



**Payment Card Industry (PCI)  
Datensicherheitsstandard  
Selbstbeurteilungsfragebogen**

---

**Anleitung und Richtlinien**

**Version 2.0**

Oktober 2010

## Dokumentänderungen

---

Datum	Version	Beschreibung
1. Oktober 2008	1.2	Anpassung der Inhalte an den neuen PCI-DSS v1.2 und Implementieren kleinerer Änderungen in der Ursprungsversion v1.1.
28. Oktober 2010	2.0	Anpassung der Inhalte an den PCI-DSS v2.0 und Erläuterung der SBF-Umgebungstypen und Qualifikationskriterien. Ergänzung des SBF C-VT für Händler mit webbasierten virtuellen Terminals

## **Inhalt**

---

<b>Anleitung und Richtlinien Version 2.0 Oktober 2010 .....</b>	<b>1</b>
<b>Dokumentänderungen .....</b>	<b>2</b>
<b>Über dieses Dokument .....</b>	<b>4</b>
<b>PCI-DSS Selbstbeurteilung: Wie alles zusammenpasst .....</b>	<b>5</b>
<b>PCI-Datensicherheitsstandard: Zugehörige Dokumente .....</b>	<b>6</b>
<b>SBF-Überblick .....</b>	<b>7</b>
<b>Warum ist die PCI-DSS-Konformität so wichtig? .....</b>	<b>8</b>
<b>Allgemeine Tipps und Strategien zur Konformitätsüberprüfung.....</b>	<b>10</b>
<b>Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind. ....</b>	<b>13</b>
SBF A – Händler, bei denen die Karte nicht vorliegt, alle Karteninhaberdaten-Funktionen wurden ausgegliedert.....	13
SBF B – Händler, die ausschließlich Abdruckgeräte oder eigenständige Terminals mit Dial-Out-Funktion verwenden. Kein elektronischer Karteninhaberdaten-Speicher. ....	15
SBF C-VT – Händler mit webbasierten virtuellen Terminals ohne elektronische Karteninhaberdaten-Speicher.....	15
SBF C – Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind, kein elektronischer Karteninhaberdaten-Speicher .....	16
SBF D – Alle anderen Händler und Dienstleister, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden. ....	17
<b>Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen .....</b>	<b>18</b>
<b>Anleitung zum Ausfüllen des SBF .....</b>	<b>18</b>
<b>Welcher SBF eignet sich am besten für meine Umgebung? .....</b>	<b>19</b>

## Über dieses Dokument

---

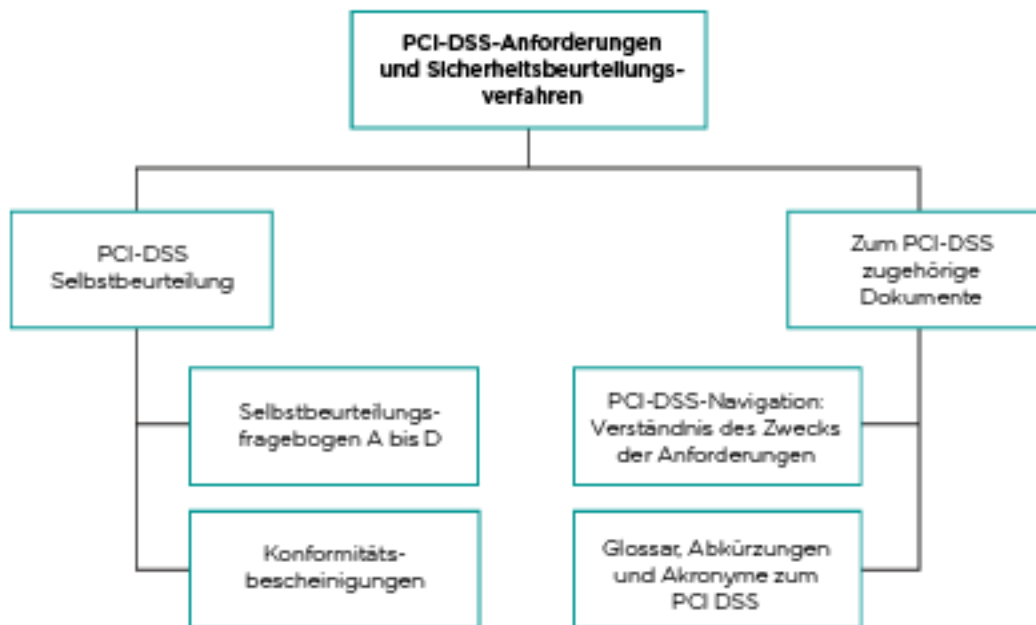
Dieses Dokument wurde als Unterstützung für Händler und Dienstleister entwickelt, um sie besser über den Selbstbeurteilungsfragebogen (SBF) zum Payment Card Industry Datensicherheitsstandard (PCI-DSS) zu informieren. Lesen Sie sich diese Anleitung und Richtlinien gründlich durch, um sich darüber zu informieren, warum der PCI-DSS für Ihr Unternehmen so wichtig ist, welche Strategien Ihr Unternehmen einsetzen kann, um die Konformitätsvalidierung zu erleichtern und ob Ihr Unternehmen qualifiziert ist, eine verkürzte Version des SBF auszufüllen. In den folgenden Abschnitten wird umrissen, was Sie über den PCI-DSS SBF wissen müssen.

