FAQ

Sicher zahlen per NFC

Mit dem Android-Smartphone kontaktlos über den NFC-Chip an der Ladenkasse zu zahlen gilt als sehr sicheres Verfahren. Warum das so ist, beantworten wir in dieser FAQ.

Von Markus Montz

Zahlungsfreigabe

Wann muss ich zum Bezahlen meine PIN am Kassenterminal eingeben, wann muss ich das Handy entsperren?

Dafür, dass beim Halten Ihres Smartphones an ein Kassenterminal über den NFC-Chip ein Bezahlvorgang ausgelöst wird, gibt es je nach App-Anbieter unterschiedliche Voraussetzungen. Wenn Sie mit den Apps der Sparkassen und Volksbanken zahlen, müssen Sie bei Beträgen bis 25 Euro auf der einfachsten Sicherheitsstufe lediglich das Display aktivieren – das Gerät muss nicht entsperrt sein. Sporadisch fragt Sie das Kassenterminal zusätzlich nach der PIN der Plastikkarte, obligatorisch ist deren Eingabe aber erst ab einer Summe von 25 Euro. Dies gilt für Girokarten ebenso wie für Kreditkarten.

Deutsche Bank und Postbank haben nahezu die gleichen Regeln wie Sparkassen und Volksbanken. Bei ihnen muss das Handy aber stets entsperrt sein, auch für Zahlungen unter 25 Euro. Die App der Fidor Bank wiederum fragt bei jeder Zahlung die Pay-PIN ab, die Sie bei der Einrichtung festlegen. Sporadisch müssen Sie sich beim Bezahlen außerdem neu in die Banking-App einloggen.

Google Pay löst Zahlungen unter 25 Euro wie die App der Sparkassen und Volksbanken bereits bei aktiviertem Display aus. Bei Zahlungen höherer Beträge verlangt dieser Dienst abweichend lediglich, das Smartphone zu entsperren und wertet dies wie eine PIN-Eingabe am Terminal. Dahinter steckt die sogenannte CDCVM (Consumer Device Cardholder Verification Method), die vom Prinzip her einer Zwei-Faktor-Authentifikation entspricht.

Wählen Sie die Entsperrmethode nicht nur beim Einsatz von Google Pay sorgfältig! Wir raten insbesondere davon ab, ein Wischmuster zu nutzen, da Dritte dieses relativ leicht erraten können.

Heimliche Abbuchungen

Können Kriminelle mit drahtlosen Bezahlterminals heimlich eine Zahlung vom Handy in der Hosen- oder Handtasche auslösen?

Unter Laborbedingungen: Ja – im Alltag müsste der Kriminelle hohe technische Hürden überwinden. Die Kommunikation zwischen dem NFC-Chip des Smartphones und dem Terminal ist nur möglich, wenn der Abstand etwa vier Zentimeter oder weniger beträgt. Außerdem müssen Sie als Besitzer des Handys – je nach verwendeter Bezahl-App – mindestens das Display aktiviert oder Ihr Gerät bereits entsperrt haben. Das schließt heimliches Auslösen in der Hosen- oder Handtasche nahezu aus.

Bei den Sicherheitsstufen der Sparkassen-App „Mobiles Bezahlen“ können Sie Sicherheit und Komfort gegeneinander abwägen.

Sollte es dem Kriminellen dennoch gelingen, etwa von einem unbeaufsichtigten Handy einen Zahlungsvorgang auszulösen, hinterlässt er eine digitale Spur: Jedes Terminal besitzt eine eigene ID und ist zudem an ein Zielkonto gebunden. Girocard-Zahlungen per Smartphone lassen sich sogar nur auf deutsche Geschäftskonten transferieren. Da eine Bank bei der Eröffnung solcher Konten die Identität des Kontoinhabers prüfen muss, steht sie im Zweifel für Schäden gerade.

Sobald die ID eines Zahlungsterminals bei Kartenfirmen oder kartenausgebenden Banken durch unplausible Buchungen auffällt, kommt der Händler zudem unter verschärfte Beobachtung. Bei Betrugsverdacht wird er gesperrt.

