KDM : KEY DELIVERY MESSAGE

Short version : A KDM is a « digital key » for encrypted DCPs.

Metaphorical version : A KDM is like a tamper-proof, sealed envelope that contains one or several keys, along with a letter containing details about these keys, what they are used for, etc.

Technical version : A KDM is an XML file containing a multitude of data, such as metadata which links the KDM to a CPL, defines validity dates, and the AES decryption keys which allow the decryption of all the encrypted assets (MXF) defined in the CPLs of a DCP.

A KDM is created by a laboratory for a theater allowing it to read an encrypted digital movie.

In which case is a KDM used ?

A KDM is required **only** in the following cases :

- To decrypt an encrypted DCP (for a theatrical projection, for example)
- To share decryption keys between two post-production entities (such as laboratories)

Thus, a KDM is not required for non-encrypted DCPs

SMPTE STANDARDS

The various standards related to the KDM :

- SMPTE 430-3 (2012) - **Generic Extra-Theatre Message Format** (ETM)
- SMPTE 430-1 (2017) - **Key Delivery Message** (KDM)
- SMPTE 430-2 (2017) - **Digital Certificate**
- SMPTE 429-2 (2020) - **DCP Operational Constraints**

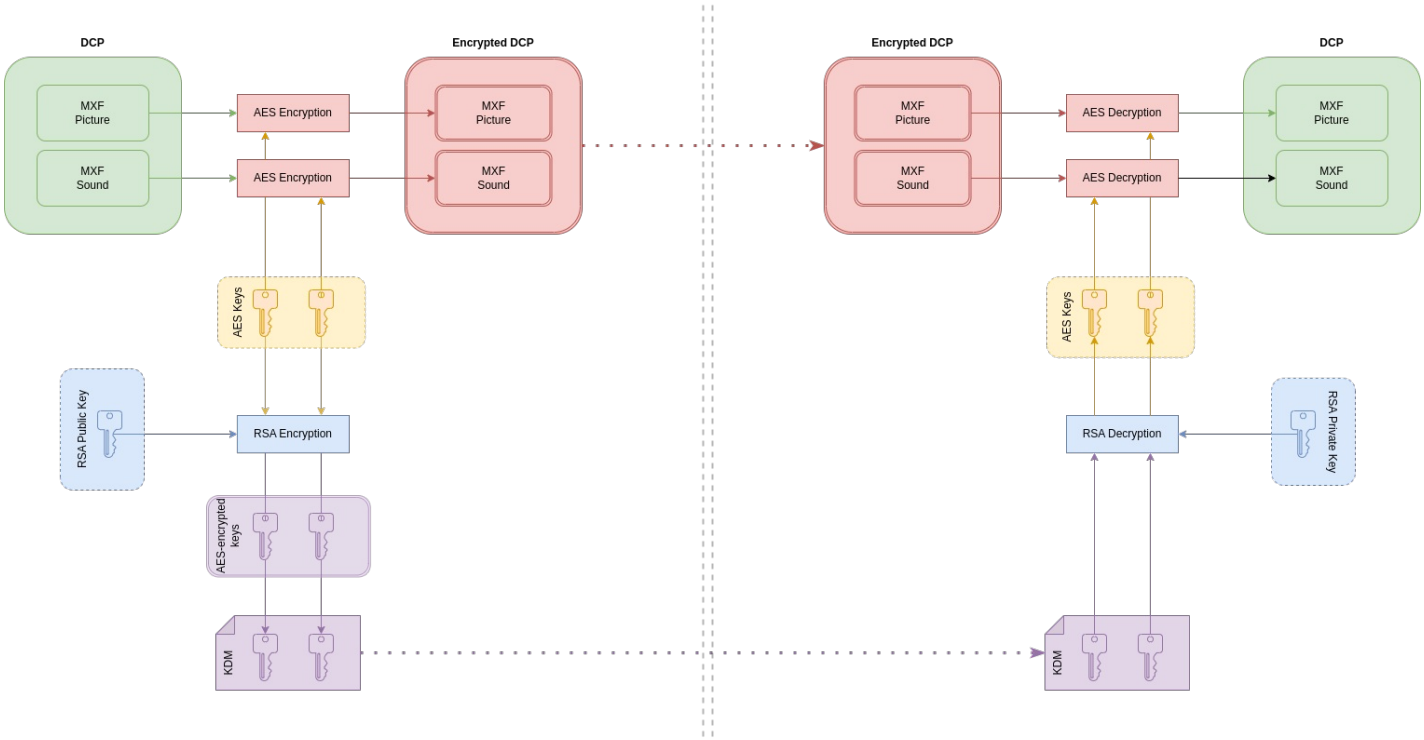
The internal structure of a KDM is based on the following standards :

- Standards **D-Cinema Generic Extra-Theater Message (ETM)**.
- Standards **Key Delivery Message (KDM)**

The first one (ETM) defines a common format (XML) for data and information exchanges between equipment or services in the digital cinema field. The second (KDM) uses the ETM format as a basis and build on it adding or removing elements in order to create a final format : the KDM.

