3D Secure!

3D Secure ist ein Sicherheitsstandard für Online-Händler:innen, der von Mastercard und Visa gemeinsam entwickelt wurde. Dadurch sollen nicht nur die Risiken durch Betrug im E-Commerce-Sektor minimiert werden, es lassen sich auch zusätzliche Umsätze generieren und die Kundenbindung über das Internet fördern. Das Verfahren ermöglicht es Karteninhaber:innen, sich während des Bezahlvorgangs mit einem persönlich vergebenen Passwort zu authentifizieren. Mit der Einführung des Sicherheitsstandards geht eine Haftungsumkehr ('Liability Shift') einher, womit ein von Kund:innen reklamierter E-Commerce-Umsatz nicht mehr den Händler:innen zurückgegeben werden kann, wenn diese die 3D Secure-Technologie unterstützen. Weitere Informationen erhalten Sie unter Mastercard Identity Check oder unter Verified by Visa.

Ablehnung

Negative Antwort auf eine Autorisierungsanfrage: Die Kartenausstellerbank (deren Repräsentant oder beauftragter Dienstleister) lehnt den angefragten Umsatz ab.

Abrechnung

Verfahrensweise zur Herbeiführung des gegenseitigen Zahlungsausgleiches der Issuer- und Acquirer-Banken untereinander für die pro Tag jeweils abgerechneten Kartenumsätze (einschl. Gebühren).

Abrechnungsdaten

Alle Transaktionsdaten, die erforderlich sind, um Kartenumsätze zwischen Acquirer- und Issuer-Banken ordnungsgemäß abzurechnen wie z.B. MCC (Merchant Category Code), Ländercode, Betrag, Uhrzeit.

Abschneiden von Daten

Bei der Transaktionsdurchführung erlangte Informationen werden nicht oder nur teilweise auf Belegen ausgedruckt. Beispiel: Mastercard schreibt vor, dass GAA-Quittungsbelege die Kartennummer nur in verkürzter Form enthalten dürfen. Auch viele Händler gehen dazu über, die Terminals so zu programmieren, dass die Kartennummer beim Quittungsbeleg nicht mehr vollständig ausgedruckt wird. Auf diese Weise kann verhindert werden, dass Betrüger durch weggeworfene Belege, z.B. aus dem Papierkorb, in den Besitz gültiger Kartendaten gelangen.

acceptance network

Die von der Händlerbank geschaffene Infrastruktur zur Gewährleistung der Akzeptanz von Zahlungskarten. Zur Infrastruktur gehören üblicherweise: Geldautomaten, POS-Terminals und Kommunikationsnetzwerke zur Steuerung (Routing) von Transaktionsdaten und –informationen.

Access Point

Dieser Begriff umfasst die gesamte Technik, die für den Netzzugang benötigt wird. Dazu gehören folgende Einzelkomponenten: Der Zugang zum Online-Routingservice, zu den

Autorisierungs-Dienstleistungen sowie zusätzliche Sicherheitsmodule für die PIN-Verschlüsselung und –Prüfung.

Account Number

Eine von der Karten ausgebenden Bank erteilte Kontonummer, um ein Kartenkonto für die Belastung mit Transaktionen zuzuordnen.

Acquirer

Händlerbank, über die das Vertragsunternehmen abrechnet.

Activity File

Die Karteneinsatzdatei enthält die Transaktionsdaten für ein bestimmtes Kartenkonto innerhalb eines bestimmten Zeitraumes. Bei 'im Auftrag einer Karten ausgebenden Bank' ausgeführten Dienstleistungen (on-behalf services) erfolgt vor jeder Autorisierung einer Transaktion ein Abgleich mit dieser Datei, um sicherzustellen, dass der von der Karten ausgebenden Bank vorgegebene Verfügungsrahmen nicht überschritten wird.

Affiliate Licensee

Mitgliedsinstitut mit Unterlizenz eines Hauptlizenzinhabers (z.B. Kartenorganisation). Unter lizenzrechtlicher Verantwortlichkeit des Hauptlizenzinhabers kann sich der Unterlizenznehmer als Issuer und/oder Acquirer betätigen.

AIS

Account Information Security. Zielsetzung von Visa AIS ist die Unterstützung von Händlerbanken, Händlern, Service Providern und anderen externen Dienstleistern beim sicheren Umgang mit sensiblen Karten- und Transaktionsdaten. Das Programm definiert Sicherheitsanforderungen für die Verarbeitung, Speicherung und Übertragung von vertraulichen Informationen. Damit sollen eventuelle Sicherheitslücken in den eigenen Systemen identifiziert und mögliche Folgeschäden abgewendet werden. AIS ist Teil des gemeinsamen Standards PCI.

Akzeptanz

Annahme von Zahlungskarten durch einen Vertragshändler (Institut – Geldautomat / Handel – POS)

Akzeptanznetz

Die von der Händlerbank geschaffene Infrastruktur zur Gewährleistung der Akzeptanz von Zahlungskarten. Zur Infrastruktur gehören üblicherweise: Geldautomaten, POS-Terminals und Kommunikationsnetzwerke zur Steuerung (Routing) von Transaktionsdaten und –informationen.

Akzeptanzstelle

Handels- und Dienstleistungsunternehmen, die mit einer Acquirer-Bank eine vertragliche Vereinbarung zur Akzeptanz von Zahlungskarten schließen. Ein solcher Akzeptanzvertrag

(Händlervertrag) regelt, unter welchen Bedingungen Zahlungksarten akzeptiert werden.

Anscheinsbeweis

Der Anscheinsbeweis (auch: Beweis des ersten Anscheins, Prima-Facie-Beweis) ist eine im Zivilprozess angewandte Methode der mittelbaren Beweisführung. Gestützt auf Erfahrungssätze lassen sich Schlüsse von bewiesenen auf zu beweisende Tatsachen ziehen. Der Sachverhalt muss einer Typik entsprechen, also nach der allgemeinen Lebenserfahrung auf eine bestimmte Ursache oder auf einen bestimmten Ablauf als maßgeblich für den Eintritt eines bestimmten Erfolges hinweisen.
Im Zahlungskartenrecht z.B. sind solche Erfahrungssätze, die auf ein bestimmtes typisches Fehlverhalten des Zahlungsdienstnutzers hinweisen, anerkannt und im Rahmen der §§ 675v-675w BGB anzuwenden. Danach spricht grundsätzlich der Anscheinsbeweis dafür, dass entweder der Zahlungsdienstnutzer eine streitige Transaktion mit Karte und PIN selbst autorisiert hat, oder dass der Zahlungsdienstnutzer gegen seine Sorgfaltspflichten beim Umgang mit Karte und PIN verstoßen hat und ein unbefugter Dritter nach der Entwendung oder dem sonstigen Abhandenkommen der Karte von der PIN nur wegen ihrer gemeinsamen Verwahrung mit der Karte (bzw. wegen sonstiger Sorgfaltspflichtverstöße) Kenntnis erlangen konnte.

API

= application programming interface: Eine Programmierschnittstelle, die von einem Softwaresystem zur Anbindung anderer Programme zur Verfügung gestellt wird.

APP Authorized Push Payment Fraud

Betrugsform, bei der Opfer dazu manipuliert werden, Echtzeitzahlungen an Betrüger:innen zu leisten, typischerweise durch Social Engineering Angriffe mit Identitätsdiebstahl.

Applikationskryptogramm

Ein Kryptogramm, welches bei der Echtheitsprüfung von abgelehnten Chiptransaktionen erstellt wird.

Approval

Eine Genehmigungsanfrage über einen Umsatz (Transaktion) wird von dem Händler weiter an die kartenausstellende Bank (Issuer) oder deren Dienstleiter geleitet. Die Genehmigung (Autorisierung) des Umsatzes erteilt der Acquirer und leitet diese bewilligte Transaktion wiederum an den Händler weiter.

Approved Contractor Scheme

Approved Contractor Scheme, ein industrieller Sicherheitsstandard zur Akkreditierung zugelassener Auftragnehmer:innen.

APT

APT-Gruppen (Advanced Persistent Threat) sind hochspezialisierte Hackergruppen, die komplexe und langfristige Cyberangriffe durchführen.

Assessment Fee

Eine Gebühr, die jede Mitgliedsbank an die Kartenorganisation für die Wahrnehmung gemeinschaftlicher Steuerungs-, Management- und Sicherheitsaufgaben zahlen muss.

Asymmetrisches Verschlüsselungsverfahren

Das asymmetrische Verschlüsselungsverfahren benötigt im Gegensatz zur symmetrischen Verschlüsselung zwei Schlüssel zum Ver- und Entschlüsseln. Beide Schlüssel sind unabhängig von einander und lassen sich nicht gegenseitig ermitteln. Siehe auch Privatschlüssel und Öffentlicher Schlüssel.

ATM

Automated Teller Machine / Geldausgabeautomat (GA/GAA)

ATS

Automated Teller System (Multfunktionsgeldautomat)

ATS

Automated Teller System: Multifunktionsgerät u.a. zur Geldausgabe und Einzahlung

Aufforderung zur Kontaktaufnahme

Nach Autorisierungsanfrage durch den Händler erhält er die Autorisierungsantwort, dass er zwecks Genehmigung mit dem Karten ausgebenden Institut oder dessen Prozessor Kontakt aufnehmen soll. Dient lediglich zur zusätzlichen Identifikation des rechtmäßigen Karteninhabers bei ungewöhnlichem Umsatzverhalten und nicht zur Bonitätsüberwachung.

Austausch von Abrechnungsdaten (Clearing)

Clearing beschreibt die Abwicklung der Zahlung (Belastung und Gutschrift des Zahlungsbetrages) zwischen der Händlerbank und dem Karten ausgebenden Institut

Authentifizierung

Legitimation des Kunden bei der Bezahlung durch seine Unterschrift, PIN-Eingabe oder andere biometrische Merkmale.

Authorisation Code

Die Genehmigungsnummer wird infolge einer Autorisierungsanfrage von der Karten ausgebenden Bank (Issuer) vergeben und wiederum von dem Acquirer an den Händler bestätigt. Ohne diese Genehmigungsnummer hat der Händler für die Transaktion keine Zahlungsgarantie.

Authorisation Limits

Das Karten ausgebende Institut setzt Parameter für die Nutzungsmöglichkeiten und das Limit der Karte fest. Jede Autorisierungsanfrage wird nach diesen Parametern geprüft und es wird ein entsprechender Antwortcode gesendet (-> Genehmigung -> Ablehnung -> Call Referral -> Karte einziehen).

Autorisierte Zertifizierungsinstanz

Zentrale Instanz innerhalb eines kryptographischen Systems, beauftragt und ermächtigt, öffentliche Schlüssel für alle Systemteilnehmer zu signieren und die Ergebnisse in Form von 'public key certificates' an die jeweiligen Schlüsselinhaber zurückzusenden.

Autorisierung

Verfahren zur Genehmigung oder Ablehnung von Kartenumsatzanfragen. Die Umsatzanfrage wird durch das Händlerterminal oder den Geldautomaten an die Karten ausgebende Bank oder Sparkasse bzw. das beauftragte Rechenzentrum (Prozessor) gerichtet. Die Antwort kann eine Genehmigung, eine Umsatzablehnung, Aufforderung zum Karteneinzug oder zur Legitimationsprüfung bedeuten.

Autorisierungsparameter

Das Karten ausgebende Institut setzt Parameter für die Nutzungsmöglichkeiten und das Limit der Karte fest. Jede Autorisierungsanfrage wird nach diesen Parametern geprüft und es wird ein entsprechender Antwortcode gesendet (-> Genehmigung -> Ablehnung -> Call Referral -> Karte einziehen).

BaFin

Abkürzung für Bundesanstalt für Finanzdienstleistungsaufsicht. Die BaFin vereinigt seit Mai 2002 die Aufsicht über Banken, Finanzdienstleister, Versicherer und den Wertpapierhandel unter einem Dach.

Balance Inquiry

Kontostandsabfrage eines Karteninhabers am Geldautomat.

Bankidentifikationsnummer

Ist die eindeutige Identifikationsnummer eines Zahlungssystems, die einer Mitgliedsbank oder –sparkasse zugeteilt wird.

BankNet

Mastercard eigenes Kommunikationsnetz zur Abwicklung des gesamten 'interregionalen' und unterschriftsgestützten Mastercard-Transaktionsverkehrs. BankNet und EPS-Netz sind über einen Zugangsknoten miteinander verbunden. Dies ermöglichst außereuropäischen Acquirer-Banken den Datenaustausch mit europäischen Issuer-Banken und umgekehrt. Siehe hierzu auch Mastercard

Debit Switch (MDS).

Banknet-Telekommunikationsnetz

Weltweites Telekommunikationsnetz von Mastercard als primäre Datenüber-tragungseinrichtung, die alle Mastercard-Kunden und Mastercard-Datenverarbeitungszentralen in ein einziges Online-Finanzdienstleistungs-netzwerk einbindet.

Bargeldabhebung

Der Vorgang der Bargeldabhebung z.B. an einem Geldautomaten (GA). Wenn mehrere Funktionen am Geldautomaten angeboten werden, z.B. Aufladen des GeldKarte-Chips, ist eine Auswahl zu treffen. Im Ausland wird die Bargeldabhebung am Geldautomaten meist mit 'Cash Withdrawal' angezeigt.

Bargeldbeschaffung

Kartenverfügung zur Bargeldbeschaffung - entweder an einem Geldautomaten (ATM) oder in der Geschäftsstelle einer Mitgliedsbank oder einer dazu ermächtigten Agentur.

Behavioural Scoring

Beobachtung des Karteneinsatzes im Hinblick auf aus dem Rahmen fallenden Transaktionen. Verhaltens-Scoring ist eine Methode zur Betrugsbekämpfung. Es wird überprüft, inwieweit sich der gegenwärtige Karteneinsatz eines Karteninhabers bezogen auf die Transaktionen im Widerspruch zu seinem bisherigen Karteneinsatz befindet.

Beitragsgebühr

Eine Gebühr, die jede Mitgliedsbank an die Kartenorganisation für die Wahrnehmung gemeinschaftlicher Steuerungs-, Management- und Sicherheitsaufgaben zahlen muss.

Betrügerischer Kartenantrag

Bezeichnet die Handlungsweise einer Person, die in Ihrem Kartenantrag gegenüber der Karten ausgebenden Bank oder Sparkasse unwahre Angaben zur betrügerischen Erlangung einer Zahlungskarte macht.

Betrügerischer Karteneinsatz

Wenn der Karteninhaber weder eine Transaktion selbst tätigt, noch eine andere Person dazu berechtigt, seine Karte oder Kartennummer einzusetzen, handelt es sich beim Zustandekommen einer Transaktion um einen betrügerischen Karteneinsatz. In manche dieser Betrugsarten kann auch der Händler/ Vertragspartner als Mittäter verwickelt sein.

Betrügerischer Vertragshändler

Dieser Begriff bezeichnet einen Händler, der sich wissentlich und vorsätzlich an betrügerischen Aktivitäten beteiligt.

BIC

BIC (Bank Identifier Code) ist eine international standardisierte Bankleitzahl, mit dem weltweit jeder direkt oder indirekt teilnehmende Partner eindeutig identifiziert werden kann. Sie besteht aus einer 8-11stelligen Buchstaben- und Zahlenkombination, die Aufschluss über Institut, Land, Ort und gegebenenfalls Niederlassung gibt.

BIN

Ist die eindeutige Identifikationsnummer eines Zahlungssystems, die einer Mitgliedsbank oder Sparkasse zugeteilt wird.

BioLogin

Ein dynamisches Authentifizierungsverfahren mittels BioPIN, bei dem alle vom Benutzer getippten Daten, d.h. der Benutzername und im Fall einer Zweifaktorauthentifizierung auch das Passwort, tippbiometrisch ausgewertet werden.

Biometrics

Technische Verfahren, die aufgrund unverwechselbarer physischer Merkmale die eindeutige Identifikation ermöglichen. Hierzu zählen beispielsweise Fingerabdrücke, Gesichtsfeldabmessungen, IRIS-Erkennung (Auge).

Biometrie

Eine Wissenschaft, die biologische Daten und Merkmale (z.B. DNA, Fingerabdruck, Iris) misst und analysiert.

Biometrische Identifizierungsverfahren

Technische Verfahren, die aufgrund unverwechselbarer physischer Merkmale die eindeutige Identifikation ermöglichen. Hierzu zählen beispielsweise Fingerabdrücke, Gesichtsfeldabmessungen, IRIS-Erkennung (Auge).

BioPIN

Vom Authentifizierungsserver erzeugte One-time-PIN, die dem Benutzer präsentiert wird und der sie in Worten einzutippen hat. Dabei wird das Tippverhalten als biometrisches Merkmal aufgezeichnet. Auf diese Weise wird die BioPIN an die eintippende Person biometrisch gebunden. Die BioPIN dient als dynamischer biometrischer Authentifizierungsfaktor im Gegensatz zum statischen Authentifizierungsfaktor Passwort und ist deshalb immun gegen Replay-Attacken.

BioTAN

Dem Wesen nach eine BioPIN, die aber nicht zufällig erzeugt, sondern aus den Daten einer vorliegenden Online-Transaktion abgeleitet wird. Damit ist die BioTAN sowohl an die Transaktion als auch an die eintippende Person gebunden.

Bitcoin

Bitcoin ist die weltweit führende Kryptowährung auf Basis eines dezentral organisierten Buchungssystems. Zahlungen werden kryptographisch legitimiert und über ein Netz gleichwertiger Rechner abgewickelt. Anders als im klassischen Banksystem üblich, ist kein zentrales Clearing der Geldbewegungen notwendig.

Black Box

Bei Black Box Angriffen verbinden Kriminelle ein nicht autorisiertes Gerät direkt mit dem Geldautomaten und veranlassen diesen, das Bargeld auszugeben. Die Black Box muss dabei über USB- oder Hardware-Schnittstellen verfügen, die sie mit dem Zielgerät verbinden.

Blankokarten

Es handelt sich um weiße Plastikkarten, die nur mit einem Magnetstreifen versehen sind. Täter bringen auf diese Blankokarten häufig die Daten von Echtkarten auf (-> Skimming = Auslesen eines Magnetstreifens einer Echtkarte) und setzen diese Karten betrügerisch ein.

Block

Von Sperrung spricht man, wenn eine Karten ausgebende Bank entscheidet, entweder bestimmte Funktionalitäten auf dem Chip oder die Nutzung der Karte an sich zu unterbinden.

Blockchain

Blockchain, dt.: Datenblockkette, bezeichnet eine innovative Technologie, die speziell für die Zahlungsabwicklung von Transaktionen mit der virtuellen Währung Bitcoin entwickelt wurde.

Botnet

Eine Gruppe illegaler, automatisierter Computerprogramme.

Branche

Unterteilung der Unternehmen in Abhängigkeit Ihrer geschäftlichen Tätigkeit bzw. Ihres Produkt- oder Dienstleistungsangebotes.

Brand

Der Markenname eines bestimmten Kartenprodukts, das innerhalb eines festgelegten Territoriums zum Einsatz als Zahlungsmedium zugelassen ist.

Brand Mark

Kombination von Namen, Symbolen und Farben als eigentumsrechtlich geschütztes Markenzeichen zur visuellen Verkörperung der Markenidentität.

BSI

Bundesamt für Sicherheit in der Informationstechnik

Business Card

Ein Kartentyp für Unternehmen, i.d.R. unter zehn Mitarbeitern, zur Bezahlung geschäftlicher Aufwendungen. Auf der Karte kann sowohl der Name des nutzungsberechtigten Karteninhabers als auch der Firmenname erscheinen. Der monatliche Zahlungsausgleich erfolgt, je nach betriebsinterner Vereinbarung, über das Geschäftskonto oder zu Lasten des Mitarbeiter-Privatkontos.

Business-to-Business Commerce

Mit der Abkürzung B2B (B-to-B, Kurzform für: business to business) werden Geschäftsbeziehungen zwischen Unternehmen bezeichnet.

Call Referral

Bei dieser Beantwortung einer Genehmigungsanfrage fordert der Issuer den Acquirer auf, zusätzliche Informationen an ihn (oder seinen Dienstleister) zu übermitteln. Erst danach wird seitens des Issuers entschieden, ob dieser Umsatz genehmigt oder abgelehnt wird.

Card Authentication Method

Verfahren zur Prüfung der Echtheit einer Karte. Bei Kreditkarten mit Magnetstreifen schließt dies auch das Vorhandensein eines Hologramms ein, das vom Händler durch Augenschein überprüft wird. Die Echtheitsprüfung der verschlüsselten Daten im Magnetstreifen erfolgt durch den Issuer. Im Falle von Chipkarten mit verschlüsselten Daten im Chip erfolgt die Echtheitsprüfung durch das Chipterminal oder ebenfalls beim Issuer.

Card Issuer

Eine Bank, die Zahlungskarten ausgibt, Transaktionen ihrer Karteninhaber von anderen Mitgliedsbanken bzw. Händlern entgegennimmt, Zahlungen mit der Karte garantiert und die entsprechenden mit der Karte getätigten Umsätze vom Konto des Karteninhabers einzieht.

card payment scheme

card payment scheme ist der englische Begriff für Kartenzahlungssystem. Ein Kartenzahlungssystem ist ein Zahlungsnetzwerk, das Kredit- und Debitkarten zur Abwicklung von Zahlungen verwendet. Seine Hauptaufgabe besteht in der Verwaltung des Zahlungsverkehrs, einschließlich Operation und Verrechnungen. Transaktionen werden gemäß einer Reihe von Verfahren, Regeln und Vereinbarungen verwaltet, die es Karteninhabern ermöglichen, ihre Karten mit Dritten (z. B. Einzelhändlern und Dienstleistern) zu verwenden. Kartenzahlungssysteme sind beispielsweise girocard, Visa, Mastercard.

Card Personalisation

Herstellung (Druck), Prägung und Kodierung der Karten sowie deren Ausstattung mit allen Merkmalen und Servicefunktionen, die eine Issuer-Bank ihren Karteninhabern zur Verfügung stellen möchte.

Card Reader Internal Skimming Geräte

Dieser Gerätetyp Typ Skimmer wird an verschiedenen Stellen im Inneren des motorisierten Kartenlesers platziert.

card risk management

Bezogen auf die Chipkarten bezeichnet dieser Begriff eine Reihe von Prüfungsmöglichkeiten und Abwicklungsoptionen, die mit einem Chip zur Verfügung stehen, um Betrugsschäden zu reduzieren. Beispielsweise könnte eine Chipkarte so programmiert sein, dass jede 'x'-te Transaktion online autorisiert werden muss. Auch ein Online-Limit – ein Betrag, ab dem eine Onlineautorisierung von der Karte verlangt wird, kann eingestellt werden.

