM:	Key Delivery Message (See SMPTE 430-1]
SM:	Security Manager
TMS:	Theater Management System
X.50:	A widely used and supported digital certificate standard.
XML:	Extensible Markup Language

5 Overview of the FLM

5.1 Basic FLM Elements and D-Cinema Relationships (Informative)

This standard presents a specification for the Facility List Message (FLM) for use in a Digital Cinema (D-Cinema) system. The D-Cinema Facility List Message is normally sent:

1. Between a theater facility and a KDM distributor, or
2. Between a KDM distributor and a content owner, or
3. Between a KDM distributor or a content owner, and a certificate authentication entity.

D-Cinema systems require that content keys and "trusted equipment" information (Trusted Device List or TDL) be created for use in exhibition facilities. The vehicle for communicating this information to the facility is the Key Delivery Message (KDM), specified in SMPTE 430-1. The FLM supplies the essential information required to create the KDMs for an exhibition facility. The message contains the D-Cinema Digital Certificate information, specified in SMPTE 430-2, of each security-related device in the facility. The general flow of information leading to the creation of KDMs is illustrated in Figure 1.

Note that the <KeyInfo> element should contain the full certificate chain for ease of processing.

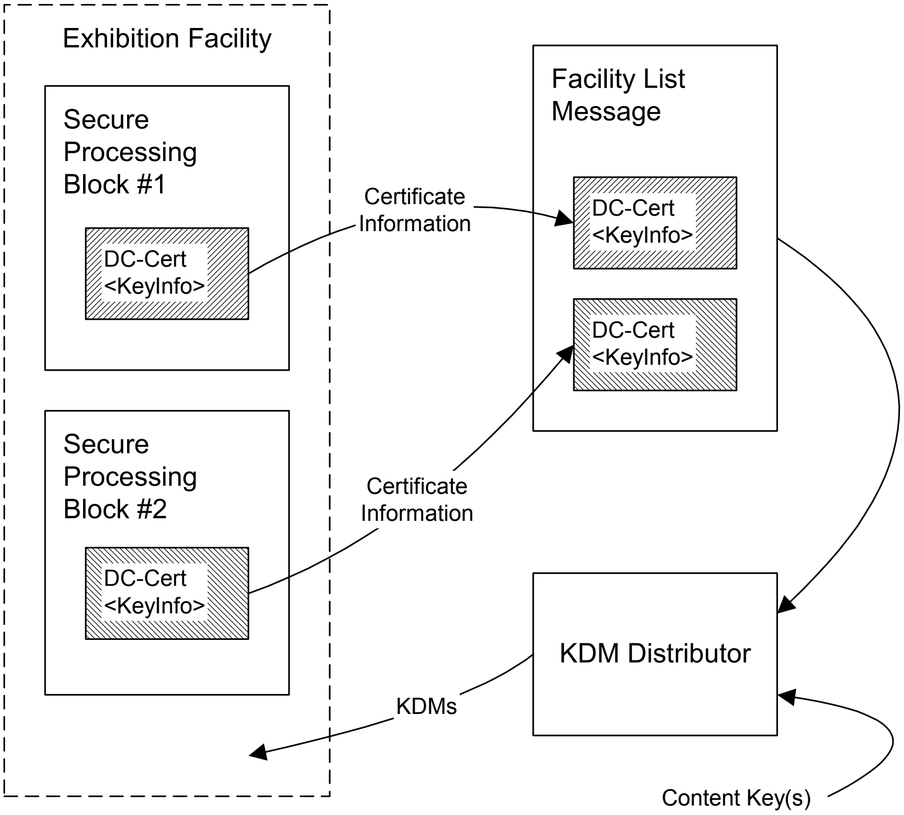


Figure 1 – FLM Information Flow

The FLM message is a particular instance of the generic XML security wrapper defined by the D-Cinema Generic Extra Theater Message Format specified in SMPTE 430-3, and uses digital certificates defined by the D-Cinema Digital Certificate specified in SMPTE 430-2. This document defines the characteristics that are specific to the FLM, and should be followed in combination with SMPTE 430-3, which in turn references the digital certificate specification.

The FLM uses XML to communicate the digital certificate data and provides security using the XML Encryption and Signature primitives. As there may be a need to authenticate each device certificate contained by the recipient of the FLM, the complete device certificate is carried. The device certificates contain only Public Key information and not Private Keys, so there is no risk of exposing secrets. The FLM does not utilize encryption to secure its payload, and so does not employ the Authenticated Private element of the ETM. However, the FLM employs the digital signature of the ETM to allow downstream entities to authenticate its payload and origin.

The essential payload of the FLM is illustrated in Figure 2 below.

