LEARNING NUGGET
#2

Tokenisation pour les cartes de débit

La protection de données de cartes sensibles et la clé pour les paiements par porte-monnaie mobile

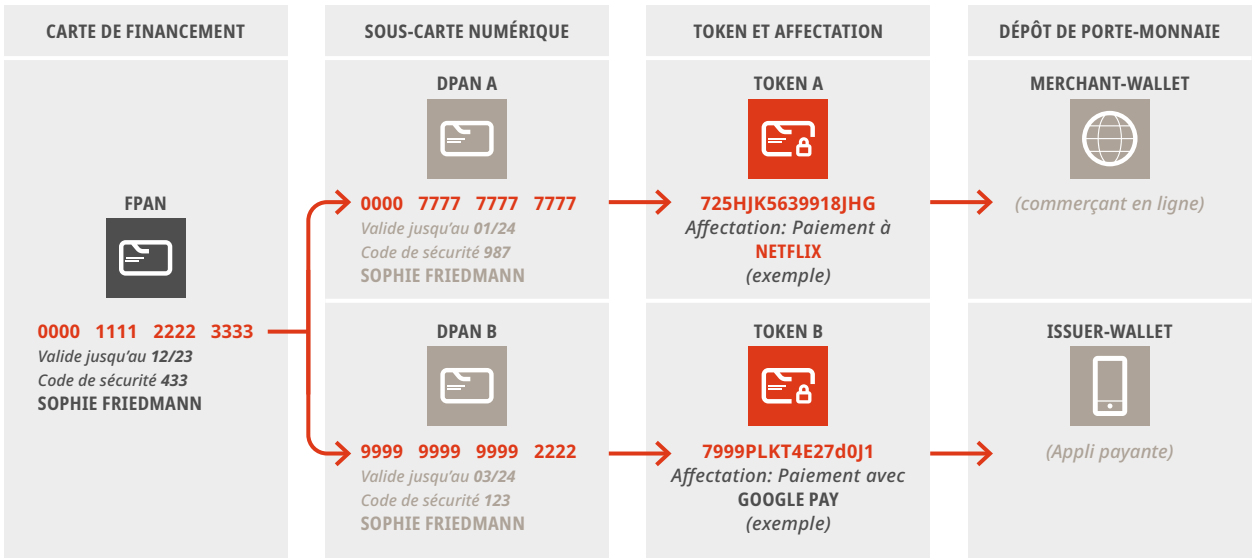
Introduction à la tokenisation de cartes de débit

Le token en tant que «code secret» pour la protection d'informations de cartes sensibles

En ce qui concerne les données sensibles, notre besoin de sécurité est très élevé. Une protection s'impose pour prévenir le vol de données et les abus, notamment lorsque plusieurs systèmes échangent des informations de cartes sensibles par l'intermédiaire d'un réseau qui nous est inconnu.

Le mécanisme de la tokenisation offre une solution optimale pour le traitement de paiements. Que ce soit aux points de vente (POS) via les «applis payantes» ou lors d'achats en ligne, nos données de carte sont enregistrées sur nos dispositifs intelligents et sur les sites Web de commerçants en ligne, et transférées par des systèmes encore différents au traitement de paiements. Si nos informations de carte sensibles venaient à être interceptées ou volées de manière délibérée, notre compte serait «sans protection» et les fraudeurs auraient accès à nos économies. Cela peut néanmoins être évité si les informations de carte sont cryptées dès le départ par une sorte de «code secret»: c'est exactement ce que fait un «token»!

Notre carte de débit et ses tokens



Dans le cas de la tokenisation, la carte de financement est tout d'abord remplacée par une sous-carte numérique: le numéro du compte principal connu de la carte de financement (FPAN) est remplacé par un numéro PAN (DPAN) numérique. Celui-ci est ensuite crypté ensemble avec sa nouvelle date d'expiration et son code de sécurité sous forme de token. La référence entre les deux «PAN» est documentée dans le service de tokenisation de la banque et auprès du Token Service Provider (TSP; systèmes). Le décryptage du token, en revanche, ne peut être effectué que par le TSP.

La numérisation et le cryptage de la carte de financement en un token ne sont, en eux-mêmes, pas encore suffisamment sûrs. En effet: bien que d'autres informations de carte soient désormais utilisées, celles-ci pourraient néanmoins aussi faire l'objet de fraudes. Le degré de sécurité supplémentaire souhaité est atteint lorsque le token est affecté à un but précis. Une carte de débit peut par conséquent avoir un nombre quelconque de tokens et DPAN. Ces sous-cartes numériques sous forme de tokens sont soumises aux mêmes règles de cycle de vie que la carte de financement; elles sont, par exemple, valables trois ans à compter de la date d'émission ou nécessitent une image numérique.

Utilisation des tokens pour carte de débit – Paiements par porte-monnaie et achats en ligne

En tant que titulaires de carte, nous avons deux possibilités différentes d'utiliser les tokens: auprès des *Merchant-Wallets*, où les tokens sont déposés aux fins des transactions en ligne et les *Issuer-Wallets,* où les tokens peuvent être utilisés dans une appli payante pour les transactions effectuées sur un appareil intelligent.

