3. Verbraucherdialog „Mobile Payment“

Empfehlungen der Arbeitsgruppe Zahlungssicherheit

Mobile Payment ist eine Form des Bezahlens, die in verschiedenen Formen ausgestaltet ist und in unterschiedlichsten Bereichen zum Einsatz kommt. Soweit der Bezahlvorgang kontaktlos erfolgt und hierfür Smartphones eingesetzt werden, ist die Verbreitung in Deutschland noch gering. Die Zahl der Angebote hingegen nimmt stetig zu. Mobile Payment wird das Potential zugesprochen, die Art des Bezahlens erheblich zu verändern. Hierfür muss das Vertrauen der Verbraucherinnen und Verbraucher gewonnen werden. Dies kann nur gelingen, wenn Angebote verbraucherfreundlich ausgestaltet werden und mit den Zahlungen von Verbraucherinnen und Verbrauchern sicher umgegangen wird.

Eine ausreichende Information versetzt Verbraucherinnen und Verbraucher in die Lage, Risiken des Mobile Payment abzuschätzen und selbstbestimmt über die Anwendung zu entscheiden.

Einsatzbereiche

Folgende Einsatzbereiche sind zu unterscheiden:

- Mobile Payment im stationären Handel (Proximity Payments)
- Mobile Payment im Internet (Remote Payments)

Immer mehr Verbreitung finden auch sogenannte Wallets. Beim Einsatz von Mobile Wallets ist zu beachten, dass Wallets grundsätzlich keine Zahlungsdienste sind, sondern Plattformen, auf denen Zahlungsdienste prozessiert werden.

Mobile Payment für Kleinstzahlungen über die Telefonrechnung (Operator Billing) wurden im Rahmen des Verbraucherdialogs nicht berücksichtigt.

Eingesetzte Technologien

Anders als bei herkömmlichen Zahlungskarten mit Chip oder Magnetstreifen wird beim Mobile Payment die Bezahlung in elektronischer Form und vor allem kontaktlos bewirkt.

Hierbei wird technologisch auf NFC (Near Field Communication), QR (Quick Response)-Code, und andere Technologien gesetzt.

Bei der häufig eingesetzten NFC-Technologie werden drei Formen des Mobile Payment unterschieden:

Passive NFC Card:

Hierbei kommuniziert ein passiver NFC-Chip mit einem NFC-Lesegerät, bspw. einem Händlerterminal. Der Bezahlvorgang wird anschließend über öffentliche Kommunikationswege (bspw. das Internet) oder mit Hilfe der Systeme des Zahlungsdienstleisters abgewickelt. Ein typisches Beispiel für eine solche Kommunikation ist das Verwenden kontaktloser Bezahlkarten für das Begleichen von geringen Geldbeträgen.

NFC Mobile Device („Smartphone“):

Hier kommuniziert das NFC Mobile Device („Smartphone“) über eine entsprechende Applikation („App“) mit dem NFC-Lesegerät, bspw. einem Händlerterminal. Der Bezahlvorgang wird anschließend über öffentliche Kommunikationswege (bspw. das Internet) oder mit Hilfe der Systeme des Zahlungsdienstleisters abgewickelt. Ein typisches Beispiel für eine solche Kommunikation sind Fahrkarten-Anwendungen für den öffentlichen Personenverkehr.

Passive NFC Card und NFC Mobile Device:

Hierbei kommuniziert die Passive NFC Card mit einem NFC Mobile Device („Smartphone“), welches als NFC-Lesegerät eingesetzt wird. Der Bezahlvorgang wird anschließend über öffentliche Kommunikationswege (bspw. das Internet) oder mit Hilfe der Systeme des Zahlungsdienstleisters abgewickelt. Typischerweise findet man solche Konfigurationen im Bereich kostengünstig zu realisierender mobiler Händlerterminals.

