Glossar kartensicherheit.de

Stand: Juni 2012

-A- 2
-B- 5
-C- 8
-D- 12
-E- 15
-F- 20
-G- 21
-H- 24
-I- 26
-J- 28
-K- 28
-L- 32
-M- 34
-N- 37
-O- 39
-P- 41
-Q- 44
-R- 45
-S- 47
-T- 52
-U- 55
-V- 57
-W- 60
-X- 61
-Y- 61
-Z- 61

-A-

Ablehnung | Decline

Negative Antwort auf eine Autorisierungsanfrage: Die Kartenausstellerbank bzw. deren Prozessor lehnt den angefragten Umsatz ab.

Abrechnung, Verrechnung | Settlement

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

Abrechnungsdaten | 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.

Abschneiden von Daten | 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.

Acquirer

Vertragsunternehmensabrechnende Bank.

AIS | 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.

Akzeptanz | Acceptance

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

Akzeptanznetz | (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.

Akzeptanzstelle | 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.

Allianzverträge | Alliance agreements

Allianzverträge zwischen Europay und MasterCard. Diese regeln das partnerschaftliche Management der beiden globalen Zahlungssysteme Debit und Kredit.

Antwortzeit | Response Time

Zeit, die zur Beantwortung einer elektronischen Anfrage benötigt wird.

Applikationskryptogramm | Application Authentication Cryptogram

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

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)

Aufforderung zur Kontaktaufnahme | 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.

Austausch von Abrechnungsdaten | Clearing

Verfahren des elektronischen Austauschs von Kartenumsatzdaten zwischen der Händlerbank und dem Karten ausgebenden Institut.

Authentifizierung | Authentification

Legitimation des Kunden bei der Bezahlung durch seine Unterschrift oder PIN-Eingabe.

Autorisierte Zertifizierungsinstanz | 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.

Autorisierung | Authorisation

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 | 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).

-B-

BIN | Bankidentifikationsnummer | Bank Identification Number

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)

Bargeldabhebung | 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.

Bargeldbeschaffung | Cash Disbursement

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

Beitragsgebühr | Assessment Fee

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

Betrügerischer Kartenantrag | 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.

Betrügerischer Karteneinsatz | 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.

Betrügerischer Vertragshändler | Collusive Merchant

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

Betrugsbekämpfung

Die Betrugsbekämpfung im Zusammenhang mit Kartenmissbrauch oder Kartenfälschungen gewinnt nicht nur in Deutschland, sondern weltweit zunehmend an Bedeutung. Die EURO Kartensysteme (EKS), ein Gemeinschaftsunternehmen der deutschen Kreditwirtschaft, widmet sich dieser Aufgabe besonders intensiv. So steht die Betrugsbekämpfung im Fokus des Geschäftsfelds „Sicherheitsmanagement für Zahlungskarten“ der EKS. Ein besonderes Augenmerk legt die EKS hierbei auf ein funktionierendes Netzwerk mit Instituten und kreditwirtschaftlichen Verbänden, der Kartenindustrie, der Polizei und den Staatsanwaltschaften. Denn: Die Organisation in der Betrugsbekämpfung muss besser und schneller werden als die organisierte Kriminalität. Intensive Aufklärung und Information sowie ein gut funktionierendes Netzwerk sind unverzichtbare Bestandteile der Betrugsbekämpfung – auch auf internationaler Ebene. Prävention geschieht nicht nur durch Technik und technische Rahmenbedingungen, sondern zu einem großen Teil auch durch verhaltensbedingte Maßnahmen.

Grundlage eines gesicherten Zahlungssystems bilden Rahmenbedingungen wie Spezifikationen (z.B. PIN-Verarbeitung, Verschlüsselung, EMV, Geldautomat, POS Terminal), Zulassungs- und Überprüfungsverfahren, Rules & Regulations von MasterCard und Visa sowie gesetzliche Vorgaben und deren stetige Überprüfung und Anpassung. Diese werden zum Teil in der Deutschen Kreditwirtschaft (DK) und/ oder gemeinsam mit den Kartenorganisationen in den entsprechenden Gremien sowie innerhalb nationaler EU- Gremien behandelt und größtenteils von diesen festgelegt.

