IDEMIA

9 questions sur la tokenisation des paiements

PAIEMENT

POSTÉ LE 01.17.23

#1 Qu'est-ce que la tokenisation des paiements ?

La tokenisation consiste à remplacer des données sensibles par un élément équivalent qui n'a aucune valeur une fois sorti d'un écosystème donné. Cet élément est connu sous le nom de « token » (qu'on traduit parfois par « jeton » en français). Dans le cas d'un paiement, le token est **une valeur de substitution qui remplace le numéro de compte primaire** (*Primary Account Number* ou PAN en anglais). Pour un PAN donné, plusieurs tokens de paiement peuvent être associés à des canaux et des cas d'usages spécifiques et à des paramètres d'utilisation particuliers. EMVCo[1] a déployé un cadre technique (l'*EMV Payment Tokenization Specification – Technical Framework v2.0*) pour générer, utiliser et gérer les tokens de paiement de manière interopérable au sein de l'écosystème de paiement. L'EMVCo y a défini plusieurs rôles, à savoir le *Token Service Provider* (TSP), qu'on peut traduire par « fournisseur de services de tokens », l'émetteur de la carte, et le *Token Requestor*, qu'on peut traduire par « demandeur de tokens ».

#2 Quels sont les avantages de la tokenisation des paiements ?

En mettant les données les plus sensibles hors de portée des fraudeurs et en associant des paramètres d'utilisation spécifiques à un token de paiement particulier, la tokenisation des paiements offre des avantages à toutes les parties prenantes du secteur des paiements. L'utilisation de tokens de paiement permet aux commerçants de réduire le risque de fuite des données et d'**augmenter les taux de validation des transactions**. Pour les émetteurs de cartes, le risque de fraude et les coûts de remplacement des cartes sont réduits. Enfin, les tokens de paiement créent des moyens plus sûrs de payer et réduisent l'impact pour les porteurs de cartes en cas de perte ou de vol de leur carte de paiement.

#3 Quels sont les cas d'usage de la tokenisation dans le domaine des paiements ?

La tokenisation peut être utilisée pour différents canaux et dans différents contextes de paiement, **qu'il s'agisse de paiements de proximité, de paiements dans une application mobile ou de paiements à distance**. Chaque token de paiement peut être associé à des paramètres spécifiques en fonction de l'usage.

Lorsqu'ils font des achats en magasin en utilisant un **portefeuille mobile** sur leur téléphone ou leur montre connectée, les consommateurs utilisent en fait un token de paiement et non les informations de leur carte pour payer. Cela peut se faire via Apple Pay, Google Pay, Samsung Pay ou même certains services « Issuers Pay » fournis par les banques qui permettent d'effectuer des paiements NFC depuis leur application bancaire Android.

Pour les **paiements en ligne ponctuels**, les tokens de paiement sous la forme d'une carte virtuelle affichée sur l'application mobile de la banque peuvent être récupérés et utilisés par le porteur de la carte pour sécuriser le paiement

sans créer de compte chez le commerçant. Les tokens de paiement peuvent également être utilisés pour sécuriser les transactions dans le cadre d'achats en ligne répétés et de **paiements récurrents** sur l'application ou le site web d'un même commerçant. L'expérience de paiement sur les sites marchands est également améliorée par les fournisseurs d'**options de paiement en un clic**, qui s'appuient eux-aussi sur la tokenisation des paiements.

#4 Qu'est-ce qu'un *Token Service Provider* (TSP) ?

Comme défini par EMVCo dans l'*EMV® Payment Tokenization Technical Framework*, le fournisseur de services de tokenisation (TSP) est chargé de générer, stocker, vérifier et gérer le cycle de vie d'un token de paiement. Il est également responsable de conserver la correspondance entre le PAN d'origine et le token de paiement dans un coffre-fort de tokens sécurisé (ou « *token vault* » en anglais) avec les paramètres d'utilisation associés. Le TSP est l'entité qui **fournit les tokens de paiement** à tous les demandeurs de tokens (*Token Requestors*) enregistrés pour les paiements de proximité, dans une application mobile et à distance **avec les paramètres d'utilisation associés**. Un TSP est généralement un réseau de paiement (international, domestique), un réseau privé (par exemple, les grands détaillants, les opérateurs de transport), un émetteur de cartes ou un fournisseur de services tiers.

#5 Qui sont les *Token Requestors* ?

Comme défini par EMVCo, un *Token Requestor* est l'entité qui initie le processus de tokenisation en demandant à un *Token Service Provider* de générer et de partager un token de paiement associé à un PAN donné. Les *Token Requestors*, qui fournissent l'interface avec le consommateur, peuvent être :

- **Des portefeuilles digitaux tiers** pour des paiements de proximité et dans une application (par exemple Apple Pay, Google Pay, Samsung Pay) ou pour des paiements en ligne (comme le Système SRC dans le cadre des options de paiement en un clic Click to Pay),
- **Des portefeuilles mobiles de banques émettrices** qui proposent des fonctions de paiement NFC sur leurs apps bancaires ou permettent d'afficher des numéros de cartes virtuelles pour sécuriser les paiements en ligne,
- **Des applications de messagerie** intégrant des fonctions de paiement par carte (WhatsApp, par exemple),
- **Des sites d'e-commerce** qui veulent sécuriser les cartes enregistrées chez eux et offrir des options de paiements récurrents.

#6 Comment fonctionne la tokenisation des paiements pour un paiement mobile sans contact ?

