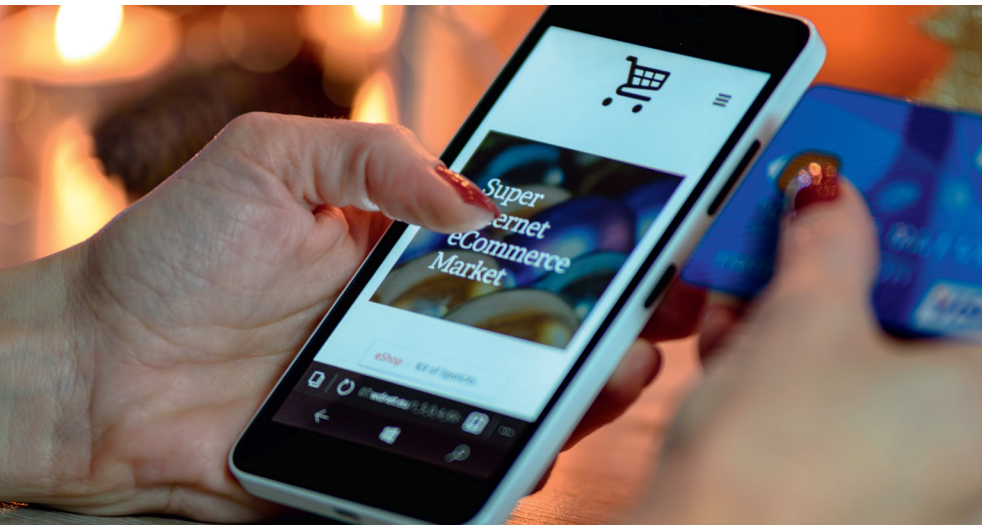
Tokenisierung im E-Commerce – neue Perspektiven durch SRC

Von Kurt Schmid



Das Sicherheitsverfahren 3D Secure lässt die Abbruchraten im E-Commerce kräftig steigen. Weil sich Tokenisierungskonzepte der Kartenorganisationen wie Masterpass oder Visa Checkout jedoch nicht durchsetzen konnten, wurde mit SRC ein neuer, übergreifender Standard entwickelt, der 3 D Secure um die Tokenisierung ergänzt. In Europa wird der Checkout per SRC erst 2020 kommen, so Kurt Schmid. Er bringt jedoch Vorteile für Händler, Payment Service Provider und die Kunden und dürfte durch mehr Bequemlichkeit für die Kunden die Konversionsraten steigen lassen. Red.

Tokenisierung ist seit ein paar Jahren stark im Kommen und wurde verstärkt im Bereich des mobilen kontaktlosen Bezahlens eingesetzt. Sowohl OEM Pays als auch HCE-Lösungen von Banken verwenden nicht die originären Kartendaten, sondern lassen von Token Services für eine Nutzung auf einem Gerät eingeschränkte Tokens erzeugen.

Die Tokenisierungsdienste der Schemes, wie MDES, VTS oder AETS sind dazu sowohl mit dem Issuer verbunden als auch mit dem Token Requestor, wie zum Beispiel die Wallet Applikation der Bank zum mobilen Bezahlen per NFC.

In Zukunft kann diese Tokenisierung auch im E-Commerce-Umfeld eingesetzt werden, was die Sicherheit und Akzeptanz erhöht. Der vorliegende Artikel zeigt die Möglichkeiten und Hintergründe dazu auf.

Zum besseren Verständnis hier ein genauerer Blick auf die Abläufe bei der Tokenisierung.

Abläufe bei der Zahlung unter der Lupe

– Die Wallet (als Token Requestor) möchte eine Karte „digitalisieren", also einen Token erzeugen, der zum Bezahlen verwendet werden kann. Dazu wird eine Digitalisierungsanfrage über den Wallet Server zum Token Service Provider des Schemes (kurz „TSP" zum Beispiel MDES oder VTS) geschickt. Dieser Request enthält die Kartennummer der zugrunde liegenden „echten" Karte, in der Fachsprache wird von der Funding PAN (FPAN) gesprochen.

– Ohne die Zustimmung des Issuers kann der Request jedoch nicht bewilligt werden. Daher geht der Token Service Provider weiter zum Issuer und fragt an, ob der Request von dieser bestimmten Wallet für die bestimmte FPAN erlaubt ist.