- PCI-DSS Selbstbeurteilung: Wie alles zusammenpasst
- PCI-DSS: Zugehörige Dokumente
- SBF-Überblick
- Warum ist die PCI-DSS-Konformität so wichtig?
- Allgemeine Tipps und Strategien zur Konformitätsüberprüfung
- Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind.
- Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen
- Anleitung zum Ausfüllen des SBF
- Welcher SBF eignet sich am besten für meine Umgebung?

## PCI-DSS Selbstbeurteilung: Wie alles zusammenpasst

Der PCI-DSS und die begleitenden Dokumente stellen einen gemeinsamen Satz von Branchentools und -messdaten dar, die den sicheren Umgang mit empfindlichen Informationen gewährleisten sollen. Der Standard schafft einen Handlungsrahmen zur Entwicklung eines robusten Sicherheitsprozesses für Kontoinformationen und zur Vermeidung und Feststellung von Sicherheitsvorfällen sowie zur Reaktion auf derartige Vorfälle. Um das Risiko einer Sicherheitsverletzung und deren Auswirkungen zu mindern, müssen alle Einheiten, die Karteninhaberdaten speichern, verarbeiten oder übertragen, dem Standard entsprechen. Das nachstehende Diagramm zeigt die Tools, die implementiert wurden, um Unternehmen zu helfen, die PCI-DSS-Anforderungen zu erfüllen und ihre Konformität selbst zu beurteilen.

Diese und andere Dokumente finden Sie unter: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).



## PCI-Datensicherheitsstandard: Zugehörige Dokumente

Die folgenden Dokumente wurden als Unterstützung für Händler und Dienstanbieter entwickelt, um sie besser über den PCI-DSS und den PCI-DSS SBF zu informieren.

Dokument	Publikum
<i>PCI-Datensicherheitsstandard: Anforderungen und Sicherheitsbeurteilungsverfahren</i>	Alle Händler und Dienstanbieter
<i>PCI-DSS-Navigation: Verständnis des Zwecks der Anforderungen</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen A und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen B und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen C-VT und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen C und Bescheinigung</i>	Qualifizierte Händler <sup>1</sup>
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungsfragebogen D und Bescheinigung</i>	Qualifizierte Händler und Dienstanbieter <sup>1</sup>
<i>PCI-Datensicherheitsstandard und Datensicherheitsstandard für Zahlungsanwendungen: Glossar für Begriffe, Abkürzungen und Akronyme</i>	Alle Händler und Dienstanbieter

<sup>1</sup> Um zu ermitteln, welcher Selbstbeurteilungsfragebogen sich am besten eignet, lesen Sie in diesem Dokument auf Seite 12 den Abschnitt „Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind“.

## SBF-Überblick

---

Der *PCI-DSS Selbstbeurteilungsfragebogen (SBF)* ist ein Validierungstool mit dem Ziel, Händler und Dienstleister bei der Selbstbeurteilung ihrer Konformität mit den Datensicherheitsstandards der Zahlungskartenindustrie (Payment Card Industry Data Security Standard oder DSS) zu unterstützen. Es gibt mehrere Versionen des PCI-DSS SBF für verschiedene Szenarien. Dieses Dokument soll Unternehmen helfen, zu bestimmen, welcher SBF für sie am besten geeignet ist.

Der PCI-DSS SBF ist ein Validierungstool für Händler und Dienstleister, die im Rahmen der *PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren* vor Ort keine Datensicherheitsbeurteilung zur Erstellung eines Konformitätsberichts durchführen müssen, welcher unter Umständen von Ihrem Acquirer oder von Ihrer Zahlungsmarke verlangt wird. Details zu den PCI-DSS-Validierungsanforderungen erhalten Sie von Ihrem Acquirer oder Ihrer Zahlungsmarke.