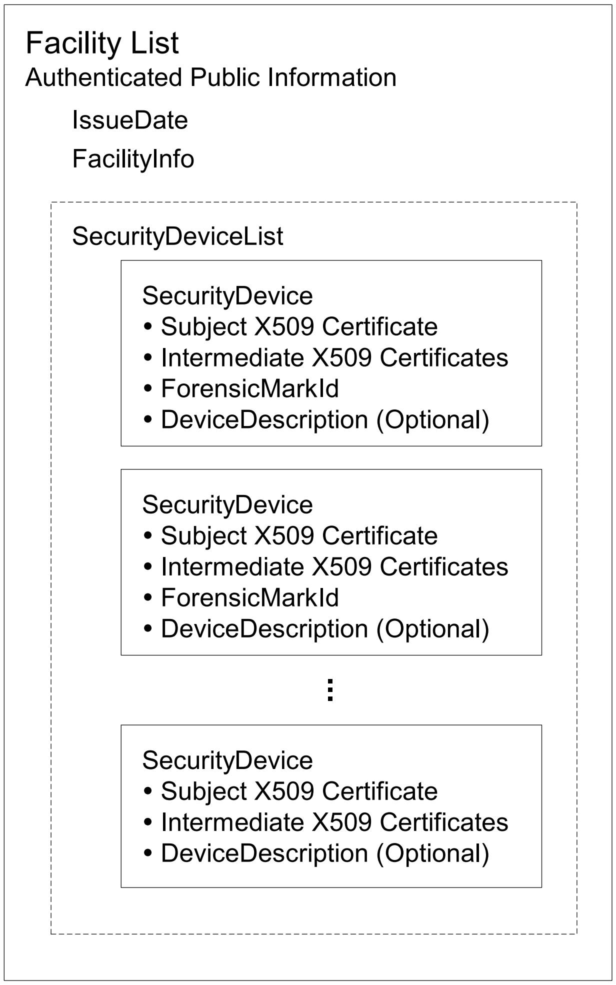

Facility List
Authenticated Public Information
IssueDate
FacilityInfo
SecurityDeviceList
SecurityDevice
• Subject X509 Certificate
• Intermediate X509 Certificates
• ForensicMarkId
• DeviceDescription (Optional)
SecurityDevice
• Subject X509 Certificate
• Intermediate X509 Certificates
• ForensicMarkId
• DeviceDescription (Optional)
⋮
SecurityDevice
• Subject X509 Certificate
• Intermediate X509 Certificates
• DeviceDescription (Optional)

Figure 2 – FLM Payload

`SecurityDevice` elements contain both descriptive and security-related information, and are listed in no particular order or organization. Subject X509 certificates and intermediate X509 certificates refer to elements of the certificate chain. The leaf certificate contained in each `SecurityDevice` element corresponds to either a KDM recipient or an entry in the `DeviceList` of the KDM. Note that the example in Figure 2 is only illustrative of how the FLM is constructed.

5.2 XML File Structure

The structures defined in this document are represented using the Extensible Markup Language (XML) [XML 1.0], and specified using XML Schema [XML Schema Part 1: Structures] and [XML Schema Part 2: Datatypes]. This specification shall be associated with a unique XML namespace name [Namespaces in XML]. The namespace name shall be the string value "`http://www.smpte-ra.org/schemas/430-7/2008/FLM`". This namespace name conveys both structural and semantic version information, but does not serve the purpose of a traditional version number field.

Table 1 lists the XML namespace names used in this specification. Namespace names are represented as Uniform Resource Identifier (URI) values [RFC 2396].[1]

Table 1 – XML Namespaces

Qualifier	URI
dcml	`http://www.smpte-ra.org/schemas/433/2008/dcmlTypes`
ds	`http://www.w3.org/2000/09/xmldsig#`
etm	`http://www.smpte-ra.org/schemas/430-3/2006/ETM`
flm	`http://www.smpte-ra.org/schemas/430-7/2008/FLM`
xenc	`http://www.w3.org/2001/04/xmlenc#`
xs	`http://www.w3.org/2001/XMLSchema`
xsi	`http://www.w3.org/2001/XMLSchema-instance`

The URIs found in Table 1 are normative. The namespace qualifier values (also called namespace prefixes in XML jargon) used in Table 1 and elsewhere in this document, namely "dcml", "ds," etm," "flm," "xenc," and "xsi", are not normative. Specifically, they may be replaced in instance documents by any XML compliant namespace prefix. In other words, implementations shall expect any arbitrary XML compliant namespace prefix value that is associated with a URI from Table 1.

5.3 XML Overview of the FLM (Informative)

Note: See Appendix C for the normative XML schema that defines the FLM. The XML diagrams in this document conform to the legend given in Section 9.

An FLM is an ETM instance which has in the `RequiredExtensions` element a child element named `FLMRequiredExtensions`.

The `FLMRequiredExtensions` element contains Digital Cinema Certificate information of secure devices within an exhibition facility complex, but does not carry or otherwise expose secret private key information. Optionally, the element may also contain Forensic Mark information, and information about the device itself.

[1] Readers unfamiliar with URI values as XML namespace names should be aware that although a URI value begins with a "method" element ("http" in this case), the value is designed primarily to be a unique string and does not necessarily correspond to an actual on-line resource. Applications implementing this standard should not attempt to resolve URI values on-line.

