CERTIFICATS : LES BASES

> Ce chapitre sera orienté sur les certificats **publics** et principalement utilisés dans le cinéma numérique

PRÉFACE

Les certificats sont la partie essentielle du workflow sécurité du cinéma numérique normé par le SMPTE et DCI.

Les spécifications DCI et la normalisation SMPTE définissent que la cryptographie asymétrique utilisée dans le cadre du cinéma numérique est la cryptographique asymétrique RSA.

Pour rappel, la **cryptographie asymétrique** nécessite de créer deux types de clefs, chacune ayant un rôle spécifique : une clef privée et une clef publique. La **clef privée servant à déchiffrer** (ou signer) et la **clef publique servant à chiffrer** (ou à vérifier la signature d'un document signé par la clef privée).

Pour distribuer la clef publique, vous pouvez :

- Distribuer la clef publique au format brut, sans aucune fioriture. Elle intègrera les valeurs cryptographiques utiles pour le chiffrement (appelés modulus et exposant, que nous croisons par la suite dans ce chapitre mais qui sont détaillées dans le chapitre RSA),
- Intégrer cette clef publique dans un containeur et l'accompagner de plus amples informations - des métadonnées - comme une identification, des dates de validité, le nom du parent ou toutes autres informations, qui permettrait d'en savoir plus sur cette clef publique ou même d'en faire la gestion.

Ce container se nomme un **Certificat**.

Les métadonnées représentent parfois beaucoup plus de données que la clef publique en elle-même :)

En résumé: un certificat n'est qu'une fiche signalétique incorporant des informations et la clef publique. Voyez cela comme une enveloppe : à l'intérieur de l'enveloppe, votre clef (publique). A l'extérieur, l'adresse du destinataire, de l'expéditeur, etc...

QUI UTILISE CES CERTIFICATS ET POURQUOI ?

Les certificats sont utilisés à plusieurs reprises dans le workflow DCI :

- **CompositionPlaylist** (CPL) : Pour l'authenticité et l'intégrité - à l'aide d'une signature.
- **PackingList** (PKL) : Pour l'authenticité et l'intégrité également - à l'aide d'une signature.
- **KDM** : Pour l'authenticité, l'intégrité mais surtout pour la confidentialité : pour le chiffrement.
- **Certificats** : Créér et signer toute la chaîne de certifications (nous verrons ce concept dans ce chapitre).

Les certificats sont utilisés par tout appareil respectant les spécifications DCI (et donc SMPTE), ainsi vous aurez - principalement - des certificats pour les players DCP, les encodeurs DCP et les générateurs de KDM.

Les certificats sont principalement échangés entre laboratoires et exploitants de cinéma pour pouvoir chiffrer et signer des KDM. [1]

ET DANS QUELS CONTEXTES ?

On va utiliser les certificats dans des cas comme :

- **A la création d'un KDM** : pour chiffrer les parties du KDM (CipherValue) qui seront déchiffrées par un récepteur [2], nous utiliserons le certificat public du dit-récepteur. Le certificat public de l'encodeur va être intégré dans le KDM.
- **A la création d'un DCP** : PKL et CPL vont être signés par la clef privée de l'encodeur. Son certificat publique sera donc intégré dans PKL et CPL.

PEUT-ON UTILISER N'IMPORTE QUEL TYPE DE CERTIFICAT ?

Réponse rapide : non :-)

Un certificat DCI / SMPTE respecte une structure de données normée par le standard X509 et sur sa version 3 qui ajoute des extensions utiles pour nos besoins spécifiques.

La normalisation du X509v3 est disponible via la RFC 5280 - Internet X509 Public Key Infrastructure Certificate. Ajoutons à cela les modifications spécifiques à la norme SMPTE 430-2 - Digital Certificate définissant les paramètres à respecter afin d'être valide dans un workflow DCI.

Pour la suite des chapitres sur les certificats, je nommerais un certificat respectant les normes SMPTE et les spécifications DCI, un **Certificat x509 DCI** ou **Certificat DCI**, afin de bien faire la différence avec les autres types de certificat x509 utilisés dans d'autres domaines.