– Wenn der Issuer nach einer Step-up Authentication des Benutzers sein OK gibt, antwortet dieser positiv und der TSP erzeugt eine Device PAN (DPAN), die an die Wallet ausgeliefert wird.

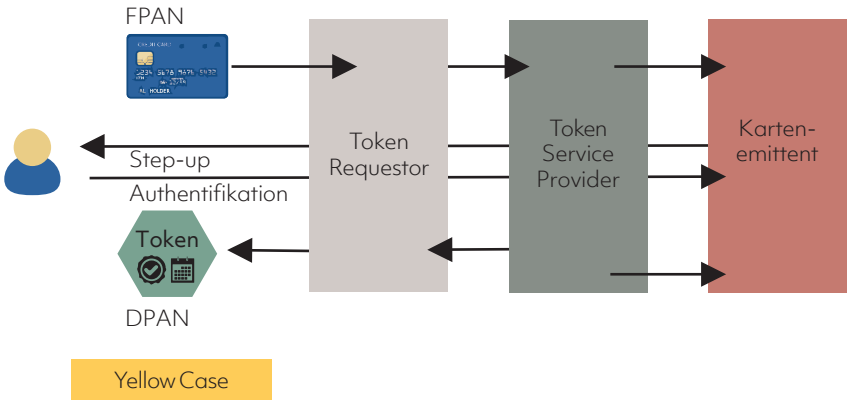
– Wenn die Issuer Wallet als Token Requestor fungiert, so kann der sogenannte „yellow case", also der case mit Step-up Authentication, durch einen für den Benutzer einfacheren „green case" ersetzt werden. Die FPAN kommt bereits verschlüsselt vom Issuer und wird dann zum Beantragen der Digitalisierung verwendet. Damit ist keine weitere Authentisierung des Benutzers erforderlich.

– Neben der DPAN wird die Wallet auch vom TSP mit Schlüsseln (sogenannten Transaction Credentials wie Single beziehungsweise Limited Use Keys) versorgt, die zur Berechnung des Kryptogramms verwendet werden. Dieses unterschreibt die Bezahlung eindeutig und kann somit verwendet werden, um „Card Present"-Zahlungen nach dem EMV-Standard sicher zu autorisieren.

Diese Autorisierung erfolgt in zwei Schritten: Zunächst werden die DPAN und das Kryptogramm zum TSP geschickt. Dort wird verifiziert, ob die

Kurt Schmid, Managing Director
Digital Payments, Netcetera GmbH, Linz

Abbildung 1: Abläufe bei der Tokenisierung



Quelle: Netcetera

DPAN gültig und das Kryptogramm echt ist. Danach wird die DPAN in die FPAN zurückübersetzt und ein für die FPAN gültiges Kryptogramm berechnet und an den Autorisierungshost des Issuers geschickt. Erst wenn dort die Transaktion bestätigt wird, erhält der Wallet-Verwender das OK über das Terminal.

Der Issuer Host erhält zudem neben der FPAN auch die Zusatzinformation, welche Wallet und welches Device die Zahlung ursprünglich ausgelöst hat.

Wallet mit „echten" Kartenbildern

Die Token Service Provider weisen neben den Use-Cases der Digitalisierung und der Versorgung des Wallet mit Schlüsseln („Replenishment") auch noch weitere Funktionalitäten auf. Die Wallet wird mit den „echten" Kartenbildern versorgt. Dies ist zum Beispiel für die OEM-Wallets von Interesse, da dann der Kunde das exakte Bild seiner physischen Karte auch in der Wallet sieht. Wallets können auch die letzten Transaktionen von den Token Service Providern abfragen.

Nicht sofort offensichtlich, aber doch wichtig, sind Life-Cycle-Management-Funktionen wie das Blockieren der DPAN im Falle, dass die physische Karte verloren gegangen ist oder die Verbindung eines Tokens mit einer neuen FPAN beziehungsweise einer mit verlängertem Gültigkeitsdatum.

Um auf die Vorteile von Tokenisierung im E-Commerce-Umfeld einzugehen, zunächst eine Betrachtung, wo die Probleme aktuell liegen.

Probleme im heutigen E-Commerce-Checkout

Das Hauptproblem für alle Beteiligten (Kunden, Bank, Händler, PSP) ist die hohe Abbruchrate von durchschnittlich 70 Prozent.[1)] Diese resultiert aus mehreren Faktoren wie der mühsamen Eingabe aller Kartendaten (insbesondere auf mobilen Geräten), dem Vergessen von Passwörtern zur Autorisierung und mehr.