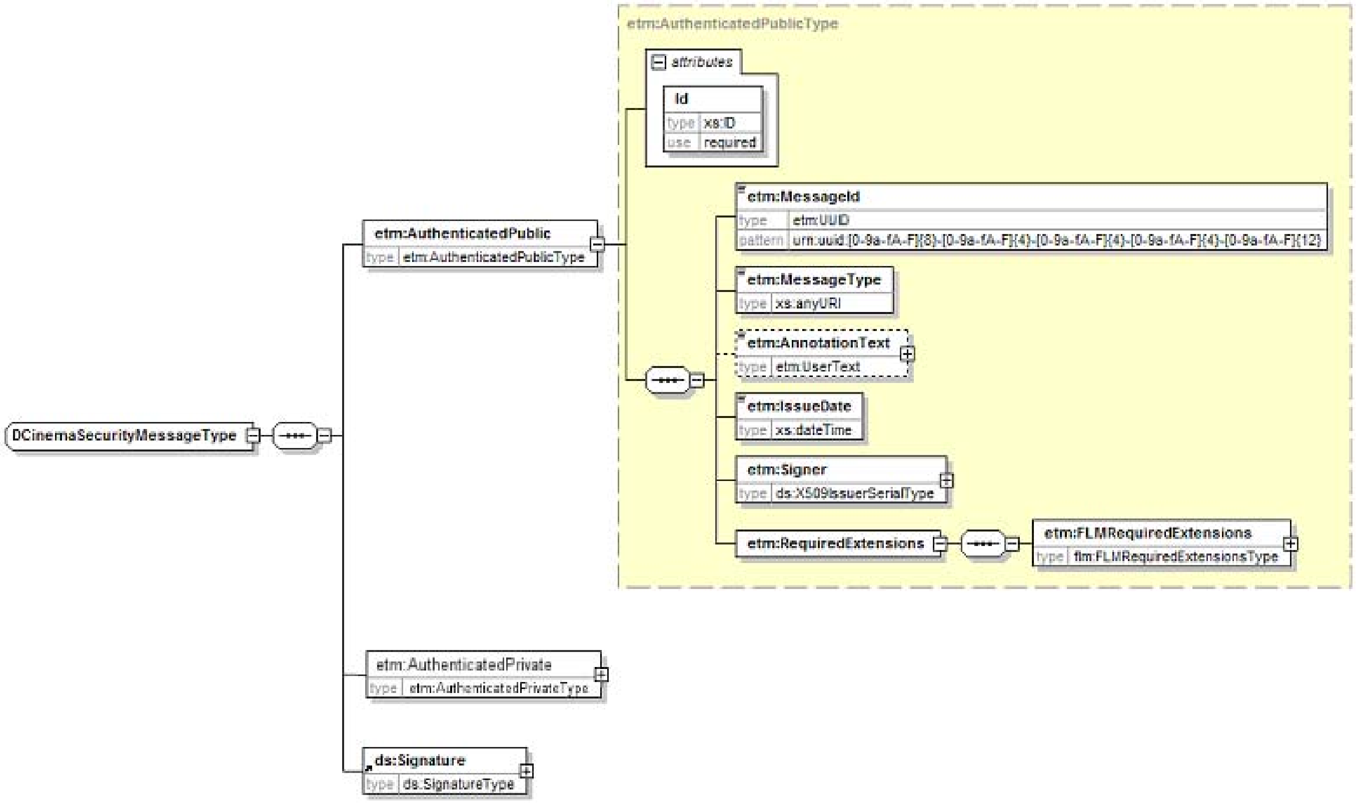

etm:AuthenticatedPublicType
attributes
Id
type xs:ID
use required
etm:MessageId
type etm:UUID
pattern urn:uuid:[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}
etm:MessageType
type xs:anyURI
etm:AnnotationText
type etm:UserText
etm:IssueDate
type xs:dateTime
etm:Signer
type ds:X509IssuerSerialType
etm:RequiredExtensions
etm:FLMRequiredExtensions
type flm:FLMRequiredExtensionsType
etm:AuthenticatedPublic
type etm:AuthenticatedPublicType
DCinemaSecurityMessageType
etm:AuthenticatedPrivate
type etm:AuthenticatedPrivateType
ds:Signature
type ds:SignatureType

Figure 3 – D-Cinema Security Message

The FLM does not utilize the `AuthenticatedPrivate` portion of the ETM. However, the `AuthenticatedPrivate` ID attribute must be included.

The `Signature` element defined in SMPTE 430-3 (ETM) carries the signer's certificate chain and protects the integrity and authenticity of the `AuthenticatedPublic` portion.

Note: The `Signature` section ensures the authenticity of the message to the extent that the recipient has prior knowledge of the certificate of the sender.

6 Authenticated and Unencrypted Information

The FLM extends the ETM by including the FLMRequiredExtensionType (see Figure 4 below) in its RequiredExtensions element.

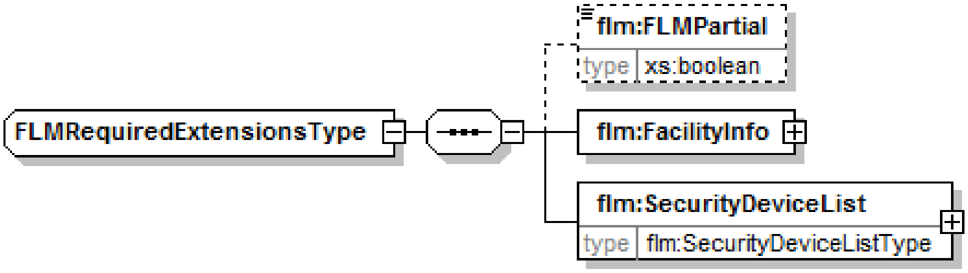


Figure 4 – FLM Required Extensions Type

The normative schema is defined in Annex C. The information in the AuthenticatedPublic element of the ETM (and thus, FLM) is digitally signed, and trust in the signature can be verified using the certificate chain in the Signature portion. This element is not encrypted, so any entity that has access to the message can extract this information. The word “public” that appears in the XML label for this element means that any entity that receives the message can view this portion.

The certificate chain is part of the information that is protected by the digital signature, which reduces the risk of an attacker who is able to create a small number of legitimate certificates (e.g., through social engineering). The following sections describe the elements in this portion.

6.1 MessageType

The MessageType field is defined in SMPTE 430-3. In a FLM, this field shall contain the following URI:

```
http://www.smpte-ra.org/schemas/430-7/2008/FLM
```

6.2 RequiredExtensions

The RequiredExtensions element of the FLM shall contain exactly one FLMRequiredExtensions element, as defined in Annex C and illustrated in Figure 4. The FLMRequiredExtensions element shall have the following child elements:

6.2.1 FLMPartial (Optional)

The FLMPartial element contains a Boolean value indicating whether the FLM is a “Partial FLM”. A Partial FLM shall be indicated when the FLM contains security certificate information pertaining to fewer auditoriums than contained in the facility complex. When an FLM is designated a Partial FLM, the ETM Annotation Text field shall be required, and the sender of the FLM shall state its purpose in detail in the ETM AnnotationText.

Note: Normal practice will be to communicate all active security device certificate information for any given facility in a single FLM. The FLMPartial option provides a means and explanation for sending a partial list whenever desired.

6.2.2 FacilityInfo

The FacilityInfo element communicates the Facility Identifier to the KDM Distributor, as well as informational data such as Contact Information.

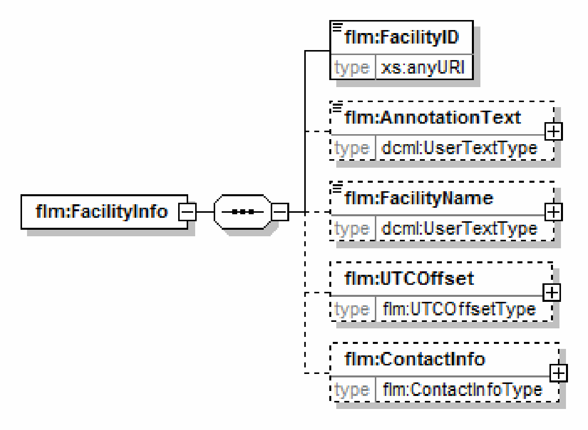


Figure 5 – Facility Info

6.2.2.1 FacilityID

The `FacilityID` element of the FLM shall be a URI identifier for the exhibition complex represented by the FLM.