A L'INTÉRIEUR D'UN CERTIFICAT DCI

La plupart des certificats sont délivrés sous forme de fichier avec l'extension `.pem` [3], ils sont lisibles simplement via un simple éditeur :

```
-----BEGIN CERTIFICATE-----
MIIEejCCA2KgAwIBAgICAoMwDQYJKoZIhvcNAQELBQAwgYIxITAfBgNVBAoTGERD
Mi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFCUy5D
T00xGjAYBgNVBAMTES5EQy5ETVMuREMyLlNNUFRFMSUwIwYDVQQuExwrTEx2dVlO
TzRZQkpTcDlKam1sdjhvaXBwelE9MB4XDTA3MDEwMTAwMDAwMFoXDTI1MTIzMTIz
NTk1OVowgY4xITAfBgNVBAoTGERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgG
A1UECxMRREMuRE9SRU1JTEFCUy5DT00xJjAkBgNVBAMTHUNTLkRNU0pQMkstODAx
MTkuREMuREMyLlNNUFRFMSUwIwYDVQQuExxTUUZZU1NxV3dqZWZwcHFhc01KbWZk
bVM2bEk9MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvGKl+zNPc1gq
agM3K1JiThcaQW9u9MOYtTJMTVRixOfu5sGIOYAFf6FmSf5VneEGG9td/iN6GplI
1e5upTvkyw1CTmiuAp3pqcqLhM8vyPntzloICTNxe9AIiuOnJQO1khLGUQ1pgD5M
vpfya/4Iiqnq8upR84PoLnnsEKvoxeuXa1iLrCyDZykP7Ybn8U5muzdAqr9YRuFz
Fzbbq8Fcrz1uPhyKeK0i6+ZQVdfT8xy4BuNGQcucimPGoImu+2yfNbEcfFQffDA5
bGzR2/XDJTLEaqNwe/WXZyGokZtIRzmFJYGb4Zy+pYGWIK5umuhjNFETufNI48my
bNZtelpjIwIDAQABo4HrMIHoMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgSwMB0G
A1UdDgQWBBRJAVhJKpbCN5+mmpqwwmZ92ZLqUjCBqwYDVR0jBIGjMIGggBT4su+5
g07hgElKn0mOaW/yiKmnNKGBhKSBgTB/MSEwHwYDVQQKExhEQzIuU01QVEUuRE9S
RU1JTEFCUy5DT00xGjAYBgNVBAsTEURDLkRPUkVNSUxBQlMuQ09NMRcwFQYDVQQD
Ew4uRE1TLkRDMi5TTVBURTElMCMGA1UELhMcUlEvNTNSbXVMc2J6Z2ZQWEdsUllt
SnJ1d01zPYIBAjANBgkqhkiG9w0BAQsFAAOCAQEAPBpZ6Tkg9TZg2LamLaOCPE6i
ngBvqmsQHR5V4b99sNU/EvdGL2eJjZFw4YLsxaEmPppIGFdMIE+QJHrED5YLaJ9i
1VvTbD1jNfrclW4Sbc6+mlQKFC6vOD5/go3hLYC8A5w92ea75iX77SuD0DCD1GIs
6FL3EGSrMXC59HFK4ahnIkxcUyhV75Cn14ujaOQpiO+zBxr/Vai/PDZoy6KSm0yY
JEh97q4+vQYQlRWSP1cF9IjLusrYBTjU30f7rygOR4vcqL8xnNQhYprBlJBn+KS3
FqNKtrUoHTF0YtLl4I5l90octl+vtQNGWxq4xU33Du9qXOBXBE9heSfG3CsmVw==
-----END CERTIFICATE-----
```

Ce format est appelé **ASN.1 PEM** :

- Le format PEM n'est qu'un synonyme pour dire encodage en Base64 :-)
- Et le format ASN.1 est une structure normée pour décrire et stocker les informations (sérialisation) du certificat x509, dans une structure binaire, appelée DER (Distinguished Encoding Rules).