Card Scheme

Kartenorganisation/en

Card Trapping

Bezeichnet eine Form des Trickdiebstahls, bei der Geldautomaten so manipuliert werden, dass die Zahlungskarten nach dem Einführen in den Karteneinzugsschlitz nicht mehr herausgegeben werden. Die Kunden gehen dann irrtümlich davon aus, dass ihre Karte einbehalten wurde. Tatsächlich aber steckt sie noch im manipulierten Karteneinzugsschlitz und wird von den Trickbetrügern entnommen, sobald sich die Geschädigten von den Automaten entfernt haben.

Card-Not-Present-Environment

Eine Umgebung, bei der Transaktionen unter den folgenden Bedingungen getätigt werden: Der Karteninhaber ist nicht in einem physischen Geschäft präsent und/oder die Karte liegt physisch nicht vor. Hierzu zählen Transaktionen in den Bereichen: electronic commerce, schriftliche oder telefonische Bestellungen (Versandhandel), Abbuchungsaufträge und telefonische Dienstleistungen.

Card-not-present-Fraud

Eine „Card-not-present-Environment“/ „Karte-nicht-präsent-Umgebung“ bezieht sich auf Transaktionen, bei denen die Karte nicht physisch vorliegt. Das heißt, bei Käufen im Internet (e-commerce), am Telefon bzw. im Versandhandel (Mail-Order/ Telephone-Order) oder bei Bestellungen per Post oder Fax. Dabei kann es auch zu Betrug kommen, dieser nennt sich dann „CNP-Fraud“. Kartenausgeber, Acquirer, Händlerbanken und teilw. Händler selbst nutzen diverse Systeme zur Vermeidung von Schäden, wie z. B. 3D-Secure.

Cardholder

Eine Person, für die eine Karte rechtmäßig ausgestellt wurde. Die Zuordnung des Kartenkontos erfolgt über die Kartennummer des Inhabers.

Cardholder activated terminal

Terminal-Automat zur Selbstbedienung, stellt bestimmte Produkte oder Dienstleistungen zur

Verfügung und ist meist in Bahnhöfen, an Flughäfen, Tankstellen, Mautstellen, in Parkhäusern sowie anderen Servicebereichen anzutreffen.

Cardholder verification method

Verfahren zur Feststellung der persönlichen Legitimation eines Karteninhabers. Hierzu zählen z.B. Unterschriftsvergleiche und PIN-Prüfung; künftig können auch biometrische Prüfungsverfahren zur Anwendung kommen.

Cash Disbursement

Kartenverfügung zur Bargeldbeschaffung - entweder an einem Geldautomaten (ATM) oder in der Geschäftsstelle einer Mitgliedsbank oder einer dazu ermächtigten Agentur.

Cash Trapping

Cash Trapping (wörtlich übersetzt Geldfalle) bezeichnet die Manipulation des Geldautomaten, bei dem am Ausgabeschacht eine täuschend echt aussehende zusätzliche Abdeckleiste so angebracht wird, dass die Ausgabe der Geldscheine verhindert wird. Bei den Kunden, die vergebens auf ihr Geld warten, entsteht der Eindruck, dass die Geldausgabe gestört ist. Sobald sich die Kunden vom Geldautomaten entfernt haben, entnehmen die Täter die Blende mit dem daran haftenden Bargeld.

Cash Withdrawal

Der Vorgang der Bargeldabhebung z.B. an einem Geldautomaten (GA). Wenn mehrere Funktionen am Geldautomaten angeboten werden, z.B. Aufladen des GeldKarte-Chips, ist eine Auswahl zu treffen. Im Ausland wird die Bargeldabhebung am Geldautomaten meist mit 'Cash Withdrawal' angezeigt.

CDA

Die Abkürzung CDA steht für „Combined Data Authentification“, ein Sicherheitsverfahren für neue Kartengenerationen mit Chips, das besser vor Missbrauch schützen soll. Bei CDA wird eine Kombination dynamischer Karten- und Terminaldaten mit einem eigenen, nicht auslesbaren RSA-Key zur Echtheitssprüfung signiert. Die Daten lassen sich nicht kopieren, und die PIN geht auch nur verschlüsselt über die Leitung. Die Deutsche Kreditwirtschaft schreibt für Debitkarten den Einsatz von DDA oder CDA zwingend vor.

Central Acquiring

Ein zentraler Acquirer verarbeitet Transaktionen von einem international tätigen Unternehmen (Airline, Hotel, Autovermietung, etc.).

Central Acquisition

Grenzüberschreitendes Vertragsunternehmensgeschäft mit zentraler Abrechnung.

Central Bank Digital Currency

Digitale Zentralbank Währung

Central Issuing

Ein internationales Unternehmen, dessen Mitarbeiter in unterschiedlichen Ländern tätig sind, gibt Karten von einer zentralen Bank heraus.

CEO-Fraud

Bei der in Deutschland noch relativ neuen Betrugsmasche gibt sich der Betrüger als Geschäftsführer oder Vorstandsmitglied des Unternehmens aus und bittet einen für die Bankgeschäfte verantwortlichen Mitarbeiter zumeist per gefälschter E-Mail-Adresse, einen hohen Geldbetrag dringend ins Ausland zu überweisen.

Certification

Dieser Vorgang dient zur Datenverschlüsselung auf der Basis so genannter öffentlicher Verschlüsselungsverfahren. Hierbei handelt es sich um die digitale Zuordnung eines 'öffentlichen Schlüssels'. Der Eigentümer übergibt diesen einer hierzu ermächtigten Zertifizierungsstelle zur digitalen Signierung. Das Resultat wird dem Eigentümer in Form eines 'public key certificate' wieder zurückgesandt

Certification Authority

Zentrale Instanz innerhalb eines kryptographischen Systems, beauftragt und ermächtigt, öffentliche Schlüssel für alle Systemteilnehmer zu signieren und die Ergebnisse in Form von 'public key certificates' an die jeweiligen Schlüsselinhaber zurückzusenden.

Charge Card

Zahlungskarte oder Kreditkarte für ein Kartenkonto, auf dem die laufenden Verfügungen/Transaktionen über einen bestimmten Zeitraum und dann per Stichtag bzw. meist monatlich gesammelt in Rechnung gestellt werden. Der Karteninhaber gleicht dann den Gesamtsaldo für den jeweiligen Abrechnungszeitraum voll aus.

Chargeback

Rückbelastung eines Kartenumsatzes an den Acquirer durch die Issuer Bank. Das Verfahren wird angewandt, wenn ein bereits abgerechneter Umsatz vom Karteninhaber aus Gründen reklamiert oder bestritten wird, für die ein Rückbelastungsrecht vorgesehen ist. Der Begriff 'chargeback' bezeichnet auch den die Rückbelastung bewirkenden elektronischen Datenaustausch zwischen Issuer-Bank und Acquirer-Bank.

Chargeback Zeitraum

Anzahl der Kalendertage, gerechnet vom Ausstellungsdatum des Transaktionsbeleges (oder dem Tag der Verarbeitung der Transaktion, je nach Anwendbarkeit), während dieser ein Issuer vom Rückbelastungsrecht Gebrauch machen kann.

Chatbot

Die smarten Programme fungieren oftmals als Online-Assistenten und werden auf Websiten oder in Apps zur Kommunikation mit Kunden eingesetzt. Sie können automatisch auf Chat-Fragen reagieren und stehen rund um die Uhr auch für sonstige Kundenanliegen zur Verfügung. Sie erkennen die Themen anhand von Stichwörtern und generieren automatisierte Antworten.

Chip Card Terminal

POS-Terminal, das Chipkarten lesen kann.

Chip-TAN-Verfahren

Das Chip-TAN-Verfahren (oft auch als SmartTAN-Verfahren bezeichnet) funktioniert nur mit einem separaten TAN-Generator. Der Kunde steckt seine mit einem Chip ausgestattete PIN-geschützte Zahlungskarte in den TAN-Generator, um die jeweilige Transaktion zu autorisieren.

Chipkarte

Karte mit integriertem Mikroprozessor (Chip) zur Durchführung von Chip- sowie auch Magnetstreifentransaktionen. Chipkarten verfügen über einen Datenspeicher und logische Rechnerkapazität. Neben der Nutzung im Zahlungsverkehr können Chipkarten noch zusätzliche Servicefunktionen übernehmen. Für Chipkarten werden häufig auch die Bezeichnungen 'smart card', 'integrated circuit card', 'ICC' und 'IC Card' verwendet.

Chipkartentransaktion

Transaktion mit Chipkarte an einem Terminal mit Chipkartenleser. Die Daten werden im Chip vom Terminal elektronisch gelesen und bei der Genehmigungsanfrage verschlüsselt mitgesandt.

Cirrus

Cirrus ist Name und Markenzeichen eines internationalen ATM-Systems (Verbund von Geldautomaten), das Mastercard International gehört und von Cirrus System Incorporated (Mastercard-Tochtergesellschaft) betrieben wird. Mastercard-Karten und bankeigene Karten nationaler Debit- und Kredit-Systeme nehmen am Cirrus-Programm teil. Karteninhaber der teilnehmenden Banken haben Zugang zu dem als Cirrus ATM Network bekannten internationalen Geldautomatennetz.

Clearing

Clearing beschreibt die Abwicklung der Zahlung (Belastung und Gutschrift des Zahlungsbetrages) zwischen der Händlerbank und dem Karten ausgebenden Institut

Clearing Data

Alle Transaktionsdaten, die erforderlich sind, um Kartenumsätze zwischen Acquirer und Issuer-Banken ordnungsgemäß abzurechnen wie z.B. MCC (Merchant Category Code), Ländercode, Betrag, Uhrzeit.

Clearnet

Das Clearnet ist im Gegensatz zum Darknet quasi das gewöhnliche Internet, das über ganz normale Browser erreichbar ist. Diese Seiten können mit normalen Suchmaschinen gefunden werden.

Cloud

Virtueller Speicherplatz

Cloud Biometric

Sensor-loses und damit Cloud-fähiges biometrisches Verfahren.

Co-Brand

Co-branded Karte = Zahlungskarte, ausgestellt von einer Mitgliedsbank in Partnerschaft mit einem anderen Unternehmen, wobei die Firmenlogos beider Organisationen auf der Karte erscheinen. Zielgruppe ist der Kundenstamm des jeweils an dem Programm beteiligten Partners aus Handel, Dienstleistungssektor oder anderen Geschäftszweigen.

Code Tampering

Eine Software-Attacke, die eine mobile App verändert. Die Änderung wird entweder vor der Ausführung der App, d.h. am kompilierten Code, oder zur Laufzeit, d.h. während der Ausführung vorgenommen. Dabei versuchen die Angreifer zum Beispiel, die Banking App auf einem Smartphone zu manipulieren, um in deren Programmierung eigene Befehle einzuschleusen. Reverse Engineering und Tampering werden häufig als Synonyme gebraucht, streng genommen bezeichnet Tampering aber im Gegensatz zum Analyseprozess den Prozess der Veränderung einer App; entweder der kompilierten, ausführbaren App (Datei) oder der App während der Ausführung/zur Laufzeit (!).

Collusion

Mittäterschaft (durch betrügerisches Einverständnis). Dieser Begriff bezeichnet die wissentliche und vorsätzliche Beteiligung an betrügerischen Aktivitäten.

Collusive Merchant

Dieser Begriff bezeichnet einen Händler, der sich wissentlich und vorsätzlich an betrügerischen Aktivitäten beteiligt.

Commission Rate

Prozentualer Anteil des Umsatzes, den eine Akzeptanzstelle an ihren Acquirer zahlt.

Common Purchase Point

Eine Akzeptanzstelle, bei der der Verdacht besteht, dass Karteninhaberdaten ohne Kenntnis des Karteninhabers unrechtmäßig verwendet wurden, z.B. durch Kopieren des

Magnetstreifen-Dateninhalts zur Erstellung von Kartendubletten ('White Plastic'). Im Debit-Bereich wird hierfür die Bezeichnung 'point of compromise' oder 'POC' verwendet.

Compliance Case

Wenn die Reklamation nicht auf herkömmlichem Wege (Chargeback Regulations) abgewickelt werden kann, besteht die Möglichkeit, den Sachverhalt unter Vorlage aller Beweismittel in einem Schlichtungsverfahren klären zu lassen.

Consumer Device Cardholder Verification Message

Consumer Device Cardholder Verification Message, die Verifizierung des Karteninhabers oder der Karteninhaberin über das Endgerät des Kunden oder der Kundin. Dazu gehören biometrische Verifizierungen, die Eingabe einer PIN oder eines Musters am Smartphone.

Conversion Date

Das Datum, zu dem ein Betrag (Kartenumsatz) von einer Währung in eine andere umgerechnet wird, und zwar unter Verwendung des für Transaktionen dieser Art zutreffenden und an diesem Tag gültigen Umrechnungskurses.

Conversion Rate

Der Kurs, zu dem Beträge von einer Währung in eine andere umgerechnet werden.

Corporate Card

Kartenprodukt von Mastercard oder Visa, das für große Unternehmen und deren Mitarbeiter zur Bezahlung geschäftsbezogener Ausgaben bestimmt ist. Auf der Karte erscheint sowohl der Firmenname als auch der Name des berechtigten Karteninhabers. Firmenkarten dienen in der Regel der Bezahlung von Reise- und Bewirtungsausgaben, die üblicherweise über ein zentrales Firmenkonto abgerechnet werden, wobei die Ausstellerbank noch Zusatzinformationen mitliefert (z.B. separate Aufführung der Mehrwertsteuer), die dem Unternehmen eine zentrale Überwachung und Kontrolle derartiger Geschäftskosten erleichtert.

Counterfeit Card

Eine zu Betrugszwecken hergestellte Kartenfälschung, die durch Aufdruck oder Prägung in einer Weise personalisiert ist und/oder Systemkennzeichen trägt, die den Eindruck erwecken, es handele sich um eine echte, von dem betreffenden Issuer tatsächlich ausgestellte Karte. Der Begriff counterfeit card wird auch für Karten benutzt, die zwar rechtmäßig ausgestellt, jedoch später durch Umprägung und Umkodierung etc. verfälscht wurden.

Country Code

Kennziffer zur Identifizierung eines bestimmten Landes. Die Ziffern gehören zu einem Block international anerkannter numerisch und alphabetisch aufgebauter Codenummern, die häufig in elektronischen Nachrichten zur Länderkennzeichnung benutzt werden.

Credit Limit

Die Ausstellerbank räumt dem Inhaber einer Kreditkarte oder Charge Card pro Abrechnungszyklus einen maximalen Verfügungsrahmen ein. Die Höhe des Rahmenbetrages bestimmt die Bank und sie richtet sich individuell nach der Bonität und der Kontohistorie des Karteninhabers.

Credit Scoring

Bei der Kreditwürdigkeitsprüfung legt die Issuer-Bank fest, ob der Kartenantrag bewilligt oder abgelehnt wird. Zu den Kriterien der Bonitätsprüfung gehören u.a. Alter, Beruf, durchschnittliches Monatseinkommen etc.

Cross Border Issuing

Karteninhaber und Karten ausgebende Bank befinden sich in unterschiedlichen Ländern.

Cross Border Transaction

Internationale Transaktion bzw. grenzüberschreitende Transaktion, indem sich der Acquirer und die Bank (Issuer) in verschiedenen Ländern befinden.

Cross-Border Debit Processing

Das Processing von Umsätzen, die mit deutschen Debitkarten im Ausland bzw. mit Karten ausländischer Banken in Deutschland getätigt werden.

Crowdfunding

Crowdfunding setzt sich zusammen aus den beiden englischen Wörtern crowd (Menschenmenge) und funding (Finanzierung) und wird im Deutschen meist mit Schwarmfinanzierung übersetzt. Bei dieser Art der Geldbeschaffung unterstützen sowohl private Geldgeber als auch Organisationen oder Unternehmen Projekte / Geschäftsideen in der Regel mit Eigenkapital. Dabei ist Crowdfunding nicht nur für die Menschen spannend, die auf diese Weise Ideen realisieren möchten, sondern auch für diejenigen, die dabei helfen. Die Finanzierung findet zumeist im Internet über eigens hierfür eingerichtete Crowdfunding-Plattformen statt.

CTI

Computer-Telephony-Integration (CTI) ist eine Technologie, die es Computern ermöglicht, mit Telefonen zu interagieren. Diese Technologie wird in erster Linie in Callcentern eingesetzt und wird oft zur Beschreibung von Desktop-Interaktionen verwendet, die die Produktivität menschlicher Agenten verbessern.

Currency Conversion

Umrechnung der Transaktionswährung in die Abrechnungswährung der Kartenausstellerbank. Dies erleichtert den Datenaustausch im Autorisierungs-, Clearing- und Settlement- Verfahren. Im EPS-Netz und BankNet (Mastercard) oder VisaNet (Visa) ist die automatische

Währungsumrechnung integraler Bestandteil beim Austausch von Autorisierungs-, Clearing- und Settlement-Daten.

Cutlet Maker

Bei dieser Angriffsart wird der Geldautomat mittels USB-Stick mit Malware infiziert und zum Auszahlen veranlasst.

CVC2

Card Verification Code (Mastercard)- Kartenverifizierungscode dient zur Sicherheit bei Mailorder- und Internet-Transaktionen. Der Karteninhaber wird von dem Händler aufgefordert, neben der Kartennummer und des Gültigkeitsdatums auch noch die Kartenprüfnummer mitzuteilen. Die Kartenprüfnummer befindet sich auf dem Unterschriftsstreifen der Kartenrückseite. Diese weitere Sicherheitsabfrage ist nötig, um sicherzustellen, dass die Daten der Kartenvorderseite allein nicht für betrügerische Zwecke über Internet oder Mailorder missbraucht werden können.

CVM

Card Verification Method. Verfahren zur Feststellung der persönlichen Legitimation eines Karteninhabers. Hierzu zählen z.B. Unterschriftsvergleiche und PIN-Prüfung; künftig können auch biometrische Prüfungsverfahren zur Anwendung kommen.

CVV2

Card Verification Value (Visa International) - Kartenverifizierungscode dient zur Sicherheit bei Mailorder- und Internet-Transaktionen. Der Karteninhaber wird von dem Händler aufgefordert, neben der Kartennummer und des Gültigkeitsdatums auch noch die Kartenprüfnummer mitzuteilen. Die Kartenprüfnummer befindet sich auf dem Unterschriftsstreifen der Kartenrückseite. Diese weitere Sicherheitsabfrage ist nötig, um sicherzustellen, dass die Daten der Kartenvorderseite nicht für betrügerische Zwecke über Internet oder Mailorder missbraucht werden.

Cybercrime

Cybercrime umfasst laut Bundeskriminalamt die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten oder mittels dieser Informationstechnik begangen werden.

Darknet

Darknets sind kriminelle Online-Marktplätze im verdeckten, anonymen Bereich des Internets (Underground Economy), in denen Waren illegal gehandelt werden.

Data Encryption Standard

Datenverschlüsselungsstandard, Algorithmus zur Datenverschlüsselung, wird überwiegend in der Kreditwirtschaft und Finanzdienstleistungsbranche zur Verschlüsselung sensitiver Daten benutzt. DES ist ein symmetrisches Verschlüsselungsverfahren und unterstützt 128-, 192- und

256-Bit-Schlüssel. Angriffe, die bei den seinerzeit 56-Bit-Schlüsseln mit spezieller Hardware schon nach wenigen Stunden entschlüsselt werden konnten, werden lt. diverser Experten auf Jahre hinaus unmöglich sein.

DDoS

DDoS steht für Denial of Service und bedeutet in der Informationstechnik, dass Internetdienste nicht verfügbar sind, obwohl sie es eigentlich sein sollten. Dies hängt meist mit einer Überlastung des Datennetzes zusammen, die gezielt herbeigeführt wird.

Debit Card

Zahlungskarte verknüpft mit einem Bank(giro)konto. Jede Transaktion, die mit dieser Karte getätigt wird, führt zu einer sofortigen Kontobelastung.

Debitkarte

Zahlungskarte verknüpft mit einem Bank(giro)konto. Jede Transaktion, die mit dieser Karte getätigt wird, führt zu einer sofortigen Kontobelastung.

Decline

Negative Antwort auf eine Autorisierungsanfrage: Die Kartenausstellerbank bzw. deren Prozessor (z.B. First Data) lehnt den angefragten Umsatz ab.

Deepweb

Das Deepweb ist ein Bereich des normalen Internets, der mit normalen Suchmaschinen aber nicht auffindbar ist. Der Grund: derartige Seiten sind nicht verlinkt, sie sind von Suchmaschinen nicht gelistet, oder man braucht Zugangsdaten um sie aufrufen zu können.

DeviceTAN

Eine auf einem separaten Gerät, dem Device oder TAN-Generator, erzeugte, vom Überweisungstext abhängige TAN.

DFÜ

Datenfernübertragung

Die Deutsche Kreditwirtschaft

In Die Deutsche Kreditwirtschaft sind die fünf Spitzenverbände der deutschen Kreditwirtschaft (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V., Bundesverband deutscher Banken e. V., Bundesverband Öffentlicher Banken Deutschlands e. V., Deutscher Sparkassen- und Giroverband e. V. und Verband deutscher Hypothekenbanken e. V.) zusammengeschlossen. Die Deutsche Kreditwirtschaft versteht sich als Interessenvertretung der kreditwirtschaftlichen Spitzenverbände.

Dienstleistungsunternehmen

Ein Unternehmen, das für eine Mitgliedsbank (oder mehrere) vertraglich vereinbarte Dienstleistungen im Kartengeschäft erbringt (-> Prozessor). Dienstleistungen in der Kartenbranche können beispielsweise sein: Autorisierung, Genehmigungsdienst, Reklamationsbearbeitung, Prävention, Missbrauchsbearbeitung, Rechnungserstellung und Versand, Ersatzkartenservice, Transaktionsprozessing, Kartenversand.

