Keyset Delivery Format Specification

Version 2.0.1 22 December 2014

Keyset Delivery Format Specification Version 2.0.1

Notice:

As of the date of publication, this document is a release candidate specification subject to DECE Member review and final adoption by vote of the Management Committee of DECE in accordance with the DECE LLC Operating Agreement. Unless there is notice to the contrary, this specification will become an adopted “Ecosystem Specification” on 5 February 2015.

Optional Implementation Agreement:

In addition to the UltraViolet License Agreements which cover implementation of the DECE Ecosystem Specifications within the UltraViolet Ecosystem, DECE offers an optional license agreement relating to the implementation of this document outside the Ecosystem (“RAND Agreement”). Entities executing the optional RAND Agreement receive the benefit of the commitments made by DECE’s members to license on reasonable and nondiscriminatory terms their patent claims necessary to the implementation of this document in exchange for a comparable patent licensing commitment. Copies of the license agreements are available at the DECE web site referenced below.

Contact Information:

Licensing and contract inquiries and requests should be addressed to us at:

http://www.uvvu.com/uv-for-business

Keyset Delivery Format Specification Version 2.0.1

Contents

1 Introduction 4
1.1 Scope 4
1.2 Document Organization 4
1.3 Document Notation and Conventions 4
1.4 Normative References 5
1.4.1 DECE Normative References 5
1.4.2 External References 5
1.5 Informative References 5
1.6 Terms, Definitions and Acronyms 6
1.7 XML Change Management 6
2 Keyset Delivery and DECE Ecosystem (Informative) 7
3 Keyset Delivery Format 9
3.1 Keyset Delivery Format Data 9
3.2 Keyset Delivery Group 9
3.3 Keyset Delivery Type 10
3.4 Version Data 10
3.5 Delivery Data 11
3.6 Container Data 11
3.7 Production Phase Data 12
4 RFC 6030 KeyContainer Constraints 13
4.1.1 KeyContainer Constraints 13
4.1.2 KeyPackage Constraints 13
4.1.3 Key Constraints 14
4.1.4 XML Schema Constraints 14
5 XML Schemas 15
5.1 PSKC Constraint Schema 15
5.2 Keyset Delivery Format Schema 15
6 Examples (Informative) 16

1 Introduction

1.1 Scope

This document specifies a format for delivering Keysets.

Keyset is defined in [DSystem], Section 1.4 as the set of all Content Keys needed to decrypt playable elements of a DCC. Keysets are used by DSPs and LASPs to issue licenses and by LASPs to decrypt DCCs for purposes of streaming. Keysets are delivered by Content Providers to DSPs, LASPs and Retailers.

1.2 Document Organization

This document is organized as follows:

1. Introduction—Provides background, scope and conventions
2. Keyset Delivery and DECE Ecosystem – Illustrates where Keysets are delivered
3. DECE Keyset Delivery Format
4. RFC 6030 KeyContainer Constraints for DECE
5. XML Schemas
6. Examples

1.3 Document Notation and Conventions

The following terms are used to specify conformance elements of this specification. These are adopted from the ISO/IEC Directives, Part 2, Annex H [ISO-P2H]. For more information, please refer to those directives.

- SHALL and SHALL NOT indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.
- 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.
- MAY and NEED NOT indicate a course of action permissible within the limits of the document.

1.4 Normative References

1.4.1 DECE Normative References

The following DECE technical specifications are cited within the normative language of this document.

[DSystem]	System Specification
[DCoord]	Coordinator API Specification
[DMeta]	Content Metadata Specification
[DMedia]	Common File Format& Media Format Specification
[DCMeta]	DECE Common Metadata Specification

1.4.2 External References

The following external references are cited within the normative language of this document.

[RFC6030]	Hoyer, P., et al, Portable Symmetric Key Container (PSKC), October 2010, http://www.ietf.org/rfc/rfc6030.txt
[XENC]	XML Encryption Syntax and Processing, W3 Recommendation 10 December 2002. http://www.w3.org/TR/xmlenc-core/
[ISO-P2H]	ISO/IEC Directives, Part 2, Annex H http://www.iec.ch/tiss/iec/Directives-part2-Ed5.pdf
[RFC4122]	Leach, P., et al, A Universally Unique IDentifier (UUID) URN Namespace, July 2005 http://www.ietf.org/rfc/rfc4122.txt

Note: Readers are encouraged to investigate the most recent publications for their applicability.

