LEARNING NUGGET
#2

# Tokenization for Debit Cards

Protecting sensitive card data and the key to mobile wallet payments

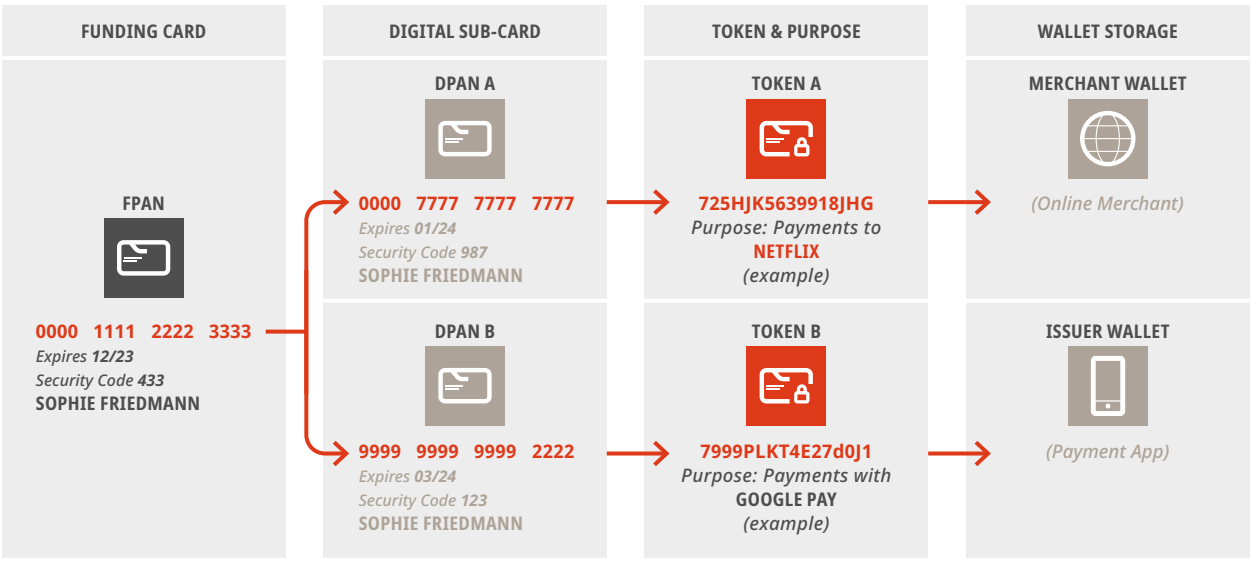
## An Introduction to Tokenization for Debit Cards

***A Token Is like a "Secret Code" That Is Used to Protect Sensitive Card Information***

Our security requirements are especially high where sensitive data is involved. Particularly in a scenario where multiple systems are involved in exchanging sensitive card information via an unknown network, this requires a form of protection to prevent data theft and misuse.

The tokenization mechanism gives us an ideal solution for processing payments. Whether at points of sale, through "payment apps" or when shopping online – our card data is stored on our smart devices and on the websites of online merchants and is forwarded via additional systems for payments processing. If our sensitive card information were to be intercepted or intentionally stolen, our account would be "unprotected" and the fraudsters would have access to our savings. This does not happen if the card information is encrypted from the outset using a type of "secret code" – and that's exactly what a "token" does!

## Our Debit Card and Its Tokens



The first step involved in tokenization is to replace the funding card with a digital sub-card. The primary account number for the funding card (FPAN) that we have on record is replaced with a digital PAN (DPAN) and is encrypted as a token together with its new expiry date and security code. The reference between the two "PANs" is recorded with the bank's tokenization service and with the relevant token service provider (TSP; schemes). Token encryption, on the other hand, can only be performed by the TSP.

But digitizing and encrypting the funding card as a token alone is still not secure enough – because although different card information is now being used, it could still be used to commit fraud. Linking the token to a specific purpose provides the additional level of security that is required. A debit card can have any number of tokens and DPANs. These digital sub-cards in token form are subject to the same lifecycle rules as funding cards; for example, they are valid for three years from the date of issue and require a digital image.