Digitale girocard

Bei der digitalen Version der Zahlungskarte werden die Informationen, die sonst in einer Chipkarte abgelegt würden, in der Software Ihres Mobiltelefons hinterlegt. Dann können Sie mit Ihrem Smartphone überall dort bezahlen, wo Sie sonst auch mit der NFC-fähigen girocard als Chipkarte kontaktlos zahlen können. Dazu muss Ihr Smartphone NFC-fähig sein. Außerdem muss die digitale girocard von Ihrer Bank oder Sparkasse angeboten werden. Dann können Sie auf Ihrem Smartphone die entsprechende App Ihres Instituts installieren. Ob Ihre Hausbank die digitale Karte für Ihr Smartphone anbietet, entnehmen Sie am besten deren Webseite, Banking-App oder Sie fragen Ihren Berater.

Digitale Signatur

Die digitale (bzw. elektronische) Signatur ist die Übertragung der Unterschrift in elektronische Medien. Mit der Signatur kann der Signierende identifiziert und vor allem authentifiziert werden, das heißt, es kann ermittelt werden, ob der Signierende auch wirklich derjenige ist, der er zu sein vorgibt. Damit ermöglicht die digitale Signatur nicht nur eine sichere Kommunikation im Internet, sondern sie fungiert auch als Siegel zu elektronischen Daten.

Direct Debit

Zahlungsmethode, bei der der Umsatz direkt per Lastschrift vom Girokonto eingezogen wird.

Disagio

Prozentualer Anteil des Umsatzes, den eine Akzeptanzstelle an ihren Acquirer zahlt.

Disclosure

Allgemeine Geschäftsbedingungen einer Karten ausgebenden Bank für die Karteninhaber.

dolos

vorsätzlich/arglistig

Domestic Interchange Fee

Eine umsatzabhängige, prozentuale oder transaktionsabhängige, fixe Gebühr, die die Händlerbank an die Karten ausgebende Bank basierend auf den nationalen Interchange Gebührenregelungen zahlen muss.

Domestic Transaction

Eine Transaktion, die im Inland zwischen dem Händler und Karteninhaber getätigt wird.

Down Option Authorisation

Wenn die Karten ausgebende Bank bei einer Autorisierungsanfrage nicht erreichbar ist, wird von einem vorher definierten Rechenzentrum eine Ersatzautorisierung durchgeführt. Voraussetzung ist, dass die Karten ausgebende Bank diesem Prozedere vorher zugestimmt hat.

Dropper

In App-Stores werden Anwendungen unter der Maskerade legitimer Zwecke angeboten, die dann bei Installation ihre schädliche Zusatzlast auf dem Gerät abwerfen.

Dual Acquirer

Bank oder Sparkasse, die eine Lizenz für das Acquiring (Anbindung von Vertragshändlern) erworben hat und sowohl Akzeptanzstellen für Mastercard als auch für Visa anschließt.

Dual Issuer

Eine Karten ausgebende Bank oder Sparkasse, die sowohl Mastercard als auch Visa Karten ausgibt.

Duale Händlervertragsbank

Bank oder Sparkasse, die eine Lizenz für das Acquiring (Anbindung von Vertragshändlern) erworben hat und sowohl Akzeptanzstellen für Mastercard als auch für Visa anschließt.

Dualer Kartenherausgeber

Eine Karten ausgebende Bank oder Sparkasse, die sowohl Mastercard als auch Visa Karten ausgibt.

Dublette

Hierbei handelt es sich um den weißen Kartenrohling. Auf dem Magnetstreifen können bei einer Kartendublette die ausgelesenen Kartendaten aufgebracht werden.

Dynamic Currency Code

Mit der dynamischen Währungsumrechnung bezahlt der Karteninhaber in seiner Heimatwährung. Bei einer korrekt durchgeführten DCC Transaktion wird der Kaufpreis von der Währung des Händlers automatisch in eine sogenannte Transaktionswährung umgerechnet, die der Währung des Karteninhabers entspricht.

Dynamic Currency Conversion

Mit DCC (dynamische Währungsumrechnung) bezahlt der Karteninhaber in seiner Heimatwährung. Bei einer korrekt durchgeführten DCC Transaktion wird der Kaufpreis von der Währung des

Händlers automatisch in eine sogenannte Transaktionswährung umgerechnet, die der Währung des Karteninhabers entspricht.

Dynamic Data Authentication

Ein Sicherheitsverfahren für neue Kartengenerationen mit Chips, das besser vor Missbrauch schützen soll. Bei DDA wird eine Kombination fester Karten- und dynamischer Terminaldaten mit einem eigenen, nicht auslesbaren RSA-Key zur Echtheitsprüfung signiert. Die Daten lassen sich nicht kopieren, und die PIN geht auch nur verschlüsselt über die Leitung. Die Deutsche Kreditwirtschaft schreibt für Debitkarten den Einsatz von DDA oder CDA (Combined Data Authentification) zwingend vor.

EAPS

Die Euro Alliance of Payments Schemes (EAPS) ist ein Verbund verschiedener nationaler Kartenzahlungssysteme, die die gegenseitige Akzeptanz der Debitkarten in den jeweiligen europäischen Ländern ermöglicht. Damit können Inhaber einer deutschen girocard im Rahmen dieses Systems in einigen Ländern Europas Bargeld beziehen und an den Kassen bezahlen. Händler wiederum, die das electronic cash-System nutzen, erweitern durch die EAPS die Zahl der ausländischen Debitkarten, die sie ohne die Nutzung eines der internationalen Bezahlsysteme von Visa oder Mastercard akzeptieren können, und zwar zu den gleichen Konditionen und Bedingungen wie bei electronic cash.

EAST

EAST steht für European Association for Secure Transactions und wurde Anfang 2004 als freiwilliger Verbund zur Bekämpfung der Kartenkriminalität in Europa gegründet. Die Mitglieder setzen sich aus Vertretern der Kreditwirtschaft (z.B. EURO Kartensysteme), Geldautomatenherstellern und Netzbetreibern zusammen. Die Teilnehmer kommen aus den meisten Ländern Europas und – da Skimming mittlerweile auch international eine große Rolle spielt - aus einigen Ländern außerhalb Europas. EAST wird von Europol, dem Europäischen Polizeiamt in Den Haag, unterstützt.

EBA

European Banking Authority / Europäische Bankenaufsichtsbehörde

EBICS

Electronic Banking Internet Communication Standard. Bezeichnet einen in Deutschland multibankfähigen Standard für die Übertragung von Zahlungsverkehrsdaten über das Internet.

Echtheitsprüfung

Sicherheitsverfahren, durch dessen Anwendung der Empfänger prüft, ob eine von ihm empfangene Nachricht nicht nur echt und vollständig ist, sondern tatsächlich auch von der in der Nachricht angegebenen Quelle stammt. Bei Chipkarten werden digitalisierte Unterschriften verwendet, wobei

zwei miteinander kommunizierende Stellen (z.B. Chipkarte und Chipterminal oder Chipkarte und Issuer-Host-Rechner der Ausstellerbank) in der Lage sind, eine gegenseitige Echtheitsprüfung durchzuführen.

Echtzeitüberweisung

(Instant Payment)... ist eine Online-Überweisung oder ein Geldtransfer zwischen Transaktionspartnern in wenigen Sekunden bzw. Minuten. Verbuchung und Valutierung der Geldbeträge erfolgen in Echtzeit.

ECRB

Das Euro Cyber Resilience Board für paneuropäische Finanzinfrastrukturen ist ein Forum für strategische Diskussionen zwischen Finanzmarktinfrastrukturen. Seine Ziele sind, das Bewusstsein für das Thema Cyberresilienz zu erhöhen – gemeinsame Initiativen zur Entwicklung wirksamer Lösungen für den Markt zu katalysieren – und einen Ort für den Austausch bewährter Praktiken zu bieten sowie Vertrauen und Zusammenarbeit zu fördern. Die Entscheidung zu Gründung des ECRB fiel während eines EZB Treffens zur Cyberresilienz im Juni 2017.

Edit Package

Eine von Visa entwickelte und den Prozessoren zur Verfügung gestellte Software, um Abrechnungsdaten des BASE II Systems (Clearing und Settlement) zu prüfen und zu verarbeiten.

Eingangstor-Netzwerk

Begriff zur Bezeichnung der zwischen zwei Netzwerken bestehenden Verbindungsknoten zur Ermöglichung globaler Netzwerkkommunikation.

Einreichung von Transaktionsdaten

Elektronische Clearing-Nachricht mit allen Umsatzdaten, die der Issuer-Bank zur Durchführung des Zahlungsausgleichs von der Acquirer-Bank zugeleitet wird.

Einreichungsgebühr

Gebühr, die von derjenigen Partei zu zahlen ist, die einen Chargeback- oder Compliance-Fall zu Schlichtungszwecken bei Mastercard einreicht. Nach abschließender Fallentscheidung durch Mastercard kann diese Gebühr auch von der gegnerischen Partei, die das Schlichtungsverfahren verloren hat, eingefordert werden.

EKS-Net

EKS-Net ist das online-gestützte System zur Erfassung, Verwaltung, Auswertung und Prävention von Schadensfällen mit Debitkarten, wie verlorene oder gestohlene Karten, Dubletten (Counterfeit) und Postwegverluste.

electronic cash

Allgemein bezeichnet dieser Terminus den Kauf und Verkauf von Waren oder Dienstleistungen unter Benutzung elektronischer Bezahlung. In Deutschland steht electronic cash für das nationale PIN-basierte Debit Zahlungsverfahren.

Electronic Commerce

Geschäftliche Transaktionen, die von den Beteiligten über elektronische Medien (z.B. Internet) durchgeführt werden und Zahlungsleistungen in elektronischer Form einschließen.

Electronic Funds Transfer

Begriff zur Bezeichnung von Transaktionsabläufen, bei denen elektronisch aufgezeichnete Kartendaten von einem Vertragshändler an Stelle von Bargeld als Zahlungsmittel akzeptiert werden.

Elektronische Geldbörse

Funktionalität einer Chipkarte, die die Speicherung eines Guthabens im Chip erlaubt. Die gespeicherte Summe reduziert sich bei jedem Einkauf um den jeweiligen Transaktionsbetrag, ohne dass hierfür eine Online-Autorisierung notwendig ist.

Elektronischer Geldtransfer

Begriff zur Bezeichnung von Transaktionsabläufen, bei denen elektronisch aufgezeichnete Kartendaten von einem Vertragshändler an Stelle von Bargeld als Zahlungsmittel akzeptiert werden.

Elektronisches Warnmeldungsbulletin

Bezeichnung für eine von Mastercard unterhaltene 'Sperrdatei', die in Verbindung mit 'stand-in'-Dienstleistungen dem Zweck dient, als 'gesperrt' eingemeldete Karten zu erkennen und Missbrauchstransaktionen zu verhindern.

ELV

elektronisches Lastschriftverfahren

Embossing

Prägung der Plastikkarten mit den erforderlichen Daten.

Emittent (Issuer)

Mitgliedsbank, die Zahlungskarten an ihre Kunden ausgibt, die Kartenkonten ihrer Kunden verwaltet, Kartentransaktionen autorisiert (entweder selbst oder über beauftragte Dienstleister) und der Acquirer-Bank gegenüber den Zahlungsausgleich für gültige Kartenumsätze garantiert.

Emotet

Emotet ist eine Form von Malware und gehört zur Kategorie der Ransomware. Einmal auf dem System, eignet sich die Software Daten des Opfers an, um mit der Veröffentlichung dieser zu drohen und/oder die Daten zu verschlüsseln und Lösegeld für die Entschlüsselung zu verlangen.

Weiterhin liest Emotet die Kontaktinformationen aus den Postfächern infizierter Systeme zur eigenen Weiterverbreitung aus und ist in der Lage, eigenständig neue Schadsoftware nachzuladen.

EMV

Europay, Mastercard, Visa - Die drei Kartenorganisationen haben sich zwecks Erarbeitung und Förderung globaler Standards für elektronische Finanztransaktionen abgestimmt. Das Kürzel 'EMV' bezieht sich auch auf die von allen drei Gesellschaften übernommenen technischen Spezifikationen zur Gewährleistung globaler Kompatibilität und Interoperabilität für Chipkarten, Chipterminals und den entsprechenden Datenformaten in der Transaktion.

EMV-Chip

Der auf einer Zahlungskarte befindliche EMV-Chip ist zuständig für die Kommunikation zwischen Chipkarte und Terminal (POS und/oder Geldautomat). Er ermöglicht es, die im Chip gespeicherten Daten gegen Verfälschung, Ausspähen bzw. Kopieren zu schützen.

EMVCo

EMVCo ist ein Gemeinschaftsunternehmen von American Express, JCB, Mastercard, UnionPay and Visa. Das Unternehmen ist für die Aufrechterhaltung und Weiterentwicklung des EMV-Standards für chip-basierte Zahlungskarten und Akzeptanzterminals (POS und Geldautomaten) zuständig und dient als offizielle Quelle für Informationen zum EMV-Standard.

Encryption

Verfahrenstechnik zur Verschlüsselung von Daten mittels eines algorithmischen Rechenvorgangs und einem Schlüssel(wert).

Encryption Key

Schlüssel, der im Rahmen eines Datenverschlüsselungs-Verfahrens verwendet wird. Diese Sicherheitskomponente, oft in Form einer bestimmten Zahlen- und/oder Buchstabenfolge, dient dazu, Daten mittels eines algorithmischen Rechenvorgangs zu verschlüsseln, um die Vertraulichkeit von Informationen zu schützen.

End-to-End-ID

Im Zuge der SEPA-Umstellung ersetzt die End-to-End-ID die bisherige Referenznummer und gilt weiterhin für Transaktionen im grenzüberschreitenden Zahlungsverkehr.

EPS-Net

Eigenes Telekommunikationsnetz von Mastercard für den in 'Echtzeit' erfolgenden Austausch von Transaktionsdaten zwischen den Mitgliedsinstituten.

Ersatzautorisierungsservice

Ersatzautorisierung: Autorisierung einer Transaktion durch ein nachgeordnetes, zentrales

Autorisierungssystem, das für die Kommunikation mit dem Banknet Kommunikationsnetzwerk entwickelt wurde und Autorisierungen anstelle des Issuers und in seinem Namen durchführt. Stand-In springt ein, wenn der Issuer nicht online-fähig ist, vorübergehend nicht erreichbar ist, oder zu spät, d. h. außerhalb der Zeitlimits, die im Netzwerk definiert sind, antwortet.

Ersatzbeleg

Bezeichnung für ein Dokument in Papierform, das ein Acquirer als 'Ersatz' für einen Kartenumsatzbeleg zur Verfügung stellt. Derartige 'Ersatzbelege' dürfen nur für folgende Transaktionskategorien erstellt werden: Mail Order/Telephone Order, Hotel/Motel, Tankstellen, Parkhäuser, Autovermietungen und Luftfahrtgesellschaften.

Erweiterte Parameter für Kontonummernbereiche

Zusätzliche Parameter, die der Issuer-Bank eine noch strengere Risikoüberwachung ihrer Karten im Rahmen des Mastercard Dynamic Stand-in - Programmes gestatten. Für Transaktionen, die eine Reihe miteinander verknüpfter Kriterien erfüllen (z.B. Ursprungsland, MCC (Merchant Category Code – Branchenschlüssel) und Transaktionsbetrag), können auf diese Weise spezielle Limits festgelegt werden.

Eurojust

Eurojust ist eine Justizbehörde der Europäischen Union mit Sitz in Den Haag. Aufgabe ist die Koordination von grenzüberschreitenden Strafverfahren auf europäischer Ebene. Dazu gehören u.a. die Abstimmung der Arbeit von nationalen Justizbehörden und der Informationsaustausch in Europa, wenn es beispielsweise um grenzüberschreitenden organisierte Kriminalität geht.

Europay Common Clearing Format

Ein einheitliches Datenverrechnungsformat, das für alle Mitgliedsbanken verbindlich ist und zum Austausch von Clearing und Settlement Daten zwischen Acquirer und Issuer genutzt wird.

Europay Module

Ein aus Hardware und Software bestehendes Interface (Prozessor)-Modul von Europay/Mastercard, das bei den einzelnen Mitgliedsinstituten vor Ort installiert ist. Es verbindet die eigenen Zentralrechner der Mitglieder mit dem EPS-Net und ermöglicht so den Zugang zu den IT-Systemen und anderen Dienstleistungen von Mastercard.

Europay Security Module

Europay Sicherheitsmodul - ein besonders abgesichertes, von einem Mikroprozessor gesteuertes und mit einem EM (Europay Module) verbundenes Gerät mit Spezialspeicher für kryptographische Geheiminformationen (Schlüssel) und zur Durchführung spezieller Kryptographie-Operationen. Hierzu zählen die Errechnung von Schlüsselwerten zur PIN-Verifizierung und Echtheitsprüfung von Transaktionsnachrichten sowie die Verschlüsselung privater Daten vor deren Übermittlung.

European Payments Council

Zusammenschluss europäischer Banken, um Grundlagen für eine kostengünstige, vollautomatische und standardisierte Zahlungsverkehrs-Infrastruktur zu schaffen.

Evidenzzentrale

Abrechnungsstelle im System der GeldKarte. Nimmt die Umsätze der Händler entgegen, leitet den Zahlungsverkehr in die Wege, prüft die Sicherheit des Systems und verrechnet die entsprechenden Entgelte unter den Beteiligten. Jeder Banksektor hat eine eigene Evidenzzentrale. Man unterscheidet Händlerevidenzzentrale und Kartenevidenzzentrale.

EWR

Europäischer Wirtschaftsraum

Excessive Chargeback Compliance Programme

Ein von Mastercard entwickeltes Programm zur zahlenmäßigen Reduktion der Rückbelastungsfälle, insbesondere bei bestimmten Transaktionsarten (z.B. Electronic Commerce). Eine Acquirer-Bank, deren monatliche Rückbelastungsquote den branchenüblichen Durchschnitt und die zulässige Toleranzschwelle übersteigt, setzt sich dem Risiko der Auferlegung von Strafgebühren aus.

Expiration Date

Bezeichnet allgemein das auf einer Zahlungskarte aufgedruckte oder aufgeprägte sowie auch im Magnetstreifen und Chip gespeicherte Gültigkeitsdatum (Monat und Jahr). Ab diesem Datum verliert die Karte ihre Gültigkeit und darf vom Karteninhaber nicht mehr für Einkäufe oder Bargeldverfügungen eingesetzt werden. Dem Händler ist es ab diesem Datum untersagt, die abgelaufene Karte weiterhin zu akzeptieren.

expressPay

expressPay heißt die kontaktlose Zahlungstechnologie von American Express. Die Kreditkarte auf Basis der Near Field Communication-Technologie (NFC) zur Zahlung einfach kurz ans Zahlterminal halten. Für Kleinbeträge ohne PIN-Eingabe oder Unterschrift!

Extended Account Range Parameters

Zusätzliche Parameter, die der Issuer-Bank eine noch strengere Risikoüberwachung ihrer Karten im Rahmen des Mastercard Dynamic Stand-in - Programmes gestatten. Für Transaktionen, die eine Reihe miteinander verknüpfter Kriterien erfüllen (z.B. Ursprungsland, MCC (Merchant Category Code – Branchenschlüssel) und Transaktionsbetrag), können auf diese Weise spezielle Limits festgelegt werden.

Face-to-Face Transaction

Transaktion, bei der Karteninhaber und Händler persönlich anwesend sind und die Karte physisch vorliegt.

Faked Terminal

Eine Terminal Attrappe, die aussieht wie ein echtes POS Terminal und ausschließlich dem Zweck dient, Kartendaten und PINs zu Betrugszwecken zu erhalten.

Fallback

Umschaltung auf Magnetstreifentechnologie als Ersatzlösung bei Chip-Funktionsausfall.

Filing Fee

Gebühr, die von derjenigen Partei zu zahlen ist, die einen Chargeback- oder Compliance-Fall zu Schlichtungszwecken bei Mastercard einreicht. Nach abschließender Fallentscheidung durch Mastercard kann diese Gebühr auch von der gegnerischen Partei, die das Schlichtungsverfahren verloren hat, eingefordert werden.

Fintech

Als Fintechs (Abkürzung für Financial Technology) bezeichnet man Unternehmen, deren Hauptgeschäftsfeld innovative, zumeist digitalisierte Technologien im Bereich Finanzdienstleistungen sind.

Floor Limit

Genehmigungsgrenze für Vertragsunternehmen. Bei dieser Genehmigungsgrenze kann der Vertragshändler die Transaktion ohne vorherige Einholung einer Genehmigung (vom Issuer) akzeptieren. Übersteigt der Betrag diese Genehmigungsgrenze, ist der Vertragshändler verpflichtet, eine Genehmigungsanfrage durchzuführen. Bei grenzüberschreitenden Umsätzen werden die für internationale Kartenumsätze geltenden 'international floor limits' durch die Kartengesellschaften (Mastercard, Visa) pro Land veröffentlicht. Die Transaktionshöhe wird nach Händlerkategorien unterschiedlich festgelegt. Bei nationalen Transaktionen (im Issuer-Inland) werden die 'floor limits' zwischen Acquirer- und Issuer-Banken in den einzelnen Ländern selbst vereinbart. Die Genehmigungsgrenze pro Transaktion wird von der Acquirer-Bank für jeden Händler individuell festgelegt.

Force Sale

eine Transaktion, die von einem Händler mit der Absicht initiiert wird, die Verbuchung der Transaktion gegen das Kundenkonto zu erzwingen, ohne die vorherige Genehmigung des Kartenherausgebers oder einen Autorisierungscode vom Acquirer des Händlers zu erhalten.

Forced Post

Erzwungene Verbuchung, ist möglich, wenn einige POS-Terminals die "Forced Sale" Funktionalität erlauben. Ein "Forced Sale" ist eine Transaktion, die von einem Händler mit der Absicht initiiert wird, die Verbuchung der Transaktion gegen das Kundenkonto zu erzwingen, ohne die vorherige Genehmigung des Kartenherausgebers oder einen Autorisierungscode vom Acquirer des Händlers zu erhalten.

Fraud and Loss Database

Als Teil des Mitgliederschutz-Programmes war SAFE die weltweit zentrale Datenbank für alle Mastercard-Betrugstransaktionen und diente der Erstellung monatlicher Berichte und statistischer Auswertungen für die Mitgliedsbanken. SAFE unterstützte die Banken bei Risikofrüherkennung und Schadensprävention und stellt darüber hinaus Auswertungsdaten zur Verfügung, die auch anderen Präventionsprogrammen als Informationsgrundlage dienen. SAFE wird nun durch "Fraud an Loss Database" abgelöst.