Rechtliche Grundlagen des Mobile Payment

Rechtliche Regelungen zur Zahlungssicherheit bzw. Haftung beim Mobile Payment finden sich u.a. im Zahlungsdiensteaufsichtsgesetz (ZAG), Kreditwesengesetz (KWG), Bürgerlichen Gesetzbuch (BGB), Telekommunikationsgesetz (TKG) sowie in diversen EU-Richtlinien (z.B. Payment Services Directive, PSD).
Während für Kreditinstitute und Zahlungsdiensteanbieter gesetzliche Rechtsgrundlagen bestehen, finden sich für Diensteanbieter, die sich verschiedenen Zahlungsmöglichkeiten bedienen, weniger homogene Regelungen.

Mögliche Risiken für Verbraucherinnen und Verbraucher im Zusammenhang mit der Teilnahme an einem Mobile Payment Angebot

a. Keine ausreichende Identifizierung und Authentifizierung

- Bei der Registrierung
- Beim Auslösen von Zahlungsvorgängen

b. Mangelnde Transparenz

- Verständlichkeit des Angebots
- Übersichtlichkeit der Entgelte und Transaktionen
- Verständlichkeit der Funktionen (insb. bzgl. Minderjähriger/Senioren)

c. Identitätsdiebstahl

- mit und ohne „Einwilligung“
- „Freiwillige“ Preisgaben

d. Unbewusste Preisgaben – legal und illegal

- Manipulation des NFC Mobile Device
- Abhören der NFC-Schnittstelle
- Klonen der NFC Card
- Relay-Attacken
- DoS-Attacken
- Software
- Veraltete Firmware am Smartphone
- Unsichere Apps

Bei der Einführung von Mobile Payment sollten daher folgende Empfehlungen berücksichtigt werden:

Empfehlungen

a. Nutzerregistrierung und Authentifizierung

Bei der Registrierung sollten nur die für die Zahlungsabwicklung entsprechend dem jeweiligen Dienst erforderlichen Daten erhoben werden. Werden die Zahlungen über

einen Zahlungsdienstleister abgewickelt, erfolgt die Identifizierung des Verbrauchers entsprechend den Regelungen des Kreditwesengesetzes.

Zur Legitimation der Registrierung wird bei Zahlungen, die über mobile Endgeräte erfolgen, ein zweistufiges Sicherheitsverfahren als sinnvoll erachtet. So sollten sowohl die Mobilfunkrufnummer als auch das Zahlverfahren verifiziert werden. Dies gilt auch für Diensteanbieter.

Sollte eine Nutzung des Dienstes bereits vor Abschluss des Verifikationsverfahrens möglich sein, hat für eine missbräuchliche Nutzung durch Dritte der Diensteanbieter zu haften, sofern der Verbraucher nicht grob fahrlässig gehandelt hat.

Nach Ansicht der AG Zahlungssicherheit ist der neue elektronische Personalausweis (nPA) eine sehr sichere Verifikationsmethode bei der Registrierung, die für die Zukunft favorisiert werden sollte. Diensteanbieter können eine entsprechende Funktion schon heute einbinden, so dass Verbraucherinnen und Verbraucher, die über einen nPA und eine entsprechende Infrastruktur verfügen, diese Art der Verifikation bereits nutzen können. Für Zahlungen im stationären Handel (proximity payments) mittels Smartphone oder Tablet ist der Einsatz des nPA derzeit allerdings nicht möglich.

b. Autorisierung von Zahlungsvorgängen

Die Bezahlfunktion einer App sollte mit einem Zugangscode gesichert sein. Unter Umständen ist es auch sinnvoll, die App als solche mit einem Passwort zu schützen, welches der Kunde selber wählen kann.

Beträge ab einer zu bestimmenden Grenze (z. B. 25 EUR) sollten immer mit einem Code frei gegeben werden müssen. Diesen Code können Verbraucherinnen und Verbraucher selbst festlegen. Zusätzlich sollten Verbraucherinnen und Verbraucher festlegen können, ob sie jede Transaktion über einen Code authentifizieren möchten.

Um einen Missbrauch des Benutzerkontos weitgehend auszuschließen, sollten die geforderten Passwörter dynamisch sein und den Sicherheitsvorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genügen.

