LEARNING NUGGET
#2

Tokenisierung für Debitkarten

Der Schutz von sensitiven Kartendaten und der Schlüssel zu Mobile-Wallet-Zahlungen

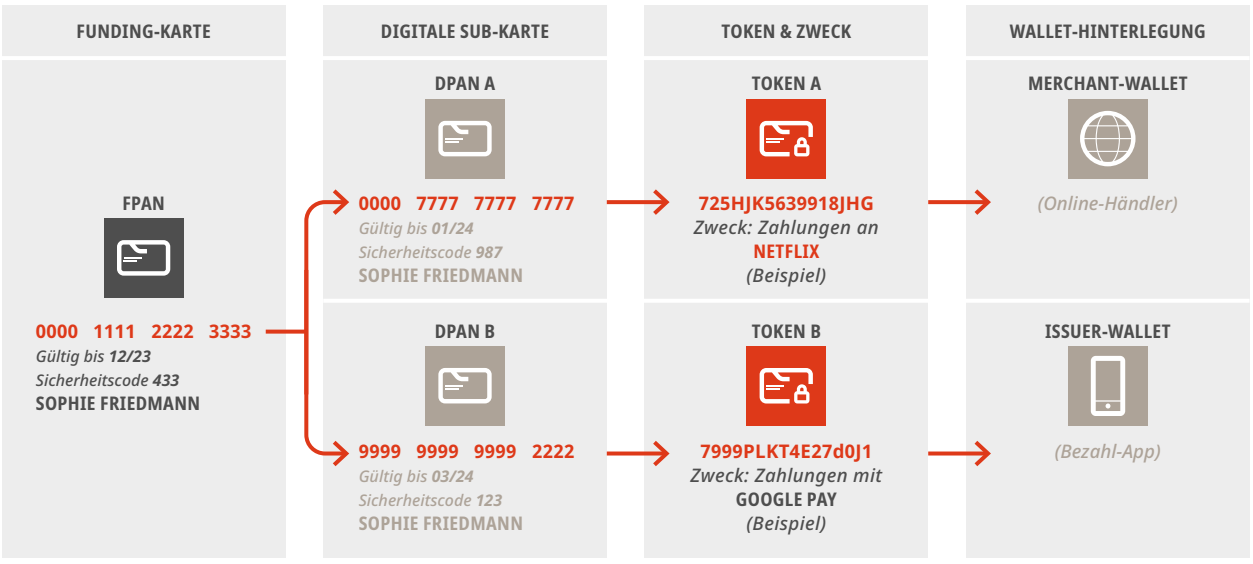
Einführung in die Tokenisierung von Debitkarten

Der Token als «Geheimcode» zum Schutz von sensitiven Karteninformationen

Im Umgang mit sensitiven Daten ist unser Bedürfnis nach Sicherheit sehr hoch. Insbesondere wenn mehrere Systeme über ein uns unbekanntes Netzwerk sensitive Karteninformationen austauschen, ist ein Schutz erforderlich, um Datenklau und Missbrauch vorzubeugen.

Für die Abwicklung von Zahlungen bietet uns der Tokenisierungs-Mechanismus eine optimale Lösung. Ob am Point-of-Sales über «Bezahl-Apps», oder beim Online-Shopping – unsere Kartendaten werden auf unseren Smartdevices und auf den Webseiten der Online-Händler gespeichert und über weitere Systeme zur Zahlungsabwicklung weitergegeben. Sollten unsere sensitiven Karteninformationen abgefangen oder vorsätzlich gestohlen werden, wäre unser Konto «ungeschützt» und die Betrüger hätten Zugang zu unserem Ersparten. Dies ist nicht der Fall, wenn die Karteninformationen von Anfang an durch eine Art «Geheimcode» verschlüsselt werden – und genau das macht ein «Token»!

Unsere Debitkarte und ihre Tokens



Bei der Tokenisierung wird als Erstes die Funding-Karte durch eine digitale Sub-Karte ersetzt: Die uns bekannte Primary-Account-Number der Funding-Karte (FPAN) wird durch eine digitale PAN (DPAN) ersetzt und zusammen mit dessen neuem Ablaufdatum und Sicherheitscode zu einem Token verschlüsselt. Die Referenz zwischen den beiden «PANs» ist im Tokenisierungsservice der Bank und bei dem entsprechenden Token Service Provider (TSP; Schemes) dokumentiert. Die Entschlüsselung des Tokens kann hingegen nur vom TSP durchgeführt werden.