Fraud Record im Zahlungsverkehr

Fraud Record im Zahlungsverkehr, das Betrugserfassungssystem der Finanzinformatik (FI) der Sparkassengruppe.

Fraudulent Application

Bezeichnet die Handlungsweise einer Person, die in Ihrem Kartenantrag gegenüber der Karten ausgebenden Bank oder Sparkasse unwahre Angaben zur betrügerischen Erlangung einer Zahlungskarte macht.

Fraudulent Transaction

Wenn der Karteninhaber weder eine Transaktion selbst tätigt, noch eine andere Person dazu berechtigt, seine Karte oder Kartennummer einzusetzen, handelt es beim Zustandekommen einer Transaktion um einen betrügerischen Karteneinsatz. In manche dieser Betrugsarten kann auch der Händler/Vertragspartner als Mittäter verwickelt sein.

Fremdverarbeitung

Bei der Fremdverarbeitung erfolgt die Datenverarbeitung durch ein externes Rechenzentrum.

Fuzzy Logic

Theorie, nach der logische Schlüsse aus unscharfen Informationen gezogen werden. Fuzzy-Technologie hat gegenüber der klassischen digitalen Logik den Vorteil steigender Steuerfunktionen. Diesen Vorteil findet man auch in neuronalen Netzen, jedoch kann man in die Fuzzy-Anwendung zusätzlich Expertenwissen implementieren.

G4C

Abkürzung für German Competence Centre against Cyber Crime e.V. Eine in 2015 gegründete und von privaten Wirtschaftsunternehmen getragene Initiative gegen Computerkriminalität. Im G4C haben sich Commerzbank, ING-DiBa und HypoVereinsbank sowie die Kooperationspartner Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammengeschlossen.

GA

Ein vom Karteninhaber selbst zu bedienender Geldausgabeautomat (GAA).

Gateway

Begriff zur Bezeichnung der zwischen zwei Netzwerken bestehenden Verbindungsknoten zur Ermöglichung globaler Netzwerkkommunikation.

Gebührenstrukturen

Neben den eigentlichen Lizenzgebühren entstehen dem kartenausgebenden Institut (Issuer) weitere Gebühren im laufenden Geschäft, die von den internationalen Kartenorganisationen Mastercard und Visa erhoben werden. Hierzu zählen unter anderem die sogenannten Assessment Fees, die beispielsweise bei Mastercard in national, intra-europäisch und inter-regional aufgeteilt sind. Hinzu kommen Gebühren für Clearing und Settlement. Mitgliedsbanken dieser beiden Organisationen können nähere Informationen über Aufteilung und Höhe dieser Gebühren bei den Büros von Mastercard und Visa abfragen. Eine wichtige Komponente im Rahmen von Gebühren bzw. Einnahmen sind die sogenannten Interchange Fees.

GeldKarte

Prepaid-Bezahlsystem der Deutschen Kreditwirtschaft. Den Chip auf der girocard kann man mit Guthaben aufladen z. B. am Geldautomaten oder online über geldkarte-laden.de und anschließend an GeldKarte-Akzeptanzstellen damit zahlen. Da mittlerweile fast überall das Bezahlen kleinerer Beträge mit der girocard zum Alltag gehört, werden künftig Bank- und Sparkassenkarten nicht mehr mit GeldKarte- bzw. girogo Funktionen ausgestattet. Verbraucher, die im Rahmen der Nutzung dieser Zusatzfunktionen über ein Prepaid-Guthaben verfügen und nicht mehr verbrauchen, können dieses bei dem jeweiligen Kreditinstitut am Geldautomaten entladen.

Genehmigung

Eine Genehmigungsanfrage über einen Umsatz (Transaktion) wird von dem Händler weiter an die kartenausstellende Bank (Issuer) oder deren Dienstleiter geleitet. Die Genehmigung (Autorisierung) des Umsatzes erteilt der Acquirer und leitet diese bewilligte Transaktion wiederum an den Händler weiter.

Genehmigungsfreier Höchstbetrag

Es gibt eine Genehmigungsgrenze für Vertragsunternehmen. Bei dieser Genehmigungsgrenze kann der Vertragshändler die Transaktion ohne vorherige Einholung einer Genehmigung (vom Issuer) akzeptieren. Übersteigt der Betrag diese Genehmigungsgrenze, ist der Vertragshändler verpflichtet, eine Genehmigungsanfrage durchzuführen. Bei grenzüberschreitenden Umsätzen werden die für internationale Kartenumsätze geltenden 'international floor limits' durch die Kartengesellschaften (Mastercard, Visa) pro Land veröffentlicht. Die Transaktionshöhe wird nach Händlerkategorien unterschiedlich festgelegt. Bei nationalen Transaktionen (im Issuer-Inland) werden die 'floor limits' zwischen Acquirer- und Issuer-Banken in den einzelnen Ländern selbst vereinbart. Die Genehmigungsgrenze pro Transaktion wird von der Acquirer-Bank für jeden Händler individuell festgelegt.

Genehmigungsnummer

Die Genehmigungsnummer wird infolge einer Autorisierungsanfrage von der Karten ausgebenden Bank (Issuer) vergeben und wiederum von dem Acquirer an den Händler bestätigt. Ohne diese Genehmigungsnummer hat der Händler für die Transaktion keine Zahlungsgarantie.

Geo-Blocking

Eine zur Schadensprävention von Instituten angewandte Maßnahme. Zahlungskarten werden für den Einsatz in bestimmten Ländern standardmäßig gesperrt (z.B. für den Einsatz außerhalb Europas) und bei Bedarf freigeschaltet.

girocard

Übergeordneter Begriff für das Deutsche Geldautomatensystem und das Bezahlsystem electronic cash (seit 2007 ebenfalls „girocard" genannt). Zudem beschreibt der Begriff „girocard" die Plastikkarte, die alle technischen Vorkehrungen für das Bezahlsystem beinhaltet.

girogo

Das kontaktlose Bezahlsystem der deutschen Kreditwirtschaft, das auf Basis der GeldKarte (kontaktbehaftet) eine Prepaid-Zahlung durch reines Vorhalten (also kontaktlos, ohne Einführen der Karte) an einem Kartenterminal ermöglicht.

Gleichbehandlungsklausel

Der Akzeptanzpartner verpflichtet sich, unabhängig der vom Kunden eingesetzten Zahlungsart (Kreditkarte, Debitkarte, bar, etc.) bei der Bezahlung keine Unterschiede (z.B. Rabatt bei Barzahlung etc.) zu machen.

Global Performance Standards

Diese Leistungsstandards sind von Mastercard definierte Standards zur Erhöhung des Leistungsniveaus von Mastercard- und Maestro-Karten. Sie beziehen sich auf Schlüsselbereiche wie Akzeptanz, Autorisierung, Clearing und Chargebacks. Mastercard überwacht die Einhaltung der Standards.

Grenzüberschreitende Akquisition

Grenzüberschreitendes Vertragsunternehmensgeschäft mit zentraler Abrechnung.

Grenzüberschreitende Kartenausgabe

Karteninhaber und Karten ausgebende Bank befinden sich in unterschiedlichen Ländern.

Grenzüberschreitende Transaktion

Internationale Transaktion bzw. grenzüberschreitende Transaktion, indem sich der Acquirer und die Bank (Issuer) in verschiedenen Ländern befinden.

Grenzüberschreitendes Karteninhabergeschäft mit zentraler Abrechnung

Ein internationales Unternehmen, dessen Mitarbeiter in unterschiedlichen Ländern tätig sind, gibt Karten von einer zentralen Bank heraus.

Grenzüberschreitendes Vertragsunternehmensgeschäft

Ein zentraler Acquirer verarbeitet Transaktionen von einem international tätigen Unternehmen (Airline, Hotel, Autovermietung, etc.).

Hacker

Eine Person, die sich unerlaubten Zugang zu Computerdateien verschafft.

Haftungsumkehr

Als Folge der Einführung der EMV-Chiptechnologie muss diejenige Transaktionspartei (Issuer oder Acquirer) die Haftung für betrügerische Transaktionen tragen, die den Betrug durch die Nutzung der neuen Technologie - EMV und/oder Karteninhaberverifikation mittels PIN - hätte verhindern können. Bei der Haftungsverteilung wird damit eine Art Verursacherprinzip eingeführt. Ist entweder das Terminal oder die Karte bei einer Transaktion EMV-fähig, trägt diejenige Transaktionspartei die Haftung für Schäden aus Kartenfälschungen, die nicht EMV-fähig war. Dies gilt sowohl für POS- als auch für Geldautomatentransaktionen der jeweiligen teilnehmenden Länder(Liability Shift-Länder). Zudem trägt die EMV-Chiptechnologie entscheidend dazu bei, Kartenfälschungen und -kopien nachhaltig zu verhindern.

Handelsgeschäfte zwischen Unternehmen

Mit einer Firmenkarte (Purchasing Card, Corporate Card etc.) bezahlt ein Unternehmen Dienstleistungen oder auch Waren an ein anderes Unternehmen.

Händlerkarte

Kundenkarte, die der Karteninhaber in einem Einzelhandelsunternehmen nutzt. Sie sind über die Hausbank erhältlich.

Händlervertrag

Schriftlicher Vertrag zwischen Händler und Acquirer-Bank. Er beinhaltet die Bedingungen, Rechte und Pflichten der Vertragsparteien hinsichtlich der Kartenakzeptanz.

Händlervertragsbank

Eine vertragsunternehmensabrechnende Bank mit vertraglicher Geschäftsbeziehung zum Händler. Die Bank rechnet die vom Händler übermittelten Kartenumsatzdaten mit dem entsprechenden Zahlungssystemen ab.

HBCI

Kommunikationsstandard des deutschen Kreditgewerbes für die sichere Abwicklung von

Bankgeschäften über das Internet.

heiße Angriffe

Bei heißen Angriffen kommen thermische Werkzeuge, wie z.B. Schweißbrenner, Sauerstofflanzen oder auch Schneidbrenner, die mit einem Gemisch aus Brenngas und Sauerstoff arbeiten, zum Einsatz. Als kalt bezeichnet man Angriffe auf Geldautomaten, wenn mechanische Werkzeuge verwendet werden, um Zugriff auf die Geldkassetten zu erlangen.

High-Risk Merchant

Hierbei handelt es sich um Vertragsunternehmen, die gemäss den Richtlinien für Risiko und Betrug im Rahmen des Visa Risk Identification Service als Risikounternehmen eingestuft wurden.

Hochprägung

Prägung der Plastikkarten mit den erforderlichen Daten.

Hologramm

Ein Hologramm ist ein flaches, dreidimensionales Abbild. Um der Kartenfälschungen entgegenzutreten, werden Hologramme verwendet.

HomeBanking Computer Interface

Kommunikationsstandard des deutschen Kreditgewerbes für die sichere Abwicklung von Bankgeschäften über das Internet.

host

Leistungsfähiger Zentralrechner, der mit einem Netzwerk verknüpft ist und als dessen EDV-Server die Anforderungen aller Netzwerkteilnehmer erfüllt. Dieser Begriff bezeichnet auch das interne Computersystem einer Mitgliedsbank.

Hot Card

Eine Karte, die sich auf einer Sperrliste befindet. Eine Akzeptanz mit dieser Karte ist darf nicht mehr erfolgen.

Hybrid Karte

Zahlungskarte, die sowohl mit Magnetstreifen als auch mit Chip ausgestattet ist. An Terminals, die mit Chiptechnologie arbeiten, werden 'hybrid cards' in ihrer Funktion als Chipkarten eingesetzt. Arbeitet das Terminal aber ausschließlich mit Magnetstreifen-Technologie, fungieren 'hybrid cards' als herkömmliche Magnetstreifenkarten.

Hybrid Terminal

Terminal für die Kartenakzeptanz, unterstützt sowohl Magnetstreifen- als auch Chiptechnologie, erfüllt die von Mastercard vorgegebenen Leistungsstandards und ist mit einer Tastatur zur

alphanumerischen PIN-Eingabe ausgestattet.

IBAN

Die International Bank Account Number (IBAN) ist eine standardisierte Kennung für Bankkontonummern und dient der Vereinheitlichung von Zahlungsverkehrssystemen unterschiedlicher Länder innerhalb der EU. Sie besteht in Deutschland aus 22 Stellen, beginnt mit dem Länderkennzeichen (z.B. DE für Deutschland), es folgen eine zweistellige Prüfziffer, die Bankleitzahl und die Kontonummer bestehend aus 10 Ziffern.

ICC

Chipkarte 'Integrated Circuit Card' Zahlungskarte mit eingebettetem Chip, einem Mikroprozessor mit integriertem Schaltkreis, wird häufig auch als 'smart card' oder 'chip card' bezeichnet.

In-Branch Terminal

Ein elektronisches Terminal mit Karten-Lesefunktion, das in Bankfilialen installiert ist und für manuelle Bargeldtransaktionen benutzt wird. Beim Einsatz von Kreditkarten unterschreibt der Karteninhaber einen Beleg. Der Bankkassierer vergleicht sodann die Belegunterschrift mit der Kartenunterschrift zur Legitimationsprüfung des Kartenvorlegers. Beim Einsatz von Debitkarten gibt der Karteninhaber seine PIN ein, die von der Issuer-Bank online bzw. offline im Kartenchip geprüft wird.

Initial Access Broker

Initial Access Broker (IAB, "Erstzugangsbroker")
sind spezialisierte Akteure der Cyberbedrohung, die sich unbefugten Zugang zu Computersystemen und -netzwerken verschaffen und diesen Zugang dann anderen spezialisierten Akteuren verkaufen.

Inlandstransaktion

Eine Transaktion, die im Inland zwischen dem Händler und Karteninhaber getätigt wird.

Instant Payment

... sind Online-Überweisungen oder Geldtransfers zwischen Transaktionspartnern in wenigen Sekunden bzw. Minuten. Verbuchung und Valutierung der Geldbeträge erfolgen in Echtzeit.

Integrated Intelligent Risk Information System

Elektronisches Sicherheitssystem, das neuronale Netze mit Fuzzy-Logic-Verfahren kombiniert. Die IRIS Produktfamilie besteht aus den drei Bausteinen IRIS Credit, IRIS Debit und IRIS Merchant.

Interaktionspunkt

Handelseinrichtung, Geldautomat oder andere personalfreie Akzeptanzumgebung, die es dem Karteninhaber gestattet, eine Zahlungstransaktion durchzuführen, Geld abzuheben bzw. eine Karte aufzuladen oder zu belasten.

Interbank Card Association

Die ICA ist eine 4-6 stellige Identifikation bei Mastercard um ein Mitglied eindeutig identifizieren zu können.

Interbank Network for Electronic Transfer

Zentrales System für die elektronische Abrechnung von Kartentransaktionen. Das System gehört Mastercard International und wird in USA eingesetzt. Es steuert den Austausch von Clearing und Settlement-Daten zwischen Mastercard International und den Mitgliedsbanken.

Interchange

Austausch von Transaktionsdaten zwischen Acquirer- und Issuer-Banken nach festgelegten Regeln. Die Interchange für Bargeldtransaktionen wird vom Issuer an den Acquirer gezahlt.

Interchange Gebühr

Die Interchange Gebühr wird von dem Acquirer für jede angewandete Transaktion an die Karten ausgebende Bank (Issuer) bezahlt.

Internet of Things

Das „Internet der Dinge“ ist der Überbegriff für eine Technologie, in der physische Geräte, Sensoren und andere Technologien miteinander vernetzt werden, um über das Internet Daten auszutauschen. So kann beispielsweise eine Waschmaschine bei einer Störung automatisch eine Wartung initiieren, und ein Versicherer könnte seinen Mitgliedern Rabatte für das Tragen von Fitness-Armbändern anbieten.

Interoperabilität

Systemüberschreitende Nutzungsmöglichkeit von Terminals: Die Fähigkeit von verschiedenen Rechnersystemen, systemüberschreitend Daten unter Nutzung eines kompatiblen Interfaces und gemeinsamer Kommunikationsmittel so auszutauschen, dass der jeweilige Empfänger sie interpretieren und in einer vorgegebenen Weise reagieren kann.

intrinsisch

von innen her, aus eigenem Antrieb

Invisible Payments

Invisible Payments beschreiben einen automatischen Zahlungsvorgang, der im Hintergrund abläuft und nicht direkt vom Nutzer ausgelöst wird. Der Nutzer hat jedoch zuvor auf einer entsprechenden Plattform, über die die Zahlung abgewickelt wird - beispielsweise bei PayPal oder bei Amazon - seine Kreditkartendaten oder die Daten für weitere Bezahlarten hinterlegt.

iOs

ein Betriebssystem von Apple für die mobilen Geräte iPhone, iPod touch und iPad sowie ab der

zweiten Generation des Apple TV

Issuer (Emittent)

Mitgliedsbank, die Zahlungskarten an ihre Kunden ausgibt, die Kartenkonten ihrer Kunden verwaltet, Kartentransaktionen autorisiert (entweder selbst oder über beauftragte Dienstleister) und der Acquirer-Bank gegenüber den Zahlungsausgleich für gültige Kartenumsätze garantiert.

Issuer Access Point

Technische Einrichtung, die dem Issuer für den Zugang zum EPS-Net (Mastercard & Maestro) oder VisaNet (VAP – Visa Access Point) benötigt.

Issuer Authentifizierungsdaten

Genehmigungsdaten der Karten ausgebenden Bank

Issuer Netzzugangspunkt

Technische Einrichtung, die der Issuer für den Zugang zum EPS-Net (Mastercard & Maestro) oder VisaNet (VAP – Visa Access Point) benötigt.

Issuing Processing

Verarbeitungsleistung rund um die Ausgabe einer Kreditkarte. Vom Kartenantrag über die Umsatzverrechnung, das Sicherheitsmanagement, das Cash-Management bis zur Bearbeitung von Reklamationen.

iTAN-Verfahren

iTANs sind Transaktionsnummern von einer gedruckten Liste, die nicht erst aus den jeweiligen Überweisungsdaten erzeugt werden, sondern universell einsetzbar sind. Bei jeder Transaktion sei es eine Überweisung oder eine sonstige Aktion, die per Online- Banking durchgeführt wird, wird eine bestimmte TAN-Nummer in der Liste zur Autorisierung der Transaktion abgefragt.

Item Charge

Eine Gebühr, die pro Transaktion erhoben wird.

Jackpotting

Beim Betrugsdelikt Jackpotting wird die Steuerungselektronik eines Geldautomaten mit Hilfe einer speziellen Hacker-Software so manipuliert, dass sämtliche Sperren des Automaten außer Betrieb gesetzt werden und der Automat den gesamten Bargeldbestand herausgibt. Eingespielt wird die Schadsoftware zumeist mit Hilfe eines USB-Sticks. Der Begriff Jackpotting geht auf den Sicherheitsexperten Barnaby Jack zurück, der diese Angriffsmethode bereits 2010 auf der Hacker-Konferenz Black Hat in Las Vegas (USA) vor Bankenvertretern demonstrierte, um diese vor dem neuen Trick zu warnen

JCB

Ein internationales Kartensystem, welches das Issuing und Acquiring selbst durchführt.

Karten ausgebende Bank

Eine Bank, die Zahlungskarten ausgibt, Transaktionen ihrer Karteninhaber von anderen Mitgliedsbanken bzw. Händlern entgegennimmt, Zahlungen mit der Karte garantiert und die entsprechenden mit der Karte getätigten Umsätze vom Konto des Karteninhabers einzieht.

Kartenechtheitsprüfung EMV

Bei der Kartenechtheitsprüfung findet im Chipumfeld eine gegenseitige Prüfung durch den Austausch von Kryptogrammen statt. Die Kartenechtheit des Kryptogramms einer Chipkarte wird von der jeweiligen Issuer-Bank überprüft, die Prüfung des Issuer-Kryptogramms geschieht durch den Chip.

Karteneinsatzdatei

Die Karteneinsatzdatei enthält die Transaktionsdaten für ein bestimmtes Kartenkonto innerhalb eines bestimmten Zeitraumes. Bei 'im Auftrag einer Karten ausgebenden Bank' ausgeführten Dienstleistungen (on-behalf services) erfolgt vor jeder Autorisierung einer Transaktion ein Abgleich mit dieser Datei, um sicherzustellen, dass der von der Karten ausgebenden Bank vorgegebene Verfügungsrahmen nicht überschritten wird.

Karteneinsatzort

Der Standort, von wo aus der Karteninhaber einen elektronischen Kartenzahlungsvorgang einleitet (z.B. am Kassenterminal im Handel, am PC zu Hause, am GAA oder einem Kartentelefon).

Karteninhaber

Eine Person, für die eine Karte rechtmäßig ausgestellt wurde. Die Zuordnung des Kartenkontos erfolgt über die Kartennummer des Inhabers.

Karteninhaber Legitimationsprüfung

Hierbei wird die Karteninhaberechtheit geprüft. Dies geschieht durch Prüfung der Unterschrift, oder auch durch die Eingabe der PIN (personal identification number – Geheimzahl).

Kartenleistungsbeleg

Der Karteninhaber erhält als Nachweis über seine getätigten Transaktionen einen papierhaften Beleg vom Terminal. Sollte der Karteninhaber einen manuell erstellten Beleg erhalten, so ist dieser von ihm zu unterschreiben. Den Beleg bezeichnet man auch als charge slip, sales draft, oder sales ticket.

Kartenpersonalisierung

Herstellung (Druck), Prägung und Kodierung der Karten sowie deren Ausstattung mit allen

Merkmalen und Servicefunktionen, die eine Issuer-Bank ihren Karteninhabern zur Verfügung stellen möchte.

Kartenprüfnummer

Die Kartenprüfnummer dient zur Sicherheit bei Mailorder- und Internet-Transaktionen. Der Karteninhaber wird von dem Händler aufgefordert, neben der Kartennummer und des Gültigkeitsdatums auch noch die Kartenprüfnummer mitzuteilen. Diese befindet sich auf dem Unterschriftsstreifen der Kartenrückseite. Diese weitere Sicherheitsabfrage ist nötig, um sicherzustellen, dass Belegdaten nicht für betrügerische Zwecke über Internet oder Mailorder missbraucht werden.

