EMV3:
Le EMV Book3 est divisé en deux parties principales: dans la première partie, on trouve la description (format de la commande, format de la réponse) des commandes utilisées après la selection d'une application, la deuxième partie décrit les différentes phases d'une transaction bancaire qui suivent la sélection de l'application bancaire:

1- Get Processing Data Options qui indique le début d'une nouvelle transaction (Initialisation de l'application). La réponse à cette commande contient l'AIP et l'AFL. L'AIP indique les fonctions supportées (SDA, CDA, ou DDA, cardholder verification,..) par la carte. L'AFL référence les fichiers dont le contenu est utilisé pour réaliser la transaction. Il indique également, pour chaque fichier, le nombre de records impliqué dans la 'offline data authentication'.
2- Read Application : Le terminal doit lire tous les enregistrements des fichiers en utilisant la commande Read record, et les garder en interne pour les utiliser dans les phases suivantes.
3- Offline data authentication : SDA (assurer l'intégrité des données (AFL ou AIP) sur la carte) ou DDA (assurer l'intégrité des données sur la carte, authentifier en offline la carte (à condition que la clé privée de la carte reste confidentielle; impossible à un attaquant de la récupérer) ou CDA(pareil que DDA) EMV Book2). Cet étape a pour effet la mise à jour des bits de TVR (Terminal Verification Results) et TSI (Terminal Status Information). Le TSI indique les vérifications qui ont été menées par le terminal, et le TVR indique les résultats de ces vérifications.
4- Processing restrictions : Le terminal vérifie la version de l'application sur la carte (elle doit avoir la même version que celle sur le terminal (par exemple MasterCard 2.0)), le terminal vérifie qu'il n 'y a pas de restrictions sur l'usage de l'application (pays, type de terminal,..), et le terminal vérifie que la date courante < la date d'expiration de l'application et > à la date effective de la mise en route de l'application. A l'issue de cette étape, le terminal doit mettre à jour le TVR.
5- Terminal Risk Managment : inclut 1) Floor limit : la valeur de la transaction (par carte bancaire) ne doit pas dépasser une certaine valeur limite définie par le commercant, 2) Random Transaction Selection: une transaction peut être sélectionnée pour passer en ligne même si il est encore possible de passer des transactions offline avec la carte. 3) Velocity check : la différence entre l'ATC et le 'Last online ATC register' (ATC value of the last transaction that went online) doit être inférieure à 'Lower consecutive transaction offline limit' et inférieur à 'Upper consecutive transaction offline limit'. A l'issue de cet étape, le terminal doit mettre à jour les bits de TVR et TSI.
6- Cardholder verification : permet d'authentifier le porteur de la carte. Le Cardholder verification method List permet au terminal de savoir la méthode qu'il faut appliquer avec la carte insérée pour authentifier le porteur (PIN (plain), PIN (enciphered), signature, ..). A l'issue de cet étape, le terminal doit mettre à jour les bits de TVR et TSI.
7- Terminal Action Analysis : Le terminal maintient 3 data objects qui s'appellent Terminal Action code- Denial, Terminal Action code- Online, Terminal Action code- Default. D'autre part, la carte maintient 3 data objects qui s'appellent Card Action code- Denial, Card Action code- Online, Card Action code- Default. Pour décider de l'action à prendre (Denial, Online, offline) le terminal fait comme suit (dans l'ordre):
* Terminal Action code- Denial (xor) TVR = R1 et Card Action code- Denial (xor) TVR = R2 : Si R1 ou R2 contient un 0, et que le bit correspondant dans TVR et Terminal (ou Card) Action code- Denial est égale à 1. L'action est donc un rejet de la transaction. Le terminal demande donc un AAC dans la commande Generate AC.
* Terminal Action code- Online (xor) TVR = R1 et Card Action code- online (xor) TVR = R2 : Si R1 ou R2 contient un 0, et que le bit correspondant dans TVR et Terminal (ou Card) Action code- online est égale à 1. L'action est donc de continer la transaction en ligne. Le terminal donc demande un ARQC dans la commande Generate AC.
*Terminal Action code- Default(xor) TVR = R1 et Card Action code- Default (xor) TVR = R2 : Si R1 ou R2 contient un 0, et que le bit correspondant dans TVR et Terminal (ou Card) Action code- Default est égale à 1. L'action est donc de demander à la carte un AAC dans la commande Generate AC. Sinon, le terminal demande un TC dans la commande Generate AC. Ce test est fait pour les terminaux qui supportent des transactions offline et online. Pour les terminaux on-line seulement, si la transaction n'est pas traité en ligne (pour une raison quelconque), le terminal envoie une demande AAC dans la commande Generate AC.
8- Card Action Analysis :
* Si le terminal a demandé un AAC, la carte répond par un AAC
* Si le terminal a demandé un TC, la carte répond par un TC ou AAC.
* Si le terminal a demandé un ARQC, la carte répond par un AAC ou ARQC.

Quand la carte répond par un ARQC, le terminal se connecte à l'issuer (la banque) pour continuer la transaction en lui envoyant le ARQC générée par la carte. Ce ARQC (AAC et TC aussi) est un MACs calculés sur des données générées par la carte et par le terminal en utilsant une clé symétrique (connue par l'issuer et la carte seulement). La banque, à la réception de la demande de terminal, vérifie le ARQC (ce qui constitue en quelque sorte une authentificaion en ligne de la carte si la vérification est ok bien sur). Et calcule le ARPC qui n'est d'autre que le chiffrement de l'ARQC xor Authorisation Response code. La banque envoie le ARPC au terminal dans le 'issuer Authentication data'.[Le terminal peut envoyer (si la carte supporte cette fonctionnalité) le 'issuer Authentication data' à la carte en utilisant le external authentication (qui permet donc de faire une 'issuer authentication';une authentification de la banque), la carte déchiffre le ARPC, vérifie le ARQC. Si elle envoie SW = 9000, c'est que l'authentification de la banque a réussit]. Le terminal envoie ensuite une 2ème Generate AC en demandant un TC ou un AAC. La carte déchiffre le ARPC, vérifie le ARQC, regarde le Authorisation response code envoyé par la banque, et renvoie au terminal un TC (la transaction approuvée par l'issuer) ou un AAC (transaction rejetée par l'issuer).

9-Transaction terminée. La banque peut envoyer des scripts dans le 'Authorisation response message' à exécuter sur la carte après le premier Generate AC et\ou le deuxième Generate AC.
Le commercant envoie un batch de transactions approuvées à sa banque (batching) chaque fin de journée. La banque du commercant contacte la banque de l'issuer: Le compte du cardholder est donc débité et la banque du commercant est crédité (clearing and settlement). Et ensuite, le compte de commercant est crédité par sa banque (fundings).