Kartendaten auslesen

Kann jemand über ein (manipuliertes) Bezahlterminal oder NFC-fähiges Lesegerät meine Kartendaten abgreifen und diese dann in Onlineshops nutzen?

Wenn Sie eine Kreditkarte in der Bezahl-App hinterlegen, wird die Original-Kartennummer nicht auf dem Smartphone gespeichert. Daher kann auch niemand aus dem NFC-Signal die echten Daten Ihrer Visa- oder Mastercard auslesen. Das gilt ebenso für Debitkarten in elektronischer Form, etwa die von PayPal. Ihr Smartphone übermittelt dem Bezahlterminal nur ein Token und einen „Single Use Key“ (Mastercard) respektive „Limited Use Key“ (Visa).

Das Token ist eine Pseudo-Kreditkartennummer, die nicht dem Original (Personal Account Number, PAN) entspricht. Das Zahlungsnetzwerk – beispielsweise VisaNet für Visa-Karten – erzeugt

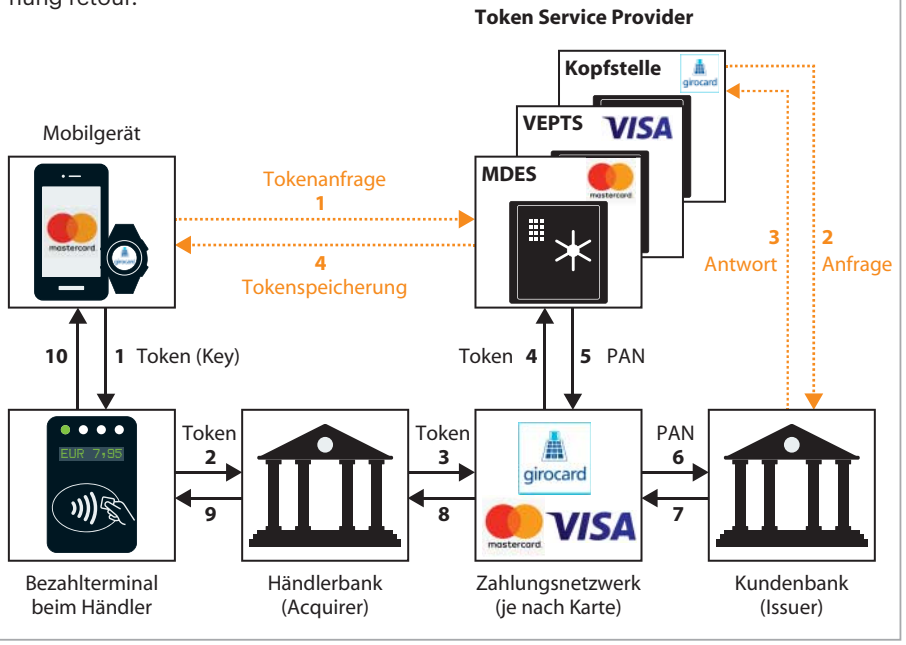
das Token, sobald Sie die Karte auf Ihrem Gerät hinterlegen. Bei den Use Keys handelt es sich um kryptografische Einmal-Schlüssel, die in einem speziell gesicherten Bereich des Betriebssystems gespeichert sind. Der NFC-Chip sendet sie gemeinsam mit dem Token. Um beide zusätzlich zu schützen, verweigern Bezahl-Apps auf gerooteten Handys den Dienst.

Während der Zahlungsabwicklung prüfen das Zahlungsnetzwerk und Ihre Bank Token und Use Key und ordnen sie Ihrer „echten“ Karte und Person zu. Der Händler erhält bei positivem Ergebnis aber nur die Freigabe sowie eine Transaktions-ID. Das Token kann man mit einem geeigneten Gerät zwar auch über den NFC-Chip auslesen, für Online-Shopping auf Ihre Kosten taugt diese Nummer in der Praxis aber nicht. Oft ist sie nicht einmal dafür freigegeben, und wenn doch, fehlen Ihr Name und die dreistellige CVC- respektive CVV-Nummer. Händler, die diese nicht abfragen, bleiben bei einer Reklamation auf den Kosten für die Bestellung sitzen.