KDM PRINCIPLE

To understand the principle, let's get back to the distribution workflow of a digital film in theater and its constraints :



When a movie is distributed in theaters, all copies of a given version of a movie (such as the French version) sent in theaters are identical. They isn't an individual copy for each theater, they are all identical.

It allows a movie to be easily distributed to several theaters. It prevents a laboratory from making several different copy for each theater that requests it: the laboratory only needs to create a single DCP and send it to all theaters.

Think of it like a DVD or Blu-ray sold in stores: everyone who buys the DVD of a movie gets the same copy. You don't get a custom-made copy just for you and your DVD player.

Why don't we create individual encrypted DCPs for each theater ?

We have to consider the logitics of theatrical delivery: In France, for example, a movie can be distributed to over 400 or even 500 screens. If a laboratory were to encrypt each DCP copy, it should encrypt tera-octets (or even peta-octets) of data to create each copy.

If that were the case, it would require extraordinary computing power — for each copy of a movie, and for every differents versions (original, dubbed, 2D, 3D, Dolby Atmos, ..), and for all movies released in the same week : that's impossible. Even more so in the early 2000s when the DCI specifications were created.

Thus, a single DCP encryption for every theater was adopted.

So, in theater, screen #1 will have the same copy as screen #2.

From this point, to decrypt a DCP, we need to deliver the encryption keys to the theaters.

For security reasons, it is impossible to deliver them to all theaters in plain sight and accessible to anyone : if these keys are leaked, they would allow anyone to decrypt the movie without any problem.

Thus, there is a second mechanism: that of encrypting the encryption keys to create derived keys with the help of another specific cryptographic method which provides a kind of "link" with the equipment in the projection booth (or in a laboratory): Therefore, we can generate a unique key for each screen.

If you haven't read it yet, I recommend reading the following chapter Cryptography that explains all cryptographic concepts involved, with beautiful diagrams.

FIGURATIVE EXPLANATIONS

Use an allegory as example :

Imagine a house (DCP) with several closed rooms (encrypted MXF) that are locked by keys (AES).

These keys (AES) must be transmitted to certain people (eg. theaters, laboratories). To do that, they provide their own mini Safe (RSA public certificate).

As soon as it's closed, these safes can only be opened with a private code (RSA private key) that each of these people has. When the safe is closed, it's impossible to open it, not even by you and someone else. Only the holder of the private code can open their own safe.

Put the key (AES) inside the safe and close it (using the RSA public certificate - which gives an encrypted data for real, but in our example, we just close the safe).

At last, for logistic reason, you put this safe inside a big delivery cardboard box (KDM) accompagnied by a letter containing some useful and public information (KDM Metadata) for those who receive or process the delivery cardboard box (such as the software in booth like TMS).

The person will receive the delivery cardboad box (KDM), they open it, read the letter (KDM Metadata) to know what the box contains. Then, with their own private code (RSA privave key), they open their own safe (for real, the safe is encrypted data) : at last, they got the key (AES).

Fundamentally and technicaly, after all the processes, the delivery cardboard box (KDM) is useless. In other words, a KDM becomes totally useless once you have access to the AES keys.

However, for several reasons (such as the right management), the DCI players store theses informations (either the entire KDM, or just the metadata) in order to determine whether a theater can or cannot exploit the movie.

To summarize :

- "The house" is our own digital movie (DCP)
- "The closed room" is our encrypted MXF.
- "The key" is our AES key [1]
- "The safe with the private code" are our RSA public certificate (safe) and RSA private certificate (private code)
- "The cardboard box" and "the letter" are own KDM and these metadata.

Thus, our KDM stores :

- Our letter : the public and non-encrypted metadata (in plaintext)
- Our safe : the private and encrypted data (AES keys)

In summary: the main purpose of a KDM is to store AES keys which will be used to decrypt the encrypted MXF and will be identified in the CPLs.

INSIDE A KDM

A KDM is a file in XML format (UTF-8 encoding).