Biometrische Identifizierungsverfahren | Biometrics

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

Blankokarten | 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.

Branche | Merchant Category

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

Brand Mark | Markenzeichen

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

Brand | Marke (Produktmarke)

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

-C-

Cardholder activated terminal | CAT | 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.

Cardholder verification method | CVM | 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.

Card-Not-Present-Environment | CNP

Eine Umgebung, bei der Transaktionen unter den folgenden Bedingungen getätigt werden: Der Karteninhaber ist nicht 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 Personalisation | 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.

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.

CAT | Cardholder-activated-Terminal

siehe Cardholder-activated-Terminal

CAT-Transaktionen

Hierbei sind zwei Arten zu unterscheiden:

1. CAT 1 sind autorisierte Transaktionen mit PIN als CVM (Card Verification Method - online oder offline). Magnetstreifen-Transaktionen benötigen eine online Autorisierung mit PIN, um als CAT 1 zu gelten.

2. CAT 2 sind autorisierte Transaktionen (online oder offline) ohne PIN als CVM. Magnetstreifen-Transaktionen müssen online ohne CVM autorisiert werden um als CAT 2 Transaktionen zu zählen.

Chargeback | 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.

Chargeback Zeitraum | Chargeback Period

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.

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.

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.

CDA | Combined Data Authentification

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 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 zwingend vor.

Chipkarte | Chip Card

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 | Chip Card Transaction

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

Clearing

Clearing beschreibt die Abwicklung der Zahlung (Belastung und Gutschrift des Zahlungsbetrages).

Co-branded Karte | Co-branded Card

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.

CPP | common purchase point

(Identifizierung eines Händlers als gemeinsame Karteneinsatz-Schnittstelle)
Begriff zur Bezeichnung einer Vertragshändlerstelle, bei der der Verdacht besteht, dass Kartendaten ohne Kenntnis des Karteninhabers kompromittiert wurden (z.B. durch Kopieren der Magnetstreifendaten zur Erstellung einer Kartendublette) – siehe auch POC (Point of Compromise).

Counterfeit-Fall

Totalfälschen/Duplizieren einer Originalkarte (Debit oder Kredit)

Cross-Border Debit Processing

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

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

Siehe Cardholder verification method.

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 allein nicht für betrügerische Zwecke über Internet oder Mailorder missbraucht werden können.

-D-

3D Secure

3D Secure ist ein Sicherheitsstandard für Online-Händler, der von MasterCard und Visa gemeinsam entwickeltet 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 Karteninhabern, sich während des Bezahlvorgangs mit einem persönlich vergebenen Passwort zu authentifizieren. Mit der Einführung des Sicherheitsstandards geht eine Haftungsumkehr („Liability Shift“) einher, womit ein vom Kunden reklamierter E-Commerce-Umsatz nicht mehr dem Händler zurückgegeben werden kann, wenn dieser die 3D Secure -Technologie unterstützt.

Data Encryption Standard | Data Encryption Standard

DES – 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.

DCC | 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. Dies geschieht direkt an der Händlerkasse (POS) bevor der Händler den Kaufbetrag zur Autorisierung einreicht. Die Software des POS-Terminals erkennt automatisch anhand der Kartennummer das Herkunftsland der vorgelegten Karte und bietet das Bezahlen in der jeweiligen Währung an. Der tagesaktuelle Kurs der Währung wird täglich neu und automatisch an das Terminal übertragen und auf dem Terminal-Beleg ausgewiesen. Der Karteninhaber findet den von ihm unterschriebenen Betrag auf seinem Abrechnungsbeleg und der Händler erhält den Original-Transaktionsbetrag wie gewohnt in Euro.

DDA | Dynamic Data Authentication

Die Abkürzung DDA steht für "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 zwingend vor.

Debitkarte | Debit Card

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

Die Deutsche Kreditwirtschaft

In der Deutschen Kreditwirtschaft (DK) sind die fünf Spitzenverbände (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.

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.

Dienstleistungsunternehmen | 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, Transaktionsprocessing, Kartenversand.

Disagio | Commission Rate

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

Duale Händlervertragsbank | 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.

Dualer Kartenherausgeber | Dual Issuer

Eine Kartenausgebende Bank oder Sparkasse, die sowohl MasterCard als auch Visa Karten ausgibt.

