Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sicher zahlen im E-Commerce

Fragen und Antworten zu Online-Bezahlverfahren

Inhaltsverzeichnis

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Als Cyber-Sicherheitsbehörde des Bundes ist es Aufgabe des BSI, Deutschland digital sicher zu machen. Seit seiner Gründung 1991 hat sich das BSI zu einem Kompetenzzentrum für Fragen der Informationssicherheit entwickelt, dessen fachliche Expertise national und international anerkannt ist.

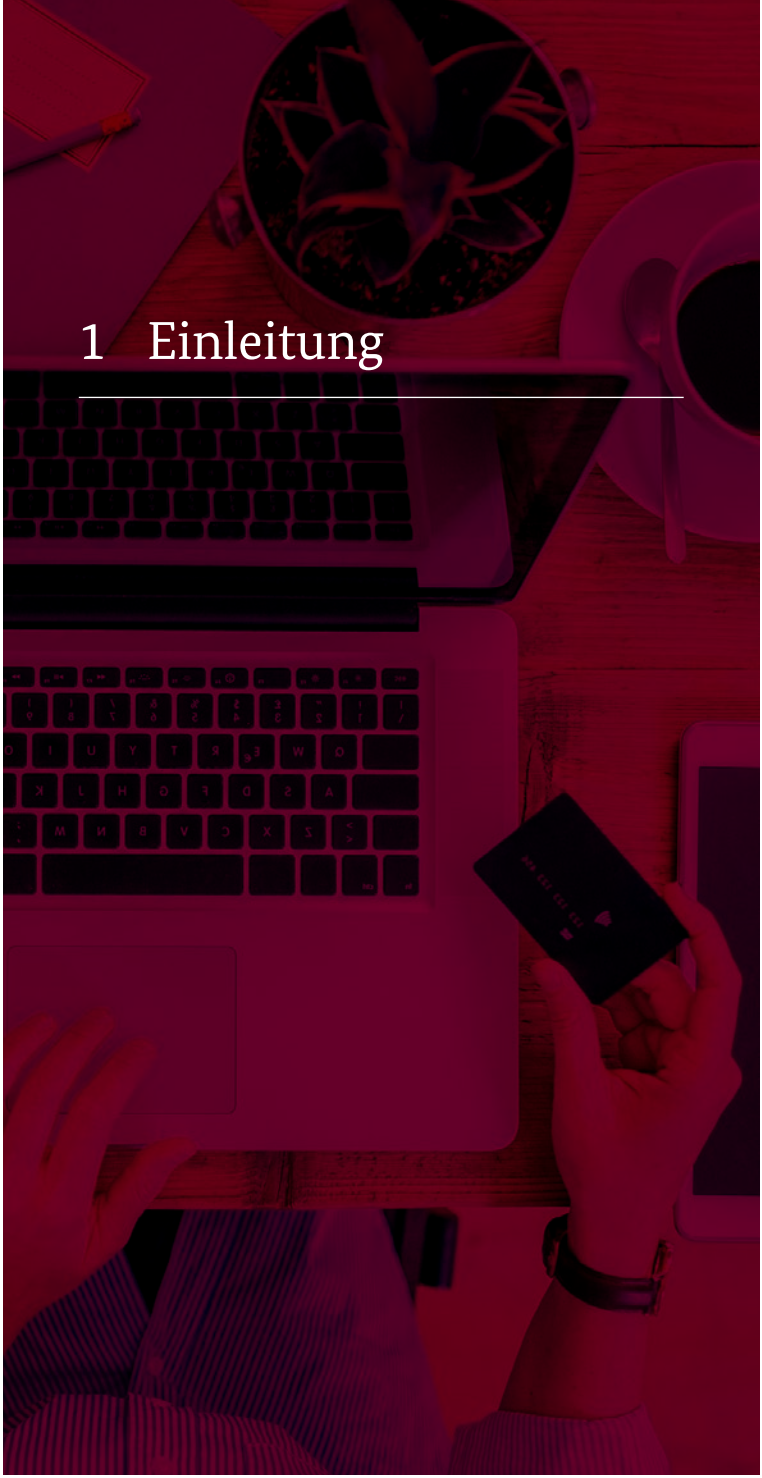
Für die Zukunft des Standorts Deutschland ist die Digitalisierung ein wesentlicher Erfolgsfaktor. Voraussetzung einer erfolgreichen Digitalisierung ist die Informationssicherheit. Deshalb beschäftigt sich das BSI damit, in welchen Anwendungsfeldern der Digitalisierung Risiken entstehen könnten und wie man diese Risiken kalkulierbar und beherrschbar machen kann.

Durch seine ausgeprägte Vernetzung nach innen und außen ist das BSI in der Lage, Know-how in den Bereichen Prävention, Detektion und Reaktion zu bündeln, Themen der Informationssicherheit fachlich zu analysieren und aus der Analyse heraus konkrete Angebote für unterschiedliche Zielgruppen in Staat, Wirtschaft und Gesellschaft abzuleiten. Das BSI nutzt dazu seine integrierte Wertschöpfungskette der Cyber-Sicherheit, die von der Abwehr und Analyse von Cyber-Angriffen über

Beratungsdienstleistungen und Zertifizierung bis hin zur Entwicklung sicherheitstechnischer Empfehlungen, Best Practices und Standards reicht.

Cyber-Sicherheit für Privatanwender

Die Digitalisierung kann nur gelingen, wenn Anwenderinnen und Anwender Vertrauen in neue Technologien entwickeln und diese zu ihrem Nutzen sicher einsetzen können. Das BSI sensibilisiert Privatanwenderinnen und -anwender für Risiken, damit sie selbstbestimmt Gefahren abwehren und souverän agieren können. Sie profitieren dabei von praxisgerechten und für Laien verständlichen Informationen und Handlungsempfehlungen für mehr Sicherheit im Internet, die das BSI auf seiner Webseite www.bsi-fuer-buerger.de oder per Hotline unter 0800-2741000 bereitstellt. In Umsetzung der Cyber-Sicherheitsstrategie der Bundesregierung entwickelt das BSI zudem ein IT-Sicherheitskennzeichen, um künftig den Verbrauchern eine Einschätzung zur Cyber-Sicherheit von IT-Produkten und -Services zu erleichtern.



1 Einleitung

Einleitung

Für Zahlungen im Internet werden zahlreiche unterschiedliche Zahlungsdienste angeboten.

Dazu zählen:

- Die Anbieter von Zahlungskonten für Händler und Kunden wie Paypal
- Kreditkartenlösungen wie 3D-Secure
- lastschriftbasierte Lösungen
- Ausführungen, die Kunden zu einer Bankwebseite weiterleiten, sowie
- Dienste, die den Zahlungsauftrag zum kontoführenden Zahlungsdienstleister weiterleiten wie bei Sofortüberweisung der Sofort GmbH (jetzt Klarna).

Zusätzlich bieten immer mehr Banken Online-Banking-Anwendungen (Banking-Apps) an. Neben den eigenen Banking-Apps werden auch freie multibankfähige Apps angeboten, die das Verwalten mehrerer Konten verschiedener Banken ermöglichen.

Die Zahlungen werden nicht mehr ausschließlich über das Internet an einem PC oder in klassischer Weise an einem stationären Point of Sale (POS) durchgeführt, sondern vermehrt mit mobilen Geräten wie Smartphones oder Tablets.

Die jeweiligen Bezahlverfahren bergen unterschiedliche Risiken für den Nutzer, also den Kunden, den Händler und auch das Kreditinstitut des Kunden. Insbesondere wenn es um Sicherheitsaspekte geht, sind Vor- und Nachteile der einzelnen Verfahren für Kunden nicht immer leicht nachvollziehbar.

Mit der vorliegenden Übersicht zu den jeweiligen Bezahlverfahren im E-Commerce und damit zusammenhängenden Themen und den entsprechenden Zwischenfazits können Nutzer für sich abwägen, welches der Verfahren zu ihnen passt und den individuellen Sicherheitsansprüchen entspricht.

2 Die PSD2 als Grundlage im E-Payment

Die PSD2 als Grundlage im E-Payment

Was ist die PSD2? Welchen Einfluss hat die PSD2 auf Authentifizierungslösungen?

Hinter der Abkürzung PSD2 (Payment Services Directive 2) verbirgt sich die EU-Richtlinie über Zahlungsdienste (DIRECTIVE (EU) 2015/2366). Ziel der Richtlinie ist es, die Sicherheit im Zahlungsverkehr zu erhöhen, den Verbraucherschutz zu stärken, Innovationen zu fördern und den Wettbewerb auf dem Markt zu steigern. So wurden aufgrund der Tatsache, dass inzwischen sowohl Zahlungsdienstleistungen als auch Bankgeschäfte in großen Teilen im Internet stattfinden und dieses durchaus Risiken im IT-Bereich birgt, mit der Richtlinie wesentliche Schnittstellen zwischen Kunde und Bank sowie zwischen den Banken und weiteren Finanzdienstleistern neu geordnet. Die PSD2 und nachgelagerte regulatorische Normen stellen höhere Anforderungen an die IT-Sicherheit der beteiligten Prozesse. Hierfür sind die „starke Kundenauthentifizierung“ und die Kontoschnittstelle für Zahlungsdrittdienstleister von besonderer Relevanz.

Worum geht`s?

Um die Anforderungen der PSD2 zu konkretisieren, wurden von der Europäischen Bankenaufsichtsbehörde (EBA) in Kooperation mit der Europäischen Zentralbank (EZB) Regulierungsstandards (Regulatory Technical Standards, RTS), unter anderem zur „starken Kundenauthentifizierung“, formuliert.

Authentifizierungslösungen, die auf zwei unabhängigen Authentifizierungselementen der Kategorien „Wissen", „Besitz" oder „Inhärenz" (Biometrie) beruhen, gelten als „starke Kundenauthentifizierung" (Strong Customer Authentication, SCA). Dazu gehören zum Beispiel die Authentifizierung mit physischer Karte in Form einer Chipkarte (Besitzfaktor) und PIN (Wissensfaktor). Auch chipTAN, SMS-TAN und pushTAN (jeweils Besitzfaktor) in Kombination mit einem wissensbasierten Authentifizierungsfaktor wie der Online-Banking-PIN oder digitale Karten (Besitzfaktor) mit Fingerabdruck (biometrischer Faktor) erfüllen die Anforderungen. Authentifizierungslösungen für den E-Commerce, die ausschließlich auf Daten beruhen, die auf der Karte aufgedruckt sind, erfüllen die technischen Anforderungen der PSD2 nicht, auch wenn zusätzlich ein Passwort verlangt wird.