Kartenrisikomanagement

Bezogen auf die Chipkarten bezeichnet dieser Begriff eine Reihe von Prüfungsmöglichkeiten und Abwicklungsoptionen, die mit einem Chip zur Verfügung stehen, um Betrugsschäden zu reduzieren. Beispielsweise könnte eine Chipkarte so programmiert sein, dass jede 'x'-te Transaktion online autorisiert werden muss. Auch ein Online-Limit - ein Betrag, ab dem eine Onlineautorisierung von der Karte verlangt wird - kann eingestellt werden.

Kartenterminal zur Selbstbedienung

Terminal-Automat zur Selbstbedienung, stellt bestimmte Produkte oder Dienstleistungen zur Verfügung und ist meist in Bahnhöfen, an Flughäfen, Tankstellen, Mautstellen, in Parkhäusern sowie anderen Servicebereichen anzutreffen.

Key Indicators

Bezeichnung für eine Reihe von Indikatoren zur Bewertung der Geschäftsentwicklung in der Kartenindustrie unter Zugrundelegung bestimmter Zeiträume. Indikatoren dieser Art können sein: Anzahl ausgegebener Karten, prozentualer Anteil genehmigter Transaktionen verglichen mit dem Gesamtaufkommen, Anzahl der Rückbelastungsfälle etc.

Keylogger

Von Hackern verwendete Hard- oder Software zur Protokollierung von Tastatureingaben wie z.B. Zugangscodes, Kennwörter oder PINs an Endgeräten.

Kognitives Computing

Kommt aus dem Big Data-Bereich und bezeichnet die systematische Nutzung von Daten aus unterschiedlichen Quellen. Ziel ist es, aus diesen Informationen intelligentes Wissen zu generieren, das Unternehmen Mehrwerte bei der Entwicklung von Innovationen und optimierte Entscheidungsfindungsprozesse liefert.

Kontaktlos

Beim kontaktlosen Bezahlen muss die Zahlungskarte nicht mehr in das Terminal gesteckt werden.

Dank Near Field Communication (kurz NFC, oder deutsch Nah-Feld-Kommunikation) genügt es, wenn die Karte oder das Smartphone (mit digitaler Karte) nah (gewöhnlich etwa 4 cm Abstand) an das Terminal gehalten wird. Die Fähigkeit einer Karte und eines Terminals zum kontaktlosen Bezahlen erkennt man am jeweiligen Wellensymbol.

Kontonummer

Eine von der Karten ausgebenden Bank erteilte Kontonummer, um ein Kartenkonto für die Belastung mit Transaktionen zuzuordnen.

Kontostandsabfrage

Kontostandsabfrage eines Karteninhabers am Geldautomat.

Kreditwürdigkeitsprüfung

Kreditwürdigkeitsprüfung legt die Issuer-Bank fest, ob der Kartenantrag bewilligt oder abgelehnt wird. Zu den Kriterien der Bonitätsprüfung gehören u.a. Alter, Beruf, durchschnittliches Monatseinkommen etc.

Kreditzahlung

Die getätigten Transaktionen des Karteninhabers werden gesammelt und in der Regel in einer monatlichen Gesamtrechnung ausgewiesen.

Kryptogramm

Ergebnis eines Verfahrens zur Datenverschlüsselung unter Verwendung kryptographischer Algorithmen, kryptographischer Schlüssel und anderer Informationen. Es wird häufig angewandt beim Austausch vertraulicher Informationen zwischen zwei Parteien. Bei Chiptransaktionen ermöglicht das Verfahren einen sicheren Datenaustausch zwischen Chip und Kartenausstellerbank.

Kryptographie

Kryptographie bedeutet Geheimschrift und ist ursprünglich die Wissenschaft zur Verschlüsselung von Informationen. Heute umfasst Kryptographie zahlreiche Methoden, Daten in einer bestimmten Form zu sichern und zu übertragen, so dass nur diejenigen, für die sie bestimmt sind, die Daten lesen und verarbeiten können. Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit von Nachrichten, Datenbeständen sowie Übertragungskanälen sind die Hauptziele von Kryptographie.

Kryptowährung

Digitales, virtuelles Zahlungsmittel auf Basis einer Blockchain und abgesichert durch die stringente Anwendung von Kryptografie über ein Netz gleichwertiger Rechner.

Kundenkarte

Kreditkarte, Charge-Karte oder Debitkarte, die von einem Handelsunternehmen (z.B. Kaufhaus- oder Supermarktkette) ausgegeben wird.

KUNO

Abkürzung für 'Kriminalitätsbekämpfung im Unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen'. Zentrale Meldestelle, die Zahlungen per Debitkarte im elektronischen Lastschriftverfahren, also mit Unterschrift, sicherer gestalten soll. Polizeibehörden des Bundes und der Länder melden hierzue angezeigte Kartendiebstähle/-verluste sowie Fälle von Kontoeröffnungsbetrug an KUNO, um hierdurch zeitnah Unternehmen des Handels und weitere Branchen vor der Verwendung der gemeldeten Debitkarten zu warnen und somit den Einsatz zu verhindern. Zu diesem Zweck werden ausschließlich Bankdaten (Bankleitzahl, Kontonummer und - falls bekannt - Kartenfolgenummer) gemeldet und an Betreiber des EC-Lastschriftverfahrens weitergeleitet.

KYC

Unter dem Know- your-customer-Prinzip (KYC), engl. für „Lerne Deinen Kunden kennen“, versteht man die Prüfung der persönlichen Daten und Geschäftsdaten von Neukunden eines Kreditinstituts zur Prävention von Geldwäsche und Terrorismusfinanzierung auf der Grundlage des Geldwäschegesetzes 2008. Quelle: Gabler Wirtschaftslexikon

KYC

Know your customer - so wird eine, insbesondere für Kreditinstitute und Versicherungen, vorgeschriebene Legitimationsprüfung von bestimmten Neukunden zur Verhinderung von Geldwäsche bezeichnet.

Lade-Transaktion

Online-Transaktion an einem Chip-Ladegerät (z.B. Geldautomat, Telefon etc.), wobei ein bestimmter Betragswert vom regulären Konto des Karteninhabers abgebucht und an dessen 'elektronische Geldbörse' transferiert wird. Über das auf diese Weise 'geladene' elektronische Guthaben kann der Karteninhaber überall dort verfügen, wo Karten mit 'elektronischer Geldbörse' akzeptiert werden.

Ländercode

Kennziffer zur Identifizierung eines bestimmten Landes. Die Ziffern gehören zu einem Block international anerkannter numerisch und alphabetisch aufgebauter Codenummern, die häufig in elektronischen Nachrichten zur Länderkennzeichnung benutzt werden.

Lastschrift

Zahlungsmethode, bei der der Umsatz direkt per Lastschrift vom Girokonto eingezogen wird.

Lebanese Loop

Als Lebanese Loop bezeichnet man eine Form des Trickdiebstahls. Dabei werden die Geldautomaten so manipuliert, dass die Zahlungskarten nach dem Einführen in den Karteneinzugsschlitz nicht mehr herausgegeben werden. Die Kunden gehen dann irrtümlich davon

aus, dass ihre Karte einbehalten wurde. Tatsächlich aber steckt sie noch im - allerdings manipulierten - Karteneinzugsschlitz und wird von den Trickbetrügern entnommen, sobald sich die Geschädigten von den Automaten entfernt haben.

Legitimate Cardholder

Karteninhaber, für den rechtmäßig eine Karte ausgestellt wurde.

Liability Shift

Als Folge der Einführung der EMV-Chiptechnologie muss diejenige Transaktionspartei (Issuer oder Acquirer) die Haftung für betrügerische Transaktionen tragen, die den Betrug durch die Nutzung der neuen Technologie - EMV und/oder Karteninhaberverifikation mittels PIN - hätte verhindern können. Bei der Haftungsverteilung wird damit eine Art Verursacherprinzip eingeführt. Ist entweder das Terminal oder die Karte bei einer Transaktion EMV-fähig, trägt diejenige Transaktionspartei die Haftung für Schäden aus Kartenfälschungen, die nicht EMV-fähig war. Dies gilt sowohl für POS- als auch für Geldautomatentransaktionen der jeweiligen teilnehmenden Länder (Liability Shift-Länder). Zudem trägt die EMV-Chiptechnologie entscheidend dazu bei, Kartenfälschungen und -kopien nachhaltig zu verhindern.

Lizenzgebühr

Gebühr, die eine Mitgliedsbank im Rahmen eines Lizenzabkommens an die Kartenorganisation (Mastercard, Visa) zahlen muss.

Lizenzvertrag

Vereinbarung, die dem Lizenznehmer das Recht zur Nutzung eines bestimmten Produktmarkenzeichens gibt, wobei dies zu den in der Vereinbarung selbst sowie in den entsprechenden Produktrichtlinien festgelegten Bedingungen erfolgt.

load transaction

Online-Transaktion an einem Chip-Ladegerät (z.B. Geldautomat, Telefon etc.), wobei ein bestimmter Betragswert vom regulären Konto des Karteninhabers abgebucht und an dessen 'elektronische Geldbörse' transferiert wird. Über das auf diese Weise 'geladene' elektronische Guthaben kann der Karteninhaber überall dort verfügen, wo Karten mit 'elektronischer Geldbörse' akzeptiert werden.

Lodge Card

Karte eines Unternehmens, die bei einem Reisebüro hinterlegt ist, um so die Reisekosten des Unternehmens darüber abzurechnen. Hierbei muss es sich nicht unbedingt um eine physische Karte handeln. Häufig ist nur eine Kartennummer im System hinterlegt.

Logo

Unverwechselbare Anordnung und Gestaltung von Schrifttypen, die den Namen einer Organisation

optisch darstellen.

Maestro

Maestro ist die Debitmarke innerhalb der Produktpalette von Mastercard Worldwide. Die mit dieser Marke ausgestatteten Karten können für Einkäufe im Handel und Bargeldbezug an Geldautomaten (GA) genutzt werden.

Magnetstreifen

Auf einer Karte befindlicher und im Magnetisierungsverfahren mit Informationen belegter Streifen (Magnetstreifen), der Kartenkontodaten des jeweiligen Karteninhabers enthält. Diese Daten können von einem Terminal ausgelesen und in einer Autorisierungsanfrage an die Kartenausstellerbank online übertragen werden.

Mail Order/Telephone Order

Eine Art des Einzelhandels (auch als Distanzhandel bezeichnet), bei dem die Produkte per Internet, Fernsehen, Katalog oder Vertreter angeboten werden. Die Bestellung kann mündlich (z. B. per Telefon oder Vertreter), schriftlich (z. B. per Brief oder Fax) oder auch online getätigt werden. Die anschließende Bezahlung kann per Kreditkarte, Nachnahme, Vorabüberweisung oder auch auf Rechnung erfolgen. Die Bonität des Kunden kann das Versandunternehmen vorab bei bestimmten Auskunfteien erfragen.

Malware

Setzt sich zusammen aus den Wörtern malicious Software und bedeutet also bösartige Software. Es handelt sich um Compterprogramme, die unerwünschte Funktionen ausführen und so die Sicherheit und Funktionsfähigkeit von Computern und Systemen beeintrachtigen können (z.B. Viren, Trojaner).

Man-in-the-Middle

Bei einem Man-in-the-Middle-Angriff versucht ein Hacker sich oder eine von ihm verwendete Software zwischen ein Opfer und die vom Opfer verwendete Ressource zu schalten, um die Kommunikation des Opfers mit der Ressource abzufangen und evtl. zu manipulieren. Der Angriff erfolgt entweder innerhalb einer Netzwerkverbindung oder zwischen den Prozessen auf einem Computer.

Manuelle Transaktion

Transaktion, für die der Händler die benötigten Kartendaten 'manuell' erlangt (anders als bei elektronischer Kartenauslesung am POS-Terminal). Dies erfolgt in der Regel durch Übertragung der hochgeprägten Kartendaten auf den Transaktionsbeleg mittels 'Imprinter'. In anderen Fällen gibt der Karteninhaber dem Händler die Kartendaten schriftlich oder telefonisch weiter.

Marke

Der Markenname eines bestimmten Kartenprodukts, das innerhalb eines festgelegten Territoriums zum Einsatz als Zahlungsmedium zugelassen ist.

Markenzeichen

Kombination von Namen, Symbolen und Farben als eigentumsrechtlich geschütztes Markenzeichen zur visuellen Verkörperung der Markenidentität.

Markets in Financial Instruments Directive

Die Abkürzung der Bezeichnung „Markets in Financial Instruments Directive“ steht für eine Richtlinie der Europäischen Union über Märkte für Finanzinstrumente, kurz Finanzmarktrichtlinie. Sie soll nicht nur für eine Harmonisierung, sondern auch für effizientere, widerstandsfähigere und transparentere Finanzmärkte im europäischen Binnenmarkt sorgen. Aus der ersten Fassung von 2004 wurde die seit 2018 gültige Richtlinie MiFID II entwickelt. Ein Ziel der EU-Kommission lag bei der Überarbeitung u.a. darin, einen erhöhten Anlegerschutz durch ein „Verbot für Provisionen bei unabhängiger Finanzberatung“ zu erreichen; dieses Verbot wurde durch das Europa-Parlament in eine Kann-Bestimmung abgeändert.

Mastercard Debit Switch

Mastercard-Netz für die Steuerung aller interregionalen Debit Card- und Mastercard Transaktionen mit PIN-Eingabe. Über einen Verbindungsknoten als Brücke zwischen MDS und EPS-Net können überseeische Acquirer-Banken mit europäischen Issuer-Banken (und umgekehrt) Transaktionsdaten austauschen. Siehe hierzu auch unter BankNet.

Mastercard Site Data Protection

Zielsetzung von SDP ist die Unterstützung von Händlerbanken, Händlern, Service Providern und anderen externen Dienstleistern beim sicheren Umgang mit sensiblen Karten- und Transaktionsdaten. Das Programm definiert Sicherheitsanforderungen für die Verarbeitung, Speicherung und Übertragung von vertraulichen Informationen. Damit sollen eventuelle Sicherheitslücken in den eigenen Systemen identifiziert und mögliche Folgeschäden abgewendet werden. SDP ist Teil des gemeinsamen Standards PCI.

Maximale Antwortzeit

Mit 'Time out' wird ein Ereignis beschrieben, bei dem eine Autorisierungsanfrage nicht oder nicht innerhalb der definierten maximalen Antwortzeit beantwortet und die Leitung unterbrochen wird.

MCC

Der MCC (Merchant Category Code, auch Card Acceptor Business Code) ist ein 4-Ziffern-langer numerischer oder alphanumerischer Branchencode, den eine Kreditkartenfirma angibt und mit dem der Service, die Branche oder das Produkt des Händlers aufgelistet wird.

mCoupons

Neben Papiergutscheinen, Coupons und Rabattkarten besteht auch eine mobile Variante. Es handelt sich dabei zunehmend um ortsgebundene elektronische Coupons, die kundenindividuell an das Mobiletelefon registrierter Stammkunden versandt und in einer Mobile Wallet oder einer App des Händlers gespeichert werden können. Der Kunde kann hierbei seinen ortsgebundenen („Location-based“) Coupon im Geschäft des Händlers einlösen, meist durch einen Scan des QR Barcodes vom Bildschirm des Mobiltelefons.

Member Service Provider

Ein Unternehmen, das für eine Mitgliedsbank (oder mehrere) vertraglich vereinbarte Dienstleistungen im Kartengeschäft erbringt (-> Prozessor). Dienstleistungen in der Kartenbranche können beispielsweise sein: Autorisierung, Genehmigungsdienst, Reklamationsbearbeitung, Prävention, Missbrauchsbearbeitung, Rechnungserstellung und Versand, Ersatzkartenservice, Transaktionsprozessing, Kartenversand.

Merchant

Handels- und Dienstleistungsunternehmen, die mit einer Acquirer-Bank eine vertragliche Vereinbarung zur Akzeptanz von Zahlungskarten schließen. Ein solcher Akzeptanzvertrag (Händlervertrag) regelt, unter welchen Bedingungen Zahlungksarten akzeptiert werden.

Merchant Agreement

Schriftlicher Vertrag zwischen Händler und Acquirer-Bank. Er beinhaltet die Bedingungen, Rechte und Pflichten der Vertragsparteien hinsichtlich der Kartenakzeptanz.

Merchant Alert To Control High-risk Merchants

Die MATCH-Datenbank von Mastercard enthält eine Liste aller gekündigten Vertragshändler. Ein Acquirer, der einen Händlervertrag kündigt, muss diesen Vorgang in die MATCH-Datenbank einmelden. Ein Acquirer, der einen neuen Händlervertrag abschließt, muss die Händlerdaten zuvor mit der MATCH-Datenbank abgleichen und darüber durch Vorlage des von MATCH generierten Antwortcodes, falls von Mastercard dazu aufgefordert, Nachweis führen.

Mining

Der Prozess zum Generieren neuer Bitcoins wird, analog zum Goldschürfen, Mining genannt. Hohe Anforderungen an die Rechenleistung und starke Konkurrenz im Mining-System, machen dabei das System sicher und verhindern, dass unkontrolliert neue Transaktionsblöcke der Blockchain hinzugefügt werden.

MISP

Malware Information Sharing Platform des EPC

Mittäterschaft

Mittäterschaft (durch betrügerisches Einverständnis). Dieser Begriff bezeichnet die wissentliche und vorsätzliche Beteiligung an betrügerischen Aktivitäten.

Mobile App Resiliency

Die Fähigkeit einer mobile Anwendung, die von einem Angreifer verursachten Widrigkeiten zu überstehen bzw. Attacken standzuhalten.

Morphing

Morphing ist ein computergeneriertes Verfahren, mit dem bei Bild– oder Tonaufzeichnungen zwischen den Einzelbildern oder Klängen Übergänge berechnet werden, so dass eine Verschmelzung der Bilder oder Klänge stattfindet.

MOTO

Eine Art des Einzelhandels (auch als Distanzhandel bezeichnet), bei dem die Produkte per Katalog, Prospekt, Internet, Fernsehen oder Vertreter angeboten werden. Die Bestellung der gewünschten Produkte kann mündlich (z. B. per Telefon oder Vertreter), schriftlich (z. B. per Brief oder Fax) oder auch online getätigt werden. Die anschließende Bezahlung kann per Kreditkarte, Nachnahme, Vorabüberweisung oder auch auf Rechnung erfolgen. Die Bonität des Kunden kann das Versandunternehmen vorab bei bestimmten Auskunfteien erfragen.

MOTO-Transaction

Eine Transaktion, die darauf beruht, dass ein Karteninhaber bei einem Händler entweder schriftlich oder telefonisch Waren oder andere Dienstleistungen bestellt und diese per Karte bezahlt.

mTAN-Verfahren

mTANs werden von den Anbietern während der entsprechenden Online- Banking-Transaktion per SMS an die von dem Kunden angegebene Mobilfunknummer versendet. Vor der finalen Freigabe der Transaktion wird dem Kunden neben dem Geldbetrag auch die Bankleitzahl des Empfängers übermittelt.

Mutual Authentication

Bei der Kartenechtheitsprüfung findet im Chipumfeld eine gegenseitige Prüfung durch den Austausch von Kryptogrammen statt. Die Kartenechtheit des Kryptogramms einer Chipkarte wird von der jeweiligen Issuer-Bank überprüft, die Prüfung des Issuer-Kryptogramms geschieht durch den Chip.

Nationale Interchange Gebühr

Eine umsatzabhängige, prozentuale oder transaktionsabhängige, fixe Gebühr, die die Händlerbank an die Karten ausgebende Bank basierend auf den nationalen Interchange Gebührenregelungen zahlen muss.

Near Field Communication (NFC)

Near Field Communication (NFC) bezeichnet das Bezahlen per Übertragungsstandard zum berührungslosen Austausch von Daten über kurze Distanzen von nur wenigen Zentimetern, z. B. mit Handy, girocard oder Kreditkarte.

Netzzugangspunkt

Dieser Begriff umfasst die gesamte Technik, die für den Netzzugang benötigt wird. Dazu gehören folgende Einzelkomponenten: Der Zugang zum Online-Routingservice, zu den Autorisierungs-Dienstleistungen sowie zusätzliche Sicherheitsmodule für die PIN-Verschlüsselung und –Prüfung.

Neuronales Netz

Selbstlernendes Netzwerk, das aufgrund von Erfahrungen neue Regeln für die Bewertung von Transaktionsdaten entwickelt.

Nicht genehmigte Transaktion

Eine Transaktion, die von der Karten ausgebenden Bank nicht genehmigt wurde.

Non-Discrimination Rule

Der Akzeptanzpartner verpflichtet sich, unabhängig der vom Kunden eingesetzten Zahlungsart (Kreditkarte, Debitkarte, bar, etc.) bei der Bezahlung keine Unterschiede (z.B. Rabatt bei Barzahlung etc.) zu machen.

Null-Limit

Herabsetzung des genehmigungsfreien Höchstbetrages (floor limit) beim Händler pro einzelnen Kartenumsatz auf 'Null' für bestimmte Transaktionsarten. Die Maßnahme verpflichtet den Händler (oder die Acquirer-Bank) zur Durchführung einer Genehmigungsanfrage (online oder telefonisch) bei der Issuer-Bank, unabhängig von der Betragshöhe. Für Geldausgabeautomaten (ATM) gilt grundsätzlich ein zero floor limit.

Öffentlicher Schlüssel

Dieser Schlüssel wird bei der asymmetrischen Verschlüsselungstechnologie zusätzlich zu dem privaten Schlüssel benötigt. Die mit dem Public Key verschlüsselten Daten können nur mit dem zugehörigen Private Key entschlüsselt werden.

Offline Autorisierung

'Offline'-Autorisierungen können im Rahmen definierter Betragsobergrenzen ('floor limit') durch einen Händler, ein Terminal, eine Acquirer-Bank (oder deren Dienstleister) oder durch eine Chipapplikation in der Karte selbst vorgenommen werden.

On behalf Services

Dienstleistungen, die Mastercard für seine Mitglieder in deren Auftrag ('on-Behalf') ausführt. Hierzu zählen: Dynamic Stand-in, Down Option, Permanent Stand-in, PIN Pre- Validation, Limit 1 Processing, Mastercard Stand-In und X-code.

On us Transaktion

Bezeichnet eine Transaktion, für die eine Mitgliedsbank sowohl der Acquirer der Transaktion als auch der Herausgeber der bei dieser Transaktion eingesetzten Karte ist.

