Mobile Bezahlsysteme sollen Kreditkarte ablösen

Durchbruch auf Raten

Bereits 2013 prognostizierten Gartner und Goldmann Sachs einen rasanten Anstieg des weltweiten Umsatzes, der über mobile Bezahlsysteme getätigt wird. Innerhalb von nur fünf Jahren sollte sich dieser mehr als vervierfachen. Bislang herrscht jedoch nach wie vor in vielen Ländern Skepsis. Mobile Payment im Rahmen dieses Artikels beschreibt einen Bezahlvorgang, der unter Einbeziehung des Smartphones an der Kasse eines Ladengeschäfts stattfindet. Hierbei dient das Smartphone des Kunden in der Regel lediglich als Ersatz für klassische Kredit- oder Debitkarten. Das bedeutet letztlich, dass das Smartphone sich dem Zahlungsterminal des Händlers gegenüber genauso wie eine Plastikkarte verhält. Hierzu nutzt das Smartphone die NFC-Schnittstelle, die seit einigen Jahren für Mastercard PayPass und Visa paywave definiert wurde. Ziel von Mobile Payment ist, das Bezahlen sowohl für Kunden als auch für Händler einfacher, schneller und sicherer zu machen, als es mit den klassischen Kartensystemen der Fall ist.

International ist der Start von Apple Pay im September 2014 als erfolgreichstes Debüt eines mobilen Zahlungssystems zu werten, denn Apple gelang es als erstem Anbieter, die Registrierung und Handhabung sehr einfach zu gestalten. Grund dafür ist eine tiefe Integration in das eigene Ökosystem. Seitdem haben auch Google und Samsung ähnliche Mobile-Payment-Systeme eingeführt, die Apple Pay in der Handhabung, Integration und Einfachheit in nichts nachstehen sollen.

Im Grunde ist die Integration in das jeweilige Ökosystem des Anbieters bei allen drei genannten mobilen Bezahlsystemen gelungen – nur eben in unterschiedlichen Ausprägungen. Google und Apple verantworten ihre mobilen Betriebssysteme und integrieren Android Pay beziehungsweise Apple Pay tief in den jeweiligen Basissystemen. Bei Apple muss noch nicht einmal eine App heruntergeladen werden, sondern Apple Pay ist bereits als zusätzliches Feature in das Betriebssystem eingebaut. Android Pay hin-

gegen ist mehr eine Payment-Schnittstelle des Basissystems, die allen Apps offensteht. Dem Nutzer steht es frei, die Android-Pay-App von Google oder die App eines anderen Anbieters zu verwenden, der die Schnittstelle nutzt. Beispiel für einen solchen Fremdanbieter ist etwa Capital One. Eine Ausnahme im Android-Universum bildet Samsung: Als einer der größten Produzenten von Smartphones bekommt das Unternehmen vor der Auslieferung die Möglichkeit, das Betriebssystem Android anzupassen. Zu diesen Anpassungen zählt zum Beispiel die Entwicklung eigener Benutzeroberflächen aber auch die Integration eigener Apps oder der Apps von Partnern in das Betriebssystem. So erhält auch Samsung die Möglichkeit, Samsung Pay als eigene Android-Pay-Variante bereits vorzuinstallieren und direkt mit seinen Smartphones an die Kunden auszuliefern.

Registrierungsprozess: Aller Anfang ist schwer?!?

Mit dem ersten Start aller Apps ist zunächst die Registrierung eines Zahlungsmittels verbunden. Hierbei handelt es sich in der Regel um Kreditkarten, da diese weltweit gleich funktionieren, während Zahlungssysteme wie die Girocard oftmals in ihrer Reichweite national beschränkt sind. Die Registrierung läuft dabei in drei Schritten ab: Zunächst gibt der Nutzer seine Kartendaten manuell ein oder lässt sie über ein Foto automatisch erkennen. Im zweiten Schritt werden die eingegebenen Daten nochmals dargestellt, um diese durch den Nutzer überprüfen zu lassen. Zuletzt muss noch verifiziert werden, dass die Karte tatsächlich dem Nutzer gehört, der diese verwenden will. Hierzu bietet der Herausgeber dem Nutzer eine oder mehrere Möglichkeiten wie beispielsweise die Eingabe einer TAN oder ein Telefonat zur Prüfung der Identität an. Letzteres war auch der größte Schwachpunkt von Apple Pay, denn oftmals verwenden die Banken leicht fälschbare Abfragen, um den Nutzer zu identifizieren sodass es Kriminellen gelang, geklaute Kreditkarten bei Apple Pay zu hinterlegen.