Wann wird die „starke Kundenauthentifizierung" eingesetzt?

Grundsätzlich beziehen sich die Anforderungen der PSD2 nur auf Authentifizierungslösungen für elektronische Zahlungen, die vom Kunden initiiert sind, im Unterschied zu solchen, die vom Händler initiiert sind. Betroffen sind Transaktionen, die mit digitalen Karten oder physischen Karten durchgeführt werden. Dazu gehören auch Transaktionen am Zahlungsterminal (POS) und Geldautomatenverfügungen sowie Zahlungen im E-Commerce, die keine Lastschriften sind. In jedem Fall ist aber auch für den Online-Zugriff auf das Zahlungskonto mindestens alle 90 Tage eine „starke Kundenauthentifizierung" erforderlich.

Für Lastschriften bestehen keine Anforderungen, da diese nicht vom Zahler initiiert sind und der Zahler jederzeit die Möglichkeit hat, die Lastschrift zurückzugeben. Allgemein gelten die Anforderungen aus dem RTS nicht für unterschriftenbasierte Kartenzahlungen.

Daneben gibt es für die Kreditinstitute auch die Möglichkeit, bei Zahlungen, die vom Zahler ausgelöst werden, keine „starke Kundenauthentifizierung“ zu verlangen. Diese Ausnahmen sind in Kapitel 3 des RTS zu finden. So kann ein Institut beispielsweise in den folgenden Fällen auf die „starke Kundenauthentifizierung“ verzichten:

- bei Zahlungen an Empfänger, die im Vorfeld als vertrauenswürdig eingestuft wurden (White List),
- bei Daueraufträgen, da diese nur beim Anlegen mittels SCA autorisiert werden müssen,
- bei Kleinbetragszahlungen unter 30 €, sofern sie bestimmte Voraussetzungen erfüllen,
- beim Login zum Online-Banking, sofern innerhalb der letzten 90 Tage eine SCA beim Einloggen durchgeführt wurde.

Grundsätzlich kann jedoch jedes Institut selbst entscheiden, ob es Ausnahmen von der SCA zulässt oder bei jeder Transaktion, unabhängig vom Risiko, eine SCA durchführen möchte.

3 Technische Grundlagen: Tokenisierung

Technische Grundlagen: Tokenisierung

Wozu dient Tokenisierung?

Zahlungen mit Debit- oder Kreditkarten müssen im E-Commerce durch Angabe der Kartennummer (PAN) in Kombination mit dem Namen des Karteninhabers und dem Kartengültigkeitsdatum freigegeben werden. Zum Teil muss bei Zahlungen mit Kreditkarten zusätzlich noch die auf der Karte aufgedruckte Kreditkartenprüfnummer (Card Validation Code, CVC) eingegeben werden. Die PAN steht auf der Karte und ist damit für jeden lesbar, der die Karte in den Händen hält. Dennoch ist die PAN aus Sicht der Banken ein Wert, dessen Vertraulichkeit zu schützen ist, denn kennt ein Betrüger die PAN (und den CVC), kann er unter falschem Namen eine E-Commerce-Transaktion durchführen. Um die Vertraulichkeit der PAN zu gewährleisten, haben die internationalen Kartenunternehmen mit dem „Payment Card Industry Data Security Standard" (PCI DSS) hohe Sicherheitsanforderungen formuliert, die von den IT-Systemen, in denen PANs von Karten gespeichert und verarbeitet werden, einzuhalten sind. Die Tokenisierung ist ein Verfahren, das zusätzlich zu diesen Sicherheitsanforderungen die Möglichkeiten zur missbräuchlichen Nutzung der PAN und der zugehörigen Daten beschränkt.

Was ist Tokenisierung?

Bei der Tokenisierung wird der PAN, also der 16-stelligen Nummer, die auf die Kreditkarte geprägt ist, eine andere zufällige

Nummer, das Token, zugeordnet, um beim Bezahlvorgang genutzt zu werden. Dabei hat das Token das gleiche „Format“ wie eine PAN, ist also ebenfalls eine Nummer mit 16 Stellen. Das Token wird generiert, ohne dass der Kunde etwas davon bemerkt: Dies geschieht zum Beispiel, wenn eine neue Karte zu einer Bezahl-App hinzugefügt wird oder eine Karte für den wiederholten, regelmäßigen Gebrauch bei einem Händler (z.B. für die Zahlung eines Abonnements) hinterlegt wird. Die Zuordnung eines Token zu einer PAN wird in der Regel vom Netzwerk der entsprechenden Kreditkartenanbieter vorgenommen. Daher wissen nur die Kartenanbieter, welches Token zu welcher PAN gehört. Wird die gleiche Karte bei mehreren Händlern bzw. in mehreren Bezahl-Apps verwendet, wird jedes Mal ein neues Token erzeugt.

Um bei einem Bezahlvorgang das korrekte Konto belasten zu können, wird die Bank, die die Karte an den Kunden ausgestellt hat, vom jeweiligen Kreditkartenanbieter entsprechend informiert. Dieser erhält vom Händler oder seiner Bank das in die Transaktion involvierte Token, ordnet dem Token die korrekte PAN zu und gibt diese zur Verarbeitung an die Bank des Kunden weiter.

Warum erhöht Tokenisierung die Sicherheit?

Durch die Tokenisierung verschwindet die PAN, also ein schützenswerter Parameter, aus den IT-Systemen des Händlers oder des Betreibers der Bezahl-App. Statt der PAN nutzen Händler also „nur“ das Token zur Abwicklung von Einkäufen – sie kennen die zugehörige PAN nicht. Für ein Token gilt, dass es eindeutig einem Händler bzw. einer Zahlungs-App zugeordnet ist. Gerät also ein Token in die Hände eines Betrügers, kann dieser das Token nur bei dem entsprechenden Händler oder über die entsprechende Bezahl-App verwenden. Dies schränkt die Möglichkeiten des Missbrauchs eines Tokens im Vergleich zur PAN ein. Da ein bestimmtes Token immer nur einer bestimmten Bezahl-App bzw. einem bestimmten Händler zugeordnet wird, ist der Angriff

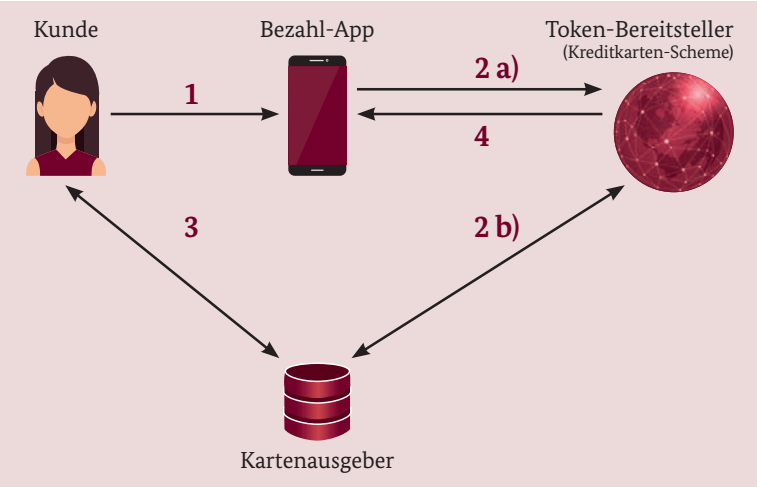
auf eine App oder einen Händler ohne Auswirkungen auf die Token, die in anderen Apps oder bei anderen Händlern hinterlegt wurden.

Wo wird Tokenisierung eingesetzt?

Die Tokenisierung wird bei Betreibern von Bezahl-Apps eingesetzt. Diese speichern die PANs der registrierten Kreditkarten jeweils in Form eines Tokens.

Ein weiterer Einsatzbereich von Token sind sogenannte „Card-On-File-Transaktionen". Dabei wird das Token zum Beispiel für regelmäßige automatische Abbuchungen bei Abonnements bei einem Händler hinterlegt.

Da ein bestimmtes Token immer nur einer bestimmten Bezahl-App bzw. einem bestimmten Händler zugeordnet wird, ist der Angriff auf eine App oder einen Händler ohne Auswirkungen auf die Token, die in anderen Apps oder bei anderen Händlern hinterlegt wurden.



Ablauf der Tokenisierung

1. Der Nutzer fügt die Karte zur Bezahl-App hinzu. Der genaue Vorgang (Abfotografieren, manuelles Eingeben der Kartendaten etc.) hängt dabei von der Bezahl-App ab.

2. **a.** Der Betreiber der App fragt bei dem Token-Bereitsteller - meistens das entsprechende Kreditkarten Scheme - das Token an.
   b. Die kartenausgebende Bank muss bestätigen, dass die Vergabe eines Tokens für die angefragte Karte und Bezahl-App zugelassen ist. Der Betreiber der Bezahl-App weist sich dazu mit einer in einem vorgelagerten Schritt erhaltenen ID gegenüber dem Kartenausgeber aus.

3. Zusätzlich überprüft der Kartenausgeber die Identität des Kunden. Dafür nutzt er die bereits bestehende Beziehung zu seinem Kunden (z.B. über das Online-Banking oder die Kontaktdaten des Kunden).