On-Device Fraud (ODF)

Bei dieser Art von Betrug werden Transaktionen von demselben Gerät initiiert, das das Opfer täglich benutzt. Die Täter schleusen einen Trojaner auf das Gerät, über den sie Fernzugriff erhalten. Der Modus Operandi ist besonders unauffällig, riskant und gefährlich.

Online Autorisierung

Autorisierung eines Kartenumsatzes aufgrund einer 'online' Genehmigungsanfrage der Acquirer-Seite bei der Issuer-Bank.

Online Terminal

Händler-Terminal, das Kartendaten elektronisch ausliest und für jede Transaktion eine 'online'-Genehmigungsanfrage an die Issuer-Bank generiert.

Online Transaktion

Über ein Händler-Terminal genehmigter oder abgelehnter Kartenumsatz nach elektronischem Echtzeitdialog zwischen Acquirer- und Issuer-Bank (oder zwischen deren Dienstleistern). Dies setzt voraus, dass das Terminal über die Acquirer-Bank mit der Issuer-Bank 'online' in Verbindung treten, Genehmigungsanfragen senden und Antwortnachrichten empfangen kann.

OSCar

OSCar (Open Standards for Cards) ist der Kern für eine Konsolidierung der europäischen Standardisierungs-Initiativen, die auf den Anforderungen des European Payments Council (EPC) basieren. In dem Konsortium arbeiten Interessengruppen wie EPAS, CIR-TWG, Berlin Group und CAS an der Vereinheitlichung der im Kartenbereich verwendeten Standards.

OWASP

OWASP steht für „Open Web Application Security Project“ und ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Software zu verbessern.

OWASP Mobile App Security Verification Standard Level 2 + R

In Ergänzung zum Test-Handbuch (MASTG) hat OWASP den Mobile App Security Verification Standard (MASVS) entwickelt, der eine Metrik und Kategorisierung der Test-Anforderungen in vier verschiedene Stufen umfasst. Die vier Stufen erlauben, den Grad der Konformität mit den

Testanforderungen für eine App zu quantifizieren. Für Finanzdienstleistungen empfiehlt OWASP das Niveau L2 + R (Defense-in-depth + Resilience Against Reverse Engineering and Tampering).

OWASP Mobile Application Security Testing Guide (MASTG)

Ein weltweit anerkanntes Handbuch zum Testen der Sicherheit von mobilen Anwendungen, das von OWASP erstellt wurde. Es beinhaltet ausführliche Empfehlungen und Testverfahren.

PAN-Schlüsseleingabe

Bezeichnet die manuelle Eingabe (über Tastatur) der Kartennummer in ein POS-Terminal statt elektronischer Einlesung über den Magnetstreifen.

Pay Before

Allgemeine Bezeichnung für Zahlungsprodukte, bei denen das Konto des Karteninhabers schon vor der eigentlichen Produktnutzung belastet wird. Beispiel: elektronische 'Geldbörse'. Zahlungsprodukte dieser Kategorie werden auch als 'pre paid products' bezeichnet.

Pay Later

Die getätigten Transaktionen des Karteninhabers werden gesammelt und in der Regel in einer monatlichen Gesamtrechnung ausgewiesen.

PayComm e.V.

Als Wissensplattform für die Payment Community wurde im Februar 2003 der Verein PayComm e.V. gegründet. Ziel von PayComm ist es vor allem, das nötige Expertenwissen bereit zu stellen, um das Fachwissen der Mitarbeiter in den unterschiedlichen Payment Unternehmen zu ergänzen bzw. zu aktualisieren. PayComm hilft aber auch neuen Mitarbeitern der Payment Unternehmen, mit der komplexen Materie rund um den bargeldlosen Zahlungsverkehr vertraut zu werden.

paydirekt

Online-Bezahlservice direkt vom Girokonto, an dem sich neben den privaten und genossenschaftlichen Banken auch die Sparkassen beteiligen.

Payment Card

Karte, die vom Karteninhaber zur Bezahlung von Waren und Dienstleistungen sowie zum Bargeldbezug eingesetzt werden kann.

Payment Card Industry Data Security Standards

Um eine einheitliche Vorgehensweise bei der Umsetzung dieser Sicherheitsanforderungen zu ermöglichen, haben sich die Kartenorganisationen Visa (AIS) und Mastercard (SDP) im Jahr 2005 auf gemeinsame Standards geeinigt. Diese tragen die Bezeichnung 'Payment Card Industry (PCI) Data Security Standards' und haben Gültigkeit für die gesamte Kartenzahlungsbranche.

Payment System

Allgemeiner Oberbegriff für Systeme, die der Wahrnehmung von Aufgaben im Zahlungsverkehr dienen.

PayPass

PayPass heißt die kontaktlose Zahlungstechnologie von Mastercard. Mit der Kreditkarte auf Basis der Near Field Communication-Technologie (NFC) können Kleingeldbeträge an kontaktlosen Lesern ohne Einstecken der Karte bargeldlos bezahlt werden. Aufgrund der niedrigen Geldbeträge entfallen hierbei die bei sonstigen Kreditkartentransaktionen erforderliche Unterschrift, eine Quittung oder die PIN-Eingabe.

PayWave

PayWave heißt die kontaktlose Zahlungstechnologie von Visa. Mit der Kreditkarte auf Basis der Near Field Communication-Technologie (NFC) können Kleingeldbeträge an kontaktlosen Lesern ohne Einstecken der Karte bargeldlos bezahlt werden. Aufgrund der niedrigen Geldbeträge entfallen hierbei die bei sonstigen Kreditkartentransaktionen erforderliche Unterschrift, eine Quittung oder die PIN-Eingabe.

PCI DSS

Im Payment Card Industry Data Security Standard (PCI DSS) sind Sicherheitsrichtlinien definiert, zu denen weltweit alle Vertragspartner verpflichtet sind, die Kartendaten übermitteln, verarbeiten oder speichern.

Peer to Peer

Rechner zu Rechner Verbindungen, bei denen alle Computer gleichberechtigt sind. Jeder Rechner kann Ressourcen, Funktionen oder Dienste anbieten oder diese in Anspruch nehmen. Die Daten sind dezentral organisiert und verteilt.

Peer-to-Peer-Geldtransfer

Die Peer-to-Peer Zahlung (auch: P2P- oder Person-to-person payment) ist ein Geldtransfer mit einem mobilen Endgerät über eigens hierfür angebotene Apps zwischen Privatpersonen (Peers), z.B. die formlose Zahlung zwischen Freunden, die sich eine Rechnung aufteilen. Privatpersonen können sich mit diesem Feature Geld so einfach und schnell senden wie eine E-Mail.

Pflichtprogramm bei überhöhtem Rückbelastungsaufkommen

Ein von Mastercard entwickeltes Programm zur zahlenmäßigen Reduktion der Rückbelastungsfälle, insbesondere bei bestimmten Transaktionsarten (z.B. Electronic Commerce). Eine Acquirer-Bank, deren monatliche Rückbelastungsquote den branchenüblichen Durchschnitt und die zulässige Toleranzschwelle übersteigt, setzt sich dem Risiko der Auferlegung von Strafgebühren aus.

Pharming

Pharming ist eine Weiterentwicklung der Internet-Betrugsmethode Phishing. Hierbei wird der Internet-Nutzer nach Eingabe einer korrekten Web-Adresse auf eine gefälschte Seite umgeleitet, die der echten täuschend ähnlich sieht. Auf der gefälschten Seite wird der Kunde dann aufgefordert, Geheimzahl (PIN) sowie Transaktionsnummern (TAN) einzugeben, mit denen die Kriminellen Geld vom Konto des Betrogenen abheben können. Da die Kriminellen oft ganze Server-Farmen mit gefälschten Websites betreiben, wird diese Methode 'Pharming' genannt.

Phishing

Phishing ist ein Kunstwort aus Passwort und Fishing. Es bezeichnet ein Verfahren, mittels gefälschten E-Mails oder Webseiten unbemerkt persönliche Daten auf fremden Rechnern auszuspionieren. Dabei erhält der Anwender eine seriös wirkende E-Mail, die den Empfänger darauf hinweist, sein Zugang bei einem Auktionshaus oder seiner Onlinebank würde verfallen oder bei einer Kreditkarte müsse eine Sicherheitsabfrage stattfinden. Um dies zu verhindern, müsse auf einen im Text enthaltenen Link geklickt werden. Diese Links führen jedoch nicht zur Bank oder zum Auktionshaus. Stattdessen landet der Anwender auf Seiten, die populären Web-Anbietern wie eBay, Amazon oder Banken zum Verwechseln ähnlich sehen. Dort sollen sie dann vertrauliche Angaben wie Name, Passwort oder PIN-Codes eingeben, die Betrüger für Straftaten nutzen.

photoTAN-Verfahren

Für dieses Verfahren benötigt der Bankkunde auf jeden Fall zwei Geräte: Ein Smartphone oder ein spezielles photoTAN-Gerät und ein weiteres Endgerät (PC, Smartphone oder Tablet). Mit einer Smartphone-App oder dem photoTAN-Gerät scannt der Kunde vor der Transaktion ein kryptografisches Bild, das auf dem zweiten Endgerät angezeigt wird. Anschließend wird die für die Überweisung benötigte TAN mit Hilfe der App oder dem Gerät generiert.

Piktogramm

Unverwechselbare Anordnung und Gestaltung von Schrifttypen, die den Namen einer Organisation optisch darstellen.

PIN

Personal Identification Number, Geheimnummer, die nur dem Karteninhaber bekannt ist und die Issuer-Bank (oder deren Dienstleister) in die Lage versetzt, die persönliche Legitimation des Karteninhabers zu überprüfen.

PIN basierte Transaktion

Kartentransaktion, bei der die persönliche Legitimation des Karteninhabers durch Prüfung der PIN erfolgt, die der Kunde am Ort der Transaktionsdurchführung ('point of interaction') in ein POS-Terminal oder in die PIN-Tastatur eines Geldautomaten eingibt.

PIN Eingabetastatur

Die PIN-Eingabetastatur als Bestandteil eines elektronischen Terminals oder als Zusatzgerät. Der

Karteninhaber gibt hier seine PIN ein, die bei einer PIN-gestützten Transaktion zur Überprüfung der persönlichen Legitimation des Karteninhabers dient.

PIN Pad

Die PIN-Eingabetastatur als Bestandteil eines elektronischen Terminals oder als Zusatzgerät. Der Karteninhaber gibt hier seine PIN ein, die bei einer PIN-gestützten Transaktion zur Überprüfung der persönlichen Legitimation des Karteninhabers dient.

PIN Prüfwert

Unter Einbeziehung eines bestimmten Wertes (als einer Funktion der Karteninhaber-PIN) sowie anderer Kartendaten wird ein spezifischer Binärwert (PVV) ermittelt. Letzterer wird immer dann vom Sicherheitsmodul der Issuer-Bank errechnet und in die Karte geschrieben (kodiert), wenn sich die betreffende Issuer-Bank im Autorisierungsprozess generell für die Nutzung des 'Pre-Validated PIN'-Verfahrens als PIN-Prüfungsmethode entschieden hat. Jedes Karten ausgebende Institut oder die von ihm beauftragte Stelle ist dann in der Lage, die Richtigkeit einer Karteninhaber-PIN für die Karten, die von dem jeweiligen Institut ausgegeben wurden, zu verifizieren.

Pin Verification Value

Unter Einbeziehung eines bestimmten Wertes (als einer Funktion der Karteninhaber-PIN) sowie anderer Kartendaten wird ein spezifischer Binärwert (PVV) ermittelt. Letzterer wird immer dann vom Sicherheitsmodul der Issuer-Bank errechnet und in die Karte geschrieben (kodiert), wenn sich die betreffende Issuer-Bank im Autorisierungsprozess generell für die Nutzung des 'Pre-Validated PIN'-Verfahrens als PIN-Prüfungsmethode entschieden hat. Jedes Karten ausgebende Institut oder die von ihm beauftragte Stelle ist dann in der Lage, die Richtigkeit einer Karteninhaber-PIN für die Karten, die von dem jeweiligen Institut ausgegeben wurden, zu verifizieren.

PIN-Prüfung

Sicherheitsverfahren im Autorisierungsprozess für alle PIN-gestützten Transaktionen. Es ermöglicht der Issuer-Bank oder deren Repräsentant zu überprüfen, ob der Karteninhaber am Ort der Transaktionsdurchführung (z.B. Händler-POS oder ATM) die korrekte PIN eingegeben hat.

Point of Compromise

Hierbei handelt es sich um den Ausgangsort, wo der Kartenbetrug startete (POC).

Point of Interaction

Der Standort, von wo aus der Karteninhaber einen elektronischen Kartenzahlungsvorgang einleitet (z.B. am Kassenterminal im Handel, am PC zu Hause, am GAA oder einem Kartentelefon).

Point of Sale

Der tatsächliche Ort, an dem der Karteninhaber einen Kauf tätigt und mit der Karte bezahlt. Es handelt sich typischerweise um ein Ladengeschäft eines Vertragshändlers.

Pre Authorisation

Von der Acquirer-Bank bei der Issuer-Bank eingeholte 'Vorab'-Genehmigung über die voraussichtliche Höhe eines Kartenumsatzes, der erst zu einem späteren Zeitpunkt abgerechnet wird. Dieses Verfahren ist typischerweise in Händlerkategorien wie Hotels, Autovermietungen und bei ähnlichen Vertragsunternehmen anzutreffen. Hierdurch ist gewährleistet, dass für die erst später erfolgende Umsatzabrechnung ausreichend Mittel auf dem Kartenkonto verfügbar sind.

Presentment

Elektronische Clearing-Nachricht mit allen Umsatzdaten, die der Issuer-Bank zur Durchführung des Zahlungsausgleichs von der Acquirer-Bank zugeleitet wird.

Primary Account Number

Zur Authentifizierung von Internet-Einkäufen mit Maestro-Karten bringen einige Kartenherausgeber – analog zur Kreditkartennummer auf Kreditkarten – die Primary Account Number (PAN) auf die Vorderseite von Debitkarten auf.

Private Label Card

Kreditkarte, Charge-Karte oder Debitkarte, die von einem Handelsunternehmen (z.B. Kaufhaus- oder Supermarktkette) ausgegeben wird.

Privatschlüssel

Teilschlüssel eines kryptographischen Schlüsselpaares, das in Verbindung mit einem öffentlichen Verschlüsselungsalgorithmus benutzt wird. Ein Privatschlüssel ist ausschließlich einem bestimmten Benutzer zugeordnet, muss sicher aufbewahrt und darf nicht an Dritte weitergegeben werden. Kryptographische Privatschlüssel dienen zur Erstellung digitaler Signaturen und zum Dechiffrieren von Mitteilungen oder Dateien, die zuvor mit dem entsprechenden öffentlichen Schlüssel verschlüsselt wurden.

Produktmarke

Der Markenname eines bestimmten Kartenprodukts, das innerhalb eines festgelegten Territoriums zum Einsatz als Zahlungsmedium zugelassen ist.

Prozessor

Bezeichnung für ein Unternehmen, das für Mitgliedsbanken als Dienstleister tätig ist. Diese Dienstleistungen umfassen in der Regel das Acquiring und das Issuing Processing.

PSD2

PSD2 ist die Abkürzung für „Payment Services Directive 2“ = Zahlungsdiensterichtlinie 2 (Richtline 2015/2366/EU vom 25.11.2015), umgesetzt in deutsches Recht durch Gesetz vom 17.07.2017 (BGBl I 2017, 2446), in Kraft seit 13.01.2018.

Public Key

Dieser Schlüssel wird bei der asymmetrischen Verschlüsselungstechnologie zusätzlich zu dem privaten Schlüssel benötigt. Die mit dem Public Key verschlüsselten Daten können nur mit dem zugehörigen Private Key entschlüsselt werden.

pushTAN-Verfahren

Beim pushTAN-Verfahren lädt der Kunde neben der Online- Banking-App eine zweite App seiner Bank auf sein Handy. Die für die jeweilige Transaktion benötigte Einmal-TAN wird über diese zweite App direkt auf dem Smartphone des Nutzers generiert. Mit dieser Transaktionsnummer kann der Kunde dann z.B. eine Überweisung autorisieren.

QR Barcode

Quick Response (QR) Barcodes können unterschiedliche, auch personalisierte Informationen enthalten. Im Handel werden QR Barcodes für Produkt-, Service- und Garantie-Informationen genutzt oder sie sind ein Medium, um Gutscheine und Coupons an Kunden zu versenden. Das Bild des QR Barcodes wird per Mobiltelefon „fotografiert“ und dann vom QR Code Reader decodiert. Die hinterlegte Information kann dann auf dem Mobiltelefon gelesen und der enthaltene Link ins Internet aktiviert werden.

Quishing

Eine Phishing-Methode, bei der Cyberkriminelle ihre Opfer über QR-Codes auf gefälschte Webseiten leiten, um dort Nutzerdaten zu stehlen.

Ransomware

Der Begriff ist abgeleitet vom englischen Wort „ransom“ für Lösegeld, Ransomware ist eine Form von Malware. Der Angreifer eignet sich die Daten des Opfers an, um mit der Veröffentlichung der Daten zu drohen und/oder die Daten zu verschlüsseln und Lösegeld für die Entschlüsselung zu verlangen.

RCEP

Regional Comprehensive Economic Partnership (RCEP) ist die größte Freihandelszone der Welt. Das Abkommen besteht seit November 2020 zwischen den 10 ASEAN-Mitgliedsstaaten und fünf weiteren Staaten der Asien-Pazifik-Region.

Real-time

Ein Dialog zwischen 2 Rechnern, wobei der Empfänger einer Mitteilung gehalten ist, dem Absender innerhalb weniger Sekunden zu antworten.

Rechtmäßiger Karteninhaber

Karteninhaber, für den rechtmäßig eine Karte ausgestellt wurde.

Referral Response

Nach Autorisierungsanfrage durch den Händler erhält er die Autorisierungsantwort, dass er zwecks Genehmigung mit dem Karten ausgebenden Institut oder dessen Prozessor Kontakt aufnehmen soll. Dient lediglich zur zusätzlichen Identifikation des rechtmäßigen Karteninhabers bei ungewöhnlichem Umsatzverhalten und nicht zur Bonitätsüberwachung.

Registration Centre

Abrechnungsstelle im System der GeldKarte. Nimmt die Umsätze der Händler entgegen, leitet den Zahlungsverkehr in die Wege, prüft die Sicherheit des Systems und verrechnet die entsprechenden Entgelte unter den Beteiligten. Jeder Banksektor hat eine eigene Evidenzzentrale. Man unterscheidet Händlerevidenzzentrale und Kartenevidenzzentrale.

Reisestellenkarte

Karte eines Unternehmens, die bei einem Reisebüro hinterlegt ist, um so die Reisekosten des Unternehmens darüber abzurechnen. Hierbei muss es sich nicht unbedingt um eine physische Karte handeln. Häufig ist nur eine Kartennummer im System hinterlegt.

Replay-Attacke

Angriff mit Hilfe eines statischen Sicherheitsmerkmals (Password, Fingerprint, etc.), welches der Angreifer ausspioniert hat und nun in seiner Hand erneut verwendet.

Response Time

Zeit, die zur Beantwortung einer elektronischen Anfrage benötigt wird.

Reversal

Im Autorisierungsverfahren: Elektronische Mitteilung zur vollen oder teilweisen Stornierung einer vorherigen Transaktion, die trotz Issuer-Genehmigung nicht erfolgreich abgeschlossen werden konnte. Im Clearingverfahren: Elektronische Mitteilung zwecks Stornierung einer früheren Transaktionseinreichung.

Reverse Engineering

Reverse Engineering einer Mobile App beschreibt den Prozess der Analyse der kompilierten, ausführbaren App, um Informationen aus dem Quellcode zu gewinnen. Das Ziel von Reverse Engineering ist, den Code zu verstehen.

Reward

(engl., bedeutet auf Deutsch so viel wie Belohnung, Vergütung, Gegenleistung)

Risk Explorer

System zur Betrugsfrüherkennung und Risikosteuerung für Issuer- und Acquirer-Banken. Es erstellt Indikatoren für die Risikobewertung aufgrund bereits abgerechneter internationaler Kartenumsätze,

die nach von der Anwenderbank vorgegebenen Kriterien analysiert und gefiltert werden. Darüber hinaus generiert das System Warnmeldungen bezüglich verdächtiger Transaktionen zur vorbeugenden Aufklärung und Rückmeldung des Ergebnisses.

Risk Management

Methodisches Vorgehen zur Identifikation, Evaluation, Handhabung und Reduktion von Risiken.

Robo Advisory

Im Geschäftsfeld Robo Advisory bündeln Finanzdienstleistungsunternehmen und Fintechs ihre digitalen Dienstleistungen im Bereich Vermögensverwaltung. Das Wort setzt sich zusammen aus Robot (Roboter) und Advisor (Berater).

Robo-Advisor

Die Bezeichnung setzt sich aus den englischen Worten Robot (Roboter) und Advisor (Berater) zusammen. Robo-Advisor haben das Ziel, die Dienstleistungen eines Finanzberaters zu digitalisieren und zu automatisieren.

Rooted Devices

Gerootete Geräte (Rooted Devices) nennt man Android-Smartphones und -Tablets, deren Betriebssystem im Bereich Zugriffsrechte manipuliert wurde, um nicht-autorisierte Funktionen einzuführen, z.B. nicht zugelassene Apps zu installieren. Der "Benutzer" (d. h. die Anwendung) mit den höchsten Privilegien – mit „Root“-Rechten – kann dann alle Daten, auch die aller anderen Anwendungen, lesen und auch verändern. Dieses gilt aber ebenso für Malware-Apps, die auf gerooteten Geräten vollständige Kontrolle über das Gerät und andere Apps erhalten.

Routing

Elektronischer Übermittlungsweg für Mitteilungen und Dateien von einem Rechnersystem oder Datennetz zum anderen. Das 'routing' stellt sicher, dass die Daten auch genau den Empfänger erreichen, für den sie bestimmt sind.

RSA

Bezeichnet einen kryptographischen Algorithmus in der öffentlichen Kryptographie (Asymmetrisches Verschlüsselungsverfahren), benannt nach seinen Erfindern Rivest, Shamir und Adleman.

Rückruf

Bei dieser Beantwortung einer Genehmigungsanfrage fordert der Issuer den Acquirer auf, zusätzliche Informationen an ihn (oder seinen Dienstleister) zu übermitteln. Erst danach wird seitens des Issuers entschieden, ob dieser Umsatz genehmigt oder abgelehnt wird.