Registrierungsprozess: Das passiert wirklich

Doch was passiert während der Registrierung neuer Karten tatsächlich alles? Prinzipiell laufen bei allen drei Mobile-Payment-Systemen dieselben Schritte im Hintergrund ab: Zuerst übermittelt der Nutzer die PAN (Personal Account Number) an den Token Requestor (siehe Schritt 1 im Bild). Der Token Requestor ist eine Komponente von Apple, Google oder Samsung, die für die übermittelte PAN einen Token anfordert, der für künftige Zahlungen verwendet wird. Dieser Token wird durch das jeweilige Kreditkartennetzwerk, das in diesem Fall als Token Service Provider auftritt, ausgegeben (Schritt 2). Alternativ können auch dritte Instanzen oder die kartenausgebenden Banken als Token Service Provider auftreten. Doch bevor ein Token ausgestellt wird, stellt der Token Service Provider eine Freigabeanfrage an die kartenausgebende Bank, ob die angegebene Karte für das jeweilige Zahlungssystem verwendet werden darf (Schritt 3). Um die Freigabe zu erleichtern, übermittelt der Token Requestor zusätzliche Informationen an die Bank. Zu diesen Informationen gehören, im Falle von Apple Pay, neben der PAN auch Informationen über das verwendete Gerät, die iTunes-/App-Store-Aktivitäten und den aktuellen Standort. Auch Google und Samsung reichern die übermittelten Daten um ähnliche Informationen an, geben jedoch nicht preis, um welche Informationen es sich im Einzelnen handelt. Die Bank identifiziert den Karteninhaber (Schritt 4) und gibt im Anschluss die Karte für die Nutzung im jeweiligen Zahlungssystem frei (Schritt 5). Der Token Service Provider generiert daraufhin den angeforderten Token, der im Falle von Apple und Samsung über den Token Requestor an das Endgerät übermittelt und dort in einem Secure Element gespeichert wird (Schritt 7). Apple betont in diesem Zusammenhang, dass der Token verschlüsselt übertragen wird und nur das Endgerät diesen Token entschlüsseln kann. Noch nicht einmal Apple selbst kennt den Token. Im Falle von Google wird der Token in der Google-Cloud gespeichert, da aufgrund der Vielfalt an Geräten nicht davon ausgegangen werden kann, dass das Endgerät über ein Secure Element verfügt, in dem die dazu notwendigen Schlüssel sicher gespeichert werden können. Siehe Abbildung 1.

Funktionsweise

Wie funktioniert nun das Bezahlen mit diesen Apps? Auch die Bezahlvorgänge ähneln sich bei den drei Apps. Bei Apple Pay und Google Pay wird der Bezahlvorgang durch das Terminal des Händlers gestartet. Dieses versucht, über seine NFC-Schnittstelle eine Verbindung mit einer kompatiblen Karte herzustellen. Die Smartphones empfangen diese Anfrage und antworten darauf, wie es eine entsprechende Karte (Kredit/Debit) tun würde. Das Terminal erbittet dann die Freigabe der Zahlung, die der Nutzer dann zum Beispiel mit seinem Fingerabdruck an seinem Smartphone erteilt. Daraufhin sendet das Smartphone ein Payment-Token-Objekt zurück, welches unter anderem ein dynamisch generiertes Kryptogramm umfasst, das dem Verifizierungswert (Card Verific - tion Value) einer normalen Karte entspricht. Dieses Objekt enthält neben der Transaktionsnummer auch Daten des Karteninhabers und den zu bezahlenden Betrag. Diese Informationen sind jedoch verschlüsselt und können weder vom Händler noch von Payment Service Providern, sondern nur vom Token Service Provider, also zum Beispiel dem Kreditkartennetzwerk, entschlüsselt werden. Bei Samsung Pay wird der Bezahlvorgang vom Nutzer initiiert. Dieser muss zuerst die App öffnen und sich authentifizi - ren. Danach läuft der Bezahlvorgang genauso ab wie bei den anderen, lediglich die Authentifikation entfällt im weiteren Verlauf, da sie bereits geschehen ist. Da bei Google Pay der Token in der Cloud gespeichert wird und kein Secure Element vorhanden sein muss, werden auch die Daten für die Transaktion dort erzeugt. Um trotzdem offline bezahlen zu können, speichert das Smartphone eine begrenzte Anzahl an „rohen" Bezahl-Token zwischen. Da die Token bei Apple Pay und Samsung Pay auf dem Smartphone gespeichert sind, können auch dort offline Zahlungen durchgeführt werden. Bei Samsung Pay sind jedoch maximal 10 Offline-Zahlungen möglich

