Mobile Wallet

Leitfaden

BITKOM

Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Steffen von Blumröder, Tel.: 030.27576-126, s.vonblumroeder@bitkom.org

Redaktion: Steffen von Blumröder

Gestaltung / Layout: Design Bureau kokliko / Matthias Winter (BITKOM)

Titelbild: © Denys Prykhodov – Fotolia.com

Mobile Wallet

Leitfaden

BITKOM

Inhaltsverzeichnis

Danksagung

Besonderen Dank für die Entstehung dieser Publikation gilt der Arbeitsgruppe Mobile Payments & Banking Innovations des BITKOM Dialogkreises Banking & Financial Services. Insbesondere möchten wir den folgenden Personen für Ihren Input danken:

Steffen von Blumröder
BITKOM e.V.

Sven Korschinowski
KPMG

Raphael Heiner
PwC

Julia Böhm
Deutsche Telekom AG

Med Ridha Ben Naceur
GFT

Dr. Matthias Terlau
Osborne Clarke

Carsten Göbel
Worldline

Mark Rüdiger
Bundesdruckerei GmbH

Michael Titsch
Steria Mummert

Dr. Danny Fundinger
IBM

Ralf Baust
Bottomline Technologies

Arne Linnemüller
PwC

Vorwort

Mobile Wallet kommt! Kommt nicht! In den vergangenen Jahren wurde viel und kontrovers über die Potenziale und das Ökosystem diskutiert.

Allerdings gab es aus BITKOM Sicht viele Berichte, die immer nur einen Teil des Gesamtsystems betrachteten oder Elemente falsch interpretiert haben. Aus diesem Grund haben wir uns in der BITKOM-Arbeitsgruppe Mobile Payments & Banking Innovations dazu entschloßen einen Leitfaden zu schreiben, der sämtliche wesentliche Facetten einbezieht und die Parameter klar definiert.

Natürlich hat der Launch des neuen Apple iPhone neue Dynamik in die Diskussion gebracht, allerdings waren sie nicht die ersten, die auf Near Field Communication (NFC) als Übertragungsschnittstelle setzten. Denn bereits seit geraumer Zeit haben sich andere Smartphone Hersteller wie Samsung, HTC und LG NFC im Markt etabliert. Wichtig bleibt dies aber ganz bestimmt, denn NFC wird hier zum Game Changer und stellt für BITKOM die Schlüsseltechnologie dar, um dem Thema Mobile Wallet die nötige Dynamik zu verleihen.

In kaum einem anderen Markt tummeln sich derzeit so viele Player aus den unterschiedlichsten Branchen. Ob Telekommunikationsunternehmen, stationäre- und Onlinehändler, Banken oder Anbieter von Zahlungssystemen, sie alle positionieren sich in diesem hoch dynamischen Umfeld, um neue Produkte und Dienstleistungen an den Mann und an die Frau zu bringen.

Noch sind einige Herausforderungen zu lösen, aber das Potenzial für Mobile Wallet ist gigantisch. Viele Anwendungsmöglichkeiten und Vereinfachungen des täglichen Lebens sind noch gar nicht erdacht oder umgesetzt. Es geht um nichts weniger als die physische Brieftasche zu ersetzen und ihren Anwendungsradius durch Digitalisierung und Verknüpfung zu erweitern.

Mit unserem Leitfaden Mobile Wallet möchten wir Ihnen einen Überblick über dieses komplexe Ökosystem und seine großen Potenziale geben und die einzelnen Bestandteile klar definieren und deutlich voneinander abgrenzen. Wallet ist nämlich nicht gleich Wallet.

Steffen v. Blumröder

Berlin, Oktober 2014

1 Executive Summary

Die Digitalisierung hat in den vergangenen Jahren fast sämtliche Branchen durch disruptive Anwendungen auf den Kopf gestellt. Die Mobile Wallet bildet hier keine Ausnahme und die Zukunftsvision der Unternehmen, die dieses Ökosystem vorantreiben, ist klar definiert: Der physische Geldbeutel soll digitalisiert und bereits digitalisierte Produkte und Dienstleistungen einfach integriert werden.

In vielen Veröffentlichungen gibt es aus BITKOM-Sicht eine unzureichende Definition was eine Mobile Wallet wirklich darstellt. Mobile Wallet wird oftmals mit einer Digital Wallet gleich gesetzt, aber Wallet ist nicht gleich Wallet. Wir geben eine klare Definition der Mobile Wallet und grenzen diese deutlich von der digitalen Wallet oder anderen synonym genutzte Begriffen ab. In den aktuellen Definitionen werden entweder nur Teilelemente rund um den Zahlungsvorgang betrachtet oder der unterschiedliche Nutzungskontext vernachlässigt. Generell muss man unterscheiden, ob die Mobile Wallet Dienste im Proximity- (physische Akzeptanzstelle) oder im Remote- (über das Web) Kontext zu verstehen sind.

Der BITKOM versteht unter einer Mobile Wallet eine offene Plattform auf einem mobilen Endgerät, die es ermöglicht verschiedene Dienste zur Authentifizierung, Identifikation und Digitalisierung von Wertgegenständen in Proximity-Szenarien zu nutzen und zu kombinieren. Dazu zählen Zahlfunktion (Debit- und Kreditkarten, Lastschriften, etc.), die Identifizierung der persönlichen Identität (Personalausweis, Führerschein, Krankenkassenkarte, Mitarbeiterausweis), Zugangsberechtigungen (Schlüssel, Tickets, etc.) sowie beliebig viele Mehrwertfunktionen und Dienstleistungen (Kundenbindungsprogramme, Couponing, Voucher, etc.), als auch Geld in digitalisierter/virtueller Form. Gemein ist allen diesen Diensten, dass sie Werte und sensible persönliche Daten des Anwenders enthalten, so dass Sicherheit und Zugriffsschutz von elementarer Bedeutung sind. Die Sicherheitsanforderungen einzelner Dienste können sich dabei allerdings stark unterscheiden (Personalausweis vs. Coupon). Als standardisierte Übertragungstechnologie wird überwiegend Near Field Communication (NFC) zum Einsatz kommen, aber auch direkte Webanbindung wie z. B. bei Mobile Ticketing. Andere Technologien wie Bluetooth Low Energy (BLE) oder Qick Response Code (QR Code) bleiben wichtig, sind aber zukünftig in erster Linie nicht für die Übertragung zwischen Smartphone und Kasse verantwortlich, sondern erweitern die Möglichkeiten für weitere Zusatzfunktionen und Angebote.

Einige mobile Anwendungen wie Mobile Ticketing, Couponing oder Access sind heute schon gängig. Und auch kontaktloses Bezahlen über NFC Chips ist heute bereits an rund 40.000 Standorten in Deutschland möglich. Allein, es fehlte der übergreifende und interagierende Schirm in Form der Mobile Wallet, um die Dienste mehrwertstiftend digital vorzuhalten und mit einander zu verknüpfen. Insgesamt wird es für den Endverbraucher dann einfacher, bequemer, sicherer und es wird endlich auch mehr Alternativen zum Bezahlen am PoS bieten.

Die für einen massenfähigen Markt benötigte Infrastruktur aus entsprechenden Smartphones und stationären Akzeptanzstellen, war bis dato nicht vorhanden, sodass es in der Vergangenheit gar nicht möglich war die Mobile Wallet flächendeckend einzusetzen. Doch dies ändert sich aktuell!

Betrachtet man sämtliche aktuellen Studien und Umfragen zum Thema, dann gehen alle in den kommenden Jahren von einer schnellen Marktdurchdringung und teilweise sogar von explosiven Wachstumsraten in Deutschland und Europa aus. Natürlich wird Bargeld nicht verschwinden, aber der Anteil wird deutlich schneller zurückgehen als dem bisherigen 1 Prozent pro Jahr.

2 Einleitung

Im Kontext der stetigen Digitalisierung von Dienstleistungen und Produkten wird das Thema Mobile Wallet seit längerer Zeit intensiv diskutiert. Nahezu täglich erscheinen Berichte und Nachrichten, über neue Anbieter, Konzepte und Lösungen rund um das mobile Bezahlen in den Medien.

Auch wenn der Begriff Mobile Wallet teilweise synonym mit den Begriffen mobiles Bezahlen (Mobile Payment) oder mobiles Banking (Mobile Banking) verwendet wird, beinhaltet die Mobile Wallet weit mehr: Sie integriert als digitaler aber mobil nutzbarer »Aufbewahrungsort« verschiedene Funktionen, Produkte, Dienstleistungen und ersetzt bzw. digitalisiert so die physische Brieftasche. Nutzbar wird die Mobile Wallet in der Regel über eine Software-Applikation (App), auf dem mobilen Endgerät (Mobile Device), z. B. Smartphone, Tablet, Phablet, Smartwatch und sonstige sogenannte tragbare Geräte (Wearables). Software alleine reicht jedoch für die Nutzung nicht aus. Insofern gewährt die Software nur den Zugriff auf die Mobile Wallet. Nur im Zusammenspiel mit den entsprechenden Hardware-Komponenten (das Gerät selbst sowie die im Geräte verbauten Transponder-(Chips) der Antenne, der SIM-Karte, des Secure Elementes, des Prozessors sowie gegebenenfalls der verwendeten Sensoren oder Kamera), wird die Mobile Wallet nutzbar.

Als wesentliche zu digitalisierende Funktionen kommen die Zahlfunktion (Debit- und Kreditkarten, Lastschriften, etc.) die Identifizierungs- und Autorisierungsfunktion (Personalausweis, Führerschein, Krankenkassenkarte, Mitarbeiterausweis), die Zugangsberechtigungen (Schlüssel, etc.), sowie beliebig viele Mehrwertfunktionen und Dienstleistungen (Kundenbindungsprogramme, Couponing und Voucher, Ticketing, etc.) in Betracht.

Damit wird die Mobile Wallet zur »All-in-One-Lösung«, die neben Ausweispapieren, Bargeld und Karten auch sämtliche anderen physischen Medien überflüssig macht. Sie bietet dann die Möglichkeit, alles digital zu verwalten, zu nutzen und miteinander zu kombinieren. Zur Komplettierung eines umfassenden Service werden dabei auch vor- und nachgelagerte Prozessschritte wie z. B. Transaktionen (Bestellungen), Bewertungen, Statusübersichten und Auswertungen berücksichtigt.

Trotz der derzeitig positiven Entwicklungen sind wir noch ein Stück von einer integrierten Lösung oder der flächendeckenden Nutzung entfernt. Aktuelle Angebote sind teilweise noch sehr jung, decken nur Teilfunktionen (z. B. den Zahlungsverkehr, Kundenbindungsprogramme, Couponing oder Ticketing) ab, oder entwickeln nicht die notwendige Reichweite bei den (End-) Nutzern.

Interface	Software	Mainboard	Sensor	Network
Dock Connector	OS	CPU	Gyrometer	GSM/Edge
Camera/Flash	Browser	SIM	Ambient light sensor	UMTS/LTE
Microphone	Appstore	Memory	Proximity sensor	WiFi
Speaker	Widgets	GPS	Accelerometer	Bluetooth
Camera/Flash	Cloud	Compass	Gesture Recognition	NFC
Microphone				
Speaker				
Display				

Abbildung 1: Smartphone Komponenten im Zusammenspiel mit der Mobile Wallet; Quelle: PwC

Darüber hinaus fehlt es an ausreichender Standardisierung. Um diesen Herausforderungen zu begegnen, schließen sich daher einige Lösungs- und Serviceanbieter in Kooperationen zusammen, um die Reichweite und den Funktionsumfang zu erhöhen. Wie die Vergangenheit zeigt, reicht dies aber noch nicht aus, um die notwendige Marktdurchdringung zu erreichen oder die Nutzer zur Adaption der neuen Technologie zu bewegen. Zentrale Adaptionshindernisse sind insbesondere in Deutschland noch das fehlende Vertrauen in die neuen technologischen Möglichkeiten (Digital Trust) sowie das immer noch fehlende Verständnis im Umgang mit der Technologie. Hier müssen Lösungsanbieter noch viel Aufklärungsarbeiten (Digital Education) leisten.

Die Gründe für die andauernde Diskussion zum Thema Mobile Wallet liegen zum einen in der Begriffsunschärfe des Themas, zum anderen in der Komplexität der mit der Mobile Wallet assoziierten Funktionen und Dienstleistungen. Darüber hinaus wird die Mobile Wallet häufig aus der Perspektive der einzelnen Stakeholder interpretiert und definiert. Entsprechend variieren Merkmalsausprägungen und damit die Definition der Mobile Wallet.

Zusätzlich versuchen sich verschiedene z.T. bisher branchenfremde Dienstleister entlang der Wertschöpfungskette der Mobile Wallet zu etablieren. Bestandteil dieses neuen, dynamischen Ökosystems können zum Beispiel Mobilfunkanbieter (MNOs), Karten-Netzbetreiber, Hersteller von mobilen Endgeräten, Chiphersteller, Banken, (Online)-Händler, Systemausrüster, Agenturen, Betreiber von Betriebssystemen (z. B. Apple, Google, Microsoft), Cloud-Anbieter und viele weitere Service-Dienstleister sein.

Neben den vielen Beteiligten der Wertschöpfungskette, spielen auch die technologischen Entwicklungen im Bereich (Netz-) Infrastruktur, Hardware, Software, IT-Security und Mobile Wallet-Applikationen eine zunehmend große Rolle. Nicht zuletzt muss aber auch die in Deutschland bzw. der Europäischen Union zunehmende Regulation in den Bereichen Wettbewerb, Datenschutz und -Sicherheit, Telemedien, Netzinfrastruktur, Zahlungsverkehr und Finanzmarkt berücksichtigt werden.

Unser Mobile Wallet Leitfaden baut auf dem BITKOM Positionspapier Mobile Payments[1] auf und stellt erstmalig einen umfassenden Überblick über den Nutzen, die Funktionen, das Ökosystem und die Rahmenbedingungen sowie die Wertschöpfungskette einer Mobile Wallet dar.

In Bezug auf den Nutzungskontext der Mobile Wallet muss man grundsätzlich zwei Bereiche unterscheiden:

- Proximity-Kontext: den Einsatz der Mobile Wallet an einem direkten physischen Gegenüber oder Akzeptanzstelle wie z. B. an einem stationären Point-of-Sale im Supermarkt, der Ticketkontrolle im Zug durch einen Kontrolleur, oder das Öffnen einer Tür an einer Zugangskontrolle

- Remote-Kontext: den Einsatz gegenüber einem »entfernten« oder virtuellen Gegenüber, wie einem online Point-of-Sale oder der Authentifizierung eines Web-Zugriffs (Remote-Einsatz).

Diese Unterscheidung ist zentral für das Verständnis der Funktionen und der Einsatzmöglichkeiten der Mobile Wallet, da sich je nach Anwendungs- oder Nutzungskontext, Funktionen, Prozesse, Infrastruktur und damit Nutzungsszenarien deutlich unterscheiden. Darüber hinaus lässt sich damit die derzeit noch bestehende Unschärfe hinsichtlich der Definition von Wallets in mobile und digitale Wallets erläutern (vgl. Kapitel 3). Allerdings konvergieren beide Konzepte immer mehr, so dass zu erwarten ist, dass es zukünftig keiner Unterscheidung mehr bedarf. Dies ist insbesondere aus Sicht des Endnutzers zu begrüßen. Für ihn ist es in der Regel uninteressant, welche technologischen, häufig infrastrukturellen Unterschiede beim Einsatz bestehen. Für den Nutzer und Kunden zählt letztlich

1 http://www.bitkom.org/de/themen/74457_75503.aspx

nur eine Mehrwert erzeugende Benutzerfreundlichkeit (Usability), eine zufriedenstellende Verbreitung bzw. Akzeptanz und Transaktionssicherheit.

Im Kontext dieses Leitfadens wird der Einsatz der Mobile Wallet daher vorwiegend am stationären Point of Sale und der Nutzung von sogenannten Proximity Diensten diskutiert. Während viele Unternehmen schon erfolgreiche Lösungen am online Point of Sale etabliert haben, bietet der stationäre Point of Sale noch enormes WachstumsPotenzial, ist er doch bis dato Bargeld-dominiert und papierbehaftet.

Neben der Darstellung von möglichen Anwendungsszenarien und Diensten, dem technologischem Funktionsumfang, der Wertschöpfungskette, des Ökosystems sowie der sich ergebenden Herausforderungen und Potenziale erläutert der Leitfaden auch den regulatorischen Rahmen für den Einsatz bzw. die Nutzung der Mobile Wallet, der durch die Europäische Union (EU), das European Payment Council (EPC) und der Europäischen Zentralbank (EZB) vorgegeben wird.

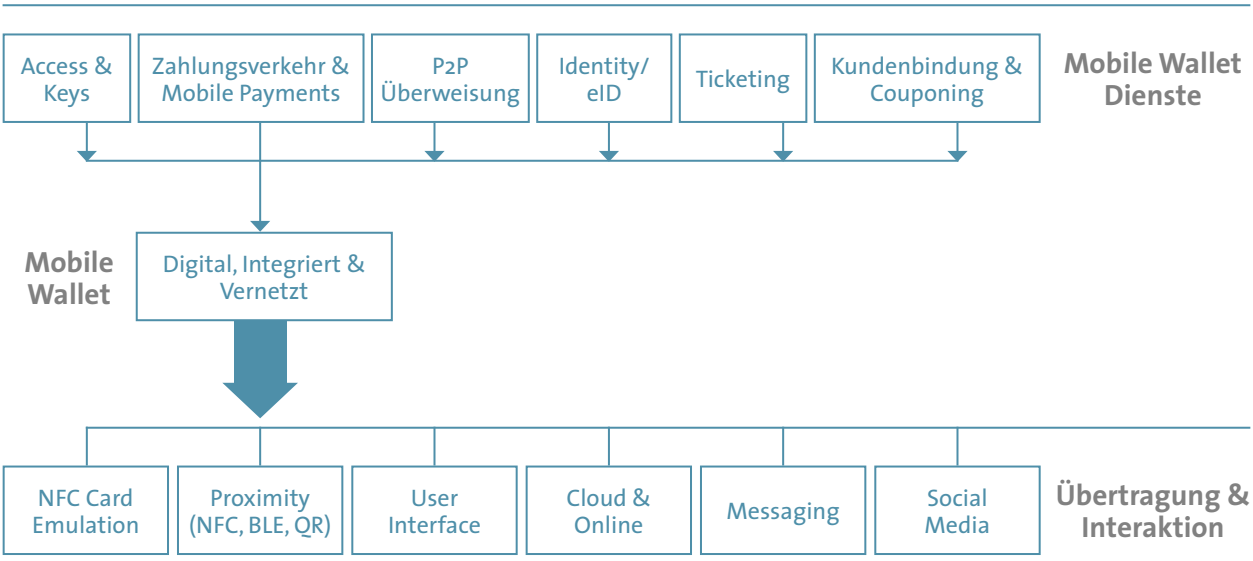

Abbildung 2: Die Mobile Wallet. Smarte Dienste integrieren und Interaktion neu gestalten; Quelle: eigene Abbildung

3 Definition der Mobile Wallet und Abgrenzungen

Aus BITKOM-Sicht ist es zum Verständnis des Nutzungskontexts der Mobile Wallet erforderlich, sie von dem Konzept der Digital Wallet und bestehender Hybrid-modelle abzugrenzen.