S.W.I.F.T.

Organisation, die für Banken im internationalen Raum unter anderem grenzüberschreitende

Geldüberweisungs-Dienstleistungen anbietet. Am Ende des jeweiligen Abrechnungszyklus erfolgt der Zahlungsausgleich über S.W.I.F.T. auf das Konto von Clearing-Banken der an Transaktionen dieser Art beteiligten Bankinstitute.

SAFE

Als Teil des Mitgliederschutz-Programmes war SAFE die weltweit zentrale Datenbank für alle Mastercard-Betrugstransaktionen und diente der Erstellung monatlicher Berichte und statistischer Auswertungen für die Mitgliedsbanken. SAFE unterstützte die Banken bei Risikofrüherkennung und Schadensprävention und stellt darüber hinaus Auswertungsdaten zur Verfügung, die auch anderen Präventionsprogrammen als Informationsgrundlage dienen. SAFE wird nun durch "Fraud an Loss Database" abgelöst.

Sales Slip

Der Karteninhaber erhält als Nachweis über seine getätigten Transaktionen einen papierhaften Beleg vom Terminal. Sollte der Karteninhaber einen manuell erstellten Beleg erhalten, so ist dieser von ihm zu unterschreiben. Den Beleg bezeichnet man auch als charge slip, sales draft, oder sales ticket.

Scammer

Ein Scammer ist ein Betrüger. Scamming ("betrügen") wird von zahlreichen Internet-Betrügern durchgeführt.

scan to pay

Bei „Scan to pay“ läuft das mobile Bezahlen mit dem Smartphone über das Scannen eines QR-Codes, der während des Bezahlvorgangs angezeigt wird. Alle Infos zur Zahlung werden daraufhin dargestellt. Zur zusätzlichen Sicherheit bestätigt man jede Zahlung dann noch mit dem eigenen, individuellen Sicherheitscode.

Schlichtungsverfahren bei Reklamation

Wenn die Reklamation nicht auf herkömmlichem Wege (Chargeback Regulations) abgewickelt werden kann, besteht die Möglichkeit, den Sachverhalt unter Vorlage aller Beweismittel in einem Schlichtungsverfahren klären zu lassen.

Schlüsselindikatoren

Bezeichnung für eine Reihe von Indikatoren zur Bewertung der Geschäftsentwicklung in der Kartenindustrie unter Zugrundelegung bestimmter Zeiträume. Indikatoren dieser Art können sein: Anzahl ausgegebener Karten, prozentualer Anteil genehmigter Transaktionen verglichen mit dem Gesamtaufkommen, Anzahl der Rückbelastungsfälle etc.

Screen Scraping

Technik zum gezielten Auslesen von Informationen aus Internetseiten, die im Zusammenhang mit

Kontoinformationen nicht mehr erlaubt ist.

SDA

Ein Sicherheitsverfahren für neue Kartengenerationen mit Chips, das besser vor Missbrauch schützen soll. Bei SDA wird eine Kombination aus festen Kartendaten mit einem RSA-Schlüssel des Herausgebers signiert.

SDP

Zielsetzung von SDP ist die Unterstützung von Händlerbanken, Händlern, Service Providern und anderen externen Dienstleistern beim sicheren Umgang mit sensiblen Karten- und Transaktionsdaten. Das Programm definiert Sicherheitsanforderungen für die Verarbeitung, Speicherung und Übertragung von vertraulichen Informationen. Damit sollen eventuelle Sicherheitslücken in den eigenen Systemen identifiziert und mögliche Folgeschäden abgewendet werden. SDP ist Teil des gemeinsamen Standards PCI.

Secure Chip Card Operating System

Eine von der deutschen Kreditwirtschaft definierte einheitliche Chipkarten-Plattform für Zahlungskarten. SECCOS verfügt über eine ausgereifte Sicherheitsarchitektur, unterstützt den EMV-Standard und ermöglichte eine Multiapplikationsstrategie. Sämtliche in Deutschland ausgegebenen Debitkarten werden mit einem SECCOS-Chip ausgestattet sein.

Secure Electronic Transaction

Ein von Mastercard, Visa und Computer-Herstellern gemeinsam entwickeltes Sicherheitsprotokoll. Es legt fest, wie sensitive Daten in öffentlichen Netzen (Internet) zu verschlüsseln sind. SET diente als Sicherheitsgrundlage für Kartenzahlungsvorgänge im elektronischen Handel (Electronic Commerce), konnte sich jedoch am Markt nicht durchsetzen. Mastercard setzt nun hier Mastercard Secure Code und Visa setzt Verified by Visa ein.

Secure Socket Layer

Das Secure Socket Layer (SSL)-Protokoll ist ein Industriestandard für Datensicherheit und Datenvertraulichkeit bei der Internet-Nutzung. Üblicherweise ist SSL Bestandteil der Internet-Browsersoftware.

SEPA

(Single European Payment Area) heißt übersetzt einheitlicher Euro-Zahlungsverkehrsraum und standardisiert europaweit Verfahren für den bargeldlosen Zahlungsverkehr (Überweisungen, Lastschriften).

Servicegebühr

Gebühr, die der Issuer an den Acquirer zahlt, und zwar für Bargeldverfügungen am GAA oder manuellen Bargeldbezug am Bankschalter. Bilateral und national können Gebühren von den

Mitgliedsbanken untereinander vereinbart werden. Sogenannte 'Fallback'-Gebühren werden von Mastercard festgelegt und veröffentlicht.

SET

Ein von Mastercard, Visa und Computer-Herstellern gemeinsam entwickeltes Sicherheitsprotokoll. Es legt fest, wie sensitive Daten in öffentlichen Netzen (Internet) zu verschlüsseln sind. SET diente als Sicherheitsgrundlage für Kartenzahlungsvorgänge im elektronischen Handel (Electronic Commerce), konnte sich jedoch am Markt nicht durchsetzen. Mastercard setzt nun hier Mastercard Secure Code und Visa setzt Verified by Visa ein.

Settlement

Verfahrensweise zur Herbeiführung des gegenseitigen Zahlungsausgleiches der Issuer- und Acquirer-Banken untereinander für die pro Tag jeweils abgerechneten Kartenumsätze (einschl. Gebühren).

Settlement Bank

Abrechnungs- oder Verrechnungsbank. Eine Bank, bei der das Netto-Abrechnungskonto einer Mitgliedsorganisation geführt und zur Abwicklung von Zahlungsvorgängen mit der jeweiligen Clearing-Bank benutzt wird.

Settlement Date

Datum, zu dem der Zahlungsausgleich zwischen Acquirer- und Issuer-Bank erfolgt.

Shoulder Surfing

Bezeichnung für eine von Betrüger:innen angewandte Technik, Karteninhabern bei der PIN-Eingabe von hinten 'über die Schulter' zu schauen und dabei per Sichtkontakt in den Besitz der PIN zu gelangen.

Sicherheitsanfrage

Einige Prozessoren bieten als Dienstleistung die Überwachung von Transaktionen zur Erkennung von potentiellem Missbrauch. Die verdächtigen Verfügungen werden von einem Expertenteam analysiert und bewertet. Wenn bei Transaktionen der Verdacht auf die missbräuchliche Nutzung einer Karte besteht, wird von dem jeweiligen Dienstleister eine Sicherheitsanfrage an das kartenausgebende Kreditinstitut gestellt. Das Kreditinstitut prüft in Abstimmung mit dem Kunden, ob die Umsätze vom Kunden selbst getätigt wurden. Bewahrheitet sich der Verdacht auf Missbrauch der Karte, sperrt die Bankdas Institut die Karte und erstellt eine Schadensmeldung. Wenn kein Missbrauch vorliegt, gibt das Kreditinstitut eine kurze Stellungnahme an Sicherheitsmanagement für Zahlungskarten.

Sicherheitsmitteilung

Das Sicherheitsmanagement für Zahlungskarten erhält aus verschiedenen Quellen, wie z.B. aus der

Analyse der Transaktionsdaten und Schadensfälle, durch Mitteilungen von Kreditinstituten oder der Polizei Informationen über bereits erfolgte Kartendatenabgriffe an Geldautomaten oder POS-Terminals. Ergibt die Analyse eine Gefahr, dass die ausgelesenen Kartendaten über Kartendubletten missbräuchlich eingesetzt werden könnten, erhalten die Kreditinstitute von dem Sicherheitsmanagement für Zahlungskarten unverzüglich eine Sicherheitsmitteilung. Seit dem 01. Januar 2005 muss zur Verhinderung weiterer Schäden in den vorab beschriebenen Fällen stets eine unverzügliche Sperrung der Karte - auch ohne Rücksprache mit den Kunden – veranlasst werden.

Signature based Transaction

Überprüfung der persönlichen Legitimation des Karteninhabers durch den Händler. Die vom Karteninhaber am Ort der Kartenverfügung geleistete Unterschrift wird mit der im Unterschriftsfeld der Karte vorhandenen Unterschrift auf Übereinstimmung verglichen.

Signature Verification

Vom Händler durchgeführte Maßnahme zur Überprüfung der Legitimation/Identität des Karteninhabers. Dies erfolgt nach Einholung der Umsatzgenehmigung durch Vergleich der vom Karteninhaber auf dem Transaktionsbeleg geleisteten Unterschrift mit der Unterschrift auf der Karte.

Signature-based

Zahlungen mit Karte und Unterschrift sind nicht garantiert und können von der Bank oder Sparkasse oder vom Kunden unbezahlt zurückgegeben werden.

Sim Swapping

Sim Swapping bezeichnet eine Betrugsmethode, bei der Kriminelle die Kontrolle über die Telefonnummer eines Opfers erlangen, indem sie die Mobilfunknummer auf eine neue SIM-Karte übertragen lassen. Dies wird meist durch Social Engineering oder gefälschte Identitätsnachweise beim Mobilfunkanbieter erreicht. Mit der übernommenen Nummer können die Täter dann Zwei-Faktor-Authentifizierungen umgehen und Zugang zu sensiblen Konten und Daten des Opfers erhalten.

SIM-Swap-Betrug

SIM-Swapping ist ein Prozess, bei dem ein Telekommunikationsanbieter die Telefonnummer des Ziels auf eine vom Angreifer gehaltene SIM-Karte überträgt. Sobald sie die Telefonnummer erhalten haben, können Hacker sie verwenden, um die Passwörter der Opfer zurückzusetzen und in ihre Konten einzubrechen

Sinkholing

Sinkholing ist eine Technik zur Umleitung von verdächtigem oder gefährlichem Datenverkehr im Internet zu einem speziellen Server, der als Sinkhole bezeichnet wird. Diese Methode wird hauptsächlich zur Abwehr von Cyberangriffen und zur Analyse von bösartigem Netzwerkverkehr

eingesetzt.

Skimming

Das rechtswidrige elektronische Kopieren des Magnetstreifen-Dateninhaltes einer Karte. Der Betrüger zieht die Karte durch ein von ihm kontrolliertes Magnetstreifen-Lesegerät. Anschließend werden die Kartenfälschungen (auch auf sogenannte 'White Plastic'-Karten) übertragen.

Smart Contract

Sind Transaktionsprotokolle bzw. Programme, die automatisch und permanent - also quasi live - die Bedingungen eines Vertrags kontrollieren und ggf. einzelne Bestimmungen eines Vertrags automatisiert ausführen. Die Kontrolle und Einhaltung basiert dabei auf die den Smart Contracts zu Verfügung gestellten Daten(banken). Mit der automatisierten Abwicklung von Verträgen lassen sich auch immense Kosten einsparen.

Smishing

Smishing setzt sich aus den Worten „SMS" und „Phishing" zusammen und bezeichnet eine Betrugsmasche, bei der versucht wird mittels fingierter SMS, die Daten der Opfer abzugreifen. In den SMS wird dazu aufgefordert, einen schadhaften Anhang zu öffnen, einen Link anzuklicken bzw. eine Telefonnummer anzurufen, die von den Betrügern betrieben werden.

SMS-TAN

Auch mTAN, Mobile TAN oder mobilTAN genannt. Bei diesem digitalen Banking Verfahren wird die geheime Transaktionsnummer per SMS auf das Handy des Nutzers gesandt. Ursprünglich als ein Nachfolger des papiernen iTAN-Verfahrens (umgangssprachlich „TAN-Liste“) von vielen Instituten eingeführt, stellen diese inzwischen zunehmend auf modernere Freigabeprozesse um.

SOC

Ein Information Security Operations Center (ISOC or SOC) ist eine Einrichtung, in der in Unternehmen Informationssysteme (Websites, Anwendungen, Datenbanken, Rechenzentren und Server, Netzwerke, Desktops und andere) überwacht, bewertet und verteidigt werden. Das SOC überwacht auch Anwendungen, um einen möglichen Cyber-Angriff oder Einbruch (Ereignis) zu identifizieren, und stellt fest, ob es sich um eine echte böswillige Bedrohung (Vorfall) handelt und ob sie das Geschäft beeinträchtigen könnte.
Quelle: Wikipedia

Social Engineering

Zwischenmenschliche Beeinflussung mit dem Ziel, an vertrauliche Informationen zu kommen oder ähnlich manipulierte Verhaltensweisen zu bewirken, so dass Finanzmittel freigegeben werden.

Society for Worldwide Interbank Financial Telecommunication

Organisation, die für Banken im internationalen Raum unter anderem grenzüberschreitende Geldüberweisungs-Dienstleistungen anbietet. Am Ende des jeweiligen Abrechnungszyklus erfolgt der Zahlungsausgleich über S.W.I.F.T. auf das Konto von Clearing-Banken der an Transaktionen dieser Art beteiligten Bankinstitute.

Spear-Phishing

Im Gegensatz zum ursprünglichen Phishing, bei dem Massenspam unpersonalisiert versendet werden, werden beim Spear-Phishing die E-Mails mit persönlichen und individuellen Informationen des Adressaten angereichert und von einem E-Mail Account aus versendet, der vertrauenswürdig erscheint. Ziel ist auch hier, Online-Zugangsdaten zu Bankkonten auszuspähen, an Passwörter zu Online-Shops oder -Auktionshäusern zu gelangen oder auch Zugriff auf alle anderen Datenbestände, die auf den Rechnern gespeichert sind, zu erhalten.

Sperrung

Von Sperrung spricht man, wenn eine Karten ausgebende Bank entscheidet, entweder bestimmte Funktionalitäten auf dem Chip oder die Nutzung der Karte an sich zu unterbinden.

Spur

Definierter Bestandteil eines Magnetstreifens zur Aufzeichnung von Daten. Auf Karten mit Zahlungsfunktion befindet sich rückseitig ein Magnetstreifen, der in drei lineare Aufzeichnungsspuren unterteilt ist. Jede einzelne kann mit Daten in definiertem Format belegt werden.

Spurdaten

Auf dem Magnetstreifen hinterlegte Information. Es gibt drei verschiedene Spuren (track 1, track 2 und track 3 Spurdaten).

Spyware

Spähprogramme, um Daten eines Computernutzers heimlich an den Hersteller dieser Schnüffelsoftware zu senden oder das Surfverhalten zu analysieren.

SSL-Sicherheitsprotokoll

Das Secure Socket Layer (SSL)-Protokoll ist ein Industriestandard für Datensicherheit und Datenvertraulichkeit bei der Internet-Nutzung. Üblicherweise ist SSL Bestandteil der Internet-Browsersoftware.

SST (Self Service Terminal)

Self Service Terminal (Selbstbedienungsterminal)

Stakeholder

Eine Person oder Gruppe, die von den unternehmerischen Tätigkeiten gegenwärtig oder in Zukunft

direkt oder indirekt betroffen sind.

Stand-in Authorisation

Autorisierung der Transaktionen durch das Netzwerk der Kartenorganisation im Auftrag einer Issuer-Bank.

Static Data Authentication

Ein Sicherheitsverfahren für neue Kartengenerationen mit Chips, das besser vor Missbrauch schützen soll. Bei SDA wird eine Kombination aus festen Kartendaten mit einem RSA-Schlüssel des Herausgebers signiert.

Storno

Im Autorisierungsverfahren: Elektronische Mitteilung zur vollen oder teilweisen Stornierung einer vorherigen Transaktion, die trotz Issuer-Genehmigung nicht erfolgreich abgeschlossen werden konnte. Im Clearingverfahren: Elektronische Mitteilung zwecks Stornierung einer früheren Transaktionseinreichung.

Substitute Draft

Bezeichnung für ein Dokument in Papierform, das ein Acquirer als 'Ersatz' für einen Kartenumsatzbeleg zur Verfügung stellt. Derartige 'Ersatzbelege' dürfen nur für folgende Transaktionskategorien erstellt werden: Mail Order/Telephone Order, Hotel/Motel, Tankstellen, Parkhäuser, Autovermietungen und Luftfahrtgesellschaften.

Symmetrisches Verschlüsselungsverfahren

Das symmetrische Verschlüsselungsverfahren verwendet im Gegensatz zum asymmetrischen Verfahren für die Ver- bzw. Entschlüsselung nur einen Schlüssel (auch Private Key Verfahren genannt).

system-immanent

System-immanenten Schwachstellen:
Einem technischen System innewohnende Elemente; konkretes Beispiel wäre ein Firmennetzwerk, in dem Endgeräte durch Trojaner kompromittiert werden.

T & E Karte

Diese Karte wird ausgegeben für den internationalen Einsatz und hauptsächlich zur Bezahlung von Reise- und Bewirtungskosten (Travel & Entertainment) eingesetzt. (Beispiel: American Express, Diners Club).

Telefonische Genehmigung

Hierbei handelt es sich um eine Dienstleistung der Acquirer-Banken für ihre Vertragshändler, die im Bedarfsfall das Call Center (Autorisierungszentrale) der Acquirer Bank anrufen, um die

Genehmigung für eine manuell durchzuführende Kartentransaktion einzuholen. Dieser Weg wird auch dann beschritten, wenn das Händlerterminal die Acquirer-Bank wegen einer Systemstörung vorübergehend nicht „online“ zu erreichen ist. Im Telefonat mit dem Call Center der Bank gibt der Händler alle relevanten Transaktionsdaten weiter. Das Call Center schickt sodann eine Genehmigungsanfrage online an die Issuer-Bank und gibt danach bei positiver Antwort den entsprechenden Genehmigungscode dem Händler durch. Diese Codenummer muss vom Händler zwingend auf dem entsprechenden Transaktionsbeleg handschriftlich vermerkt werden.

Terminal

Endgerät zum Versenden und Empfangen elektronischer Daten sowie zur Aktivierung von Funktionen in einem externen Rechnersystem. Im Zusammenhang mit kartengestützten Transaktionen ist ein Terminal (entweder vom Händler betreut oder als Selbstbedienungseinrichtung) am Ort des Karteneinsatzes ('point of interaction') installiert und ermöglicht dem Karteninhaber die Durchführung elektronischer Transaktionen.

Terminal Attrappe

Eine Terminal Attrappe, die aussieht wie ein echtes POS Terminal und ausschließlich dem Zweck dient, Kartendaten und PINs zu Betrugszwecken zu erhalten.

Terminal innerhalb einer Bankfiliale

In-Branch-Terminal: Ein elektronisches Terminal mit Karten-Lesefunktion, das in Bankfilialen installiert ist und für manuelle Bargeldtransaktionen benutzt wird. Beim Einsatz von Kreditkarten unterschreibt der Karteninhaber einen Beleg. Der Bankkassierer vergleicht sodann die Belegunterschrift mit der Kartenunterschrift zur Legitimationsprüfung des Kartenvorlegers. Beim Einsatz von Debitkarten gibt der Karteninhaber seine PIN ein, die von der Issuer-Bank online bzw. offline im Kartenchip geprüft wird.

Terminal mit Chipkartenleser

POS-Terminal, das Chipkarten lesen kann.

Third Party Processing

Bei der Fremdverarbeitung erfolgt die Datenverarbeitung durch ein externes Rechenzentrum.

Throat Inlay Skimming Devices

Der Angriff ist nicht einfach zu erkennen und bleibt oft über einen längeren Zeitraum unbemerkt. Der Lesekopf dieses Gerätetyps Skimmers befindet sich in der „Kehle" des Geldautomaten oder in der rechtmäßigen Lünette und in jedem Fall vor dem Verschluss des Kartenlesers.

Time out Value

Mit 'Time out' wird ein Ereignis beschrieben, bei dem eine Autorisierungsanfrage nicht oder nicht innerhalb der definierten maximalen Antwortzeit beantwortet und die Leitung unterbrochen wird.

Token

Ein Token (oder Security-Token) bezeichnet u.a. eine Hardwarekomponente, in die in der Regel eine Chipkarte eingeführt werden kann, aus der keine Daten herauskopiert oder manipuliert werden können. Der Token kann an einem USB-Port angeschlossen werden und integriert somit die Vorteile einer Smartcard, ohne dabei ein Kartenlesegerät zu benötigen.

Tokenisierung

Tokenisierung - in Bezug auf Datensicherheit - bezeichnet einen Prozess, bei dem vertrauliche oder sensible Originaldaten wie Kreditkarten-, Konto- oder Sozialversicherungsnummern durch Referenzwerte so genannte Tokens - in verschlüsselter Form ersetzt werden. Ziel ist es, diese Daten vor Diebstahl oder Missbrauch zu schützen.Speziell bei Bezahltransaktionen, bei denen die Zahlungskarte nicht physisch präsent ist wie bei NFC-Zahlungen oder im Internet- und Online-Handel - bietet die Tokenisierung die größten Sicherheitsvorteile, lassen Tokens doch keinerlei Rückschlüsse auf die ursprünglichen Daten zu.

TOPP

Das Terminal ohne PIN-Pad ermöglicht kontaktlose Transaktionen mit der girocard über die NFC-Schnittstelle (Near Field Communication) in vielen Einsatzbereichen (Bsp. Automaten, Bäckereien). Es benötigt keinen Einsteckleser und kein PIN-Pad. Transaktionen bis 25 Euro können so ohne PIN schnell und bequem getätigt werden.

Track

Definierter Bestandteil eines Magnetstreifens zur Aufzeichnung von Daten. Auf Karten mit Zahlungsfunktion befindet sich rückseitig ein Magnetstreifen, der in drei lineare Aufzeichnungsspuren unterteilt ist. Jede einzelne kann mit Daten in definiertem Format belegt werden.

track data

Auf dem Magnetstreifen hinterlegte Information. Es gibt drei verschiedene Spuren (track 1, track 2 und track 3 Spurdaten).