Voraussetzungen

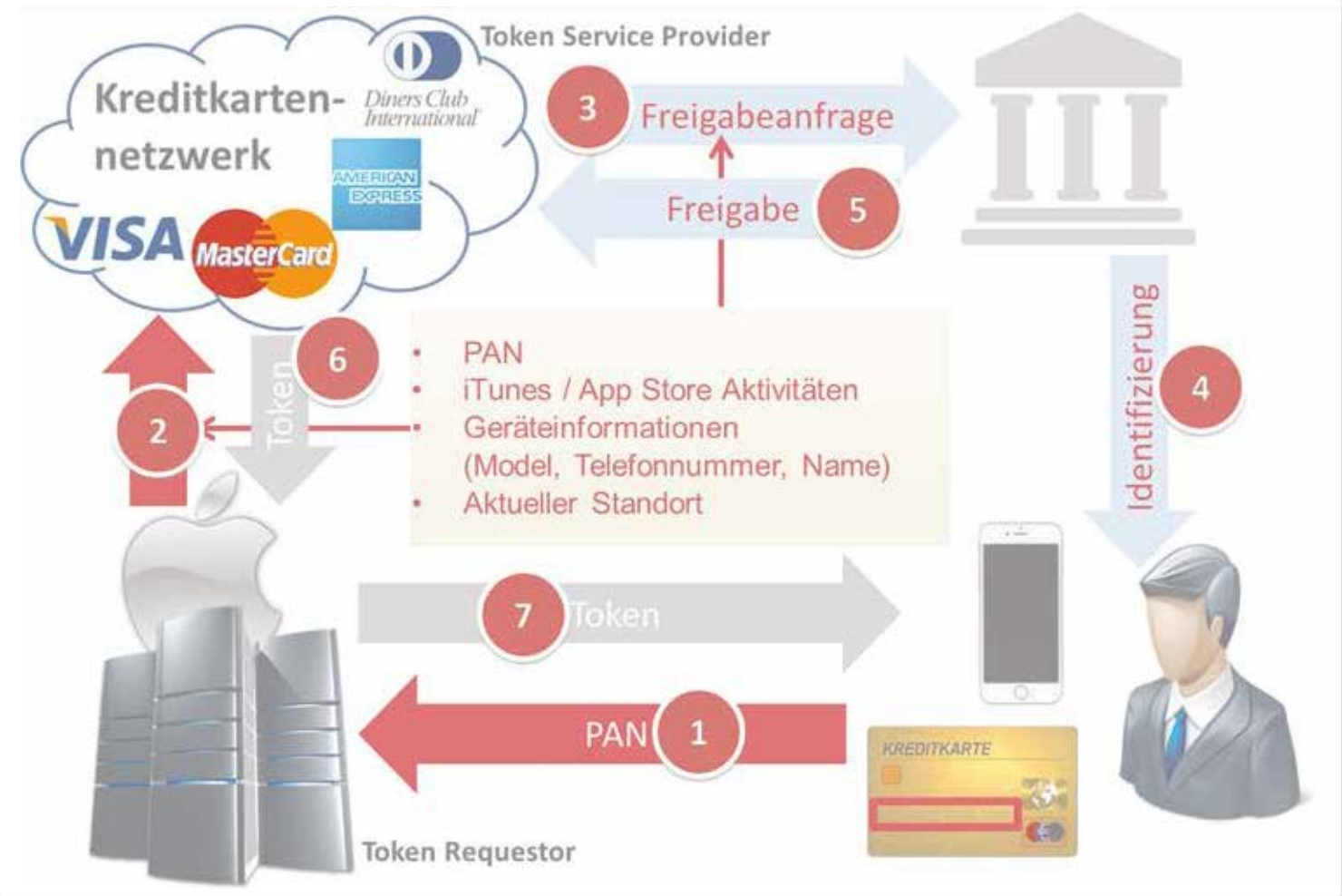
Doch was benötigt eigentlich der Nutzer, wenn er eines der Mobile-Payment-Systeme