3.1 Definitionen einer Mobile und Digital Wallet

Aus Sicht des BITKOM sowie der Erfahrung und Wahrnehmung der Mitglieder der Arbeitsgruppe Mobile Payments wird die Mobile Wallet häufig entweder aus der jeweiligen Industriesicht, oder aus technologischer Sicht, selten aber aus Nutzersicht definiert. Festzustellen ist insoweit, dass sich die Definitionen teilweise unterscheiden, teilweise aber auch überschneiden. Die Begründung dieser Unterscheidung bzw. Überschneidung liegt regelmäßig am unterschiedlich interpretierten Funktions- bzw. Nutzungsumfangs der Wallet. So fokussiert z. B. der Finanzsektor überwiegend auf den Zahlungsverkehr und Banktransaktionen. Die Mobilfunkanbieter und Netzbetreiber auf Mehrwertdienste rund um ihr Kerngeschäft (Zahlungsverkehr, Air-Time Top-Up, Location Based Services) und Technologieanbieter auf Technologie und Services (unter anderem Bereitstellung der Wallet als Cloud-basierter Service). Da es derzeit keine allgemein verbindliche oder anerkannte Definition einer Mobile Wallet gibt, hat der BITKOM eine eigene Definition formuliert, die die Mobile Wallet anhand des Nutzungskontext, der Übertragungstechnologie und der PoS Lokation definiert. Zur besseren Einordnung haben wir die BITKOM-Definition den gängigen Definitionen der Marktteilnehmer gegenüber gestellt.

Außer Betracht bleiben aufgrund des unterschiedlichen Nutzungszusammenhanges und der unterschiedlichen Infrastruktur Wallet-Modelle (von Mobilfunknetzbetreibern wie Millicom, Safaricom/Vodafone, Airtel, Singtel, etc) aus Entwicklungs- und Schwellenländern, die derzeit noch unter dem Begriff mobile Finanzdienstleistungen (Mobile Financial Services) zusammengefasst werden können (z. B. m-pesa, Pago, m-Pago, etc.). Darüber hinaus werden Anwendungsfälle für Featurephones nicht diskutiert.

3.1.1 Mobile Wallet Definition des BITKOM

Der BITKOM versteht unter einer Mobile Wallet eine offene Plattform auf einem mobilen Endgerät, die es ermöglicht verschiedene Dienste zur Authentifizierung, Identifikation und Digitalisierung von Wertgegenständen in Proximity-Szenarien zu nutzen und zu kombinieren. Dazu zählen Zahlfunktion (Debit- und Kreditkarten, Lastschriften, etc.), die Identifizierung der persönlichen Identität (Personalausweis, Führerschein, Krankenkassenkarte, Mitarbeiterausweis), Zugangsberechtigungen (Schlüssel, Tickets, etc) sowie beliebig viele Mehrwertfunktionen und Dienstleistungen (Kundenbindungsprogramme, Couponing und Voucher, etc.) als auch Bargeld in digitalisierter/virtueller Form. Gemein ist allen diesen Diensten, dass sie Werte und sensible persönliche Daten des Anwenders enthalten, so dass Sicherheit und Zugriffsschutz von elementarer Bedeutung sind. Die Sicherheitsanforderungen einzelner Dienste können sich dabei allerdings stark unterscheiden (Personalausweis vs. Coupon).

3.1.2 Definition einer Mobile Wallet des Mobey Forum

Das Mobey Forum[2] definiert die Mobile Wallet als Funktionalität auf einem mobilen Endgerät, die eine sichere Interaktion mit digitalisierten Wertgegenständen

2 Das Mobey Forum ist ein global agierender Interessensverband von Banken und anderen Finanzinstituten mit dem Ziel, zukünftig eine führende Position in mobilen Finanzgeschäften einzunehmen http://www.mobeyforum.org/about-us/

ermöglicht. Die Mobile Wallet kann sich auf einem mobilen Gerät oder auch auf einem Remote-Netzwerk bzw. sicheren Server befinden. Der Zugriff, die Steuerung und die Nutzung erfolgt über das mobile Gerät. Die Steuerung erfolgt immer durch den Wallet-Inhaber. Die Mobile Wallet kann einen breiten Funktionsumfang haben und unterschiedliche Wertgegenstände enthalten. Aus Marktsicht interpretiert das Mobey Forum die Mobile Wallet als offenes Plattformsystem, an dem die verschiedenen Dienstleiter ihre Dienste anbieten können. Inwieweit es sich um ein generisches, ggf. zentral verwaltetes System oder mehrere parallel bestehende (Provider-) Systeme handelt, bleibt offen[3].

3.1.3 Mobile Wallet Definition der GSMA Association

Die GSMA[4] definiert die Mobile Wallet aus Sicht der Mobilfunkanbieter und Netzbetreiber und zielt dabei auf die Übertragungstechnologie ab. Insofern definiert sie die Mobile Wallet als Applikation die es ermöglicht, das durch den MNO zur Verfügung gestellte Dienstleistungsportfolio auf einem mobilen Endgerät mit der Near-Field-Technologie (NFC) zu nutzen. Dabei schließt sie nicht aus, dass auch andere Dienstleister Mehrwertdienste über die Mobile Wallet anbieten können.

Die Kerneigenschaften der Mobile Wallet sollten immer interoperabel sein und dem Benutzer die Möglichkeit bieten, bestimmte NFC-Dienste anderen vorzuziehen, wie z. B. der Gebrauch präferierter Zahlungsinstrumente. Im Gegensatz zum Mobey Forum definiert die GSMA die Mobile Wallet damit nicht als offene Plattform, sondern als individualisierte (Mehrwert-) Applikation die einem Kunden im Rahmen eines konkreten Dienstleistungsverhältnisses zwischen MNO und dem Kunden zur Verfügung gestellt wird und über die Systeme des jeweiligen MNO provisioniert werden. Dienstleistungen von Drittanbietern können durch zur Verfügung gestellte Schnittstellen (API) und SDK integriert werden. Letztlich ist der jeweilige MNO für die Plattform verantwortlich, auf der die Mobile Wallet dem Kunden zur Verfügung gestellt wird. Als zentrale Übertragungstechnologien kommen NFC sowie traditionelle Funkübertragung in den Bandbreiten des jeweiligen Mobilfunknetzes in Betracht[5].

3.1.4 Definition der Digital Wallet des European Payment Council

Der European Payment Council (EPC) interpretiert die Digitale Wallet im Wesentlichen aus Sicht des Zahlungsverkehrs sowie der notwendigen Vereinheitlichung des europäischen Zahlungsverkehrsraums. Insoweit kann der Versuch einer Definition der Digital Wallet durch den EPC als konsequente Fortsetzung der Bemühungen um ein einheitliches Zahlungsverkehrsverständnis gesehen werden. Oder plastisch ausgedrückt: Vereinheitlichung des europäischen Zahlungsverkehrs mit digitalen Mitteln.

Insofern stellt die Digital Wallet aus Sicht des EPC eine digitale Verwaltung von Identifikationsmechanismen, digitalen Signaturen und Zertifikaten dar, die dazu berechtigen, Transaktionen zu autorisieren, Informationen freizugeben oder Zugriff zu erlauben. An die jeweiligen (persönlichen) Identifikationsmechanismen sind auch die ebenfalls in der Wallet hinterlegten Zahlungsarten geknüpft. Darüber hinaus können digitalisierte Wertgegenstände und Einheiten (z. B. Coupons, virtuelle Währungen), Inhaber- und Urheberrechte (z. B. Bilder, Marken, Lizenzen, Mandate), biometrische Daten, Dokumente, Kundenbindungsprogramme des Wallet-Inhabers mit der digitalen Identifikation (e-ID) verknüpft werden. Das EPC definiert die digitale Wallet damit als Meta-Applikation mit Fokus auf der Verwaltung und der Sicherheit von Identifikation und Autorisierung, ohne jedoch auf Operabilität und den spezifischen Nutzungskontext bzw. Anwendungsbereich einzugehen[6].

3 Mobey Forum White Paper Seite 1ff 2011
4 GSMA ist eine globale Interessensvertretung von Mobilfunkunternehmen http://www.gsma.com/aboutus/history
5 GSMA White Paper Mobile Wallet: http://www.gsma.com/digitalcommerce/wp-content/uploads/2012/10/GSMA-Mobile-Wallet-White-Paper-Version-1-0.pdf
6 White Paper Mobile Wallet Payments, EPC163-13 v.20, http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/white-paper-mobile-payments-edition-october-2012/

3.2 Mobile- vs. Digital Wallet

Originär werden Mobile Wallets aus Sicht des Kunden bzw. Nutzers in Proximity-Szenarien eingesetzt. Digital Wallets hingegen in Remote-Szenarien. Diese Unterscheidung hat einen maßgeblichen Einfluss auf den Nutzungskontext der Wallet sowie die benötigte Zugangs-, Transaktions-, und Übertragungstechnologie. Insofern lassen sich digitale Wallets und mobile Wallets nach Auffassung des BITKOM an diesen Kriterien unterscheiden. Während sich die digitale Wallet und deren begrifflicher Vorläufer die e-Wallet, aus dem klassischen e-Commerce (Online-Handel) entwickelt hat und als Lösung zur Bezahlung in Online-Szenarien verstanden werden kann, so hat sich die Mobile Wallet aus dem Einsatz von NFC-Technologie und QR Code zur Bezahlung am stationären PoS entwickelt, einem ganz anderen Nutzungskontext also. Wie in der Einleitung bereits vorangestellt, geht der BITKOM jedoch von der zunehmenden Konvergenz von Digital- und Mobile Wallets aus, so dass eine Unterscheidung zukünftig obsolet wird. Bis jedoch eine, in Bezug auf den PoS, lokations- und geräteunabhängige Wallet realisiert wird, wird es noch dauern.

Beide Wallet-Konzepte basieren auf einer technischen Infrastruktur, die eine sichere Speicherung, Verarbeitung und Kommunikation von Informationen des Inhabers, des Anbieters und des Service-Providers ermöglichen. Dabei können alle Funktionalitäten direkt oder über einen Remote-Zugriff bereitgestellt werden. Zugang zu einem oder mehreren Diensten wie z. B. Zahlungsverkehr, erhält der Verbraucher bzw. Nutzer, indem er sich über eine Applikation mit Username und Passwort authentifiziert. Über eine gesicherte Verbindung zwischen Endgerät und Server wird der Prozess dann initiiert und durchgeführt, ggf. ergänzt um eine Zwei-Faktor-Authentifizierung.

Sowohl auf die Digital Wallet als auch auf eine Mobile Wallet kann über ein mobiles Gerät (Smartphone, Tablet etc.) zugegriffen werden. Neben Zahlungsdiensten können weitere Anwendungen und Dienstleistungen verwaltet und genutzt werden. Dabei können alle Funktionalitäten direkt auf dem mobilen Gerät oder über einen Remote-Zugriff bereitgestellt werden.

Der Anbieter stellt die Funktionalitäten bereit, die der Wallet-Inhaber nutzt. Die Transaktionsautorisierung erfolgt im Gegensatz zur Digital Wallet bei der Mobile Wallet auf Basis von persönlichen Daten (u.a. Identifikation) und Sicherheitsmerkmalen, die auf einem Chip verschlüsselt gespeichert sind. Das Speicherelement dieser Daten wird herkömmlich als Secure Element bezeichnet, und entspricht einem Smartcard-Chip. Die Verwendung des Secure Element ermöglicht insbesondere die Emulation von Smartcards über NFC, und somit auch die Wiederverwendung der entsprechenden Infrastrukturen. Dieses Secure Element kann sich entweder auf der SIM-Karte des Mobilfunknetzbetreibers, dem geräteabhängigen NFC-Chip, einer externen SD-Karte oder in der Cloud befinden. Die Technik zur Emulation des Secure Elements in der Cloud wird Host Card Emulation (HCE) genannt und soll insbesondere die Notwendigkeit eines zusätzlichen Hardware-Elements im Smartphone, und die Abhängigkeit von dessen Inhaber im Bereich der NFC-Technologie überwinden. Bei der Mobile Wallet (Proximity) erfolgt die Datenübertragung (Autorisierung, Transaktion) Dank Smartcard-Emulation über die Annäherung des mobilen Endgerätes an einen NFC-Empfänger (z. B. PoS-Terminal an der Kasse).

Im Unterschied dazu werden bei einer digitalen Wallet die Nutzerdaten in einer gesicherten Umgebung auf den Servern des Anbieters (Providers) gespeichert. Ein Secure Element kommt nicht zum Einsatz, und daher ist auch keine Smartcard-Emulation möglich. Digitale Wallets kommen hauptsächlich zur Abwicklung von Zahlungen im E-Commerce zum Einsatz. Die Herausforderung beim Einsatz von Digital Wallets in Proximity Szenarien ist die fehlende Konnektivität mit stationären PoS, da keine Smartcard-Emulation möglich ist, und eine E-Payment Transaktion durchgeführt werden muss, die auch eine Online-Verbindung für die Bezahlung voraussetzt. Gerade in strukturschwachen Gebieten kann dies oft nicht gewährleistet werden.

Beide Wallet-Ansätze haben Vor- und Nachteile: So sind Mobile Wallets auf Basis einer NFC-Schnittstelle generell auf ein Secure Element und eine NFC-Schnittstelle angewiesen, die beide nicht in allen Mobiltelefonen technisch

integriert sind. Dafür sind aber auch offline Transaktionen möglich. Bei digitalen Wallets ist die Benutzung generell unabhängig vom Endgerät möglich, Voraussetzung ist aber eine Verbindung zum Internet und die Integration neuer Schnittstellen in die Kassensysteme der Händler. Eine weitere Konsequenz bei digitalen Wallets: einfaches Tappen wie bei NFC ist nicht möglich. Die Digital Wallet ist somit für den stationären PoS derzeit weniger nutzerfreundlich und die Bezahlung deutlich zeitintensiver. Hinzu kommt, dass aufgrund der vorgesehenen Regulierung für die Autorisierung von Transaktionen über 25 Euro bzw. bei cloudbasierten Verfahren auch darunter, jeweils zwei »Identifier« PIN/TAN, PIN/PIN oder biometrische Identifikation zuzüglich PIN erforderlich sind (vgl. auch Kapitel 7). Dies schwächt die Akzeptanz beim Handel, bei dem es an der Kasse auf jede Sekunde ankommt.

3.3 Weitere Begriffsdefinitionen

Der Begriff Mobile Wallet wird in vielen Beiträgen und Diskussionen oft im Zusammenhang mit Begriffen wie Mobile Payment, Mobile Commerce oder Mobile Banking verwendet oder gar synonym genutzt. Insofern geht es darum, exemplarisch die genannten Begriffe kurz zu erklären und den Merkmalen einer Mobile Wallet gegenüberzustellen, die im vorigen Abschnitt dargestellt worden sind.

- M-Commerce: Hierunter fallen alle Transaktionen, die einen Austausch von Rechten oder Eigentum an Gütern oder Dienstleistungen beinhalten und die mit einem mobilen Endgerät initiiert und oder abgeschlossen worden sind und dies unabhängig von der Übertragungstechnologie

- M-Payment: Bezahlvorgänge, bei denen mindestens der Zahlungspflichtige mobile elektronische Techniken zur Initiierung, Autorisierung oder Realisierung der Zahlung einsetzt, etwa mittels mobiler Geräte wie Smartphone oder Tablet und dies grundsätzlich unabhängig von der Übertragungstechnologie

- M-Banking: Abwicklung von Bankgeschäften, die unter Zuhilfenahme von mobilen Endgeräten wie Smartphone oder Tablet stattfindet

In Bezug auf die Mobile Wallet-Definition des BITKOM kann man festhalten, dass sämtliche Begriffe einzelne Dienste einer Mobile Wallet darstellen, aber eigenständig sind. Die Aufzählung kann allerdings nicht abschließend sein, da der Markt sehr dynamisch ist und immer wieder neue Begriffe mit der Mobile Wallet assoziiert werden und entsprechend ihrer Charakteristika unter der Mobile- oder der Digital Wallet subsumiert werden können. Nach BITKOM-Auffassung ist dies jeweils im Kontext des Nutzungszusammenhanges sowie der damit verbundenen Technologie zu entscheiden.

3.4 Zusammenfassung

Das Kapitel hat gezeigt, dass Wallet nicht gleich Wallet ist. Die Definitionen unterscheiden sich erheblich voneinander. Einzig BITKOM zeigt daher mit der Orientierung nach drei wesentlichen Merkmalen eine eindeutige und ganzheitliche Sichtweise:

- Nutzungskontext
- Übertragungstechnologie
- Lokationskontext

Keine andere Definition konnte dies ausreichend darstellen, sondern betrachtet immer nur Teilaspekte. Auch die Abgrenzung zu den weiteren Begrifflichkeiten wird dem Interessierten ein besseres Verständnis geben. Dies ist wichtig, um einzelne Sachzusammenhänge klar voneinander zu trennen und nicht miteinander zu vermischen. Ergänzend sind im Anhang weitere Wallet Konzepte zu finden wie z. B. vertikale- vs. horizontale Wallet oder integrierte- vs. Umbrella Wallet.