Note: The `FacilityID` and `MessageID` elements are not related to the `DeviceListIdentifier` found in KDM.

6.2.2.2 AnnotationText (Optional)

The `AnnotationText` element of `FacilityInfo` shall be a text field containing descriptive text about the theater or theater circuit. A language attribute is optional. If the optional language attribute of UserTextType (as defined in [SMPTE 433]) is not present, the default value "en" shall be used.

6.2.2.3 FacilityName (Optional)

The `FacilityName` element of `FacilityInfo` shall be a text field containing the theater name. A language attribute is optional. If the optional language attribute of UserTextType (as defined in [SMPTE 433]) is not present, the default value "en" shall be used.

6.2.2.4 UTCOffset (Optional)

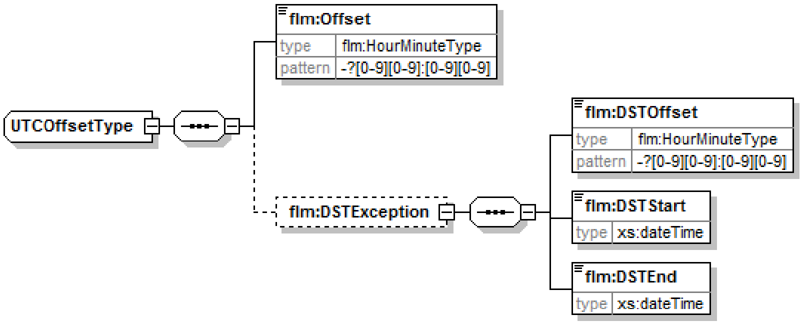


Figure 6 – UTC Offset Type

The `UTCOffset` element structure contains the local time offset from Universal Coordinated Time (UTC) and optionally information concerning the occurrence of daylight savings time.

6.2.2.4.1 Offset

The `Offset` element of UTCOffset shall be time duration of form HH:MM representing the local time offset from UTC.

6.2.2.4.2 DSTException (Optional)

6.2.2.4.2.1 DSTOffset

`DSTOffset` shall be a time duration of form HH:MM representing the local time offset from UTC when daylight savings time occurs.

6.2.2.4.2.1.1 DSTStart

`DSTStart` shall be a date-time stamp representing the start time for the next transition to daylight savings time for the local time zone. The Seconds and TZ Offset fields must be zero.

6.2.2.4.2.1.2 DSTEnd

`DSTEnd` shall be a date-time stamp representing the start time for the next transition to standard time for the local time zone. The Seconds and TZ Offset fields must be zero.

6.2.2.5 ContactInfo (Optional)

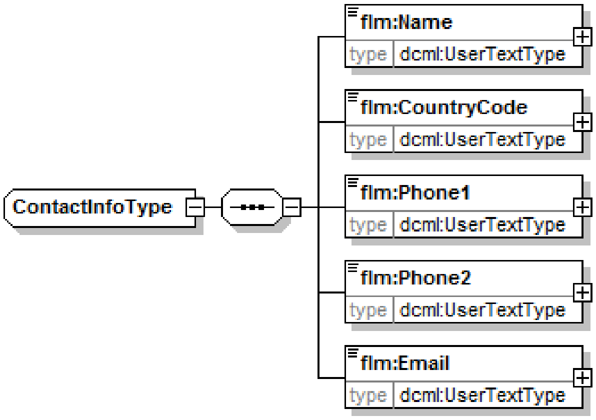


Figure 7 – Contact Information Type

6.2.2.5.1 Name

The Name element of `ContactInfo` shall be a text field containing the name of the contact person. A language attribute is optional. If the optional language attribute of UserTextType (as defined in [SMPTE 433]) is not present, the default value "en" shall be used.

6.2.2.5.2 CountryDialingCode

The `CountryDialingCode` element of `ContactInfo` shall contain the numeric International Direct Dialing code [CountryDialingCode] for the country where the contact person is located.

6.2.2.5.3 Phone1 and Phone 2

The `Phone1` and `Phone2` elements of `ContactInfo` shall contain the phone number (sans International Direct Dialing code) of the contact person. Numbers that are only to be used with local dialing and not to be used with international dialing shall be placed in parenthesis.

6.2.2.5.4 Email

The `Email` element of `ContactInfo` contains the email address of the contact person, as defined in RFC 822.

6.2.3 SecurityDeviceList

`SecurityDeviceList` shall be encoded as either one or more `CertOnlyType` elements, or one or more `CombinedType` elements, but not mixed. A list of `CombinedType` contains that information present in `CertOnlyType` along with information specific to the device. An instance of a `CombinedType` element shall be named `SecurityDevice`. An instance of `CertOnlyType` element shall be named `SecurityDeviceCertificate`.

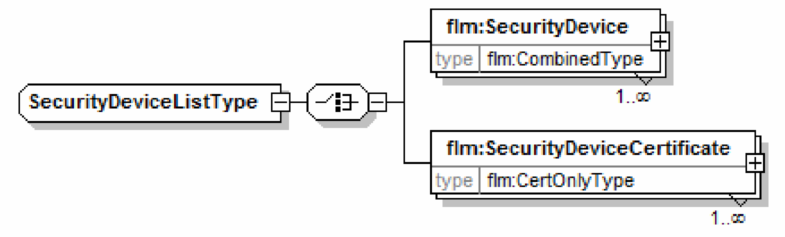


Figure 8 – Security Device List Type

6.2.3.1 SecurityDeviceCertificate

The `SecurityDeviceCertificate` list shall be encoded as one or more `CertOnlyType` elements as defined by this document.