Si nous enlevons notre surcouche base64, voici ce que nous trouvons :

```
$ openssl base64 -d -in certificate.pem \
    | xxd -c 32   # affichage

00000000: 3082 047a 3082 0362 a003 0201 0202 0202 8330 0d06 092a 8648 86f7 0d01 010b 0500  0..z0..b.........0...*.H.
00000020: 3081 8231 2130 1f06 0355 040a 1318 4443 322e 534d 5054 452e 444f 5245 4d49 4c41  0..1!0...U....DC2.SMPTE.DO
00000040: 4253 2e43 4f4d 311a 3018 0603 5504 0b13 1144 432e 444f 5245 4d49 4c41 4253 2e43  BS.COM1.0...U....DC.DOREMI
00000060: 4f4d 311a 3018 0603 5504 0313 112e 4443 2e44 4d53 2e44 4332 2e53 4d50 5445 3125  OM1.0...U.....DC.DMS.DC2.S
00000080: 3023 0603 5504 2e13 1c2b 4c4c 7675 594e 4f34 5942 4a53 7039 4a6a 6d6c 7638 6f69  0#..U....+LLvuYNO4YBJSp9Jj
000000a0: 7070 7a51 3d30 1e17 0d30 3730 3130 3130 3030 3030 305a 170d 3235 3132 3331 3233  ppzQ=0...070101000000Z..25
000000c0: 3539 3539 5a30 818e 3121 301f 0603 5504 0a13 1844 4332 2e53 4d50 5445 2e44 4f52  5959Z0..1!0...U....DC2.SMP
000000e0: 454d 494c 4142 532e 434f 4d31 1a30 1806 0355 040b 1311 4443 2e44 4f52 454d 494c  EMILABS.COM1.0...U....DC.D
00000100: 4142 532e 434f 4d31 2630 2406 0355 0403 131d 4353 2e44 4d53 4a50 324b 2d38 3031  ABS.COM1&0$..U....CS.DMSJP
00000120: 3139 2e44 432e 4443 322e 534d 5054 4531 2530 2306 0355 042e 131c 5351 4659 5353  19.DC.DC2.SMPTE1%0#..U...
00000140: 7157 776a 6566 7070 7161 734d 4a6d 6664 6d53 366c 493d 3082 0122 300d 0609 2a86  qWwjefppqasMJmfdmS6lI=0..'
00000160: 4886 f70d 0101 0105 0003 8201 0f00 3082 010a 0282 0101 00bc 62a5 fb33 4f73 582a  H.............0.........b
00000180: 6a03 372b 5262 4e17 1a41 6f6e f4c3 98b5 324c 4d54 62c4 e7ee e6c1 8839 8005 7fa1  j.7+RbN..Aon....2LMTb....
000001a0: 6649 fe55 9de1 061b db5d fe23 7a1a 9948 d5ee 6ea5 3be4 cb0d 424e 68ae 029d e9a9  fI.U.....].#z..H..n.;...BN
000001c0: ca8b 84cf 2fc8 f9ed ce5a 0809 3371 7bd0 088a e3a7 2503 b592 12c6 510d 6980 3e4c  ..../....Z..3q{.....%....
000001e0: be97 f26b fe08 8aa9 eaf2 ea51 f383 e82e 79ec 10ab e8c5 eb97 6b58 8bac 2c83 6729  ...k.......Q....y.......kX
00000200: 0fed 86e7 f14e 66bb 3740 aabf 5846 e173 1736 dbab c15c af3d 6e3e 1c8a 78ad 22eb  .....Nf.7@..XF.s.6...\.=n>