1.5 Informative References

The following external references are cited within the informative language of this document.

[DPublisher]	DECE Content Publishing Specification, Version 1.0.3

[CENC]	ISO/IEC 23001-7:2012, First edition 2012-02-01, "Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files"

1.6 Terms, Definitions and Acronyms

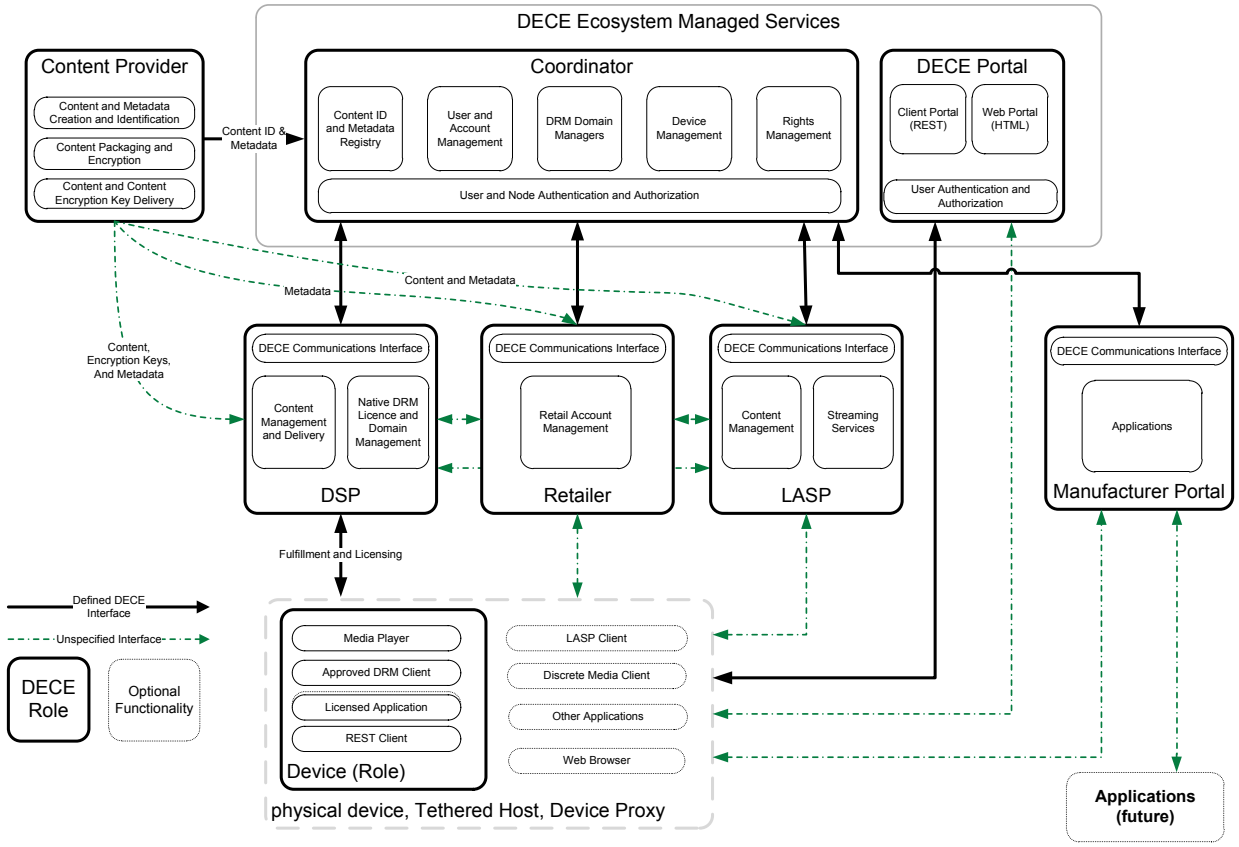
Media Key	An encryption key used to encrypt media samples or portions of media samples. This should not be confused with the MediaKey algorithm profile. Media Key corresponds with 'Content Key' in [DSystem] and 'encryption key' in [DMedia].
Keyset Delivery Format	A data structure used for transmittal of Keysets.
KID, Key ID	A descriptor in the ISO File Format 'cenc' encryption scheme that identifies the Media Key used to encrypt a track or portions of a track. KID is a value selected to have a one to one correspondence to a Media Key value within a DCC. Key ID corresponds with 'key identifier' and 'KID' in [DMedia].