Der PCI-DSS SBF besteht aus folgenden Komponenten:

1. Fragen zu den PCI-DSS-Anforderungen, die für Dienstleister und Händler vorgesehen sind: Siehe „Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind“ in diesem Dokument.
2. Konformitätsbescheinigung: Die Bescheinigung bestätigt, dass Sie für die Durchführung einer PCI-DSS-Selbstbeurteilung qualifiziert sind und diese durchgeführt haben.

## Warum ist die PCI-DSS-Konformität so wichtig?

---

Die Mitglieder des PCI Security Standards Council (American Express, Discover, JCB, MasterCard und Visa) überwachen kontinuierlich Fälle von Sicherheitsverletzungen von Kontodaten. Diese Sicherheitsverletzungen umfassen das gesamte Unternehmensspektrum, von sehr kleinen bis hin zu sehr großen Händlern und Dienst Anbietern.

Eine Sicherheitsverletzung und die dadurch entstandene Gefährdung von Zahlungsdaten haben weit reichende Konsequenzen für die betroffenen Unternehmen, u. a.:

1. Auflagen zur Benachrichtigung von Behörden;
2. Rufverlust;
3. Kundenverlust;
4. Potenzielle finanzielle Haftung (z. B. durch gesetzliche Auflagen, Gebühren und Strafzahlungen); und
5. Juristische Folgen.

Bei der Analyse von bereits aufgetretenen Sicherheitsverletzungen wurden allgemeine Sicherheitsschwächen ermittelt, die vom PCI-DSS angesprochen werden, aber zum Zeitpunkt der Sicherheitsverletzung nicht implementiert waren. Der PCI-DSS wurde genau aus diesem Grund entwickelt und enthält detaillierte Anforderungen, um die Gefahr einer Sicherheitsverletzung und deren Auswirkungen zu minimieren.

Untersuchungen nach Sicherheitsverletzungen weisen einheitlich auf häufige PCI-DSS-Verletzungen hin. U. a. folgende Punkte treten dabei zutage:

- Speicherung von Magnetstreifendaten (Anforderung 3.2). Es muss darauf hingewiesen werden, dass viele Stellen, bei denen es zu Sicherheitsverletzungen kam, gar nicht wussten, dass diese Daten auf ihren Systemen gespeichert waren.
- Unzureichende Zugriffskontrollen aufgrund inkorrekt installierter Händler-POS-Systeme, wodurch böswillige Benutzer auf für POS-Händler vorgesehene Wege eindringen konnten (Anforderungen 7.1, 7.2, 8.2 und 8.3);
- Standardsystemeinstellungen und Kennwörter, die bei der Systemeinrichtung nicht geändert wurden (Anforderung 2.1);
- Unnötige und unsichere Dienste, die nicht gelöscht oder geschützt wurden, als das System eingerichtet wurde (Anforderungen 2.2.2 und 2.2.4);
- Schlecht programmierte Webanwendungen, die zu SQL-Injektionen und anderen Anfälligkeiten führen, wodurch direkt von der Website aus auf die Datenbank mit den Karteninhaberdaten zugegriffen werden kann (Anforderung 6.5);
- Fehlende und veraltete Sicherheitspatches (Anforderung 6.1);
- Mangelnde Protokollierung (Anforderung 10);
- Mangelnde Überwachung (mittels Protokollüberprüfungen, Intrusionserfassung/-prävention, vierteljährliche Anfälligkeitsscans und Systeme zur Überwachung der Dateintegrität) (Anforderungen 10.6, 11.2, 11.4 und 11.5);
- Schlecht implementierte Netzwerksegmentierung, die dazu führt, dass die Karteninhaberdaten-Umgebung unwissentlich in anderen Teilen des Netzwerks, die nicht entsprechend des PCI-DSS gesichert wurden, Schwachstellen ausgesetzt ist (z. B. durch unsichere Zugriffspunkte auf

drahtlose Netzwerke und Schwachstellen, die über Mitarbeiter-E-Mails und Webbrowser verursacht werden) (Anforderung 1.2, 1.3 und 1.4);

## Allgemeine Tipps und Strategien zur Konformitätsüberprüfung

---

Es folgen einige allgemeine Tipps und Strategien für den Beginn Ihrer PCI-DSS-Konformitäts-Überprüfungsbemühungen. Mit diesen Tipps können Sie nicht benötigte Daten eliminieren, die benötigten Daten in definierten und kontrollierten zentralisierten Bereichen isolieren und den Umfang Ihrer PCI-DSS-Konformitäts-Überprüfungsbemühungen eingrenzen. Beispielsweise können Sie aus dem Umfang Ihrer Selbstbeurteilung nicht benötigte Daten löschen und/oder Daten in definierten und kontrollierten Bereichen isolieren, Sie können Systeme und Netzwerke entfernen, die keine Karteninhaberdaten speichern, verarbeiten oder übertragen und die nicht mit Systemen verbunden sind, die dies tun.

