



## Payment Card Industry Data Security Standard (PCI DSS)

**Das Vertrauen der Verbraucher in moderne Zahlungssysteme ist die elementare Grundlage für den wirtschaftlichen Erfolg. Nur durch angemessen hohe Sicherheitsstandards kann das Vertrauen Ihrer Kunden langfristig gesichert werden. Der PCI DSS stellt ein wichtiges Werkzeug zur Erreichung dieses Ziels dar.**

Die usd.de AG ist einer der wenigen durch den PCI Security Standards Council akkreditierten Qualified Security Assessors (QSA) im deutschsprachigen Raum. Zusätzlich bieten wir Schwachstellen Scans und Unterstützung bei Selbstauskünften (Self Audits) im Rahmen des PCI DSS-Programms an und verfügen über die entsprechende Akkreditierung als Approved Scanning Vendor (ASV).

### Wie ist PCI DSS entstanden?

Um dem Diebstahl und Missbrauch von Kreditkartendaten vorzubeugen, schreiben VISA und MasterCard international verpflichtende Sicherheitsprogramme vor: AIS (Account Information Security) von VISA und SDP (Site Data Protection) von MasterCard. Mit dem Ziel der Vereinheitlichung konkreter Sicherheitsanforderungen wurde 2005 der »Payment Card Industry Data Security Standard« (PCI DSS) definiert und in die Sicherheitsprogramme AIS und SDP integriert. Der PCI DSS wurde von allen namhaften Kreditkartenunternehmen als gemeinsamer Standard anerkannt. Neben VISA und MasterCard sind das American Express, JCB und Discover Financial Services. Zur unabhängigen Pflege und Weiterentwicklung des

PCI DSS wurde das PCI Security Standards Council (PCI SSC) gegründet. Mitglieder sind neben den Kartenorganisationen Vertreter aus Handel und dem Kreditkartengewerbe. QSA und ASV dürfen zur Wahrung ihrer Neutralität nicht Mitglied sein.

### Wen betrifft der Standard?

Der Standard betrifft alle Unternehmen die Kreditkartendaten verarbeiten, übertragen oder speichern. Darunter fallen Händler (Merchants) Händlerbanken (Acquirer) und Service Provider (Dienstleister für Zahlungsverkehr, E-Commerce Dienstleister, Web-Hosting Provider).

### Welche Prüfmethode gibt es?

In Abhängigkeit der Einstufung des Schadensrisikos bei Merchants und Service Providern werden unterschiedlich starke Prüfmethode im Rahmen des Zertifizierungsprozesses verlangt. Ausschlaggebend ist hierbei das Transaktionsvolumen.

Je nach Level Einstufung wird die Durchführung eines Onsite Audits durch einen Qualified Security Assessor (QSA), die Durchführung von PCI Vulnerability Scans durch einen Approved Scanning Vendor (ASV) oder das Ausfüllen eines Self Assessment Questionnaires (SAQ) gefordert. Der Fragebogen dient der Selbstbeurteilung und fragt je nach Geschäftsmodell des jeweiligen Unternehmens unterschiedliche Anforderungen des PCI DSS ab (SAQ Typ A-D). Nachfolgende Tabelle gibt Ihnen einen Überblick über die Einstufungskriterien von Händlern und Service Providern und den damit verbundenen



Prüfungsanforderungen. Bitte beachten Sie, dass sich die Einstufungen der Kreditkartenorganisationen jeweils leicht unterscheiden. Zudem kommt es gelegentlich zu Anpassungen der Einstufungskriterien durch die Kreditkartenorganisationen. Um sicher zu sein, sollten Sie sich vor Ihrer Zertifizierung über die aktuelle Einstufung bei der usd.de AG oder direkt bei den Kreditkartenorganisationen informieren.

Für Händler (Merchants) der Level 3 und 4 sind keine PCI Vulnerability Scans erforderlich, sofern sie keine Kreditkartendaten speichern, verarbeiten oder übertragen und zusätzlich mit einem PCI DSS zertifizierten Payment Service Provider arbeiten. Service Provider des Levels 1 werden mit Nachweis der Compliance durch VISA Europe als „PCI DSS compliant“ Service Provider veröffentlicht, Service Provider der Level 2 nicht.