Die Digitalisierung und Verschlüsselung der Funding-Karte zu einem Token allein ist noch nicht sicher genug. Denn auch wenn nun andere Karteninformationen verwendet werden, könnte anhand dieser nach wie vor Betrug durchgeführt werden. Die gewünschte Zusatzsicherheit wird erreicht, wenn der Token an einen bestimmten Zweck gebunden wird. Eine Debitkarte kann also x-beliebig viele Tokens und DPANs haben. Diese digitalen Sub-Karten in Form von Tokens unterliegen den gleichen Lifecycle-Regeln wie die Funding-Karte; sie sind beispielsweise ab dem Ausstellungsdatum drei Jahre gültig oder brauchen ein digitales Abbild.

Einsatz der Tokens für Debitkarte – Wallet-Payments und Online-Shopping

Für uns Karteninhaber gibt es zwei verschiedene Einsatzmöglichkeiten von Tokens; bei *Merchant-Wallets*, wo Tokens für Online-Transaktionen hinterlegt werden und *Issuer-Wallets*, wo Tokens in einer Bezahl-App für Transaktionen mit einem Smartdevice verwendet werden können.

Merchant-Wallets

Die sogenannte «Merchant-Tokenisierung» ist für uns oftmals nicht ersichtlich, denn die dazugehörigen Prozesse laufen meist im Hintergrund ab. Für uns Karteninhaber macht es aus einer Userexperience-Sicht keinen Unterschied, ob es sich bei der Transaktion um eine normale «Card-on-File-Transaktion» (der Händler speichert die Kartendaten) oder eine «tokenbasierte Transaktion» (der Händler speichert nur den Token) handelt. Für die Online-Händler hingegen bringt die Tokenisierung grosse Vorteile; ohne Tokens müssen die sensitiven Kartendaten mit aufwändig teuren Sicherheitsstandards wie PCI-DSS geschützt werden. Durch die Verwendung von Tokens reduzieren sich diese Schutzmassnahmen. Um dies zu veranschaulichen: Der Online-Händler legt für den Kunden bei sich ein «Merchant-Wallet» an und hinterlegt den zugehörigen Token.

Issuer-Tokenisierung

Die zweite und wohl bekanntere Einsatzmöglichkeit von Tokens ist die sogenannte «Issuer-Tokenisierung», auch bekannt als «Mobile Payment Wallets» oder «Bezahl-Apps». Dabei wird der Token in einer Bezahl-App auf unserem Smartdevice hinterlegt und kann so als wiederkehrendes Zahlungsmittel eingesetzt werden. Zu den bekanntesten Bezahl-Apps gehören Apple Pay, Samsung Pay oder Google Pay. Auch «Small Pay» wie Fitbit, Garmin oder Swatch bieten eine Bezahlfunktion auf ihren Geräten an und gehören in diese Kategorie. Weiter versteht man unter dieser Form der Tokenisierung auch eigene Bezahl-Apps von Banken, Software-Providern oder Händlern.

Im Gegensatz zur Merchant-Tokenisierung ist die Zweckbindung nicht an einen einzelnen Händler gebunden, sondern an die Bezahl-App und das entsprechende Smartdevice. Der Anbieter der Bezahl-App ist verpflichtet, die Karteninhaber-Authentifikation vorgängig sicherzustellen.

Unterschiedliche Technologien von Wallets in Bezahl-Apps

Bei den Wallets in Bezahl-Apps wird zwischen zwei Technologien unterschieden; *cloudbasierte HCE-Wallets* und lokal auf Smartdevice gespeicherte *SE-Wallets*.