Wenn Sie mit einer in der App hinterlegten Girocard zahlen, übermittelt der Chip Bankleitzahl und Kontonummer (PAN), verschlüsselt mit einem Use Key. Dieser Code wird an sogenannten Kopfstellen der Kartendienstleister verifiziert und von der kartenausgebenden Bank Ihrer Person zugeordnet. Selbst wenn ein Krimineller die IBAN ermitteln könnte, ließe sich nur Geld auf ein Konto einziehen, das für Lastschriften zugelassen ist – und Sie können solch eine Lastschrift außerdem zurückbuchen.

Das passiert beim kontaktlosen Zahlen per Token (Host-Card-Emulation, HCE)

Beim kontaktlosen Bezahlen mit dem Android-Smartphone überträgt das Gerät an die Bank des Händlers bei einer Kreditkarte eine Pseudo-Kartennummer (Token) und einen Einmalschlüssel, bei der Girocard die echte Kartennummer in einem Schlüssel plus die sogenannte Kartenfolgenummer. Erst das Zahlungsnetzwerk kann daraus beim eigenen Token Service Provider die PAN ermitteln. Nachdem die Kundenbank das zugehörige Konto auf Deckung und Sperrung geprüft hat, gehen die Bestätigung plus eine Transaktions-ID oder eine Ablehnung retour.



Smartphone verloren oder gestohlen

Wie verhindere ich einen Missbrauch, wenn mir das Gerät abhanden gekommen ist? Und was könnte ein Krimineller grundsätzlich erreichen?

Zunächst tun Sie, was Sie auch bei Verlust Ihrer Plastikkarten tun würden: Lassen Sie die im Smartphone hinterlegten digitalen Karten sperren. Bei deutschen Banken geht das fast immer über die kostenlose Nummer (+49) 116 116 des Sperr-Notrufs e. V. Aus Haftungsgründen müssen Sie die Sperrung unverzüglich in die Wege leiten.

Solange Sie die Karten noch nicht geblockt haben, hängen die Möglichkeiten des Diebes davon ab, ob er die Schutzmechanismen der jeweiligen Bezahl-App überwindet (siehe Antwort auf die erste Frage). Bei einem Blick in die Bezahl-App selbst sieht der Dieb von der Originalnummer Ihrer Kreditkarte höchstens die letzten vier Ziffern ohne die CVC- oder CVV-Nummer. In den Apps von Volksbanken und Sparkassen könnte er zusätzlich zwar die IBAN und Ihren Namen auf Ihrer Girocard im Klartext einsehen, das befähigt ihn aber wiederum nur zu einer Lastschrift.

Haftung

Wer haftet bei Missbrauch?

Falls Sie beim Missbrauch durch Dritte fahrlässig gehandelt haben, haften Sie derzeit bis maximal 50 Euro selbst, bei grob fahrlässiger oder vorsätzlicher Handlung unbegrenzt. Grob fahrlässig wäre es etwa, die Karte erst Tage nach dem Verlust des Handys sperren lassen. Sie müssen außerdem in einem vertretbaren Umfang dafür Sorge getragen haben, dass Ihr Smartphone nicht durch Malware kompromittiert werden kann.

Details erfahren Sie in den Bestimmungen Ihres Kreditinstitutes: So übernehmen etwa die Sparkassen auch dann die Haftung, wenn Dritte Ihr Smartphone für Zahlungen unter 25 Euro ohne PIN missbrauchen.

Unbeabsichtigte Zahlungen

Sind Doppelbuchungen oder versehentliche Zahlungsauslösungen möglich?

Damit unbeabsichtigt Geld fließen kann, müssten Sie mit einem zahlungsbereiten Smartphone nahe genug an einem Terminal sein, das ebenfalls gerade für eine Zahlung aktiviert ist. Ähnlich verhält es sich bei Doppelbuchungen: Sobald das Terminal eine Transaktion erfolgreich abgeschlossen – oder abgelehnt – hat, muss der Kassierer es für die nächste erst neu aktivieren. *(mon@ct.de)*