00000220: e650 55d7 d3f3 1cb8 06e3 4641 cb9c 8a63 c6a0 89ae fb6c 9f35 b11c 7c54 1f7c 3039  .PU.......FA...c.....l.5.
00000240: 6c6c d1db f5c3 2532 c46a a370 7bf5 9767 21a8 919b 4847 3985 2581 9be1 9cbe a581  ll....%2.j.p{..g!...HG9.%
00000260: 9620 ae6e 9ae8 6334 5113 b9f3 48e3 c9b2 6cd6 6d7a 5a63 2302 0301 0001 a381 eb30  . .n..c4Q...H...l.mzZc#..
00000280: 81e8 300c 0603 551d 1301 01ff 0402 3000 300b 0603 551d 0f04 0403 0204 b030 1d06  ..0...U.......0.0...U....
000002a0: 0355 1d0e 0416 0414 4901 5849 2a96 c237 9fa6 9a9a b0c2 667d d992 ea52 3081 ab06  .U......I.XI*..7......f}.
000002c0: 0355 1d23 0481 a330 81a0 8014 f8b2 efb9 834e e180 494a 9f49 8e69 6ff2 88a9 a734  .U.#...0.........N..IJ.I.i
000002e0: a181 84a4 8181 307f 3121 301f 0603 5504 0a13 1844 4332 2e53 4d50 5445 2e44 4f52  ......0.1!0...U....DC2.SMP
00000300: 454d 494c 4142 532e 434f 4d31 1a30 1806 0355 040b 1311 4443 2e44 4f52 454d 494c  EMILABS.COM1.0...U....DC.D
00000320: 4142 532e 434f 4d31 1730 1506 0355 0403 130e 2e44 4d53 2e44 4332 2e53 4d50 5445  ABS.COM1.0...U.....DMS.DC2
00000340: 3125 3023 0603 5504 2e13 1c52 512f 3533 526d 754c 7362 7a67 6650 5847 6c52 596d  1%0#..U....RQ/53RmuLsbzgfP
00000360: 4a72 7577 4d73 3d82 0102 300d 0609 2a86 4886 f70d 0101 0b05 0003 8201 0100 3c1a  JruwMs=...0...*.H.........
00000380: 59e9 3920 f536 60d8 b6a6 2da3 823c 4ea2 9e00 6faa 6b10 1d1e 55e1 bf7d b0d5 3f12  Y.9 .6`...-..<N...o.k...U
000003a0: f746 2f67 898d 9170 e182 ecc5 a126 3e9a 4818 574c 204f 9024 7ac4 0f96 0b68 9f62  .F/g...p.....&>.H.WL O.$z
000003c0: d55b d36c 3d63 35fa dc95 6e12 6dce be9a 540a 142e af38 3e7f 828d e12d 80bc 039c  .[.l=c5...n.m...T....8>..
000003e0: 3dd9 e6bb e625 fbed 2b83 d030 83d4 622c e852 f710 64ab 3170 b9f4 714a e1a8 6722  =....%..+..0..b,.R..d.1p.
00000400: 4c5c 5328 55ef 90a7 d78b a368 e429 88ef b307 1aff 55a8 bf3c 3668 cba2 929b 4c98  L\S(U......h.)......U..<6h
00000420: 2448 7dee ae3e bd06 1095 1592 3f57 05f4 88cb baca d805 38d4 df47 fbaf 280e 478b  $H}..>......?W........8..(
00000440: dca8 bf31 9cd4 2162 9ac1 9490 67f8 a4b7 16a3 4ab6 b528 1d31 7462 d2e5 e08e 65f7  ...1..!b....g.....J..(.1tb
00000460: 4a1c b65f afb5 0346 5b1a b8c5 4df7 0eef 6a5c e057 044f 6179 27c6 dc2b 2657       J.._...F[...M...j\.W.Oay'
```