Transaction Amount

Die Betragssumme einer Kartentransaktion, ausgedrückt in der Landeswährung der jeweiligen Acquirer-Bank.

Transaction Certificate

Bezeichnung für eine 'elektronische Unterschrift'. Diese generiert im Chip nach erfolgreicher Durchführung die Genehmigung einer Transaktion. Das Kryptogramm ermöglicht dem Issuer die Prüfung, dass der Transaktion eine echte Karte zugrunde lag und kritische Daten (die dem Chip zum Transaktionszeitpunkt zur Verfügung standen und für Risikomanagementzwecke benutzt wurden) nach Erteilung der Transaktionsgenehmigung nicht mehr verändert wurden. In Erweiterung

ihrer Bedeutung bezieht sich die Bezeichnung 'transaction certificate (TC)' auch auf sämtliche Daten, die zur Kalkulation des Kryptogramms benutzt wurden. Das Transaktionszertifikat muss vom Acquirer aufbewahrt und dem Issuer auf dessen Wunsch zur Verfügung gestellt werden. Darüber hinaus kann der Acquirer das Zertifikat auch gleich in der Clearing-Message mitschicken.

Transaction Date

Datum, an dem eine Transaktion durchgeführt wird (= Tag, an dem der Karteninhaber einen Warenkauf und/oder andere Dienstleistung mit der Karte bezahlt oder eine Bargeldverfügung vornimmt).

Transaction Fee

Gebühr, die eine Acquirer-Bank einem Händler für am POS-Terminal durchgeführte Kartentransaktionen belastet.

Transaction Reversal Fraud

Bei der Manipulationsart Transaction Reversal Fraud, kurz TRF, brechen Täter den Geldabhebevorgang zu dem Zeitpunkt ab, an dem der angeforderte Betrag bereits bereitsteht. So wird dem Konto nichts abgebucht und die Täter können das Geld mit Hilfe eines Greifers oder ähnlichem Werkzeug, oder über die Manipulation des Geldausgabeschachtes mit der Hand aus dem Schacht fischen.

Transaktion

Geschäftsvorgang (Kartenverfügung) zwischen Karteninhaber und Vertragshändler oder Karteninhaber und Mitgliedsbank mit Umsatzaktivität auf dem Karteninhaberkonto.

Transaktionsbetrag

Die Betragssumme einer Kartentransaktion, ausgedrückt in der Landeswährung der jeweiligen Acquirer-Bank.

Transaktionsdatum

Datum, an dem eine Transaktion durchgeführt wird (= Tag, an dem der Karteninhaber einen Warenkauf und/oder andere Dienstleistung mit der Karte bezahlt oder eine Bargeldverfügung vornimmt).

Transaktionszertifikat

Bezeichnung für eine 'elektronische Unterschrift'. Diese generiert im Chip nach erfolgreicher Durchführung die Genehmigung einer Transaktion. Das Kryptogramm ermöglicht dem Issuer die Prüfung, dass der Transaktion eine echte Karte zugrunde lag und kritische Daten (die dem Chip zum Transaktionszeitpunkt zur Verfügung standen und für Risikomanagementzwecke benutzt wurden) nach Erteilung der Transaktionsgenehmigung nicht mehr verändert wurden. In Erweiterung ihrer Bedeutung bezieht sich die Bezeichnung 'transaction certificate (TC)' auch auf sämtliche

Daten, die zur Kalkulation des Kryptogramms benutzt wurden. Das Transaktionszertifikat muss vom Acquirer aufbewahrt und dem Issuer auf dessen Wunsch zur Verfügung gestellt werden. Darüber hinaus kann der Acquirer das Zertifikat auch gleich in der Clearing-Message mitschicken.

Trojaner

Trojaner sind schädliche Programme, die von Hackern oder Computerkriminellen über infizierte E-Mails oder Websites auf den Computer ihrer Opfer geladen werden. Dort spähen diese Programme persönliche Identifikationsnummern (PINs) und Transaktionsnummern (TANs) zum Beispiel beim Online-Banking aus. Die meisten Trojaner sind auf Bankbetrug ausgerichtet. Schutz vor Trojanern bieten regelmäßige Software-Updates, Antivirenprogramme und Firewalls.

Truncation

Bei der Transaktionsdurchführung erlangte Informationen werden nicht oder nur teilweise auf Belegen ausgedruckt. Beispiel: Mastercard schreibt vor, dass GAA-Quittungsbelege die Kartennummer nur in verkürzter Form enthalten dürfen. Auch viele Händler gehen dazu über, die Terminals so zu programmieren, dass die Kartennummer beim Quittungsbeleg nicht mehr vollständig ausgedruckt wird. Auf diese Weise kann verhindert werden, dass Betrüger durch weggeworfene Belege, z.B. aus dem Papierkorb, in den Besitz gültiger Kartendaten gelangen.

UEBA

Die Analyse des Benutzer- und Entitätsverhaltens (User and Entity Behaviour Analytics, UEBA) ist ein Cyber-Sicherheitsprozess, der das normale Verhalten der Benutzer zur Kenntnis nimmt und im Gegenzug jedes anomale Verhalten oder Fälle, in denen es Abweichungen von diesen "normalen" Mustern gibt, erkennt. Das UEBA setzt maschinelles Lernen, Algorithmen und statistische Analysen ein, um zu wissen, wann es eine Abweichung von den etablierten Mustern gibt.

Umlagegebühr

Bezeichnet den Zahlungsbeitrag einer Mitgliedsbank an die das Zahlungssystem betreibende Verbundorganisation zur Wahrnehmung gemeinschaftlicher Steuerungs-, Management- und Sicherheitsaufgaben.

Umrechnungsdatum

Das Datum, zu dem ein Betrag (Kartenumsatz) von einer Währung in eine andere umgerechnet wird, und zwar unter Verwendung des für Transaktionen dieser Art zutreffenden und an diesem Tag gültigen Umrechnungskurses.

Umsatzrückbelastung

Rückbelastung eines Kartenumsatzes an den Acquirer durch die Issuer Bank. Das Verfahren wird angewandt, wenn ein bereits abgerechneter Umsatz vom Karteninhaber aus Gründen reklamiert oder bestritten wird, für die ein Rückbelastungsrecht vorgesehen ist. Der Begriff 'chargeback' bezeichnet auch den die Rückbelastung bewirkenden elektronischen Datenaustausch zwischen

Issuer-Bank und Acquirer-Bank.

Umschaltung auf Magnetstreifen

Umschaltung auf Magnetstreifentechnologie als Ersatzlösung bei Chip-Funktionsausfall.

Unauthorised Transaction

Eine Transaktion, die von der Karten ausgebenden Bank nicht genehmigt wurde.

Unique Merchant Identification System

Jede Akzeptanzstelle erhält von ihrem Acquirer eine einmalige Vertragsnummer zugewiesen. Dieses System erlaubt die weltweite Identifizierung jeder einzelnen Akzeptanzstelle.

Unterlizenz

Mitgliedsinstitut mit Unterlizenz eines Hauptlizenzinhabers (z.B. Kartenorganisation). Unter lizenzrechtlicher Verantwortlichkeit des Hauptlizenzinhabers kann sich der Unterlizenznehmer als Issuer und/oder Acquirer betätigen.

Unterschrift basierte Transaktion

Überprüfung der persönlichen Legitimation des Karteninhabers durch den Händler. Die vom Karteninhaber am Ort der Kartenverfügung geleistete Unterschrift wird mit der im Unterschriftsfeld der Karte vorhandenen Unterschrift auf Übereinstimmung verglichen.

Unterschriftsprüfung

Vom Händler durchgeführte Maßnahme zur Überprüfung der Legitimation/Identität des Karteninhabers. Dies erfolgt nach Einholung der Umsatzgenehmigung durch Vergleich der vom Karteninhaber auf dem Transaktionsbeleg geleisteten Unterschrift mit der Unterschrift auf der Karte.

UPT

Unattended Payment Terminal/Unbeaufsichtigtes Zahlungsterminal

User Interface

Das User Interface stellt eine Art "Schnittstelle" zwischen Mensch (User) und Maschine dar. Das UI unterstützt den User beim Kontrollieren von Soft- und Hardware.

UTP

Unattended Payment Terminal - Ein unbeaufsichtigtes Zahlungsterminal (UPT) ist ein Selbstbedienungsgerät, bei dem der Karteninhaber Kartenzahlungen leisten kann, z.B. an Tankstellen.

V Pay

V PAY ist das ChipPIN-basierte Debitverfahren von Visa Europe, das POS-Zahlungen und

Geldbezug am Geldautomaten in ganz Europa ermöglicht.

Vending

Der Begriff leitet sich aus dem Lateinischen ab (vendere: verkaufen, veräußern) und steht für den Verkauf von Waren und Dienstleistungen am Automaten.

Verdächtige Akzeptanzstelle

Eine Akzeptanzstelle, bei der der Verdacht besteht, dass Karteninhaberdaten ohne Kenntnis des Karteninhabers unrechtmäßig verwendet wurden, z.B. durch Kopieren des Magnetstreifen-Dateninhalts zur Erstellung von Kartendubletten ('White Plastic'). Im Debit-Bereich wird hierfür die Bezeichnung 'point of compromise' oder 'POC' verwendet.

Verfahren zur Kartenechtheitsprüfung

Verfahren zur Prüfung der Echtheit einer Karte. Bei Kreditkarten mit Magnetstreifen schließt dies auch das Vorhandensein eines Hologramms ein, das vom Händler durch Augenschein überprüft wird. Die Echtheitsprüfung der verschlüsselten Daten im Magnetstreifen erfolgt durch den Issuer. Im Falle von Chipkarten mit verschlüsselten Daten im Chip erfolgt die Echtheitsprüfung durch das Chipterminal oder ebenfalls beim Issuer.

Verfahren zur Legitimationsprüfung von Karteninhabern

Verfahren zur Feststellung der persönlichen Legitimation eines Karteninhabers. Hierzu zählen z.B. Unterschriftsvergleiche und PIN-Prüfung; künftig können auch biometrische Prüfungsverfahren zur Anwendung kommen.

Verfallsdatum

Bezeichnet allgemein das auf einer Zahlungskarte aufgedruckte oder aufgeprägte sowie auch im Magnetstreifen und Chip gespeicherte Gültigkeitsdatum (Monat und Jahr). Ab diesem Datum verliert die Karte ihre Gültigkeit und darf vom Karteninhaber nicht mehr für Einkäufe oder Bargeldverfügungen eingesetzt werden. Dem Händler ist es ab diesem Datum untersagt, die abgelaufene Karte weiterhin zu akzeptieren.

Verfügungsrahmen Kreditkarte

Die Ausstellerbank räumt dem Inhaber einer Kreditkarte oder Charge Card pro Abrechnungszyklus einen maximalen Verfügungsrahmen ein. Die Höhe des Rahmenbetrages bestimmt die Bank und sie richtet sich individuell nach der Bonität und der Kontohistorie des Karteninhabers.

Verhaltens-Scoring

Beobachtung des Karteneinsatzes im Hinblick auf aus dem Rahmen fallenden Transaktionen. Verhaltens-Scoring ist eine Methode zur Betrugsbekämpfung. Es wird überprüft, inwieweit sich der gegenwärtige Karteneinsatz eines Karteninhabers bezogen auf die Transaktionen im Widerspruch zu seinem bisherigen Karteneinsatz befindet.

Verkaufspunkt

Der tatsächliche Ort, an dem der Karteninhaber einen Kauf tätigt und mit der Karte bezahlt. Es handelt sich typischerweise um ein Ladengeschäft eines Vertragshändlers.

Verrechnung

Verfahrensweise zur Herbeiführung des gegenseitigen Zahlungsausgleiches der Issuer- und Acquirer-Banken untereinander für die pro Tag jeweils abgerechneten Kartenumsätze (einschl. Gebühren).

Verrechnungsbank

Abrechnungs- oder Verrechnungsbank. Eine Bank, bei der das Netto-Abrechnungskonto einer Mitgliedsorganisation geführt und zur Abwicklung von Zahlungsvorgängen mit der jeweiligen Clearing-Bank benutzt wird.

Verrechnungsdatum

Datum, zu dem der Zahlungsausgleich zwischen Acquirer- und Issuer-Bank erfolgt.

Versandhandel

Eine Art des Einzelhandels (auch als Distanzhandel bezeichnet), bei dem die Produkte per Katalog, Prospekt, Internet, Fernsehen oder Vertreter angeboten werden. Die Bestellung der gewünschten Produkte kann mündlich (z. B. per Telefon oder Vertreter), schriftlich (z. B. per Brief oder Fax) oder auch online getätigt werden. Die anschließende Bezahlung kann per Kreditkarte, Nachnahme, Vorabüberweisung oder auch auf Rechnung erfolgen. Die Bonität des Kunden kann das Versandunternehmen vorab bei bestimmten Auskunfteien erfragen.

Verschlüsselung

Verfahrenstechnik zur Verschlüsselung von Daten mittels eines algorithmischen Rechenvorgangs und einem Schlüssel(wert).

Vertragsnummernsystem

Jede Akzeptanzstelle erhält von ihrem Acquirer eine einmalige Vertragsnummer zugewiesen. Dieses System erlaubt die weltweite Identifizierung jeder einzelnen Akzeptanzstelle.

Visa Account Information Security

Zielsetzung von AIS ist die Unterstützung von Händlerbanken, Händlern, Service Providern und anderen externen Dienstleistern beim sicheren Umgang mit sensiblen Karten- und Transaktionsdaten. Das Programm definiert Sicherheitsanforderungen für die Verarbeitung, Speicherung und Übertragung von vertraulichen Informationen. Damit sollen eventuelle Sicherheitslücken in den eigenen Systemen identifiziert und mögliche Folgeschäden abgewendet werden. AIS ist Teil des gemeinsamen Standards PCI.

VisaNet

Processing-System von Visa Europe, das in Europa betrieben wird und das weltweite Transaktionen abwickelt. Eigentümer des Processing-Systems sind die Mitgliedsbanken von Visa Europe.

Vishing

Vishing setzt sich aus den Worten „Voice" und „Phishing" zusammen und bezeichnet eine Betrugsmasche, bei der versucht wird, mittels fingierter Anrufe an Daten der Opfer zu gelangen (bspw. an Passwörter oder Kreditkartendaten). Neben der Herausgabe der Daten versuchen die Betrüger dabei häufig auch die Opfer in dem Gespräch zu Geldüberweisungen zu verleiten.

Visuelle Datenausspähung

Bezeichnung für eine von Betrügern angewandte Technik, einem Karteninhaber bei der PIN-Eingabe von hinten 'über die Schulter' zu schauen und dabei per Sichtkontakt in den Besitz der PIN zu gelangen.

voice authorization

Hierbei handelt es sich um eine Dienstleistung der Acquirer-Banken für ihre Vertragshändler, die im Bedarfsfall das Call Center (Autorisierungszentrale) der Acquirer Bank anrufen, um die Genehmigung für eine manuell durchzuführende Kartentransaktion einzuholen. Dieser Weg wird auch dann beschritten, wenn das Händlerterminal die Acquirer-Bank wegen einer Systemstörung vorübergehend nicht „online“ zu erreichen ist. Im Telefonat mit dem Call Center der Bank gibt der Händler alle relevanten Transaktionsdaten weiter. Das Call Center schickt sodann eine Genehmigungsanfrage online an die Issuer-Bank und gibt danach bei positiver Antwort den entsprechenden Genehmigungscode dem Händler durch. Diese Codenummer muss vom Händler zwingend auf dem entsprechenden Transaktionsbeleg handschriftlich vermerkt werden.

Vorauszahlung

Allgemeine Bezeichnung für Zahlungsprodukte, bei denen das Konto des Karteninhabers schon vor der eigentlichen Produktnutzung belastet wird. Beispiel: elektronische 'Geldbörse'. Zahlungsprodukte dieser Kategorie werden auch als 'pre paid products' bezeichnet.

Vorautorisierung

Von der Acquirer-Bank bei der Issuer-Bank eingeholte 'Vorab'-Genehmigung über die voraussichtliche Höhe eines Kartenumsatzes, der erst zu einem späteren Zeitpunkt abgerechnet wird. Dieses Verfahren ist typischerweise in Händlerkategorien wie Hotels, Autovermietungen und bei ähnlichen Vertragsunternehmen anzutreffen. Hierdurch ist gewährleistet, dass für die erst später erfolgende Umsatzabrechnung ausreichend Mittel auf dem Kartenkonto verfügbar sind.

Währungsumrechnung

Umrechnung der Transaktionswährung in die Abrechnungswährung der Kartenausstellerbank. Dies erleichtert den Datenaustausch im Autorisierungs-, Clearing- und Settlement- Verfahren. Im

EPS-Netz und BankNet (Mastercard) oder VisaNet (Visa) ist die automatische Währungsumrechnung integraler Bestandteil beim Austausch von Autorisierungs-, Clearing- und Settlement-Daten.

Waiver

Ausnahmegenehmigungen

Wechselkurs

Der Kurs, zu dem Beträge von einer Währung in eine andere umgerechnet werden.

Weltweite Leistungsstandards

Diese Leistungsstandards sind von Mastercard definierte Standards zur Erhöhung des Leistungsniveaus von Mastercard- und Maestro-Karten. Sie beziehen sich auf Schlüsselbereiche wie Akzeptanz, Autorisierung, Clearing und Chargebacks. Mastercard überwacht die Einhaltung der Standards.

WERO

Wero ist der europäische Echtzeit-Zahlungsdienst der European Payment Initiative EPI. Als Anwendung für P2P-Transaktionen ist Wero im Juli 2024 gestartet; sukzessive Erweiterungen für E-Commerce und POS folgen. Wero ist mit dem Girokonto gekoppelt und ohne Einrichtung sofort nutzbar.

White Plastic

Es handelt sich um weiße Plastikkarten, die nur mit einem Magnetstreifen versehen sind. Täter bringen auf diese Blankokarten häufig die Daten von Echtkarten auf (-> Skimming = Auslesen eines Magnetstreifens einer Echtkarte) und setzen diese Karten betrügerisch ein.

Whitelisting

In der Informationstechnik bezeichnet Whitelisting eine Auswahl von Datensätzen als Positivliste. Diese Ausnahmeliste dient als Sammlung von Angaben, die durch ihren Verfasser als vertrauenswürdig eingestuft wurden. Im Gegensatz zu einer schwarzen Liste bzw. Blacklist oder Negativliste, die als Werkzeug in der digitalen Kommunikation dazu genutzt wird, nicht vertrauenswürdige Elemente zusammenzufassen.

WinPot

Eine neue Form von ATM Malware, die auf die Anzahl der Banknoten im Geldautomaten Einfluss nimmt.

ZAG

Zahlungsdiensteaufsichtsgesetz

Zahlungsdiensterichtlinie

Eine EU-Richtlinie der Europäischen Kommission, man spricht auch von der PSD2 (Payment Services Directive 2)
(Richtline 2015/2366/EU vom 25.11.2015), umgesetzt in deutsches Recht durch Gesetz vom 17.07.2017 (BGBl I 2017, 2446), in Kraft seit 13.01.2018.

Zahlungskarte

Karte, die vom Karteninhaber zur Bezahlung von Waren und Dienstleistungen sowie zum Bargeldbezug eingesetzt werden kann.

Zahlungssystem

Allgemeiner Oberbegriff für Systeme, die der Wahrnehmung von Aufgaben im Zahlungsverkehr dienen.

Zentrale Debit-Schadensbekämpfung

1983 beschlossen die Spitzenverbände der deutschen Kreditwirtschaft, eine eigene Zentralstelle zur Schadensbekämpfung (Zentrale Debitschadensbekämpfung, ZDS) im eurocheque-Bereich aufzubauen (zu dieser Zeit angesiedelt innerhalb der GZS Gesellschaft für Zahlungssysteme mbH, die 1982 durch die Zusammenführung der EUROCARD Deutschland und der DEZ Deutsche eurocheque Zentrale entstanden war). 1997 betraute die deutsche Kreditwirtschaft die EURO Kartensysteme mit dem Sicherheitsmanagement und der Sicherheitswerbung im kartengestützten Zahlungsverkehr.

Zentraler Kreditausschuss

Ehemaliger Name von Die Deutsche Kreditwirtschaft.

Zentralrechner

Ein mit einem Netzwerk verknüpfter Zentralrechner. Er erfüllt als EDV-Server die Anforderungen aller Netzwerkteilnehmer. Im Allgemeinen ist mit dem Begriff 'host' das interne Computer-System einer Mitgliedsbank (im Sinne von 'acquirer host', 'issuer host' oder 'member host') gemeint als einer der Endpunkte in der Kommunikation mit den Netzwerken der Kartenorganisationen.

Zero Floor Limit

Herabsetzung des genehmigungsfreien Höchstbetrages (floor limit) beim Händler pro einzelnen Kartenumsatz auf 'Null' für bestimmte Transaktionsarten. Die Maßnahme verpflichtet den Händler (oder die Acquirer-Bank) zur Durchführung einer Genehmigungsanfrage (online oder telefonisch) bei der Issuer-Bank unabhängig von der Betragshöhe. Für Geldausgabeautomaten (ATM) gilt grundsätzlich ein zero floor limit.

Zertifizierung

Dieser Vorgang dient zur Datenverschlüsselung auf der Basis so genannter öffentlicher

Verschlüsselungsverfahren. Hierbei handelt es sich um die digitale Zuordnung eines 'öffentlichen Schlüssels'. Der Eigentümer übergibt diesen einer hierzu ermächtigten Zertifizierungsstelle zur digitalen Signierung. Das Resultat wird dem Eigentümer in Form eines 'public key certificate' wieder zurückgesandt

ZKA

Ehemaliger Name von Die Deutsche Kreditwirtschaft.

Zwei-Faktor-Authentifizierung

Durch die europäische Zahlungsdiensterichtlinie „PSD2“ sind Händler:innen und Zahlungsdienstleister:innen zur sogenannten „Starken Kundenauthentifizierung“ bei Online-Zahlungen verpflichtet. Bis auf vom Gesetzgeber definierte Ausnahmen müpssen Herausgeber:innen von Karten zum Schutz vor Missbrauch sicherstellen, dass bei der Authentifizierung zwei von drei Faktoren erfüllt werden: Besitz (z. B. Karte, Handy), Wissen (z. B. PIN) oder Inhärenz wie etwa biometrische Eigenschaften (z. B. Fingerabdruck).