

# Payment Card Industry (PCI) Data Security Standard



**Informationen und Hinweise für  
Händler  
zur Umsetzung der Programme**

**MasterCard Site Data Protection (SDP)  
und  
Visa Account Information Security (AIS)**



Von

**ConCardis GmbH  
Solmsstr. 4  
D-60486 Frankfurt am Main**

## Einleitung

Die Kreditkartenorganisationen MasterCard International und Visa International haben angesichts der steigenden Missbrauchsrate bei der Nutzung von Kreditkarten die Programme **MasterCard Site Data Protection (SDP)** und **Visa Account Information Security (AIS)** initiiert, um die Sicherheit bei der Speicherung, Verarbeitung und/oder Weiterleitung von Kartendaten zu verbessern und eine Kompromittierung von Kartendaten wirksam zu verhindern.

### **Die Programme SDP und AIS richten sich an Händler und Service Provider, die Kreditkartendaten auf eigenen Systemen speichern, verarbeiten und/oder weiterleiten.**

Im Falle einer Kompromittierung von Kartendaten (mit E-Commerce-, MOTO- oder POS-Akzeptanzvertrag) drohen erhebliche Schadensersatzforderungen durch die Zahlungssysteme und Acquirer, sollte der Händler bzw. dessen Service Provider nicht die Einhaltung der Sicherheitsanforderungen nachweisen können.

Daher sind Händler und deren Service Provider aufgefordert, den Nachweis zu erbringen, dass angemessene technische und organisatorische Maßnahmen zum Schutz vor Angriffen und Kompromittierung von Kartendaten, Transaktions- oder Konteninformationen getroffen wurden.

### **Händlern und Service Providern, die die Anforderungen der Programme erfüllen, werden im Falle der Kompromittierung eine teilweise oder vollständige Befreiung von den Strafen gewährt (sog. MasterCard „Safe Harbour“ Regel).**

Im Dezember 2004 (MasterCard) bzw. Februar 2005 (Visa) wurden die zuvor voneinander unabhängigen technischen Anforderungen der Zahlungssysteme (AIS/SDP) zu dem sog. **Payment Card Industry (PCI) Data Security Standard** zusammengeführt.



Im September 2006 haben die Unternehmen American Express, Discover Financial Services, JCB, MasterCard Worldwide und Visa International die Gründung eines unabhängigen Gremiums, dem PCI Security Standards Council (PCI SSC) bekannt gegeben. Dieses Gremium ist nun alleine für die Weiterentwicklung des Payment Card Industry Data Security Standards zuständig.

Das PCI SSC aktualisierte im Oktober 2008 die PCI DSS Version 1.1 auf die PCI DSS Version 1.2. (<https://www.pcisecuritystandards.org>).

Der neue Standard setzt sich zusammen aus

- PCI DSS - Requirements and Security Assessment Procedures  
Version 1.2, October 2008
- PCI DSS - Self-Assessment Questionnaire and Attestation of Compliance  
Types A -D, Version 1.2, October 2008
- PCI DSS - Security Scanning Procedures  
Version 1.1, September 2006  
Version 1.2 coming soon

Welche Maßnahmen der Händler oder Service Provider umsetzen muss, um die PCI-Compliance (Umsetzung/Einhaltung von PCI DSS) zu erlangen, hängt von der Anzahl der im Jahr getätigten Transaktionen ab (gemäß den Anforderungen von MasterCard<sup>1</sup> und Visa<sup>2</sup>).

	Kategorie Händler	Self Assessment	Security Scan	Security Audit
	<b>Level 1</b> > 6. Mio TRX p.a. und Marke über alle Vertriebskanäle (POS, E-Comm., MoTo)	-	4 x pro Jahr	1 x pro Jahr
	<b>Level 2</b> 1 Mio. bis 6 Mio. TRX p.a. und Marke über alle Vertriebskanäle (POS, E-Comm., MoTo)	1 x pro Jahr	4 x pro Jahr	-
	<b>Level 3</b> 20.000 bis 1 Mio. E-Commerce-TRX p.a. und Marke	1 x pro Jahr	4 x pro Jahr	-
	<b>Level 4</b> alle anderen Händler	1 x pro Jahr	4 x pro Jahr	-

In Abhängigkeit von deren Einstufung in die Händlerkategorien sind folgende Schritte durchzuführen:

- Der Händler nimmt eine erste Bewertung seiner Sicherheitsmaßnahmen anhand eines Selbsteinschätzung-Fragebogens (**PCI Self-Assessment Questionnaire**) vor. Dieser Fragebogen muss jährlich neu ausgefüllt werden.
- Es werden jährlich vier PCI Security Scans der Internet-Schnittstelle des Händlers (sofern relevant) mit dem Ziel durchgeführt ggf. vorhandene Schwachstellen in Netzwerkkomponenten, Betriebssystemen und Applikationen aufzudecken, die durch Angreifer ausgenutzt werden könnten.
- Die Einhaltung der Sicherheitsanforderungen wird vor Ort mittels eines PCI Security Audits geprüft (Sicherheitsprüfung durch Ortsbegehung).

<sup>1</sup> gemäß MasterCard Global Security Bulletin No. 1, 14 January 2005

<sup>2</sup> gemäß Visa Member Letter EU 06/05, 2. February 2005

## **Für alle Händler der Kategorien Level 1 bis 4 ist die Erbringung des Nachweises über die Umsetzung der PCI Standards, Version 1.1 zwingend.**

Die sog. Compliance Validation (PCI-Umsetzungsgültigkeit) mittels PCI Fragebogen, PCI Security Scans und PCI Security Audits wird von akkreditierten Partnern der Kreditkartenorganisationen durchgeführt.

Die Security Scans werden durch PCI Approved Scanning Vendor (ASV) bzw. die Security Audits durch PCI Qualified Security Assessor (QSA) durchgeführt.

### **Vorteile der Umsetzung des PCI DSS für Sie als Händler:**

Der PCI DSS mit seinen verbindlichen Regeln für mehr IT-Sicherheit soll der Betrugskriminalität einen Riegel vorschieben. Durch verstärkte Schutzmaßnahmen bei der Verarbeitung von Zahlungskartendaten gemäß PCI entstehen Ihnen vor allem folgende Vorteile:

- Erhöhte Datensicherheit und Schutz Ihrer Kunden
- Gesteigertes Kundenvertrauen und somit ggf. Steigerung der Kreditkarteneinsatzes und -umsatzes
- Größere Absicherung von finanziellen Schäden und Schadenersatz aufgrund von Sicherheitsverletzungen
- Schutz des Unternehmens-Image
- Bewertung des Sicherheitsschutzes von Systemen zur Speicherung, Verarbeitung und/oder Übermittlung von Karteninhaberdaten
- Datenminimierung und-vermeidung führen zur Reduzierung des Unternehmensrisikos
- Netzwerkstrukturierung reduziert die Kosten der Aufrechterhaltung der PCI Compliance

### **Zeitliche Vorgaben zur Umsetzung des PCI DSS sind je nach Kreditkartenunternehmen und Land verschieden.**

Zu den wichtigsten durch **VISA Europe** gesetzten Fristen zählen:

- 30. Juni 2005 – Datum, bis zu dem Händler der Level 1 bis 3 belegen müssen, dass sie PCI DSS vollständig umgesetzt haben.
- 31. Dezember 2008 – Verschiebung der Umsetzungsfrist für alle neuen Händler des Levels 2; Datum, bis zu dem alle neuen Händler des Levels 2 den PCI DSS vollständig umgesetzt haben müssen.
- 30. Juni 2007 - Bis zu diesem Datum müssen Händlerbanken bestätigen, dass der PCI DSS von ihren Händlern vollständig umgesetzt worden ist.
- 01. Oktober 2009 - e-Commerce Händler, die bis zu 1 Million Transaktionen im Jahr abwickeln (Level 3 und 4 Händler) müssen einen PCI DSS zertifizierten Service Provider verwenden oder selbst PCI DSS compliant zertifiziert sein

Zu den wichtigsten von **MasterCard Europe** gesetzten Fristen gehören:

- 30. Juni 2005 - Datum, bis zu dem alle Händler der Level 1 bis 3 den PCI DSS vollständig umgesetzt haben müssen.
- 31. Dezember 2008 – Verschiebung der Umsetzungsfrist für alle neuen Händler des Levels 2; Datum, bis zu dem alle neuen Händler des Levels 2 den PCI DSS vollständig umgesetzt haben müssen.

ConCardis besteht auf die Umsetzung der PCI DSS bei allen Händlern der Level 1 bis Level 4.

Bei Nichteinhaltung der Fristen können Strafen der Marken in sechsstelliger Höhe entstehen.