On constate plusieurs choses :

- Ça pique les yeux
- Nous avons des parties lisibles dans la colonne à droite
- Elle débute par un `0x3082` : c'est un entête typique d'une structure **ASN.1 DER** [4]

Si nous passons notre sortie au format **ASN.1 DER** dans un **parseur ASN.1**, nous allons voir toutes les entrées composant le certificat :

```
openssl base64 -d -in certificate.pem \
    | openssl asn1parse \
        -inform DER \    # notre input sera au format DER
        -i \             # petite indentation
        -dump            # dump hex form
```

```
  0:d=0  hl=4 l=1146 cons: SEQUENCE
  4:d=1  hl=4 l= 866 cons:  SEQUENCE
  8:d=2  hl=2 l=   3 cons:   cont [ 0 ]
 10:d=3  hl=2 l=   1 prim:    INTEGER           :02
 13:d=2  hl=2 l=   2 prim:   INTEGER           :0283
 17:d=2  hl=2 l=  13 cons:   SEQUENCE
 19:d=3  hl=2 l=   9 prim:    OBJECT            :sha256WithRSAEncryption
 30:d=3  hl=2 l=   0 prim:    NULL
 32:d=2  hl=3 l= 130 cons:   SEQUENCE
 35:d=3  hl=2 l=  33 cons:    SET
 37:d=4  hl=2 l=  31 cons:     SEQUENCE
 39:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
```

```
 44:d=5  hl=2 l=  24 prim:      PRINTABLESTRING   :DC2.SMPTE.DOREMILABS.COM
 70:d=3  hl=2 l=  26 cons:    SET
 72:d=4  hl=2 l=  24 cons:     SEQUENCE
 74:d=5  hl=2 l=   3 prim:      OBJECT            :organizationalUnitName
 79:d=5  hl=2 l=  17 prim:      PRINTABLESTRING   :DC.DOREMILABS.COM
 98:d=3  hl=2 l=  26 cons:    SET
100:d=4  hl=2 l=  24 cons:     SEQUENCE
102:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
107:d=5  hl=2 l=  17 prim:      PRINTABLESTRING   :.DC.DMS.DC2.SMPTE
126:d=3  hl=2 l=  37 cons:    SET
128:d=4  hl=2 l=  35 cons:     SEQUENCE
130:d=5  hl=2 l=   3 prim:      OBJECT            :dnQualifier
135:d=5  hl=2 l=  28 prim:      PRINTABLESTRING   :+LLvuYNO4YBJSp9Jjmlv8oippzQ=
165:d=2  hl=2 l=  30 cons:   SEQUENCE
167:d=3  hl=2 l=  13 prim:    UTCTIME           :070101000000Z
182:d=3  hl=2 l=  13 prim:    UTCTIME           :251231235959Z
197:d=2  hl=3 l= 142 cons:   SEQUENCE
200:d=3  hl=2 l=  33 cons:    SET
202:d=4  hl=2 l=  31 cons:     SEQUENCE
204:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
209:d=5  hl=2 l=  24 prim:      PRINTABLESTRING   :DC2.SMPTE.DOREMILABS.COM
235:d=3  hl=2 l=  26 cons:    SET
237:d=4  hl=2 l=  24 cons:     SEQUENCE
239:d=5  hl=2 l=   3 prim:      OBJECT            :organizationalUnitName
244:d=5  hl=2 l=  17 prim:      PRINTABLESTRING   :DC.DOREMILABS.COM
263:d=3  hl=2 l=  38 cons:    SET
265:d=4  hl=2 l=  36 cons:     SEQUENCE
267:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
272:d=5  hl=2 l=  29 prim:      PRINTABLESTRING   :CS.DMSJP2K-80119.DC.DC2.SMPTE
303:d=3  hl=2 l=  37 cons:    SET
305:d=4  hl=2 l=  35 cons:     SEQUENCE
307:d=5  hl=2 l=   3 prim:      OBJECT            :dnQualifier
312:d=5  hl=2 l=  28 prim:      PRINTABLESTRING   :SQFYSSqWwjefppqasMJmfdmS6lI=
342:d=2  hl=4 l= 290 cons:   SEQUENCE
346:d=3  hl=2 l=  13 cons:    SEQUENCE
348:d=4  hl=2 l=   9 prim:     OBJECT            :rsaEncryption
359:d=4  hl=2 l=   0 prim:     NULL
361:d=3  hl=4 l= 271 prim:    BIT STRING
    0000 - 00 30 82 01 0a 02 82 01-01 00 bc 62 a5 fb 33 4f   .0.........b..3O
    0010 - 73 58 2a 6a 03 37 2b 52-62 4e 17 1a 41 6f 6e f4   sX*j.7+RbN..Aon.
    0020 - c3 98 b5 32 4c 4d 54 62-c4 e7 ee e6 c1 88 39 80   ...2LMTb......9.
    0030 - 05 7f a1 66 49 fe 55 9d-e1 06 1b db 5d fe 23 7a   ...fI.U.....].#z
    0040 - 1a 99 48 d5 ee 6e a5 3b-e4 cb 0d 42 4e 68 ae 02   ..H..n.;...BNh..
    0050 - 9d e9 a9 ca 8b 84 cf 2f-c8 f9 ed ce 5a 08 09 33   ......./....Z..3
    0060 - 71 7b d0 08 8a e3 a7 25-03 b5 92 12 c6 51 0d 69   q{.....%.....Q.i
    0070 - 80 3e 4c be 97 f2 6b fe-08 8a a9 ea f2 ea 51 f3   .>L...k.......Q.
    0080 - 83 e8 2e 79 ec 10 ab e8-c5 eb 97 6b 58 8b ac 2c   ...y.......kX..,
