Händlerservice

Sicherheit im Fokus

Eine erfolgreiche Kartenzahlung beruht auf Sicherheit.

Beim Thema Kartenzahlung wird viel über Sicherheit und Missbrauch gesprochen. Es stehen heute gute Lösungen und Möglichkeiten zur Verfügung, um die Risiken zu minimieren und Sicherheit beim Bezahlvorgang gewährleisten zu können. Gegenüber Bargeldzahlungen können Kartenzahlungen mitunter die bessere Wahl in puncto Sicherheit sein.

Der Sparkassen-Händlerservice stellt sich diesem Thema und leistet insbesondere bei der Aufklärung und Vorsorge gemeinsam mit Ihnen einen großen Beitrag. Die Zusammenarbeit mit dem Sparkassen-Händlerservice bietet beim Thema Sicherheit ein gutes Maß an Sorgenfreiheit.

Unser Produkt-Portfolio weist exzellente und umfassende Sicherheitsprodukte auf – und darüber hinaus zahlreiche Zusatzservices. Wir selbst sind zertifiziert durch SRC Security Research & Consulting und gehen verantwortungsbewusst mit dem Thema Datenschutz um.

→ erfahren Sie,

dass Datenschutz und Sicherheit bei dem S-Händlerservice höchste Priorität haben.

→ informieren Sie

sich über Maßnahmen, die Kartenzahlungen sicherer machen.

→ schulen Sie

die eigene Vorsicht beim Bezahlvorgang mit Karten.

→ lernen Sie,

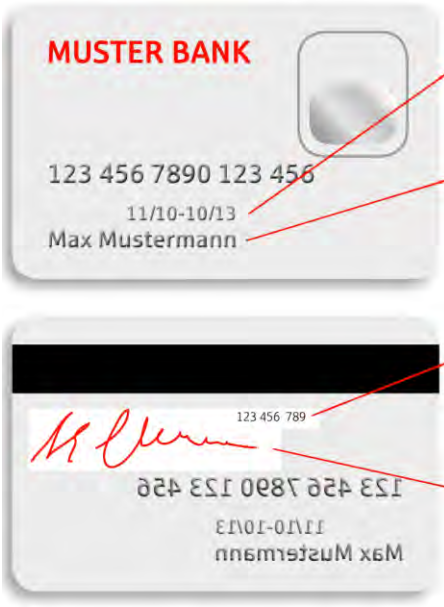
dass Sicherheitsverfahren die Zahlungsabwicklungen im Internet schützen können.

Händlerservice

Sicherheit im Fokus

Achtsamkeit erhöht die Sicherheit bei Kartenzahlung.

Im Folgenden möchten wir Ihnen einen kurzen Überblick zum Thema Schutz vor Betrug beim Bezahlvorgang an der Kasse geben.



Die Gültigkeitsprüfung.
Achten Sie darauf, dass das Gültigkeitsdatum auf der Karte nicht überschritten ist und die Karte nicht abgelaufen ist.

Die Karteninhaberüberprüfung.
Vergewissern Sie sich, das der Name des Karteninhabers mit dem Geschlecht des Zahlenden übereinstimmt.

Die Kartenprüfnummer (KPN).
Diese Nummer wird abgefragt bei E-Commerce-Bestellungen. Die dreistellige Nummer darf nicht gespeichert werden.

Der Unterschriftenvergleich.
Vergleichen Sie, ob die Unterschrift auf dem Beleg mit der Unterschrift auf der Karte und dem Namen übereinstimmt.

Weitere Hinweise für mehr Sicherheit:

- → Lassen Sie den Kunden immer den Betrag kontrollieren und überprüfen Sie diesen selbst noch einmal, um Tastatureingabefehler vor Abschluss der Kartenzahlung zu erkennen.
- → Stellen Sie sicher, dass Ihre Kunden ihre PIN oder ihre Geheimzahl unbeobachtet eingeben können.
- → Entsorgen Sie alte Kartenbelege so, dass Daten darauf nicht in den Besitz von Dritten gelangen können.
- → Verwahren Sie Ihr Terminal außerhalb der Ladenöffnungszeiten an einem sicheren Ort.
- → Lassen Sie keine unbefugten Personen an das Terminal.
- → Melden Sie einen Manipulationsverdacht am Terminal umgehend der Polizei und dem Sparkassen Händlerservice.

→ weitere Hinweise

zu den Kartensicherheitsmerkmalen finden Sie ebenfalls auf den Webseiten der Kartenorganisationen:

www.visa.de
www.mastercard.com

Händlerservice

Sicherheit im Fokus

Tipps zur Einhaltung des Payment Card Industry Data Security Standard (PCI DSS).