Merchant-Wallets

Souvent, la «tokenisation merchant» n'est pas visible pour nous car les processus correspondants sont exécutés en arrière-plan. Pour nous, en tant que titulaires de carte, l'expérience montre que cela ne fait aucune différence que la transaction en question soit une «transaction Card-on-File» normale (le commerçant enregistre les données de carte) ou une «transaction basée sur un token» (le commerçant n'enregistre que le token). Pour les commerçants en ligne, par contre, la tokenisation présente des avantages évidents; sans tokens, les données de carte sensibles doivent être protégées par des normes de sécurité complexes et chères, telles que PCI-DSS. Par l'utilisation de tokens, ces mesures de protection peuvent être réduites. Pour illustrer cela: le commerçant en ligne crée chez lui un porte-monnaie pour le client, le «Merchant-Wallet», et dépose le token correspondant.

Tokenisation de l'émetteur

La seconde possibilité d'utilisation des tokens, et certainement la plus connue, est la «tokenisation de l'émetteur», également connue sous le nom de «Mobile Payment Wallets» ou «applis payantes». Le token est dans ce cas enregistré dans une appli payante qui est installée sur notre appareil intelligent. Il peut ainsi être utilisé comme moyen de paiement récurrent. Apple Pay, Samsung Pay ou Google Pay comptent parmi les applis payantes les plus connues. Les «Small Pay», tel que Fitbit, Garmin ou Swatch offrent également une fonction de paiement sur leurs appareils et tombent dans cette catégorie. Sous cette forme de la tokenisation, on entend également des applis payantes propres des banques, des fournisseurs de logiciels ou des commerçants.

Contrairement à la tokenisation merchant, l'affectation n'est pas liée à un commerçant particulier, mais à l'appli payante et à l'appareil intelligent correspondant. Le fournisseur de l'appli payante est tenu de garantir préalablement l'authentification du titulaire de carte.

Technologies de porte-monnaies (wallets) différentes dans les applis payantes

On distingue deux technologies différentes dans les porte-monnaies des applis payantes*: les HCE-Wallets basés sur le cloud* et les *SE-Wallets enregistrés localement sur les appareils intelligents*.

HCE-Wallets basés sur le cloud

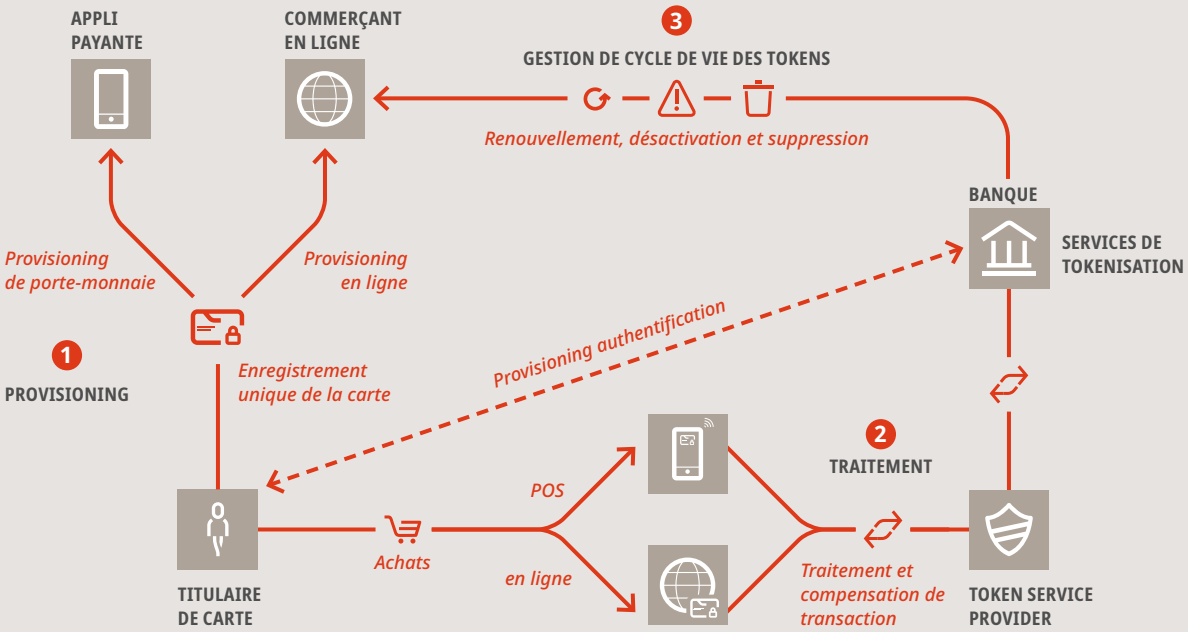
S'agissant de l'approche «Host Card Emulation» (HCE), le porte-monnaie ainsi que le token se trouvent dans un cloud sécurisé du fournisseur et nécessitent une connexion Internet. Pour que cela fonctionne aussi hors ligne, des «sous-clés» individuelles qui sont régulièrement renouvelées sont mises à disposition des applis payantes. Ceci est comparable à un carnet de coupons qui est remplacé dès que tous les coupons ont été utilisés. Cette technologie est souvent utilisée pour les solutions propres aux banques ou par les fournisseurs de porte-monnaies indépendants du système d'exploitation. Un exemple bien connu est Google Pay.