    0090 - 83 67 29 0f ed 86 e7 f1-4e 66 bb 37 40 aa bf 58   .g).....Nf.7@..X
    00a0 - 46 e1 73 17 36 db ab c1-5c af 3d 6e 3e 1c 8a 78   F.s.6...\.=n>..x
    00b0 - ad 22 eb e6 50 55 d7 d3-f3 1c b8 06 e3 46 41 cb   ."..PU.......FA.
    00c0 - 9c 8a 63 c6 a0 89 ae fb-6c 9f 35 b1 1c 7c 54 1f   ..c.....l.5..|T.
    00d0 - 7c 30 39 6c 6c d1 db f5-c3 25 32 c4 6a a3 70 7b   |09ll....%2.j.p{
    00e0 - f5 97 67 21 a8 91 9b 48-47 39 85 25 81 9b e1 9c   ..g!...HG9.%....
    00f0 - be a5 81 96 20 ae 6e 9a-e8 63 34 51 13 b9 f3 48   .... .n..c4Q...H
    0100 - e3 c9 b2 6c d6 6d 7a 5a-63 23 02 03 01 00 01      ...l.mzZc#.....
636:d=2  hl=3 l= 235 cons:   cont [ 3 ]
639:d=3  hl=3 l= 232 cons:    SEQUENCE
642:d=4  hl=2 l=  12 cons:     SEQUENCE
644:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Basic Constraints
649:d=5  hl=2 l=   1 prim:      BOOLEAN           :255
652:d=5  hl=2 l=   2 prim:      OCTET STRING
    0000 - 30 00                                             0.
656:d=4  hl=2 l=  11 cons:     SEQUENCE
658:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Key Usage
663:d=5  hl=2 l=   4 prim:      OCTET STRING
    0000 - 03 02 04 b0                                       ....
669:d=4  hl=2 l=  29 cons:     SEQUENCE
671:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Subject Key Identifier
676:d=5  hl=2 l=  22 prim:      OCTET STRING
    0000 - 04 14 49 01 58 49 2a 96-c2 37 9f a6 9a 9a b0 c2   ..I.XI*..7......
    0010 - 66 7d d9 92 ea 52                                 f}...R
700:d=4  hl=3 l= 171 cons:     SEQUENCE
703:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Authority Key Identifier
708:d=5  hl=3 l= 163 prim:      OCTET STRING
    0000 - 30 81 a0 80 14 f8 b2 ef-b9 83 4e e1 80 49 4a 9f   0.........N..IJ.
```

```
    0010 - 49 8e 69 6f f2 88 a9 a7-34 a1 81 84 a4 81 81 30   I.io....4......0
    0020 - 7f 31 21 30 1f 06 03 55-04 0a 13 18 44 43 32 2e   .1!0...U....DC2.
    0030 - 53 4d 50 54 45 2e 44 4f-52 45 4d 49 4c 41 42 53   SMPTE.DOREMILABS
    0040 - 2e 43 4f 4d 31 1a 30 18-06 03 55 04 0b 13 11 44   .COM1.0...U....D
    0050 - 43 2e 44 4f 52 45 4d 49-4c 41 42 53 2e 43 4f 4d   C.DOREMILABS.COM
    0060 - 31 17 30 15 06 03 55 04-03 13 0e 2e 44 4d 53 2e   1.0...U.....DMS.
    0070 - 44 43 32 2e 53 4d 50 54-45 31 25 30 23 06 03 55   DC2.SMPTE1%0#..U
    0080 - 04 2e 13 1c 52 51 2f 35-33 52 6d 75 4c 73 62 7a   ....RQ/53RmuLsbz
    0090 - 67 66 50 58 47 6c 52 59-6d 4a 72 75 77 4d 73 3d   gfPXGlRYmJruwMs=
    00a0 - 82 01 02                                          ...
874:d=1  hl=2 l=  13 cons:  SEQUENCE
876:d=2  hl=2 l=   9 prim:   OBJECT            :sha256WithRSAEncryption
887:d=2  hl=2 l=   0 prim:   NULL
889:d=1  hl=4 l= 257 prim:  BIT STRING
    0000 - 00 3c 1a 59 e9 39 20 f5-36 60 d8 b6 a6 2d a3 82   .<.Y.9 .6`...-..
    0010 - 3c 4e a2 9e 00 6f aa 6b-10 1d 1e 55 e1 bf 7d b0   .H.WL O.$z....
    0040 - 68 9f 62 d5 5b d3 6c 3d-63 35 fa dc 95 6e 12 6d   h.b.[.l=c5...n.m
    0050 - ce be 9a 54 0a 14 2e af-38 3e 7f 82 8d e1 2d 80   ...T....8>....-.
    0060 - bc 03 9c 3d d9 e6 bb e6-25 fb ed 2b 83 d0 30 83   ...=....%..+..0.
    0070 - d4 62 2c e8 52 f7 10 64-ab 31 70 b9 f4 71 4a e1   .b,.R..d.1p..qJ.
    0080 - a8 67 22 4c 5c 53 28 55-ef 90 a7 d7 8b a3 68 e4   .g"L\S(U......h.
    0090 - 29 88 ef b3 07 1a ff 55-a8 bf 3c 36 68 cb a2 92   )......U..<6h...
    00a0 - 9b 4c 98 24 48 7d ee ae-3e bd 06 10 95 15 92 3f   .L.$H}..>......?
    00b0 - 57 05 f4 88 cb ba ca d8-05 38 d4 df 47 fb af 28   W........8..G..(
    00c0 - 0e 47 8b dc a8 bf 31 9c-d4 21 62 9a c1 94 90 67   .G....1..!b....g
    00d0 - f8 a4 b7 16 a3 4a b6 b5-28 1d 31 74 62 d2 e5 e0   .....J..(.1tb...
    00e0 - 8e 65 f7 4a 1c b6 5f af-b5 03 46 5b 1a b8 c5 4d   .e.J.._...F[...M
    00f0 - f7 0e ef 6a 5c e0 57 04-4f 61 79 27 c6 dc 2b 26   ...j\.W.Oay'..+&
    0100 - 57                                                W
```

