» Industry Guide

MARQETA

All about tokenization

As more transactions move to digital, merchants, card issuers, and their processors are looking for ways to help reduce fraud associated with stolen card credentials, data breaches, and account takeovers. Tokenization of card details can help increase the security of digital transactions and has opened up payment use cases that provide added convenience for cardholders.

What is tokenization and how does it work?

In payments, card tokenization is the process of protecting sensitive data by replacing it with more secure, surrogate data, called a token. With tokenization, cards can be programmatically pushed to digital wallets such as Apple Pay, Google Pay, and Samsung Pay for convenient contactless payments, or stored with merchants for convenient payments online. When a tokenized card is used for payment, only the token is used, without exposing sensitive card details like a personal account number (PAN), making the payment more secure.

> *Tokenization of card details can help increase the security of digital transactions and has opened up payment use cases that provide added convenience for cardholders.*

Tokenization across payments

What types of tokenization exist?

Multiple types of tokenization exist within payments and vary depending on which parties in the payment ecosystem (merchants, acquirers, issuers, or card networks) are involved.

Security tokenization

Security tokenization (or acquirer tokenization) typically involves the acquirer processor using their own specified token format to tokenize cards of individual shoppers stored in a digital vault specific to that processor. This service helps the merchant protect sensitive data and meet payment card industry (PCI) requirements. These types of tokens can also be used to store credentials for future purchases, recurring payments, and one-click payments for quicker checkout experiences.

Network tokenization

Network tokenization (or payment tokenization) is a newer protocol developed by the EMVCo in 2014 and involves multiple parties to approve the token request. Unlike security tokenization, the token is interoperable and the PAN is protected at more points in the payments ecosystem vs. just at the merchant or acquiring side. Network tokenization involves the card network (or a partner of the network) acting as a token service provider to issue tokens to a token requestor (e.g., a digital wallet or merchant) that are approved by the card issuer. Network tokens can be more easily updated with new card information, as the protocol directly involves the card issuer and network, and like security tokenization it can help parties reduce PCI compliance burden. The majority of this guide is focused on network tokenization.

Tokenization for diverse use cases

What are the use cases for tokenization?

Digital wallets — Cards can be tokenized and enabled in popular digital and mobile wallets such as Apple Pay, Google Pay, and Samsung Pay.

Push provisioning (in-app) — A card can be automatically tokenized and pushed to a cardholder's wallet in their device from the card issuer's app. In this method, the wallet requests the token after the card issuer provides the necessary card data via a direct integration and initiates the "push."

Manual provisioning — In this method, the cardholder manually enters their card details into the wallet and the wallet initiates the token request.

Card-on-file provisioning — In this use case, the online merchant, typically through its acquirer processor or payment gateway, initiates a token request from the network after the cardholder inputs their card information for the first time. This "card on file" is useful for recurring payments and one-click checkouts.

What are some verticals that can benefit?

Digital banking — Cardholders can be onboarded quickly and have immediate access to start using their funds with a card provisioned into their digital wallet vs. waiting for a physical card.

On-demand services — Payment cards can be automatically pushed to a courier's wallet on their device so that they can start work immediately without having to wait for a physical card to arrive. The digital wallet also enables contactless payments, keeping the courier safe while shopping in-store or at a restaurant.

POS lending — Users can apply for a loan in-store using the POS lender's app and be immediately issued a card with funds to their digital wallet to pay the merchant. No integration with the merchant's POS is needed.

Expense management — New employees can start spending funds anywhere digital wallets are accepted even if they have not been issued a physical card.

Tokenization — the details

What are the benefits of network tokenization?

Enhanced Security — Tokenization protects sensitive data from being exposed. If a fraudster tries to intercept a transaction or hack a database, the tokens without a PAN can't be used to make fraudulent purchases, and therefore are less likely to result in fraud. And if a data breach occurs at a merchant, only that token needs to be replaced because tokens are merchant or device-specific.

Payment continuity — Tokens can also be used to enhance the cardholder experience. When an underlying card is lost, stolen, expired, or terminated, network tokens in devices or stored at merchants can be dynamically updated without requiring the cardholder to wait for a new card and re-enter their details. This is highly beneficial for payments where the cardholder is not always present, such as a monthly subscription. Similarly, when a device with a token is lost or stolen, the token can be disabled and the physical card will continue to work.