4 Anwendungsszenarien und Dienste der Mobile Wallet

Wie beschrieben ist eine Mobile Wallet mehr als ein Dienst für Endkonsumenten. Die Mobile Wallet muss vielmehr als eine partner- und branchenübergreifende Plattform verstanden werden, die unterschiedliche Funktionen verbindet. Dies können Zugang (Access) zu Informationen, Orten und lokationsbezogenen Dienste (Location Based Services), Kommunikation, eigenen und fremdinitiierten Transaktionen (z. B. Zahlungsverkehr), Identifikation von Personen und Rechten mit Elementen des Marketings, der Kundenbindung und des Vertriebes sein. Dabei muss die Mobile Wallet sich dynamisch dem jeweiligen Nutzungskontext anpassen und die notwendigen Rahmenbedingungen wie Datenschutz und -sicherheit berücksichtigen. Insofern entsteht auf Basis der Mobile Wallet ein eigenes Ökosystem mit neuen Wertschöpfungsketten. Ob sich dieses Ökosystem hinreichend kommerzialisieren bzw. monetisieren lässt, hängt von der Akzeptanz durch den Endkunden (Verbraucher, Nutzer) ab. Dabei wird eine reichweitenstarke Adaption nur dann gelingen, wenn der Verbraucher signifikante Mehrwerte durch die Nutzung erhält und Vertrauen in die Nutzung einer Mobile Wallet hat.

Die Mehrwerterzeugung beim Nutzer reicht jedoch alleine nicht aus. Alle Beteiligten des Mobile Wallet Ökosystems sollten profitieren. In einem Mehrwertszena-rio sollte das Leben durch eine Mobile Wallet erleichtert werden. Physische Karten, die normalerweise im Geldbeutel mitgeführt werden, sollen »digitalisiert« werden. Papiertickets oder -Coupons werden der Vergangenheit angehören, da sie jederzeit auf dem mobilen Endgerät zugänglich, in der Applikation oder in der Cloud abgespeichert sind, dabei die Umwelt schonen und einen physischen Versand hinfällig machen. Ein ständiger Überblick über die Finanzen, den Bonuspunkte-Stand oder die ortsnahen Rabatt-Aktionen soll möglich werden und aufgrund von kontaktlosen Bezahloptionen, den Einsatz von Bargeld schrittweise überflüssig machen. Darüber hinaus sollen Kosten reduziert und (Verwaltungs-) Prozesse effizienter gestaltet und ggf. überwacht werden. Insofern ist nachvollziehbar, dass auch die öffentliche Verwaltung darüber nachdenkt Krankenkassen- und Gesundheitskarten, sowie Ausweise bzw. sonstige Identifikationspapiere (Erlaubnisverbriefungen) zu digitalisieren. Es ergeben sich durch den technologische Fortschritt neue Anwendungsszenarien wie der mobile Schlüssel oder der komfortable Zugriff auf Inhalte und Berechtigungen aller Art sowie Angebote mit einer immer größeren Individualisierung.

4.1 Die Mobile Wallet im 24 h Einsatz

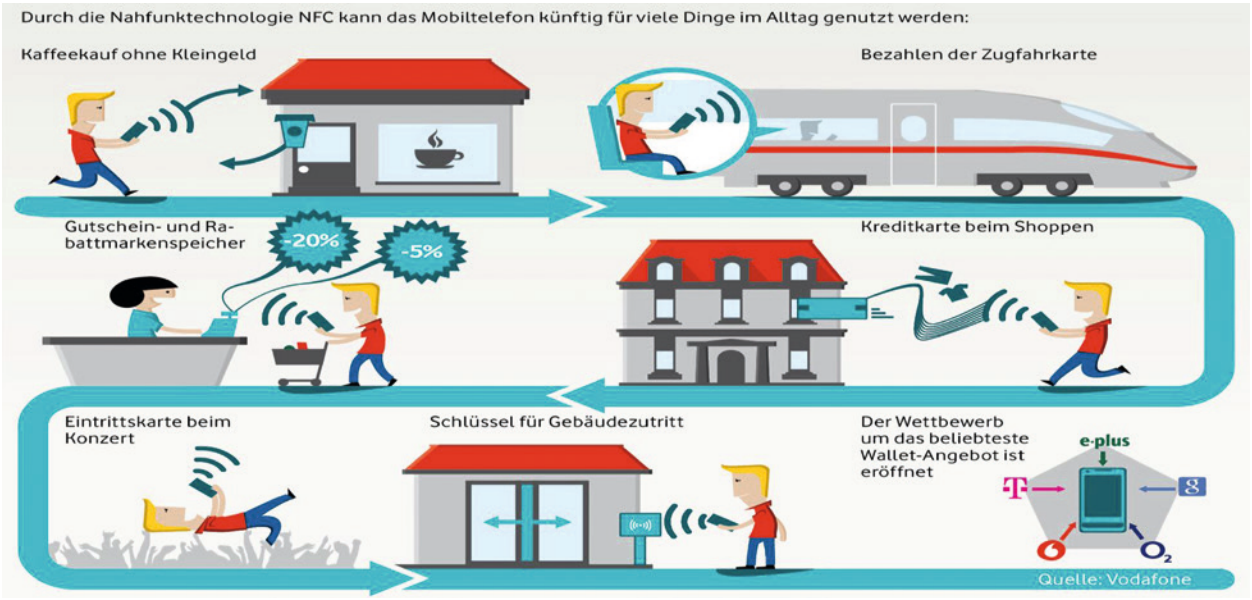

Abbildung 3: Die Mobile Wallet im 24 h Einsatz; Quelle: Vodafone

Die obige Graphik beschreibt beispielhaft, wie ein Tag mit einer Mobile Wallet aussehen kann.

Nach einer von PwC 2014 durchgeführten Online-Befragung sind Endkonsumenten am ehesten dazu bereit eine Mobile Wallet zur Digitalisierung von Papiertickets zu verwenden. 66 Prozent der Befragten empfinden es als angenehm, auf das lästige Ausdrucken von Tickets verzichten zu können und durch die digitale Verfügbarkeit ein etwaiges Vergessen dieser vermeiden zu können.

58 Prozent würden ihre Versichertenkarten gerne in eine Mobile Wallet integrieren. Für 57 Prozent der Befragten wäre es relevant alle Kundenkarten in einer Mobile Wallet zusammen zu führen und somit die physische Mitnahme der Plastikkarten unnötig werden zu lassen. Von dem Erhalt ortsabhängiger Coupons zu profitieren, stellt für 56 Prozent einen relevanten Vorteil einer Mobile Wallet dar.

4.2 Ausgewählte Mobile Wallet-Dienste im Überblick

Das aktuelle Anwendungsszenario einer Mobile Wallet fokussiert noch auf die Durchführung von kommerziellen Transaktionen mit den nachgelagerten Prozessen Zahlung und Kundenbindung. Diese rein auf die transaktionsbezogene Funktionen beschränkte Sichtweise ist jedoch ungenügend und spiegelt bei weitem nicht das Potenzial einer Mobile Wallet in der Definition des BITKOM wieder. Nachfolgend stellen wir die für die Zukunft wichtigsten (Mehrwert-) Dienste dar, die in der Mobile Wallet zusammengeführt werden (können).

4.2.1 Zugangskontrolle: Access-Lösungen und mobiler Schlüsselersatz

Unter »Access« versteht man den Zugang zu Informationen und Rechten (z. B. Lizenzen, Mandaten, Zertifizierungen) sowie den Zutritt zu grundsätzlich gesicherten Orten (z. B. Gebäuden, Zimmern) oder Gegenständen. Darüber hinaus kann man auch die damit zusammenhängende

Verwaltung von Berechtigungen unter den Begriff Zugang subsumieren.

Für den Zugang wird ein elektronischer Schlüssel benötigt, der in der Mobile Wallet abgelegt bzw. gespeichert wird. Die Nutzung des Schlüssel kann dann je nach Nutzungskonzept abhängig vom Übertragungsstandard (z. B. Funk, Licht d.h. optisch) erfolgen. Beispiele sind insbesondere der Zugang zu Hotelzimmern, Bürogebäuden sowie öffentlichen Bereichen und Veranstaltungsräumen. Der Ersatz von Auto- oder Haustürschlüssel ist ebenfalls denkbar, scheitert derzeit aber noch an der notwendigen technologischen Infrastruktur, der fehlenden Standardisierung sowie der Skepsis der Verbraucher in Bezug auf Sicherheit und Datenschutz. Dennoch ist der Einsatz auch heute schon im Bereich Carsharing, Hotellerie und Gebäudemanagement praktikabel und in Pilotinstallationen realisiert.

4.2.2 Zahlungsverkehr und mobile Payment

In der Mobile Wallet können eine oder mehrere Bezahlarten in digitaler Form hinterlegt sein. Dabei ist die Mobile Wallet selbst kein Zahlungsinstrument, sondern bietet nur den Zugang bei dem die einzelnen Zahlarten ausgewählt und transaktionsspezifisch autorisiert werden. Als gängige zu hinterlegenden Zahlungverfahren und/oder Instrumente kommen in Betracht:

- Debit- und Kreditkarten
- Elektronische Lastschriftverfahren mit der hinterlegten Kontoverbindung
- Rechnungskauf
- Prepaid-Verfahren und Modelle (Karten oder Konten)
- Path-Through- oder »on-behalf-of«-Zahldienste mit und ohne Zahlungsgarantie (z. B. PayPal, Click & Buy, Yapital)
- Wertverbriefende Gutscheine, Coupons und Voucher
- Wertverbriefende Zahlungsäquivalente aus Bonitätsprogrammen
- Digitalisierter Bestand an virtuellen Währungen (z. B. Bitcoins)

Obwohl die Nutzung einer Mobile Wallet auch ohne eine Zahlungsverkehrsfunktion denkbar ist, stellt sie derzeit noch die zentrale Funktion dar. Sie dient den Anbietern von Mobile Wallets daher auch als »Ankerfunktion« ihrer Produkte und Dienstleistungen. Allerdings ergibt sich aus Marktstudien, dass eine alleinige Fokussierung oder Beschränkung auf den Zahlungsverkehr nicht ausreicht um eine Mobile Wallet aus Anbietersicht gewinnbringend zu monetisieren.

Wie in allen anderen Anwendungsszenarien auch, ist der Dienstanbieter (in diesem Falle also die Zahlungsdienstanbieter, die kartenherausgebende Bank, der Coupondienstleister, etc.) für den Service, die Integration und damit verbundene Sicherheits- und regulatorisch relevante Aspekte verantwortlich.

4.2.3 Peer2Peer-Überweisung

Hierbei handelt es sich um einen Dienst mit dem sich Verbraucher untereinander bequem Geld senden können und das nahezu in Echtzeit. Um diese Funktionalität nutzen zu können, müssen sich Sender und Empfänger zunächst verifizieren und für den Dienst registrieren. Dies erfolgt häufig auf Basis der Mobilfunknummer oder einer eindeutigen ID, die vom jeweiligen Anbieter vergeben wird. Im Anschluss kann nach Bestätigung der wechselseitigen IDs und entsprechender Autorisierung Geld transferiert werden. Zahlreiche Start-ups sind in diesem recht neuen Segment zu finden: Cringle, Pocket United, Paymy, Cashcloud, Number26 oder Payfriendz. PwC kam bei ihrer Umfrage zu dem Ergebnis, dass fast die Hälfte der Befragten (45 %) Geld über das Smartphone zu anderen Nutzern transferieren würden. Auch hier gilt, dass der Dienste- und nicht der Walletanbieter für die Erfüllung möglicher regulatorischer Anforderungen verantwortlich ist.

4.2.4 Identity/ eID & Führerschein

Trotz zahlreicher Sicherheitsbedenken, lassen sich sichere Identitäten problemlos in die digitale Welt und auch in die Anwendungsbereiche moderner Smartphones übertragen. Das zeigen zum Beispiel aktuelle Entwicklungen der Berliner Bundesdruckerei, die darauf abzielen, Mobiltelefone für temporäre Ausweisfunktionen nutzbar zu machen. Voraussetzung für solche Mobile Wallet-Anwendungen ist ein vertrauenswürdiger Schutz verlässlicher Identitätsdaten, die auf hoheitlichen Dokumenten wie dem Personalausweis oder dem EU-Führerschein basieren. Denn nur sie sind der Vertrauensanker, um valide Identitäten sicher abzuleiten.

Mithilfe der Online-Ausweisfunktion (eID-Funktion) des Personalausweises ist sichergestellt, dass all den Anwendungen, die in diesem Leitfaden beschrieben sind, auch eine sichere Identität auf eine speziell autorisierte Instanz, der sogenannten »Trusted Service Platform« (TSP), übertragen und via Sicherheitstoken direkt zur Verwendung freigeschaltet werden können. Zur Ausführung einer mobilen Ausweisfunktion über Smartphones Sicherheitselemente, die zum Beispiel in Form einer SIM- oder providerunabhängigen microSD-Karte in ein Smartphone integriert werden. Der Zugang zu einer solchen Mobile Wallet Ausweisfunktion kann einfach realisiert werden: Auf Basis einer kostenlos heruntergeladenen App und eines geeigneten Lesegeräts meldet sich der Nutzer über seinen Personalausweis mit aktivierter Online-Ausweisfunktion und seiner geheimen Ausweis-PIN persönlich für die entsprechende Funktion an. Das sichere Ableiten der Identitätsdaten aus dem Sicherheitschip im Ausweisdokument könnte alternativ auch in Behörden über die Self-Service-Terminals der Bundesdruckerei erfolgen. Im zweiten Schritt wird die im Handy integrierte SIM- oder microSD-Karte über die individuelle Karten-PIN für den Empfang der gesicherten Ausweisdaten freigegeben.

Selbst wenn das für mobile Identitätsanwendungen genutzte Smartphone in falsche Hände gerät, bleiben die Daten geschützt: Ohne den Besitz des hoheitlichen Dokuments in Kombination mit der Kenntnis der geheimen Ausweis- und Karten-PIN erfolgt seitens des TSP-Systems keine Freischaltung der angeforderten Daten. Aus technologischer Sicht sind die Weichen zur Realisierung solcher Mobile Wallet-Anwendungen längst gestellt.

4.2.5 Ticketing

Ticketing beschreibt die Digitalisierung eines Inhaberpapiers, welches das Recht verbrieft, eine Dienstleistung in Anspruch zu nehmen. In Betracht kommen hier z. B. Fahrkarten und Eintrittskarten. Hauptanwendungsszenario für die Mobile Wallet ist der Kauf und die Speicherung von Fahrkarten des ÖPNV, der Bahn oder der Fluglinien. Darüber hinaus stellen Eintrittskarten für Messen und Museen, Sportveranstaltungen, Konzerte, etc. einen beliebten Anwendungsfall dar. Insbesondere bei letzterem bietet sich eine Kombination mit vorausbezahlten Verbrauchs-Guthaben oder speziellen Zugangsberechtigungen z. B. zu VIP-Bereichen an.

Ticketing ist einer der Dienste einer Mobile Wallet, der für viele Endkonsumenten auch heute schon einen echten Mehrwert darstellt. Elektronische oder digitalisierte Tickets können umweltschonend in der Mobile Wallet abgespeichert, verwaltet und an den Kontrollstellen ausgelesen werden. In der entsprechenden Kombination mit Zahlungsverkehr können darüber hinaus Kosten reduziert werden (Bargeldversorgung/ -endsorgung), Durchlaufzeiten verringert und Betrugsfälle (Fraud) eingedämmt werden.

4.2.6 Kundenbindungsprogramme (Loyalty) und Couponing/ Voucher

Der Erhalt von Rabatten oder Coupons ist ein weiterer zentraler Anwendungsdienst im Nutzungskontext der Mobile Wallet. Unter »Couponing« versteht man die Digitalisierung einer Berechtigung zur Inanspruchnahme eines Rabattes im Rahmen einer kommerziellen Transaktion (i.d.R. Kauf). Rabatte können dabei z.B. in Form von Preis- oder Mengenrabatten gewährt werden. Coupons können auf verschiedene Wege in die Wallet integriert werden, z.B.:

- Nutzung von Aggregatoren (z.B. Payback, Coupies, etc.), die mit dem Backendsystem der Mobile Wallet verbunden sind. Diese erhalten einen Platz in der Wallet – ähnlich einem Marktplatz – für entsprechende Angebote.

- Hersteller, bzw. Händler und Markenartikler stellen Coupons direkt über das Backendsystem in die Mobile Wallet ein.

Aus allen Coupon-Angeboten kann der Kunde mehrere Coupons für die Nutzung aktivieren.

Loyalty beschreibt die Digitalisierung von Kundenbindungsprogrammen und den regelmäßig in diesem Zusammenhang ausgegebenen Kundenkarten. Der Verbraucher kann die digitalisierten Kundenkarten an der gewünschten Akzeptanzstelle einsetzen. Voraussetzung ist die Installation und Speicherung der Kundenkarten in der Mobile Wallet sowie die passende elektronische Akzeptanzstelle.

Integrierbare Kundenbindungskarten können in verschieden Klassen kategorisiert werden:

- Prämienmodelle – unternehmensübergreifend (z.B. Payback, Deutschland Card)

- Rabattmodelle – unternehmenseigene (z.B. OBI, IKEA, Shell)

- Gutscheinmodell – Einzelhandel und Gastronomie (z.B. Stempelkarten kleinerer Unternehmen)

4.3 Zusammenfassung

Die Zahlungsfunktion ist derzeit noch der Hauptaufhänger und die Ankerfunktion für viele Unternehmen im Mobile-Wallet Ökosystem. Für eine Adaption durch den Endkunden ist es jedoch entscheidend, möglichst viele, Mehrwert stiftende Dienste in einer partner- und branchenübergreifenden Plattform zusammenzuführen und miteinander zu kombinieren. Zu den hier ausgewählten Funktionen wie Zugang (Access) zu Informationen, Orten und lokationsbezogenen Diensten (Location Based Services), fremdinitiierte Transaktionen (z.B. Zahlungsverkehr), Identifikation von Personen und Rechten mit Elementen des Marketings, der Kundenbindung und des Vertriebes verbindet, können und sollten in Zukunft weitere hinzugefügt werden können. Offene Schnittstellen und Interoperabilität können genauso helfen für eine reichweitenstarke Adaption zu sorgen, wie signifikante Mehrwerte. Entscheidend wird für die Mobile Wallet und Dienstanbieter letztendlich auch sein, ein hohes Maß an Vertrauen beim Endverbraucher zu entwickeln.