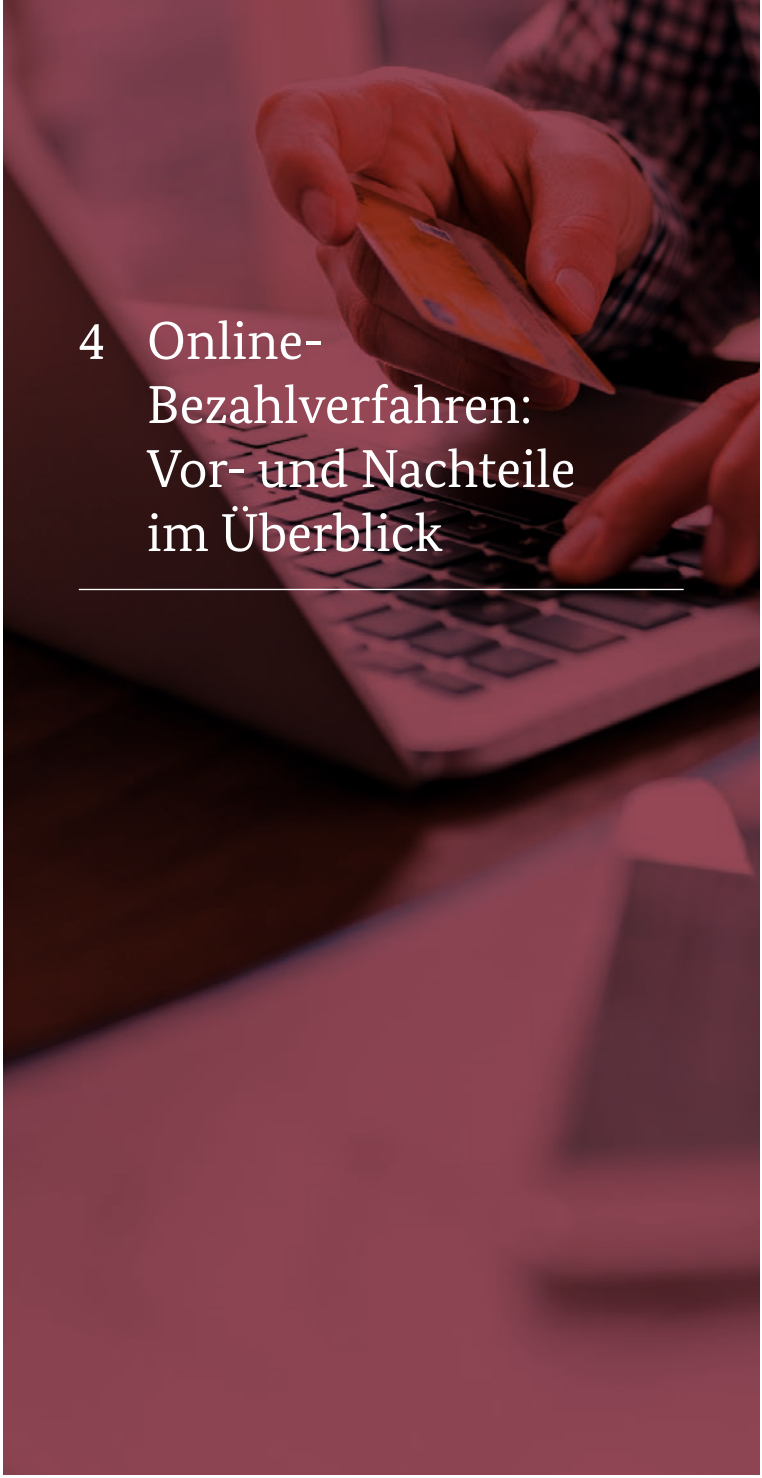
4. Der Bereitsteller des Tokens wandelt die PAN der Karte in ein Token um und liefert dieses an die Bezahl-App. Dort wird das Token sicher gespeichert; entweder in einem Hardware-Element oder in einer vergleichbar sicheren Software-Umgebung.

Fazit:

Die Tokenisierung ist eine Technologie, die die Sicherheit des jeweiligen Bezahlverfahrens erhöht. Dabei gilt, dass Angriffe durch die Tokenisierung zwar nicht verhindert werden, diese jedoch dazu führt, dass unrechtmäßig abgegriffene Zahlungs- und Kartendaten nur eingeschränkt nutzbar sind. In der Folge wird daher durch die Tokenisierung das potenzielle Ausmaß von möglichen Schäden verringert. Zusätzlich wird durch die Tokenisierung verhindert, dass Händler oder Betreiber von Bezahl-Apps Zugriff auf sensible Zahlungs- und Kartendaten erhalten, da sie lediglich das Token der im Einkaufsprozess verwendeten Karte erhalten. Zum Beispiel wird dadurch ein Angriff auf die sensiblen Kartendaten innerhalb der Systeme des Händlers verhindert.

Ob eine Tokenisierung stattfindet oder nicht, hängt von den Betreibern der Bezahl-Apps, den Händlern sowie den Kartenausgebern ab. Der Kunde kann dies nicht aktiv beeinflussen.

Die Tokenisierung wird nicht nur im Bereich Zahlungsverkehr eingesetzt, sondern dient auch in anderen Bereichen dem Schutz von sensiblen und schützenswerten Informationen, so zum Beispiel im Bereich digitaler Identitäten.



4 Online-Bezahlverfahren: Vor- und Nachteile im Überblick

4.1 Online bezahlen mit Kreditkarte

Was ist eine Card-Not-Present-Transaktion (mit der Kreditkarte)?

Wird im E-Commerce mit einer Kreditkarte bezahlt, liegt dem Händler die Karte nicht physisch vor. Der Händler kann daher nicht die Sicherheitseigenschaften des Chips einer physischen Kreditkarte nutzen. Bei der Card-Not-Present-Transaktion im E-Commerce muss der Kunde Kartendaten in die Maske des Shops eingeben, nämlich die Kartennummer, den Namen des Karteninhabers, das Gültigkeitsdatum und die Kartenprüfnummer (CVC). Der Kunde benötigt für einen Einkauf im E-Commerce via Card-Not-Present-Transaktion also nur die Kartendaten, die auf der Kreditkarte ablesbar sind, aber nicht notwendigerweise die physische Karte.

Wie wird dieses Bezahlverfahren aktiviert?

Eine explizite Aktivierung des Verfahrens, also eine „Freischaltung der Kreditkarte für Zahlungen im E-Commerce“, ist nicht notwendig. Die Kreditkarte selbst kann bei der kartenausgebenden Bank beantragt werden.

Separate Authentifizierungsverfahren, die mit der Kreditkarte genutzt werden können, wie zum Beispiel 3D-Secure, erfordern eine Aktivierung bei der Bank des Kunden.

Wie kann eine mit Kreditkarte gezahlte Transaktion im E-Commerce widerrufen werden?

Abbuchungen über betrügerische Kreditkartentransaktionen können innerhalb von acht Wochen zurückgefordert werden. Die Beantragung der Rückbuchung erfolgt beim Kartenausgeber, der Bank. Der genaue Vorgang ist dabei institutsabhängig.

Was muss bei Card-Not-Present-Transaktionen mit der Kreditkarte beachtet werden?

Bei diesem Bezahlverfahren ist darauf zu achten, dass die Eingabe der Daten auf einer gesicherten Webseite des Händlers stattfindet (https), so dass die Übertragung abgesichert ist. Besteht der Verdacht auf einen Betrugsfall mit der Karte oder wurde die Karte gestohlen bzw. verloren, sollte diese umgehend über die Sperrhotline gesperrt werden. Eine Reaktivierung ist nur in seltenen Fällen möglich; üblicherweise wird nach einer Sperrung eine neue Karte ausgestellt.

Vorteile des Bezahlens mit Kreditkarte

- Keine Registrierung für den Gebrauch der Kreditkarte im E-Commerce notwendig.
- Rückbuchungen von betrügerischen Transaktionen leicht möglich.
- Einfache Handhabung
- Kein gesondertes Kundenkonto o. Ä. erforderlich.
- Für den Kunden fallen keine Kosten für Transaktionen im E-Commerce an.

Nachteile des Bezahlens mit Kreditkarte

- Eingabe der sensiblen Kartendaten bei jedem Einkauf.
- Händler hat Zugriff auf sensible Kartendaten.
- Phishing-Attacken sind möglich.

4.2 Online bezahlen mit Kreditkarte und 3D-Secure

Was ist 3D-Secure?

3D-Secure ist ein von den internationalen Kartenunternehmen (heute unter der Hoheit von EMVCo, einem Zusammenschluss der globalen Kartenzahlungssysteme) entwickeltes Authentifizierungsverfahren, das es dem Kunden im E-Commerce ermöglicht, sich als rechtmäßiger Inhaber einer Karte zu authentisieren und eine mit der Karte verbundene Zahlung freizugeben. Wird 3D-Secure in einer Card-Not-Present-Transaktion mit der Kreditkarte verwendet, genügt es nicht, wie im Falle der „einfachen" Kreditkartentransaktion, die Kartennummer (PAN) zusammen mit dem Namen des Karteninhabers und dem Kartengültigkeitsdatum anzugeben. Eine zusätzliche Authentifizierung ist erforderlich. Welche zusätzlichen Sicherheitsabfragen zur Authentifizierung durchgeführt werden, hängt vom Institut ab. 3D-Secure ist der technische Name des Verfahrens und deutet auf die Zusammenarbeit von drei verschiedenen Kartenunternehmen hin, die in den Prozess einbezogen sind. Aber auch andere Anbieter von Kreditkarten haben den Sicherheitsmechanismus bei sich implementiert. Die einzelnen Kartenunternehmen betreiben das Verfahren jeweils unter einem eigenen Label: Mastercard® Identity Check (ehemals Mastercard SecureCode), Visa Secure (ehemals Verified by Visa), Safe Key von American Express, J/Secure™ von JBC (Japan Credit Bureau).

3D-Secure kann auch außerhalb von Zahlungen zur Authentifizierung eines Karteninhabers genutzt werden, zum Beispiel zur Identitätsverifizierung beim Hinzufügen neuer Karten in eine Bezahl-App.

Wie wird eine Zahlung durch 3D-Secure authentifiziert?

Die Authentifizierung des rechtmäßigen Karteninhabers findet durch die kartenausgebende Bank statt. Wie genau die Interaktion von kartenausgebender Bank und Kunde aussieht, wird von der Bank festgelegt. Das Protokoll von 3D-Secure ermöglicht die Interaktion dieser beiden Akteure, bevor der Händler die Zahlung final zur Weiterverarbeitung an seine Bank freigibt. Mögliche Authentisierungen sind die Abfrage von statischen Passwörtern und von Einmal-Passwörtern, wie zum Beispiel SMS-TANs, oder auch von biometrischen Faktoren.

Darüber hinaus gibt es unterschiedliche Versionen von 3D-Secure. Alle haben gemeinsam, dass sie im Gegensatz zu Transaktionen ohne 3D-Secure eine Verbindung zwischen Kartenausgeber (kartenausgebender Bank) und Kunde herstellen, die zur Authentifizierung genutzt werden kann. Frühere Versionen von 3D-Secure unterstützten in der Regel die statischen Authentifizierungsverfahren, die neben der gewohnten Angabe von Kartendaten die Eingabe eines statischen Codes, zum Beispiel eines Passworts, verlangten.

Mit der neueren Version von 3D-Secure werden Authentifizierungsverfahren eingesetzt, die den Ansprüchen der „starken Kundenauthentifizierung“ gerecht werden und deren Umsetzung erleichtern. Dabei wird zum einen der Zahler durch einen Faktor der Kategorie „Wissen” (z.B. Passwort) oder „Biometrie” (z.B. Fingerabdruck) und zum anderen der Zahler und die Zahlung dynamisch durch einen Faktor der Kategorie „Besitz” (z.B. SMS-TAN oder Bezahl-App) authentifiziert.

