CRYPTOGRAPHIE : PRÉFACE

La cryptographie dans l'univers du DCP est un sujet assez vaste : il existe plusieurs utilisations entre le chiffrement des données, les empreintes cryptographiques, authentification et identification.

Toutes ces méthodes sont dispatchées un peu partout dans le workflow DCI / SMPTE.

Mais pas de panique, nous pouvons simplifier tout ceci par deux grands principes : le MXF va utiliser l'algorithme cryptographique symétrique AES, le KDM va utiliser l'algorithme cryptographique asymétrique RSA et PKL et CPL vont utiliser RSA pour l'authentification.

MXF, KDM, PKL et CPL vont utiliser une multitude d'autres algorithmes cryptographiques comme SHA1, HMAC, ...

Toutes ces méthodes sont étudiées dans les différents sous-chapitres.

DIFFÉRENCES ENTRE CRYPTOGRAPHIE SYMÉTRIQUE ET ASYMÉTRIQUE

Effectuons déjà un petit topo sur **la différence entre cryptographie symétrique et cryptographique asymétrie** :

- La **cryptographie symétrique** utilise un algorithme qui a besoin d'**une unique clef** qui permet de chiffrer ET de déchiffrer.
- La **cryptographie asymétrique** utilise un algorithme qui a besoin de **deux clefs** : une clef qui permet de chiffrer et une autre clef qui permet de déchiffrer. Indirectement, la cryptographie asymétrique permet également une authentification des données, c'est-à-dire de valider que des données n'ont pas été modifiées.

Notez que nous reviendrons plus en profondeur dans chaque chapitre utilisant l'une ou l'autre méthode, et surtout le pourquoi.

LE WORKFLOW DU CHIFFREMENT D'UN DCP

Pour des raisons de simplicité dans ce petit paragraphe, nous n'évoquerons que la partie chiffrement pur d'un DCP

Je vais essayer de vous présenter rapidement en quelques lignes les besoins et l'utilisation de ces deux principaux algorithmes, en sachant que nous y reviendrons plus en détails dans les sous-chapitre.

Pour chiffrer les données dans le MXF, on va utiliser l'algorithme symétrique **AES** et donc l'utilisation d'une seule clef.

Cette clef **AES** va servir également à déchiffrer les données du MXF, il faut donc que les salles de cinéma puissent le faire, et donc récupérer la clef.

Sauf que pour distribuer cette clef de déchiffrement comme cela, sans un minimum de sécurité, ça serait un désastre.

On va donc chiffrer cette clef symétrique **AES** en utilisant l'algorithme asymétrique **RSA** !

Si vous vous souvenez, nous évoquions deux clefs pour la cryptographie asymétrique **RSA**, nous allons utiliser la clef de chiffrement RSA pour chiffrer la clef **AES**.