1.7 XML Change Management

Recipients of XML Documents encoded using this specification SHALL comply with XML Change Management defined in [DSystem], Section 1.6.

2 Keyset Delivery and DECE Ecosystem (Informative)

Content Keys are delivered from Content Providers to DSPs as shown in the following diagram. Also, although not specifically shown, Content Providers can also deliver Digital CFF Containers (DCCs) to LASPs. Content Keys may be delivered through Retailers.



This workflow differs from traditional distribution models because of Common Encryption. In a traditional model, the content provider distributes unencrypted files and encryption happens in a DRM-specific manner by a distribution entity. However, in DECE all Original DECE Common File Format Containers (ODCCs), produced by the Content Provider as described in DPublisher, are already encrypted in a DRM-neutral fashion. The keys are distributed with the ODCC.

In the diagram above, the Content Provider delivers “Content, Encryption Keys, and Metadata” to the DSP. This specification describes packaging for those Encryption Keys. Although not shown on the diagram, LASPs can also receive Encryption Keys, especially when the distribution is in Common File Format (CFF) as described in DMedia.

Keyset Delivery Format Specification Version 2.0.1

This Keyset Delivery Format is based on Portable Symmetric Key Container (PSKC) documented in [RFC6030]. PSKC allows the secure transfer of keys, in this case DECE's use of Common Encryption as described in [DMedia], Section 3. PSKC requires a Public Key Infrastructure (PKI). DSPs and LASPs provide their public keys to the Content Provider, in accordance with bilateral arrangements, and possibly using a Certificate Authority (CA) to establish a chain of trust. Using the public key of the DSP or LASP, the Content Provider encrypts DECE Keysets and completes the PSKC Container portions (`KeyContainer` elements) as specified in this document. The remaining portions are also included as required.

Keyset Delivery Format does not specify delivery method. That is at the discretion of the parties exchanging data. Possible delivery methods include email, file transfer and web services.

3 Keyset Delivery Format

A Keyset is the set of all Content Keys (Media Keys) needed to decrypt playable elements of a DCC This section defines a format for secure distribution of CFF Keysets, typically from Content Providers to DSPs and LASPs.

The DECE Keyset Delivery Format provides a standard format for the transmittal of Keysets.

The DECE Keyset Delivery Format does not specify a protocol for how the keys are actually exchanged between parties. For example, a DECE Keyset Delivery Format document could be delivered in a file via FTP, or via a web services interface.

Optional elements are not required, but recommended. It is also acceptable to include additional information as part of `Extensions` elements.

Types in the 'md:' namespace are defined in [DCMeta].

3.1 Keyset Delivery Format Data

Keyset Delivery Format is an XML document with a root type of KeysetDelivery defined as follows.

Element	Attribute	Definition	Type	Card.
KeysetDelivery Group		Keyset Delivery for one or more Keysets	keydelivery:KeysetDelivery-type	

3.2 Keyset Delivery Group

This is used to deliver one or more keysets. It contains common delivery data and multiple instances of the keyset delivery information.