Level	Einstufungskriterien für Händler	Onsite Audit	Self-Assessment Questionnaire	PCI Vulnerability Scans
1	<ul style="list-style-type: none"> <li>Alle Händler, die unabhängig vom Vertriebsweg (POS, MOTO oder E-Commerce) mehr als 6 Mio. Transaktionen pro Jahr tätigen, oder bereits Opfer eines Kreditkartenmissbrauchs waren.</li> <li>Alle Händler, die von einer anderen Kreditkartenorganisation als Level1 Händler eingestuft sind.</li> </ul>	Jährlich		Vierteljährlich
2	<ul style="list-style-type: none"> <li>Alle Händler, die jährlich zwischen 1 Mio. und 6 Mio. E-Commerce-Transaktionen durchführen.</li> <li>Alle Händler, die von einer anderen Kreditkartenorganisation als Level-2 Händler eingestuft sind.</li> </ul>		Jährlich	Vierteljährlich
3	<ul style="list-style-type: none"> <li>Alle Händler, die für MasterCard oder Visa jährlich zwischen 20.000 und 1 Mio. E-Commerce-Transaktionen durchführen.</li> <li>Alle Händler, die von einer anderen Kreditkartenorganisation als Level-3 Händler eingestuft sind.</li> </ul>		Jährlich	Vierteljährlich
4	<ul style="list-style-type: none"> <li>Alle Händler, die nicht als Level-1, Level-2 oder Level-3 eingestuft sind.</li> </ul>		Jährlich	Vierteljährlich

Level	Einstufungskriterien für Service Provider	Onsite Audit	Self-Assessment Questionnaire	PCI Vulnerability Scans
1	<ul style="list-style-type: none"> <li>VisaNet Prozessoren oder sonstige Service Provider die über 300.000 Transaktionen pro Jahr speichern, verarbeiten oder übertragen.</li> </ul>	Jährlich		Vierteljährlich
2	<ul style="list-style-type: none"> <li>Jeder Service Provider der unter 300.000 Transaktionen pro Jahr speichert, verarbeitet oder überträgt.</li> </ul>		Jährlich	Vierteljährlich

Stand der Einstufungskriterien Juli 2009



## Welche Vorteile haben Sie von der Zertifizierung?

Die Implementierung des PCI DSS erzeugt nicht nur eine Erhöhung des Sicherheitsniveaus zum Schutz der Kreditkartendaten sondern schafft auch einen Mehrwert für das gesamte Unternehmen:

- Identifizierung von Risiken bei Speicherung und Übermittlung von Kundendaten
- Darstellung eines klaren Weges zur Behandlung und Behebung von Risiken im Bereich der Datensicherheit
- Gewährleistung, dass andere Geschäftspartner Ihr Geschäft nicht gefährden
- Verbesserung des bereits bestehenden internen Kontrollsystems
- Demonstration der Wichtigkeit von Datensicherheit gegenüber Ihren Kunden
- Zusätzlich verbessern Sie den Schutz vor finanziellen Haftungsrisiken, Rechtskosten, Beweissicherungskosten und Imageschäden

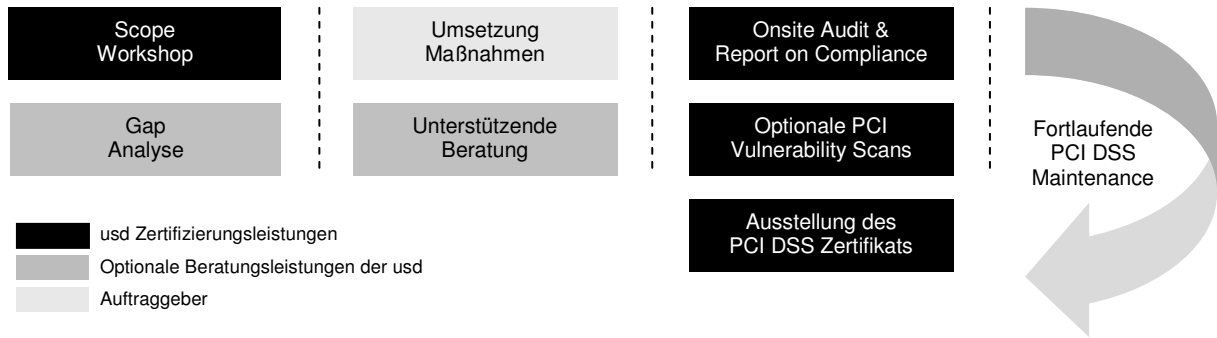
## Wie sehen die Anforderungen des Standards aus?