## Vorgehensweise und Ablauf

Der Händler/Service Provider registriert sich zunächst bei einem PCI-Zertifizierer der Wahl.

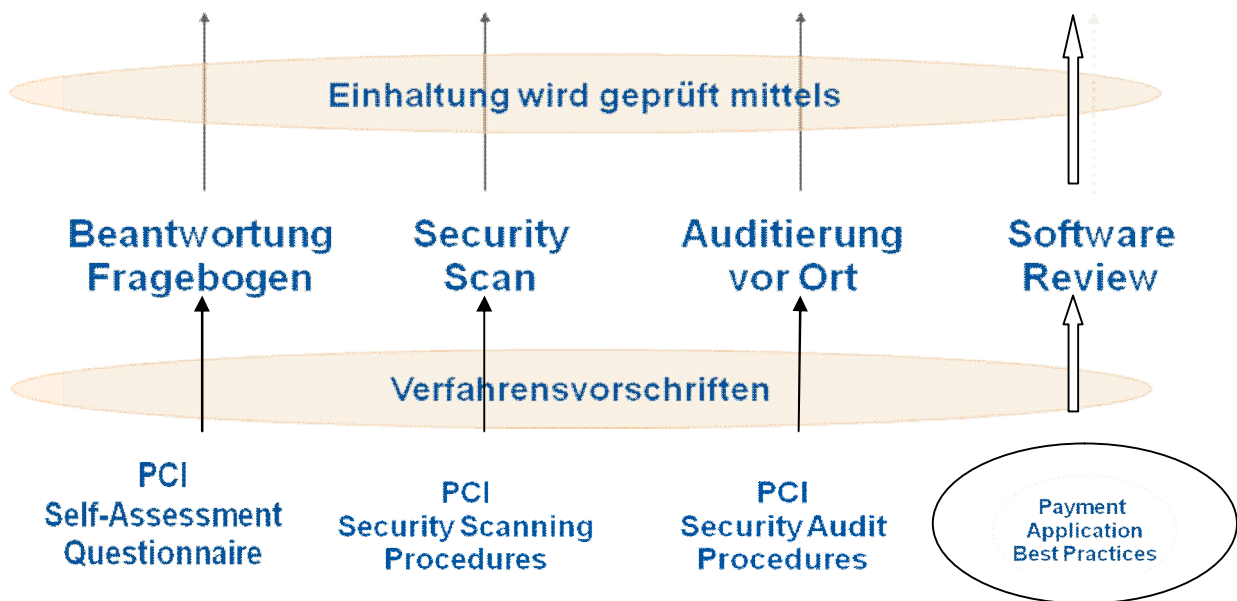
Eine aktuelle Liste der akkreditierten PCI-Zertifizierer finden Sie unter [www.concardis.com](http://www.concardis.com) oder [https://www.pcisecuritystandards.org/resources/qualified\\_security\\_assessors.htm](https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm)

Im Rahmen der kostenlosen Registrierung müssen in einem Web-Formular verschiedene Fragen beantwortet werden, wie z. B.:

- Name der Firma, Adresse, Ansprechpartner und Kontaktdaten (E-Mail und Telefon);
- Anzahl der Transaktionen mit MasterCard-, Visa-, American Express-, Diners-, JCB- und Discovery-Kreditkarten;
- Angabe, ob Kreditkartendaten auf eigenen Systemen gespeichert, verarbeitet oder weitergeleitet werden;
- Ggf. Name des (Payment) Service Providers für die Abwicklung der Transaktionen.

Anhand der vorgenommenen Klassifikation wird der Händler für die Nutzung des Online-Fragebogens (PCI **Self-Assessment Questionnaire**) freigeschaltet und per E-Mail informiert bzw. die Termine und die weitere Vorgehensweise für die erforderlichen PCI **Security Scans** und **Security Audits** werden nachfolgend zwischen dem Händler und dem Zertifizierer vereinbart.

## PCI Data Security Standard (PCI DSS)



**Payment Application Best Practices sind standardisierte, PCI-zertifizierte Zahlungssoftware-Lösungen, die von den Kreditkartengesellschaften empfohlen werden.**

## Elektronischer Online-Fragebogen/PCI Self-Assessment Questionnaire

Ein Händler (Level 2-4) muss **jährlich** eine Bewertung der technischen und organisatorischen Maßnahmen durch Beantwortung des vorgegebenen PCI Self-Assessment Questionnaires (Fragebogen zur Selbsteinschätzung) als Online-Fragebogen durchführen.