Oui, ça pique (encore trop) les yeux, même avec l'aide colorimétrique.

Ceci est la structure **ASN.1 DER** d'un certificat x509 DCI - avec ses différents tags (**SEQUENCE**, **INTEGER**, **OBJECT**, **BIT STRING**, etc.).

Vous allez me demander pourquoi je vous montre cela, on est pas là pour souffrir. Je suis obligé de vous montrer ceci car elle aura son importance lors de certains calculs d'empreintes que nous verrons un peu plus tard dans les prochains chapitres.

Cela reste assez illisible pour le quidam qui n'a pas fait un master RFC et une thèse sur l'ASN.1.

Fort heureusement, OpenSSL nous permet d'interpréter sa structure avec une sortie plus lisible :

```
openssl x509 -in certificate.pem -text
```

```
Data:
    Version: 3 (0x2)
    Serial Number: 643 (0x283)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = .DC.DMS.DC2.SMPTE, dnQualifier = "+LLvuYNO4Y
    Validity
        Not Before: Jan  1 00:00:00 2007 GMT
        Not After : Dec 31 23:59:59 2025 GMT
    Subject: O = DC2.SMPTE.DOREMILABS.COM, OU = DC.DOREMILABS.COM, CN = CS.DMSJP2K-80119.DC.DC2.SMPTE, dnQualifier
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:bc:62:a5:fb:33:4f:73:58:2a:6a:03:37:2b:52:
                62:4e:17:1a:41:6f:6e:f4:c3:98:b5:32:4c:4d:54:
                62:c4:e7:ee:e6:c1:88:39:80:05:7f:a1:66:49:fe:
                55:9d:e1:06:1b:db:5d:fe:23:7a:1a:99:48:d5:ee:
                6e:a5:3b:e4:cb:0d:42:4e:68:ae:02:9d:e9:a9:ca:
                8b:84:cf:2f:c8:f9:ed:ce:5a:08:09:33:71:7b:d0:
                08:8a:e3:a7:25:03:b5:92:12:c6:51:0d:69:80:3e:
                4c:be:97:f2:6b:fe:08:8a:a9:ea:f2:ea:51:f3:83:
                e8:2e:79:ec:10:ab:e8:c5:eb:97:6b:58:8b:ac:2c:
                83:67:29:0f:ed:86:e7:f1:4e:66:bb:37:40:aa:bf:
                58:46:e1:73:17:36:db:ab:c1:5c:af:3d:6e:3e:1c:
                8a:78:ad:22:eb:e6:50:55:d7:d3:f3:1c:b8:06:e3:
                46:41:cb:9c:8a:63:c6:a0:89:ae:fb:6c:9f:35:b1:
                1c:7c:54:1f:7c:30:39:6c:6c:d1:db:f5:c3:25:32:
                c4:6a:a3:70:7b:f5:97:67:21:a8:91:9b:48:47:39:
                85:25:81:9b:e1:9c:be:a5:81:96:20:ae:6e:9a:e8:
                63:34:51:13:b9:f3:48:e3:c9:b2:6c:d6:6d:7a:5a:
                63:23
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Key Usage:
            Digital Signature, Key Encipherment, Data Encipherment
        X509v3 Subject Key Identifier:
            49:01:58:49:2A:96:C2:37:9F:A6:9A:9A:B0:C2:66:7D:D9:92:EA:52
        X509v3 Authority Key Identifier:
            keyid:F8:B2:EF:B9:83:4E:E1:80:49:4A:9F:49:8E:69:6F:F2:88:A9:A7:34
            DirName:/O=DC2.SMPTE.DOREMILABS.COM/OU=DC.DOREMILABS.COM/CN=.DMS.DC2.SMPTE/dnQualifier=RQ\/53RmuLsbzgfP
            serial:02
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
    3c:1a:59:e9:39:20:f5:36:60:d8:b6:a6:2d:a3:82:3c:4e:a2:
    9e:00:6f:aa:6b:10:1d:1e:55:e1:bf:7d:b0:d5:3f:12:f7:46:
    2f:67:89:8d:91:70:e1:82:ec:c5:a1:26:3e:9a:48:18:57:4c:
    20:4f:90:24:7a:c4:0f:96:0b:68:9f:62:d5:5b:d3:6c:3d:63:
    35:fa:dc:95:6e:12:6d:ce:be:9a:54:0a:14:2e:af:38:3e:7f:
    82:8d:e1:2d:80:bc:03:9c:3d:d9:e6:bb:e6:25:fb:ed:2b:83:
    d0:30:83:d4:62:2c:e8:52:f7:10:64:ab:31:70:b9:f4:71:4a:
    e1:a8:67:22:4c:5c:53:28:55:ef:90:a7:d7:8b:a3:68:e4:29:
    88:ef:b3:07:1a:ff:55:a8:bf:3c:36:68:cb:a2:92:9b:4c:98:
    24:48:7d:ee:ae:3e:bd:06:10:95:15:92:3f:57:05:f4:88:cb:
    ba:ca:d8:05:38:d4:df:47:fb:af:28:0e:47:8b:dc:a8:bf:31:
    9c:d4:21:62:9a:c1:94:90:67:f8:a4:b7:16:a3:4a:b6:b5:28:
    1d:31:74:62:d2:e5:e0:8e:65:f7:4a:1c:b6:5f:af:b5:03:46:
    5b:1a:b8:c5:4d:f7:0e:ef:6a:5c:e0:57:04:4f:61:79:27:c6:
    dc:2b:26:57
```

En vert, nous avons les données d'identifications principalement. En orange est la clef public (modulus et son exposant, voir chapitre RSA pour mieux comprendre). En bleu, nous avons les extensions x509v3 très utiles pour comprendre le rôle de ce certificat. Et enfin, en rose, la signature de ce certificat.

Chaque entrée est appelé « Champ » ou « Field »

(nous les étudierons un par un dans le prochain chapitre)

AUTRES VISUALISEURS DE CERTIFICATS

Vous avez aussi la possibilité de prévisualiser les métadonnées d'un certificat via d'autres différents outils, par exemple, sous MacOS, via l'outil KeyChain :

Ou également la possibilité de visualiser via des outils en ligne :

Site	Description	Niveau
certificatedecoder.dev	Visualiseur x509 minimaliste	Débutant
certlogik.com/decoder	Visualiseur x509 complet + visualisateur structure ASN.1 normée RFC	Intermédiaire
lapo.it/asn1js	Visualiseur de la structure ASN.1 en mode binaire et normée RFC	Expert