Cloudbasierte HCE-Wallets

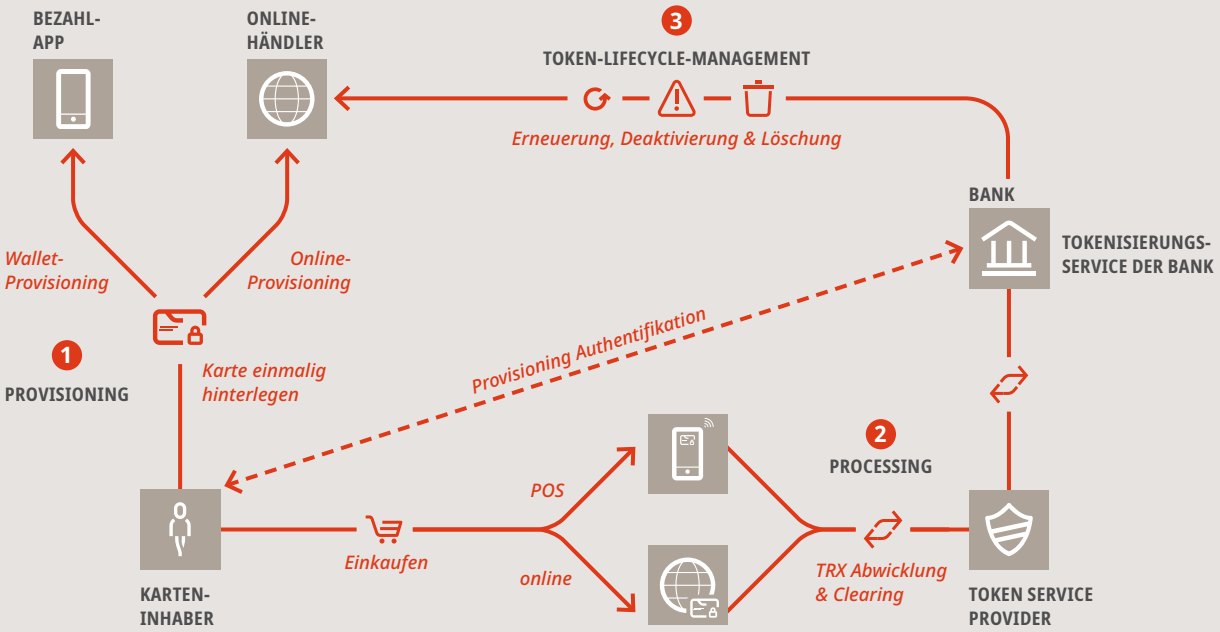
Beim «Host Card Emulation»-Ansatz (HCE) befindet sich das Wallet mit dem Token in einer sicheren Cloud des Anbieters und bedarf somit einer Internetverbindung. Damit dies auch offline funktioniert, werden der Bezahl-App einzelne «Sub-Keys» zur Verfügung gestellt, welche regelmässig erneuert werden. Dies ist vergleichbar mit einem Couponheft, welches erneuert wird, sobald alle Coupons aufgebraucht sind. Diese Technologie kommt häufig bei bankeigenen Lösungen zum Einsatz oder bei betriebssystemunabhängigen Wallet-Providern. Ein bekanntes Beispiel dazu ist Google Pay.

Auf Smartdevice gespeicherte SE-Wallets

Das Gegenstück zur cloudbasierten Technologie sind im Smartdevice integrierte Wallets. Dabei spricht man von einem «Secure-Element» (SE), das heisst Wallet samt Token liegen in einem sicheren Speicher des Smartdevices. Entsprechend braucht dieser Ansatz keine Internetverbindung und ist jederzeit auch offline verfügbar. Häufig wird diese Technologie bei Bezahl-Apps eingesetzt, welche auf dem Hard- und Betriebssystem des gleichen Anbieters laufen, wie beispielsweise Samsung Pay und Apple Pay.

Tokenisierung im Detail

Übersicht der Tokenisierungs-Landschaft
Damit der Schutzmechanismus für unsere Debitkarten angewendet werden kann, braucht es verschiedene Parteien, Services und entsprechende Abläufe.



1 Provisioning:
Hinterlegen der Karteninformationen

Das Provisioning ist der erste Schritt bei der Tokenisierung. Unter «Provisioning» wird die Hinterlegung der Kartendetails in ein Wallet eines Online-Händlers (Online-Provisioning) oder einer Bezahl-App (Wallet-Provisioning) verstanden.