Increased authorizations — Knowing a card has been securely tokenized can give card issuers greater confidence to authorize transactions, and with dynamic token updates, card declines are reduced as card details are always kept up to date.

Who are the parties involved in network tokenization?

Token service provider — (e.g., the card network such as Visa or Mastercard) provides services for creating, storing, and managing tokens.

Card issuer — (e.g., the card issuing bank, card program provider, or Marqeta) issues the payment card from which the token is derived, and must approve each request to provision tokens for these cards. This approval process requires integration and certification with tokenization services at the token service provider.

Token requestor — (e.g., Apple Pay, Google Pay, or online merchant) requests and stores tokens for payment cards. Token requestors undergo certification in order to utilize network tokenization services, allowing them to request and make purchases with tokens.

Cardholder — owns the card that will be or has been tokenized. Cardholders provide their card data to the token requestor, which then contacts the token service provider and requests a token.

What is the process to tokenize a card in network tokenization?

1. First, the token requestor (e.g., a digital wallet or merchant) initiates the token request.
2. The token service provider (e.g., the card network) may send the request to the card issuer for validation.
3. If extra verification or step-up is required, the cardholder can be authenticated via a one-time password or other method.
4. Once completed, the token service provider approves the request and issues the token (that replaces the sensitive data) to the token requestor. The token is ready for use.

How is a network tokenization payment processed?

1. A payment with a token is initiated, such as a monthly subscription or a cardholder using thier digital wallet at a point of sale (POS).
2. The merchant sends the token to the acquirer processor who begins authorization by sending the token to the token service provider/card network.
3. The token service provider/card network then maps the token back to the original PAN and sends both to the card issuer to authorize the transaction as they normally would for a card payment.
4. The issuer then sends the authorization decision and token back to the card network.
5. The card network routes the decision back to the acquirer processor to complete the transaction.

Tokenization, PCI Compliance, and Encryption

How does tokenization work with PCI compliance?

Because tokenization replaces sensitive data, it can be used by parties within the payments ecosystem to help meet PCI compliance requirements. Although tokenization does not ensure PCI compliance, it can help reduce scope, especially for merchants who deal with sensitive cardholder data. Typically, the merchant's payment gateway or acquirer processor will store the sensitive data in a digital vault and provide tokens to the merchant. With network tokenization, the card network issues the token and can also help merchants meet PCI requirements.

How is tokenization different from encryption?

Both tokenization and encryption are methods to increase the security of sensitive data. Tokenization replaces sensitive data with new data — the token — and only the party who created the token can map the token back to the original data. Encryption, on the other hand, transforms or disguises the data using an algorithm. Encrypted data can be decrypted by any party that has the encryption key to obtain the original data.

The future of tokenization

What are recent developments in network tokenization?

Merchants, card networks, and card issuers are seeing the benefits of network tokenization across the payments ecosystem. One new payment method built on network tokenization is Secure Remote Commerce (SRC and branded as Click to Pay to consumers), and was recently introduced by the major card networks. SRC creates a guest checkout-like experience for cardholders on merchants' websites similar to "buy now" buttons that allow cardholders to store their payment details using tokenization.

Want to learn more? See Marqeta's digital wallet and tokenization solutions.

Looking to launch a digital wallet program? Talk to a Marqeta sales expert.

Ready to integrate? See the Marqeta developer guides.

MARQETA

About Marqeta

The global standard for modern card issuing, Marqeta powers modern payment solutions for companies, innovating new services and process flows in a digital world.

We enable modern payment solutions for:

- Instant card issuing of virtual, tokenized, and physical cards
- Real-time funding using our exclusive Just-in-Time (JIT) Funding feature
- Push provisioning to digital wallets and customizable webhooks
- Full program management resources and PCI compliance tools
- Actionable data insights, reporting, and advanced analytics tools with our DiVA API

Our platform, open API, and advanced analytics provide unprecedented control for companies to issue cards, authorize transactions, and manage payment operations with ease. Highly configurable, secure, and reliable, Marqeta built its technology from the ground up to help companies bring products to market faster, design seamless user experiences, streamline purchase flows, and reduce fraud risk.

www marqeta.com   f facebook.com/marqetainc   in linkedin.com/company/marqeta-inc   twitter.com/marqeta