nutzen will? Alle drei mobilen Bezahlsysteme haben ähnliche Voraussetzungen. Zum einen sind dies aktuelle Hard- und Software. Bei Apple heißt das mindestens ein iPhone 6 mit mindestens iOS 8.1 oder eine Apple Watch, die auch in Kombination mit einem iPhone 5 genutzt werden kann. Samsung Pay setzt ein Galaxy S6, Galaxy S6 Edge, Galaxy S6 Edge+, Note5 oder eine Gear S2 voraus, wobei diese nicht gerootet sein dürfen. Dass nur nichtgerootete Geräte von Samsung Pay unterstützt werden, hat Sicherheitsgründe: Da auf dem Smartphone sensible Bezahldaten verarbeitet werden und bei gerooteten Smartphones nicht garantiert werden kann, dass keine Schadsoftware Samsung Pay in seiner Funktionsweise einschränkt oder diese Daten abfängt und missbraucht, verbaut Samsung einen sogenannten eFUSE-Chip, der durchbrennt, sobald das Gerät gerootet wird, und dieses so als potenziell unsicher markiert.

Bei Google Pay sind die Anforderungen an die Hardware mit NFC recht einfach. Auf dem Smartphone muss allerdings mindestens Android 4.4 (KitKat) installiert sein, da erst ab dieser Version Host Card Emulation (HCE) enthalten ist, was das Emulieren eines Secure Elements durch das Smartphone erlaubt. Zum anderen wird eine Kredit- oder Debitkarte einer unterstützenden Bank benötigt. In diesem Punkt unterscheiden sich die drei Mobile-Payment-Systeme. Während Apple Pay in den USA von 1.201 Instituten unterstützt wird, ist dies bei Google Pay nur bei 41 Banken und bei Samsung Pay sogar nur bei sechs Banken der Fall. Apple Pay und Google Pay sind auch unabhängig vom Mobilfunkanbieter, Samsung Pay benötigt jedoch die Unterstützung des Mobilfunkanbieters, da dieser eine SIM-Karte mit einem Secure Element bereitstellen muss. Bisher wird dies nur von 5 Mobilfunkanbietern unterstützt. Da alle drei Mobile-Payment-Systeme in etwa gleich ablaufen, unterscheiden sich die Anforderungen an Händler nicht allzu sehr: Für Android und Apple Pay muss lediglich ein NFC-fähiges Terminal vorhanden sein. Samsung Pay funktioniert aufgrund der eingesetzten Magnetic-Secure-Transmission-Technologie zusätzlich auch mit älteren Terminals, die den Magnetstreifen einer Karte auslesen. Solche Terminals sind in den USA aktuell noch weit verbreitet. Somit unterscheiden sich auch die Akzeptanzstellen nicht sonderlich: Alle drei Mobile-Payment-Systeme können an über 1.000.000 Akzeptanzstellen verwendet werden.

Sicherheit und Datenschutz

Was Sicherheit und Datenschutz angeht, gibt es in vielen Ländern noch Bedenken. Da auch Deutschland zu den Ländern gehört, die sich noch ausführliche Prüfungen vorbehalten, wird sich der Start von Android, Apple und Samsung Pay hier sicher noch etwas hinauszögern. Dabei haben die mobilen Bezahlsysteme im Vergleich mit den Kredit- und Debitkarten mit NFC-Schnittstelle auch durchaus Vorteile in Sachen Sicherheit: Anders als die Plastikkarten funken Mobile-Payment-Systeme nicht ständig, machen seinen Nutzer somit auch nicht permanent verfolgbar. Gerade das deutsche Girogo-System ist hier in der Vergangenheit negativ aufgefallen, denn die Plastikkarte ist mit



einfachsten Mitteln über die NFC-Schnittstelle auslesbar. Sie übermittelt dabei in jedem Fall eine eindeutige ID. Hat der Besitzer bereits mit der Karte bezahlt, so sind auch die letzten 15 Transaktionen problemlos auslesbar. Hier sind die Mobile-Payment-Systeme eindeutig im Vorteil.