Die Fragen betreffen sämtliche sechs Bereiche des PCI Data Security Standards und beinhalten zwölf Prüfungsanforderungen:

- I. **Aufbau und Instandhaltung des sicheren Netzwerks (Build and Maintain a Secure Network)**
  1. Anforderung 1: Einrichtung und Instandhaltung der Firewallkonfiguration zum Schutz der Daten
  2. Anforderung 2: Keine Verwendung der vom Händler ausgelieferten und voreingestellten System-Passwörter bzw. anderer Sicherheitsparameter
- II. **Schutz der Karteninhaberdaten (Protect Cardholder Data)**
  3. Anforderung 3: Schutz der gespeicherten Daten
  4. Anforderung 4: Verschlüsselte Übertragung der Karteninhaberdaten und sensibler Informationen über öffentliche Netze
- III. **Aufrechterhaltung eines Programms zur Handhabung der Schwachstellen (Maintain a Vulnerability Management Program)**
  5. Anforderung 5: Gebrauch und regelmäßige Aktualisierung der Anti-Viren-Programme
  6. Anforderung 6: Entwicklung und Aufrechterhaltung von sicheren Systemen und Anwendungen
- IV. **Einführung von strengen Zugriffskontrolle-Maßnahmen (Implement Strong Access Control Measures)**
  7. Anforderung 7: Beschränkung des Zugriffs auf die Daten nach dem need-to-know Prinzip
  8. Anforderung 8: Zuweisung von eindeutigen Kennungen an alle Personen mit Computer-Zugriff
  9. Anforderung 9: Einschränkung des physischen Zugangs zu Karteninhaberdaten
- V. **Regelmäßige Überwachung und Untersuchung der Netzwerke (Regularly Monitor and Test Networks)**
  10. Anforderung 10: Verfolgung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen sowie Karteninhaberdaten
  11. Anforderung 11: Regelmäßige Prüfungen der Sicherheitssysteme und -prozesse

## VI. *Aufrechterhaltung einer Informationssicherheitspolitik (Maintain an Information Security Policy)*

### 12. Anforderung 12: Aufrechterhaltung von Informationssicherheitspolitik

Mit dem Fragebogen wird die Einhaltung der Sicherheitsanforderungen des PCI Data Security Standards mittels Selbstauskunft geprüft.



## PCI Security Scan

Security Scans haben das Ziel, Schwachstellen in Architektur und Konfiguration der untersuchten Systeme aufzudecken, die ein Angreifer ausnutzen könnte, um Kreditkartendaten zu kompromittieren.

Ein akkreditierter PCI-Zertifizierer führt die PCI Security Scans entsprechend der Anforderungen aus den „PCI Security Scanning Procedures“<sup>3</sup> durch. Diese werden als „**non-intrusive**“ bzw. „**non-destructive**“ durchgeführt, d.h. es werden keine Angriffe durchgeführt oder Schwachstellen ausgenutzt, die die Verfügbarkeit oder Integrität der Zielsysteme beeinflussen. Vielmehr werden reguläre Anfragen an die Zielsysteme gerichtet, die in der Regel keine Auswirkungen auf den ordnungsgemäßen Betrieb haben.

Die Systeme werden dabei aus dem Internet netzseitig mit Hilfe von Security Scannern und manuellen Analysen auf mögliche Schwächen hin untersucht. Die eingesetzten Werkzeuge prüfen auf bekannte Schwächen von Netzwerkkomponenten, Betriebssystemen und Applikationen.

Der genaue Termin für die Durchführung der PCI Security Scans wird zuvor mit dem Händler abgestimmt. Anschließend wird anhand einer einheitlichen und durch die „PCI Security Scanning Procedures“ vorgegebenen Vorgehensweise der PCI Security Scan durchgeführt. Das Ergebnis des PCI Security Scans wird in Form eines schriftlichen Berichts in **englischer** Sprache an den Internet-Händler übergeben. Der Bericht entspricht den Vorgaben von MasterCard und Visa und beinhaltet eine fünfstufige Kategorisierung (low, ..., urgent) der ggf. gefundenen Schwachstellen.

Die Untersuchung hat den Zweck, gezielt **einzelne** Schwachstellen oder Fehler aufzudecken, die zu Angriffen auf das System ausgenutzt werden können.