Für beide Arten gibt es eine Antragsprüfung – ein sogenannter Token-Request. Dabei wird einerseits die Integrität des Antragsstellers und andererseits die Karteninhaberberechtigung geprüft.

Beim Online-Provisioning wird die Prüfung auf Karten- und Karteninhaberebene durch den Tokenisierungsservice der Bank sichergestellt. Dies ermöglicht eine unterbruchfreie Userexperience.

Beim Wallet-Provisioning kommt eine zusätzliche Komplexität hinzu; der Karteninhaber muss während der Antragsprüfung durch die Bank authentifiziert werden. Die benötigte Authentifikationsstufe ist abhängig vom Einstiegskanal des Karteninhabers:

- **App-gesteuertes Provisioning:** der Karteninhaber startet aus der bankeigenen App, welche die Karteninformationen dem Wallet fürs Provisioning übergibt. Dabei hat die Authentifikation vorgängig schon stattgefunden und entfällt somit. Dieser Vorgang wird je nach Anbieter auch «Push-Provisioning» oder «In-App-Provisioning» genannt.
- **Manuelles Provisioning:** der Karteninhaber startet direkt im Wallet und gibt die Karteninformationen manuell ein. Aus Sicht der Bank ist dies eine nicht-authentifizierte Umgebung. Die Authentifikation ist lediglich durch das Smartdevice erfolgt, was für die Bank potenziell nicht genügt. Entsprechend muss eine zusätzliche Authentifikation des Karteninhabers durchgeführt werden.

Zusätzliche Authentifikation des Karteninhabers beim manuellen Provisioning

GRÜNER-FLOW	GELBER-FLOW	ROTER-FLOW
		
Authentifikation des Smart-devices ist ausreichend. Token-Request genehmigt.	*Authentifikation des Karten-inhabers über einen verifizierten Kanal notwendig.*	*Token-Request wird abgelehnt und es wird kein Token erstellt.*

Die zusätzliche Authentifikation des Karteninhabers beim gelben Flow kann über verschiedene Kanäle stattfinden, wie beispielsweise:
- OTP: Einmaliger Authentifikations-Code per SMS oder Mail
- Callcenter-Authentifikation
- App-Authentifikation: Karteninhaber kann sich über eine App analog zum 3D-Secure-Verfahren authentifizieren.
- SIM-Authentifikation

2 Processing:

Tokenbasierte Transaktionsverarbeitung

Auch tokenbasierte Transaktionen laufen durch die uns bekannten Verarbeitungsschritte. Sie werden auf der FPAN-Ebene autorisiert, jedoch werden Zusatzinformationen, wie die dazugehörige DPAN und der Zweck, mitgeliefert. Anders als bei klassischen Autorisierungen entfallen gewisse Prüfungen, da diese bereits vorgängig bei der Entschlüsselung des Tokens durch den TSP durchgeführt wurden. So wird sichergestellt, dass die Transaktion der richtigen Karte zugeordnet werden kann, und ersichtlich ist, dass es sich um eine tokenbasierte Transaktion handelt.

3 Token-Lifecycle-Management:

Verwaltung der Tokens

Auch das Token-Lifecycle-Management beinhaltet grundsätzlich die gleichen Elemente wie das Lifecycle-Management von normalen Karten. Allerdings ist diese Form etwas komplexer, da die Verbindung zur Funding-Karte berücksichtigt werden muss, das heisst, Lifecycle-Events der digitalen Sub-Karte stehen immer in Relation zur Funding-Karte. Mit der Gültigkeit eines Tokens kann dies schön veranschaulicht werden; sowohl eine Funding-Karte als auch ein Token haben beide je eine Laufzeit von drei Jahren ab Ausstellungsdatum. Diese werden mit grosser Wahrscheinlichkeit nicht zum gleichen Zeitpunkt ausgestellt und haben keine identischen Ablaufdaten. Daher ist es wichtig, über die Lifecycle-Events klar zu definieren, wie sich diese Daten gegenseitig verhalten. Gleiches gilt auch für die Verhaltensweisen eines Tokens bei Sperrung der Funding-Karte.

SIX BBS AG
Hardturmstrasse 201
Postfach
8021 Zürich
T +41 58 399 4012
pm.debit@six-group.com