PCI DSS ist ein Best Practice Standard. Nachfolgende Übersicht zeigt die 12 Hauptanforderungen, die sich in ca. 160 Einzelrichtlinien konkretisieren:

Kontrollziel	Nr	Hauptanforderung
Aufbau und Betrieb eines sicheren Netzwerkes	1	Betrieb einer Firewall – Umgebung
	2	Vermeidung von herstellereigenen Standards für Systempasswörter und andere Sicherheitseinstellungen
Schutz der Kreditkartendaten	3	Schutz gespeicherter Daten
	4	Verschlüsselung der Übermittlung von Kreditkarten- und anderer sensibler Information über öffentliche Netzwerke
Management von Schwachstellen	5	Benutzung und regelmäßige Aktualisierung von Anti-Virus Software
	6	Entwicklung und Pflege sicherer Systeme und Anwendungen
Starker Zugriffsschutz	7	Beschränkung des Zugriffs auf Daten nach dem Need-to-Know- Prinzip
	8	Zuordnung einer individuellen USER-ID an Personen mit IT-Zugriff
	9	Beschränkung des physischen Zugriffs auf Kreditkarteninformationen
Regelmäßige Prüfung und Test des Netzwerkes	10	Überwachung und Nachverfolgung jeglicher Zugriffe auf Netzwerkressourcen und Kreditkarteninformationen
	11	Regelmäßige Tests der Sicherheitssysteme und -prozesse
Pflege einer Information Security Policy	12	Pflege einer Policy, welche die Informationssicherheit adressiert



## Wie sieht der Zertifizierungsprozess durch usd.de AG aus?



Die usd.de AG begleitet ihre Kunden während des gesamten Zertifizierungsprozesses, der im Allgemeinen folgende Phasen umfasst:

**Scope Workshop:** Im Scope Workshop wird eine vorläufige Festlegung des Zertifizierungsumfangs durchgeführt und die folgenden Phasen geplant.

**Gap Analyse:** Hier werden alle zu betrachtenden Systeme detailliert geprüft. Hilfsmittel und Methoden sind Interviews mit Prozess- und Systemverantwortlichen, Prüfung der Nachweisfähigkeit der relevanten Sicherheitsprozesse und System- bzw. Applikationsprüfungen. Das Ergebnis dieser Phase ist ein Action Plan in dem alle identifizierten Schwachstellen inklusive der Umsetzungstermine aufgeführt sind

**PCI Vulnerability Scans:** Sowohl externe Scans durch den ASV, als auch interne Penetrationstests müssen vor Durchführung des Onsite Audits erfolgreich durchgeführt werden. Die usd.de AG bietet die externen PCI Vulnerability Scans über ihr Scanportal isas unter <http://isas.usd.de> an.

**Umsetzungsphase:** In dieser Phase werden alle identifizierten Schwachstellen und Abweichungen vom Standard korrigiert. Experten der usd.de AG unterstützen diese Phase optional.

**Onsite Audit:** Das Zertifizierungsaudit ist ein formaler Prozess, der alle im Scope befindlichen Prozesse, Applikationen und Systeme auf Übereinstimmung mit dem Standard prüft.

**Berichterstellung:** Nach Abschluss des Zertifizierungsaudits wird vom QSA der Report on Compliance erstellt, der die jeweilige Implementierung der Anforderungen genau beschreibt und aufzeigt, wie der Auditor diese abgeprüft hat.

**Zertifikatsausstellung:** Nach erfolgreichem Abschluss der PCI Prüfungen und Freigabe des Reports on Compliance durch die Kreditartenorganisationen beziehungsweise durch das PCI Security Standards Council erhalten Sie von der usd Ihr persönliches PCI DSS Zertifikat und Prüfsiegel.

**Sie interessieren sich für unsere Leistungen?**  
Dann wenden Sie sich bitte an:

[kontakt@usd.de](mailto:kontakt@usd.de)  
+49 6103 90 34 69

Weitere Informationen zu PCI DSS und PCI Vulnerability Scans erhalten Sie unter:  
<http://isas.usd.de>

