Network Tokenization: securing, streamlining and transforming digital payments

EESTEL – A European Network of Experts in Digital Transactions

Network tokenization is establishing itself as a new standard in the payment ecosystem. Much more than a simple security tool, it is transforming the way card data is stored, updated and used, resulting in smoother customer journeys, improved authorization rates and a significant reduction in fraud.

Already widely deployed by Visa and Mastercard, and soon by the CB Economic Interest Group, it is becoming essential in the face of new regulatory obligations and network requirements. This blog looks at how it works, its benefits, its impact... and the strategic choices you need to make today.

As digital uses become more widespread, payment paths are becoming more diverse and intensive: online purchases, fractional payments, subscriptions, digital wallets, mobile applications, etc. Against this backdrop, securing payment data has become a priority for all players in the ecosystem: merchants, payment service providers, banks and, of course, the networks themselves.

Among the technological solutions deployed on a large scale, *network tokenization* is now emerging as a key development. More than just a cybersecurity tool, it is profoundly transforming the way card data is stored, transmitted and used in payment chains. It will enhance security, improve conversion rates and optimise the customer experience, while paving the way for new services.

But this technology is not neutral: it is reshaping the balance between the various players, raising questions of governance, as well as issues of sovereignty and interoperability. The aim of this blog is to decipher how network tokens work, their practical benefits, future obligations, and the points to watch out for if they are to be implemented properly.

Market challenges and player expectations

Increasingly complex payment paths

Payment is no longer just a one-off transaction between a customer and a merchant. It is now part of a continuous, omnichannel and personalized experience. The growth of e-commerce, subscription services, fractional payments (BNPL), wallets and mobile applications is placing greater demands on merchants and payment providers to offer payments that are smooth, fast and secure, whatever the channel, terminal or time.

This sophistication of payment paths creates new technical and regulatory constraints: management of customer consent, compliance with PCI DSS standards, updating of card data, support for deferred or recurring payments, strong authentication (SCA), etc.

The limitations of traditional approaches

Historically, merchants stored their bankcard numbers (PANs) in highly secure environments or used *PCI tokenisation* solutions provided by their technical acceptance providers (TAPs). These so-called "private" tokens made it possible to leave the PCI DSS perimeter while facilitating recurring or one-click payments.

But this approach has several limitations:

- PCI tokens are specific to each TAP, with no interoperability.
- The PAN remains in the payment flow, exposing a residual risk.
- Card data updates remain manual or limited, leading to payment failures.
- No contextual data is associated with the token, which limits value-added services.

In addition, *Merchant-Initiated Transactions* (MIT), which are widely used in subscription models, have a higher fraud rate than Customer Initiated Transactions (CIT), particularly when they are based on the PAN or PCI tokens.

High expectations on the part of merchants and issuers

Faced with these facts, merchants and service providers are looking for solutions that enable them to:

- **Secure card data** throughout its lifecycle.
- **Automate data updates** to avoid customer friction.
- **Increase authorization rates** through better recognition of transactions by issuers.
- **Simplify compliance** with PCI DSS requirements and authentication rules.
- **Enable enhanced services** such as Click-to-Pay, multi-device payment and intelligent management of payment identifiers.

On the network side, the aim is also to standardize the value chain, capture more transactional data, and strengthen their central role in the ecosystem.

Against this backdrop, network tokenisation is gradually emerging as the technical, commercial and regulatory answer to these multiple challenges.

How network tokens meet these challenges

What is a network token?

A *network token* is a unique identifier, generated and managed by a payment network (Visa, Mastercard, etc.), which replaces the bank card number (PAN) throughout the payment cycle. Unlike PCI tokens, which are issued locally by a technical service provider for restricted use, network tokens are recognized and can be used throughout the payment chain.

Each network token **is linked to the card-merchant pairing**, making it a value that cannot be used outside of that specific context. This principle greatly limits fraudulent use in the event of compromise and strengthens traceability.

Operation linked to the ecosystem

Network tokens are issued via centralized platforms such as :

- **Visa Token Service (VTS)**, including services such as VDCU (automatic update), CTF (Device Binding), Click-to-Pay, etc.
- **Mastercard Digital Enablement Service (MDES)**, with similar modules.
- Other networks are also starting to develop their own infrastructure, such as **GIE Cartes Bancaires**, with a CB token planned for 2025.

