



*Your complimentary
use period has ended.
Thank you for using
PDF Complete.*

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)



Payment Card Industry (PCI) Datensicherheitsstandard

Konformitätsbescheinigung für Selbstbeurteilungs-Fragebogen – Version für Händler

Version 1.2

Oktober 2008

Konformitätsbescheinigung, SBF D – Version für Händler

Anleitung zum Einreichen

Der Händler muss diese Konformitätsbescheinigung einreichen, um zu bestätigen, dass er den Konformitätsstatus mit den *Payment Card Industry Datensicherheitsstandard (PCI DSS)-Anforderungen und Sicherheitsbeurteilungsverfahren erfüllt*. Füllen Sie alle zutreffenden Abschnitte aus und schlagen Sie die Anleitung zum Einreichen unter *sPCI DSS-Konformität* . Schritte zum Ausfüllen%in diesem Dokument nach.

Teil 1. Informationen zum Unternehmen des Qualified Security Assessors (falls vorhanden)

Name des Unternehmens:					
QSA-Leiter:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2. Informationen zum Händlerunternehmen

Name des Unternehmens:		DBA(S):			
Name des Ansprechpartners:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2a. Typ des Händlerunternehmens (alle zutreffenden Optionen auswählen):

- Einzelhändler
 Telekommunikation
 Lebensmitteleinzelhandel und Supermärkte
 Erdöl/Erdgas
 E-Commerce
 Versandhandel
 Sonstiges (bitte genau angeben):

Liste der Einrichtungen und Standorte, die in der PCI DSS-Prüfung berücksichtigt wurden:

Teil 2b. Beziehungen

Hat Ihr Unternehmen eine Beziehung mit einem oder mehreren Drittdienstleistern (z. B. Gateways, Webhosting-Anbieter, Flugreiseagenturen, Anbieter von Kundentreueprogrammen usw.)? Ja Nein

Hat Ihr Unternehmen eine Beziehung zu mehr als einem Acquirer? Ja Nein



*Your complimentary
use period has ended.
Thank you for using
PDF Complete.*

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

Verwendete Zahlungsanwendung:

Version der Zahlungsanwendung:

Teil 3. PCI DSS-Validierung

Anhand der Ergebnisse, die in SBF D mit Datum vom (*Ausfülldatum*) notiert wurden, bestätigt (*Name des Händlerunternehmens*) folgenden Konformitätsstatus (eine Option auswählen):

- Konform:** Alle Abschnitte des PCI SBF sind komplett und alle Fragen wurden mit *Ja* beantwortet, was zu der Gesamtbewertung **KONFORM** geführt hat, **und** es wurde ein Scan von einem von PCI SSC zugelassenen Approved Scanning Vendor durchgeführt und bestanden, wodurch (*Name des Händlerunternehmens*) volle Konformität mit dem PCI DSS demonstriert hat.
- Nicht konform:** Nicht alle Abschnitte des PCI DSS SBF sind komplett oder einige Fragen wurden mit *Nein* beantwortet, was zu der Gesamtbewertung **NICHT KONFORM** geführt hat, **oder** es wurde kein Scan von einem von PCI SSC zugelassenen Approved Scanning Vendor durchgeführt und bestanden, wodurch (*Name des Händlerunternehmens*) nicht die volle Konformität mit dem PCI DSS demonstriert hat.

Zieldatum für Konformität:

Eine Stelle, die dieses Formular mit dem Status *Nicht konform* einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

Teil 3a. Bestätigung des Status „Konform“

Händler bestätigt:

- PCI DSS Selbstbeurteilungs-Fragebogen D, Version (*Version des SBF*), wurde den enthaltenen Anleitungen gemäß ausgefüllt.
- Alle Informationen im oben genannten SBF und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung in allen materiellen Aspekten korrekt dar.
- Mein POS-Systemanbieter hat mir bestätigt, dass in meinem POS-System nach der Autorisierung keine vertraulichen Authentifizierungsdaten gespeichert werden.
- Ich habe den PCI DSS gelesen und erkenne an, dass ich jederzeit eine vollständige PCI DSS-Konformität aufweisen muss.
- Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifendaten (aus einer Spur),¹CAV2-, CVC2-, CID- oder CVV2-Daten²oder PIN-Daten³ gespeichert wurden.

Teil 3b. Bestätigung durch den Händler

<i>Unterschrift des Beauftragten des Händlers</i> ↑	<i>Datum</i> ↑
<i>Name des Beauftragten des Händlers</i> ↑	<i>Titel</i> ↑

¹ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Spurdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

² Der drei- oder vierstellige Wert, der im oder rechts neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

³ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen Konformitätsstatus für jede Anforderung aus. Wenn Sie eine der Anforderungen mit „NEIN“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung erfüllt. Geben Sie außerdem eine kurze Beschreibung der Aktionen an, die unternommen werden, um die Anforderung zu erfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

PCI DSS- Anforderung	Anforderungsbeschreibung	Konformitätsstatus (eine Option auswählen)		Abhilfedatum und Aktionen (bei Konformitätsstatus „NEIN“)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	<input type="checkbox"/>	<input type="checkbox"/>	
3	Schutz gespeicherter Karteninhaberdaten	<input type="checkbox"/>	<input type="checkbox"/>	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	<input type="checkbox"/>	<input type="checkbox"/>	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	<input type="checkbox"/>	<input type="checkbox"/>	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	<input type="checkbox"/>	<input type="checkbox"/>	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	<input type="checkbox"/>	<input type="checkbox"/>	
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	<input type="checkbox"/>	<input type="checkbox"/>	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	<input type="checkbox"/>	<input type="checkbox"/>	
12	Befolgung einer Informationssicherheits-Richtlinie	<input type="checkbox"/>	<input type="checkbox"/>	



*Your complimentary
use period has ended.
Thank you for using
PDF Complete.*

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)