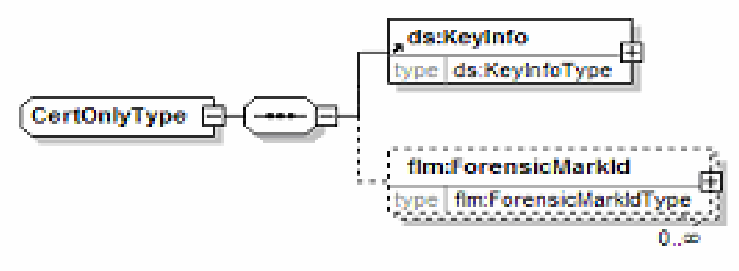


Figure 9 – Certificate Only Type

6.2.3.1.1 KeyInfo

The `KeyInfo` element shall contain at least one X509Data element, as defined in W3C XML-Signature Syntax and Processing, W3C Recommendation 12 Feb 2002, The KeyInfo Element." Both subject and intermediate certificates shall be present.

6.2.3.1.2 ForensicMarkId (Optional)

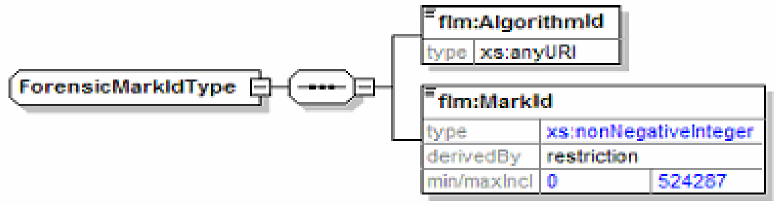


Figure 10 – Forensic Mark Id Type

The ForensicMarkId element, if present, describes the Forensic Marking Technologies implemented by the device. There shall be one instance of this element for each Forensic Marking Technology implemented in the device.

6.2.3.1.2.1 AlgorithmId

The AlgorithmId element shall be a URI. The AlgorithmId shall uniquely identify the forensic marking algorithm used to mark essence.

6.2.3.1.2.2 MarkId

The MarkId shall be a base-10 integer value in the range 0 – 524287 (this corresponds to a 19-bit unsigned integer). The MarkId is a unique number inserted by the forensic marking algorithm in the essence at playback.

6.2.3.2 Security Device

The SecurityDevice element shall be encoded as one or more CombinedType elements. A CombinedType element is a combination of a CertOnlyType element and a DeviceDescription element.

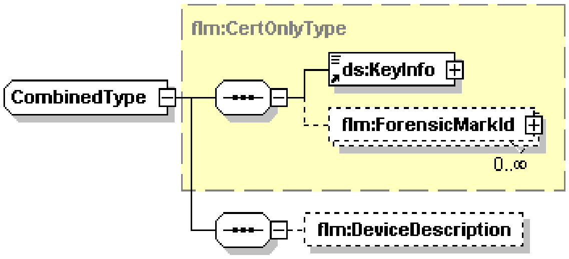


Figure 11 – Combined Type

6.2.3.2.1 DeviceDescription (Optional)

Optionally, SecurityDevice shall contain exactly one DeviceDescription element, as defined in SMPTE 433 XML Data Types for Digital Cinema. DeviceDescription shall be that of the device whose certificates are indicated in the KeyInfo element.

6.3 NonCriticalExtensions

This field is defined in SMPTE 430-3 (ETM).

Note: This element may contain proprietary extensions. Conforming implementations should ignore the contents of this element.

7 Authenticated and Private (Encrypted) Information

The AuthenicatedPrivate element of the ETM shall be empty, with only the Id attribute present.

8 Signature Information

This portion of the KDM message is defined in SMPTE 430-3 (ETM).

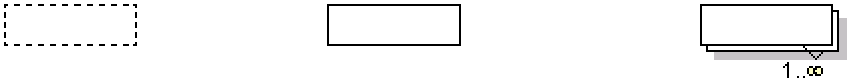
The ETM requires that the Signature contain two reference fields, one each for the AuthenticatedPublic and AuthenticatedPrivate elements. Signature elements shall be supplied for each of these nodes.

9 XML Diagram Legend (Informative)

The following provides a legend for notation used in diagrams depicting XML structures.

9.1 Element Symbols

In the schema design diagrams presented above in this document, only the elements are drawn. Attributes are not visible. The cardinality of the element (0..1, 1 exactly, 0..n, 1..n) is indicated by the border of the elements. Optional elements are drawn with a dashed line; required elements with a solid line. A maximum occurrence greater one is indicated by a double border.

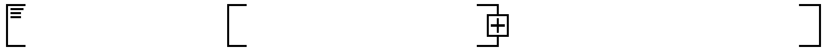


Optional element
Min. occurrence = 0,
Max. occurrence = 1

Required single element
Min. occurrence = 1,
Max. occurrence = 1

Required repeated element
Min. occurrence = 1,
Max. occurrence = unbounded

The content model of elements is symbolized on the left and right side of the element boxes. The left side indicates whether the element contains a simple type (text, numbers, dates, etc.) or a complex type (further elements). The right side of the element symbol indicates whether it contains child elements or not:



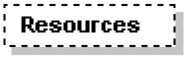
simple content

complex content

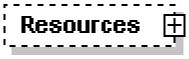
complex content
with child elements

no element content
(simple type, attributes
only, or empty element)

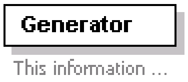
9.1.1 Examples



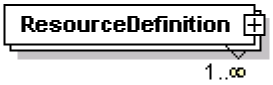
Optional single element without child elements. Minimum Occurrence = 0, Maximum Occurrence = 1, content = complex.



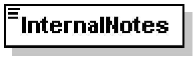
As above, but with child elements. The "plus" at the right side indicates the presence of one or more undisplayed child elements.



Mandatory single element. Minimum Occurrence = 1, Maximum Occurrence = 1, content = complex, no child elements (i.e., this denotes an *empty element*). The gray or green text below the element displays the xml-schema annotation associated with the element.



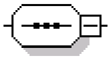
Mandatory multiple element containing child elements (content = complex). This element must occur at least once (Minimum Occurrence = 1) and may occur as often as desired (Maximum Occurrence = unbounded).



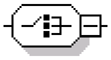
Mandatory single element with containing simple content (e.g., text) or mixed complex content (e.g., text with xhtml markup). Minimum Occurrence = 1, Maximum Occurrence = 1, type = xsd:string (for example), content = simple. The three lines in the upper left corner are used for both text and numeric content.