Die Sicherheit von traditionellen E-Commerce-Zahlungen („Card Not Present", kurz CNP) beruht auf der sehr schwachen Vertraulichkeit von Kreditkartendaten (PAN, Ablaufdatum und CVC sind faktisch kaum vertraulich) und damit im Wesentlichen auf der Sicherheit der 3-D Secure-Autorisierung (kurz 3DS). Diese erfolgt per Passwort, per SMS-TAN oder moderner Push-TAN über die Banking App. Mit der RTS der PSD2-Regulierung wird es per 14. September 2019 verpflichtend, Strong Customer Authentication (SCA) einzuführen. Damit müssen zwei voneinander unabhängige Faktoren verwendet werden wie zum Beispiel die Registrierung eines Gerätes (Besitz des Smartphones) und Validierung des Fingerabdrucks (Eigenschaft des Benutzers). Damit wird die Hürde für den Zahlenden insbesondere, was die Registrierung betrifft noch höher.

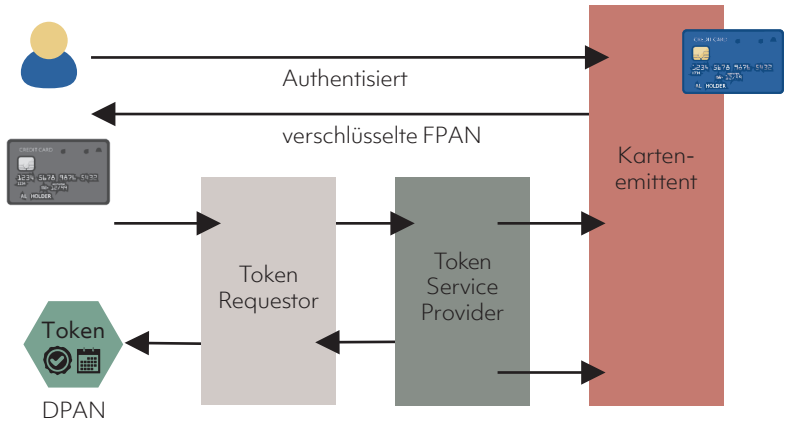
Untersuchungen von Mastercard und Wordpay haben zudem ergeben, dass die Ablehnrate bei Verwendung von 3D Secure 24 Prozent beträgt, während sie ohne 3D Secure bei nur 17 Prozent liegt. Das bedeutet, dass mit Verpflichtung für die Verwendung von 3DS weniger Transaktionen erfolgreich bestätigt werden. Zudem ist die Betrugsrate („Fraud") bei Card-Not-Present-Zahlungen um den Faktor 10 höher als bei Card-Present-Zahlungen, die über ein Kryptogramm deutlich besser gesichert werden.

SRC als neuer Standard

In den letzten Jahren haben die Schemes jeweils getrennt versucht, Wallets auch im E-Commerce zu etablieren. Visa Checkout und Masterpass von Mastercard haben es jedoch in den meisten Ländern nicht geschafft, ausreichend Kunden und Issuer zu überzeugen.

Vielversprechender ist ein übergreifender Ansatz, der auch vom Konsumenten

Abbildung 2: Vereinfachter Prozess der Authentifikation



Quelle: Netcetera

verwendet werden kann, egal welche Payment-Karte von welchem Scheme er einsetzt. Dazu haben die Schemes übergreifend in der EMVCo zusammengearbeitet und gemeinsam mit Feedback der Industrie einen neuen Standard entwickelt: Secure Remote Commerce (kurz SRC).[2] SRC wird durch 3DS 2.0 und durch Tokenisierung ergänzt. In dieser Kombination sollen für alle Arten einer Kartenzahlung im Internet eine Verbesserung der Benutzerfreundlichkeit und Sicherheit erreicht werden.

Prinzipiell gibt es folgende Einsatzmöglichkeiten:

– Der Kunde hat bereits seine Karte beim Händler beziehungsweise beim PSPs des Händlers hinterlegt („Card On File" = COF).

– Der Kunde gibt die Kartendaten auf seinem eigenen Gerät ein.

– Der Kunde macht einen Gast-Checkout ohne dass seine Kartendaten für einen Folgeeinkauf gespeichert werden, da er den Einkauf nicht auf einem seiner eigenen Geräte macht.