Wie wird 3D-Secure aktiviert?

Die Authentifizierung mit 3D-Secure setzt immer eine bereits bestehende Verbindung zwischen der Bank als Kartenausgeber und dem Kunden der Bank als Karteninhaber voraus. Ein Karteninhaber registriert sich vor dem ersten Einsatz des Verfahrens bei der Bank, die auch die Kreditkarte ausgestellt hat, zum Beispiel über Online-Banking. Die Bank liefert dem Karteninhaber dann die notwendigen Authentisierungsmittel, wie zum Beispiel den Zugang zum TAN-Verfahren oder ein statisches Passwort. Anhand dieser Authentisierungsmittel kann der Karteninhaber bei Transaktionen seiner Karte zugeordnet werden.

Werden Kartenzahlungen im E-Commerce ohne 3D-Secure weiterhin angeboten?

Zahlungen im E-Commerce durch alleinige Angabe von Kartennummer (PAN), Name des Karteninhabers, Gültigkeitsdatum und Cardholder Verification Code (CVC) sind weiterhin möglich.

Wann wird eine Zahlung mit 3D-Secure authentifiziert?

Um eine Zahlung mit 3D-Secure authentifizieren zu können, muss der E-Commerce-Händler in der Lage sein, das Verfahren in den Bezahlvorgang einbauen zu können, d.h. die Technik wird in den Online-Shop integriert. Der Händler und die Bank müssen zudem beide technisch in der Lage sein, 3D-Secure zu unterstützen.

Allerdings muss eine Zahlung mit Kreditkarte nicht unbedingt mit 3D-Secure authentifiziert werden. Auch hier greifen die in der PSD2 festgelegten Ausnahmen, wie in dem Kapitel zur PSD2 bereits ausgeführt.

Wird eine Zahlung nicht mit 3D-Secure abgesichert, kann diese wie bisher unter alleiniger Angabe von PAN, Name des Karteninhabers, Gültigkeitsdatum und CVC freigegeben werden – immer unter der Prämisse, dass Händler und Bank diese Transaktion so freigeben. Der Kunde selbst kann nicht beeinflussen, ob Zahlungen mit oder ohne 3D-Secure authentifiziert werden. Die Entscheidung liegt letztendlich bei der Bank und so ist ein Einfluss des Kunden nur mittelbar über den Transaktionsbetrag und weitere Risikoparameter möglich. Tätigt der Kunde eine Transaktion, die einen Kleinstbetrag umfasst und einen Händler im Inland betrifft, bei dem er zuvor schon eingekauft hat, ist die Wahrscheinlichkeit, dass 3D-Secure eingesetzt wird, geringer. Die genauen Ausnahmen von 3D-Secure Zahlungen kann der Nutzer meistens auf der Webseite seiner Bank erfahren.

Wie sicher ist 3D-Secure?

Wie beim Online-Banking hängt die Sicherheit von 3D-Secure vom Authentifizierungsverfahren ab, das die Bank anbietet. Ein statisches Verfahren, wie die Nutzung eines Passworts, ist dabei unsicherer als ein dynamisches Verfahren, wie eine Transaktion via Chip-TAN. Insgesamt entsteht mehr Aufwand für den Kunden als bei Kreditkartenzahlungen ohne 3D-Secure, um mehr Sicherheit zu gewinnen.

Vorteile des Bezahlens mit Kreditkarte und 3D-Secure

- Zur Nutzung ist eine Registrierung bei der Bank erforderlich.
- Erfordert Informationen, die über die auf der Karte ablesbaren hinausgehen und ist daher sicherer als die bloße Eingabe der Kreditkartendaten.
- Betrug wird erschwert, da Authentifizierung des Kunden stattfindet.
- Keine zusätzlichen Kosten für den Nutzer.

Nachteile des Bezahlens mit Kreditkarte und 3D-Secure

- Registrierung bei der Bank erforderlich – aus Nutzersicht eher umständlich.
- Bezahlen im E-Commerce erfordert die Nutzung der Authentisierungsmittel wie beim Online-Banking.

4.3 Sofortüberweisung

Was ist Sofortüberweisung?

Sofortüberweisung ist ein Zahlungsdienst, bei dem der Kunde eine Zahlung mit den gewohnten Online-Banking-Daten abschließen und damit per Überweisung sofort bezahlen kann. Für die Freigabe der Zahlung nutzt der Kunde die Authentisierungsmittel, die ihm von seiner Bank für das Online-Banking bereitgestellt wurden (z.B. Lesegerät und Karte oder Banking-App auf einem mobilen Endgerät). Der Kunde gibt die Zahlung in der Regel durch die Online-Banking-PIN und eine TAN frei. Bei Sofortüberweisung wird eine sichere Datenverbindung zur Bank des Kunden aufgebaut und zur Übertragung der Transaktionsdaten genutzt. Wie genau eine Zahlung freigegeben wird, entscheidet die Bank. Für den Zahlungsdienst Sofortüberweisung muss mindestens eine Möglichkeit von der Bank bereitgestellt werden.

Manche Banken fordern die Authentifizierungsdaten für Sofortüberweisung über eine eigene Maske an. Diese Maske ist vergleichbar mit den Eingabefeldern, die auch beim Online-Banking Verwendung finden. Bei anderen Banken wird der Nutzer von Sofortüberweisung zur Freigabe der Zahlung kurzzeitig auf die Seite seiner Bank gelenkt, wo der Kunde sein Authentisierungsmittel nutzt, wie er es aus dem Online-Banking kennt. Hier werden die Daten (z.B. Online-Banking-PIN und TAN) direkt bei seiner Bank eingegeben. Sofortüberweisung erhält keinen Zugriff auf diese Daten. Die Bank teilt Sofortüberweisung das Ergebnis der Authentifizierung mit.

Ist die Banking-App das Authentisierungsmittel, so kann die Bank den Kunden auch direkt über die Banking-App auf einem mobilen Endgerät auffordern, die Zahlung für Sofortüberweisung freizugeben. Auch in diesem Fall erhält Sofortüberweisung keinen Zugriff auf die Daten, sondern wird von der Bank über das Ergebnis der Authentifizierung informiert.

Wie wird Sofortüberweisung aktiviert?

Für die Nutzung von Sofortüberweisung benötigt der Kunde kein Benutzerkonto bei Sofortüberweisung, daher ist auch keine Aktivierung erforderlich. Das bedeutet, dass von Sofortüberweisung keine persönlichen Kundendaten benötigt werden.

Was muss bei der Eingabe von Online-Banking-PIN und TAN beachtet werden?

Sofortüberweisung ist ein regulierter Zahlungsdienstleister. Der Kunde sollte sicherstellen, dass die angezeigte Transaktion tatsächlich ausgeführt wird. Dazu sollten die von Sofortüberweisung bereitgestellten Einkaufsinformationen, insbesondere der Betrag und der Empfänger, unbedingt abschließend überprüft werden.

Auch bei Sofortüberweisung muss die Zahlung durch den Kauf einer Ware oder einer Dienstleistung veranlasst werden. Weder die Online-Banking-PIN noch eine TAN sollten auf einer Web-Seite im Internet eingegeben werden, wenn zuvor kein Kauf getätigt und keine Zahlung initiiert wurde („Phishing-Angriffe“).

Was muss noch aus Sicherheitsgründen beachtet werden?

Mit der Eingabe der Zugangsdaten ist Sofortüberweisung technisch in der Lage, die Kontodaten zu lesen. Daher sollte der Kunde vor der Nutzung von Sofortüberweisung in den Nutzungsbedingungen überprüfen, welche Rechte er an den Anbieter überträgt.

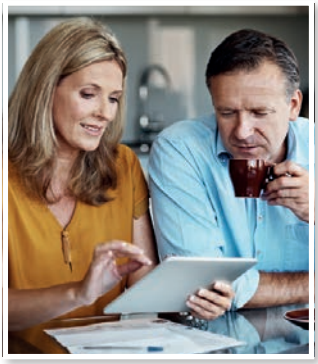
Vorteile von Sofortüberweisung

- Es ist keine gesonderte Registrierung mit Benutzername und Passwort für den Dienst notwendig. Die Abwicklung erfolgt über die Daten des Online-Bankings.
- Kontodaten müssen nicht bei jedem Händler eingegeben werden. Lediglich ein Zahlungsdienstleister erhält die Daten. Dadurch einfach wie das Online-Banking.
- Weite Verbreitung

Nachteile von Sofortüberweisung

- Preisgabe der Kontodaten sowie der PIN und TAN gegenüber einem Drittdienst.
- Die Beziehung zwischen Nutzer und seiner Bank ist durch die Zwischenschaltung eines Zahlungsdienstleisters, der gegenüber der Bank als Kunde auftritt, getrennt. Der Zahlungsdienstleister agiert im Namen des Kunden.
- Gefahr von „Phishing-Angriffen“

4.4 Paypal



Was ist PayPal?

PayPal ist ein wichtiges E-Commerce-Bezahlverfahren in Deutschland. Benutzer können durch einfaches Einrichten eines eigenen PayPal-Kontos dieses Bezahlverfahren nutzen. Eine Nutzung des Verfahrens via App ist ebenfalls möglich.

Grundlage für eine PayPal-Zahlung ist immer das Versenden von E-Geld von einem PayPal-Konto des Zahlers an ein PayPal-Konto des Zahlungsempfängers. Für das Ausgleichen seines PayPal-Kontos muss ein Zahler bei seinem PayPal-Konto eine oder mehrere Zahlungsquellen hinterlegen. Zahlungsquellen können Girokonten oder Kreditkarten des Zahlers sein.

Bei der Zahlung mit einem PayPal-Konto wird die Zahlungsquelle des Zahlers entsprechend belastet und der Betrag in eine äquivalente Summe E-Geld umgewandelt. Das so erhaltene E-Geld wird dann von dem PayPal-Konto des Zahlers auf das PayPal-Konto des Zahlungsempfängers PayPal-intern umgebucht.

Der Inhaber eines PayPal-Kontos kann auf seinem PayPal-Konto auch E-Geld von anderen PayPal-Konten erhalten und so an ein E-Geld-Guthaben gelangen. Dieses Guthaben kann auf eine seiner Zahlungsquellen umgebucht werden.

Wie wird ein PayPal-Konto eingerichtet?

Ein neues PayPal-Konto kann über die Webseite des Anbieters unter www.paypal.de eingerichtet werden. Zur Einrichtung muss der Benutzer neben einer E-Mail-Adresse als Benutzerkennung ein Passwort für den Zugang festlegen und mindestens eine Zahlungsquelle zu dem PayPal-Konto hinzufügen.