Dublette | White plastics

Siehe Kartenfälschung.

-E-

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. Über die EPCS, European Payment Card Solution GmbH, eine im Oktober 2007 gegründete 100%ige Tochtergesellschaft der EURO Kartensysteme GmbH, sind die deutschen Systeme an der Brüsseler EAPS-Gesellschaft mit insgesamt 30% beteiligt. Weitere Informationen zur EAPS unter **http://www.card-alliance.eu**

EAST | European ATM Security Team

EAST wurde Anfang 2004 als freiwilliger Verbund zur Bekämpfung der Kartenkriminalität in Europa gegründet. Die Mitglieder setzen sich aus Vertretern der Kreditwirtschaft (wie beispielsweise die 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.

ECCF | 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.

Echtheitsprüfung | Authentication

Es handelt sich um ein 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 verwandt, 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.

Echtzeit | Real-time

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

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 | Gateway

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

Einreichung von Transaktionsdaten | Presentment

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

Einreichungsgebühr | 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.

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.

Elektronische Geldbörse | Electronic Purse

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 | Electronic Funds Transfer

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

Elektronisches Warnmeldungsbulletin | Electronic Warning Bulletin

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.

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.

EMV

Europay, MasterCard, Visa = EMV
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 EMV-Chip ist ein technischer Sicherheitsstandard für die Kommunikation zwischen Chipkarte und Terminal (POS und Geldautomat) zur Abwicklung von Debit- oder Kreditkarten-Transaktionen. Der Chip auf der Karte ermöglicht es, die im Chip

gespeicherten Daten gegen Verfälschung und auch gegen Kopieren zu schützen. Es gibt zwei Varianten des Chips - DDA und SDA.

EPC | European Payments Council

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

EPC-Sichtschutz

Der European Payments Council, ein Zusammenschluss europäischer Banken, hat im März 2009 einen Standard für neu zuzulassende Sichtschutzgeräte an Geldautomaten und POS-Terminals verabschiedet. Demnach sollen nicht mehr nur die numerischen Tasten zur PIN-Eingabe, sondern auch sämtliche Funktionstasten der Tastaturen vor unerwünschten Blicken geschützt werden. Der Standard leistet nicht nur konkrete Umsetzungshilfe für Gerätehersteller, er dokumentiert auch die umfassende Sicherheitsstrategie des EPC zur Erhöhung der Sicherheit kartenbasierter Systeme.

EPS-Net

Eigenes Telekommunikationsnetz von MasterCard für den in "Echtzeit " erfolgenden Austausch von Transaktionsdaten zwischen den Mitgliedsinstituten.

Ersatzautorisierung (1) | Stand-in Authorisation

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

Ersatzautorisierung (2) | 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.

Ersatzautorisierungsservice | 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.

Ersatzbeleg | 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.

Erweiterte Parameter für Kontonummernbereiche | 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.

ESM

"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.

Europay Module (EM)

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.

Evidenzzentrale | 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.

expressPay

expressPay heißt die kontaktlose Zahlungstechnologie von American Express. Mit der Kreditkarte auf Basis der Near Field Communication-Technologie (NFC) können Kleingeldbeträge von 20 bis 25 Euro 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.

-F-

Face to Face Transaktion | Face-to-Face Transaction

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

Fallback to magnetic Stripe | Umschaltung auf Magnetstreifen

Umschaltung auf Magnetstreifentechnologie als Ersatzlösung bei Chip-Funktionsausfall.

Firmenkarte (1) | 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.

Firmenkarte (2) | 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.

Fremdverarbeitung | Third Party Processing

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.

-G-

GA/GAA
Ein vom Karteninhaber selbst zu bedienender Geldausgabeautomat (GAA).

Gateway | Eingangstor-Netzwerk
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.

Geldautomat | GA / ATM
Ein Automat zur Ausgabe von Bargeld mittels Karte und PIN. Auch automated teller machine (ATM) genannt.

Genehmigung | 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.

Genehmigungsfreier Höchstbetrag | 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.

Genehmigungsnummer | 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.

Geschäftsbedingungen | Disclosure

Allgemeine Geschäftsbedingungen einer Karten ausgebenden Bank für die Karteninhaber.