Vous pouvez faire des tests sur les différents sites en effectuant un copier/coller du certificat public ci-dessous :

```
-----BEGIN CERTIFICATE-----
MIIEejCCA2KgAwIBAgICAoMwDQYJKoZIhvcNAQELBQAwgYIxITAfBgNVBAoTGERD
Mi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgGA1UECxMRREMuRE9SRU1JTEFCUy5D
T00xGjAYBgNVBAMTES5EQy5ETVMuREMyLlNNUFRFMSUwIwYDVQQuExwrTEx2dVlO
TzRZQkpTcDlKam1sdjhvaXBwelE9MB4XDTA3MDEwMTAwMDAwMFoXDTI1MTIzMTIz
NTk1OVowgY4xITAfBgNVBAoTGERDMi5TTVBURS5ET1JFTUlMQUJTLkNPTTEaMBgG
A1UECxMRREMuRE9SRU1JTEFCUy5DT00xJjAkBgNVBAMTHUNTLkRNU0pQMkstODAx
MTkuREMuREMyLlNNUFRFMSUwIwYDVQQuExxTUUZZU1NxV3dqZWZwcHFhc01KbWZk
bVM2bEk9MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvGKl+zNPc1gq
agM3K1JiThcaQW9u9MOYtTJMTVRixOfu5sGIOYAFf6FmSf5VneEGG9td/iN6GplI
1e5upTvkyw1CTmiuAp3pqcqLhM8vyPntzloICTNxe9AIiuOnJQO1khLGUQ1pgD5M
vpfya/4Iiqnq8upR84PoLnnsEKvoxeuXa1iLrCyDZykP7Ybn8U5muzdAqr9YRuFz
Fzbbq8Fcrz1uPhyKeK0i6+ZQVdfT8xy4BuNGQcucimPGoImu+2yfNbEcfFQffDA5
bGzR2/XDJTLEaqNwe/WXZyGokZtIRzmFJYGb4Zy+pYGWIK5umuhjNFETufNI48my
bNZtelpjIwIDAQABo4HrMIHoMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgSwMB0G
A1UdDgQWBBRJAVhJKpbCN5+mmpqwwmZ92ZLqUjCBqwYDVR0jBIGjMIGggBT4su+5
g07hgElKn0mOaW/yiKmnNKGBhKSBgTB/MSEwHwYDVQQKExhEQzIuU01QVEUuRE9S
RU1JTEFCUy5DT00xGjAYBgNVBAsTEURDLkRPUkVNSUxBQlMuQ09NMRcwFQYDVQQD
Ew4uRE1TLkRDMi5TTVBURTElMCMGA1UELhMcUlEvNTNSbXVMc2J6Z2ZQWEdsUllt
SnJ1d01zPYIBAjANBgkqhkiG9w0BAQsFAAOCAQEAPBpZ6Tkg9TZg2LamLaOCPE6i
ngBvqmsQHR5V4b99sNU/EvdGL2eJjZFw4YLsxaEmPppIGFdMIE+QJHrED5YLaJ9i
1VvTbD1jNfrclW4Sbc6+mlQKFC6vOD5/go3hLYC8A5w92ea75iX77SuD0DCD1GIs
6FL3EGSrMXC59HFK4ahnIkxcUyhV75Cn14ujaOQpiO+zBxr/Vai/PDZoy6KSm0yY
JEh97q4+vQYQlRWSP1cF9IjLusrYBTjU30f7rygOR4vcqL8xnNQhYprBlJBn+KS3
FqNKtrUoHTF0YtLl4I5l90octl+vtQNGWxq4xU33Du9qXOBXBE9heSfG3CsmVw==
-----END CERTIFICATE-----
```

CONCLUSION

Nous avons rapidement vu ce qu'était un certificat, nous pouvons voir maintenant ce que représente chaque entrée dans le chapitre suivant sur les champs (fields) d'un certificat x509 DCI.

CHAPITRES ANNEXES

- Certificats - Les bases ⬅ vous êtes ici
- Certificats - Les champs (fields) d'un certificat x509 DCI
- Certificats - Identity Attributes - les attributs et leurs rôles
- Certificats - La chaîne de certification
- Certificats - Certificate Thumbprint - l'empreinte du certificat
- Certificats - Public Key Thumbprint (dnQualifier) - l'empreinte de la clef public
- Certificats - Création : Nos propres certificats
- RSA - La cryptographie asymétrique pour le chiffrement et les signatures.

RÉFÉRENCES

Liens vers les principales normes et spécifications :

- SMPTE 430-2 - Digital Certificate
- DCI - Digital Cinema System Specification: Compliance Test Plan - 1.3.3
- RFC 3280 - Internet X.509 Public Key Infrastructure Certificate

NOTES

1. Entre autres. Nous avons d'autres cas, comme des échanges de certificats entre laboratoires pour des échanges de clefs AES par exemple. Les certificats étant publics, vous pouvez les retrouver sur les sites des différents constructeurs. ↩

2. Par exemple, un player DCP ou un autre encodeur - qui va recevoir un DKDM :) ↩

3. L'extension n'est qu'une convention de nommage. On peut trouver des certificats stockés dans fichiers ayant l'extension `.txt`, `.crt`, `.cert`, etc. A noter également que ces certificats peuvent être délivrés même en dehors d'un fichier, par exemple si vous demandez un certificat via l'API du player, il vous délivrera un flux contenant le certificat directement. Aucune obligation d'être dans un fichier donc :) ↩

4. Pour être plus précis, ASN.1 respecte le TLV qui est ... comme un KLV ;-) ↩

   - TLV voulant dire **Type** (ou **Tag** suivant les inspirations des auteurs) **Length Value**,
   - KLV voulant dire **Key Length Value**.

   La seule différence entre les deux semble être sur la taille du **Tag** (1-4 bytes pour TLV, 1-16 pour KLV)

   Voici un exemple d'un TLV **SEQUENCE** d'un x509 :

   ```
   +------+
   |  30  | Tag SEQUENCE
   +------+
   |  82  | Code indiquant que les 2 prochains bytes seront la taille des données (voir KLV)
   +......+
   |  LL  |
   |  LL  |--- the length (ex: 047A : 1146 bytes)
   +------+
   |  DD  |
   |  DD  |___ Les données :)
   |  DD  |
   |  ..  |
   +------+
   ```

   C'est la même chose qu'un KLV, vous pouvez lire la documentation du KLV pour comprendre ainsi la structure binaire interne d'un certificat x509.