Wie ist das Einloggen bei einem PayPal-Konto abgesichert?

Beim Einloggen muss der Benutzer seine Benutzerkennung und sein Passwort eingeben.

Als Benutzerkennung wird die E-Mail-Adresse genutzt, die der Benutzer beim Einrichten des PayPal-Kontos angegeben hat. Das Passwort legt der Benutzer beim Einrichten des PayPal-Kontos selbst fest. Es kann durch den Benutzer nach dem Einloggen in sein Konto in den Sicherheitseinstellungen geändert werden.

Optional kann das Einloggen durch eine zweistufige Verifizierung, also der Eingabe eines zusätzlichen Sicherheitscodes, abgesichert werden. Dabei wird ein einmal gültiger zufälliger Sicherheitscode durch PayPal mittels SMS an eine Mobiltelefonnummer gesendet, die der Benutzer bei seinem PayPal-Konto hinterlegt hat. Der Benutzer muss den empfangenen Sicherheitscode beim Einloggen eingeben. Alternativ kann hier auch eine Authentifizierungs-App eingesetzt werden.

Die Nutzung des zusätzlichen Sicherheitscodes kann durch den Benutzer nach dem Einloggen aktiviert und auch wieder deaktiviert werden. Es wird dringend empfohlen, die Nutzung des zusätzlichen Sicherheitscodes zu aktivieren.

Durch die Aktivierung des zusätzlichen Sicherheitscodes wird das Einloggen in ein PayPal-Konto durch eine Zwei-Faktor-Authentifizierung abgesichert.

Wie wird eine Zahlung mit PayPal ausgelöst?

Zunächst muss im Online-Shop PayPal als Bezahlverfahren ausgewählt werden. Danach wird der Kunde auf die PayPal-Seite weitergeleitet. Dort muss er sich in sein PayPal-Konto einloggen. Der Name des Online-Händlers und der Betrag der Zahlung werden angezeigt. Nach Kontrolle der angezeigten Daten kann die Zahlung mittels OK-Button bestätigt werden.

Sind im PayPal-Konto mehrere Zahlungsquellen (z.B. verschiedene Bankkonten) hinterlegt, wird nach dem Einloggen eine Liste der möglichen Zahlungsquellen angezeigt. Vor Bestätigung der Zahlung muss die für die Zahlung zu verwendende Zahlungsquelle ausgewählt werden.

Wird für die PayPal-Zahlung eine hinterlegte Kreditkarte genutzt, kann es vorkommen, dass die Kreditkartenzahlung zusätzlich über ein 3D-Secure-Verfahren bestätigt werden muss. Das entsprechende Vorgehen ist vom Herausgeber der Kreditkarte vorgegeben.

Wie kann ein PayPal-Konto gesperrt werden?

Sollte ein Einloggen in das PayPal-Konto noch möglich sein, kann das Konto nach dem Einloggen unter der Option „Konto schließen" nach Klicken des Zahnrad-Symbols gesperrt weden. Die anschließende Nachfrage von PayPal, ob dies wirklich durchgeführt werden soll, muss bestätigt werden.

Ist ein Einloggen nicht möglich (z.B. bei vergessenem Passwort), kann der Zugang zum PayPal-Konto durch mehrfache Eingabe

eines falschen Passworts gesperrt werden. Dadurch wird das PayPal-Konto jedoch nicht aufgelöst oder endgültig gesperrt, sondern der Zugang kann durch Vergabe eines neuen Passworts reaktiviert werden. Dazu muss beim Einloggen auf „Probleme beim Einloggen“ geklickt werden. Danach muss der Benutzer nachweisen, dass er der Inhaber des PayPal-Kontos ist. Dazu werden verschiedene Möglichkeiten zur Auswahl angeboten. Abhängig von der Einrichtung des PayPal-Kontos kann dies über den Versand einer E-Mail durch PayPal an die für das Konto hinterlegte E-Mail-Adresse, durch den Versand einer SMS an die für das Konto hinterlegte Mobiltelefonnummer oder durch die Beantwortung einer bei der Einrichtung des Kontos vereinbarten Sicherheitsfrage erfolgen. Wurde für das PayPal-Konto eine Kreditkarte als Zahlungsquelle hinzugefügt, kann auch die Eingabe der Kreditkartennummer als Sicherheitsfrage genutzt werden.

Die endgültige Sperrung des PayPal-Kontos ohne Einloggen kann nur telefonisch über den Kundenservice von PayPal durchgeführt werden, der jedoch nicht rund um die Uhr erreichbar ist. Bei Anruf muss sich der Benutzer durch Angabe der Kundenservice-PIN authentifizieren. Diese Kundenservice-PIN muss vorher im PayPal-Konto eingerichtet werden. Ohne Kundenservice-PIN kann der telefonische Kundenservice nicht genutzt werden.

Ein einmal gesperrtes PayPal-Konto kann nicht wieder entsperrt bzw. reaktiviert werden. Der Kunde kann jedoch ein neues PayPal-Konto eröffnen. Für die Eröffnung eines neuen PayPal-Kontos kann die gleiche E-Mail-Adresse als Benutzerkennung verwendet werden, wie bei der Eröffnung des vorherigen, jetzt gesperrten PayPal-Kontos.

Was muss noch aus Sicherheitsgründen beachtet werden?

Bei jedem PayPal-Konto sollte die Nutzung des Sicherheitscodes als zweiter Faktor beim Einloggen aktiviert werden.

Für den obligatorischen ersten Faktor, das Passwort, gelten die Hinweise des BSI zu Länge, Einmaligkeit etc. (vgl. https://www.bsi-fuer-buerger.de/Passwoerter).

Die Möglichkeit, beim PayPal-Konto eingeloggt zu bleiben, muss in jedem Fall deaktiviert sein, da es die betrügerische Nutzung von Zahlungsmitteln, die im PayPal-Konto hinterlegt sind, vereinfacht.

Per E-Mail von PayPal eingehende Zahlungsbestätigungen müssen immer daraufhin kontrolliert werden, ob sie den gerade getätigten Transaktionen entsprechen oder die Abwicklung eines eingerichteten Abonnements enthalten.

Eine PayPal-Zahlung sollte durch Einloggen nur dann bestätigt werden, wenn zuvor PayPal für das Bezahlen in einem Online-Shop als Bezahlverfahren ausgewählt wurde.

Bei Verdacht auf Missbrauch eines PayPal-Kontos muss dieses unverzüglich gesperrt werden. Falls dies aufgrund eines vergessenen Passworts nicht durch Einloggen in das PayPal-Konto durchgeführt werden kann, sollte hilfsweise mehrfach ein falsches Passwort eingegeben werden, bis der Zugang gesperrt ist.

Ist für ein PayPal-Konto eine Kreditkarte als Zahlungsquelle hinterlegt, sollte für diese das 3D-Secure-Verfahren aktiviert sein, da PayPal eine Authentifizierung des Karteninhabers mittels 3D-Secure-Verfahren verlangen kann. Informationen zum Vorgehen sind beim kartenausgebenden Unternehmen erhältlich.

Bei einem PayPal-Konto sollten nur die Zahlungsquellen (Konto, Kreditkarte) hinterlegt werden, die auch wirklich benötigt werden. In der Regel ist es ausreichend, eine Zahlungsquelle zu hinterlegen.

Vorteile von PayPal

- Weite Verbreitung
- Sehr einfache Handhabung
- Zusätzlicher Sicherheitscode als zweiter Faktor beim Einloggen möglich.
- Händler erhält nur Informationen über den erfolgreichen Zahlungsvorgang, nicht aber über die Kreditkarte oder die Kontoverbindung des Kunden.
- Falls ein Einloggen in das PayPal-Konto möglich ist, kann es einfach gesperrt werden. Zahlungsquellen können einfach aus dem Konto gelöscht werden.

Nachteile von PayPal

- Falls der Sicherheitscode nicht aktiviert wurde und kein 3D-Secure durchgeführt wird, ist das Auslösen einer Zahlung nur mittels Passwort möglich.
- Sperrung eines PayPal-Kontos, bei dem das Einloggen durch zu häufige Login-Versuche (z.B. bei vergessenem Passwort) nicht mehr möglich ist, kann unter Umständen zeitkritisch sein.
- Ein gesperrtes PayPal-Konto kann durch die Option „Passwort wiederherstellen“ wieder aktiviert werden.

4.5 Apple Pay

Was ist Apple Pay?

Apple Pay ist eine Technologielösung für Banken, um ihren Kunden die Möglichkeit zu bieten, in Geschäften kontaktlos mit Bezahlkarten der Bank des Kunden über Near Field Communication (NFC) am Zahlungsterminal (POS), oder im Internet (E-Commerce) zu bezahlen. In beiden Fällen muss die Transaktion vom Konsumenten biometrisch (durch Touch ID oder Face ID) oder über den Passcode des Smartphones bestätigt werden. Kunden verwenden immer die von der Bank ausgegebenen Karten, um Zahlungen über den Apple Pay Service zu tätigen, und alle Transaktionen werden vom Kartenaussteller authentifiziert. Am POS hält der Kunde das mobile Apple Endgerät an das Zahlungsterminal. Auch im E-Commerce wird Apple Pay inzwischen oft als Bezahlart angeboten. Hier wird die Transaktion über das Internet von der Bank des Kunden authentifiziert. In beiden Fällen muss die Transaktion durch Touch ID bzw. Face ID oder den Passcode des Smartphones bestätigt werden.

Wie wird Apple Pay aktiviert?

Beteiligt sich die Bank des Kunden an Apple Pay, wird zur Aktivierung von Apple Pay die Debit- oder Kreditkarte dieser Bank vom Kunden als Token in einem Chip, dem „Secure Element" verarbeitet und gespeichert. Dabei handelt es sich um ein besonders abgesichertes Hardware Element im Endgerät, das in diesem Kontext ähnlich zu einem Chip auf einer Karte agiert. Der Kunde kann diesen Prozess direkt über die mobile App seiner Bank oder durch Hinzufügen seiner Kartendaten bei der Einrichtung seines

neuen Geräts oder über die Wallet-App initiieren. Die Bank führt dann eine Identitätsprüfung durch, bevor die Karte für den Dienst freigeschaltet wird. Dieser Prozess kann von Bank zu Bank variieren. In der Regel werden die Authentisierungsmittel des Online-Bankings genutzt.

Wie wird die Zahlung durch den Besitz des Smartphones authentifiziert?