SE-Wallets enregistrés sur les appareils intelligents

La contrepartie de la technologie basée sur le cloud est le porte-monnaie intégré aux appareils intelligents. On parle alors de «Secure-Element» (SE), c'est-à-dire que le porte-monnaie et le token se trouvent dans une mémoire sécurisée de l'appareil intelligent. En conséquence, cette approche n'a nullement besoin d'une connexion Internet et est disponible à tout moment, également hors ligne Cette technologie est souvent utilisée dans le cas des applis payantes qui sont installées sur le matériel et le système d'exploitation du même fournisseur, par exemple Samsung Pay et Apple Pay.

Tokenisation dans le détail

Aperçu du paysage de la tokenisation
Pour que le mécanisme de protection puisse être appliqué pour nos cartes de débit, plusieurs parties, services et déroulements correspondants sont nécessaires.



1 Provisioning: enregistrement d'informations de carte

Le provisioning est la première étape de la tokenisation. Le «Provisioning» signifie que les détails de carte sont fournis et enregistrés dans un porte-monnaie de commerçant en ligne (provisioning en ligne) ou une appli payante (provisioning de porte-monnaie).

Les deux types de provisioning font l'objet d'une vérification de la demande, ce qu'on appelle la «token request». D'une part, l'intégrité du demandeur et d'autre part l'autorisation du titulaire de carte est vérifiée.

Dans le cas du provisioning en ligne, la vérification est garantie par le service de tokenisation de la banque au niveau des cartes et des titulaires de carte. Cette pratique permet une expérience utilisateur sans interruption.

Dans le cas du provisioning de porte-monnaie, une complexité supplémentaire s'ajoute: le titulaire de carte doit être authentifié pendant la vérification de la demande par la banque. L'étape d'authentification nécessaire dépend du canal d'entrée du titulaire de carte:

- **Provisioning commandé par l'appli:** le titulaire de carte part de l'appli de la banque qui transfère les informations de carte au porte-monnaie aux fins du provisioning. L'authentification a déjà eu lieu en amont et n'est donc plus nécessaire. Selon les fournisseurs, cette procédure est appelée «Push-Provisioning» ou «In-App-Provisioning».
- **Provisioning manuel:** le titulaire de carte part directement du porte-monnaie et saisit manuellement les informations de carte. Du point de vue de la banque, il s'agit ici d'un environnement non authentifié. L'authentification a été effectuée seulement par l'appareil intelligent, ce qui, potentiellement, ne suffit pas à la banque. Par conséquent, une authentification supplémentaire du titulaire de carte doit être effectuée.

Authentification supplémentaire du titulaire de carte dans le provisioning manuel

FLUX VERT

Authentification de l'appareil intelligent suffisante. Token-Request autorisée.

FLUX JAUNE

Authentification du titulaire de carte par un canal vérifié nécessaire.

FLUX ROUGE

Token-Request refusée et un token ne peut pas être établi.

L'authentification supplémentaire du titulaire de carte du flux jaune peut avoir lieu par différents canaux, par exemple:

- OTP: code d'authentification unique par SMS ou e-mail
- Authentification centre d'appel
- Authentification par appli: le titulaire de carte peut s'authentifier via une appli de manière analogue à la procédure 3D Secure.
- Authentification SIM

2 Traitement:

traitement des transactions basé sur un token

Les transactions basées sur un token suivent elles aussi les étapes de traitement qui nous sont connues. Elles sont autorisées au niveau FPAN, mais en plus, des informations supplémentaires, telles que le DPAN correspondant et l'affectation, sont transférées simultanément. Contrairement aux autorisations classiques, certaines vérifications n'ont pas lieu, car elles ont d'ores et déjà été effectuées en amont lors du décryptage du token par le TSP. Ceci garantit que la transaction peut être affectée à la carte adéquate et il est clair qu'il s'agit d'une transaction basée sur un token.

3 Gestion de cycle de vie des tokens:

gestion des tokens

D'une manière générale, la gestion du cycle de vie des tokens contient les mêmes éléments que la gestion du cycle de vie des cartes normales. Néanmoins, cette forme est légèrement plus complexe, car il faut tenir compte du lien à la carte de financement; cela signifie que les événements de cycle de vie de la sous-carte numérique sont toujours en liaison avec la carte de financement. Ceci peut parfaitement être illustré par la validité d'un token; la carte de financement et le token ont tous deux une validité de trois ans à compter de la date d'émission. Ils ne sont très probablement pas établis à la même date et n'ont pas de dates d'expiration identiques. Il est par conséquent important de définir par ces événements de cycle de vie quel est le comportement mutuel de ces données. Il en va de même pour le comportement d'un token dans le cas du blocage de la carte de financement.

SAVOIR PLUS

SIX BBS SA
Hardturmstrasse 201
Case postale
8021 Zurich
T +41 58 399 4012
pm.debit@six-group.com