Allerdings nehmen mit Apple, Google und Samsung weitere Akteure am Bezahlprozess teil, die – so die Sorge potenzieller Kunden – Daten abgreifen können. Diese Sorge ist allerdings zumindest im Falle von Apple und Samsung unberechtigt, denn Apple und Samsung sind in den Bezahlprozess nicht involviert. Die ausgestellten Token werden auf dem jeweiligen Gerät gespeichert, und dort werden auch die notwendigen Bezahl-Token generiert, ohne dies an Apple oder Samsung zu kommunizieren. Lediglich bei der initialen Ausstellung des Tokens sind die Anbieter beteiligt. Allerdings wird der Token verschlüsselt zwischen dem Token Service Provider und dem Endgerät ausgetauscht. Damit sind Apple und Samsung in Sachen Datenschutz auf einem Level mit den klassischen Bezahlkarten.

Anders sieht dies jedoch bei Android Pay aus, denn hier wird der Token in der Google-Cloud gespeichert und der Bezahl-Token bei Bedarf aus der Cloud angefordert. Besteht keine Internetverbindung, kann allerdings auch ein lokaler Token genutzt werden. Google erfährt also im Unterschied zu Apple und Samsung, wann eine Transaktion durchgeführt wird, und kann anhand der Ortungsdienste auch herausfinden wo die Zahlung getätigt wird. In Sachen Datenschutz steht Android Pay also klar schlechter da als die Konkurrenz von Apple und Samsung.

Die Sicherheit aus technischer Perspektive betrachtet ist im Falle von Apple Pay mindestens gut. Denn dadurch, dass Apple das komplette Ökosystem aus Hardware und Software verantwortet und das Sicherheitskonzept Zugriffe auf das Secure Element, die NFC-Hardware und die App Apple Pay für andere Apps einschränkt, ist ein Angriff auf das Bezahlsystem äußerst schwierig. Android hingegen hat kein derart strenges Sicherheitskonzept. Samsung versucht zumindest, den Root-Zugriff zu verhindern. Android Pay hingegen bringt keine derartigen Vorkehrungen mit, da die hierfür notwendige Hardware nicht vorausgesetzt werden kann. Google versucht stattdessen, gerootete Geräte über das Betriebssystem zu erkennen. Da Nutzer nach dem Rooten jedoch Zugriff auf alle Teile des Betriebssystems haben, ist es durch einige Anpassungen auch möglich, Android Pay wieder funktionsfähig zu machen.

Zusammenfassung

Alle drei vorgestellten Mobile-Payment-Systeme sind in der Handhabung recht ähnlich: Der Benutzer fügt Kredit- oder Debitkarten per Bilderkennungsfunktion oder manueller Eingabe hinzu. Hält er sein Smartphone an ein kompatibles Terminal und authentifiziert sich, wird die Zahlung automatisch durchgeführt.

Dabei unterscheiden sich die Mobile-Payment-Systeme jedoch in einigen Punkten: bei der maximalen Anzahl an Karten und der Menge der möglichen Offline-Zahlu - gen. Apple Pay und Samsung Pay limitieren die hinzugefügten Kredit-, Debit-, Treue- und Gutscheinkarten auf acht (Apple Pay) beziehungsweise zehn (Samsung Pay), während Android Pay unbegrenzt viele Karten erlaubt. Dies liegt wahrscheinlich daran, dass die Informationen zur Token-Generierung bei Apple Pay und Samsung Pay auf dem internen Secure Element gespeichert werden, bei Google aber in der Cloud bleiben. Android Pay und Samsung Pay limitieren die Anzahl der möglichen Offline-Za - lungen. Samsung Pay ermöglicht maximal zehn Offline-Zahlungen bei Android Pay sind keine genauen Angaben verfügbar, Berichte sprechen aber von acht bis zwölf Offline-Zahlungen. Apple Pay ermöglicht unbegrenzt viele Offline-Zahlungen