## Use of Tokens for Debit Cards – Wallet Payments and Online Shopping

For us card holders, there are two different ways of using tokens: *merchant wallets*, where tokens are stored for online transactions, and *issuer wallets*, where tokens can be used in a payment app for transactions involving a smart device.

### *Merchant Wallets*

Often, we are not even aware of "merchant tokenization" because most of the processes it involves occur in the background. For us card holders, it makes no difference from a user experience point of view whether the transaction is a normal "card-on-file transaction" (the merchant stores the card data) or a "token-based transaction" (the merchant stores the token only). For online merchants, however, tokenization offers some major advantages: Without tokens, the sensitive card data has to be protected using incredibly expensive security standards such as PCI-DSS. Using tokens reduces the number of protective measures that have to be taken. To illustrate this: All the online merchant has to do is create a "merchant wallet" for the customer and store the relevant token.

### *Issuer Tokenization*

The second and arguably more well-known method of using tokens is "issuer tokenization," which can also be called "mobile payment wallets" or "payment apps." This is where the token is stored in a payment app on our smart device, allowing it to be used as a recurring means of payment. The most well-known payment apps are Apple Pay, Samsung Pay and Google Pay. Even "small pay" devices like Fitbit, Garmin and Swatch offer a payment function, which puts them in this category as well. Not only this, but this form of tokenization also includes banks', software providers' and merchants' own proprietary payment apps.

Unlike merchant tokenization, the purpose is not linked to an individual merchant but to the payment app and the corresponding smart device. The payment app provider has an obligation to perform card holder authentication in advance.

## Different Wallet Technology in Payment Apps

There are two different types of technology for wallets in payment apps: *cloud-based HCE wallets* and local *SE wallets stored on the smart device.*

### *Cloud-Based HCE Wallets*

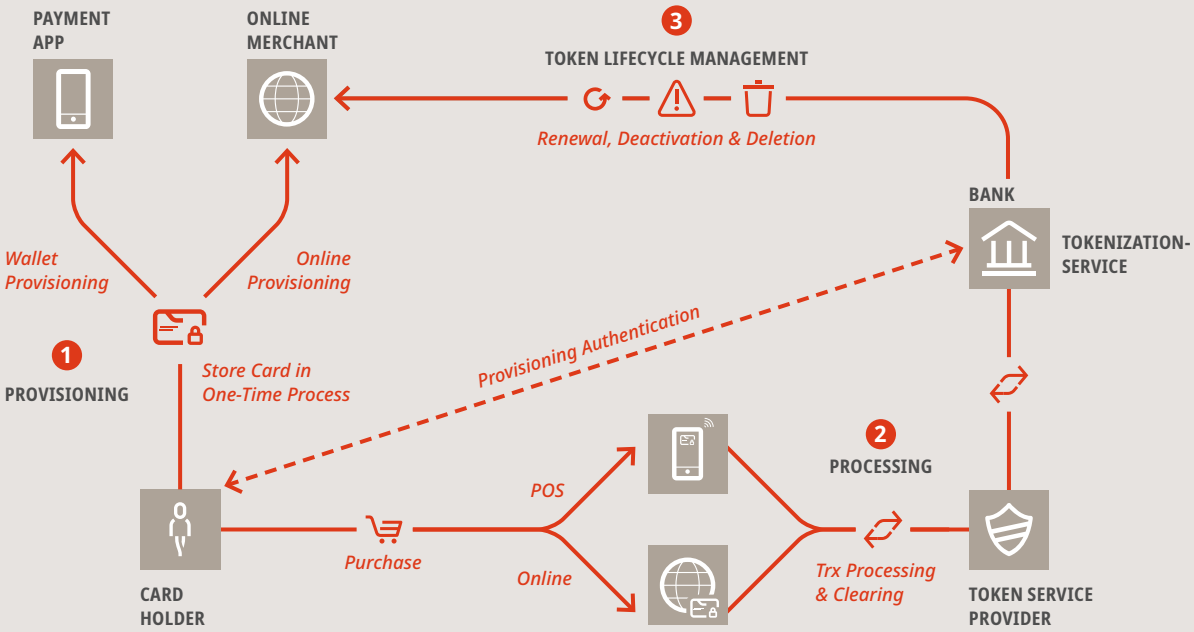
The "host card emulation" (HCE) method is where the wallet containing the token is stored in a secure cloud belonging to the provider, which requires an internet connection. To ensure that this process works offline, too, the payment app is provided with individual "sub-keys," which are renewed on a regular basis. This is akin to a book of coupons that is renewed as soon as all the coupons have been used up. Banks commonly use this technology for their own solutions, as do wallet providers that are not dependent on a particular operating system. One prominent example is Google Pay.