Gesperrte Karte | Hot Card

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

girocard

girocard ist der übergeordnete und neutrale Rahmen der deutschen Kreditwirtschaft für das bewährte Debit-Zahlungssystem electronic cash am POS und das Deutsche Geldautomatensystem und garantiert den stets sicheren und einfachen Einsatz von Debitkarten unter Verwendung der persönlichen Geheimzahl (PIN, Personal Identification Number). girocard erleichtert vor allem die internationale Akzeptanz der deutschen Debitkarten durch die Schaffung eines einheitlichen Logos für den SEPA-Raum.

Gleichbehandlungsklausel | Non-Discrimination Rule (NDR)

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.

Grenzüberschreitende Akquisition | Central Acquisition

Grenzüberschreitendes Vertragsunternehmensgeschäft mit zentraler Abrechnung.

Grenzüberschreitende Kartenausgabe | Cross Border Issuing

Karteninhaber und Karten ausgebende Bank befinden sich in unterschiedlichen Ländern.

Grenzüberschreitendes Karteninhabergeschäft mit zentraler Abrechnung| Central Issuing

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

Grenzüberschreitende Transaktion | Cross Border Transaction

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

Grenzüberschreitendes Vertragsunternehmensgeschäft | Central Acquiring

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

-H-

HBCI | HomeBanking Computer Interface

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

Hacker

Eine Person, die sich unerlaubten Zugang zu Computerdateien verschafft.

Handelsgeschäfte zwischen Unternehmen | Business-to-Business Commerce

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

Händlerkarte | Retailer Card

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

Händlervertrag | Merchant Agreement

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

Händlervertragsbank | Acquirer

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

Hochprägung | Embossing

Prägung der Plastikkarten mit den erforderlichen Daten.

Hologramm | Hologram

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

Host-Computersystem | 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.

Hybrid Karte | Hybrid Card

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.

-|-

ICA:

Interbank Card Association; Kennung der Mitglieder des Europay- / MasterCard-Verbunds.

ICC

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

INET (MasterCard's 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.

Inlandstransaktion | Domestic Transaction

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

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 | Interchange Fee

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

Interoperabilität | Interoperability

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.

IRIS | 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.

Issuer Authentifizierungsdaten | Issuer Authentication Data

Genehmigungsdaten der Karten ausgebenden Bank

Issuer Netzzugangspunkt | Issuer Access Point

Technische Einrichtung, die dem 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.

-J-

JCB

Ein internationales Kartensystem welches das Issuing und Acquiring selbst durchführt.

-K-

Karten ausgebende Bank | 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.

Kartenechtheitsprüfung EMV | 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.

Karteneinsatzdatei | 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.

Karteneinsatzort | Point of Interaction / Point of Sale

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

Kartenfälschung (1) | 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.

Kartenfälschung (2) | 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.

Karteninhaber | Cardholder

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

Karteninhaber Legitimationsprüfung | Cardholder Verification Method

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

Kartenleistungsbeleg | 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.

Kartenpersonalisierung | 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.

Kartenprüfnummer | Card Verification Code (CVC2) bei MasterCard - Card Verification Value (CVV2) bei Visa International

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 | 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.

Kontonummer | Account Number

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

Kontostandsabfrage | Balance Inquiry

Kontostandsabfrage eines Karteninhabers am Geldautomat.

Kreditwürdigkeitsprüfung | Credit Scoring

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 | Pay Later

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

Kryptogramm | Cryptogram

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.

Kundenkarte | Private Label Card

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

-L-

Lade-Transaktion | 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.

Ländercode | 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.

Lastschrift | Direct Debit

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

Lebanese Loop | Libanesische Schlinge

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.

Liability Shift | 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.

Lizenzgebühr | Licence Fee

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

Lizenzvertrag | Licence Agreement

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.

Logo | Piktogramm

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

-M-

Maestro

Debit-Zahlungssystem von Maestro International. Ermöglicht den zugelassenen Karten den weltweiten elektronischen Einsatz an Geldautomaten und in Geschäften.

mag-stripe | 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.

Manuelle Transaktion | Manual Transaction

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.