Element	Attribute	Definition	Type	Card.
KeysetDeliveryGroup-type				
DeliveryData		Delivery information that covers all instances of KeysetDelivery	keydelivery:DataDelivery-type	0..1

KeysetDelivery		Information about one Keyset	keydelivery:KeysetDelivery-type	1..n

3.3 Keyset Delivery Type

Element	Attribute	Definition	Type	Card.
KeysetDelivery-type		Complex type definition for Keyset Delivery Format		
APID		APID for the Container for which the Keyset is being delivered	md:id-type	
PresentationID		PresentationID associated with APID.	md:id-type	0..1
KeyContainer		RFC6030 KeyContainer as constrained under KeysetConstraints	pskc:KeyContainer Type (as constrained)	
VersionData		Additional information about the version of the KeyContainer	keydelivery:VersionData-type	0..1
ContainerData		Additional data about the DCC	keydelivery:ContainerData-type	0..1
ProductionPhase		Information about relevant production phases. One entry per phase.	keydelivery:ProductionPhase-type	0..n

3.4 Version Data

Element	Attribute	Definition	Type	Card.
VersionData-type				
KeyContainerSerialNumber		Serial number of the Keyset Delivery information. This is used to refer to the entire KeysetDelivery element.	xs:string	0..1

ReplacesKeyContainer SerialNumber		Serial number of Keyset Delivery information that are replaced by this Keyset Delivery Container. To be used when previous information is to be replaced.	xs:string	0..1
KeyContainerCreation Date		The UTC date and time of creation. If exact time is not known, use 12:00 midnight (0:00).	xs:dateTime	0..1

3.5 Delivery Data

Element	Attribute	Definition	Type	Card.
DeliveryData-type				
Description		Description of delivery	xs:string	0..1
SendingOrganization		Organization sending keyset	md:OrgName-type	0..1
SenderPointofContact		Point of contact at sending organization	md:ContactInfo-type	0..1
ReceivingOrganization		Information about the organization(s) to which this Keyset is intended.	md:OrgName-type	0..n
Extensions		Any desired extensions	any ##other	0..n

3.6 Container Data

Element	Attribute	Definition	Type	Card.
ContainerData-type				
Description		Description of DCC. This might describe title and media profile	xs:string	0..1
MediaProfile		Media profiles as defined in [DCoord]	xs:anyURI	0..1

EIDRS		EIDR identifier in short format	xs:string, pattern "[\dA-F]{4}-[\dA-F]{4}-[\dA-F]{4}-[\dA-F]{4}-[\dA-F]{4}-[\dA-Z]"	0..1
DMediaVersion		Version of [DMedia] to which the DCC was built	xs:string	0..1
FileHash		Cryptographic hash of the entire DCC	xs:string	0..1
	algorithm	Hash algorithm used to create FileHash, if not included assumed to be SHA-1.	xs:string	0..1
Extensions		Any desired extensions	any ##other	0..n

3.7 Production Phase Data

Element	Attribute	Definition	Type	Card.
ProductionPhase-type				
Description		Description of this phase	xs:string	0..1
Sequence		Phase number (used to construct ordering)	xs:positiveInteger	0..1
Organization		Organization doing production	md:OrgName-type	0..1
Facility		Name of facility where production took place	xs:string	0..1
ToolName		Tool used in production	xs:string	0..1
ToolVersion		Version of tool used in production	xs:string	0..1
ProductionNotes		Any production notes as desired	xs:string	0..1
Contact		Point of Contact at production facility	md:ContactInfo-type	0..1
Extensions		Any desired extensions	any ##other	0..n

4 RFC 6030 KeyContainer Constraints

The DECE Keyset Delivery Format uses the 'algorithm profile' of the Portable Symmetric Key Container (PSKC) specification [RFC6030]. The DECE algorithm profile, which constrains PSKC, is called MediaKey. The identifier for the MediaKey algorithm profile is `urn:dece:pskc:contentkey`.

DECE Keyset Delivery Format documents SHALL be an XML document with a `KeyContainer` element as defined in [RFC6030].

The DECE Keyset Delivery Format documents SHALL comply with the constraints of the MediaKey algorithm profile as defined in following sections.

4.1.1 KeyContainer Constraints

The following are constraints for the `KeyContainer` element.

The `EncryptionKey` element SHALL be present in the `KeyContainer` element and it SHALL contain one `X509Data` element describing the certificate used to encrypt the content keys in the `KeyContainer` element.