5 Mobile Wallet-Ökosystem und aktuelle Ansätze

Das Ökosystem kann als das Gesamtspektrum von allen an der Mobile Wallet Wertschöpfung beteiligten Einheiten definiert werden. Dies betrifft sowohl die Hauptbeteiligten als auch die Anbieter von Mehrwertdiensten. Der Markt für Mobile Wallets ist sehr dynamisch und schnelllebig. Die etablierten Stakeholder versuchen ihre Rolle zu erweitern und ihre Position am Markt zu stärken. Im Gegenzug werden neue Anbieter ihre Möglichkeiten nutzen, um in den Mobile Wallet Markt einzudringen und Marktanteile zu gewinnen. Aufgrund der Komplexität der Mobile Wallet Strukturen gehen wir im vorliegenden Leitfaden nicht auf jeden einzelnen etablierten oder potentiellen Beteiligten detailliert ein, sondern setzten den Fokus auf die Schlüsselakteure.

5.1 Rolle der einzelnen Mobile Wallet Stakeholder

Auf den ersten Blick scheint das Ökosystem einer Mobile Wallet aus vier Parteien zu bestehen – Kunde, Händler, Bank und Mobilfunkunternehmen/ Mobile Network Operator (MNO). Auf den zweiten Blick aber wird die Komplexität deutlicher. Dies soll am Beispiel des Ökosystems für den Dienst Mobile Payments auf Basis von Kartenemulation mit SIM Karte als Secure Element exemplarisch dargestellt werden. Nicht weniger als fünfzehn unterschiedliche Player sind allein daran beteiligt. Dabei sind die Berührungspunkte sehr unterschiedlich. Im folgenden Abschnitt fokussieren wir uns auf die folgenden Hauptakteure Kunde, MNOs, Handel, Banken & Payment Scheems. Darüber hinaus spielen die sogenannten »Digital Over The Top Player« eine zunehmend große Rolle.

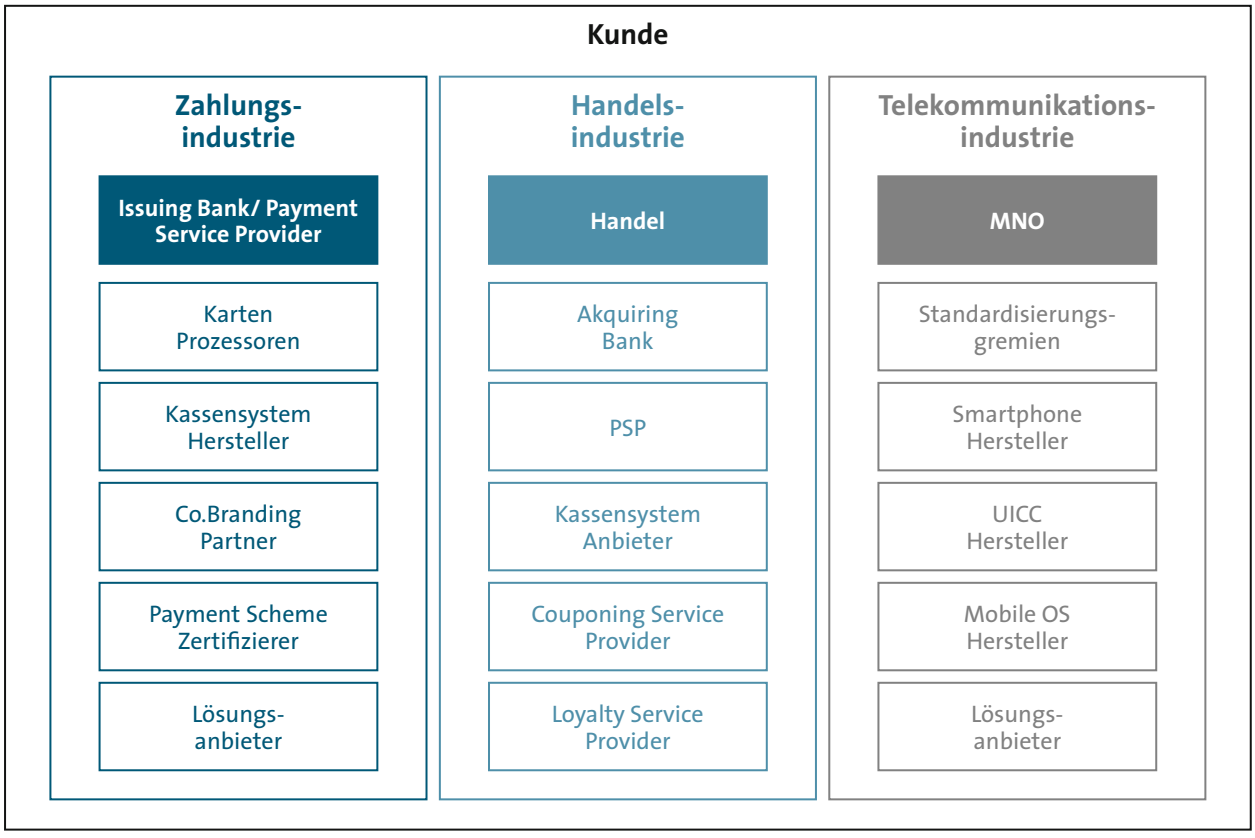

Abbildung 4: Mobile Wallet Ökosystem; Quelle: Vodafone

5.1.1 Der Kunde

Im Zentrum des Mobile Wallet-Systems steht der Kunde. Um dessen Bedürfnisse werden Dienstleistungen entwickelt, die Ihm einen Mehrwert stiften müssen. Denn nur unter dieser Prämisse, ist er bereit neue Dienste gegen alte Gewohnheiten zu substituieren. Für viele Unternehmen, gerade aus dem Finanzumfeld ist der komplette Fokus auf den Kunden eine Art Paradigmenwechsel. Der Kunde ist immer bereit einen gewissen Trade-off zwischen Sicherheit und Kundenfreundlichkeit in Kauf zu nehmen. Viele Kunden sind bereit persönliche Daten abzugeben, wenn sie dadurch einen finanziellen oder anders gearteten individualisierten Mehrwert haben. Die Diskussion über die Hoheit der Kundendaten ist eine der am schwierigsten zu beantwortenden Fragen rund um die Mobile Wallet, da jeder Stakeholder diese »Kundenhoheit« für sich beansprucht.

5.1.2 Die Mobilfunkunternehmen/ Mobile Network Operator (MNO)

Die MNOs waren in der Vergangenheit hauptsächlich mit der Bereitstellung und Betreuung von Infrastruktur und Netzwerken beschäftigt. Dieses Businessmodell hat sich grundsätzlich geändert, da sie aufgrund der Digitalisierung für bestimmte Geschäftszweige neue Wege entdeckt haben, um neue Geschäftsfelder zu besetzten und eine engere Kundenbindung zu erreichen. Angebote für mobile Endgeräte stehen hier besonders im Fokus.

MNOs können ein entscheidender Faktor bei der Etablierung und der Verbreitung von Mobile Wallets sein, da sie bereits eine breite Kundenbasis mit Kommunikationsdienstleistungen versorgen. Zudem stellen sie das Kommunikationsnetzwerk und die SIM-Karten zur Verfügung. Sie sind in der Lage neue Funktionalitäten und Applikationen in das mobile Endgerät zu integrieren.

Die MNOs bieten viele Mobile Wallet Leistungsangebote über ihre strategischen Kooperationen an. So haben Deutsche Telekom, Vodafone und O2 (Telefonica Deutschland) den gemeinsamen Service mPASS entwickelt. Sämtliche MNOs haben eigenen Wallet-Lösungen in Deutschland und weiteren Ländern eingeführt.

5.1.3 Der Handel

Beim Handel muss man zwischen den Online-Händlern wie Amazon und Ebay, sowie den stationären Händlern unterscheiden. Beide Seiten bieten inzwischen unterschiedliche Wallet Konzepte an. Die meisten Online-Händler verfolgen schon länger eigene Digital Wallet Konzepte (vgl. Kapitel 3.2) und bieten diese am Markt an.

Der stationäre Einzelhandel unterliegt aktuell Veränderungsprozessen, die weit über Mobile Wallets hinausgehen bzw. sehr viel früher anfangen. Die Entscheidung für eine Mobile Wallet-Lösung bettet sich in diese Überlegungen ein. So haben viele Händler Studien und Business-Case-Berechnungen durchgeführt, die aus ökonomischer, Akzeptanz- und Nutzensicht den Einsatz von Mobile Wallet untersucht haben. Einige stationäre Händler bieten inzwischen eigene proprietäre Wallets im Markt an. Häufig befinden sich Lösungen aber auch im Pilotstadium (»silent roll-out«). Dabei setzen die Händler auf verschiedene, technische Lösungen: NFC- oder App-basiert.

Ein Beispiel hierfür: Netto hat eine eigene App (in Kooperation mit Valuephone) umgesetzt. Neben dem Bezahlen kann der Kunde Einkaufslisten erstellen sowie Coupons und Gutscheine einlösen. An der Kasse wird mittels der App eine vierstellige Nutzer-ID erstellt, die der Kassiererin zu nennen und von ihr in der Kasse einzugeben ist. Damit ist der Bezahlvorgang beendet.

Händler stellen einen Schlüsselfaktor für den Erfolg von Mobile Wallets dar. Ohne ihre aktive Beteiligung insbesondere die Information und Schulung der Mitarbeiter am PoS, sowie die Anpassung der Infrastruktur auf Mobile Wallets-Prozesse sind die Entwicklung und die Verbreitung solch neuer Ansätzen nicht möglich. Vielerlei Angebote werden bereits heute in digitaler (Kredit-/Debit-Karten Zahlungen) oder auch in analoger (Gutscheine, Treuepunkte etc.) Form unterbreitet. Mobile Wallets öffnen Händlern neue und kostengünstige Möglichkeiten, die bereits vorhandenen Prozesse vollständig

zu digitalisieren, um das Kundenverhalten effektiv zu analysieren und Angebote individualisiert ausrichten zu können.

Darüber hinaus ermöglichen Mobile Wallets den Händlern eine stärkere Kundenbindung und eine effizientere Betreuung durch gezielte Angebote und Marketingmaßnahmen, welche Rabatte, Treuepunkte, Coupons bis hin zu Gutscheinen umfassen können.

5.1.4 Banken

Mit ihren vorhandenen Zahlungsinfrastrukturen und -dienstleistungen können Banken einen wesentlichen Beitrag im gesamten Mobile Wallet Ökosystem leisten. Banken genießen ein hohes Vertrauen seitens der Kunden bezgl. der angebotenen Finanzdienstleitungen (Bankkonto, Kreditkarten, Zahlungsverkehr, Darlehen etc.) sowie der Sicherheit der Prozesse und Systeme.

Durch die direkte Kundenbeziehung und die bestehende Abwicklung des Zahlungsverkehrs als Ankerservice für Mobile Wallets haben diese zudem auch die Möglichkeit sich selbst stärker im Wallet-Umfeld zu positionieren und tun dies teilweise auch schon. Zudem bringen sie durch das Online-Banking bereits existierende Registrierungs- und Authentisierungsmechanismen ein, die im Mobile Wallet Umfeld wiederverwendet werden können und so dem Verbraucher die Nutzung der Wallet vereinfachen, da er auf bekanntes und bewährtes aufbauen kann.

Kreativität, Flexibilität und innovative Ansätze stellen Schlüsselfaktoren dar, um bereits vorhandene Vorteile gegenüber anderen Wettbewerbern optimal einzusetzen. Ein Umdenken beziehungsweise der kontinuierlichen Reduzierung bezgl. der Abwicklungszeiten von Finanztransaktionen (Stichwort: Faster Payments), neuer Sicherheitsmaßnahmen und Authentifizierungsprozesse muss stattfinden, damit die Beziehung zu den Bankkunden gefestigt und gegebenenfalls ausgebaut werden kann.

In anderen Ländern sind Banken deutlich aktiver als hierzulande. Ein entscheidender Faktor liegt in der heterogenen Struktur des deutschen Bankensystems. So ist es in anderen Ländern erheblich einfacher innovativen Lösungen die erforderliche Masse zu geben und Standards zu setzen, da sich in der Regel nur einige wenige Großbanken einigen müssen. So bietet die BBVA über Wizzo in Spanien an, »Peer-to-Peer« Geld über das Handy zu senden und zu erhalten oder mit dem »Sticker Wizzo« kontaktlos zu bezahlen. Das Angebot ist vor allem an junge Leute gerichtet. Die Barclays Bank bietet mit Pingit in Großbritannien ebenfalls eine Bezahllösung mittel QR-Code-Scanning und für »Peer-to-Peer-Zahlungen« an. Zudem ist Pingit verknüpft mit Pay:m, einer Anwendung, mit der Zahlungen über die Mobilfunk-Nummer real-time getätigt werden können, ohne dass dem anderen dabei Kontendaten übermittelt werden müssen. In Frankreich haben sich initial drei Banken (Société Générale, BNP Paribas und La Banque Postale) zusammengeschlossen und bieten in Zusammenarbeit mit Worldline eine Wallet unter dem Namen »Paylib« an.

5.1.5 Digital Over the Top Player

Internetanbieter wie Google, Apple oder Microsoft haben bereits eine beachtliche Kundenbasis durch Online-Mehrwertdienste aufgebaut. Mobile Wallets dienen als zusätzliche Plattformen und sollen künftig neue Services am Markt etablieren und verschiedene Dienste miteinander kombinieren. Die aus dem Konsumentenverhalten resultierenden Daten können wiederum als zusätzliche Dienste an die angebundenen Online-Händlern angeboten werden. Auf Basis dessen können die Händler gezielt Werbe-Rabattaktionen gestalten, Coupons und Treuepunkte vergeben. Die enorme Kundenbasis macht es ihnen möglich auch margenschwache Services schnell gewinnbringend zu vermarkten. Mobile Wallets bieten ihnen die Möglichkeit, ein hochkomplexes Ökosystem von Anfang mitzugestalten und ihren Einfluss auf wichtige Prozesse auszuüben.

Alle drei Player sind jeweils für ein mobiles Operating System (OS) verantwortlich und haben ein großes Interesse an der Entwicklung des Marktes für Mobile Wallets. Sie können jederzeit über das OS Dienstleistungen erweitern und neue Angebote in Form von Werbenachrichten verteilen.

Sie können wichtige Sicherheitsmechanismen und eigene Applikationen in das Betriebssystem integrieren und kontinuierlich überwachen, um garantieren zu können, dass die Nutzung der Geräte trotz der dynamischen Entwicklung des Marktes weiterhin sicher bleibt. Ihr Beitrag ist immens wichtig für die Akzeptanz der Nutzer von Mobile Wallets.

5.1.6 Payment Scheme Owner

Sowohl die Kreditkartenunternehmen MasterCard und VISA als auch die Zahlungsdienstanbieter PayPal, Yapital und Click&Buy haben Digital Wallets eingeführt. Der Fokus liegt auf einer Bezahlapplikation, die den Check-Out im Warenkorb eines E-Commerce Händlers vereinfachen soll. Hierzu kooperieren die Kreditkartenschemes in Europa im engen Verbund mit den Banken. So werden z.B. für Deutschland die Sparda-Banken zum Ende diesen Jahres die erste bankenintegrierte MasterPass-Wallet auf den Markt bringen.

Die Kreditkartenunternehmen gehören aktuell zu den Treibern von Mobile Wallet Lösungen, da Sie derzeit als einziger Zahlungsdienst in den MNO Wallets integriert sind und durch die NFC Schnittstelle bereits bei vielen Händlern akzeptiert werden. Perspektivisch sollen die digitalen Wallets, etwa V.me von VISA oder MasterPass von MasterCard auch Mehrwertdienste außerhalb des Payments, z.B. Couponing oder Loyalty, integrieren. Somit sind die Grenzen zwischen Wallet- und Service-Anbietern mitunter fließend.

Zahlungsdienstanbieter arbeiten derzeit an vielen Stellen daran, ihren Service auch am PoS Terminal empfangbar zu machen. Auch hier kann NFC in Zukunft dafür sorgen, dass wir mehr Vielfalt an unterschiedlichen Zahlungsdiensten sehen werden, die den prozentualen Anteil von nicht baren Zahlungen weiter reduzieren.

5.1.7 White Label Mobile Wallet Anbieter

Im Mobile Wallet-Markt gibt es auch Anbieter von White Label-Lösungen, also Produkten und Anwendungen, die unter einer anderen Marke eines Unternehmens vertrieben werden. Sie sind in unserem Sinne keine Marktteilnehmer, sondern stellen ihre Infrastruktur und Technologie anderen Unternehmern zur Verfügung.

5.2 Zusammenfassung

Der Wettbewerb zwischen den verschieden Akteuren bleibt insofern offen, da jeder versucht sich entsprechend am Markt zu positionieren und die Kundenwahrnehmung zu gewinnen. Banken, Kreditkartenanbieter oder auch Mobilfunkanbieter haben traditionell enge Kundenbeziehungen und verfügen bereits über entsprechende Netzwerke, kundenorientierte Prozesse und IT-Infrastrukturen. Dies können sie zu ihrem Vorteil nutzen, wenn sie entsprechend auf die Anforderungen der Kunden an Mobile Wallets eingehen. Nichtsdestotrotz kann jeder Player durch ein innovatives und für die Kunden attraktives Angebot diese für sich gewinnen. Der Launch des iPhone 6 zeigt, dass einer der großen Over the Top Player mit der enormen Kundenbasis und der Netzwerkökonomie den Markt in kürzester Zeit enorm beeinflussen kann.