Hat der Händler beziehungsweise der PSP des Händlers bereits die Kartendaten gespeichert (also die FPAN), so trägt er damit auch die volle Verantwortung gemäß PCI-Anforderungen. Wenn FPANs gestohlen werden, so ist dies ein massiver Schadensfall, da alle betroffenen Issuer die Karten neu ausgeben müssen. Die Haftung dafür kann einen Händler/Payment Service Provider im Fall einer erfolgreichen Attacke in den finanziellen Abgrund reißen. Besser ist es daher, über die Schemes zu jeder FPAN eine MPAN (Merchant PAN) als Token anzufordern. Damit muss keine FPAN mehr gespeichert werden. Im Falle der Autorisierung wird die MPAN von den TSP geprüft und wie beschrieben in eine FPAN rückübersetzt.

Drei weitere Vorteile ergeben sich zudem: Der Konsument sieht sein echtes Kartenbild und hat damit mehr Übersicht und Vertrauen, was den Bezahlvorgang betrifft. Zum zweiten kann bei Ablauf der Karte eine automatische Erneuerung über den Token ermöglicht beziehungsweise eine neue FPAN an den bestehenden Token (MPAN) angebunden werden. Zudem erhält der Kunden eine Übersicht, wo seine Kartendaten gespeichert sind. Über die App seines Issuers kann er sehen, wo zu seiner Karte Tokens erzeugt worden sind. Eine Übersicht über alle DPANs und MPANs erleichtert die Verwaltung.

Tokenisierung im E-Commerce-Device-Checkout-Szenario

Wenn der Kunde auf einem seiner Geräte einen Checkout macht, so ermöglicht der SRC-Standard, den Token auf dem Gerät zu pairen. Damit kann ein folgender Checkout mit einer One-Click-Experience erfolgen. Das Pairing kann auch von der Banking-App initiiert werden, wodurch keine Eingabe von Kartendaten mehr notwendig ist.

Ansonsten wird die FPAN nach der Eingabe sofort in eine DPAN umgewandelt. Die weiteren Vorteile sind äquivalent der Tokenisierung im COF-Umfeld. Allerdings gibt es eine weitere wichtige Verbesserung unter Sicherheitsaspekten: Die Händler-/PSP-Checkout-Funktionalität fordert nicht nur einen Token an, sondern es werden von den TSP auch die entsprechenden Kryptogramme generiert. Damit wird das Sicherheitsniveau auf das einer Card-Present-Transaktion angehoben. Folgende Vorteile ergeben sich aus SRC:

– Benutzer brechen Checkout- Vorgänge seltener ab, da der Ablauf deutlich einfacher und schneller erfolgen kann;

– die Entkoppelung von physischen Kartendaten vermeidet Ablehnungen wegen Kartenablauf oder -wechsel;

– durch verbesserte Sicherheitsmaßnahmen lehnen Betrugssysteme Tokentransaktionen deutlich seltener ab;

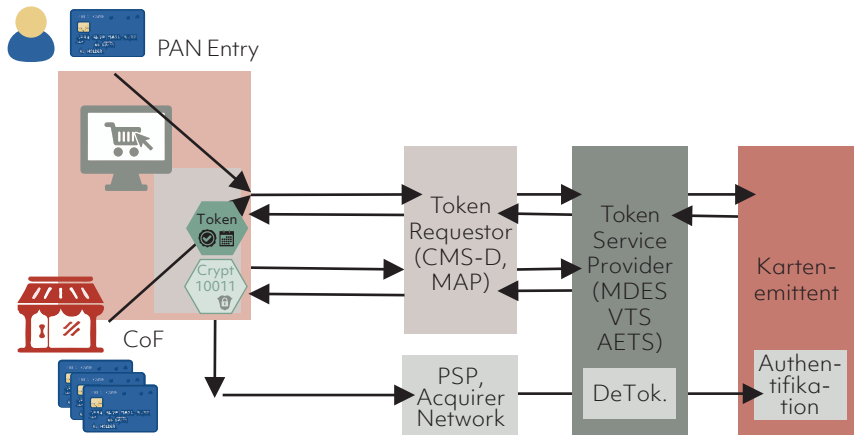
– PSPs und Händler tragen ein deutlich geringeres Risiko;

– weniger operativer Aufwand für den Issuer;

– bessere Übersicht und Sicherheitsempfinden für den Benutzer, da er sieht, wo seine Tokens verwendet werden.