Die Mobile-Payment-Systeme unterscheiden sich auch in ihrem Verbreitungsgrad. Dazu gehören die Länder, in denen das Mobile-Payment-System verfügbar ist, die unterstützten Kredit- und Debit-Karteninstitute und Banken, unterstützende Mobilfunkprovider und verfügbare Akzeptanzstellen. Alle drei Mobile-Payment-Systeme sind in den USA verfügbar. Während Android Pay sich bis dato darauf beschränkt, ist Apple Pay zusätzlich in Kanada, Australien, Großbritannien und China verfügbar, Samsung Pay in Südkorea. Durch die „Tokenisation" ist der Bezahlvorgang zum Großteil standardisiert. Daher unterstützen viele Akzeptanzstellen mehrere, wenn nicht alle der Mobile-Payment-Systeme. Samsung Pay unterstützt jedoch zusätzlich Magnetic Secure Transmission, was die Benutzung herkömmlicher Magnetkartenleser erlaubt. Da diese in den USA sehr verbreitet sind, besitzt Samsung Pay die meisten Akzeptanzstellen.

Bei Apple Pay besitzt nur das restriktive Betriebssystem iOS Zugriff auf den NFC-Chip und dessen Bezahlfunktion sowie das Secure Element. Wird dem Sicherheitskonzept von Apple vertraut, kann auch Apple Pay als sicher betrachtet werden. Die Android-Pay-API steht allen Android-Entwicklern zur Verfügung und erlaubt es ihnen, eigene Payment-Apps zu entwickeln. Ein Beispiel hierfür liefert die Capital One Wallet, welche die API nutzt, um NFC-Zahlungen in die App zu integrieren.