6 Herausforderungen, Kundenadaption und Potenziale

6.1 Mobile Wallet-Herausforderungen in Deutschland

In den vergangenen Jahren wurde immer wieder darüber gesprochen, dass nun endlich der Zeitpunkt gekommen sei, dass das Mobile Wallet Ökosystem abhebt. Inzwischen ist schon einiges passiert, meist aber als Insellösungen mit überschaubarer Nutzer- bzw. Transaktionszahl oder als Piloten mit wenigen Nutzern in einem regionalen Testgebiet. Vergleicht man verschiedene internationale Initiativen, erkennt man, dass sich Geschäftsmodelle länderspezifisch und in unterschiedlichem Maße durchgesetzt haben. Dies liegt an vielen Parametern, zum einen an der technischen wie auch der bankseitigen Infrastruktur, aber auch den sehr unterschiedlichen Zahlungsgewohnheiten und -verhalten der Endverbraucher. In Deutschland werden zurzeit noch stärker als in anderen Ländern Sicherheitsbedenken in den Vordergrund gestellt, was die Akzeptanz neuer Anwendungen hemmt. Wichtig ist die Unterscheidung von »gefühlter« Sicherheit im Gegensatz zu tatsächlicher Sicherheit bei Zugang und Übertragung von Werten und Informationen. Aktuelle Marktentwicklungen zeigen, dass Letzteres technisch gelöst werden wird. Parallel muss auch die Wahrnehmung und das Empfinden von Sicherheit beim Nutzer offensiver von den Akteuren und Anbietern angegangen werden. Ist dieser erst einmal überzeugt, wird er nicht nur zum aktiven Anwender, sondern zumeist auch zu einem Verstärker und Multiplikator.

Ein einheitlicher Datenübertragungsstandard ist mit NFC in Deutschland kurz vor dem Durchbruch. NFC, QR-Codes oder doch BLE? Im Laufe dieses Kapitels klären wir, welche Datenübertragung für welche Anwendungsszenarien zum Tragen kommt.

Es wird viel vom Verhalten der Verbraucher und ihren Konsummustern sowie der Akzeptanz der Bezahlverfahren abhängen. Kreditkarten spielen z. B. in den USA eine wesentlich größere Rolle als in Deutschland. Geschäftsmodelle, die in anderen Ländern funktionieren, müssen sich nicht zwangsweise auch hierzulande durchsetzen.

Die Verbreitung von Mobile Wallet-Konzepten ist im Ländervergleich sehr heterogen. Attraktive Anwendungen sind eine wichtige Voraussetzung dafür, dass die neuen Lösungen von den Kunden angenommen werden. Da innovative Lösungen für mobile Zahlungen sich jedoch in wichtigen technologischen und strukturellen Charakteristika länderübergreifend ähneln und große internationale Wettbewerber ihre Einführung vorantreiben, ist eine zunehmende Konvergenz der Systeme zu erwarten.

Die heranwachsende Generation der »Digital Natives« ist 24/7 online und damit viel stärker in der virtuellen Welt verankert, als viele dies noch vor wenigen Jahren prophezeit hätten. Realtime wird von dieser Generation in allen Lebensbereichen als Standard und nicht als technologische Extravaganz angesehen. Es gilt diese Potenziale mit entsprechenden Diensten und Angeboten in der Mobile Wallet zu heben.

6.1.1 Datenübertragung im Kontext der Mobile Wallet

Die Interaktion und der Informations- bzw. Datenaustausch des Nutzers mit den verschiedenen Dienstleistern und Händlern ist die zentrale Aufgabe einer Mobile Wallet. Der Vorteil einer Mobile Wallet im Vergleich mit anderen Medien und Formaten liegt dabei in der Nutzung bzw. Kombination der verschiedenen Übertragungstechnologien und der Kompatibilität mit verschiedenen Empfängern. Darüber hinaus lassen sich je nach Wahl der Übertragungstechnologie größere Datenvolumen bidirektional übertragen. So können im Rahmen einer Transaktion Daten additiv genutzt, übertragen, in Echtzeit verarbeitet und gespeichert werden. Die Verarbeitung und Speicherung kann dabei je nach Verfahren im Online- oder Offline-Modus erfolgen.

Kontextbasierte Verfahren

Bei kontextbasierten Verfahren steht die Datenübertragung im Kontext einer dedizierten Aktion. Das heißt der Anwender initiiert oder bestätigt die zweckbestimmte Datenübertragung unmittelbar durch Ausführen der Aktion. Beispiele hierfür sind das Berühren oder das Abfotografieren eines Kinoplakates, um weitergehende Informationen zu dem Film zu erhalten, oder die Bezahlung an der Kasse durch das Berühren des mobilen Gerätes mit dem Bezahlterminal. Derartige Aktionen sind für Anwender schnell und intuitiv umsetzbar, da sie eng an die menschliche Gestik des Zeigens und Berührens angelehnt sind.

- Near Field Communication (NFC):

In Deutschland wird die Technik beispielsweise von den Kreditkartenunternehmen zur kontaklosen Bezahlung unter den Namen PayPass (Mastercard) und paywave (Visa) angeboten, und von den Sparkassen, unter dem Namen girogo, zur Zahlung von Summen bis zu 20 Euro. NFC wird auch von der Deutschen Bahn in ihrem Touch & Travel-System eingesetzt. Auch viele Hochschulen nutzen NFC-Chips in Studentenausweisen zur Zahlung kleinerer Beträge. Die Übertragung von Daten kann bei NFC in drei verschiedenen Modi erfolgen:

  - Reader Mode: Auslesen von Daten mit einem aktiven NFC Gerät (mobiles Endgerät) aus einem passiven NFC Tag. Die NFC Tags sind Chips die kleine Mengen von Daten enthalten, wie z. B. Links, Bilder oder Text. Aufgrund ihrer Robustheit, und der geringen Größe und niedrigen Kosten können diese Tags sehr vielfältig eingesetzt werden, wie z. B. in Postern (Smart Poster) oder als Sticker. Bei der Berührung mit einem NFC-fähigen Smart Phone werden die enthaltenen Informationen ausgelesen.

  - P2P Mode: Austausch von Daten zwischen zwei aktiven Geräten. Beide Geräte können hierbei bei Berührung Informationen senden und empfangen, so dass hier eine komplexe Kommunikation zwischen beiden Geräten möglich ist. Android Beam ist ein Beispiel für den Einsatz dieses Modus.

  - Card Emulation Mode: In diesem Modus emuliert das NFC-Gerät eine kontaktlose Smart Card gegenüber einem Smart Card Lesegerät. Hierdurch wird es möglich kontaktlos zu bezahlen. Dies geschieht durch einfaches Heranführen einer NFC-kompatiblen Karte oder Mobiltelefon an ein NFC-fähiges Bezahlterminal und wird auch als »tap and go« bezeichnet. Dieser Modus erfordert eine deutlich komplexere technische Infrastruktur als die beiden anderen Modi, da zusätzlich ein Secure Element, also Smart-Card-Chip, zum Einsatz kommt. Das Verfahren bietet aber den großen Vorteil, dass eine bestehende Infrastruktur für Smart Cards weiter verwendet werden kann, und Kunden ohne NFC-fähiges Gerät alternativ auch eine Smart Card verwenden können. Bezahlen mit NFC Card Emulation in Deutschland basiert auf wenigen Standards, etwa Paypass von MasterCard oder Paywave von VISA, die bereits für den deutschen Markt implementiert sind. Für weitere NFC-Standards sind die Markeintrittsbarrieren sehr hoch, da eine Vielzahl von Parteien in dem Markteinführungsprozess involviert werden müssen. So müsste ein Bezahlformat etwa durch die Deutsche Kreditwirtschaft genehmigt werden, die Terminalhersteller und Issuer, die entsprechende Applikation bei sich integrieren, und Acquirer diese Applikation letztendlich auch vertreiben.

  - Host Card Emulation (HCE): Eine Variante des Card Emulation Mode ist die sogenannte HCE. Hierbei werden die Kartendaten nicht in einem Secure Element direkt im NFC-fähigen Gerät abgelegt, sondern »remote« auf Servern. Im Gegensatz zu dem bereits relativ ausgereiften Secure Element-Ansatz wird der HCE-Ansatz erst seit der Veröffentlichung des mobilen Betriebssystems Android Kitkat 4.4 von Google stärker wahrgenommen und befindet sich noch in der Entwicklung zu einer marktfähigen Lösung. HCE benötigt generell eine Internetverbindung um die Daten vom Server

abrufen zu können. Um eine Offline Transaktion zu ermöglichen, werden sogenannte Tokens schon von der Transaktion generiert, die nur für eine begrenzte Anzahl von Transaktionen verwendet werden können. Diese Tokens werden dann auf dem Mobiltelefon gespeichert und können für Offline Transaktionen verwendet werden. Dies erfolgt meist jedoch nicht in einer derartig abgesicherten Umgebung wie bei einem Secure Element, da das Missbrauchsrisiko aufgrund der Begrenzung deutlich eingeschränkt ist. Um das Risiko im Falle der Kompromittierung zu mindern, kommen mehrere Sicherheitsmechanismen zum Einsatz, so kann u.a. die Verwendung des Token nach mehreren Faktoren begrenzt werden, z. B. Einmalzahlung oder Betragshöhe. Zudem funktioniert HCE zurzeit nur mit Mobiltelefonen, die das Betriebssystem Android Kitkat 4.4 installiert haben, welches im November 2013 veröffentlich wurde. Die Marktanteile dieses Betriebssystems steigen jedoch permanent

Kontaktloses Bezahlen über NFC ist heute bereits an 40.000 Standorten in Deutschland möglich. Über moderne Verschlüsselung und bei Beträgen über 25 Euro zusätzlich mit PIN-Abfrage, findet ein sicherer Transfer der auf dem Secure Element abgelegten Kreditkartendetails und somit die Bezahlung statt. Dem Endkonsumenten wird somit schnelles, bequemes Bezahlen mit mehr Kontrolle über seine Ausgaben, dem Wegfall von Wartezeiten und einem höheren Sicherheitsfaktor als bei der Bargeldabwicklung gewährleistet.

- Quick Response Code (QR-Code):

Bei diesem Verfahren sorgt das Smartphone für die Übertragung der Transaktionsdaten und der Zahlungsverkehrsdaten des Kunden an die Hintergrundsysteme. Ist die Transaktion erfolgreich, wird sowohl der Kunde als auch der Händler vom Hintergrundsystem informiert. Dies setzt aber voraus, dass der Akzeptanzpartner über einen eigenständigen Kommunikationskanal mit dem Zahlungsdienstanbieter verfügt, über die er gesichert die Information über die erfolgreiche Abwicklung der Transaktion erhält. Eine andere Möglichkeit besteht in der Übermittlung der erfolgreichen Transaktion in Form eines QR-Codes, die auf dem Kundengerät angezeigt und dann vom Händler abgelesen wird.

Alternativ können in ähnlicher Weise QR-Codes auch für eine Vielzahl andere Anwendungsfälle genutzt werden. So werden heute QR-Codes auf Plakaten oder in Katalogen eingesetzt, um weitere Informationen zu Produkten zu erhalten, oder eine Bestellung zu initiieren.

- Optical Character Recognition (OCR)

Als eine weitere, vergleichbare Alternative bietet sich die Bilderkennung an. Gegenstände oder Zeichen werden abfotografiert, und deren Inhalte und Bedeutung mit Verfahren der Bilderkennung analysiert und auf einen passenden Kontext ausgewertet. Entsprechende Verfahren, denen teils sehr aufwendige Berechnungen zugrunde liegen, haben sich in den letzten Jahren erheblich weiterentwickelt und sind gerade bei Auslagerung der Berechnung in die Cloud heute schon sehr gut anwendbar. So können insbesondere Logos, Produkte und Verpackungen erkannt, und mit weiteren Informationen und Aktionen verknüpft werden. In ersten Versuchen wird OCR auch schon in mobilen Geräten wie Smart Glasses erprobt, um Produkte zu erkennen und durch das bloße Anschauen bei Bedarf durch den Anwender eine Kaufaktion auslösen zu können.

Lokationsbasierte Verfahren

Darüber hinaus kann man verschiedene Verfahren als lokationsbasiert subsummieren. Hier spielen Positionen des Endnutzers und Marketingaspekte die entscheidende Rolle. Es können Daten auf mittlerer Distanz mit einem Radius von mehreren Metern ausgetauscht werden. Die Datenübermittlung ist bei solch einem Verfahren allerdings nicht mehr kontextbasiert. Die Initiierung und Zustimmung zu einer Aktion muss also unabhängig von der Datenübertragung erfolgen. Allerdings kann mit den entsprechenden Verfahren eine Positionsbestimmung des Anwenders innerhalb der Sende-/Empfangsdistanz erfolgen. Dies ermöglicht einerseits, eine genaue

Positionsbestimmung zu betreiben und Bewegungsmuster bzw. Häufungen zu identifizieren, andererseits kann auch eine Navigation in dem Senderaum durchgeführt werden. Ein weiteres wichtiges Merkmal dieser Verfahren ist, dass sie einen Check-In und die Identifizierung des Kunden ermöglichen können. So kann z. B. ein Händler erkennen welche Kunden gerade in seinem Laden sind. Hierbei kann der Kunden sowohl anonym oder persönlich erkannt werden. Gerade bei der Bezahlung könnten lokationsbasierte Indoor- Verfahren wie BLE verwendet werden, um ein sogenanntes »Frictionless Payment« zu ermöglichen. Ein Händler erhält an seinem Bezahlterminal einen Überblick aller im Laden anwesenden Kunden. Anhand des Namens oder eines Bildes kann der Kunde identifiziert werden, und mit dessen Zustimmung eine Bezahltransaktion durchgeführt werden, ohne dass der Kunde dafür sein Smart Phone aus der Tasche nehmen muss.

- Bluetooth Low Energy (BLE)

Mit Triangulation über mehrere Beacons kann damit eine Indoor-Positionsbestimmung erfolgen. Beacons selbst senden hierbei nur Signale zur eigenen Identifikation in regelmäßigen Abständen an mutmaßliche Empfänger, können selbst aber keine Daten verarbeiten. Es obliegt also der Kontrolle des Smartphones ob, wie und von wem eine Auswertung von Daten und Positionsbestimmungen erfolgen soll. BLE und Beacons haben einen deutlichen Aufmerksamkeitsschub erhalten, seit die Technologie von Apple, unter der Marke iBeacon, oder PayPal eingesetzt wird. Basierend auf BLE sind eine Reihe von Diensten möglich: Diese reichen von der gezielten Einblendung von Produktinformationen am PoS über Sonderangebote, Lenkung der Besucherwege beim Betreten eines Geschäftes bis zum mobilen Einkauf im Einzelhandel. Zudem erlauben die erfassten Daten eine detaillierte Analyse des Kaufverhaltens.

Im Museum können Besucher anhand von Beacons, die an einzelnen Ausstellungsstücken angebracht sind, durch das Museum geleitet werden. An einem Ausstellungsstück angekommen werden weitere Informationen, ein Interview mit dem Künstler und Videos der Herstellung bereitgestellt. Das Smartphone ersetzt zukünftig also klobige Audio-Guides.

- Geofencing

Bei Geofencing-Verfahren, deren Nutzung schon stark etabliert ist, wird eine Positionsbestimmung und Kommunikation über große Distanzen ermöglicht. Die Verfahren kommen gewöhnlich dann zum Einsatz, wenn der Kunde einen Laden oder ein Gebäude noch nicht betreten hat. Händler oder andere Dienstleister können über diese Verfahren mit Kunden kommunizieren, wenn diese sich nicht in unmittelbarer Nähe zu ihrem Ladenlokal befinden. Dies kann genutzt werden, um Kunden gezielt zu einer bestimmten Lokation zu führen, z. B. durch personalisierte Angebote oder Standortbestimmungen und Navigationsdienste, oder auch um Kunden Transaktionen und Dienste wie z. B. mobile Ticketing oder remote Payment-Verfahren außerhalb der eigenen physischen Lokation anbieten zu können. Dies kann sowohl über das Mobilfunknetz, GPS oder WLAN/Wifi durchgeführt werden.

6.1.2 Reichweite durch fehlende Akzeptanzstellen

Viele der beschriebenen Mobile Wallet Definitionen und Konzepte setzen auf NFC Kartenemulation. Voraussetzung ist, dass die Anwender mobile Endgeräte bzw. die Händler Terminals besitzen, mit denen NFC genutzt werden kann. Der Einsatz von NFC-Stickern kann dabei als Übergangstechnologie helfen die Akzeptanz zu erhöhen. NFC ist universell und kostengünstig einsetzbar. Durch die geringe Funkreichweite (im Zentimeterbereich), ist es weniger angreifbar durch Dritte.

Für eine erfolgreiche Marktdurchdringung von NFC-basierten Walletdiensten müssen folgende Faktoren gegeben sein:

- Die Händler müssen NFC-fähige Terminals an ihren Kassen einsetzen

- Die Issuer müssen NFC-kompatible Apps herausgeben

- Ein Secure Element muss von einem vertrauenswürdigen Anbieter ausgegeben werden. Zum Beispiel können MNO's SIM-Karten herausgeben, auf der das Secure Element platziert werden kann

- Die Verbraucher müssen einen Nutzen erkennen, um diese Technologie letztendlich einzusetzen

Nach einer aktuellen Studie[7] von GS1 und EHI werden sich in rund zwei Jahren NFC-Chips sowohl in mobilen Endgeräten als auch in Händlerterminals so verbreitet haben, dass man von einem massenfähigen Markt sprechen kann.

Die aktuell führenden Smartphone Hersteller (Samsung, Apple, LG, HTC) bieten alle Geräte mit entsprechendem NFC-Chip an. Diese Unternehmen verfügen über eine gute Ausgangslage, dieses Ökosystem nachhaltig zu beeinflussen. Sie verfügen durch ihre starken Marken und die bereits vorhandenen Vertriebs- und Marketingkanäle über einen exklusiven Zugang zu den Kunden. Der wesentliche Beitrag der Mobiltelefonhersteller in dem Mobile Wallet-Ökosystem besteht darin, die kompatible Hardware bereitzustellen, welche die höchsten technologischen Standards zur Abbildung und Verbreitung von Mobile Wallets erlaubt. Die Hersteller erfahren durch ihre langjährigen Erfahrungen das Vertrauen von den Kunden, was Sicherheit, technologischen Standard und den Nutzungsannehmlichkeiten der Mobiltelefone anbelangt.

