

ain insights into the shift towards payment tokenization and digital cards, already surpassing physical cards in circulation. This paper aims to highlight the driving factors behind the market adoption, providing a comprehensive understanding of the functions and benefits that payment tokens bring to all the stakeholders of the payment ecosystem. Delve into the dynamic evolution of payment tokens as their influence extends to e-commerce beyond proximity payments. And explore why cardholders find value in payment tokens through the capability to configure their uses and the enhanced security features it brings.

# Contents

>	Introduction	4
1.	A no-brainer for digital payments	5
2.	A token you control	6
3.	Token migration from device to cloud	7
>	Conclusion	9

The use of payment tokens in the digital economy involves replacing sensitive card data with a non-sensitive string of numbers. A single card may be associated with different tokens. Each token is programmable for a specific usage, ensuring payment security and accelerating payment innovation. Consumers can now save their card on a mobile wallet or device, with online merchants for recurring and monthly subscription payments, or even in their vehicle for "in-car payments". One card, many tokens!



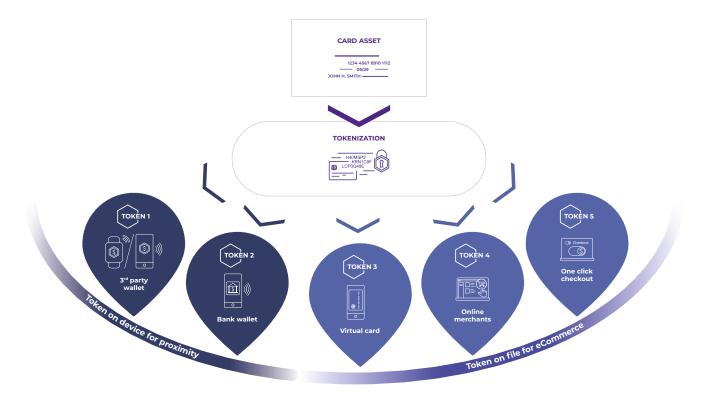
It's very likely that you've already experienced the ease of using payment tokens. If you've ever tapped your smartphone or connected watch on an NFC-enabled point-of-sale terminal, you are actually using a token to pay—not your actual card details. This seamless transaction is facilitated by third party digital wallets such as Apple Pay, Google Pay or Samsung Pay, or directly within your mobile banking app using its contactless payment features. Tokens may also be generated for virtual card purchases or to replace card-on-file for repeated and recurring transactions (which is the case for one-click payment option, for instance).



## A no-brainer for digital payments

e cannot consider the future of digital payments without discussing tokenization. With the rise of digital wallets and eCommerce, consumers are saving their payment card information across various websites and multiple devices, such as smartphones, tablets, and laptops. Building consumer trust in digital payment security is paramount and the boom in payment tokens is a great way to unlock new opportunities.

Tokenization is the process of replacing sensitive information with a token, i.e., non-sensitive data that has no value once taken out of the system. In payments, tokens can replace the card number so that payments can be processed without exposing Primary Account Number (PAN) details that could potentially be compromised. Payment tokens (also called network tokens) are generated and managed by payment networks and used for in-store mobile transactions, in-app purchases or online payments. In addition to improving security, payment tokenization also reduces friction in the payment process as consumers do not have to manually update card details stored with merchants if their physical card expires, is stolen or lost. Any updates are automatically pushed to that specific token via the issuing bank and the associated card network.



# A token you control

okenization is very secure because, if a payment token is compromised, the initial card details are still protected. **Usage restrictions** are also assigned to each token, which limits the risk even further. A token constraint restricts its use to a particular channel, merchant type, time slot, number of transactions or amount.



These constraints are configurable by the card issuer and the selection of usage parameters can also be presented to consumers, giving them more control over their "cards" (or "tokens"). For example, after enrolling a card on a digital wallet, a payment token is generated by the token service provider—usually a payment network—in accordance with specific constraints and following identity checks and stored on a specific device. If the consumer decides to activate the same card on their smartwatch, a dedicated payment token will be generated and associated with this new device.

Another example is a **virtual card number**. Some banks allow their cardholders to generate and display a virtual card on the mobile app for secure eCommerce transactions. Each virtual card may be set up for a specific intended use case and limited to a maximum number of transactions or an individual or cumulative amount. A consumer can also create a virtual card, restrict its use to a specific merchant (or category of merchants), configure it to be disposable or reusable, and set a time limit for its usage validity.

### Token migration from device to cloud

ayment card tokenization was initially designed by industry stakeholders to secure the first generation of mobile contactless payments. As previously mentioned, a unique token was associated with a specific device and securely stored on it. For each transaction, the same device token is used.

With the rise of eCommerce, consumers are saving their payment card information across a myriad of merchant sites, which need to heavily invest in security to store and protect these data and meet stringent PCI compliance requirements. With payment tokenization, once consumers register a card with a specific merchant, a unique token is generated by the associated payment network acting as a network token service provider. This network token is safely stored in the token service provider vault. Network tokenization removes sensitive payment data from the merchant's environment, **reducing the merchant's PCI scope**.

The next big thing in eCommerce is the rise of advanced one-click payment solutions such as **Click to Pay**, enabling consumers to auto-fill their checkout details and complete transactions in a single click. Payment tokenization is also an underlying security measure in Click to Pay. Instead of registering a card with each merchant, consumers enroll their card only once on this shared digital wallet in the cloud.





#### Conclusion

Payment tokens not only protect consumers and merchants, they also improve the overall payment experience. Tokens are now omnipresent and are even overtaking the number of physical cards in circulation. Tokens keep customer details safe and secure in case the card expires, is stolen or gets lost. Tokenization has become the best, most secure way to tackle a diverse range of in-store, in-app and web browser payment use cases.