Sind aufgrund aufgedeckter Schwachstellen die Ergebnisse des PCI Security Scans im Sinne der „PCI Security Scanning Procedures“ nicht zufriedenstellend, sind entsprechende Nachbesserungen durch den Händler erforderlich. Deren Wirksamkeit wird durch eine Wiederholung des PCI Security Scans geprüft.

<sup>3</sup> [https://www.pcisecuritystandards.org/pdfs/pci\\_scanning\\_procedures\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf)

## Durchführung des Security Audits

Mit der Durchführung eines PCI Security Audits wird die Umsetzung des PCI Data Security Standards vor Ort geprüft. Im Rahmen des Security Audits werden bei Händlern des Levels 1 zusätzlich nachfolgend beschriebene Prüfungsschritte durchgeführt.

Zur **Vorbereitung** des PCI Security Audits sind folgende Schritte durchzuführen:

1. Formelle Beauftragung der Dienstleistung bei einem Zertifizierer und vorläufige Vereinbarung eines Termins für das PCI Security Audit.
2. Auslieferung der Dokumente zur Durchführung des Security Audit:  
Der PCI-Zertifizierer übersendet die Dokumente „PCI Security Audit Procedures and Reporting“ und die „Guideline for the preparation of the PCI security audit“ an den Kunden in elektronischer Form. Gleichzeitig stimmt der Zertifizierer ein Passwort ab bzw. übermittelt einen öffentlichen PGP-Schlüssel für die Absicherung der weiteren Kommunikation.
3. Der elektronische Online-Fragebogen (PCI Self-Assessment Questionnaire) wird freigeschaltet, um dem Kunden die erste, optionale Bewertung seiner PCI-Compliance zu ermöglichen.

### Schritt 1: Bewertung der Dokumente

Die entsprechenden Informationen und Dokumente sind spätestens **zwei Wochen** vor dem abgestimmten Security Audit-Termin an den Zertifizierer zu übermitteln.

### Schritt 2: Security Audit vor Ort (Ortsbegehung)

Der Zertifizierer wird im Rahmen des PCI Security Audit die Angaben des Händlers vor Ort stichprobenartig prüfen. Die Prüfung deckt alle sechs Bereiche des PCI Data Security Standards ab und beinhaltet u.a.:

- Vorstellung des Geschäftsmodells,
- Ablauf einer Kreditkartentransaktion innerhalb der IT-Systeme (Datenfluss),
- Interviews mit Mitarbeitern, insbesondere auch mit Personen, die
  - Sicherheitsfunktionen im Unternehmen wahrnehmen,
  - Zugriff auf Kreditkartendaten haben,
  - für die Wartung und den Betrieb von Systemen verantwortlich sind, auf denen Kreditkartendaten gespeichert, verarbeitet oder weitergeleitet werden
- Einsichtnahme in Logdateien der relevanten Anwendungen,
- Besichtigung der Räume, des Rechenzentrums, des Serverraums, usw.

Für den Fall, dass der Händler andere als in der Checkliste vorgegebene Sicherheitslösungen umgesetzt hat (so genannte Compensating Controls –

Ersatzmaßnahmen), wird der Zertifizierer diese überprüfen und im Hinblick auf die Angemessenheit und Umsetzung des PCI Data Security Standard bewerten.

### Schritt 3: Berichtsentwurf

Der Zertifizierer erstellt einen ersten Entwurf des abschließenden Audit-Berichts auf Basis des Dokuments „PCI Security Audit Procedures“ und stimmt diesen mit dem Händler ab.

### Schritt 4: Vorab-Version des Reports

Der Zertifizierer arbeitet die Kommentare des Händlers nach gegenseitiger Abstimmung in den Berichtsentwurf ein und übermittelt diesen an die Zahlungssysteme. Dieser wird von den Zahlungssystemen geprüft, ggf. kommentiert und an den Zertifizierer zurückgesendet.

### Schritt 5: Endgültige Version des Reports

Der Zertifizierer wird abschließend die Kommentare der Zahlungssysteme in den Audit-Bericht einarbeiten und diesen anschließend an den Händler und die Zahlungssysteme weiterleiten.

## Kontakt für Rückfragen

Zu allen PCI-relevanten Fragen stehen Ihnen die Mitarbeiter der ConCardis GmbH gerne unter [PCI@concardis.com](mailto:PCI@concardis.com) zur Verfügung.