Tout commence par l'enregistrement de la carte. **Le porteur de la carte initie une demande d'enregistrement** de sa carte dans un portefeuille mobile et l'application envoie une demande au *Token Service Provider* associé pour enregistrer la carte. Le TSP est en charge du processus d'authentification du porteur de carte et demande à l'émetteur de la carte de vérifier **l'éligibilité de la carte et la légitimité du porteur**. Une fois cette étape d'authentification effectuée par l'émetteur, le TSP peut générer un token de paiement associé au PAN original et intégrer ce token de paiement dans le portefeuille mobile.

Lorsqu'il effectue un paiement mobile sans contact, le porteur de la carte tape son smartphone sur le terminal de paiement compatible NFC qui déclenche alors une demande d'autorisation de transaction intégrant le token de paiement. La banque acquéreuse du commerçant redirige la demande d'autorisation de transaction vers le réseau de paiement concerné, qui la redirige à son tour vers le TSP concerné. Le TSP procède à la **détokenisation** pour convertir le token de paiement et obtenir le PAN. Enfin, le *Token Service Provider* transfère la demande d'autorisation de transaction à l'émetteur avec le PAN original et les résultats des vérifications de sécurité. Tout cela se produit

instantanément et est **complètement transparent pour le consommateur**.

#7 Comment fonctionne la tokenisation des paiements pour le paiement avec une carte enregistrée chez un commerçant en ligne ?

Une fois encore, c'est le porteur de la carte qui initie l'enregistrement de la carte, mais dans ce cas, pour un commerçant en ligne bien précis. Le commerçant envoie ensuite une demande de tokenisation au Token Service Provider associé et ce dernier demande à l'émetteur de la carte de vérifier le statut de la carte et du compte. L'émetteur de la carte envoie ensuite une réponse positive, et **le TSP peut générer un token de paiement pour ce cas d'usage et ce marchand en particulier**, autrement dire en définissant les paramètres d'utilisation. Le token de paiement est ensuite stocké par le *Token Service Provider* dans son coffre-fort à tokens, ou il peut éventuellement être stocké par le commerçant lui-même (si le réseau de paiement dont dépend la carte l'autorise).

Lorsque le consommateur effectue un paiement en utilisant la carte précédemment enregistrée auprès d'un commerçant, la banque acquéreuse du commerçant **demande le token de paiement** au *Token Service Provider* (dans le cas où elle ne le stocke pas elle-même). La banque du commerçant partage alors les données nécessaires pour traiter la transaction, y compris le token de paiement, avec le réseau de paiement associé qui redirige la demande de paiement vers le TSP associé. Ensuite, le *Token Service Provider* procède à la **détokenisation** pour reconvertir le token de paiement en PAN et effectue des contrôles de vélocité supplémentaires, c'est-à-dire une analyse des données de la transaction. Enfin, le *Token Service Provider* transfère la demande d'autorisation de la transaction à l'émetteur avec le PAN original et les résultats des vérifications de sécurité. **En quelques secondes seulement, le paiement est effectué.**

#8 Pourquoi la tokenisation des paiements est-elle importante pour les réseaux de paiement ?

Il est crucial pour les réseaux de paiement internationaux, domestiques et privés d'utiliser la tokenisation s'ils veulent que les cartes émises sur leurs réseaux soient présentes et utilisées dans le monde digital. La tokenisation des paiements leur permet de prendre en charge les différents scénarios de paiements digitaux pour les transactions de proximité, dans une application mobile, en P2P (*peer-to-peer*) et à distance, et d'offrir aux porteurs de cartes davantage de moyens de paiement, de façon à ce que leur carte soit privilégiée par les consommateurs. En disposant de leur propre **plateforme de tokenisation** ils peuvent contrôler l'évolution technique de leurs services et ont l'autonomie indispensable pour proposer comme ils le souhaitent des expériences innovantes ou des parcours avant tout digitaux aux porteurs de cartes, tout en assurant la sécurité nécessaire à tous les acteurs de leurs écosystèmes respectifs (émetteurs, commerçants) dans le monde digital.

#9 Comment choisir un *Token Service Provider* ?

Les réseaux de paiement qui souhaitent avoir la liberté de gérer l'évolution technique de leurs services digitaux doivent choisir un fournisseur de technologie indépendant parmi les *Token Service Providers* tiers approuvés par EMVCo et répertoriés dans le programme d'enregistrement des *Token Service Providers* d'EMVCo[2]. Les principaux critères à prendre en compte pour faire leur choix sont les suivants :

- **L'étendue de la solution :** les services de tokenisation doivent être modulaires, très extensibles et omnicanaux afin de prendre en charge tous les principaux cas d'usage (paiements de proximité, dans une application mobile, en P2P, à distance) ;

- **Les capacités d'activation des services :** ils doivent privilégier un fournisseur qui expose des APIs faciles à intégrer, à la fois pour simplifier la collaboration avec les banques émettrices participantes et pour s'interfacer avec les Token Requestors ainsi qu'avec d'autres fournisseurs potentiels de coffres-forts de tokens ;
- **La sécurité de la solution :** il est primordial d'opter pour une solution qui répond aux normes de sécurité PCI, comme l'exigent la plupart des réseaux de paiement ;
- **L'expérience du fournisseur :** pour garantir un service fiable et pérenne, les réseaux internationaux, domestiques et privés doivent opter pour un fournisseur qui a l'expérience de déploiements majeurs et a l'habitude de gérer des services à grande échelle.

---

[1] https://www.emvco.com/about-us/overview-of-emvco/
[2] https://www.emvco.com/processes/token-service-provider-registration-programme-2/