Sensitive Daten der hinterlegten Debit- oder Kreditkarte werden im Smartphone nicht gespeichert. Stattdessen erzeugt die Bank des Kunden neue Daten für das Gerät („Tokenisierung“), die es der Bank ermöglichen, das Smartphone der hinterlegten Karte zuzuordnen. Diese Daten werden im „Secure Element” verarbeitet und gespeichert. Das Smartphone erzeugt aus den Daten im Secure Element einen für den Kunden nicht sichtbaren dynamischen Authentifizierungscode. Dieser Code wird bei der Zahlung an die Bank übermittelt und ermöglicht es der Bank, den Kunden anhand des Eigentums am Gerät zu authentifizieren. Der Händler erhält von Apple Pay keine Kundendaten, sondern nur die Information, dass die Zahlung erfolgt ist.

Wie wird eine Zahlung durch das zweite Element authentifiziert?

Zahlungen über Apple Pay werden unabhängig vom Zahlungsbetrag immer über zwei unabhängige Elemente authentifiziert: Zum einen über das Smartphone („Besitz”), zum anderen über Touch ID bzw. Face ID („Inhärenz”) oder Geräte-Passcode („Wissen”).

Um im Geschäft zu bezahlen, hält der Kunde das Smartphone an das Terminal und authentifiziert sich mit Touch ID bzw. Face ID. Selbst wenn ein Betrüger das Smartphone stiehlt, kann er keine Zahlung freigeben, da er nicht über die an die Touch ID

bzw. an die Face ID gekoppelten biometrischen Merkmale des Kunden verfügt. Außerdem kann ein Betrüger das Smartphone nicht unbemerkt über die NFC-Schnittstelle kontaktieren und eine Zahlung auslösen („Relay-Angriffe“), da die Authentifizierung mittels Touch ID bzw. Face ID nicht vorgenommen wurde.

Wann muss Apple Pay gesperrt werden?

Wird das Smartphone gestohlen, sollte der Kunde die Sperrung von Apple Pay veranlassen. Hierzu stehen Möglichkeiten über das Service-Center der Bank, die Funktion „Mein iPhone suchen” und über die Apple-ID zur Verfügung. Außerdem kann die hinterlegte Karte über die Bank des Kunden deaktiviert werden. Einige Banken bieten dem Kunden die Möglichkeit, seine Plastikkarte weiterhin zu verwenden, wenn sie nicht verloren oder gestohlen wurde. Grundsätzlich ist eine Sperrung bei Verlust des Smartphones aufgrund der Tokenisierung nicht notwendig, doch die Umsetzung dieser Funktion liegt in der Verantwortung des Kunden.

Was muss noch aus Sicherheitsgründen beachtet werden?

Der gewählte Passcode sollte schwer zu erraten sein. Da alle für das mobile Endgerät freigeschalteten Nutzer die Funktion von Apple Pay verwenden können, sollte der Nutzer nur die eigenen biometrischen Merkmale hinterlegen und nicht die anderer Personen.

Hinterlegte Debit- oder Kreditkarten sollten aus der Apple Wallet entfernt werden, wenn das mobile Endgerät verkauft wird. Dazu muss der Kunde, die in der Apple Pay Wallet hinterlegte Karte löschen. Wenn sich der Kunde jedoch von seinem iCloud-Konto abmeldet, werden alle Karten auf diesem Gerät automatisch entfernt. Soll Apple Pay auf einem neuen Gerät genutzt werden, muss die Karte dort erneut in der Wallet hinterlegt werden.

Wie sicher ist Apple Pay?

Sicherheitsupdates sollten entsprechend den Empfehlungen in das mobile Endgerät eingespielt werden. Außerdem sollten die Betriebssystemrechte des mobilen Endgerätes nicht außer Kraft gesetzt werden („Jailbreak"), um eine möglichst hohe Sicherheit des Verfahrens zu gewährleisten. Mit der Tokenisierung und der Nutzung des Passcodes bzw. der biometrischen Merkmale bei jeder Transaktion stehen Sicherheitsfunktionen zur Verfügung, die die Transaktionsdaten schützen.

Vorteile von Apple Pay

- Sensitive Daten werden im Secure Element verarbeitet und gespeichert.
- Tokenisierung
- Wird von der Mehrheit deutscher Banken angeboten.
- Relay-Angriffe erschwert
- Sperrung leicht möglich
- Auch bei Kleinbeträgen wird der Passcode oder das biometrische Merkmal geprüft.

Nachteile von Apple Pay

- Alle Nutzer, die für das mobile Endgerät freigeschaltet sind, können Apple Pay nutzen.
- Einsatz auf Apple Produkte beschränkt

4.6 Google Pay

Was ist Google Pay?

Google Pay ist ein mobiles Bezahlverfahren, mit dem im Geschäft kontaktlos über NFC am Zahlungsterminal (POS) oder im Internet (E-Commerce) bezahlt werden kann. Am POS hält der Kunde das Smartphone mit dem entsperrten Display an das Zahlungsterminal. Im E-Commerce kann beim Kauf das Bezahlen via Google Pay ausgewählt werden. Hier wird das Smartphone über das Internet authentifiziert. Handelt es sich nicht um kleinere Zahlungen unter derzeit 25 Euro, so muss die Transaktion durch die biometrische Funktion (z.B. Fingerabdruck) oder den Passcode des Smartphones bestätigt werden.

Wie wird Google Pay aktiviert?

Beteiligt sich die Bank eines Kunden an Google Pay, muss zur Aktivierung von Google Pay die Debit- oder Kreditkarte dieser Bank vom Kunden in der Google Wallet hinterlegt werden. Hat der Kunde kein Konto bei einer entsprechenden Bank, kann anstelle einer Karte auch ein PayPal-Benutzerkonto hinterlegt werden. Hierzu muss die App „Google Pay“ im Play Store geladen werden. Die Kartendaten werden dann entweder manuell oder fotografisch übertragen. Zur Identitätsprüfung durchläuft der Kunde ein Authentisierungsverfahren, das je nach Bank unterschiedlich sein kann. In der Regel werden die Authentisierungsmittel des Online-Bankings genutzt.

Wie wird die Zahlung durch den Besitz des Smartphones authentifiziert?

Sensitive Daten der hinterlegten Debit- oder Kreditkarte werden im Smartphone nicht gespeichert. Stattdessen werden im Gerät neue Daten erzeugt („Tokenisierung"), die es der Bank ermöglichen, das Smartphone der hinterlegten Karte zuzuordnen. Diese Daten werden in der Bezahl-App verarbeitet und gespeichert. Das Smartphone erzeugt daraus einen für den Kunden nicht sichtbaren, dynamischen Authentifizierungscode, der beim Bezahlen an die Bank übertragen wird und der Bank ermöglicht, den Kunden über den Besitz des Smartphones zu authentifizieren. Der Händler erhält von Google Pay keine Kundendaten, sondern nur die Information, dass die Zahlung erfolgt ist.

Wie wird eine Zahlung durch das zweite Element authentifiziert?

Handelt es sich nicht um Kleinbeträge (unter 25 EUR), werden Zahlungen über Google Pay mit zwei unabhängigen Elementen authentifiziert. Zum einen über das Smartphone („Besitz"), zum anderen muss das Gerät über Fingerabdruck bzw. Gesichtserkennung („Inhärenz") oder Geräte-Passcode („Wissen") vom Kunden entsperrt werden. Zum Bezahlen im Geschäft aktiviert der Kunde den Bildschirm, hält das Smartphone an das Zahlungsterminal (POS) und authentisiert sich über Fingerabdruck bzw. Gesichtserkennung oder Geräte-Passcode. Zahlungen, die keine Kleinbeträge sind, werden also immer durch die Prüfung des Passcodes oder des Fingerabdrucks bzw. des Gesichts authentifiziert. Dadurch kann ein Betrüger bei Diebstahl des Smartphones oder bei unbemerkter Kontaktierung der NFC-Schnittstelle nur Kleinbeträge freigeben („Relay-Angriffe").

Wann muss Google Pay gesperrt werden?

Wird das Smartphone gestohlen, sollte der Kunde die Sperrung von Google Pay veranlassen. Bei Verlust oder Diebstahl des Geräts kann der Kunde dies über „Mein Gerät finden", „suchen", „sperren" oder „löschen" veranlassen. Ist das Smartphone gesperrt, kann Google Pay nicht verwendet werden. Der Kunde kann das an die hinterlegte Karte gebundene Google Pay auch über seine Bank sperren lassen, wobei die hinterlegte Debit- oder Kreditkarte nicht gesperrt wird. Eine Sperrung der hinterlegten physischen Debit- oder Kreditkarte ist bei Verlust des Smartphones aufgrund der Tokenisierung nicht erforderlich.

Was muss noch aus Sicherheitsgründen beachtet werden?

Der gewählte Passcode sollte schwer zu erraten sein. Da alle für das Smartphone freigeschalteten Nutzer Google Pay anwenden können, sollte der Nutzer nur die eigenen biometrischen Merkmale hinterlegen und nicht die anderer Personen. Bei der Betätigung des Home-Buttons ist darauf zu achten, dass nicht versehentlich eine Zahlung mittels Fingerabdruck freigegeben wird.

Hinterlegte Debit- oder Kreditkarten sollten aus der Google Wallet entfernt werden, wenn das Smartphone verkauft wird.

Wie sicher ist Google Pay?

Sicherheitsupdates sollten frühzeitig in das Smartphone eingespielt werden. Außerdem sollten die Betriebssystemrechte des Geräts nicht außer Kraft gesetzt werden („Rooting"), um eine möglichst hohe Sicherheit des Verfahrens zu gewährleisten.