Tokens are used from the initial enrolment of the customer (CIT transaction) and can then be used to manage recurring or deferred payments (MIT) with maximum security and fluidity.

Benefits for payment players

For merchants:

- **Reduced fraud**: tokens cannot be used out of context.
- **Improved authorization rates**: issuers are better able to recognize the token and the associated history.
- **Automatic updates**: no loss of transactions when a card is renewed.
- **Smooth user experience (frictionless)**: one-click, recurring payment, omnichannel.
- **Activation of enhanced services**: Click-to-Pay, Device Binding, etc.

For issuers :

- **Consolidated monitoring of card usage** (via PAR - Payment Account Reference).
- **Enhanced security**: less PAN exposure.
- **Easier compliance with regulatory requirements** (SCA, PCI DSS).

For networks:

- **Standardization of the value chain**.
- **Enhanced ecosystem management** using tokens as anchor points.
- **Easier deployment of loyalty or contextual scoring services.**

Technological and strategic leverage

Behind its technical benefits, the network token is also a **major strategic tool for international networks**. By capturing the relationship between merchant and customer via a token that they control, Visa and Mastercard are strengthening their central role in the ecosystem, sometimes at the risk of limiting interoperability or restricting merchant choice (risk of "lock-in").

In addition, the mandates and penalties imposed by the networks are speeding up the transition to these tokens, making their de facto adoption inevitable in the coming months.

Maturity of the technology and examples of deployment

A technology already widely deployed

The major international networks have already industrialised tokenisation on a global scale:

- **Visa** offers its *Visa Token Service (VTS)* infrastructure, deployed in over 200 countries. It enables the activation of network tokens for e-commerce, wallets, recurring payments, virtual cards and more. Additional modules such as the *Visa Digital Credential Updater (VDCU)* automatically update card data.
- **Mastercard** has generalised the use of *Mastercard Digital Enablement Service (MDES*), integrating services such as *Secure Remote Commerce (SRC)* and *Token Connect* for simplified integration on the merchant side.

These platforms enable centralised governance of tokens, their distribution to authorised partners (wallets, PSPs, banks) and their immediate deactivation in the event of compromise.

Ongoing compliance mandates

The networks have not just made their services available - they are now enforcing their use.

- From **October 2024**, **Visa** will apply **penalties** to COF (Card-On-File) transactions without a token. From **July 2025**, Visa will refuse all recurring MIT transactions without a network token.

- **Mastercard** has already introduced a surcharge (+0.05%) on tokenless COF transactions and plans to **stop processing PANs completely** by **the end of 2025**.

These deadlines are tangible elements of the transition. They are forcing merchants and manufacturers to review their payment architecture, on pain of downgrading or transaction refusal.

Concrete use cases in the customer journey

Network tokenisation is already used in many cases:

- **Payments via Apple Pay, Google Pay, Samsung Pay**, which rely on network tokens for each device and each card.
- **Click-to-Pay**, which allows customers to identify themselves and pay in one click, via a secure token associated with their card.
- **Online subscriptions** (streaming, mobility, energy): tokenisation drastically reduces payment failures linked to card expiry or renewal.
- **Multi-channel retailers**: the use of a single token for all channels (web, mobile, shop) ensures a fluid, consistent experience.

A dynamic ecosystem, including local ones

In France, **GIE CB** has recognised the strategic importance of tokenisation and is developing its own **CB token**, which is expected to be rolled out in 2025. An initial service, **MDC - PAN Update**, is already active with French banks to reduce friction on COFs.

However, as long as CB tokens are not available, the use of tokens from international networks is **practically unavoidable** for e-commerce transactions and digital services based on MITs.

Conclusion

Network tokenisation is no longer a technological option: it is becoming an operational standard for all players in the payment ecosystem. It offers real benefits - security, fluidity, compliance - but requires a clear understanding of the technical and strategic implications.

Against a backdrop of imposed mandates, regulatory changes and concentration of players, businesses need to act now to anticipate developments, integrate network tokens into their payment architecture, and preserve their freedom of choice over the channels and networks used.

Contributors

- *Author : Arnaud Crouzet, Vice President, Consult Hyperion*
- *Reviewer : Pierre CREGO, CEO, Mercury Technologies*