- Bei der Registrierung sollte ein Hinweis dahingehend erfolgen, wie sicher das gewählte Passwort ist.
  Umsetzungsbeispiel: nur kleine Buchstaben – Alarmfarbe Rot, Klein- und Großbuchstaben – gelb; Klein- und Großbuchstaben und Sonderzeichen – grün.

- Beim Einkauf im Internet (Remote Mobile Payments) müssen Verbraucherinnen und Verbraucher vom Diensteanbieter darauf aufmerksam gemacht werden, dass sie im eigenen Interesse Kennwort/ Passwort-Kombinationen wählen sollten, die möglichst für jeden Dienst unterschiedlich sind.

c. Transparenz und Kostenkontrolle

Die AG Zahlungssicherheit empfiehlt, dass Verbraucherinnen und Verbraucher die Möglichkeit haben, beim Diensteanbieter zur Kostenkontrolle ein Ausgabenlimit festzusetzen. Eine mögliche Begrenzung sollte zwischen den Partnern (Verbraucher/Diensteanbieter) geregelt werden. Eine Obergrenze ist aus Gründen der Zahlungsausfallsicherung auch für den Diensteanbieter sinnvoll. Die Höhe des Ausgabenlimits sollte den realistischen Nutzungsmöglichkeiten genügen.

Verbraucherinnen und Verbraucher müssen vor und nach ihrer Entscheidung für ein Bezahlsystem die Möglichkeit haben, sich über Entgelte umfassend und in einfacher

Form zu informieren. Entgelte dürfen nur für Leistungen berechnet werden, die ein Dienst nicht bereits im Rahmen der normalen Nutzung erbringen muss.

Verbraucherinnen und Verbraucher sollten u.a. Informationen zum Abbuchungsdatum der Rechnungen sowie zum Ablauf eines möglichen Mahnverfahrens erhalten.

Die getätigten Transaktionen müssen für Verbraucherinnen und Verbraucher nachvollziehbar sein. Verbraucherinnen und Verbraucher müssen in Textform einen Transaktionsbeleg einschließlich der genauen Rechnungsbestandteile (Waren, Dienstleistungen) erhalten. Die getätigten Transaktionen sollten auf der Internetseite des Diensteanbieters einsehbar sein.

Es sollte gewährleistet sein, dass auch Verbraucherinnen und Verbraucher ohne ausreichende Bonität sowie Minderjährige sicher an Mobile-Payment-Angeboten teilnehmen können.

d. Service

Die zentrale Sperrnummer (116 116) bei Verlust oder Diebstahl des Handys sollte auch für alle Mobile Payment Dienste gelten, damit auch die Nutzung aller auf dem Handy verfügbaren Mobile Payment Dienste zentral und einfach gesperrt werden kann.

Kundendienstanfragen sollten unverzüglich und für Verbraucherinnen und Verbraucher kostenfrei beantwortet werden. Telefonische Hotlines müssen den Vorgaben des Gesetzes zur Umsetzung der Verbraucherrechterichtlinie entsprechen.

e. Technische Sicherheit und Standards

Zur technischen Absicherung kontaktloser Bezahlverfahren wird empfohlen,

- eine gegenseitige Authentisierung der Kommunikationspartner zu verwenden,
- Nutzinformationen, die kontaktlos ausgetauscht oder gespeichert werden zu verschlüsseln und
- Vertrauensanker (Secure Elements) zu nutzen, um potenziell unsichere Smartphones für sicheres kontaktloses Bezahlen nutzbar zu machen.

Zahlungen am POS sollten grundsätzlich ohne Konnektivität möglich sein, da eine Internetkonnektivität nicht jederzeit und überall gewährleistet ist.

Sofern Wallets zum Einsatz kommen, ist eine Interoperabilität der Wallets wünschenswert, damit Verbraucherinnen und Verbraucher bei Wechsel des Wallet-Anbieters bislang genutzte Dienste auch weiterhin in Anspruch nehmen können.

Stand: 04.11.2013