EMV Book2:

La partie 2 des specs EMV explique les mécanismes d'authentification possibles pour authentifier la carte et/ou l'emetteur. Elle décrit également les mécanismes permettant de sécuriser les échanges entre le lecteur et la carte. Et enfin, elle discute de la politique de sécurité que les systèmes de paiement membres de EMVco (ex : Visa, Master card,..) doivent suivre pour gérer le cycle de vie des clés de l'autorité de certification (I.e : c'est à dire l'entité logique ou physique, au sein du système de paiement; qui s'occupe des certificats et de génération de clés pour les banques)

Mécanismes d'authentification:

1- Static Data Authentication : Elle se déroule suivant les étapes suivantes :

0 – IC card envoie CA index + Signed Static Data+ Issuer PK certificate.
1- Terminal retrouve la CA PK certificate en se basant sur le RID de l'application et le CA index.
2- Terminal vérifie la Issuer PK certificate en utilisant la CA PK certificate.
3- Si 2 est OK. Le terminal vérifie la Signed Static Data en utilisant la Issuer PK certificate.
4- Si 3 est OK. Mettre le 'Data Authentication Code' dans le tag 9745.

*Il est important de noter que l'algorithme de signature/vérification est spécifique aux specs EMV (il faut suivre le Book2, pour savoir comment il faut signer/vérifier les données)
*La Signed Static Data sont des données statiques (AFL et AIP) signées avec la clé privée de l'Issuer et mis dans la carte en même temps que la Issuer PK certificate (à la phase de personnalisation de la carte ?)
*Le terminal peut stocker jusqu'à 6 CA par RID.
* Le CA index permet au terminal de trouver dans sa table interne, en fonction du RID, le CA qu'il faut utiliser , et l'algorithme qu'il faut utiliser avec ce CA.
*La Static Data Authentication fait intervenir la PK de l'issuer et de la CA seulement; elle permet donc une authentification de l'emetteur et une vérification de l'intégrité des données embarquées sur la carte.

2-Dynamic Data Authentication : Elle se déroule suivant les étapes suivantes :

0- IC card envoie CA index + Issuer PK certificate + ICC PK certificate + 'Static Data to be authenticated (AFL et AIP)'.
1- Terminal vérifie la Issuer PK certificate en utilisant la CA PK certificate.
2- Terminal vérifie la ICC PK certificate en utilisant la Issuer PK certificate.
3- Si 1 et 2 sont ok. Le terminal envoie la commande 'Internal Authenticate' avec le DDOL
4-Le DDOL en plus d'un nombre généré aléatoirement (ICC unpredictable number) par la carte représente principalement (il y a d'autres informations) les données dynamiques que la carte signera avec la ICC private key pour obtenir la 'Signed Dynamic Data'.
5- Terminal vérifie la Signed Dynamic Data avec la ICC PK certificate.
6- Si 5 est ok, mettre le ICC unpredictable number dans le tag '9F4C'

* Le DDOL est obligatoire. Soit il est envoyé par le lecteur, soit c'est celui qui existe par défaut (mais optionnellement) dans la carte qui est utilisé.
* La Dynamic Data Authentication fait intervenir la CA PK certificate, la Issuer PK certificate et la ICC PK certificate et des données statiques inclues dans le certificat de la ICC. Donc cette authentification permet l'authentification de l'emetteur et de la carte, et la vérification de l'intégrité des données stockées dans la carte.

3-Combined Data Authentication : La CDA consiste à demander une signature CDA à la carte dans la commande Generate Application Cryptogram envoyée par le terminal au cours d'une transaction bancaire. La vérification de la signature est faite une fois la réponse à la commande generate AC est reçue. Elle se déroule suivant les étapes suivantes :

0- Le terminal décide de l'action à prendre pour la transaction en cours; il choisit quel type de cryptograme il va demander à la carte : AAC, TC ou ARQC.
1- Si le type est un AAC, il doit envoyer la commande sans demander une signature CDA.
2- Si le type est un TC, il doit envoyer la commande avec une demande de signature CDA.
3- Si le type est un ARQC, il peut envoyer la commande avec ou sans une demande de signature CDA.
4- La carte doit répondre en envoyant le cryptogramme (TC ou ARQC ou AAC). Si le cryptogramme est TC ou ARQC et que la signature CDA était demandée, elle envoie en plus du cryptogramme la signature CDA. Cette signature est le résultat de la signature de données dynamiques (nombre aléatoire générée par la carte + PDOL +CDOL+..d'autres infos) avec la clé privée de la carte. (Les flowcharts pg 78,79,80 expliquent en détail les différents cas possibles en fonction de la commande Generate AC envoyée par le lecteur et la réponse générée par la carte)

5- Terminal vérifie la signature CDA en utilisant la ICC PK certificate.
6 – Si 5 est ok, mettre le ICC dynamic number dans le tag 9F4C et le cryptogramme dans 9F26

Le secure messaging :

Il permet d'assurer la sécurité (confidentialité, intégrité et authentification) des échanges entre le lecteur et la carte.

Commande unsecure : CLA INS P1 P2 L DATA (CLA = X0)
Commande Secure : CLA INS P1 P2 L DATA' (CLA = XC)

Pour assurer la confidentialité des échanges, chiffrer les données (DATA) et les mettre dans DATA' sous la forme TLV où V est les données chiffrées. Et T égale à 86 ou 87, en utilisant une clé dérivée d'une clé maitre propre à la ICC et résérvée pour le chiffrement.

Pour assurer l'intégrité des échanges, calculer le MAC et le mettre dans le champ DATA' sous la forme TLV : 81 L DATA 8E L(MAC) MAC, en utilisant une clé dérivée d'une clé maitre (propre à la ICC et résérvée pour le calcul du MAC).

Pour assurer l'intégrité et la confidentialité des échanges, chiffrer les données (DATA) et calculer le MAC, mettre le champ TLV : 87 L 01 || enciphered data field 8E L(MAC) MAC dans DATA'.

L'annexe D2 donne un exemple de chaque cas d'utilisation (chiffrement, MAC, chiffrement+MAC)

Le chiffrement de PIN:

0 – La carte envoie le CA index, la Issuer PK certificate, la ICC PIN Enciphrement PK certifciate.
1- Le terminal vérifie la Issuer PK certificate en utilisant la CA PK certificate.
2- Le terminal vérifie la ICC PIN Enciphrement PK certifciate en utilisant la Issuer PK certificate.
3- Le terminal chiffre le PIN + ICC unpredictable number + Random Padding (généré par le terminal) en utilisant la ICC PIN Enciphrement PK.
4- La carte vérifie le PIN en déchiffrant ce que le terminal lui a envoyé (en utilisant la ICC PIN Enciphrement private key), et en le comprant avec le PIN stockée sur la carte.

La politique de sécurité :

Elle décrit les règles de sécurité que les systèmes de paiement doivent respecter durant le cycle de vie des certificats de l'autorité de certification:

La CA a principalement deux rôles : Il est embarqué dans le terminal pour lui permettre de vérifier l'identité de l'émetteur de la carte. Et il est utilisé par les émetteurs de cartes (les banques) pour signer leur clés publiques qu'ils vont embarquer sur les cartes bancaires de ses clients.

Le cycle de vie d'un certificat:

1-Planning
2-Génération de clé.
3-Distribution de certificats
3-Utilisation des certificats.
4-Révocation