9.2 Model Symbols ("Compositors")

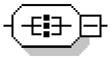
A sequence of elements. The elements must appear exactly in the sequence in which they appear in the schema diagram.



A choice of elements. Only a single element from those in the choice may appear at this position.

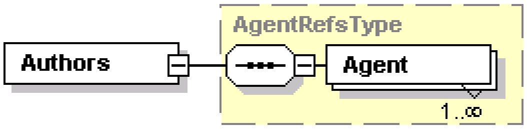


The "all" model, in which the sequence of elements is not fixed.

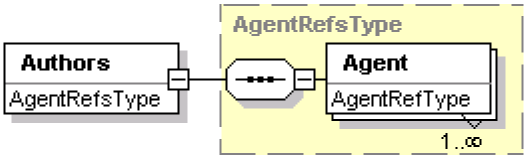


9.3 Types

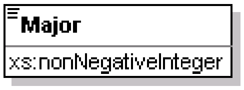
If an element refers to a complex global type, the type is shown with a border and yellow background. You can click on the gray type name shown at the top to jump to the type definition itself.



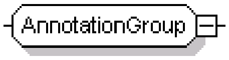
Depending on the settings in xml spy when generating the schema diagrams, the type name may be shown in the line below the element name:



In that case, the type names of simple types are shown as well:

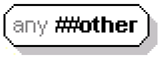


9.4 Model Groups and References

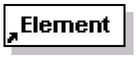


An *element group* is a named container with one or several elements. The group of elements can be reused at multiple places in the schema. Model groups are invisible in the instance document (in contrast to types, which require). Model groups have been used sparingly since they do not map to a feature in object-oriented programming languages (unless they support multiple inheritance).

Important note on reading the diagrams for model groups: If the model group symbol is drawn with simple lines (i.e., not dashed), this does not imply that the elements in the model group are required. The optionality of the group depends on the optionality of elements contained in the model group. (Model groups can be made optional, e.g., to make a model group with required elements optional in some cases, but this has not been used.)



The *"any"* group is a special kind of model group. It is a placeholder for elements not defined in the schema. The "any" element defines points where the schema can be extended. After the "Any" keyword, the namespace from which the elements may come is defined; for example, "##other" specifies that the extension elements may come from any namespace, except from the current schema namespace.



Element references are indicated through a link arrow in the lower left corner. They are similar to references to model groups within a schema, but instead of refining the model group, they directly refer to a single global element. The global element can then be reused in multiple places.

Annex A (Informative) **Design Features and Security Goals**

This section summarizes the main design features and security goals of the FLM. Additional considerations appear in SMPTE 430-3 (ETM).

- The FLM is designed such that its creation can be automated within the theater system.

- Optional descriptive information pertaining to the device, DeviceDescription, is associated with each device grouping of X.509 certificates.

- The facility complex represented by the FLM is identified by the FacilityID.

- The FLM is dated by the IssueDate field described in SMPTE 430-3 (ETM).

- The FLM is digitally signed, to allow a user to validate authenticity.

- The FLM does not pre-sort devices and certificates. Those tasked with creating KDMs can sort and identify public keys of D-Cinema Certificates having the Digital Cinema Role (CommonName) of type Media Block (xMB).

Annex B (Informative) Bibliography

This section contains informative references that provide helpful background information.

[ASN.1] For a collection of useful links to ASN.1 resources.
See: http://www.cs.columbia.edu/~hgs/internet/asn.1.html

[Base64] MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. See: http://www.ietf.org/rfc/rfc1521.txt

[Ferguson] “Practical Cryptography” 2003 By Neils Ferguson and Bruce Schneier. Wiley Publishing, Indianapolis, Indiana.

[Gutmann] “X.509 Style Guide” By Peter Gutmann.
See: http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt

[RFC2459] “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” by R. Housley, W. Ford, W. Polk, D. Solo, January 1999. See: http://www.ietf.org/rfc/rfc2459.txt

[RFC2693] “SPKI Certificate Theory” by C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, September 1999. See: http://www.ietf.org/rfc/rfc2693.txt

[Schneier] Applied Cryptography by Bruce Schneier. Second Edition. 1996. John Wiley & Sons. ISBN 0-471-11709-9.

SMPTE 430-1-2006, D-Cinema Operations — Key Delivery Message

SMPTE 430-2-2006, D-Cinema Operations — Digital Certificate

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology — Open Systems Interconnection — The Directory: Authentication Framework, June 1997.

Annex C (Normative)
XML Schema for FLM

The XML Schema document presented in this appendix normatively defines the structure of a Facility List Message using a machine-readable language. While this schema is intended to faithfully represent the structure presented in the normative prose portions (Sections 5 and 6) of this document, conflicts in definition may occur. In the event of such a conflict, the normative prose shall be the authoritative expression of the standard.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
                            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                            xmlns:flm="http://www.smpte-ra.org/schemas/430-7/2008/FLM"
                            xmlns:etm="http://www.smpte-ra.org/schemas/430-3/2006/ETM"
                            xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes"
                            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                            targetNamespace="http://www.smpte-ra.org/schemas/430-7/2008/FLM"
                            elementFormDefault="qualified" attributeFormDefault="unqualified"
                            id="FacilityListMessage">
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
                            schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
                            20020212/xmldsig-core-schema.xsd"/>
  <xs:import namespace="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes"
                            schemaLocation="./dcmlTypes.xsd"/>
  <xs:complexType name="FLMRequiredExtensionsType">
    <xs:sequence>
      <xs:element name="FLMPartial" type="xs:boolean" minOccurs="0"/>
      <xs:element name="FacilityInfo">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="FacilityID" type="xs:anyURI"/>
            <xs:element name="AnnotationText" type="dcml:UserTextType" minOccurs="0"/>
            <xs:element name="FacilityName" type="dcml:UserTextType" minOccurs="0"/>
            <xs:element name="UTCOffset" type="flm:UTCOffsetType" minOccurs="0"/>
            <xs:element name="ContactInfo" type="flm:ContactInfoType" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="SecurityDeviceList" type="flm:SecurityDeviceListType"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="SecurityDeviceListType">
    <xs:choice>
      <xs:element name="SecurityDevice" type="flm:CombinedType" maxOccurs="unbounded"/>
      <xs:element name="SecurityDeviceCertificate" type="flm:CertOnlyType"
                            maxOccurs="unbounded"/>
    </xs:choice>
  </xs:complexType>