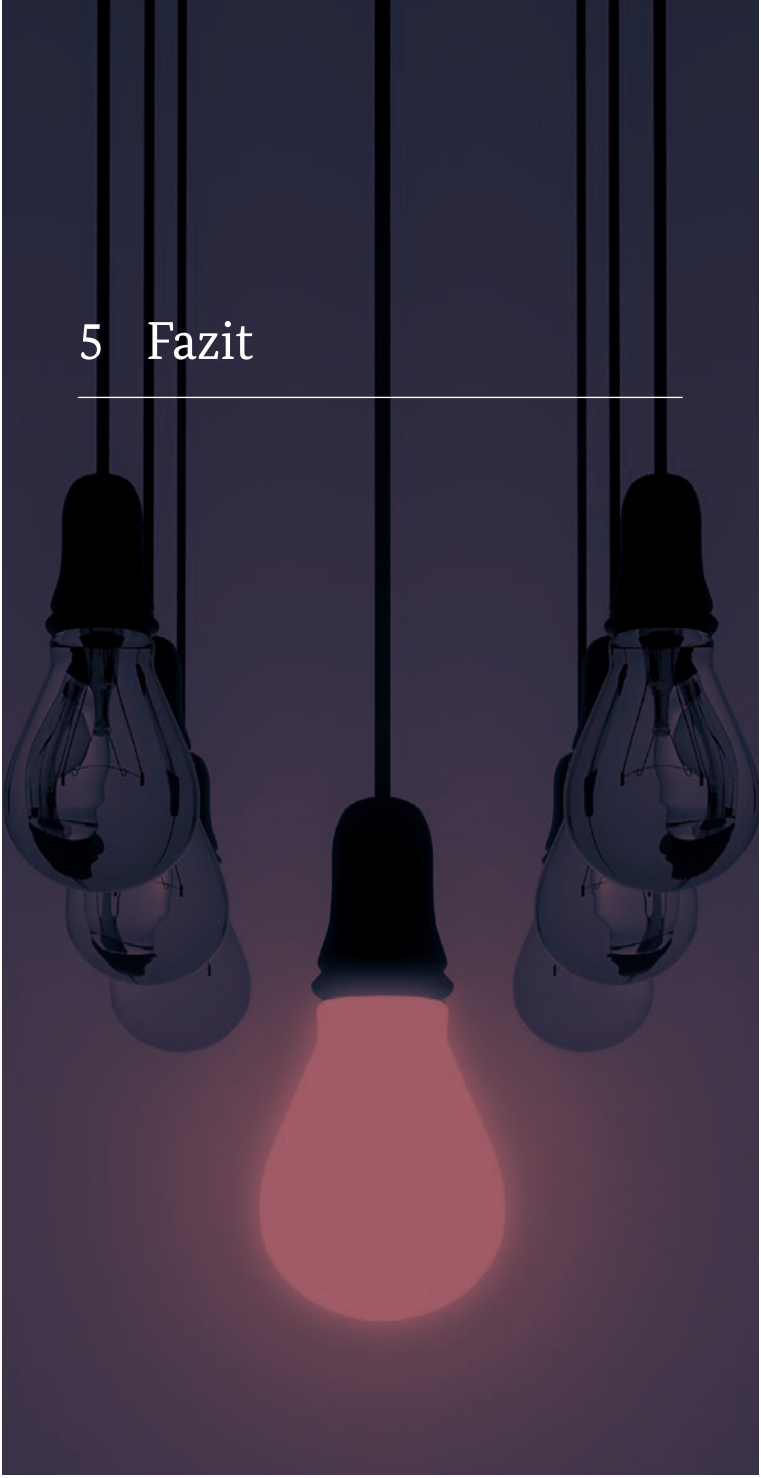
Vorteile von Google Pay

- Tokenisierung
- Sperrung leicht möglich
- Relay-Angriffe sind nur bei Kleinbeträgen denkbar.

Nachteile von Google Pay

- Sensitive Daten werden in der Regel nicht in einem Secure Element verarbeitet und gespeichert.
- Sind biometrische Merkmale mehrerer Personen hinterlegt, ermöglicht dies ungewollte Zahlungsauslösungen.
- Nur nutzbar mit einem Smartphone mit Android-Betriebssystem.
- Bei Kleinbeträgen ist die Nutzung des Passcodes oder des biometrischen Merkmals nicht erforderlich.

5 Fazit



Fazit

Bezahlverfahren haben sich in den letzten Jahren grundlegend gewandelt. Dafür ist das Bezahlen mit mobilen Geräten ein gutes Beispiel: Aufgrund immer leistungsstärkerer Smartphones mit immer größeren Displays und der Bereitstellung verschiedenster Funktionen zu Verbindung wie Near Field Communication (NFC), Beacon und Bluetooth Low Energy (BLE), Barcode und Quick Response Code (QR-Code), steigt die Benutzerfreundlichkeit und auch die mobilen Bezahllösungen selbst werden funktioneller und einfacher in der Bedienung.

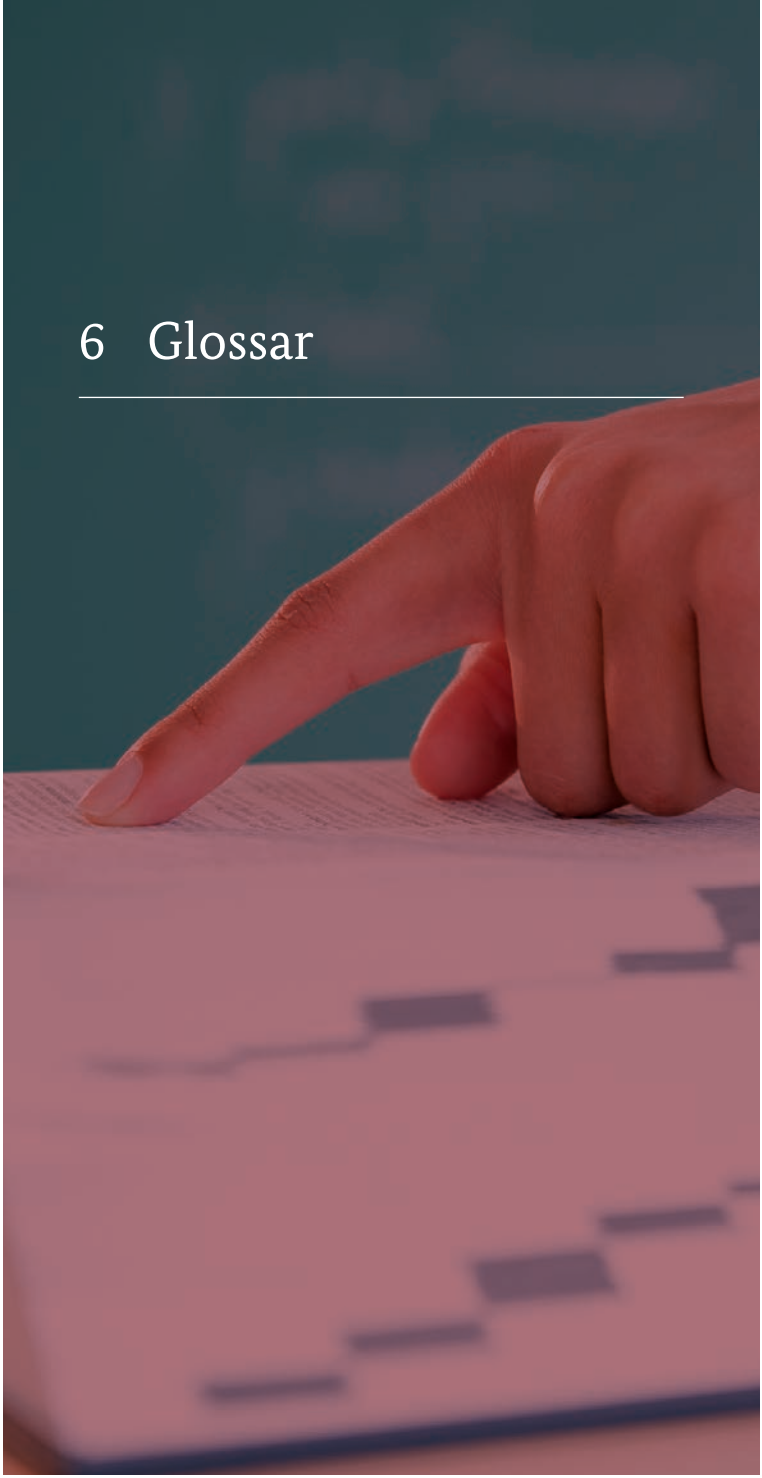
Alternativ bieten Banken und auch Zahlungsdienstleister neben dem klassischen Online-Banking via Webportal vermehrt Anwendungen mit sogenannten Banking-Apps an. Diese können teilweise für klassische Bankgeschäfte wie Transaktionen oder Daueraufträge genutzt werden, aber auch für Zahlungen am Point of Sale (POS) und im E-Commerce. Der Nutzer wird bei der Wahl seines Bezahlverfahrens vielleicht durch die Auswahl seines Smartphones bzw. des Betriebssystems eingeschränkt – Apple-Nutzer wählen Apple Pay, Android-Nutzer eben Google Pay. Besonders wichtig ist es aber, sich nicht von Bequemlichkeit leiten zu lassen, sondern der Sicherheit den Vorzug zu geben. Die Anwendung von 3D-Secure bei Online-Einkäufen mit Kreditkarte ist noch nicht vollständig verpflichtend. Hier kann der Nutzer keinen Einfluss nehmen, da der Online-Händler bestimmt, wie er dieses Authentisierungsverfahren implementiert. Nutzer können aber zum Beispiel darauf achten, in Online-Shops einzukaufen, bei denen die Nutzung der Kreditkarte durch 3D-Secure abgesichert ist.

Aus Gründen der Herstellerneutralität gibt das BSI keine Empfehlungen für oder gegen ein konkretes Bezahlverfahren.

Auch sind die Anforderungen der Nutzer viel zu individuell, um ein Produkt für alle gleichermaßen zu empfehlen.