To help with understanding the rest of the document, Get straight to the core with an example of a complete KDM [2], including optional elements, for a CPL generated for this particular case :

```
<?xml version="1.0" encoding="UTF-8"?>
<DCinemaSecurityMessage xmlns="http://www.smpte-ra.org/schemas/430-3/2006/ETM">
  <AuthenticatedPublic Id="ID_AuthenticatedPublic">
    <MessageId>urn:uuid:324767c2-b6c9-40ab-90a1-cb947849e097</MessageId>
    <MessageType>http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type</MessageType>
    <AnnotationText language="en">KDM</AnnotationText>
    <IssueDate>2022-10-02T21:07:09+00:00</IssueDate>
    <Signer xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509IssuerName>dnQualifier=\+LLvuYNO4YBJSp9Jjmlv8oippzQ=,CN=.DC.DMS.DC2.SMPTE,OU=DC.DOREMILABS.COM,O=DC2.SM
      <ds:X509SerialNumber>643</ds:X509SerialNumber>
    </Signer>
    <RequiredExtensions>
      <KDMRequiredExtensions xmlns="http://www.smpte-ra.org/schemas/430-1/2006/KDM">
        <Recipient>
          <X509IssuerSerial xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
            <ds:X509IssuerName>dnQualifier=BnB0iDJLgyqiWUjn1uqrOy2/DEE=,CN=.US1.DCS.DOLPHIN.DC2.SMPTE,OU=DC.DOREMILAB
            <ds:X509SerialNumber>88529450606517722</ds:X509SerialNumber>
          </X509IssuerSerial>
          <X509SubjectName>dnQualifier=1xGSxNEWLq7EwRnJ2EAEBoOTfIY=,CN=LE SPB MD FM SM.IMB-239697.DC.DOLPHIN.DC2.SMPT
        </Recipient>
        <CompositionPlaylistId>urn:uuid:1ce461e5-548f-4b91-a70a-60b7bc077fb5</CompositionPlaylistId>
        <ContentTitleText language="en">DCP-INSIDE KDM</ContentTitleText>
        <ContentAuthenticator>86yEpVl81kHxy/8bbkZTeXJcVx4=</ContentAuthenticator>
        <ContentKeysNotValidBefore>2010-01-01T00:00:00+02:00</ContentKeysNotValidBefore>
        <ContentKeysNotValidAfter>2040-12-31T23:59:59+02:00</ContentKeysNotValidAfter>
      <AuthorizedDeviceInfo>
        <DeviceListIdentifier>urn:uuid:8d000cc3-1ac2-4b65-a01e-aeb3f17a0211</DeviceListIdentifier>
        <DeviceListDescription language="en">my device list</DeviceListDescription>
        <DeviceList>
          <CertificateThumbprint>2jmj7l5rSw0yVb/vlWAYkK/YBwk=</CertificateThumbprint>
        </DeviceList>
      </AuthorizedDeviceInfo>
      <KeyIdList>
        <TypedKeyId>
          <KeyType scope="http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type">MDIK</KeyType>
          <KeyId>urn:uuid:abadcafe-abad-cafe-abad-cafe00000001</KeyId>
        </TypedKeyId>
        <TypedKeyId>
          <KeyType scope="http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type">MDAK</KeyType>
          <KeyId>urn:uuid:abadcafe-abad-cafe-abad-cafe00000002</KeyId>
        </TypedKeyId>
        <TypedKeyId>
          <KeyType scope="http://www.smpte-ra.org/430-1/2006/KDM#kdm-key-type">MDSK</KeyType>
          <KeyId>urn:uuid:abadcafe-abad-cafe-abad-cafe00000003</KeyId>
        </TypedKeyId>
        <TypedKeyId>
          <KeyType scope="http://www.dolby.com/cp850/2012/KDM#kdm-key-type">MDEK</KeyType>
          <KeyId>urn:uuid:abadcafe-abad-cafe-abad-cafe00000004</KeyId>
        </TypedKeyId>
      </KeyIdList>
      <ForensicMarkFlagList>
          <ForensicMarkFlag>http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-picture-disable</ForensicMarkFlag>
