KDM : KEY DELIVERY MESSAGE

Version courte : Un[1] KDM est une « clef numérique » pour les DCPs chiffrés.

Version imagée : Un KDM est comme une enveloppe inviolable, scellée et hermétique qui contient une ou plusieurs clefs à l'intérieur, ainsi qu'une lettre contenant des informations à propos de ces clefs, à quoi elles servent, etc.

Version technique : Un KDM est un fichier XML comprenant une multitude de données allant des métadonnées permettant de relier le KDM à une CPL, de définir les dates de validité, jusqu'aux clefs de déchiffrement AES permettant de déchiffrer les assets chiffrés (MXF) qui sont définis dans les CPL d'un DCP.

Un KDM est créé par un laboratoire à destination d'une salle de cinéma pour lui permettre de lire un film numérique chiffré.

Dans quels cas utilise-t-on un KDM ?

Un KDM est utile **que** dans ces deux cas :

- Pour déchiffrer un DCP chiffré (pour une projection, par exemple)
- Partager des clefs de déchiffrements entre deux entités de postproduction (des laboratoires, par exemple)

Un KDM n'est donc pas utile pour des DCP non-chiffrés.

LES NORMES SMPTE

Les différentes normes se rapportant de près ou de loin au 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**

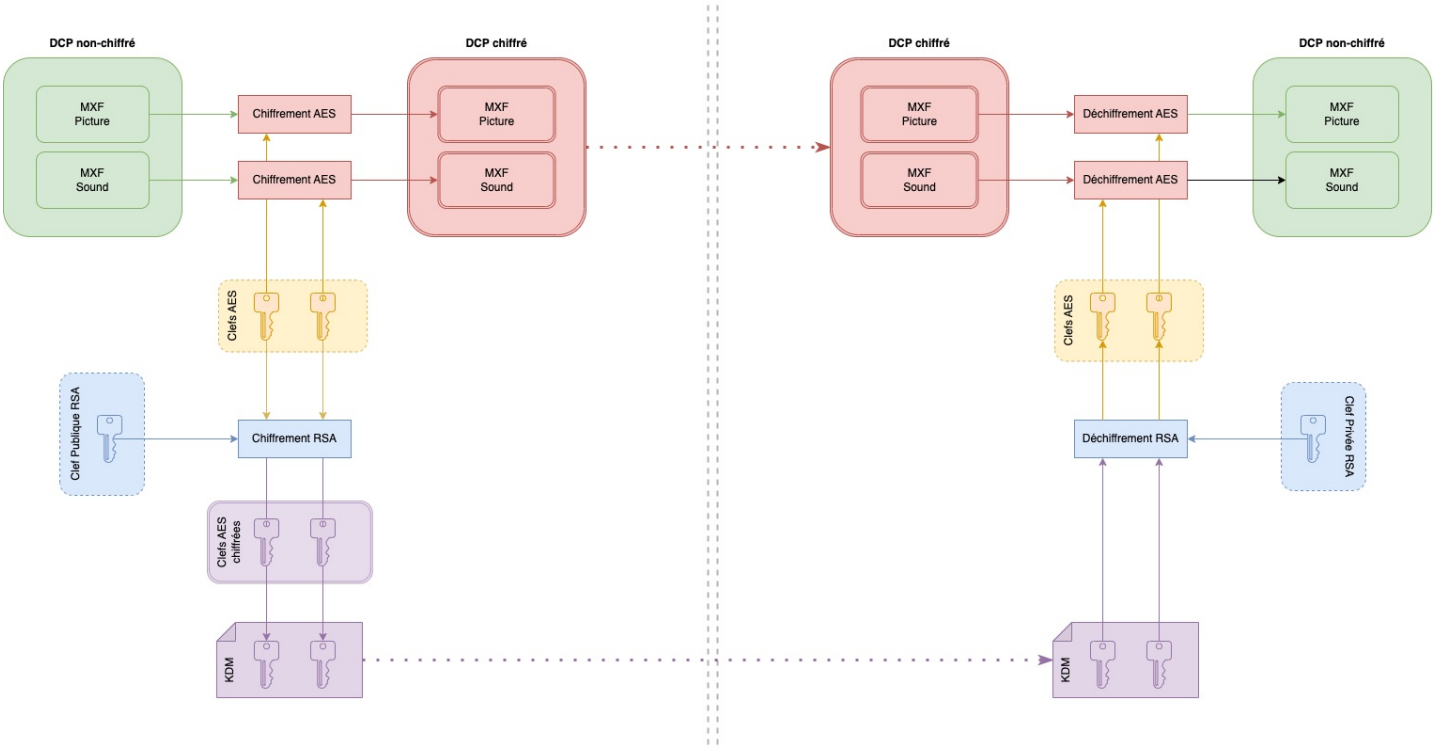
Le format interne d'un KDM est basé sur ces deux normes :