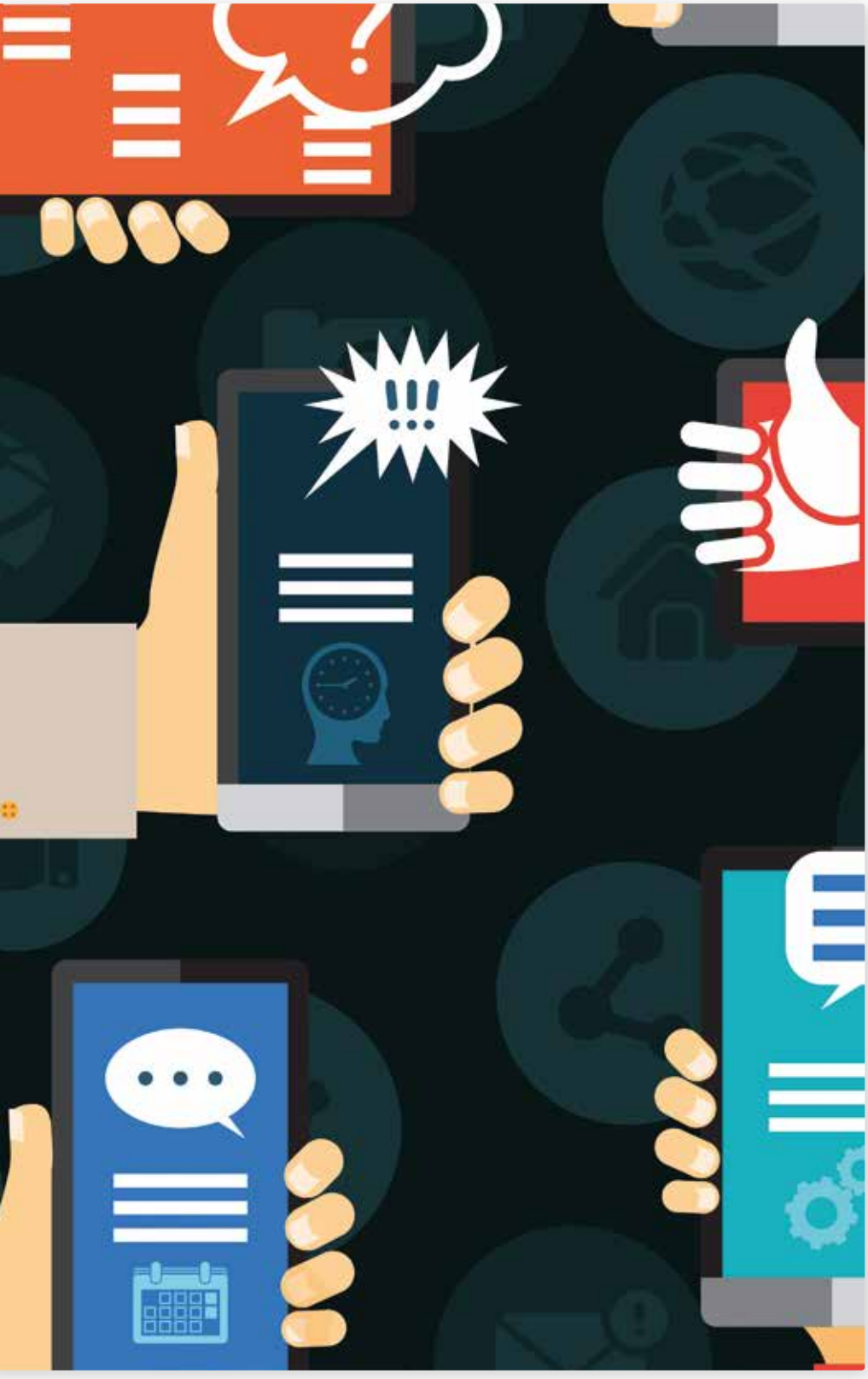
Ausblick für deutsche Nutzer

Doch was bedeutet das für den Nutzer in Deutschland? Keines der genannten Mobile-Payment-Systeme wird bisher auf dem deutschen Markt angeboten. Müssen die Deutschen also derzeit auf Mobile Payment verzichten? Keineswegs! In Deutschland haben seit dem ersten ausgerufenen Durchbruch verschiedene Anbieter versucht, sich auf dem Markt zu etablieren. Der Handelsriese Otto startete 2011 Yapital mit dem Ziel ‚bis 2015 1 Million Nutzer zu gewinnen. Als absehbar war, dass dies nicht gelingen würde, suchte Otto erfolglos einen Käufer für Yapital und beendete das Endkundengeschäft schließlich Anfang des Jahres ganz. Mit paymey entstand ein Crowdfunding-finanzie - tes Mobile-Payment-System, das genau wie Yapital auf QR-Codes setzte. Über eine iOS-App kam paymey jedoch nie hinaus und wurde, noch bevor Partner im Handel gewonnen werden konnten, wieder eingestellt.

Aktuell haben die Mobilfunkanbieter Vodafone, Telekom und Base Wallets entwickelt, die ähnlich wie Apple, Google und Samsung arbeiten. Einen Test von Vodafone Smart-Pass und Base Wallet stellt die PSW Group auf ihren Webseiten zur Verfügung. Parallel bereitet Payback den Start seines Mobile-Payment-Systems vor, das sowohl auf QR-Codes als auch auf NFC basiert. Erste Kommentatoren rufen auch mit dem Start von Payback Pay den großen Durchbruch für Mobile Payment aus. Grund hierfür ist, dass Payback als erster Anbieter auf dem deutschen Markt mit 28 Millionen bereits eine große Anzahl an Nutzern hat – hinzu kommen 8,5 Millionen Downloads der Payback-

App. Außerdem bietet das Unternehmen neben der Bezahlfunktion weitere Mehrwerte wie das Sammeln von Punkten und das Einlösen von Rabattcoupons. Letztlich ist das Rennen um ein erfolgreiches Mobile-Payment-System in Deutschland aber auch nach dem Markteintritt von Payback noch nicht entschieden und die Zukunft wird zeigen, ob und wann ein Durchbruch von mobilen Bezahlsystemen tatsächlich erfolgt.

Sicherlich wäre auch ein deutsches/europäisches eigenständiges Mobile-Payment-System auf der Basis von elektronischen Signaturen nach der neuen europaweiten Verordnung eIDAS eine wirtschaftlich interessante Alternative. Dieses könnte deutlich mehr Unabhängigkeit von US-dominierten Zahlungssystemen bringen und für die Kunden sowie Händler signifikant preisgünstiger werden. ■



JAN-HENDRIK FRINTROP
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Zahlungssystemen und Banktransaktionen.

NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT

TIM ZIEGLER
ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und im Forschungsbereich Zahlungssysteme und Banktransaktionen tätig.