          <ForensicMarkFlag>http://www.smpte-ra.org/430-1/2006/KDM#mrkflg-audio-disable</ForensicMarkFlag>
          <ForensicMarkFlag>http://www.dcimovies.com/430-1/2006/KDM#mrkflg-audio-disable-above-channel-12</ForensicMa
      </ForensicMarkFlagList>
      </KDMRequiredExtensions>
    </RequiredExtensions>
    <NonCriticalExtensions/>
  </AuthenticatedPublic>
  <AuthenticatedPrivate Id="ID_AuthenticatedPrivate" xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
    <enc:EncryptedKey>
      <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
        <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#s
      </enc:EncryptionMethod>
      <enc:CipherData>
        <enc:CipherValue>MEXikAS/9WQTEG1mZs8gBICWym2OciZCq7hR0YCdsPr6jvPMeASr
mU0WxFbUHpkUASZa737KfgPo/XB2VXt2exUUvskbLetkoMlpICeLU5/JdNPBhWPbphDXAXqzO8wE
riNFSmUQaKd5ds5Z5nPDhfTsPX70vfrqX6HeUz6aX676/D2GfuZyhxnamLYYJprxbnTTridP5WUs
8JM8L5qEwqdxLZK0UoYEW9gRpfg3iYpBr8dqIdLC2kvGzaEuKU0F0kOHiTANlwnXKEZkRLcHBlti
5O0RN9Tzce+t/D1LZG2MvvzwVnWNYoyD/ozuww+wISOC5TOQwAUgPg2IrKIW1A==</enc:CipherValue>
      </enc:CipherData>
    </enc:EncryptedKey>
    <enc:EncryptedKey>
      <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
        <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#s
      </enc:EncryptionMethod>
      <enc:CipherData>
        <enc:CipherValue>SlaeGHfhbm2YgVosrN2qSLsxz+K7N7t09YGWxh3+Ud3HtBElFap5
ayhGBFgPEhnpof3XBsAxbW73C+D/GcXWHkCNEFIaDbYG6cL8EyWIwYeoYstdAPVjLatj4L0InD4H
DV4YeM5xnTpoqMHYS5ICSr0SlJYyHzCLp+Plj0Fv/IS0y9CXTrUisX+rFM8ivLdOOOZoBoDn4jyD
eKBm38Fcw9fTpve8hDFR5syGXM4bc5S17dUfO+IWcwJlSlq1GpTa3GrZ6Hpdse35GJRm3utk1ma1
VTJ602hjAMu+mjRWbBPFbfaUlmh0iTdCIjSfFo78ChGoJpHdTENCxbDaKC0cpw==</enc:CipherValue>
      </enc:CipherData>
    </enc:EncryptedKey>
    <enc:EncryptedKey>
      <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
        <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#s
      </enc:EncryptionMethod>
      <enc:CipherData>
        <enc:CipherValue>PmqCZD7E45n0Tor7cFJIZnI5sutG1wcgzsMj4wENiQYyiutYB8SH
```

```
7Jc2v8yKwVJGvTUurz2+kimRUb3pDEVW8BneQBZfdmx3McvUE9ZftTHTKkpOXJQmhtoEVor+6NcG
HSo4K+crPBbuRmJXmFPh1Nh+0jFCz1KW6MsMFgu1yNGBs54I6q1OwJXsX6vnYsLst6zYfxwSfpcK
OPJBebpfpe3L1xjpDe7iteoGg+yIObmunkBKvNXKf5rtIVUJ7mVkAnqHIUZpOd25S4dS6SOPW88k
mGtBDVClC+t1GYmgRk82VW6FoN7tU1HE6VOVHO61X0AQw3GUqIU2cGQAB9AAmw==</enc:CipherValue>
      </enc:CipherData>
    </enc:EncryptedKey>
    <enc:EncryptedKey>
      <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
        <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000/09/xmldsig#
      </enc:EncryptionMethod>
      <enc:CipherData>
        <enc:CipherValue>mNZp/GPjPaWDIzmbBvF1XcX5AoXVcYUOdeXkAcdUTHK+YxNrqm0N
HZoSp7watPwjFHS+FwcH5r62SDHf9hbWlLI9EBakj6xXQ1EkStd/i7gviUA6LJhAnTjjlMTdWclj
v5Dqto6yOZwg/yZbo+ea87GoscZvFO4BuMuwUic/U1iPjYg3eM87r8VsH9+MqriV/8XeJ8xnn38c
r6mI5/TbHf53Slu+Ft4dk49DsN6MMHos5WWr7J6GFtNRJICa9F7IrXMiCqG9CZxw7Zlt8Z90l5uz
4m3lip/a2DjuiruUKD/XAz4uSCGCMYD3Q8eUw5tpLKkPmKqlY1K4pkSbueuXKg==</enc:CipherValue>
      </enc:CipherData>
    </enc:EncryptedKey>
  </AuthenticatedPrivate>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#ID_AuthenticatedPublic">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>qN4dvJpemd94ppazl6ii6nmo9JflBczdpT9yXb3ltow=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference URI="#ID_AuthenticatedPrivate">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>9bowz05/W7f4qTJfO4K1VXTYEI14uQgJDYr6Z1uP/Ho=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>FylhfvacbWQ8mcxLiGI3B6HL0EczuISQBYd+Ebkrll4oWs5R