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

La première norme (ETM) définit un format commun (XML) pour des échanges de données et d'informations entre équipements ou services dans l'univers du cinéma numérique. La seconde norme (KDM) utilise l'ETM comme base et la complète en y ajoutant des éléments ou en supprimant d'autres afin de créer le format final : le KDM.

LE PRINCIPE D'UN KDM

Pour comprendre le principe, revenons sur le workflow de distribution d'un film numérique au cinéma et des contraintes.



Quand un film est distribué en salle, toutes les copies d'une version d'un film (par exemple une VF) envoyées dans les différentes salles sont les mêmes. Il n'y a pas une copie chiffrée pour tel cinéma et une autre copie - différente - chiffrée pour un autre cinéma. Elles sont toutes identiques.

Cela permet de distribuer très facilement un film à plusieurs cinémas. Elle évite à un laboratoire de faire plusieurs copies différentes pour chaque cinéma qui en demande : il suffit au laboratoire de faire un seul et unique DCP puis de l'envoyer aux différents cinémas.

Voyez cela comme pour un DVD ou un Bluray dans le commerce : toutes les personnes qui achètent le DVD d'un film auront la même copie, vous ne possédez pas une copie particulière pressée exclusivement pour vous et pour votre lecteur DVD / Bluray.

Vous me direz pourquoi ne pas avoir plusieurs DCPs chiffrés spécifiquement pour tel ou tels salles de cinéma ?

Il faut prendre en compte la logistique de distribution en salle : En France par exemple, un film peut être distribué sur plus de 400-500 salles. Si un laboratoire devait chiffrer chaque copie de DCP unique pour chaque salle, il faudrait chiffrer des téraoctets (voire des pétaoctets) de données afin de pouvoir créer l'ensemble des copies.

Si c'était le cas, il faudrait des puissances de calculs extra-ordinaires, et cela pour chaque copie d'un film, mais également pour ses différentes versions (VO, VF, 2D, 3D, Dolby Atmos, ...) - et également pour les autres films qui sortiront la même semaine : c'est impensable, d'autant plus au début des années 2000 quand les spécifications DCI étaient conçues.

Ainsi, il a été décidé de faire un seul chiffrement unique du DCP puis d'envoyer cette copie chiffrée à l'ensemble des salles.

Ainsi, la salle du cinéma n°1 aura la même copie que la salle du cinéma n°2.

À partir de là, pour déchiffrer le DCP, il faut faire parvenir aux différents cinémas, cette clef de chiffrement qui a servi à chiffrer le DCP.

Pour des raisons de sécurité, il est impensable de donner cette clef de chiffrement unique à l'ensemble des salles en clair et à la vue de tous : si cette clef fuitait, elle permettrait de déchiffrer le film sans aucun souci.

Il existe donc un second mécanisme : celui de chiffrer cette clef et d'en créer une clef dérivée - à l'aide d'un autre procédé cryptographique qui sera lié au lecteur qui se trouve dans la cabine de projection (ou dans un laboratoire) : ainsi nous pouvons générer une clef spécifique pour chaque salle de cinéma.

Si vous ne l'avez pas encore vu, je vous conseille de lire le chapitre Cryptographie qui explique toutes les implications cryptographiques, avec de beaux schémas.