Diese Vorteile in Summe verbessern die Konversionsrate durch deutlich höhere Approval rates signifikant. Experten erwarten zumindest eine um 10 Prozent gesteigerte Konversionsrate.

Abbildung 3: Tokenisierung im E-Commerce im Card-on-File-Szenario*



* Kartendaten beim Händler gespeichert

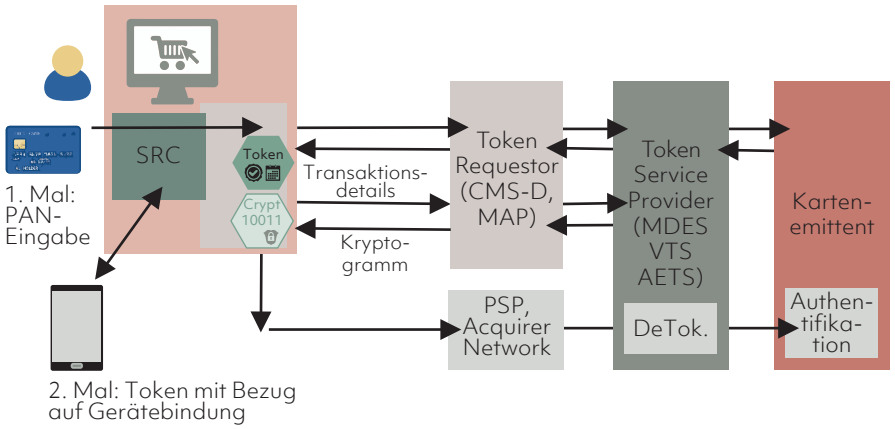
Quelle: Netcetera

Bis Ende 2019 bereit

Die Tokenisierungsdienste der Schemes sind bereits seit langem für Device Tokenisierung im Einsatz. Dies betrifft solche Dienste für Issuer Wallets und OEM Pays in fast allen Ländern Europas.

Zudem sind viele Issuer bereits an diese Services angeschlossen. Man rechnet, dass bis Ende 2019 nur ein kleiner Teil (weniger als fünf Prozent) des europäischen Kartenportfolios nicht an MDES und VTS angeschlossen sein werden. Die Schemes erfordern, dass Tokenisierungsanfragen von Händlern immer positiv beantwortet werden müssen. Alle Issuer, die noch nicht an die Tolken Service Provider angebunden sind, werden einen kostenpflichtigen On-Behalf-

Abbildung 4: Tokenisierung im Device-Checkout-Szenario



Quelle: Netcetera

Service anbieten müssen. Damit ist zu erwarten, dass in Europa bis Ende 2019 alle Karten zur Digitalisierung im Merchant-Umfeld bereitstehen werden.

Checkout per SRC erst 2020 in Europa

Wegen der höheren Konversionsrate sind die Händler motiviert, diese Technologie rasch zu implementieren. Zusätzlich ist zu erwarten, dass es Anreize beziehungsweise Motivatoren von den Schemes dafür geben wird, Tokenisierung einzusetzen. Dazu könnten zum Beispiel zählen: bessere Gebühren für E-Commerce-Transaktionen, die mit Kryptogrammen und Tokens gesichert werden, Mandate, FPAN nicht mehr für E-Commerce-Transaktionen zuzulassen oder Liability Shift auf Merchants für herkömmliche Card-Not-Present-Transaktionen.

Der Checkout per SRC wird erst 2020 nach Europa kommen, da die Schemes mit einer Implementierung in den USA starten. Dort ist auch der erste Kunde für die E-Commerce-Tokenisierung angebunden worden und zwar Netflix.

Was müssen Händler in diesem Zusammenhang vorbereiten? Sehr große Händler werden direkt Projekte mit den Schemes umsetzen. Andere Händler werden mit PSPs zusammenarbeiten, die wiederum mit Technologiepartnern und Aggregatoren für solche Dienste kooperieren werden. Denn wenn jeder Händler über PSPs mit allen Schemes integriert werden muss, wird die Skalierung nicht rasch genug voranschreiten.

In jedem Fall bietet eine kluge Kombination von 3DS 2.0, Device und E-Commerce-Tokenisierung mit einer Issuer Wallet, das die PSD2 SCA Anforderungen erfüllt, gute Chancen im Markt.

Fußnoten
1) Wikipedia: https://en.wikipedia.org
2) Details unter www.emvco.com.