UaKnq4GA6o6+LE2myNf2OdNcJ/7IKPvrDw8NFXR7KVrDWcJa9CGaXd87uxFpsUiBBj3u9Q/E
IM4gaBH/RaaRsy0tKmEenguo6JWMVBBLE20bfLdOrBirpIyTbaIDUCyiUaI4qLrxR0uhuHvJ
gTejDcNbznGPn4esFjcZHTO/C6EDW1U/N3t+AGOcCCjYBf80dIoAOluhVNyglWtVDNeW02sM
tYuWc7m1swzjYqiBk+INkHnPrUvRsxZgzWoo3XGfgbXr15e2TY/IFN2C7bdJ5r6vXpB4dPfH
ThNxmg==</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>dnQualifier=\+LLvuYNO4YBJSp9Jjmlv8oippzQ=,CN=.DC.DMS.DC2.SMPTE,OU=DC.DOREMILABS.COM,O=
            <ds:X509SerialNumber>643</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
          <ds:X509Certificate>MIIEejCCA2KgAwIBAgICAoMwDQYJKoZIhvcNAQELBQAwgYIx
ITAfBgNVBAoTGERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFC
Uy5DT00xGjAYBgNVBAMTES5EQy5ETVMuREMyLlNNUFRFMSUwIwYDVQQuExwrTEx2dVlOTzRZQkpT
cDlKam1sdjhvaXBwelE9MB4XDTA3MDEwMTAwMDAwMFoXDTI1MTIzMTIzNTk1OVowgY4xITAfBgNV
BAoTGERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFCUy5DT00x
JjAkBgNVBAMTHUNTLkRNU0pQMkstODAxMTkuREMuREMyLlNNUFRFMSUwIwYDVQQuExxTUUZZU1Nx
V3dqZWZwcHFhc01KbWZkbVM2bEk9MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvGKl
+zNPc1gqagM3K1JiThcaQW9u9MOYtTJMTVRixOfu5sGIOYAFf6FmSf5VneEGG9td/iN6GplI1e5u
pTvkyw1CTmiuAp3pqcqLhM8vyPntzloICTNxe9AIiuOnJQO1khLGUQ1pgD5Mvpfya/4Iiqnq8upR
84PoLnnsEKvoxeuXa1iLrCyDZykP7Ybn8U5muzdAqr9YRuFzFzbbq8Fcrz1uPhyKeK0i6+ZQVdfT
8xy4BuNGQcucimPGoImu+2yfNbEcfFQffDA5bGzR2/XDJTLEaqNwe/WXZyGokZtIRzmFJYGb4Zy+
pYGWIK5umuhjNFETufNI48mybNZtelpjIwIDAQABo4HrMIHoMAwGA1UdEwEB/wQCMAAwCwYDVR0P
BAQDAgSwMB0GA1UdDgQWBBRJAVhJKpbCN5+mmpqwwmZ92ZLqUjCBqwYDVR0jBIGjMIGggBT4su+5
g07hgElKn0mOaW/yiKmnNKGBhKSBgTB/MSEwHwYDVQQKExhEQzIuU01QVEUuRE9SRU1JTEFCUy5D
T00xGjAYBgNVBAsTEURDLkRPUkVNSUxBQlMuQ09NMRcwFQYDVQQDEw4uRE1TLkRDMi5TTVBURTEl
MCMGA1UELhMcUlEvNTNSbXVMc2J6Z2ZQWEdsUlltSnJ1d01zPYIBAjANBgkqhkiG9w0BAQsFAAOC
AQEAPBpZ6Tkg9TZg2LamLaOCPE6ingBvqmsQHR5V4b99sNU/EvdGL2eJjZFw4YLsxaEmPppIGFdM
IE+QJHrED5YLaJ9i1VvTbD1jNfrclW4Sbc6+mlQKFC6vOD5/go3hLYC8A5w92ea75iX77SuD0DCD
1GIs6FL3EGSrMXC59HFK4ahnIkxcUyhV75Cn14ujaOQpiO+zBxr/Vai/PDZoy6KSm0yYJEh97q4+
vQYQlRWSP1cF9IjLusrYBTjU30f7rygOR4vcqL8xnNQhYprBlJBn+KS3FqNKtrUoHTF0YtLl4I5l
90octl+vtQNGWxq4xU33Du9qXOBXBE9heSfG3CsmVw==</ds:X509Certificate>
        </ds:X509Data>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>dnQualifier=RQ/53RmuLsbzgfPXGlRYmJruwMs=,CN=.DMS.DC2.SMPTE,OU=DC.DOREMILABS.COM,O=DC2
            <ds:X509SerialNumber>2</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
          <ds:X509Certificate>MIIEdjCCA16gAwIBAgIBAjANBgkqhkiG9w0BAQsFADB/MSEw
HwYDVQQKExhEQzIuU01QVEUuRE9SRU1JTEFCUy5DT00xGjAYBgNVBAsTEURDLkRPUkVNSUxBQlMu
Q09NMRcwFQYDVQQDEw4uRE1TLkRDMi5TTVBURTElMCMGA1UELhMcUlEvNTNSbXVMc2J6Z2ZQWEds
UlltSnJ1d01zPTAeFw0wNzAxMDEwMDAwMDBaFw0yNTEyMzEyMzU5NTlaMIGCMSEwHwYDVQQKExhE
```

```
QzIuU01QVEUuRE9SRU1JTEFCUy5DT00xGjAYBgNVBAsTEURDLkRPUkVNSUxBQlMuQ09NMRowGAYD
VQQDExEuREMuRE1TLkRDMi5TTVBURTElMCMGA1UELhMcK0xMdnVZTk80WUJKU3A5SmptbHY4b2lw
cHpRPTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMUyBakS7Eb79G3ZFMZ4zOOn/cZ3
qJcck+MAMwjwV8LkK303uBv51cXYNWxalMQQ6h1iPAu6si9RR9XNLGqakHFLUfjt0eC8VJ5/YaC+
DvVq1j9iM5/Jz+CjSqkOlrzXbX92HyMNE0hjCGa4WU6oyRCzFvPZclOI5a2LDKOxC/ngD0LomWjo