If more than one KID is used per piece of content, then multiple `KeyPackage` entities SHALL be present in the `KeyContainer` element, each containing one `Key` element.

A Keyset Delivery Format document describing a PD or SD Profile DECE file SHALL contain one `KeyPackage` element.

A Keyset Delivery Format document describing an HD Profile DECE file SHALL contain one or two `KeyPackage` elements.

The `MACMethod` element SHALL be omitted.

4.1.2 KeyPackage Constraints

The following are constraints for the `KeyPackage` element.

The `DeviceInfo` element SHALL be omitted.

The `CryptModuleInfo` element SHALL be omitted.

4.1.3 Key Constraints

The following are constraints for the `Key` element.

The `Id` attribute of the `Key` element SHALL be present and SHALL be set to the value of the KID in the ODCC using this key; as defined in [DMedia] Section 3.2. It SHALL be encoded as a "UUID" as defined in [RFC4122], Section 3 without any dashes.

The Algorithm attribute of the `Key` element SHALL be set to `urn:dece:pskc:contentkey` to identify the DECE MediaKey profile.

Each Key element SHALL contain exactly one `Data` element with exactly one `Secret` element containing exactly one `EncryptedValue` element. The EncryptedValue element SHALL use the `http://www.w3.org/2001/04/xmlenc#rsa_1_5` encryption method as per [XENC], 5.4.1 RSA Version 1.5.

The KeyProfileId element SHALL be included and have a value as follows:

- 'video' for a key associated with video track
- 'audio' for a key associated with audio track
- 'subtitle' for a key associated with a subtitle track (note that [DMedia] does not currently support subtitle track encryption).
- 'videoplus' for a key that is associated with multiple track types, including at least one video track

The `Policy` element SHALL be omitted.

The `UserId` element SHALL be omitted.

The `MACMethod` element SHALL be omitted.

4.1.4 XML Schema Constraints

Section 11 of [RFC6030] defines the Schema of a PSKC document.

5 XML Schemas

5.1 PSKC Constraint Schema

The schema `pskc_dece_redefine.xsd` constrains RFC 6030 schema to DECE requirements as stated in this document.

As the constraint generates XML documents complete compliant with RFC 6030, the namespace does not change. RFC 6030 including XML redefines to constrain XML documents to DECE requirements as stated in this specification.

The DECE schemas are derived from the IETF PSKC schema (with a filename of pskc.xsd) which must be present in the same directory. The PSKC schema can be found in IETF RFC 6030, Section 11.

5.2 Keyset Delivery Format Schema

The XML Schema for use with this document is called `keydelivery.xsd`. This schema contains the base element KeysetDelivery as defined above. The namespace used is `http://www.decellc.org/schema/2012/12/keydelivery`.