  <xs:complexType name="CertOnlyType">
    <xs:sequence>
      <xs:element ref="ds:KeyInfo"/>
      <xs:element name="ForensicMarkId" type="flm:ForensicMarkIdType" minOccurs="0"
                            maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="CombinedType">
    <xs:complexContent>
      <xs:extension base="flm:CertOnlyType">
        <xs:sequence>
          <xs:element name="DeviceDescription" type="dcml:deviceDescriptionType"
                            minOccurs="0"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="ForensicMarkIdType">
    <xs:sequence>
      <xs:element name="AlgorithmId" type="xs:anyURI"/>
      <xs:element name="MarkId">
        <xs:simpleType>
          <xs:restriction base="xs:nonNegativeInteger">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="524287"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ContactInfoType">
    <xs:sequence>
      <xs:element name="Name" type="dcml:UserTextType"/>
      <xs:element name="CountryCode" type="dcml:UserTextType"/>
      <xs:element name="Phone1" type="dcml:UserTextType"/>
      <xs:element name="Phone2" type="dcml:UserTextType"/>
      <xs:element name="Email" type="dcml:UserTextType"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="UTCOffsetType">
    <xs:sequence>
      <xs:element name="Offset" type="flm:HourMinuteType"/>
      <xs:element name="DSTException" minOccurs="0">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="DSTOffset" type="flm:HourMinuteType"/>
            <xs:element name="DSTStart" type="xs:dateTime"/>
            <xs:element name="DSTEnd" type="xs:dateTime"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="HourMinuteType">
    <xs:restriction base="xs:string">
      <xs:pattern value="-?[0-9][0-9]:[0-9][0-9]"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