Abschließend bleibt festzuhalten, dass die Wahl eines sicheren Online-Bezahlverfahrens nur eine von vielen Maßnahmen zur Verbesserung der persönlichen Cyber-Sicherheit ist. Zu vielen weiteren Themen gibt das BSI Hilfestellungen über sein Portal „BSI für Bürger“ (www.bsi-fuer-buerger.de)

6 Glossar



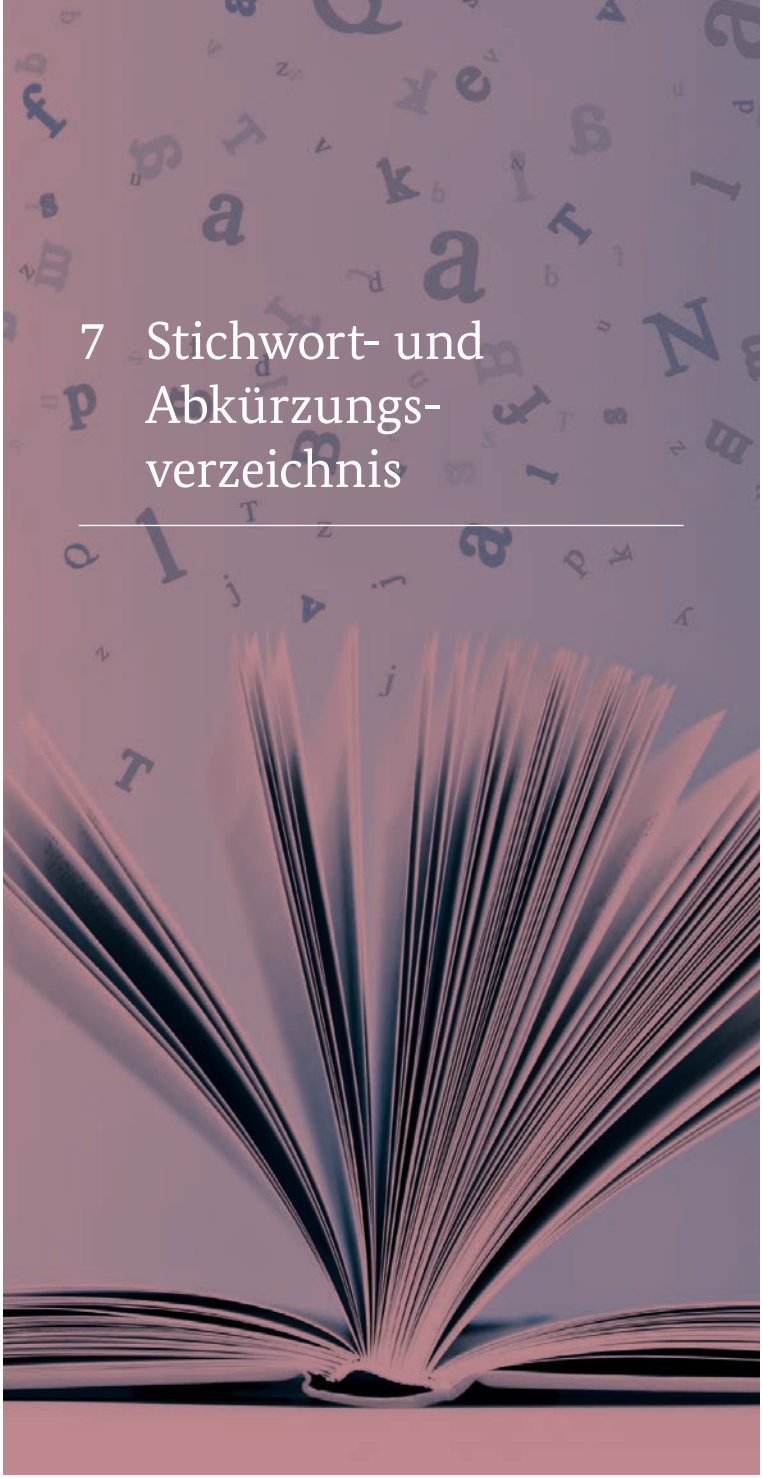
Glossar

BEGRIFF	ERKLÄRUNG
3D-Secure	Verfahren der Kreditkartenunternehmen, das die Authentisierung des Karteninhabers mittels Wissen, Biometrie oder Besitz im E-Commerce ermöglicht.
AGB	Allgemeine Geschäftsbedingungen
AES	Advanced Encryption Standard. Moderner, kryptographischer Algorithmus, der auf symmetrischen Schlüsseln basiert.
Bezahl-App	App auf einem mobilen Endgerät, die eine Zahlung über NFC am POS oder im E-Commerce ermöglicht.
BGB	Bürgerliches Gesetzbuch. Das Bürgerliche Gesetzbuch ist die zentrale Kodifikation des deutschen allgemeinen Privatrechts, wobei Bürger im Sinne von Staatsbürger verstanden wird.
Card-Not-Present-Transaktion	Zahlungstransaktion mit einer Karte ohne Verwendung der EMV-Technologie (EMV), bei der Karteninhaber die Karte zum Zeitpunkt der Bestellung nicht physisch vorlegen, auch nicht zur Prüfung eines Händlers, wie z. B. bei Bestellungen über Katalog per Post, Fax, Telefon oder Internet.
Card-On-File-Transaktion	Spezialfall einer Card-Not-Present-Transaktion, bei der Karteninhaber die relevanten Kartendaten nicht eingeben, sondern stattdessen bereits vorher gespeicherte Kartendaten verwendet werden.
CVC	Cardholder Verification Code. Code mit meistens drei Ziffern, der auf der Rückseite einer Kreditkarte aufgedruckt ist.
digitale Karte	In einem mobilen Endgerät abgelegte Kartendaten, die Zahlungen über das mobile Endgerät möglich machen.
EBA	European Banking Authority. Die Europäische Bankenaufsichtsbehörde ist eine unabhängige EU-Behörde, deren Aufgabe es ist, ein wirksames und kohärentes Maß an Regulierung und Beaufsichtigung im europäischen Bankensektor zu gewährleisten. Die EBA ist unabhängig, jedoch gegenüber dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission rechenschaftspflichtig.
E-Commerce	Handel und zugehörige Zahlungstransaktionen, die im Internet stattfinden, im Gegensatz zum Nahgeschäft am POS.

E-Geld	E-Geld ist jeder elektronisch oder auch magnetisch gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge durchzuführen, und der auch von anderen Personen als dem Emittenten angenommen wird (vgl. §1a(3) ZAG).
EMV	Europay International Mastercard and Visa: Spezifikation für Zahlkarten, die mit einem Chip ausgestattet sind und die entsprechenden Geräte wie zum Beispiel POS Terminals und Bankautomaten.
EMV-Schlüssel	Im Kontext dieses Dokuments ein symmetrischer Schlüssel (Triple-DES, AES), mit dem Applikationskryptogramme berechnet werden. Der EMV-Schlüssel adressiert dabei eindeutig eine PAN oder das zugehörige Token. Mit dem EMV-Schlüssel kann sich der Karteninhaber kryptographisch gegenüber dem Kartenausgeber authentisieren.
EMVCo	Zusammenschluss der globalen Kartenzahlungssysteme, insbesondere MasterCard und VISA, um gemeinsame Standards für Karten umzusetzen.
EWR	Europäischer Wirtschaftsraum
EZB	Europäische Zentralbank. Die Europäische Zentralbank (EZB) ist die Zentralbank der 19 Mitgliedstaaten der Europäischen Union, die den Euro eingeführt haben.
Geldautomat	Terminal zur Geldabhebung mit Karte als Selbstbedienung
Jailbreak	Ein Jailbreak eines Smartphones mit dem Betriebssystem iOS entspricht einem Rooting bei einem Smartphone mit dem Betriebssystem Android. Siehe dort.
mobiles Bezahlverfahren	Bezahlverfahren, bei dem sich der Kunde über sein mobiles Endgerät authentisiert.
mobiles Endgerät	Tragbares elektronisches Gerät wie beispielsweise Smartphone, Tablet oder Smartwatch.
NFC	Near Field Communication
PAN	Primary Account Number. Nummer, anhand derer das Zahlungskonto des Karteninhabers identifiziert wird.
PCI DSS	Payment Card Industry Data Security Standard
physische Karte	Im Gegensatz zur digitalen Karte besteht die physische Karte aus einem Kartenkörper aus Kunststoff mit aufgedruckten Kartendaten, der in der Regel mit einem Chip versehen ist.
POS	Point-of-Sale. Handel und zugehörige Zahlungstransaktionen im Nahgeschäft, im Gegensatz zu Online-Transaktionen, die remote im Internet durchgeführt werden.

PSD2	Revised Payment Services Directive (Zweite Zahlungsdienst-erichtlinie)
Rooting	Durch das Rooting eines Smartphones mit dem Betriebs-system Android erhält der Benutzer erweiterte Rechte zum Installieren und Ausführen von Apps. Die erweiterten Rechte werden auch als Root-Rechte, wie beim UNIX Betriebssystem, oder Administratorrechte genannt. Nach einem Rooting können installierte Apps zum Beispiel direkten Zugriff auf Systemdateien und Daten anderer Apps erhalten. Aus Sicht der Sicherheit des mobilen Endgeräts ist das Rooting problematisch, da Sicherheitsmechanismen einzelner Apps und des Betriebssystems umgangen werden können.
RTS	Regulatory Technical Standard (Technischer Regulierungs-standard). Der RTS zur PSD2 spezifiziert die dortigen Angaben näher, insbesondere zur SCA.
SCA	Strong Customer Authentication (Starke Kunden-authentifizierung). In der PSD2 definiert als Authenti-fizierung, die auf mindestens zwei unabhängigen Faktoren beruht, die den Kategorien „Wissen", „Besitz" und „Inhärenz" angehören.
Secure Element	Ein hardwaretechnisch geschützter Baustein ähnlich dem einer Chipkarte, der in einem mobilen Endgerät verbaut ist, und dort kryptographische Operationen vor Offenlegung und Manipulation auf hohem Sicherheitsniveau schützt.
TAN	Transaktionsnummer. Ein Authentifizierungscode ähnlich dem Applikationskryptogramm, der Trans-aktionsdaten authentisiert. Der Authentifizierungscode kann statisch oder dynamisch sein. Er kann wie das Applikationskryptogramm auf der Grundlage einer kryptographischen Operation berechnet oder zufällig erzeugt worden sein (SMS-TAN).
Token	Eine sich von der PAN unterscheidende, vom Format jedoch identisch aussehende Nummer (16-stellig), die es erlaubt, Transaktionen über das Kartenkonto der PAN durchzuführen. Aus dem Token kann die PAN nicht abgeleitet werden.
ZAG	Zahlungsdiensteaufsichtsgesetz

7 Stichwort- und Abkürzungs-verzeichnis



Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
E-Mail: payment@bsi.bund.de
Internet: www.bsi.bund.de/payment
Telefon +49 (0) 22899 9582 - 0
Telefax +49 (0) 22899 9582 - 5400
Internet: www.bsi.bund.de

Stand
Oktober 2020

Angaben zur Druckerei:
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3
96277 Schneckenlohe
Internet: www.ak-druck-medien.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bildnachweis
Titel: GettyImages © Westend, S. 4: BSI, S. 5: BSI, S. 6: GettyImages © Westend, S. 9: GettyImages © Travel_Motion; S. 10: GettyImages © Altmodern, S. 13: GettyImages © Maciej Frolow, S. 14: GettyImages © Yuichiro Chino, S. 16: BSI, S. 19: GettyImages © Westend61, S. 20: GettyImages © Maskot, S. 23: GettyImages © KTSDESIGN/SCIENCE PHOTO LIBRARY, S. 28: GettyImages © skegbydave, S. 32: GettyImages © kupicoo, S.38: GettyImages © VioletaStoimenova, S. 42: GettyImages © VioletaStoimenova, S. 46: GettyImages © artpartner-images, S. 49: GettyImages © Jamie Grill, S. 53: GettyImages © domin_domin

Artikelnummer
BSI-MIBro20/34

www.bsi.bund.de