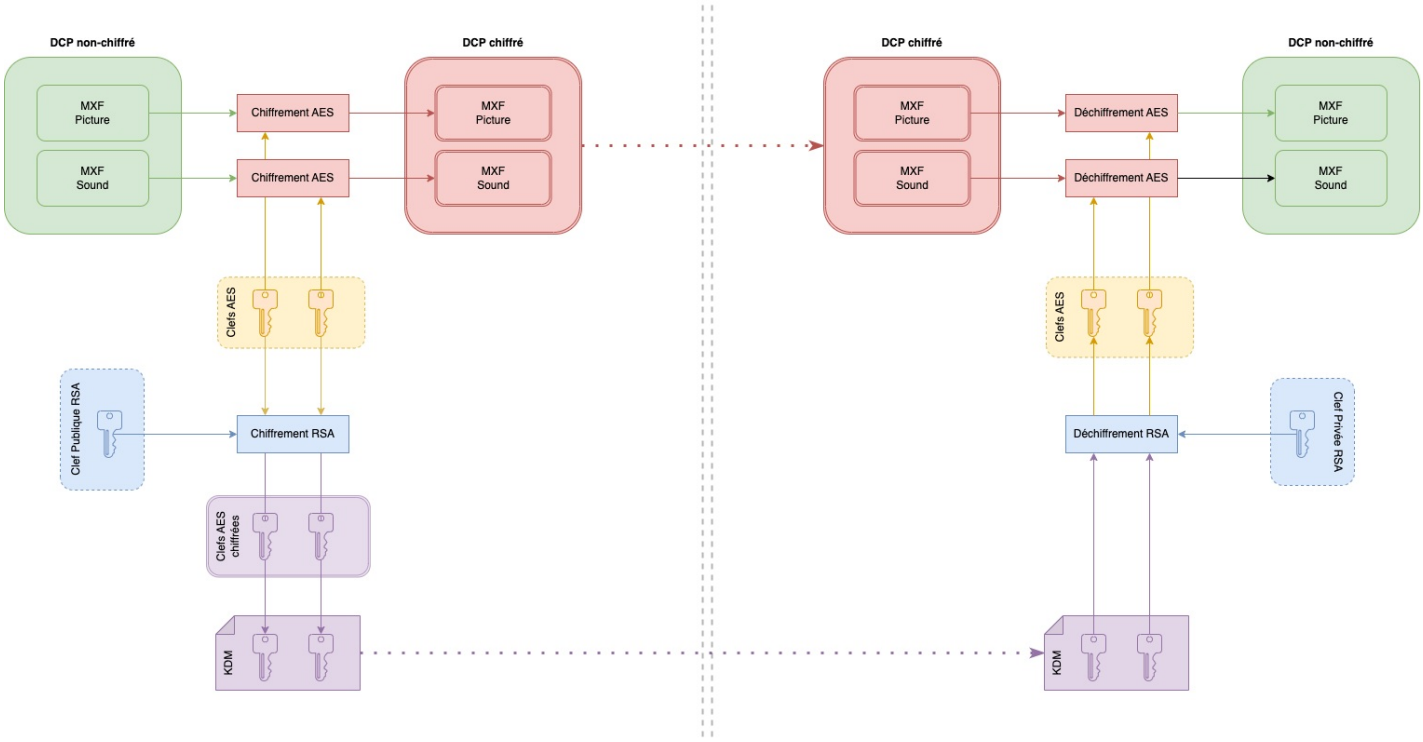
Mais alors qui possède la clef de déchiffrement **RSA** ? L'équipement dans la salle de cinéma !

C'est là toute l'importance de ce workflow cryptographique DCI avec l'algorithme asymétrique **RSA** : les équipes

dans les salles de cinémas possèdent toute une clef RSA qui permettront de déchiffrer les données chiffrées avec l'algorithme asymétrique **RSA**.

Ainsi, on peut distribuer la clef **AES** - qui va nous permettre de lire le DCP - à l'ensemble des salles de cinémas qui en ont besoin et cela sans problème de sécurité majeur.

Voici un schéma résumant ce long monologue ;-)



La partie de gauche est la génération d'un DCP chiffré, nous allons produire des clefs AES pour chaque asset (MXF), puis nous chiffrerons les clefs AES à l'aide de la clef de chiffrement RSA, appelée aussi clef publique RSA. On stocke le résultat dans un message appelé KDM.

DCP et KDM sont transmis au cinéma (à droite).

La seule entité capable de déchiffrer le DCP sera celle qui détient la clef de déchiffrement RSA, appelée aussi clef privée RSA, qui va permettre de déchiffrer les clefs AES chiffrées et ainsi déchiffrer les différents assets du DCP.

Maintenant que vous avez compris cela, vous comprendrez maintenant mieux les différents chapitres et leurs implications.

LES CHAPITRES SUR LA CRYPTOGRAPHIE LIÉE AU DCP

- La cryptographie dans un MXF : Le chiffrement des assets d'un film.
- La cryptographie dans un KDM : les "clefs" de déchiffrement des DCP.

LES ALGORITHMES ET MÉTHODES UTILISÉS

- La cryptographie AES-CBC : Le coeur du chiffrement symétrique.
- La cryptographie RSA : Le coeur du chiffrement asymétrique.
- Les Certificats DCI

ÉVOLUTION(S) FUTURE(S)

- Le SHA1 est considéré comme obsolète, il est à l'étude de faire évoluer l'utilisation du SHA dans les différents composants l'utilisant vers une nouvelle version.

- FIPS 140-2 est considéré comme obsolète, il est à l'étude de passer à FIPS 140-3.