Auch auf Terminalseite ist eine zunehmende Verbreitung dieses Standards gegeben. So wird zudem seitens der Kreditkartenschemes wie MasterCard dafür gesorgt, dass sich terminalseitig NFC durchsetzen wird. Mastercard liefert ab 1. 1. 2015 alle neuen Terminals mit NFC aus, bis 2018 sollen alle Terminals in DE NFC-fähig sein.

Viele Mobile Wallet-Projekte sind derzeit noch nicht in den massenhaften Roll-Out gegangen, sondern befinden sich in Pilotphasen. Somit kann auch bezüglich der Verbraucherakzeptanz zurzeit nur spekuliert werden.

Der Markt für Mobiles Wallet Dienste ist in Deutschland jedoch Dank der Einführung von NFC in Bewegung geraten.

6.1.3 Interoperabilität und Kompatibilität

Viele verschiedene Lösungen (NFC, QR-Codes, proprietäre Produkte) mit zum Teil nur regionaler Reichweite prägen zurzeit noch das Bild. Doch das Interesse an einer praxistauglichen mobilen Alternative wächst auch am klassischen Point of Sale. Handelsunternehmen sehen die Chance, Bezahlprozesse zu beschleunigen und damit die Durchlauf-Frequenz an der Kasse zu erhöhen. Weniger Bargeld bedeutet zudem weniger Aufwand für Zählung und Bargeldlogistik. Nicht zuletzt können die Händler mit neuen Services bei ihren Kunden punkten.

Für den Erfolg der Mobile Wallet müssen viele Parteien ihren Beitrag leisten. Bei der daraus resultierenden hohen Komplexität der unterschiedlichen Geschäftsmodelle, an denen jede Partei gewinn- bzw. nutzbringend partizipieren kann, verwundert es nicht, dass die Marktdurchdringung eher schleppend verläuft. Hierfür ist es wichtig, dass Lösungen ein hohes Maß an Interoperabilität aufweisen. Mit zunehmender technologischer Reife, flächendeckender Akzeptanzinfrastruktur einer breiten Vielfalt von weiteren Diensten neben der Bezahlung, wird es Anbietern in den nächsten Jahren gelingen, eine höhere Konsumentenakzeptanz für Mobile Wallets zu erreichen. KPMG geht aktuell mit Steigerungsraten der Ausgaben mittels Mobile Wallet in Europa von durchschnittlich 350 Prozent in den nächsten fünf Jahren aus[8]. Um das Wachstumspotenzial auch realisieren zu können bedarf es eine höheren Standardisierung der Produkte und Reichweite der Anbieter durch strategische Partnerschaften.

Die Herausforderung eines neuen Ökosystems, wenn eine Vielzahl von Unternehmen mit unterschiedlichen Geschäftsmodellen zusammen agiert, ist die Kompatibilität. Der Schlüsselfaktor für die Akzeptanz von Mobile Wallets durch die Kunden, ist der daraus entstehende

7 GSI Studie: http://www.gs1-germany.de/fileadmin/gs1/basis_informationen/mobile_in_retail_management_summary.pdf
8 Vgl. Steinbeis Research Center for Financial Services (2012): Mobile Payment – Wohin geht die Reise?

Nutzen bzw. Annehmlichkeit (Convenience). Diese können nur entstehen, wenn verschiedene Anbieter innerhalb des Ökosystems offen und konstruktiv zusammenarbeiten.

Interoperabilität sowie nichtdiskriminierende Standardisierung zwischen heterogenen technischen Systemen waren und sind ein Leitprinzip bei der Entwicklung des World Wide Web. Entwicklerschnittstellen (APIs) werden zunehmend als klassische Plattformstrategie eingesetzt, um Drittanbieter mit weiteren Nischenangeboten an das Ökosystem zu binden. Dabei werden in frühen Phasen Drittanbieter und Programmierer mit Hilfe offener Schnittstellen dazu animiert, eigene Dienste und Anwendungen auf Basis der jeweiligen Plattform aufzubauen.

Offene APIs dienen als Voraussetzung für eine nahtlose Verbindung zwischen Schnittstellen, Diensten und Applikationen (Apps), damit digitale Inhalte innerhalb und außerhalb von existierenden Webseiten zugänglich sind. Durch den Einsatz offener APIs ergeben sich für das Ökosysteme zwei entscheidende Vorteile: Erstens eröffnen sich für die Konsumenten durch die externen Applikationen neue Einsatzmöglichkeiten, während der Plattformbetreiber die Entwicklergemeinde an sich bindet und zusätzliche Lock-In-Effekte schafft. Zweitens wächst auch für das Ökosystem selbst die Attraktivität seiner Dienste, wenn komplementäre Angebote von Drittanbietern den Kundennutzen erhöhen.

Offenheit und Interoperabilität als Instrumente eines Mobile Wallet-Ökosystems leisten der Innovation, insbesondere im Bereich der ITK, gute Dienste. Sie können auf volkswirtschaftlicher Ebene zu mehr Effizienz, Produktivität und Wirtschaftswachstum führen. Zudem stellt eine grenzüberschreitende Kompatibilität einen weiteren Schlüsselfaktor für Mobile Wallet dar. Momentan werden die meisten Dienste in sich geschlossenen Netzwerken angeboten. Die Implementierung von grenzübergreifenden Lösungen für Mobile Wallets kann eine positive Rolle bei der Adaption durch die Kunden darstellen. Das Ziel ist schließlich, die physische durch die digitale Brieftasche vollständige zu ersetzen. Dies soll sowohl im In- als auch im Ausland gelten.

6.1.4 Regulierung und Compliance im Kontext der Mobile Wallet

Eine große Herausforderung stellt derzeit die aktuelle und zukünftige Gesetzgebung dar. Da dies ein sehr komplexes Umfeld darstellt, haben wir dem Ganzen ein eigenes Kapitel gewidmet. In Kapitel 7 stellen wir die drei maßgeblichen Institutionen dar, die für die Normenlandschaft und deren Aufsicht im Umfeld der Mobile Wallet verantwortlich zeichnen.

6.2 Adaption durch den Verbraucher und Aufklärung

Die Akzeptanz der Endkonsumenten zu erlangen, ist in einem gesättigten und höchst kompetitiven Markt keine leichte Aufgabe. Bereits ausgereifte Debit- und Kreditkarten-Lösungen, mit denen nahezu überall problemlos bargeldlos bezahlt werden kann, lassen Konsumenten nicht sofort erkennen, warum sie von diesem bewährten und funktionierenden zu einem neuen System, ohne offensichtlichen Mehrwert wechseln sollten. Ähnlich ergeht es Händlern, die zunächst in neue Technologie und Mitarbeiterschulungen investieren müssen, um die Wallet-Dienste über NFC-Terminals möglich zu machen. Die Finanzierung der Mobile Wallet-Infrastruktur bzw. das Erlösmodell für die Diensteanbieter ist insgesamt die größte Herausforderung.

Wie schnell sich Mobile Wallets in Deutschland etablieren werden, hängt maßgeblich davon ab, ob es den Anbietern zukünftig gelingt, Produkte mit erkennbarem Mehrwert für den Nutzer zu entwerfen. Am ehesten werden sich in Zukunft Produkte durchsetzen, die nicht nur das Komfort- und Sicherheitsbedürfnis der Konsumenten befriedigen, sondern einen konkreten Nutzen z. B. durch eine stärkere Integration von verschiedenen Services (z. B. Ticketing, Loyalty, Couponing, Access) gewährleisten.

Das Konsumentenverhalten in Bezug auf verschiedene Mobile Wallet Dienste hat sich in den vergangenen Jahren aber positiv entwickelt. Die Verbreitung von Coupons und Kundenbindungsprogrammen ist historisch bedingt. In

den USA wurden Coupons z.B. im Kontext des »Pricings« von Produkten bereits in den 40er Jahren eingesetzt und dadurch als ein positives Empfinden abgespeichert. In Deutschland und teilweise auch anderen europäischen Ländern waren Coupons als Teil rund um das Thema Versorgung/staatliche Zuteilung sehr negativ belegt.

Inzwischen haben ca. 60 Prozent der Deutschen eine Payback- oder Deutschlandkarte und kaufen mit entsprechenden Coupons ein. Darüber hinaus erfreuen sich Bonusprogramme z.B. von H&M, Deutsche Bahn, Carsharing, Mietwagen, Douglas oder von Hotelketten enormer Beliebtheit. Diese inzwischen überhand nehmenden Bonus und Treuekarten dem Endverbraucher in digitaler Form zur Verfügung zu stellen, bringt einen deutlichen Mehrwert und erhöhen die Chance für eine Adaption der Mobile Wallet durch den Endverbraucher.

6.3 Potenziale

Bei der weiteren Entwicklung ist eher davon auszugehen, dass Zusatzfunktionen sukzessive hinzukommen und die Wallets um Mehrwerte erweitert werden. In Deutschland konkurrieren derzeit ca. 30 Anbieter, die sich meist wenig voneinander differenzieren und teilweise sogar blockieren. Die Anbieter müssen aufpassen, dass sie die Anwender durch komplizierte, unausgegorene und wenig standardisierte Lösungen nicht verschrecken.

Sämtliche Studien zum Thema sehen zwar enormes WachstumsPotenzial für das Mobile Wallet Ökosystem, allerdings fokussieren sie fast ausschließlich auf dem B2C Markt. BITKOM sieht jedoch auch im B2B Segment enorme Potenziale. Derzeit gibt es keine Mobile Wallet Lösung, die auf die speziellen B2B Bedürfnisse abzielen, wie z.B. Rechnungsintegration und Controlling-Systeme & -Prozess. Das MarktPotenzial ist groß, da das Transaktionsvolumen in der Regel deutlich höher ist, als im B2C- Bereich.

Ein bis dato ebenfalls unterschätzter Bereich sind Anwendungen rund um e-Government Anwendungen wie Strafzettel, Behördenrechnungen oder Nachzahlungen, die derzeit von vielen Behörden umgesetzt werden.

6.4 Zusammenfassung

Die vollumfängliche Mobile Wallet ist noch eine Vision, der erhoffte Durchbruch ist nicht mehr fern. Sind die Deutschen einfach zu skeptisch was die Digitalisierung angeht (insbesondere auch wegen der Sicherheitsbedenken) oder sind die bestehenden Infrastrukturen so gut, dass Neuerungen nur schwer umsetzbar sind? Auch gibt es noch eine Vielzahl an Personen, die über kein Smartphone besitzen und Ältere, die mit der rasanten technologischen Entwicklung mithalten müssen. Schaffen wir es diese auf dem Weg mitzunehmen und sorgen wir für die richtigen Angebote, wird sich mit der weiteren Digitalisierung auch die Digitalisierung der Geldbörse nicht aufhalten lassen.

Natürlich gibt es in einem so komplexen Ökosystem noch einige Herausforderungen zu bewältigen, aber BITKOM ist sich sicher, dass diese Hürden in den kommenden Jahren überwunden werden. Die Aussichten sind sehr positiv zu bewerten. Das nun sämtliche führende Smartphone Hersteller auf NFC als die Schlüsselübertragungstechnologie setzten, hilft in den kommenden Jahren einen massenfähigen Markt abbilden zu können. Gemeinsam mit QR-Codes und BLE lassen sich weitere spannende Anwendungsszenarien in Kombination abbilden, sodass wir davon ausgehen, dass viele innovative neue Dienste in diesem dynamischen Ökosystem entwickelt werden.

7 Einordnung der Mobile Wallet in den regulatorischen Rahmen

Die regulatorischen Rahmenbedingungen für eine Mobile Wallet sind komplex, da sie sehr unterschiedliche Marktteilnehmer involvieren und einen durchaus komplexen Sachverhalt beurteilen müssen. Im folgenden Kapitel möchten wir darstellen, welche Institution für welchen Teil der Regulierung verantwortlich zeichnet. Darüber hinaus möchten wir auf die Debatte rund um die Verwendung von Daten eingehen, da diese Diskussion unserer Meinung nach sehr einseitig geführt wird. Das Kapitel soll helfen ein einheitliches Verständnis unter den einzelnen Gesetzgebungsinstanzen herzustellen und diese bestmöglich vor allem bei der technischen Umsetzbarkeit der Normen unterstützten. Angefangen von einer einheitlichen Begriffsdefinition der Mobile Wallet bis hin zum Umfang von regulatorischen Anforderungen im digitalen Zahlungsverkehr. Eine Überregulierung sollte hier unbedingt vermieden werden, um einen jungen Markt nicht in der Entstehung zu behindern.

7.1 Regulierung in drei Akten

Die Regulierung und Beaufsichtigung der verschiedenen Akteure im Rahmen einer Mobile Wallet kann sehr unterschiedliche Ausprägungen annehmen je nach Spielart der Mobile Wallet. Entscheidend ist zum einen, ob die Mobile Wallet eine oder mehrere Zahlfunktionen beinhaltet oder nicht. Ist dies nicht der Fall, so sind insbesondere Datenschutzaspekte zu berücksichtigen. Wenn Zahlfunktionen enthalten sind, ist zu prüfen, ob die Zahlungsdiensteaufsichtsregulierung zur Anwendung kommt. Hinzu kommen in solchen Fällen sodann häufig Pflichten zur Geldwäscheprävention.

Im Zahlungsverkehr sind auf europäischer Ebene folgende Institutionen maßgeblich für die Regulierung, sowie die Aufsicht verantwortlich. Dies sind zum einen das Europäische Parlament und Rat, die auf Vorschlag der Europäischen Kommission die für den Zahlungsverkehr maßgeblichen Richtlinien, die Zahlungsdiensterichtlinie-PSD 1[9] und die Erste[10] und Zweite E-Geld-Richtlinie[11], erlassen haben. Europäische Richtlinien entfalten ihre volle Wirkung erst, wenn sie in nationales Recht umgesetzt sind; hierzu sind die Mitgliedstaaten innerhalb eines Zeitraums von in der Regel 2 Jahren nach Erlass verpflichtet. In der Folge der PSD1 und der Zweiten E-Geld-Richtlinie hat jeder Mitgliedstaat sein nationales, von den Richtlinien geprägtes Zahlungsdiensteaufsichtsrecht und E-Geld-Aufsichtsrecht (in Deutschland beides im ZAG) erlassen; die Vorschriften sind wegen der vereinheitlichenden Wirkung der Richtlinien ganz überwiegend identisch.

Die PSD 1 wird derzeit überarbeitet. Zudem läuft derzeit noch ein Gesetzgebungsverfahren für den Erlass einer Verordnung für Debit- und Kreditkarten (bekannt als Verordnung über Multilaterale Interchange Gebühren). Mit einem Inkrafttreten der reformierten Zahlungsdiensterichtlinie (PSD 2) wird derzeit im Frühjahr 2015 gerechnet. Die neuen Regelungen müssen sodann voraussichtlich innerhalb einer Frist von zwei Jahren in nationales Recht umgesetzt werden und finden erst danach Anwendung auf die Erbringung von Zahlungsdiensten.

Weiterhin sind im Zahlungsverkehr die Empfehlungen (z. B. die SecuRe Pay Empfehlungen) der Europäischen Zentralbank (EZB) von Bedeutung; diese Empfehlungen sind von den beaufsichtigten Finanzinstituten nach dem

9 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG, ABl. EU L 319, S. 1.

10 Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, ABl. EU L 275, S. 39.

11 Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, ABl. EU L 267, S. 7.

Grundsatz »comply or explain« umzusetzen. Die Europäische Bankenaufsichtsbehörde (EBA) mit Sitz in London hat im Zahlungsverkehr keine unmittelbaren aufsichtsrechtlichen Eingriffsbefugnisse; nach der im Gesetzgebungsverfahren befindlichen, zukünftigen Regulierung (PSD2) soll sie insbesondere ein zentrales Register führen sowie in Ausführung der PSD2 einheitliche Richtlinien für Datenschutz und Sicherheit bei Zahlungstransaktionen erlassen.

Als weiterer Akteur ist das European Payments Council (EPC) zu nennen, welches eine Einrichtung der Kreditinstitute in der EU ist. Das EPC hat in der Vergangenheit zahlreiche Standards für die wesentlichen Zahlungsarten, insbesondere Überweisungen, Lastschriften und Kartenzahlungen, erlassen. Zweck ist die Realisierung und Umsetzung des einheitlichen Euro-Zahlungsverkehrsraums SEPA (Single Euro Payments Area).

Im nationalen Rahmen und in der Praxis entscheidend sind die nationalen Aufsichtsbehörden, deren Aufgabe die Anwendung und Durchsetzung des europäisch geprägten Aufsichtsrechts ist. In Deutschland kommt hier der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine ganz wesentliche Bedeutung zu. Auch die Bundesbank spielt eine wichtige Rolle im Rahmen der nationalen Zahlungsverkehrsaufsicht.

7.1.1 Zahlungsdiensteregulierung auf europäischer und nationaler Ebene

Als Anbieter kommen Unternehmen in Frage, die eine mobile Applikation entwickelt und die dahinter liegende Infrastruktur der Abwicklung von Transaktionen, Bestellservices und Akzeptanzstellen errichtet haben, in Betracht. Hier möchten wir uns wieder auf die Definition aus Kapitel 3.1.1 beziehen, nach der eine Mobile Wallet selbst kein Zahlungsdienst ist, sondern nur eine Infrastruktur die es ermöglicht eine oder mehrere Paymentdienste/Zahlungsinstrumente gemäß Kapitel 4.2.1 neben weiteren Diensten im Wallet anzubieten. Sofern allerdings Zahlungsdienste in die Wallet integriert werden, ist zu prüfen, ob der Betreiber der Wallet und / oder der Anbieter des jeweiligen Zahlungsdienstes von der Zahlungsregulierung erfasst werden. Klassische Zahlungsdienste, wie z. B. Prepaid-Kreditkarten oder Lastschriftverfahren, die in der Mobile Wallet hinterlegt werden können, unterfallen grundsätzlich der Regulierung nach den jeweiligen zahlungsaufsichtsrechtlichen Regelungen.