MDP7BSkUUzqQnZ2fRuXdOgAfzWm+hBxruWcyEqSGwmV93YBnoHB2WpxVfD+Ztinnp/NJKCadiKf/
sSQpPoqe4j97gY+Zw2DtgT6wddx97ZtCf10QASF5hXgKyCku6O7IlGLroM4TUOldrTClNjR2xSGc
THxcxOltUQcCAwEAAaOB+DCB9TATBgNVHRMBAf8ECTAHAQH/AgIA7TALBgNVHQ8EBAMCAQYwHQYD
VR0OBBYEFPiy77mDTuGASUqfSY5pb/KIqac0MIGxBgNVHSMEgakwgaaAFEUP+d0Zri7G84Hz1xpU
WJia7sDLoYGKpIGHMIGEMSEwHwYDVQQKExhEQzIuU01QVEUuRE9SRU1JTEFCUy5DT00xGjAYBgNV
BAsTEURDLkRPUkVNSUxBQlMuQ09NMRwwGgYDVQQDExMuUFJPRFVDVFMuREMyLlNNUFRFMSUwIwYD
VQQuExxwa0NCOWo1S3JBam5kaGNCa2MzZk9kZkwvQlE9ggEEMA0GCSqGSIb3DQEBCwUAA4IBAQCd
l6G6uFf9+waSrTQqG946Ff1t0b1ANkI6IQQo2sq15aArKjehmrCJzctBfFm3vQj1KlRBI191Mj2m
5Oh/sxcwtG40bSzFeyGZPg9zKA2Cd8oRdw35/8ZLnP96Z/rCxoGNVJAmy9EP8jP9AT/bOk50KvZ/
wo//VN/pscoDrDCaZVLNPAkTdsMNWy+YpV9cnzUGx73jK/iMao++GQ/SEWssBHhjxn3oHWiZi4Xt
ykib8XQqQjyKu4c66jDwu6Ct+MVqUd7ZFPTFListIamu55RnpTXhDKkoN8fIunBsWOs9KbqbxglX
4zsyE0AGuj2nDstRBWLRy+5SlCByTIKp/PL/</ds:X509Certificate>
        </ds:X509Data>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>dnQualifier=pkCB9j5KrAjndhcBkc3fOdfL/BQ=,CN=.PRODUCTS.DC2.SMPTE,OU=DC.DOREMILABS.COM,
            <ds:X509SerialNumber>4</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
          <ds:X509Certificate>MIIEdDCCA1ygAwIBAgIBBDANBgkqhkiG9w0BAQsFADCBhDEh
MB8GA1UEChMYREMyLlNNUFRFLkRPUkVNSUxBQlMuQ09NMRowGAYDVQQLExFEQy5ET1JFTUlMQUJT
LkNPTTEcMBoGA1UEAxMTLlBST0RVQ1RTLkRDMi5TTVBURTElMCMGA1UELhMccGtDQjlqNUtyQWpu
ZGhjQmtjM2ZPZGZML0JRPTAeFw0wNzAxMDEwMDAwMDBaFw0yNTEyMzEyMzU5NTlaMH8xITAfBgNV
BAoTGERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFCUy5DT00x
FzAVBgNVBAMTDi5ETVMuREMyLlNNUFRFMSUwIwYDVQQuExxSUS81M1JtdUxzYnpnZlBYR2xSWW1K
cnV3TXM9MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuqXUXsGFKhmSNFaqAMHloGUp
vTFkFlnjHwRYxUv1JhQjKmysUhyqvXRf7jnx54zsRKdvOXUw3HfGrX9R9gPODL8uVbME406OTqD1
fhhhZ0co02TgXPpaYxkQZlgv9Ygz3pHA51+qXOaMRbPU364gTMPVgXyqljIlDKknZTXeiqp8KB1N
iTdslrn3IajOxm3pd1Mh2kq2/FyC9qAyZJPbgdcSfm4ZWkxgvllikZ4HQGEuT+P31xmN3K7SQrpk
3jRS1PgFHvUUnCeyQh1jtRlepy2Im4SPpWh1sY+hiR2dakqZCFNKB11wEyZOX3nCqOeDfJL60BNm
9RKgSwPVh6SSywIDAQABo4H0MIHxMBMGA1UdEwEB/wQJMAcBAf8CAgDuMAsGA1UdDwQEAwIBBjAd
BgNVHQ4EFgQURQ/53RmuLsbzgfPXGlRYmJruwMswga0GA1UdIwSBpTCBooAUpkCB9j5KrAjndhcB
kc3fOdfL/BShgYakgYMwgYAxITAfBgNVBAoTGERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgG
A1UECxMRREMuRE9SRU1JTEFCUy5DT00xGDAWBgNVBAMTDy5ST09ULkRDMi5TTVBURTElMCMGA1UE
LhMcYS93VUlITHVGVzdSS1hwTlFHbVE5NjZ4T3Y4PYIBAjANBgkqhkiG9w0BAQsFAAOCAQEAXgI7
+4euCqODivtBpzIunWJBGr+v5jojDLFp6e3fBDznYEY6p4R4B741C7HZ6qE39vV6ZqcBmDjDi7cE
fOa9QmC7Mj0MUM/XXrVlLvHmIRwVcOoZdxz/5JSfQkwPGyXT2MTmgGyTAqeB/NXazjR6YzCOcoqm
CcFRgvubRscN4V5GFC2k7JdvP/s9QeU5cGBePy09sUTm54aFS9MbdQGZa+hqCoNetMvjEGhuUxpe
twOLhXUca9KMT2ikxoA4bNc1P5Ekma8HqX0Dv/BKXtz7YTYUUN2YE12PMaqFLonjvl/mB/n9CHc/
AAVM+A/J+q+l4LJqcElnzHkvNTv2Qvp5+g==</ds:X509Certificate>
        </ds:X509Data>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>dnQualifier=a/wUIHLuFW7RKXpNQGmQ966xOv8=,CN=.ROOT.DC2.SMPTE,OU=DC.DOREMILABS.COM,O=DC
            <ds:X509SerialNumber>2</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
          <ds:X509Certificate>MIIEdjCCA16gAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBgDEh
MB8GA1UEChMYREMyLlNNUFRFLkRPUkVNSUxBQlMuQ09NMRowGAYDVQQLExFEQy5ET1JFTUlMQUJT
LkNPTTEYMBYGA1UEAxMPLlJPT1QuREMyLlNNUFRFMSUwIwYDVQQuExxhL3dVSUhMdUZXN1JLWHBO