Annex D (Informative)
XML Example FLM

```
<?xml version="1.0" encoding="UTF-8"?>
<etm:DCinemaSecurityMessage xsi:schemaLocation="http://www.smpte-ra.org/schemas/430-3/2006/ETM
                            etm4flm.xsd"
                            xmlns:dcml="http://www.smpte-ra.org/schemas/433/2008/dcmlTypes"
                            xmlns:etm="http://www.smpte-ra.org/schemas/430-3/2006/ETM"
                            xmlns:flm="http://www.smpte-ra.org/schemas/430-7/2008/FLM"
                            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <etm:AuthenticatedPublic Id="ID_1">
    <etm:MessageId>urn:uuid:00000000-0000-0000-0000-000000000000</etm:MessageId>
    <etm:MessageType>http://ExampleFLM</etm:MessageType>
    <etm:AnnotationText language="en">Example FLM</etm:AnnotationText>
    <etm:IssueDate>2001-12-17T09:30:47.0Z</etm:IssueDate>
    <etm:Signer>
      <ds:X509IssuerName>String</ds:X509IssuerName>
      <ds:X509SerialNumber>0</ds:X509SerialNumber>
    </etm:Signer>
    <etm:RequiredExtensions>
      <etm:FLMRequiredExtensions>
        <flm:FLMPartial>false</flm:FLMPartial>
        <flm:FacilityInfo>
          <flm:FacilityID>http://www.facility.com</flm:FacilityID>
          <flm:AnnotationText language="en">String</flm:AnnotationText>
          <flm:FacilityName language="en">String</flm:FacilityName>
          <flm:UTCOffset>
            <flm:Offset>00:00</flm:Offset>
            <flm:DSTException>
              <flm:DSTOffset>00:00</flm:DSTOffset>
              <flm:DSTStart>2001-12-17T09:30:47.0Z</flm:DSTStart>
              <flm:DSTEnd>2001-12-17T09:30:47.0Z</flm:DSTEnd>
            </flm:DSTException>
          </flm:UTCOffset>
          <flm:ContactInfo>
            <flm:Name language="en">String</flm:Name>
            <flm:CountryCode language="en">String</flm:CountryCode>
            <flm:Phone1 language="en">String</flm:Phone1>
            <flm:Phone2 language="en">String</flm:Phone2>
            <flm:Email language="en">String</flm:Email>
          </flm:ContactInfo>
        </flm:FacilityInfo>
        <flm:SecurityDeviceList>
          <flm:SecurityDevice>
            <ds:KeyInfo Id="ID_2">
              <ds:KeyName>String</ds:KeyName>
              <ds:KeyName>String</ds:KeyName>
              <ds:KeyName>String</ds:KeyName>
            </ds:KeyInfo>
            <flm:ForensicMarkId>
              <flm:AlgorithmId>http://www.facility.com</flm:AlgorithmId>
              <flm:MarkId>0</flm:MarkId>
            </flm:ForensicMarkId>
            <flm:ForensicMarkId>
              <flm:AlgorithmId>http://www.facility.com</flm:AlgorithmId>
              <flm:MarkId>0</flm:MarkId>
            </flm:ForensicMarkId>
            <flm:ForensicMarkId>
              <flm:AlgorithmId>http://www.facility.com</flm:AlgorithmId>
              <flm:MarkId>0</flm:MarkId>
            </flm:ForensicMarkId>
            <flm:DeviceDescription>
              <dcml:DeviceIdentifier idtype="DeviceUID">urn:uuid:00000000-0000-0000-0000-
                          000000000000</dcml:DeviceIdentifier>
              <dcml:DeviceTypeID scope="http://www.smpte-
                          ra.org/schemas/433/2008/DCMLTypes/#DeviceTypeTokens">token</dcml:Device
                          TypeID>
        <dcml:DeviceSubsystemTypeID scope="http://www.smpte-
                  ra.org/schemas/433/2008/DCMLTypes/#DeviceTypeTokens">token</dcml:Device
                  SubsystemTypeID>
        <dcml:DeviceSerial>String</dcml:DeviceSerial>
        <dcml:ManufacturerID>urn:uuid:00000000-0000-0000-0000-
                  000000000000</dcml:ManufacturerID>

                          <dcml:ManufacturerCertID>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0
                  dU1GUXhEUzhi</dcml:ManufacturerCertID>

                          <dcml:DeviceCertID>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUX
                  hEUzhi</dcml:DeviceCertID>
        <dcml:ManufacturerName>String</dcml:ManufacturerName>
        <dcml:DeviceName>String</dcml:DeviceName>
        <dcml:ModelNumber>String</dcml:ModelNumber>
        <dcml:VersionInfo>
          <dcml:Name>String</dcml:Name>
          <dcml:Value>String</dcml:Value>
        </dcml:VersionInfo>
        <dcml:DeviceComment language="en">String</dcml:DeviceComment>
      </flm:DeviceDescription>
    </flm:SecurityDevice>
    <flm:SecurityDevice>
      <ds:KeyInfo Id="ID_3">
        <ds:KeyName>String</ds:KeyName>
        <ds:KeyName>String</ds:KeyName>
        <ds:KeyName>String</ds:KeyName>
      </ds:KeyInfo>
      <flm:ForensicMarkId>
        <flm:AlgorithmId>http://www.altova.com</flm:AlgorithmId>
        <flm:MarkId>0</flm:MarkId>
      </flm:ForensicMarkId>
      <flm:ForensicMarkId>
        <flm:AlgorithmId>http://www.altova.com</flm:AlgorithmId>
        <flm:MarkId>0</flm:MarkId>
      </flm:ForensicMarkId>
      <flm:ForensicMarkId>
        <flm:AlgorithmId>http://www.altova.com</flm:AlgorithmId>
        <flm:MarkId>0</flm:MarkId>
      </flm:ForensicMarkId>
      <flm:DeviceDescription>
        <dcml:DeviceIdentifier idtype="DeviceUID">urn:uuid:00000000-0000-0000-0000-
                  000000000000</dcml:DeviceIdentifier>
        <dcml:DeviceTypeID scope="http://www.smpte-
                  ra.org/schemas/433/2008/DCMLTypes/#DeviceTypeTokens">token</dcml:Dev
                  iceTypeID>
        <dcml:DeviceSubsystemTypeID scope="http://www.smpte-
                  ra.org/schemas/433/2008/DCMLTypes/#DeviceTypeTokens">token</dcml:Dev
                  iceSubsystemTypeID>
        <dcml:DeviceSerial>String</dcml:DeviceSerial>
        <dcml:ManufacturerID>urn:uuid:00000000-0000-0000-0000-
                  000000000000</dcml:ManufacturerID>

                          <dcml:ManufacturerCertID>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0
                  dU1GUXhEUzhi</dcml:ManufacturerCertID>

                          <dcml:DeviceCertID>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUX
                  hEUzhi</dcml:DeviceCertID>
        <dcml:ManufacturerName>String</dcml:ManufacturerName>
        <dcml:DeviceName>String</dcml:DeviceName>
        <dcml:ModelNumber>String</dcml:ModelNumber>
        <dcml:VersionInfo>
          <dcml:Name>String</dcml:Name>
          <dcml:Value>String</dcml:Value>
        </dcml:VersionInfo>
        <dcml:DeviceComment language="en">String</dcml:DeviceComment>
      </flm:DeviceDescription>
    </flm:SecurityDevice>
    <flm:SecurityDevice>
      <ds:KeyInfo Id="ID_4">
        <ds:KeyName>String</ds:KeyName>
```

```
              <ds:KeyName>String</ds:KeyName>
              <ds:KeyName>String</ds:KeyName>
            </ds:KeyInfo>
            <flm:ForensicMarkId>
              <flm:AlgorithmId>http://www.altova.com</flm:AlgorithmId>
              <flm:MarkId>0</flm:MarkId>
            </flm:ForensicMarkId>
            <flm:ForensicMarkId>
              <flm:AlgorithmId>http://www.altova.com</flm:AlgorithmId>
              <flm:MarkId>0</flm:MarkId>
            </flm:ForensicMarkId>
            <flm:ForensicMarkId>
              <flm:AlgorithmId>http://www.altova.com</flm:AlgorithmId>
              <flm:MarkId>0</flm:MarkId>
            </flm:ForensicMarkId>
            <flm:DeviceDescription>
              <dcml:DeviceIdentifier idtype="DeviceUID">urn:uuid:00000000-0000-0000-0000-
                      000000000000</dcml:DeviceIdentifier>
              <dcml:DeviceTypeID scope="http://www.smpte-
                      ra.org/schemas/433/2008/DCMLTypes/#DeviceTypeTokens">token</dcml:Dev
                      iceTypeID>
              <dcml:DeviceSubsystemTypeID scope="http://www.smpte-
                      ra.org/schemas/433/2008/DCMLTypes/#DeviceTypeTokens">token</dcml:Dev
                      iceSubsystemTypeID>
              <dcml:DeviceSerial>String</dcml:DeviceSerial>
              <dcml:ManufacturerID>urn:uuid:00000000-0000-0000-0000-
                      000000000000</dcml:ManufacturerID>

                            <dcml:ManufacturerCertID>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0
                      dU1GUXhEUzhi</dcml:ManufacturerCertID>

                            <dcml:DeviceCertID>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUX
                      hEUzhi</dcml:DeviceCertID>
              <dcml:ManufacturerName>String</dcml:ManufacturerName>
              <dcml:DeviceName>String</dcml:DeviceName>
              <dcml:ModelNumber>String</dcml:ModelNumber>
              <dcml:VersionInfo>
                <dcml:Name>String</dcml:Name>
                <dcml:Value>String</dcml:Value>
              </dcml:VersionInfo>
              <dcml:DeviceComment language="en">String</dcml:DeviceComment>
            </flm:DeviceDescription>
          </flm:SecurityDevice>
        </flm:SecurityDeviceList>
      </etm:FLMRequiredExtensions>
    </etm:RequiredExtensions>
  </etm:AuthenticatedPublic>
</etm:DCinemaSecurityMessage>
```