Sie als Händler verarbeiten, speichern und leiten Karteninhaberdaten weiter. Daher sollten Sie sich mit den Schritten vertraut machen, die erforderlich sind, um den Payment Card Industry Data Security Standard (PCI DSS) einzuhalten und zu erfüllen. Denn der PCI DSS enthält verbindliche Regeln für Händler, die Kartenzahlungen anbieten, um Daten vor Missbrauch und Diebstahl zu schützen.

Payment Card Industry Data Security Standard (PCI DSS)

regelt die weltweit gültigen Sicherheitsstandards der führenden internationalen Kreditkartenorganisationen.

Die PCI-Compliance, das bedeutet die Einhaltung aller PCI-DSS-Sicherheitsanforderungen, muss nachgewiesen werden. Der Nach-weis ist über unterschiedliche externe und interne Prüfungen zu erbringen – die sich nach dem Umfang Ihrer jährlichen Kartentrans-aktionen richten. Dabei wird beispielsweise Ihre Netzwerkarchitektur untersucht oder der Umgang mit kritischem Datenmaterial überprüft. 12 Punkte innerhalb des PCI-DSS-Regelwerkes müssen Sie als Händler einhalten.

Die 12 Punkte des PCI-DSS-Regelwerkes für Sie im Überblick:

- → Installation und regelmäßige Aktualisierung einer Firewall zum Schutz von Daten
- → Keine Verwendung vorgegebener Werte (seitens Lieferanten/ Hersteller) für System-Passwörter oder andere Sicherheitsparameter
- → Absicherung gespeicherter Daten: Karten- und Transaktionsdaten nicht unnötig speichern, wie etwa die vollständige Kartennummer, Daten der Magnetstreifenspuren, Kartenverifizierungsode (CVV2) oder PIN
- → Verschlüsselte Übertragung von Karteninhaberdaten und sensiblen Informationen in offenen Netzwerken
- → Verwendung und regelmäßige Aktualisierung einer Anti-Viren-Software
- → Entwicklung und Verwendung sicherer Systeme und Anwendungen
- → Beschränkung des Datenzugriffs - ausschließlich für geschäftliche Zwecke
- → Zuteilung einer persönlichen ID für jede Person mit Zugang zum Computersystem
- → Zugriffsberechtigungen im Zusammenhang mit sensiblen Karteninhaberdaten einschränken
- → Nachvollziehbarkeit und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Karteninhaberdaten
- → Regelmäßige Überprüfung von Sicherheitssystemen und Prozessabläufen
- → Unternehmensrichtlinie, die das Thema Informationssicherheit regelt

Händlerservice

Sicherheit im Fokus

Sicherheitshinweise für Kartenzahlungen im Internet.

Sicherheitsverfahren wie Verified by Visa und MasterCard SecureCode, Merkmale wie die Kartenprüfnummer und Programme wie die PCI-Zertifizierung gewährleisten höchste Sicherheit bei der Zahlungsabwicklung im E-Commerce und Mailorder. Die unterschiedlichen Sicherheitsverfahren stellen wir Ihnen im Folgenden kurz vor.

Die Sicherheitsverfahren in E-Commerce und Mailorder:

Verified by Visa (VbV) und MasterCard SecureCode (MSC)
Die Sicherheitsstandards VbV von Visa und MSC von MasterCard für Kreditkartenzahlungen schützen Sie vor Rückbelastungen mit der Begründung „Transaktion vom Karteninhaber nicht durchgeführt/ autorisiert“ (Haftungsumkehr) durch einen zusätzlichen Identifikationsprozess.

Kartenprüfnummer (KPN)
Zusätzlich zur Kreditkartennummer wird im Fernabsatzgeschäft die Kartenprüfnummer abgefragt. Dadurch kann die Sicherheit, dass dem Käufer die Karte auch tatsächlich vorliegt, erhöht werden.

Prüfroutinen
Algorithmus (Luhncheck) zur logischen Prüfung der Kreditkartennummer. Bei allen Lastschriftzahlungen prüft der S-Händlerservice die Bankleitzahl sowie deren logische Zuordnung zur Kontonummer.

PCI DSS bei E-Payment-Software
Unsere E-Payment-Software erfüllt die Anforderungen der Kreditkartenorganisationen gemäß Payment Card Industry Data Security Standard (PCI DSS).

Zusätzlich bieten wir weitere Sicherheitsleistungen – in Abhängigkeit von der jeweiligen E-Payment-Software:

- → Schwellwertprüfungen nach Umsatz-und Transaktionenanzahl
- → Geo-IP-Location (Besteller) ermöglicht, zum Zeitpunkt der Bestellung jede Internet-IP-Adresse über ihren Nummernkreis oder Aufbau geographisch zuzuordnen.
- → Ländercheck (Besteller – Lieferland)

Detaillierte Informationen

finden Sie im Maßnahmenkatalog „Risk Management im E-Commerce“. Er hilft, Betrug zu erkennen und zu reduzieren.