UUdtUTk2NnhPdjg9MB4XDTA3MDEwMTAwMDAwMFoXDTI1MTIzMTIzNTk1OVowgYQxITAfBgNVBAoT
GERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFCUy5DT00xHDAa
BgNVBAMTEy5QUk9EVUNUUy5EQzIuU01QVEUxJTAjBgNVBC4THHBrQ0I5ajVLckFqbmRoY0JrYzNm
T2RmTC9CUT0wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDTXmBvZYW1jYsr8GaPzJeD
zeWN+Vus/RDVdaWQ9hLXKw2nLjNFNX+RYB76QiugCGUwBZ71kOL0RQ6kSAkz9FBQGYca9sh2imTc
pEuw/qjbHxClO7DNyd0af5oYtZdopBBy71ksrUWOIFeKgfa1C3iLKJWVeTDZll4s78Xzo0hdQVwF
oFyVRiQRkyr2urj0euMMcykBD5KD+hjKNpxZukzxu8VKKBSJwjifL4SsmV+zsTDJH/nRaySnhLCB
L+aO7MF6d4DF+ANKcD5LX6CQW3NIqPHhdPFC+lAol2/6sPBkbnFEfbWiHbDHS34LJaWaLkqJ3tt/
/ETe6FZe761vkeUbAgMBAAGjgfQwgfEwEwYDVR0TAQH/BAkwBwEB/wICAO8wCwYDVR0PBAQDAgEG
MB0GA1UdDgQWBBSmQIH2PkqsCOd2FwGRzd8518v8FDCBrQYDVR0jBIGlMIGigBRr/BQgcu4VbtEp
ek1AaZD3rrE6/6GBhqSBgzCBgDEhMB8GA1UEChMYREMyLlNNUFRFLkRPUkVNSUxBQlMuQ09NMRow
GAYDVQQLExFEQy5ET1JFTUlMQUJTLkNPTTEYMBYGA1UEAxMPLlJPT1QuREMyLlNNUFRFMSUwIwYD
VQQuExxhL3dVSUhMdUZXN1JLWHBOUUdtUTk2NnhPdjg9ggEBMA0GCSqGSIb3DQEBCwUAA4IBAQCd
sDTq1a3Q96o8ShsyKmEKVUCNnX6ez5XcVg5LXb8QJxXzLD+ffbf15Jj201iElpPQCNU9QHNOOoR9
IoObGZBOLi5ekMhfpfffcpwkwmq3nmb3h6WPLU7PAxLYcE3nNZdbv5QocblNs3e4Ecc3nK2bIS0K
9/e+75UT6wfOCWWCF+AHQt+1Uej6G2f2yZJ5aWqeOv3mqXEtWV8W/iiUEhz6pONdb8Vs0Bhn6FMa
jjTkpSVaC/w7W38htkG0Nk9T5Lf/TdIQHjoALB12suLTZymj8hq53PVxIN+aa0cboVE0PEtwYI5J
tIY/GaHgNIVKoTRvgq7YXTVnvGqgolL1zwDx</ds:X509Certificate>
        </ds:X509Data>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>dnQualifier=a/wUIHLuFW7RKXpNQGmQ966xOv8=,CN=.ROOT.DC2.SMPTE,OU=DC.DOREMILABS.COM,O=DC
```

```
            <ds:X509SerialNumber>1</ds:X509SerialNumber>
          </ds:X509IssuerSerial>
          <ds:X509Certificate>MIIEcjCCA1qgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBgDEh
MB8GA1UEChMYREMyLlNNUFRFLkRPUkVNSUxBQlMuQ09NMRowGAYDVQQLExFEQy5ET1JFTUlMQUJT
LkNPTTEYMBYGA1UEAxMPLlJPT1QuREMyLlNNUFRFMSUwIwYDVQQuExxhL3dVSUhMdUZXN1JLWHBO
UUdtUTk2NnhPdjg9MB4XDTA3MDEwMTAwMDAwMFoXDTI1MTIzMTIzNTk1OVowgYAxITAfBgNVBAoT
GERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFCUy5DT00xGDAW
BgNVBAMTDy5ST09ULkRDMi5TTVBURTElMCMGA1UELhMcYS93VUlITHVGVzdSS1hwTlFHbVE5NjZ4
T3Y4PTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/xde0jhq2qV0aBlsyv8Cl4vH1+
RRiAl7DyBwKFk0riupyj+/8naVxcWG0Mx9zkWNyDJKowhMqMAMzNzssphxJoFGTOSVDM+WDlS3JZ
BEgdIrvyTjERWMea32nC3uUu8I6JdEhuiUZBHb2FmQBVsp6S3ss9m0iV5zo/zf3Ev2J0j7mDxcp3
Q68zcpmIeik48qpgtfez+svz2tX9eI1mYZW77v9oQiMRZXMGlaiwNlXp3FqkBjAD6MTEWGInEp6b
OtjksVXwZPbFlHlke+wK1wlWMB0wPFAwGsTfeUbTlaaonSHz0JAf0MORYW49cIbInKJffdrZMRBR
tPmsmNDvlIMCAwEAAaOB9DCB8TATBgNVHRMBAf8ECTAHAQH/AgIA8DALBgNVHQ8EBAMCAQYwHQYD
VR0OBBYEFGv8FCBy7hVu0Sl6TUBpkPeusTr/MIGtBgNVHSMEgaUwgaKAFGv8FCBy7hVu0Sl6TUBp
kPeusTr/oYGGpIGDMIGAMSEwHwYDVQQKExhEQzIuU01QVEUuRE9SRU1JTEFCUy5DT00xGjAYBgNV
BAsTEURDLkRPUkVNSUxBQlMuQ09NMRgwFgYDVQQDEw8uUk9PVC5EQzIuU01QVEUxJTAjBgNVBC4T
HGEvd1VJSEx1Rlc3UktYcE5RR21ROTY2eE92OD2CAQEwDQYJKoZIhvcNAQELBQADggEBAH+n8SDy
Hs9JItFnOOgdxKY9/d8iZUJh5GFWdDpInaW6XRoz5dV6vdXPGAiQwvZuKDniWgg4yhrBbesp4RU4
64p2jzL+YUqnUPews7ZT+u2YVbSfh+fO011kSHZLdzTkdA8BWQCVM0e0rCVLRZMw4VPQpwYmnkeM
gheqKfNSyGKiafhuKGqTnqDrr/74/gIq8ZGl/doidoF/DBiiQlYR7eqlMCsTDam+C9E2cpwBN3A1
5yeuD8d+foFVYVmIR71pHFrJ6tRzuRDwqWdVNQa6/kk3pS1Lut7AWpmNirjIhKWJgDW57KlDGIsw
Bw/YZzykpHYmuzBxLriBb5TYsWziILI=</ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
</DCinemaSecurityMessage>
```


