Kartenmanagement-**Glossar**

Tokenization

Von Ewald Judt und Walter Bödenauer

In letzter Zeit wird im Hinblick auf die Datensicherheit bei bargeldlosen Zahlungen immer häufiger der Begriff „Tokenization" verwendet. Dieser Begriff ist nicht neu und wird nunmehr vermehrt für den Schutz von Daten herangezogen. In diesem Sinne ist Tokenization nichts anderes als der Ersatz eines sensitiven durch ein nicht-sensitives Datenelement, das keine/n Bedeutung/Wert hat und auch keinen Rückschluss auf die ursprüngliche Information ermöglicht. Dieses nicht-sensitive Datenelement wird „Token" genannt. Es ist somit ein Referenzwert, der nur durch das Tokenization-System zum sensiblen Datenelement führt.

Im E-Commerce schon lange gebräuchlich

Im Zahlungsverkehr wurde dieses Konzept zuerst im E-Commerce durch (große) Online-Shops angewandt. Der Kunde hinterlegt bei der Registrierung und somit vorweg und einmalig auch seine Zahlungsinformation zum Beispiel die dazu notwendigen Kreditkartendaten. Für die Zahlung selbst muss er diese dann nicht mehr eingeben, sondern nur das zwischen ihm und dem E-Commerce-Unternehmen vereinbarte Passwort. Ein typisches Beispiel hierfür ist amazon.de.

Eine Alternative dazu ist, dass ein Online-Shop sich für die Zahlungsabwicklung eines Payment Services Providers (PSP) bedient. Dabei wird – wenn es zum Zahlungsvorgang kommt – eine Verbindung vom Online-Shop zum PSP hergestellt, der die Zahlung in einer sicheren Infrastruktur wie Mastercard Secure Code/Verified by Visa abwickelt. Vom PSP zum Online-Shop werden über die durchgeführte Transaktion keine sensitiven Daten, sondern nur eine Referenznummer (der sogenannte Token) übermittelt. Das bedeutet eine hohe Sicherheit dadurch, dass der Kunde bei einer kartenbasierten Zahlung an den Akzeptanten entweder keine Kartendaten überträgt oder die Weiterleitung der Daten in einem sicheren Bereich erfolgt.

Ausweitung durch Mobile Payment

Zu einer Ausweitung der Anwendung des Token-Verfahrens kam es mit dem Aufkommen der Mobilfunktechnologie. Heute stehen den Konsumenten unterschiedlichste mobile Endgeräte wie Laptops, Tablets oder Smartphones zur Verfügung, die ihnen aufgrund der im Gerät (in der Regel in einem Wallet) hinterlegten Zahlungsdaten die Möglichkeit bieten, im Face-to-Face-Commerce (PoS-Payment) an jedem NFC-fähigen Terminal zu bezahlen und wann immer und wo immer am virtuellen Marktplatz im Non-Face-to-Face-Commerce (M-Payment) teilzunehmen. Das bedeutet eine hohe Sicherheit durch den Ersatz der Kartendaten mit dem Token bei der Transaktion.

Für die Tokenization auf Basis einer Wallet-Lösung gibt es eine Reihe unterschiedlicher Verfahren, wobei die von Apple Pay aufgrund der weltweiten Promotion derzeit die höchste Aufmerksamkeit genießt. Hierbei werden bei der Registrierung alle erforderliche Kartendaten im mobilen Endgerät erfasst und anschließend über eine sichere Verbindung an einen Token-Vault, der ein Datentresor ist, übertragen. Die Daten werden dort sicher gespeichert. Nach Genehmigung der Registrierung durch den Karten-Issuer wird an das mobile Endgerät des Kunden ein Token zurückgesandt, der im Wallet gespeichert wird. Danach wird nur mehr der nicht-sensitive Token verwendet.

Bei einer Zahlung identifiziert sich der Kunde mit dem entsprechenden Passwort (oder einem anderen Verifikationsverfahren wie zum Beispiel bei Apple Pay mit einem Fingerabdruck). Damit kann der Kunde die Zahlung beim Handels- und Dienstleistungsunternehmen egal ob real oder virtuell starten.

Statische und dynamische Verfahren

Es wird der Token anstelle der Kartendaten mit einem entsprechenden Hinweis im Datensatz an das Zahlungsmodul des Zahlungsakzeptanten übertragen und aufgrund des Hinweises an den Token-Vault weitergeleitet, wo er auf die ursprünglichen Kartendaten umgeschlüsselt und eine Genehmigungsanfrage beim Issuer gestartet wird. Genehmigt der Issuer die Transaktion, wird dies via Acquirer dem Handels- und Dienstleistungsunternehmen mitgeteilt, womit die Zahlung abgeschlossen ist.

Eine derartig abgewickelte Token-Transaktion wird als statisches Verfahren bezeichnet. Hierbei hat der kartenbasierte Token einen fixen Wert über die Laufzeit der Originalkarte.

Eine weitere Verbesserung der Sicherheit bietet das dynamische Verfahren. Die Registrierung entspricht dem des statischen Verfahrens, die digitale Brieftasche ist aber in der Lage, für jede Transaktion einen

neuen Token zu generieren. Somit wird bei diesem Verfahren für jede Transaktion ein neuer Token erzeugt. Der Token Vault ist auch beim dynamischen Verfahren in der Lage, den von der Wallet individuell erzeugten Token der entsprechenden Kartennummer zuzuordnen.

Risikokosten bargeldloser Zahlungen weiter reduzieren

Der Vorteil der Tokenization-Technologie ist die hohe Sicherheit. Diese wird im E-Commerce dadurch erreicht, dass der Akzeptant oder der PSP die sensiblen Kartendaten verschlüsselt in einem entsprechend abgesicherten EDV-System speichert und auf diese Daten nur mit dem Token zugegriffen werden kann.

Im Face-to-Face- und Non-Face-to-Face-Commerce wird die gewünschte hohe Sicherheit durch den Ersatz der Kartendaten mit einem Token im Wallet erreicht. Sollte ein derartiger Token bei einem Datendiebstahl in kriminelle Hände gelangen, fängt der Täter damit nichts an, da der Token nur dann als gültig erkannt wird, wenn er von der Wallet aus verwendet wird, an die der Token bei der Registrierung übermittelt wurde.

Ein Token-Vault kann entweder vom Rechenzentrum eines Zahlungsakzeptanten selbst, von einem Payment Service Provider oder einem Zahlungsscheme betrieben werden, wobei der von EMVCo vorgegebene Standard erfüllt werden muss.

Mit den unterschiedlichsten Formen der Tokenization wurde eine weitere Verbesserung der Sicherheit bei der Verwendung von Zahlungsdaten erreicht. Damit können die Risikokosten von bargeldlosen Zahlungen reduziert werden.

Dr. Ewald Judt ist Honorarprofessor der Wirtschaftsuniversität Wien, ewald.judt@wu.ac.at; Walter Bödenauer ist Prokurist der PayLife Bank, Wien, walter.boedenauer@paylife.at.