CRYPTOGRAPHY : PREFACE

Cryptography in the DCP world is quite a broad topic : there are many uses including data encryption, hashing, authentification and identification.

All of these methods are spread throughout the DCI / SMPTE workflow.

Don't panic, we are going to simplify all of this into two main principles : the MXF uses symmetric cryptographic algorithm AES, the KDM uses asymmetric cryptographic algorithm RSA, and PKL and CPL use RSA for authentication.

MXF, KDM, PKL and CPL use various cryptographic algorithms such as SHA1, HMAC, ...

All of this will be studied in the following chapters.

DIFFERENCES BETWEEN SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY

Let's start with a quick summary of **the difference between symmetric and asymmetric cryptography** :

- **Symmetric cryptography** uses an algorithm that needs **a unique key** that allows encryption ET decryption.
- **Asymmetric cryptography** uses an algorithm that needs **two keys** : one key that allows encryption and another key that allows decryption. In other way, the symmetric cryptographic allows also a data authentication, in other words, to validate whether the data has not been modified.

We will cover these topics in the following paragraphs and chapters.

THE ENCRYPTION WORKFLOW OF A DCP

For simplicity in this paragraph, we only mention the cryptographic part of a DCP.

I will try to introduce the needs and uses of these two main algorithms, knowing that we will cover each of them in detail in following chapters.

To encrypt data from a MXF, we use symmetric algorithm **AES** which only requires one key.

This **AES** key will be used to decrypt the data in the MXF, therefore the theater must be able to do it, thus retrieve this key.

However, distributing this decryption key without security would be a disaster.

Thus, we will encrypt this **AES** symetric key using the **RSA** asymmetric algorithm !

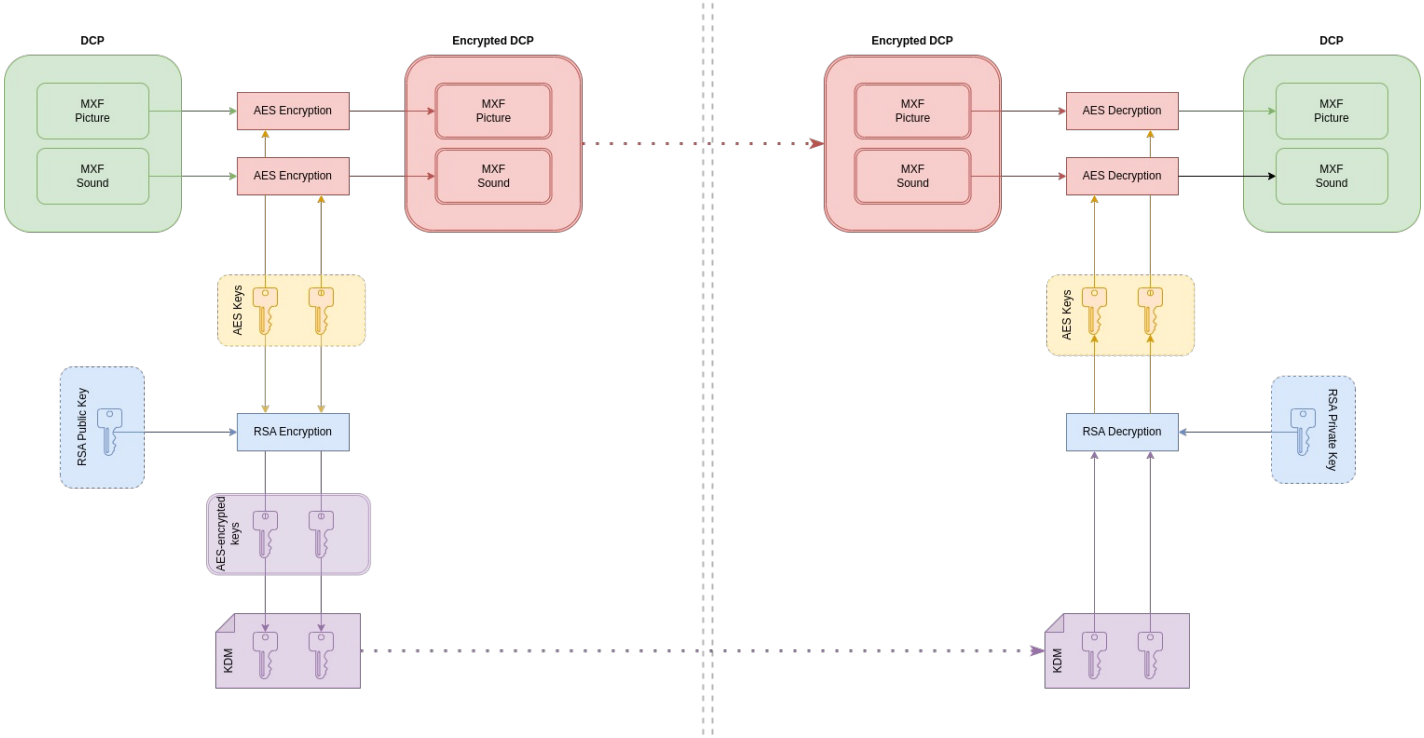
If you remember, we have two keys for asymmetric cryptography **RSA**, so we will use the RSA encryption key to encrypt the **AES** key.

But, who holds the **RSA** decryption key? The equipment in the theater!

That's the whole point of this DCI cryptographic workflow using asymmetric **RSA** algorithm: All theater equipment holds a RSA key that allows them to decrypt data encrypted with asymmetric **RSA** algorithm.

Thus, we can distribute the **AES** key, which allows the DCP to be read, to all theaters that need it and without any security issues.

Here is a diagram that summarizes this long monologue ;-)



The left part shows the generation workflow for an encrypted DCP : we generate AES keys for each assets (MXF), then encrypt each AES keys using RSA encrypt key also called "RSA public key". The result is written into a message called a KDM.

DCP and KDM are transmitted to the theater (right side).

The only entity able to decrypt the DCP is the one that holds the RSA decryption key, also called "RSA private key", which allows it to decrypt the AES-encrypted keys and, thus to decrypt all encrypted assets in the DCP.

Now that you understand this, you'll have a much better understanding of the following chapters.

CHAPTERS ON CRYPTOGRAPHY RELATED TO THE DCP

- Cryptography in MXF : the encryption workflow of the assets.
- Cryptography in KDM : the decryption "keys" for DCP.

ALGORITHMS AND METHODS USED

- AES-CBC cryptography : The core of symmetric encryption.
- RSA cryptography : The core of asymmetric encryption.
- DCI Certificates

FUTURE DEVELOPMENT(S)

- SHA1, which is considered as outdated, should be replaced by a newer version
- FIPS 140-2, which is also considered as outdated, should be replaced by FIPS 140-3.