Den Maßnahmenkatalog finden Sie auf unserer Webseite unter:

→ www.s-haendler-service.de/e-commerce

Händlerservice

Sicherheit im Fokus

Die beiden gängigsten Sicherheitsverfahren für E-Commerce im Detail.

Verified by Visa (VbV) und MasterCard SecureCode (MSC): Diese beiden Sicherheitsverfahren im E-Commerce ermöglichen neben der Authentifizierung der Karteninhaber auch den Schutz vor Kartenmissbrauch im Internet.

Wie funktionieren die Sicherheitsverfahren?

Ihre Kunden werden automatisch auf eine sichere Seite der Karten ausgebenden Bank weitergeleitet und haben dort ihre Zahlung per Passworteingabe zu bestätigen. Im Anschluss daran erfolgt die tatsächliche Online-Autorisierung. Für Ihren Kunden ist dann eine Zahlungsrückgabe unter Angabe des Arguments „Transaktion nicht durchgeführt“ (Haftungsumkehr) nicht mehr möglich. Das funktioniert auch, wenn die Bank des Kunden nicht an den Sicherheitsverfahren VbV oder MSC teilnimmt.

Vorteile

- → Schutz vor betrügerischem Kartenmissbrauch
- → Verringerung berechtigter Rückbelastungen mit dem Argument „Transaktion nicht durchgeführt“
- → Erhöhung der Zahlungssicherheit
- → Einfache Integration des Merchant Plug-in für die sichere Datenübertragung zu der jeweiligen Kartenorganisation bzw. Karten ausgebenden Bank

Voraussetzungen

- → E-Payment-Software mit zertifzierter VbV- und MSC-Funktion
- → Vereinbarung mit S-Händlerservice für VbV und/oder MSC
- → Aktivierung der Merchant Plug-in-Nutzung
- → Meldung der VbV- und/oder MSC-Vertragsdaten an alle beteiligten Parteien
- → Kennzeichnung der Transaktionen in der E-Payment-Software
- → Anwendung der Sicherheitsverfahren bei jeder Zahlung
- → Für Maestro-Zahlungen: MSC Freischaltungen für alle Beteiligten (Karteninhaber, Händler, Karten-inhaberbank)

Zahlungsarten

- → Visa
- → MasterCard
- → Maestro

Händlerservice

Sicherheit im Fokus

Das Thema Sicherheit hat beim S-Händlerservice höchste Priorität.

B+S hat das Datenschutz-Zertifikat

Der Schutz sensibler Daten wie z. B. Kreditkartennummern oder Bankverbindungen hat für B+S höchste Priorität. Im Rahmen einer freiwilligen Prüfung hat uns der unabhängige Gutachter SRC Security Research & Consulting bescheinigt, dass wir alle Vorgaben aus dem Bundesdatenschutzgesetz (BDSG) bei der Auftragsdatenverarbeitung erfüllen. Das bestätigt offiziell das SRC-Zertifikat.

Qualitätskriterium Datenschutz

Das Zertifikat erspart unseren Kunden die Kontrolle der gemäß Bundesdatenschutzgesetz geforderten technischen und organisatorischen Maßnahmen zum Schutz der Daten. Das ist für den S-Händlerservice bedeutend, da der Datenschutz ein immer wichtigeres Qualitätskriterium in unserem Geschäft darstellt. Hier liegt auch der Grund dafür, sich im Rahmen eines freiwilligen Datenschutz-Audits zertifizieren zu lassen. Bereits im Jahr 2009 wurde B+S Card Service als erstem Unter-nehmen in Deutschland, das sowohl Acquiring als auch einen eigenen Netzbetrieb anbietet, die vollständige PCI-DSS-Compliance bestätigt.

Der S-Händlerservice hat die PCI-DSS-Zertifizierung

PCI DSS steht für Payment Card Industry Data Security Standard und bezeichnet einen Katalog von verbindlichen Regeln des PCI Security Standards Council. Dieser betrifft den Schutz sensibler Karteninhaberdaten, den alle Unternehmen gewährleisten müssen, die Kreditkartentransaktionen speichern, übermitteln oder verarbeiten.

Der S-Händlerservice baut auf Know-how

Sämtliche PCI-DSS-relevanten Systeme, Netzwerke und Prozesse bei B+S Card Service werden regelmäßig von dem Zertifizierer SRC GmbH im Rahmen eines Datenschutz-Audits geprüft und in ihrer Übereinstimmung mit den Anforderungen des Standards bestätigt. Im Rahmen des Zertifizierungsprozesses hat B+S in allen Bereichen des Unternehmens die notwendigen Anpassungen vorgenommen und dabei ein umfangreiches PCI-DSS-Know-how aufgebaut.

Sparkassen-Händlerservice
Lyoner Straße 9
60528 Frankfurt/Main
Tel.: +49 (0)69 6630-5806
Fax: +49 (0)69 6630-5625
www.s-haendlerservice.de