### *SE Wallets Stored on the Smart Device*

Wallets that are integrated in a smart device are the counterpart to cloud-based technology. It is referred to as "secure element" (SE), meaning that the wallet is stored along with the token in a secure repository on the smart device. As such, this method does not require an internet connection and is also available offline at all times. This technology is often used for payment apps, which run on the hardware and operating system of the same provider. Examples include Samsung Pay and Apple Pay.

## Tokenization in Detail

***Overview of the Tokenization Landscape***
Various parties, services and relevant processes are involved in enabling the protection mechanism to be used for our debit cards.




### 1 Provisioning:
**Storing the Card Information**

Provisioning is the first step involved in tokenization. "Provisioning" means storing the card details in an online merchant's wallet (online provisioning) or a payment app (wallet provisioning).

Both require what is known as a token request. This process verifies both the integrity of the requester and the authorization of the card holder.

Online provisioning is where the bank's tokenization service performs the verification of the card and the card holder. This provides an uninterrupted user experience.

Wallet provisioning involves an additional element of complexity in that the card holder must be authenticated by the bank when the request is made. The level of authentication required is based on the card holder's entry channel:

- **App-based provisioning:** The card holder's point of entry is the bank's own app, which forwards the card information to the wallet for provisioning. The authentication has therefore already been performed in advance so is no longer required. Providers also call this process "push provisioning" and "in-app provisioning."
- **Manual provisioning:** The card holder's point of entry is directly in the wallet where the card information is entered manually. From the bank's perspective, this is a non-authenticated environment. Authentication is performed by the smart device only, which may potentially not be sufficient for the bank. Hence an additional card holder authentication process must be carried out.

***Additional Card Holder Authentication Needed for Manual Provisioning***

| GREEN FLOW | YELLOW FLOW | RED FLOW |
|---|---|---|
|  |  |  |
| *Authentication of the smart device is sufficient. Token request approved.* | *Card holder authentication required through a verified channel.* | *Token request declined, and a token cannot be created.* |

In the yellow flow, additional card holder authentication can take place via various channels including:
- OTP: one-time authentication code by SMS or e-mail
- Call center authentication
- App authentication: The card holder can self-authenticate via an app in a similar way to the 3D Secure process
- SIM authentication

## 2 Processing:

**Token-Based Transaction Processing**

Even token-based transactions operate through processing steps that are familiar to us. They are authorized at FPAN level, but additional information such as the corresponding DPAN and the purpose are included as well. Unlike with traditional authorizations, this does not include certain checks as these are already performed in advance when the token is encrypted by the TSP. This ensures that the transaction can be assigned to the correct card, and makes it clear that the transaction is token-based.

## 3 Token Lifecycle Management:

**Managing Tokens**

Token lifecycle management is also based on the same elements as the lifecycle management of regular cards. But this form is slightly more complex as it has to take into account the connection to the funding card. This means that lifecycle events for the digital sub-card are always related to the funding card. This can be illustrated nicely using the example of token validity: Both funding cards and tokens are valid for three years from the date of issue. In all likelihood, they are not issued at the same time and do not have identical expiry dates. That is why it is important to clearly set out, via lifecycle events, how this data is related. The same also applies to a token's response when the funding card is blocked.


**SIX BBS Ltd**
Hardturmstrasse 201
P. O. Box
8021 Zurich
T +41 58 399 4012
pm.debit@six-group.com