EXPLICATIONS IMAGÉES

Utilisons un exemple un peu imagé :

Imaginons une maison (DCP) avec plusieurs chambres fermées (MXF chiffré) à l'aide de clefs (AES).

Ces clefs (AES) doivent être transmises à des personnes tierces (cinémas / labos). Pour ce faire, ces dernières fournissent leur propre mini-coffre-fort (certificat RSA public).

Ces mini-coffres-forts - sitôt fermés - ne peuvent s'ouvrir que via un code privé et unique (certificat RSA privé) que seules les personnes tierces détiennent : dès que vous fermez ce coffre, il vous sera impossible de l'ouvrir, même par vous, seule la personne tierce ayant le code pour son propre coffre pourra ouvrir cette dernière.

Vous mettez votre clef (AES) dans le mini-coffre-fort et vous fermez la porte (en utilisant le certificat RSA public, ce qui va donner une donnée chiffrée, cette procédure ressemble - dans notre exemple - à l'action de fermer la porte du coffre définitivement : vous scellez le tout).

Enfin, pour des raisons de logistique, vous mettez ce mini-coffre-fort dans un énorme carton de livraison (KDM) accompagné d'une lettre contenant quelques informations utiles et publiques (metadonnées KDM) pour celui qui va réceptionner ou même ceux pouvant traiter le colis (par exemple, les logiciels en cabine comme les TMS).

La personne tierce va réceptionner son colis (KDM), elle va l'ouvrir, va lire la lettre (metadonnées KDM) pour savoir ce dont il s'agit, puis - à l'aide de son code privé (certificat RSA privé) - ouvre le coffre (dans notre cas de figure, notre coffre sera notre donnée chiffrée) et elle aura enfin accès à sa clef (AES).

Fondamentalement et techniquement, après ce traitement, l'ensemble du colis est inutile, en d'autres termes, un KDM ne sert plus à rien après avoir accès aux clefs AES.

Cependant, pour des raisons diverses comme la gestion de droits par exemple (DRM), les players DCI conservent ces informations (soit le KDM entier, soit juste ses métadonnées) afin de savoir si l'exploitant peut ou non encore exploiter le film.

En résumé :

- La maison, c'est notre film numérique (DCP)
- La chambre fermée, c'est notre MXF chiffré.
- La clef, c'est notre clef AES [2]
- Le coffre et son code unique, ce sont notre certificat RSA public (coffre) et certificat RSA privé (code d'ouverture)
- Le carton et la lettre, notre KDM et ses métadonnées.

Ainsi notre KDM stocke :

- Notre lettre : ses métadonnées publiques et non-chiffrées (en clair)
- Un "coffre-fort" : nos données privées et chiffrées (clefs AES)

En résumé : la principale activité d'un KDM et de stocker les clefs AES qui serviront à déchiffrer les MXF chiffrés et qui sont identifiées dans la ou les CPL.

A L'INTÉRIEUR D'UN KDM

Un KDM est un fichier au format XML (encodage UTF-8)

Afin qu'on puisse se comprendre dans la suite du document, allons directement au coeur de la bête avec un KDM d'exemple complet [3] incluant même les éléments optionnels - pour une CPL fabriquée pour l'occasion :

```
<?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.SMPTE.DOREMILABS.C
      <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.DOREMILABS.COM,O=DC2.SMPT
            <ds:X509SerialNumber>88529450606517722</ds:X509SerialNumber>
          </X509IssuerSerial>
          <X509SubjectName>dnQualifier=1xGSxNEWLq7EwRnJ2EAEBoOTfIY=,CN=LE SPB MD FM SM.IMB-239697.DC.DOLPHIN.DC2.SMPTE,OU=DC.DOREMILA
        </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</ForensicMarkFlag>
      </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#sha1"/>
      </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#sha1"/>
      </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#sha1"/>
      </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#sha1"/>
      </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>Fylhfvacb WQ8mcxLiGI3B6HL0EczuISQBYd+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=DC2.SMPTE.DOREMI
            <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.SMPTE.DOREMILABS
            <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,O=DC2.SMPTE.DOREM
            <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+14LJqcElnzHkvNTv2Qvp5+g==</ds:X509Certificate>
        </ds:X509Data>
        <ds:X509Data>
          <ds:X509IssuerSerial>
            <ds:X509IssuerName>dnQualifier=a/wUIHLuFW7RKXpNQGmQ966xOv8=,CN=.ROOT.DC2.SMPTE,OU=DC.DOREMILABS.COM,O=DC2.SMPTE.DOREMILAB
            <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=DC2.SMPTE.DOREMILAB
            <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>
```