Der Walletbetreiber und/ oder der Anbieter eines Zahlungsdienstes für Mobile Wallets können jedoch entscheiden, ihr Geschäft derart zu gestalten, dass sie dieses außerhalb der Zahlungsdiensteregulierung betreiben können. Hier stehen gewisse Ausnahmebestimmungen im Rahmen der Zahlungsaufsichtsgesetze zur Verfügung.

Der Betreiber eines Mobile Wallets kann selbst bei Einbindung von Zahlungsdiensten seine Tätigkeit so ausgestalten, dass er von der Ausnahmeregelung für technische Dienstleister profitiert: Dienste, die von technischen Dienstleistern erbracht werden, die zwar zur Erbringung der Zahlungsdienste beitragen, jedoch zu keiner Zeit in den Besitz der zu transferierenden Geldbeträge gelangen, wie die Verarbeitung und Speicherung von Daten, vertrauensbildende Maßnahmen und Dienste zum Schutz der Privatsphäre, Nachrichten- und Instanzenauthentisierung, Bereitstellung von Informationstechnologie- (IT-) und Kommunikationsnetzen sowie Bereitstellung und Wartung der für Zahlungsdienste genutzten Endgeräte und Einrichtungen unterfallen nicht dem Anwendungsbereich des ZAG / PSD 1.

Diese Gestaltung kommt in Betracht, wenn die Zahlungsfunktion nicht von dem Betreiber der Wallet, sondern von einem zugelassenen Zahlungsinstitut, von einem E-Geld-Institut oder von einer Bank bereitgestellt wird. Es ist dann noch immer zu prüfen, ob der Betreiber der Mobile Wallet nicht E-Geld-Agent oder Zahlungsagent ist und deshalb bestimmte Anzeigepflichten und sonstige Formalia zu erfüllen sind.

Beschränkt sich der Anbieter der Wallet nicht auf die technische Dienstleistung der Bereitstellung der Wallet-Infrastruktur, so stehen ihm ggf. andere Ausnahmebestimmungen zur Verfügung. Der Anbieter kann entscheiden, lediglich ein beschränktes Angebot an Produkten (z. B.

Tickets im ÖPNV, Tankstellenprodukte) oder Dienstleistungen (Beförderungsleistungen) über die Mobile Wallet bezahlen zu lassen. In solchen Fällen kann es möglich sein, die Zahlungen ohne Erlaubnis nach dem Zahlungsaufsichtsrecht abzuwickeln; Einzelfälle sollten sorgfältig geprüft und ggfs. mit der nationalen Aufsichtsbehörde abgestimmt werden. Erlaubnisfrei sind Zahlungsdienste auch, wenn hierüber nur bei wenigen angeschlossenen Akzeptanzstellen (z. B. alle Getränkeanbieter innerhalb eines Fußballstadions, sonst regional begrenzte Angebote oder beschränkt auf eine bestimmte Ladenkette) bezahlt werden kann[12]. Ob Lösungen für Franchiseketten oder innerhalb von Einzelhandelskonzernen[13] erlaubnisfrei sind, kann nur im Einzelfall beurteilt werden.

Die Nutzung von Ausnahmen für digitale Güter kommt z. B. für MNO's in Betracht. Wenn mit der Mobile Wallet nur solche Güter bezahlt werden können, die der Kunde über sein Smartphone, seinen PC oder Tablet beziehen und nutzen kann (digitale Zeitungen, Klingeltöne, Apps, Musikdownloads), ist dies für den MNO, der die Bezahlung über die Telefonrechnung oder über die Handy-Prepaidcard abrechnet, erlaubnisfrei. Im Einzelfall können weitere Ausnahmevorschriften eingreifen.

Im oben angesprochenen Gesetzgebungsverfahren zur PSD 2 sind auch die Ausnahmebestimmungen Gegenstand intensiver Debatten. In der Tendenz gehen die Bestrebungen der europäischen Institutionen (Kommission, Parlament und Rat) dahin, die Ausnahmen im Rahmen der Reform mehr oder weniger stark einzuschränken. In den Details besteht hier noch keine Einigkeit[14].

Die genannten Ausnahmen sollten mit den zuständigen Aufsichtsbehörden, in Deutschland mit der Bundesanstalt für Finanzaufsicht, abgestimmt werden.

Im Rahmen der Ausgestaltung einer Mobile Wallet ist eine der Weichenstellungen die Frage, ob eine Mobile Wallet von der Zahlungsregulierung erfasst wird und in der Folge deshalb eine Erlaubnis nach dem Zahlungsdiensteaufsichtsgesetz (ZAG) in Deutschland oder – bei Sitz außerhalb Deutschlands – den entsprechenden Zahlungsaufsichtsgesetzen anderer EU-Länder benötigen; diese Gesetze sind innerhalb der EU und des EWR auf Basis der PSD 1 und der Zweiten E-Geld-Richtlinie weitestgehend vereinheitlicht. Mobile Wallets sind weder in den Richtlinien noch im ZAG definiert.

Wenn der Anbieter der Mobile Wallet die Zahlfunktionen nicht derart beschränken will, wie es die Ausnahmebestimmungen verlangen, unterfallen die Zahlungsdienste – wie oben erwähnt – der Erlaubnispflicht nach dem Zahlungsdiensteaufsichtrecht und es bleiben dem Anbieter der Mobile Wallet im Wesentlichen zwei Lösungsmöglichkeiten. Er kann selbst für den Zahlungsdienst eine Erlaubnis als Zahlungsinstitut oder eine Erlaubnis als E-Geld-Institut im Staat seines Sitzes beantragen. Möchte der Payment-Anbieter vermeiden, selbst der Regulierung von Zahlungsgeschäften oder E-Geld zu unterfallen, so kann er eine Kooperation mit einem Zahlungsinstitut, einem E-Geld-Institut oder einer Bank vereinbaren. Im letzteren greift der Anbieter auf die aufsichtsrechtliche Erlaubnis dieser Institute zurück und kann zugleich ggf. von dessen Mitgliedschaft bei Mastercard und Visa oder von dessen Angebot an alternativen Zahlungslösungen profitieren.

Im Fall einer Kooperation zwischen dem Anbieter des Mobile Wallet Payment Dienst und einem Institut (Zahlungsinstitut, E-Geld-Institut oder Bank) trägt das Institut die aufsichtsrechtliche Verantwortung für die Abwicklung der Zahlungen, für die Herausgabe des E-Geldes und für die Sicherheit der Kundengelder. Zudem obliegt dem Institut auch die Einhaltung der geldwäscherechtlichen Sorgfaltspflichten; gerade letztere Compliance-Obliegenheit war in der Vergangenheit oftmals entscheidend für die Gestaltung von Mobile Payment-Produkten. Eine Änderung hat sich jüngst ergeben, indem das Bundesministerium der Finanzen die Möglichkeit einer Online-Identifizierung zugelassen hat[15]. Das Institut, unter

12 Weitere Beispiele bei Findeisen, in: Ellenberger/Findeisen/Nobbe, Zahlungsverkehrsrecht, 2. Aufl. 2013, §1a Rn. 80ff.; Terlau, in: Casper/Terlau, Zahlungsdiensteaufsichtsgesetz, 1. Aufl. 2014, §1a Rn. 79 ff.

13 In Frankreich gab es hierzu die Printemps-Entscheidung des obersten franz. Verwaltungsgerichts, vgl. Terlau, Betriebsberater 2013, 1996 ff.

14 Vgl. die einzelnen Berichte auf www.payment-law.eu

dessen regulatorischem Erlaubnisschirm die Zahlungen im Rahmen der Mobile Wallet abgewickelt werden, ist zudem für die Einhaltung der (privatrechtlichen) Regularien der verschiedenen Zahlungsarten (Kreditkartenschemes, PayPal, Yapital, Sofort AG, Giropay etc.) und sonstiger privatrechtlicher Regularien (z. B. der EMVCo: NFC-Zahlung mit dem EMV-Chip ohne PIN bis maximal 25 Euro pro Transaktion) verantwortlich. Diese verschiedenen Compliance-Verantwortlichkeiten wird das Institut im Vertrag mit dem Anbieter der Mobile Wallet regeln wollen und ist hierzu aufsichtsrechtlich (Stichwort: finanzaufsichtsrechtliche Auslagerung) und aufgrund der privatrechtlichen Regularien der Zahlungsschemes verpflichtet.

Wird die Zahlfunktion der Mobile Wallet über E-Geld angeboten, so kommt als Institut für eine Kooperation nur ein E-Geld-Institut oder eine Bank (Kreditinstitut im Sinn der EU-Bankenrichtlinie) in Betracht. Beispiele für E-Geld sind: PayPal, Yapital, prepaid-Kreditkarten. In diesem Fall ist der Anbieter der Mobile Wallet in der Regel ein sogenannter E-Geld-Agent. Dies hat eigene aufsichtsrechtliche Pflichten des Anbieters zur Folge, in Deutschland insbesondere auch wesentliche geldwäscherechtliche Pflichten. Dieses Pflichtenprogramm sollte dringend mit in die Gestaltung des Produktes und der Aufgabenverteilung zwischen dem Anbieter und dem Institut einbezogen werden.

Im Rahmen von E-Geld-Produkten und zukünftig auch bei Zahlungskonten kommt zudem in Betracht, die geldwäscherechtliche Compliance der Produkte, insbesondere durch betragliche (100 Euro) und Verwendungs-Beschränkungen, aber auch durch besonderes Monitoring der Institute, so zu gestalten, dass vereinfachte Prüfungspflichten eingreifen, die das Freischalten von neuen Kunden wesentlich vereinfachen. In diesem Fall ist es jedoch erforderlich einen entsprechenden Antrag auf vereinfachte Sorgfaltspflichten bei der BaFin zu stellen und das Ergebnis der Prüfung abzuwarten.

Eine Besonderheit wird sich nach Inkrafttreten und Umsetzung der PSD2, also voraussichtlich ab 2017, für Mobile Payment-Produkte ergeben, die Überweisungen und Lastschriften verwenden. Im Rahmen der PSD2 wurde die Figur des dritten Zahlungsdienstleisters (auch TPP – third party payment services provider – genannt) erfunden. Hierbei handelt es sich um einen Dienstleister, der den Zugang zu Informationen eines Zahlungskontos eröffnet oder der die Autorisierung von Zahlungsvorgängen (Überweisungen und Lastschriften) über ein Zahlungskonto ermöglicht, ohne selbst das kontoführende Institut zu sein. Dies könnte für viele Anbieter von Mobile Payments zur Folge haben, dass sie bereits aus diesem Grund der Eröffnung des Zugangs zu einem Zahlungskonto der Erlaubnispflicht als Zahlungsinstitut unterfallen werden. Allerdings dürfte diese regulierte Tätigkeit auch der Auslagerung zugänglich sein, so dass ein Anbieter auch hier im Rahmen einer Kooperation mit einem regulierten Institut ohne eigene Lizenz tätig werden kann. Der im Juli 2013 in das Gesetzgebungsverfahren eingebrachte Vorschlag der EU-Kommission hat seither zahlreiche, teils gravierende Änderungen im Parlament und jüngst im Rat erfahren[16]. Es ist noch nicht klar vorhersehbar, wie die Regulierung hier im Detail im Jahr 2017 aussehen wird. Entscheidend ist, den Gesetzgebungsorganen und den beteiligten Behörden klar zu machen, dass die beabsichtigte Regulierung des TPP nicht unerwünschte Auswirkungen auf andere Zahlungsdienste, wie z. B. Zahlungsfunktionen in Mobile Wallets, hat.

7.1.2 Mobile Wallets und Sicherheit – Europäische Zentralbank (EZB)

In den vergangenen Jahren ist der E-Commerce eines der dynamischen Wachstumssegmente gewesen. Die EU strebt vor diesem Hintergrund eine Neuregelung der Sicherheit in der Zahlungspraxis an. Die Europäische Kommission hat in ihrem Entwurf der PSD 2 vom 23. Juli 2013 einen gesonderten Artikel für die Zahlungssicherheit bei elektronischen Zahlungsvorgängen vorgesehen; die PSD 2

15 Hierzu Terlau, Interview in der Börsen-Zeitung vom 23. August 2014; ders., Auf dem Weg zur Wettbewerbsfähigkeit der deutschen Zahlungsverkehrsregulierung – Anerkennung der Online-Identifizierung durch das Bundesministerium der Finanzen, jurisPR-BKR 8/2014, Anm. 1; www.juris.de, erschienen am 19.8.2014.

16 Auch hierzu vgl. verschiedene Abhandlungen unter www.payment-law.eu.

befindet sich derzeit im europäischen Gesetzgebungsverfahren. Die EZB hat dazu gemeinsam mit den Aufsichtsbehörden und Zentralbanken der Mitgliedstaaten (das sog. SecurRe Pay Forum) Empfehlungen für den sicheren Zahlungsverkehr im Internet und auf mobilen Endgeräten (SecuRePay) auf den Weg gebracht.

Bis Februar 2015 (Internetzahlungen) und bis Februar 2017 (mobile Zahlungen) sollen die Empfehlungen der EZB von den darin adressierten Banken, Zahlungsinstituten und E-Geld-Instituten umgesetzt sein. Ein weiteres Empfehlungswerk zu Account Access Providers befindet sich ebenfalls in der Diskussion.

Die Empfehlungen der EZB sind nicht ein verbindliches Regelwerk. Vielmehr gilt der Grundsatz »Comply« or »Explain and Justify«, d.h. die darin angesprochenen Zahlungsdienstleister werden nach Ablauf der Umsetzungsfrist im Rahmen der Prüfung ihrer internen Organisation und ihres Risikomanagements durch die nationale Aufsichtsbehörde und/ oder ihren Abschlussprüfer die Befolgung darlegen müssen oder aber die von ihnen erarbeiteten, alternativen Vorkehrungen erläutern und im Hinblick auf das Regelungsanliegen der Empfehlungen ggf. rechtfertigen müssen.

Wesentliche SecurRe Pay Empfehlung ist die starke Authentifizierung. Diese Empfehlung ist insbesondere für mobile Zahlungen als auch für Sicherheitsanforderungen bei dem Zugriff auf Zahlungsdaten aus der Cloud bedeutsam. Starke Authentifizierung gemäß SecuRePay ist grundsätzlich eine Zwei-Faktor-Authentifizierung.

In der laufenden Diskussion haben wir festgestellt, dass viele mit dem Terminus starke / harte Authentifikation Probleme haben. Daher haben wir diese im folgenden Abschnitt ausführlich dargestellt.

Authentifizierung bezieht sich auf eine Definition der PSD 1, wonach Authentifizierung ein Verfahren ist, mit dessen Hilfe der Zahlungsdienstleister die Nutzung eines bestimmten Zahlungsinstruments, einschließlich seiner personalisierten Sicherheitsmerkmale, überprüfen kann. Anders als bei der Identifizierung nach dem Geldwäschegesetz geht es hierbei also nicht um die Identität der Person, sondern um die Berechtigung zur Nutzung des ausgegebenen Zahlungsinstruments (z.B. Nutzung einer Online-Banking-Überweisung).

Bei den Authentifizierungsarten unterscheidet man drei Kategorien:

- Wissensbasierte Authentifizierung
- Besitzbasierte Authentifizierung
- Eigenschaftsbasierte Authentifizierung

Die wissensbasierte Authentifizierung erfordert ein spezielles, nur dem Benutzer bekanntes Wissen, beispielsweise ein Passwort, eine PIN oder die Antwort auf eine vordefinierte Frage. Dabei spielt die Güte des Authentifizierungsmerkmals für die Effektivität eine zentrale Rolle, welche sich beispielsweise durch eine Passwort-Policy beeinflussen lässt. Normalerweise werden wissensbasierte Authentifizierungsmerkmale in Kombination mit einer Benutzerkennung verwendet, die auch öffentlich bekannt sein darf. Dabei ist aber die Benutzerkennung selbst kein Mittel der Authentifizierung im Sinn der SecuRe Pay Empfehlungen.

Die besitzbasierte Authentifizierung beruht auf dem persönlichen Besitz eines Benutzers. Dabei wird z.B. bei der Authentifizierung der Besitz einer SIM-Karte, eines Zertifikats oder eines Smartphones vorausgesetzt. Diese Methode ist oftmals kosten- bzw. aufwandsintensiver als die wissensbasierte Authentifizierung, da sie die Anschaffung von Objekten voraussetzt und diese wiederum defekt sein oder verloren gehen können.