Markenzeichen | Brand Mark

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

MasterCard

Die üblicherweise benutzte Bezeichnung "MasterCard" bezieht sich in ihrer Bedeutung sowohl auf die Organisation selbst als auch auf die funktionale Einheit aller von MasterCard zur Verfügung gestellten Netzwerk-Services und Produkte.

MasterCard Karte

Eigentums- und urheberrechtlich geschütztes Kreditkartenprodukt, das MasterCard seinen Mitgliedsbanken zur Emission anbietet. Das MasterCard-Logo auf der Karte garantiert weltweite Akzeptanz. Kreditkarten dieser Art ermöglichen dem Inhaber die Bezahlung von Waren und Dienstleistungen sowie den Bargeldbezug an Geldautomaten.

MasterCard Debit Switch | MDS

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.

MATCH | 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.

Maximale Antwortzeit | 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.

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.

Mittäterschaft | Collusion

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

MM-Merkmal

Seit 1979 befindet sich das so genannte MM-Merkmal auf allen deutschen Debitkarten. "MM" steht für "moduliertes Merkmal", eine im Kartenkörper eingebrachte, geheime maschinenlesbare Substanz. Das MM-Merkmal in der Karte korrespondiert mit der "MM-Box", die sich in allen deutschen Geldautomaten befindet. Nach erfolgreicher EMV-Einführung in 2011 werden zunehmend auch

Debitkarten ohne MM-Merkmal ausgegeben, da über die sichere EMV-Technologie eine ebenso effektive Kartenechtheitsprüfung erfolgt.

MOTO | Mail Order/Telephone Order | 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.

MOTO-Transaction | Mail Order/Telephone Order Transaction | Schriftlich/telefonische Warenbestellung

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.

-N-

Nationale Interchange Gebühr | 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.

Near Field Communication

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, GeldKarte oder Kreditkarte. NFC kann mittlerweile auch als Zugriffsmedium auf Produktinformationen sowie auf Mobile Services wie Kinokarten, Online-Unterhaltung, Check-In/check-out Dienste und Zugangskontrollen verwendet werden. Die Kartenzahlungen werden über einen kontaktlosen NFC Dialog mit einem kontaktlosen Leser an der Handelskasse, an Verkaufsautomaten oder an Smart Postern ausgeführt. Funktionsweise: Eine – zum Beispiel in die GeldKarte integrierte Antenne – dient, zusammen mit dem Chip, der Kommunikation mit dem NFC-Leseterminal, wobei die Antennen-Reichweite auf zehn Zentimeter beschränkt ist. Das Einführen der Karte in ein Lesegerät entfällt damit. Bei einer derartigen Zahlung muss weder unterschrieben noch eine PIN eingegeben werden.

Netzzugangspunkt | 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.

Neuronales Netz

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

Nicht genehmigte Transaktion | Unauthorised Transaction

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

Null-Limit | 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-Bankunabhängig von der Betragshöhe. Für Geldausgabeautomaten (ATM) gilt grundsätzlich ein zero floor limit.

-O-

Öffentlicher Schlüssel | 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. Siehe auch Privatschlüssel.

Offline Autorisierung | Offline Authorisation

"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 us Transaktion | On us Transaction

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

Online

Betriebsmodus, bei dem ein technisches Gerät oder System mit einem anderen System zu gegenseitigem Informationsaustausch in Verbindung tritt. Der Begriff bezeichnet speziell auch den Betriebsmodus, bei dem die Mitgliedsorganisationen über ihren eigenen Zentralrechner unmittelbar mit dem Netz der Kartenorganisation in Verbindung treten und in Echtzeit auf aktuelle Transaktionsdateien zugreifen. Ebenso bezieht sich "online" auf den Betriebsmodus eines Kartenakzeptanz-Geräts (CAD), wenn dieses bei der Transaktionsdurchführung mit einem zentralen Rechnersystem oder Kommunikationsnetzwerk verbunden ist und die Fähigkeit besitzt, mit diesen externen Systemen gegenseitig Daten auszutauschen und Befehle zu empfangen.

Online Autorisierung | Online Authorisation

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

Online POS-Terminal | Online Terminal

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

Online Transaktion | Online Transaction

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.

-P-

PAN-Schlüsseleingabe | PAN Key Entry

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

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.