Ne vous inquiétez pas sur la teneur du contenu, elle parait complexe mais elle est plus simple qu'elle n'y parait.

La norme ETM définie déjà la base des éléments que nous voyons ci-dessus. La norme KDM en ajoute et en supprime d'autres : **Un KDM est donc la version étendue d'un ETM**.

Si on simplifie un KDM pour avoir une vision d'ensemble, voici ce qu'on verrait :

```
<DCinemaSecurityMessage>
  <AuthenticatedPublic/>    <!-- (1)ère partie -->
  <AuthenticatedPrivate/>   <!-- (2)ème partie -->
  <Signature/>              <!-- (3)ème partie -->
</DCinemaSecurityMessage>
```

Tout de suite, cela devient plus lisible, non ? :)

On constate assez rapidement qu'un KDM est séparé en trois parties majeures distinctes :

	Nom du bloc	Description
1	**Authenticated Public**	C'est la partie en clair, sans chiffrement. Libre d'accès, elle peut être lue par n'importe qui sans contrainte cryptographique majeure. **Elle contient les métadonnées nécessaires pour la gestion**.
2	**Authenticated Private**	C'est la partie chiffrée. Elle ne peut être lue que grâce au certificat privé du récepteur (player ou encodeur de laboratoire). **Elle contient les clefs AES chiffrées**.
3	**Signature**	C'est la partie qui sert à authentifier le message. **Elle contient plusieurs empreintes et signatures et des certificats**.

Les différentes parties étant très épaisses, elles sont disponibles en sous-chapitres :

SOUS CHAPITRES

- **KDM - Authenticated Public** : notre partie lisible par tous
- **KDM - Authenticated Private** : notre partie lisible uniquement par le récepteur
- **KDM - Signature** : notre partie pour authentifier et valider le KDM
- **KDM - Codes** : Codes sources et techniques sur les différentes parties du KDM

CHAPITRES CONNEXES

- **La cryptographie** : Pour tout savoir sur la cryptographie utilisée dans le cinéma numérique.
- **Certificats** : Les certificats utilisés dans le cinéma numérique, leurs vies, leurs oeuvres.
- **Cryptographie AES** : La cryptographie symétrique utilisée pour chiffrer les MXF.
- **Cryptographie RSA** : La cryptographie asymétrique utilisée dans les KDM pour chiffrer les clefs AES - entre autres.

NOTES

1. **Un ou une KDM ?** : KDM est l'abréviation de **Key Delivery Message** que nous pourrions traduire par **Message de Livraison de(s) Clef(s)**. Le sujet se porte sur *le message* et non sur *la clef*. Certains peuvent dire *une* KDM car ils pensent automatiquement à "*une clef KDM*". Or, le KDM n'est pas concrètement la clef d'un DCP, ce n'est qu'un containeur stockant des métadonnées dont notamment les clefs de (dé)chiffrement utilisées sur les différents MXF de notre DCP. ↩
2. pour être plus précis, la clef AES servira à déchiffrer les données chiffrées dans les seules couches chiffrées du MXF. Voir chapitre cryptographie pour plus de détails. ↩
3. Pour les besoins de la documentation, les éléments du KDM ont été modifiés, ils sont donc syntaxiquement corrects et valides mais cryptographiquement erronées. Par exemple, les signatures sont cassées et ne valideront plus sur un système Digital Cinema (DCI) et certains UUID modifiés. N'essayez pas de valider vos outils avec ce KDM d'exemple. ↩