



OmniScripting

Une étape importante dans l'univers des puces de cartes

Le centre de compétences dédié aux puces de SIX a réussi à développer une fonction supplémentaire pour la puce EMV120: l'OmniScripting. Les émetteurs de cartes de débit obtiennent ainsi une plus grande flexibilité pour les configurations ultérieures de la puce de carte.

Le cycle de vie d'une carte à puce se limite généralement à trois ans. Elle est ensuite remplacée par une nouvelle. Le défi pour la banque émettrice de la carte consiste à définir au préalable l'étendue des fonctions de base de la puce pour le cycle de vie. Les modifications ultérieures, à savoir la configuration de la puce, ne sont possibles que partiellement avec un scripting standard de l'émetteur.

Scripts d'émetteurs: restriction de la taille maximale des données

La norme technique EMV établie et applicable à l'échelle internationale pour les paiements par carte d'EMVCo (BOX) prévoit certes des scripts dits d'émetteurs pour les modifications ultérieures de la configuration de la puce, mais elle les limite à une taille maximale de données d'environ 100 octets pour une transaction par carte.

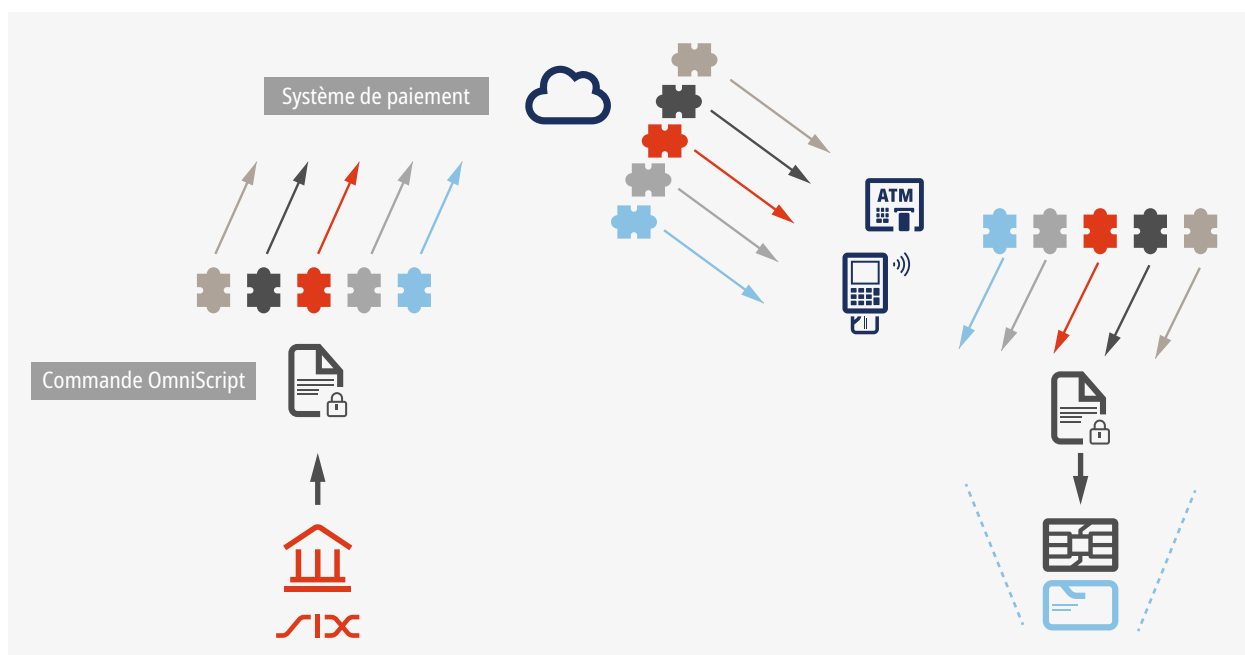
Pour que les certificats numériques sur les cartes puissent être renouvelés, les longueurs dites de clé pour les clés RSA requises doivent être, conformément aux exigences de sécurité applicables, nettement plus longues que la restriction de 100 octets.

Or, cette restriction ne s'applique pas seulement aux certificats de cartes eux-mêmes. Les données de cartes déterminantes en matière de sécurité doivent être signées par ces certificats, et donc protégées d'un point de vue cryptographique. Ainsi, toute modification nécessite impérativement une modification du certificat y afférent. Par conséquent, les données essentielles des cartes ne peuvent pas être modifiées avec les scripts standard d'émetteurs.

OmniScripting offre la solution

Grâce à la fonction OmniScripting, SIX a maintenant introduit de nouvelles commandes de scripts qui satisfont à toutes les exigences de la norme EMV. En conséquence, ces commandes OmniScript sont également transmises comme des commandes standard de scripts depuis l'hôte émetteur de SIX avec la puce EMV120.

Le fonctionnement de l'OmniScripting



Une seule commande OmniScript ne contient toujours qu'une partie des données à modifier sur la puce. Chaque commande OmniScript supplémentaire contient d'autres parties de la modification que la puce assemble dans la mémoire interne. La modification n'est exécutée que lorsque l'intégralité des informations nécessaires sont disponibles.

L'ensemble du processus est sécurisé par voie cryptographique et ne peut être effectué avec succès que par l'hôte émetteur de SIX. Cette nouvelle procédure permet de répartir la transmission des données sur plusieurs transactions par carte. Cette opération peut avoir lieu dans le monde entier pour chaque transaction au terminal du point de vente ou au DAB en arrière-plan, et ce, sans ajustement nécessaire de la part du titulaire de carte.



Avantages pour les émetteurs de cartes de débit

Grâce à l'OmniScripting, d'importantes modifications peuvent être apportées aux cartes qui sont déjà en cours d'utilisation. La flexibilité des banques s'en trouve accrue. En outre, les frais qui seraient occasionnés dans le cas d'un remplacement non prévu des cartes peuvent être réduits.

Les configurations après l'émission de la carte sont variées. Une fonctionnalité peut par exemple y être ajoutée, comme la prise en charge des paiements sans contact aux bancomats (DAB). Ou alors un problème technique survient, concernant par exemple la validité d'un certificat qui ne coïncide pas avec la date d'expiration de la carte. Avec la fonction OmniScripting, le certificat peut être remplacé et la carte conservée.

EMVCo est l'organisme technique mondial qui facilite l'interopérabilité et l'acceptation des transactions de paiement sécurisées dans le monde entier en gérant et en faisant évoluer les spécifications EMV®. (EMVCo: <https://www.emvco.com/about/overview/>)