Don't worry about this content, it may seem complex, but it is actually simpler than it looks.

The ETM standard already defines the basic elements we see above.
The KDM standard adds and removes more.
Thus, a KDM is an extended version of an ETM

If we simplify a KDM for a global overview, we can see this :

```
<DCinemaSecurityMessage>
  <AuthenticatedPublic/>    <!-- (1)st part -->
  <AuthenticatedPrivate/>   <!-- (2)th part -->
  <Signature/>              <!-- (3)st part -->
</DCinemaSecurityMessage>
```

Suddenly, it looks much clearer, isn't it ? :)

We quickly notice that a KDM is divided into three main parts :

	Block name	Description
1	**Authenticated Public**	It's the non-encrypted part (plaintext) Freely accessible, it can be read by anyone without cryptographic constraints **It contains necessary metadata for management**.
2	**Authenticated Private**	It's the encrypted part It can only be read using the private certificate of the receiver (player or encoder). **It contains the encrypted AES keys**.
3	**Signature**	It's the part used to authenticated the message. **It contains several fingerprints, signatures and certificates**.

Each part being quite dense, they are covered in the following chapters :

SUBCHAPTERS

- **KDM - Authenticated Public** : the non-encrypted part and readable by anyone
- **KDM - Authenticated Private** : the encrypted part and readable only by the receiver
- **KDM - Signature** : our part in authenticating and validating the KDM

- **KDM - Codes** : Source code and technical tips on each part of the KDM

RELATED CHAPTERS

- **Cryptography** : To understanding the cryptography used in digital cinema.
- **Certificate** : The certificates used in digital cinema.
- **AES Cryptography** : The symmetric cryptography used to encrypt the MXF.
- **RSA Cryptography** : The asymmetric cryptography used in KDM to encrypt AES keys (among others things).

NOTES

1. To be precise, the AES keys will be used to decrypt the encrypted data in the encrypted layer in MXF. See the cryptograhy inside the MXF chapter for details. ↩
2. For the needs of this document, the KDM elements has been modified. They are syntactically correct but cryptographically wrong. For example, signatures are broken and some UUIDs are modified. Don't use it to validate your tools. ↩