9 questions about payment tokenization

PAYMENT

POSTED ON 01.17.23

#1 What is payment tokenization?

Tokenization means replacing valuable data by an equivalent element that has no value once taken out of the system. This element is known as a token. Where payment is concerned, the token is a surrogate value that **replaces the Primary Account Number (PAN)**. For a given PAN, multiple payment tokens may be associated with specific channels and use cases and with specific usage parameters. EMVCo has deployed a technical framework (EMV Payment Tokenization Specification – Technical Framework v2.0) to generate, use and manage payment tokens in an interoperable way within the payment ecosystem. EMVCo defines several roles within the payment tokenization ecosystem, namely the Token Service Provider (TSP), the card issuer and the Token Requestor.

#2 What are the benefits of payment tokenization?

By putting the most valuable data beyond the reach of fraudsters and associating specific usage parameters with a given payment token, payment tokenization provides benefits to all payment industry stakeholders. Using payment tokens enables merchants to mitigate the threat of data breaches and **boost transaction approval rates**. Card issuers benefit from a reduced risk of both fraud and card replacement costs. For the cardholder, payment tokens **create more secure ways to pay** and **reduce the impact of a stolen or lost payment card**.

#3 What are the use cases of payment tokenization?

Payment tokenization can be used in different channels and for a variety of payment use cases, including **proximity, in-app and remote payments**. Each payment token can be associated with specific parameters[1] related to payment usage.

When shopping in stores using a **mobile wallet** on their phone or connected watch, customers actually use a payment token and not their card details to pay. This may be done via Apple Pay, Google Pay, Samsung Pay or even certain "Issuers Pay" services provided by banks that enable NFC payments via their Android banking app.

For **one-off online payments**, payment tokens in the form of a virtual card displayed on the bank's mobile app can be retrieved and used by the cardholder to secure guest checkout, i.e., without creating an account with this specific merchant. Payment tokens can also be used to secure **card-on-file transactions** in the context of repeat online purchases and recurring payments on the same merchant's app or website. Moreover, eCommerce payments are also enhanced by providers of **one-click payment options** which rely on payment tokenization.

#4 What is a Token Service Provider (TSP)?

As defined by EMVCo in the EMV® Payment Tokenization Technical Framework, the Token Service Provider is in charge of the generation, storage, verification and lifecycle management of a payment token. It is also responsible for maintaining the mapping between the original PAN and the payment token in a secure token vault along with its associated usage parameters. The TSP is the entity that **provides payment tokens** to any registered Token Requestors for proximity, in-app and remote payments **with associated usage parameters**. A TSP is typically a payment network (international, domestic), a private network (e.g. major retailers, transit operators), a card issuer, or a third-party service provider.

#5 Who are the Token Requestors?

As defined by EMVCo, a Token Requestor is the entity that initiates the tokenization process by requesting a Token Service Provider to generate and share a payment token associated with a given PAN. Token Requestors, which provide the consumer-facing interface, can include:

- **Third-party digital wallets** for proximity and in-app payments (e.g. Apple Pay, Google Pay, Samsung Pay) or for online payments (such as SRC Systems in the context of Click to Pay one-click payment options),
- **Card issuer's wallets** for banks willing to host NFC payment features on their banking apps or display virtual card numbers to secure online payments,
- **Messaging apps** with integrated card-based payment facilities (e.g. WhatsApp),
- **eCommerce merchants** willing to secure card-on-file and recurring payment options.

#6 How does payment tokenization work for a mobile contactless payment?

The process always starts with card enrollment. The **cardholder initiates a request** to register a card to a given mobile wallet and the wallet application sends a request to the associated Token Service Provider to enroll the card. The TSP is responsible for initiating the **cardholder authentication** process and requests the card issuer to verify the **card eligibility** and the cardholder's legitimacy. Once this authentication step is approved by the issuer, the TSP can generate a payment token associated with the initial PAN and integrate this payment token into the mobile wallet.

When making a mobile contactless payment, the cardholder taps the smartphone on the NFC-enabled POS device which initiates a transaction authorization request that incorporates the payment token. The merchant's acquiring bank redirects the transaction authorization request to the related payment network, which in turn redirects it to the related TSP. The TSP proceeds to **detokenization** to convert the payment token to the PAN. Finally, the Token Service Provider transfers the transaction authorization request to the issuer along with the initial PAN and **security check results**. All this happens instantaneously and is **seamless for the consumer**.

#7 How does payment tokenization work for merchant card-on-file payment?

Once again it starts with the cardholder initiating card enrollment, but in this case for a selected online merchant. The merchant then sends a tokenization request to the associated Token Service Provider and the latter requests the card issuer to verify the card and account status. Then the card issuer sends the approved response, and **the TSP can generate a payment token for this specific use case and merchant**—i.e. the usage parameters. The payment token is

then stored by the Token Service Provider on its token vault, or it can be stored by the merchant itself (if allowed by the card scheme).

When the consumer is making a payment using the card previously registered with a given merchant, the merchant's acquiring bank **requests the payment token** from the Token Service Provider—in the case where they do not store it themselves. Then the merchant's acquiring bank shares the payment payload—i.e. all the data necessary to process the transaction, including the payment token—with the associated payment network which will redirect the payment request to the associated TSP. Then, the Token Service Provider proceeds to **detokenization** to convert the payment token back to the PAN and performs additional velocity checks, i.e., an analysis of the transaction data. Finally, the Token Service Provider transfers the transaction authorization request to the issuer along with the initial PAN and security check results. **In just a few seconds, the payment is made.**

#8 Why does payment tokenization matter for payment networks?

It is crucial for international, domestic and private payment networks to use tokenization if they want the cards issued on their networks to be present and used in the digital world. Payment tokenization enables them to support the different digital payment scenarios for proximity, in-app, peer-to-peer (P2P) and remote payments and then offer cardholders more ways to pay, ensuring the card has a top-of-the-wallet position. Having their own **tokenization platform** enables them to control their digital roadmap and have the autonomy to propose disruptive experiences or digital-first journeys to cardholders as they wish, while providing security for their respective ecosystems (issuers, merchants) in the digital world.

#9 How to select a Token Service Provider?

Payment networks that want the freedom to **manage their digital services roadmap** should choose an independent technology provider from among third-party Token Service Providers approved by EMVCo and registered with the EMVCo Token Service Provider Registration Program[2]. The main criteria they should look at when making their choice are as follows:

- **The breadth of the solution:** the tokenization services should be modular, highly scalable and omni-channel in order to support all major payment use cases (proximity, in-app, P2P, remote payments);
- **Service enablement capabilities:** they should favor a provider that makes it easy to integrate APIs both to onboard participating issuers and to interface with Token Requestors as well as other potential token vault providers;
- **Security of the solution:** opting for a solution that meets PCI security standards, as required by most payment networks, is paramount;
- **Experience of the provider:** to ensure reliable and future-proof service, international, domestic and private networks should opt for a tokenization provider who is already involved in major deployments and large-scale operations.

---

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