PayPass

PayPass heißt die kontaktlose Zahlungstechnologie von MasterCard. Mit der Kreditkarte auf Basis der Near Field Communication-Technologie (NFC) können Kleingeldbeträge bis 25 Euro 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 bis 25 Euro 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 | 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.

Persönliche Geheimzahl (PIN) | Personal Identification Number (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.

Pflichtprogramm bei überhöhtem Rückbelastungsaufkommen | 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.

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.

PIN Eingabetastatur | 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 | PIN Verification Value PVV

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 basierte Transaktion | PIN based Transaction

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-Prüfung | PIN Verification

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.

POC | Point of Compromise

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

PoI | Point of Interaction | Interaktionspunkt

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

POS | 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.

PoZ | Point of Sale ohne Zahlungsgarantie

Es wird keine Zahlungsgarantie ausgesprochen, da weniger Sicherheitsmerkmale geprüft werden. Aus dem Magnetstreifen der Karte werden die Kontonummer und die Bankleitzahl des Kunden ermittelt und ein Lastschriftbeleg wird erstellt. Der

Karteninhaber akzeptiert den Betrag durch seine Unterschrift. Seit dem 31.12.2006 ist dieses Verfahren eingestellt.

Privatschlüssel | Private Key

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.

Prozessor | Processor

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

Public Key | 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.

-Q-

QR Barcode

Quick Response (QR) Barcodes sind eine Weiterentwicklung des 2D Barcodes. QR Barcodes findet man z. B. auf Zeitungsannoncen, auf Werbeplakaten oder auf Produktblättern. Sie werden auch per MMS Dienst versandt und 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 werden, der enthaltene Link ins Internet kann aktiviert werden, oder die mobile Bordkarte, die Kinokarte oder der Gutschein/Coupon können eingesetzt werden. Um QR Barcodes entschlüsseln zu können, benötigt ein Mobiltelefon eine QR Code-Reader App, die per Download auf das Mobiletelefon geladen wird.

-R-

Rechtmäßiger Karteninhaber | Legitimate Cardholder

Karteninhaber, für den rechtmäßig eine Karte ausgestellt wurde.

Reisestellenkarte | 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.

Risiko-Händler | 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.

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.

Routing | 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 | RSA

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

Rückruf | 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.

-S-

SAFE | System to Avoid Fraud Effectively

Weltweite Zentraldatei für Betrugsschäden im MasterCard-Verbund. Als Teil des Mitgliederschutz-Programmes ist SAFE die weltweit zentrale Datenbank für alle MasterCard-Betrugstransaktionen und dient der Erstellung monatlicher Berichte und statistischer Auswertungen für die Mitgliedsbanken. SAFE unterstützt die Banken bei Risikofrüherkennung und Schadensprävention und stellt darüber hinaus Auswertungsdaten zur Verfügung, die auch anderen Präventionsprogrammen als Informationsgrundlage dienen.

Schlichtungsverfahren bei Reklamation | 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.

Schlüssel | 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.

Schlüsselindikatoren | 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.

Schriftlich/telefonische Warenbestellung | Mail Order/Telephone Order Transaction | 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.

SDA | 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.

SDP | 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.

SECCOS | 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.

SEPA | Single European Payment Area

Die europäische Kreditwirtschaft arbeitet derzeit an der Realisierung eines einheitlichen europäischen Zahlungsverkehrsraums (SEPA). Ziel ist es, den Bürgern die Möglichkeit zu eröffnen, Zahlungsverkehrsdienstleistungen im Euro-Raum zu den gleichen Konditionen auszuführen zu können wie im Heimatland. Die Plattformtechnologie ist dabei EMV.

Servicegebühr | Service Fee

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 | 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.

Shoulder Surfing | 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.

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 Karten ausgebende 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 das Institut die Karte und erstellt eine Schadensmeldung.

Sicherheitsmanagement

Sich immer wieder aktualisierender Prozess zur Gewährleistung von Vertrauen in und Zuverlässigkeit von Systemen sowie deren Verfügbarkeit, Integrität und Authentizität.