Die eigenschaftsbasierte Authentifizierung oder auch biometrische Authentifizieurng (die PSD 2 spricht von »Inharenz«) erfolgt auf Basis eindeutiger Merkmale des Benutzers, so wie beispielsweise seines Fingerabdrucks, der Stimme oder der Iris. Im Gegensatz zu wissens- oder besitzbasierten Authentifizierungsmerkmalen, sind diese nicht einfach auf andere Personen übertragbar. Dabei ist zu beachten, dass sich auch biometrische Merkmale, wie beispielsweise das Gesicht, durch Alterung verändern könnten. Dies sollte bei der Wahl eines zur

Vorteile	Herausforderungen
■ Kostengünstig und einfach zu implementieren, keine Zusatzhardware/-software beim Nutzer nötig ■ Keine Erkennungsfehler bzw. fehlerhafte Zurückweisungen (es gibt u.a. keine Abnutzung wie beispielsweise bei Smartcards) ■ Einfache Verfügbarkeit ■ Sicherheit steigt mit Zunahme des Informationsgehalts	■ Wissensbasierte Authentifizierungsmerkmale sollten nicht wiederverwendet werden – bei vielen Diensten steigt die Komplexität / sinkt die Praktikabilität ■ Wissensbasierte Authentifizierungsmerkmale sollten nicht wiederverwendet werden – bei vielen Diensten steigt die Komplexität / sinkt die Praktikabilität ■ Bietet Möglichkeit zur unbemerkten Vervielfältigung ■ Durch Komplexität sinkt die Praktikabilität – bei geringer Komplexität besteht das Risiko einer Entschlüsselung

Tabelle 1: Wissensbasierte Authentifizierung; Quelle:KPMG

Vorteile	Herausforderungen
■ Kompromittierung kann schnell und einfach erkannt werden ■ Merkmal kann bei Bedarf ausgetauscht oder ersetzt werden ■ Merkmal kann einer Person eindeutig zugewiesen werden ■ Die Anfertigung einer Kopie ist nur mit hohem Aufwand möglich	■ Bei physischen besitzorientierten Authentifizierungsmerkmalen kann es durch Abnutzung zu Erkennungsfehlern bzw. falscher Zurückweisung kommen ■ Können verloren bzw. gestohlen werden ■ Eventuelle Zusatzsoftware /-hardware muss beschafft werden und verursacht Kosten ■ Sind nicht immer verfügbar (können z.B. zu Hause vergessen werden)

Tabelle 2: Besitzbasierte Authentifizierung; Quelle:KPMG

Vorteile	Herausforderungen
■ Die Komplexität des persönlichen Merkmals ist nicht durch kognitive Fähigkeiten eingeschränkt ■ Einzigartiges Authentifizierungsmerkmal / lässt sich eindeutig einer Person zuordnen ■ Kann nicht unmittelbar gestohlen oder weitergegeben werden ■ Hohe Praktikabilität	■ Einige Merkmale können sich im Laufe der Zeit verändern (z.B. durch Alterung) und dadurch zu Erkennungsfehlern bzw. falscher Zurückweisung führen ■ Bei Kompromittierung kann das Merkmal nicht gewechselt werden / Extrem Fehlerintolerant ■ Eventuelle Zusatzsoftware /-hardware muss beschafft werden und verursacht Kosten – Technische Umsetzung teilweise zu aufwändig ■ Personenbezogene Daten / Datenschutz

Tabelle 3: Eigenschaftsbasierte Authentifizierung; Quelle:KPMG

Authentifizierung geeigneten biometrischen Merkmals berücksichtigt werden, da dieses sich unmittelbar, fehlerfrei und eindeutig identifizieren lassen sollte.

Für die Realisierung einer starken Authentifizierung – die für die eindeutige Identifikation eines Individuums unabdingbar ist – ist es notwendig mindestens zwei der drei beschriebenen Authentifizierungsarten in den Prozess einzubinden. Hier spricht man dann von einer starken oder einer zwei Faktor-Authentifizierung. Zudem ist erforderlich, dass einer der beiden Faktoren lediglich einmal verwendbar ist (z. B. One-Time-Passwords) oder aber aus der Kategorie Inhärenz stammt. Es kommen noch weitere Anforderungen hinzu, die in den SecuRe Pay Empfehlungen sowie in der dazu ergangenen Guidance ersichtlich sind . Werden allerdings nur zwei Authentifizierungsmerkmale einer Methode genutzt (z. B. ein Schlüssel und eine Zugangskarte) spricht man nicht von einer starken Authentifizierung, da die Mindestanforderung in diesem Fall nicht erfüllt ist. Erst durch die Kombination der Methoden werden die Schwachstellen der jeweiligen Authentifizierungsarten größtenteils kompensiert. So werden z. B. der Verlust eines besitzbasierten Merkmals oder die unbefugte Weitergabe eines wissensbasierten Kriteriums in ihren negativen Folgen beschränkt. Ein klassisches Beispiel für starke Authentifizierung ist das Geldabheben an einem Geldautomaten, bei dem sowohl Wissen (PIN) als auch der Besitz (Geldkarte) zur Authentifizierung genutzt wird.

7.1.3 Mobile Wallets und SEPA – European Payments Council (EPC)

Die SEPA (Single Euro Payments Area) ist ein Raum, in dem Bürger, Unternehmen und sonstige Wirtschaftsakteure innerhalb Europas (unabhängig von ihrem Wohn- oder Aufenthaltsort) Euro-Transaktionen in Form der SEPA-Überweisung (SEPA Credit Transfer) und SEPA-Lastschrift (SEPA Direct Debit) nutzen können. Zur Realisierung der SEPA gründeten die europäischen Kreditinstitute das EPC, welches im ersten Schritt ein Regelwerk für die SEPA-Überweisung und die SEPA-Lastschrift erarbeitete und im weiteren Schritt u.a. die SEPA Kartenzahlung (SEPA Cards Clearing) betrachtet.

Die europäische Kommission sieht die SEPA als weiteren wichtigen Schritt zur Vollendung des europäischen Binnenmarktes nach der Einführung des Euro. Dem zu Folge hat sie eine EU-Verordnung (»SEPA-Regulation«) veranlasst, die europaweit die Nutzung der SEPA-Instrumente sowie die Abschaltung der lokalen Verfahren (in Deutschland die DTA-Überweisung und DTA-Lastschrift) ab 1. Februar 2014 vorschreibt. Das deutsche SEPA-Begleitgesetz wurde am 8.November 2012 durch den Deutschen Bundestag in zweiter und dritter Lesung verabschiedet und regelt, welche Optionen der EU-Verordnung für Deutschland in Anspruch genommen werden und dass die BaFin die zuständige Aufsichtsbehörde ist, welche die Verstöße gegen die EU-Verordnung sanktioniert.

Für viele Teilnehmer war gerade die unterschiedliche Interpretation und Auslegung zwischen SEPA Rulebooks des EPC und der EU Verordnung sehr verwirrend. BITKOM setzt sich nach wie vor für eine Vereinfachung der Rulebooks im Sinne der deutschen Wirtschaft ein und steht in ständigem Austausch mit den entsprechenden Gremien.

SEPA bringt eine Vielzahl von Neuerung mit sich, die für sämtliche Marktteilnehmer sowohl Chancen als auch Risiken birgt, insbesondere für Firmenkunden und Lastschrifteinreicher. Das SEPA Direct Debit (SDD), welches im Zuge der SEPA Einführung die herkömmliche Lastschrift abgelöst hat, ist hier auch der Link zur Mobile Wallet. In vielen Wallets ist als Zahlungsmittel eine SDD hinterlegt. Leider ist es dem EPC bis dato nicht gelungen eine zukunftsträchtige Definition des dafür nötigen Mandats in den entsprechenden SEPA Rulebooks zu hinterlegen. BITKOM tritt dafür ein, dass es die Möglichkeit für nationale Lösungen geben muss, wenn diese dem nationalen Recht entsprechen. In Deutschland sind dies Lösungen, die der Textform und telekommunikativer Übertragung Rechnung tragen.

7.2 Datenschutz und Mobile Wallets

Neben den Aspekten rund um den Zahlungsdienst spielen gerade die Datenschutzaspekte bei der Etablierung eines

Mobile Wallet-Ökosystems in Deutschland mehr noch als in anderen Ländern eine entscheidende Rolle.

Die Behandlung von Daten muss sensibel betrachtet und behandelt werden, da sich aus ihnen ableiten lässt, was ein Kunde zu welchem Zeitpunkt und an welchem Ort gekauft hat.

Die Datenschutzdiskussion in Deutschland ist jedoch davon geprägt, dass die Risiken von Datensammlungen und -auswertungen sehr einseitig betont werden. Die Chancen, auch zur Verbesserung der Lebensqualität der Konsumenten, die sich durch die zielgerichtete Verarbeitung ergeben, werden in der Diskussion noch zu oft vernachlässigt. Daher empfinden Konsumenten die datenschutzrechtliche Diskussion um neue Technologien und Verfahren oft als bedrohlich, was sich erkennbar auch in erheblicher Verunsicherung auf die schnelle Verbreitung sinnvoller Verfahren auswirkt.

Wichtig ist festzuhalten, dass viele dieser Daten für Risikomanagementsysteme verwendet werden, die helfen gezielt Betrugsmuster zu erkennen, den Endkonsumenten vor Missbrauch zu schützen und insgesamt die Sicherheit im Zahlungsverkehr zu gewährleisten. Der BITKOM möchte daher die zentrale Frage rund um Datensicherheit & Betrugsprävention in einem offenen und konstruktiven Dialog angehen, um über Chancen und Risiken frühzeitig aufzuklären, und bei der Findung eines gesellschaftlichen Konsenses mit einer ausgewogenen Balance aktiv zu unterstützen.

7.3 Zusammenfassung

Bei der Umsetzung der Authentifizierungsmethoden im mobilen Bereich ist sowohl die Sicherheit, als auch die Anwenderfreundlichkeit zu berücksichtigen. Das heißt, dass die Gegebenheiten bzw. Leistungseigenschaften der Geräte, aber auch die IT-Kenntnisse der Anwender bei den Authentifizierungstechniken berücksichtigt werden müssen, damit das Mobile Wallet eine weite Verbreitung finden kann. Zudem gilt es zu beachten, dass der Smartphone-Markt in seinen Standards und Spezifikationen stark heterogen ist, was auf viele verschiedene Hersteller und die enorme Innovationsgeschwindigkeit zurückzuführen ist. Der BITKOM ist der Meinung, dass eine

umfassende starke Authentifizierung gemäß SecuRePay nicht zielführend ist, sondern durch eine entsprechend risikobasierend angemessene Authentifizierung ersetzt werden sollte.

Es besteht kein Zweifel daran, dass ein Missbrauch von personenbezogenen Daten auch im Mobile Wallet-Ökosystem verhindert werden muss. Andererseits müssen die Konsumenten auch wie mündige Bürger behandelt werden, die selbst bestimmen dürfen, dass sie im Zweifel auch einer umfassenden Datenverarbeitung zustimmen, wenn aus ihrer Sicht die Vorteile überwiegen. Wichtige Aspekte um die Akzeptanz zu steigern sind auch, dass das Haftungsrisiken beim Wechsel von Debit- auf Kreditsysteme ausgeschlossen werden, spezielle Vorkehrungen zum Schutz von Jugendlichen getroffen werden, oder auch die Nutzungsbarrieren für besondere Personengruppen zu senken.

Es ist daher Vorsicht geboten um diesen noch jungen Markt nicht durch Überregulierung oder auch zu kritische Debatte das WachstumsPotenzial zu entziehen und damit Innovation und Fortschritt in Deutschland zu bremsen. Durch diesen Ansatz vermeidet man Misstrauen und Ablehnung. Nutzerdaten werden heute fast in jedem Bereich des Alltags verwendet und ausgewertet. Das wissen jedoch nur wenige Kunden, daher sind viele verunsichert, wenn sie über Umwege (z. B. von Datenschutzverbänden, Verbraucherverbänden) darüber informiert und sensibilisiert werden. Die im Ökosystem teilnehmenden Partner sollten daher mit dem Thema Datensicherheit transparent umgehen und für ihre Position beim Kunden werben.

Wesentlich für den Erfolg der Mobile Wallets im deutschen Markt wird sein, dass auf der einen Seite ein junger sich entwickelnder Markt nicht durch übermäßige Regulierung in der Entstehung behindert wird und auf der anderen Seite Betrugs- oder Missbrauchsszenarien verhindert werden, um das Vertrauen der Verbraucher nicht zu enttäuschen. Es gilt also eine Balance zwischen den verschiedenen Rechtsgütern zu finden und Regulierung nur mit Augenmaß anzulegen.

8 Fazit und Ausblick

Fakt ist: die Mobile Wallet kommt! Und dies schneller als aktuell von vielen prognostiziert. Allerdings gibt es natürlich noch einige Herausforderungen, die es gilt zu adressieren.

Während Dinge wie Übertragungsstandard und fehlende Akzeptanzstellen nur eine Frage der Zeit sind, gilt es das Kundenvertrauen zu adressieren und die Vereinbarkeit von Innovationen/ neuen Geschäftsmodellen und zukünftigen Gesetztesvorhaben zu diskutieren.

Nachdem sich inzwischen sämtliche führende Smartphone Hersteller zum NFC Standard bekannt haben und die Kassenterminals immer weiter umgerüstet werden, fällt das von vielen heraufbeschworene Henne/ Ei Dilemma weg. Es wird nicht mehr heißen, wer folgt wem, sondern nur noch wer macht nicht mit!

Durch die anhaltende sehr einseitig betrachtete Diskussion rund um Daten- und Informationssicherheit, haben wir festgestellt, dass das allgemeine Vertrauen in Internetanwendungen gelitten hat. Hier gilt es, die Kunden über entsprechende Sicherheitsvorkehrungen aufzuklären und sie in die Lage zu versetzten, digitale Anwendungen zu verstehen. Nur wenn der Endkunde den Mobile Wallet Stakeholdern im Umgang mit seinen sensiblen Daten Vertrauen entgegen bringt, werden sich erfolgreiche Geschäftsmodelle entwickeln und Kunden Loyalität einstellen. Es besteht kein Zweifel daran, dass ein Missbrauch von personenbezogenen Daten auch im Mobile Wallet-Ökosystem verhindert werden muss. Andererseits gibt es Verbraucher die durchaus bereit sind Informationen von sich preis zu geben, wenn Sie damit aus Ihrer Sicht einen Vorteil erlangen. Von Payback, über Deutschland Karte bis zu Miles&More gibt es unzählige Beispiele, die in der Mobile Wallet nicht anders, sondern nur digital genutzt werden und seit Jahren gängige und gelebte Praxis darstellen.

Bei zukünftigen Regulierungsbestrebungen muss aus BITKOM-Sicht stärker die Risikoabschätzung des jeweiligen Anwendungsszenarios im Vordergrund stehen, um sowohl die Sicherheit, als auch die Anwenderfreundlichkeit in entsprechendem Maße zu berücksichtigen. Es ist daher Vorsicht geboten um diesen noch jungen Markt nicht durch Überregulierung oder auch zu kritische Debatte das WachstumsPotenzial zu entziehen und damit Innovation und Fortschritt in Deutschland zu bremsen.

Wesentlich für den Erfolg der Mobile Wallets im deutschen Markt wird sein, dass auf der einen Seite ein junger sich entwickelnder Markt nicht durch übermäßige Regulierung in der Entstehung behindert wird und auf der anderen Seite Betrugs- oder Missbrauchsszenarien verhindert werden, um das Vertrauen der Verbraucher nicht zu enttäuschen. Es gilt also eine Balance zwischen den verschiedenen Rechtsgütern zu finden und Regulierung nur mit Augenmaß anzulegen.

18 EPC White Paper Mobile Wallet Payments
19 EPC White Paper Mobile Wallet Payments

Anhang A – Weitere Wallet Kategorien

- Vertical- vs. Horizontal Wallet

Eine Vertical Wallet wird in der Regel von einem einzigen Dienstleister entwickelt und ist begrenzt auf die mobilen Services des Anbieters. Die Vertical Wallet sollte daher einfacher zu verwalten sein und ist skalierbarer im Hinblick auf die Kosten-, Wartungs- und Betriebsmodelle. Typischerweise wird diese vom Anbieter mit einer Reihe von vorinstallierten Dienstleistungen versehen. Als Beispiel hierzu wird das Starbucks Square Wallet genannt, die einen geschlossenen Service mit hinterlegter Zahlungsart anbieten[18].

Eine Horizontal Wallet hingegen hat die Möglichkeit verschiedene mobile Dienste von unterschiedlichen Anbietern zu vereinen. Dies soll einer offene Wallet für Kundendienstleistungen ermöglichen. Die Endverbraucher haben dabei die Möglichkeit von verschiedenen Anbietern mobile Dienste zu nutzen[19].

- Integrierte Wallet vs. Umbrella Wallet

Eine integrierte Wallet ist eine Sammlung von unterschiedlichen Funktionalitäten verschiedener Service Provider, die unter der Marke des Wallet Providers angeboten werden. Der Wallet Anbieter bestimmt hierbei die Funktionalitäten, die unter dem Brand oder Marke des Wallet Anbieters bereitgestellt werden. Eigenschaften und Merkmale der Funktionen, Benutzeroberfläche usw. gehören zu einigen der Vorgaben, die der Wallet Provider an die zu integrierenden Services vorgeben kann. Nur Services, die genau den Vorgaben entsprechen, werden in eine integrierte Wallet aufgenommen; sogenannte approved Services. Als Beispiele können hier ISIS Wallet oder Google Wallet aufgeführt werden.

Das Umbrella Wallet ist dadurch gekennzeichnet, dass die Vorgaben von dem Wallet Provider weniger signifikant und restriktiv sind. Der Fokus liegt hier mehr auf dem Management der Priorität und Status der unterschiedlichen Services, die von Wallet Drittanbietern erstellt werden. Auf diese Wallets kann der Nutzer über die Benutzerumgebung des Umbrella Wallets zugreifen, oder diese umgehen und direkt über die Benutzerumgebung des Third Party Anbieters. Das Umbrella Wallet verfolgt daher im Gegensatz zu einem integrierten Wallet einen offenen Systemansatz. Ein Beispiel ist das QuickTap Wallet von Orange.

- E-Wallet

E-Wallets beinhaltet Zahlungskarten und Zugang, um auf eine Webseite angemeldet werden zu können und bezieht sich auf alle Online-Channels. Wikipedia verwendet hierbei Cyberwallet als Synonym für E-Wallet. Der Nutzer eines E-Wallets lädt seine virtuelle Geldbörse mit einer von ihm festgelegten Summe auf, das durch die von ihm bevorzugte Zahlungsweise, abhängig von den vom Anbieter ermöglichten Methoden, geschieht. Am häufigsten kommt die Kreditkartenzahlung vor, aber auch Überweisungen oder das Lastschriftverfahren sind möglich. In seltenen Fällen können auch telefonische Transaktionen vorgenommen werden

- Virtual Wallet

Wallets, die als »Software as a service« Modell angeboten werden und i.d.R. als Cloud-Lösungen Verwendung finden.

Anhang B – Weiterführende Links

- BITKOM, Banking & Financial Services
- European Payments Council (EPC)
- Deutsche Bundesbank, Zahlungsverkehr
- Bundesdruckerei
- Bottomline Technologies
- Deutsche Telekom AG
- GFT
- IBM
- KPMG
- Osborne Clarke
- PwC
- Steria Mummert
- Worldline
- EU PSD
- EZB
- Mobey Forum
- GSMA
- EPC White Paper Mobile Payments
- GSI Studie

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. Mehr als drei Viertel der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils knapp 10 Prozent kommen aus sonstigen Ländern der EU und den USA, 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org