6 Examples (Informative)

The following illustrates the use of the Key Delivery Format.

```
<?xml version="1.0" encoding="UTF-8"?>
<keydelivery:KeysetDeliveryGroup
xsi:schemaLocation="http://www.decellc.org/schema/2012/12/keydelivery keydelivery.xsd"
xmlns:keydelivery="http://www.decellc.org/schema/2012/12/keydelivery"
xmlns:md="http://www.movielabs.com/schema/md/v2.2/md"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <keydelivery:DeliveryData>
      <keydelivery:Description>Keys for My Favorite Movie, Part II</keydelivery:Description>
      <keydelivery:SendingOrganization>
         <md:DisplayName>The Motion Picture Studio</md:DisplayName>
         <md:SortName>Motion Picture Studio</md:SortName>
      </keydelivery:SendingOrganization>
      <keydelivery:SenderPointofContact>
         <md:Name>Friendly M Person</md:Name>
         <md:PrimaryEmail>friend@motionpicturestudio.biz</md:PrimaryEmail>
         <md:AlternateEmail>anotherfriend@motionpicturestudio.biz</md:AlternateEmail>
         <md:Address>1234 Main Street, Anytown CA, USA, 12345</md:Address>
         <md:Phone type="String">1-555-555-5555</md:Phone>
      </keydelivery:SenderPointofContact>
      <keydelivery:ReceivingOrganization>
         <md:DisplayName>My Favorite LASP</md:DisplayName>
         <md:SortName>Favorite LASP</md:SortName>
      </keydelivery:ReceivingOrganization>
   </keydelivery:DeliveryData>
   <keydelivery:KeysetDelivery>
      <keydelivery:APID>urn:dece:apid:eidr-s:abcd-abcd-abcd-abcd-abcd-e</keydelivery:APID>
      <keydelivery:KeyContainer Version="1.0">
         <pskc:EncryptionKey>
            <ds:X509Data>
               <ds:X509Certificate>abcd1234</ds:X509Certificate>
            </ds:X509Data>
         </pskc:EncryptionKey>
         <pskc:KeyPackage>
            <pskc:Key Id="f81d4fae7dec11d0a76500a0c91e6bf6" Algorithm="urn:dece:pskc:contentkey">
               <pskc:KeyProfileId>video</pskc:KeyProfileId>
               <pskc:Data>
                  <pskc:Secret>
                     <pskc:EncryptedValue>
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa_1_5"/>
                        <xenc:CipherData>

   <xenc:CipherValue>hJ+fvpoMPMO9BYpK2rdyQYGIxiATYHTHC7e/sPLKYo5/r1v+4xTYG3gJolCWuV
MydJ7Ta0GaiBPHcWa8ctCVYmHKfSz5fdeV5nqbZApe6dofTqhRwZK6Yx4ufevi91cjN2vBpSxYafvN3c3+x
Igk0EnTV4iVPRCR0rBwyfFrPc4=</xenc:CipherValue>
                        </xenc:CipherData>
```

```
                    </pskc:EncryptedValue>
                  </pskc:Secret>
                </pskc:Data>
              </pskc:Key>
            </pskc:KeyPackage>
        </keydelivery:KeyContainer>
        <keydelivery:VersionData>
            <keydelivery:KeyContainerSerialNumber>1002-30004-
0001</keydelivery:KeyContainerSerialNumber>
            <keydelivery:ReplacesKeyContainerSerialNumber>1002-30004-
0000</keydelivery:ReplacesKeyContainerSerialNumber>
            <keydelivery:KeyContainerCreationDate>2012-03-
29T23:30:47Z</keydelivery:KeyContainerCreationDate>
        </keydelivery:VersionData>
        <keydelivery:ContainerData>
            <keydelivery:Description>My Favorite Movie</keydelivery:Description>
            <keydelivery:MediaProfile>SD</keydelivery:MediaProfile>
            <keydelivery:EIDRS>ABCD-ABCD-ABCD-ABCD-ABCD-M</keydelivery:EIDRS>
            <keydelivery:DMediaVersion>1.0.3</keydelivery:DMediaVersion>
            <keydelivery:FileHash algorithm="SHA-
1">e0d123e5f316bef78bfdf5a008837577</keydelivery:FileHash>
        </keydelivery:ContainerData>
        <keydelivery:ProductionPhase>
            <keydelivery:Description>text</keydelivery:Description>
            <keydelivery:Sequence>2</keydelivery:Sequence>
            <keydelivery:Organization>
                <md:DisplayName>My Favorite Post</md:DisplayName>
                <md:SortName>Favorite Post</md:SortName>
            </keydelivery:Organization>
            <keydelivery:Facility>North Burbank</keydelivery:Facility>
            <keydelivery:ToolName>Super Tools</keydelivery:ToolName>
            <keydelivery:ToolVersion>7.3</keydelivery:ToolVersion>
            <keydelivery:ProductionNotes>We applied the frizzle filter.</keydelivery:ProductionNotes>
            <keydelivery:Contact>
                <md:Name>John Doe</md:Name>
                <md:PrimaryEmail>Jon@myfavoritepostproductionplace.com</md:PrimaryEmail>
                <md:Address>122 Main Street, Anytown CA, USA 12345</md:Address>
                <md:Phone type="String">555-556-5555</md:Phone>
            </keydelivery:Contact>
        </keydelivery:ProductionPhase>
    </keydelivery:KeysetDelivery>
</keydelivery:KeysetDeliveryGroup>
```

END