Sicherheitsmitteilung

Die Zentrale Debit-Schadensbekämpfung 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 der Zentralen Debit-Schadensbekämpfung 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 | Unterschriftbasierte Transaktion

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

Skimming

Kopieren des Magnetstreifens, Ausspionieren des PIN, Duplizieren der Karte. Dabei wird am Schlitz des Zahlungsterminals ein Lesegerät angebracht, das die Daten der eingeschobenen Karte kopiert. Über eine Videokamera, die das Zahlenfeld anvisiert, wird die Geheimnummer des Kunden aufgenommen. Mit den Daten wird die Karte dupliziert und anschließend zum Schaden des rechtmäßigen Besitzers missbraucht.

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 | 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.

Spur | 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.

SSL-Sicherheitsprotokoll | Secure Socket Layer (SSL)

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

Storno | 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.

S.W.I.F.T. | 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.

Symmetrisches Verschlüsselungsverfahren

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

-T-

T & E Karte | T & E Card

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 | 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.

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 | Faked Terminal

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 | Chip Card Terminal

POS-Terminal, das Chipkarten lesen kann.

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.

Die Benutzung erfolgt folgendermaßen:

1. Token am USB anschließen
2. PIN eingeben
3. Erhalt des auf dem Token gespeicherten langen Schlüssels

Es gibt auch Token ohne USB-Anschluss, welche entweder eine stetig wechselnde oder nach Freischaltung durch Eingabe einer PIN auf der Tastatur des Tokens eine zeitlich begrenzt gültige Zahlenkombination anzeigen. Token und Server errechnen diese pseudozufällige Zahl gleichzeitig. Somit ist eine eindeutige Authentifizierung möglich.

track data | Spurdaten

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

Transaktion | Transaction

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

Transaktionsbetrag | Transaction Amount

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

Transaktionsdatum | 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).

Transaktionsgebühr (1) | Transaction Fee

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

Transaktionsgebühr (2) | Item Charge

Eine Gebühr, die pro Transaktion erhoben wird.

Transaktionszertifikat | 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.

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.

-U-

Umlagegebühr | Assessment Fee

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

Umrechnungsdatum | 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.

Umsatzrückbelastung | 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.

Umschaltung auf Magnetstreifen | Fallback to magnetic Stripe

Umschaltung auf Magnetstreifentechnologie als Ersatzlösung bei Chip-Funktionsausfall.

Unterlizenz | 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.

Unterschrift-basierte Transaktion | 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.

Unterschriftsprüfung | 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.

-V-

Verdächtige Akzeptanzstelle | 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.

Verfahren zur Kartenechtheitsprüfung | 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.

Verfallsdatum | 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.

Verfügungsrahmen Kreditkarte | 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.

Verhaltens-Scoring | 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.

Verkaufspunkt | 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.

Verrechnungsbank | 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.

Verrechnungsdatum | Settlement Date

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

Versandhandel | Mail Order/Telephone Order | 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.

Verschlüsselung | Encryption

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

Vertragsnummernsystem | Unique Merchant Identification System

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

Visuelle Datenausspähung | Shoulder Surfing

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.

Vorauszahlung | 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.

Vorautorisierung | 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.

V Pay

V PAY ist das Chip+PIN-basierte Debitverfahren von Visa Europe, das POS-Zahlungen und Geldbezug am Geldautomaten in ganz Europa ermöglicht.

-W-

Waiver
Ausnahmegenehmigungen

Währungsumrechnung | 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.

Wechselkurs | Conversion Rate
Der Kurs, zu dem Beträge von einer Währung in eine andere umgerechnet werden.

Weltweite Leistungsstandards | 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.

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

-X-

Kein Eintrag.

-Y-

Kein Eintrag.

-Z-

Zahlungskarte | Payment Card

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

Zahlungssystem | Payment System

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

ZDS | Zentrale Debit-Schadensbekämpfung

1983 beschlossen die Spitzenverbände der deutschen Kreditwirtschaft, eine eigene Zentralstelle zur Schadensbekämpfung (heutige Zentrale Debitschadensbekämpfung, ZDS) im eurocheque-Bereich aufzubauen (angesiedelt innerhalb der ehemaligen 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.

Zentralrechner | Host

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.

Zertifizierung | 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

ZKA | Zentraler Kreditausschuss

Ehemaliger Name von Die Deutsche Kreditwirtschaft.