1. **Empfindliche Authentifizierungsdaten (umfasst gesamten Inhalt des Magnetstreifens, Kartenüberprüfungs-codes und -werte, PINs und PIN-Blöcke):**
  - a. Sie dürfen diese Daten **unter keinen Umständen speichern**.
  - b. Falls Sie sich nicht sicher sind, fragen Sie den Anbieter Ihres POS-Systems, ob das Softwareprodukt und die Version, die Sie verwenden, diese Daten speichert. Sie können auch einen qualifizierten Sicherheitsexperten beauftragen, um für Sie zu bestimmen, ob empfindliche Authentifizierungsinformationen irgendwo in Ihren Systemen gespeichert, protokolliert oder erfasst werden.
2. **Falls Sie ein Händler sind, wenden Sie sich mit den folgenden von uns vorgeschlagenen Fragen zur Sicherheit an den Anbieter Ihres POS-Systems:**
  - a. Wurde meine POS-Software gemäß Payment Application Data Security Standard (PA-DSS) validiert? (Konsultieren Sie die Liste PCI-DSS-validierter Zahlungsanwendungen.)
  - b. Speichert meine POS-Software Daten vom Magnetstreifen (Verfolgungsdaten) oder PIN-Blöcke? Falls ja: Ein solcher Speicher ist verboten. Wie schnell können Sie mir helfen, ihn zu entfernen?
  - c. Speichert meine POS-Software Primary Account Numbers (PANs)? Falls ja: Dieser Speicher muss geschützt werden. Wie schützt die POS-Software diese Daten?
  - d. Dokumentieren Sie die Liste der von der Anwendung geschriebenen Dateien mit einer Zusammenfassung des Inhalts jeder Datei, um zu gewährleisten, dass die genannten, verbotenen Daten nicht gespeichert werden?
  - e. Erfordert Ihr POS-System, dass ich eine Firewall installiere, um meine Systeme vor unberechtigten Zugriffen zu schützen?
  - f. Sind komplexe und einmalige Kennwörter erforderlich, um auf meine Systeme zuzugreifen? Können Sie bestätigen, dass Sie für mein System sowie die von Ihnen unterstützten Systeme anderer Händler keine gemeinsamen oder Standardkennwörter verwenden?
  - g. Wurden die Standardeinstellungen und -kennwörter auf den Systemen und in den Datenbanken, die Teil des POS-Systems sind, geändert?
  - h. Wurden alle unnötigen und unsicheren Dienste von den Systemen und Datenbanken, die Teil des POS-Systems sind, entfernt?
  - i. Greifen Sie remote auf mein POS-System zu? Falls ja, haben Sie angemessene Kontrollen implementiert, damit niemand anders auf mein POS-System zugreifen kann, z. B. werden sichere Remote-Zugriffsmethoden und keine gemeinsamen oder Standardkennwörter verwendet? Wie oft greifen Sie remote auf mein POS-System zu und warum? Wer ist berechtigt, remote auf mein POS-System zuzugreifen?
  - j. Wurden alle Systeme und Datenbanken, die Teil des POS-Systems sind, mit allen geltenden Sicherheitsupdates aktualisiert?

- k. Wurde die Protokollfunktion für die Systeme und Datenbanken, die Teil des POS-Systems sind, aktiviert?
- l. Falls vorherige Versionen meiner POS-Software Verfolgungsdaten gespeichert haben, wurde diese Funktion bei aktuellen Updates der POS-Software entfernt? Wurde zum Entfernen dieser Daten ein sicheres Löschverfahren (Secure Wipe) verwendet?

### 3. Karteninhaberdaten – falls nicht benötigt, nicht speichern!

- a. Zahlungsmarkenregeln gestatten das Speichern der persönlichen Kontonummer (Personal Account Number oder PAN), des Ablaufdatums, des Karteninhabernamens und des Servicecodes.
- b. Machen Sie eine Inventur aller Gründe und Orte zum Speichern dieser Daten. Dienen die Daten keinem nützlichen Geschäftszweck, sollten Sie sie löschen.
- c. Überlegen Sie sich, ob das Speichern dieser Daten und der dadurch unterstützte Geschäftsprozess Folgendes wert sind:
  - i. Das Risiko, das unbefugte Personen darauf zugreifen;
  - ii. Zusätzlicher PCI-DSS-Aufwand zum Schutz dieser Daten;
  - iii. Kontinuierlicher Pflegeaufwand, um die PCI-DSS-Kompatibilität aufrecht zu erhalten.

### 4. Karteninhaberdaten – falls benötigt, konsolidieren und isolieren!

Sie können den Umfang einer PCI-DSS-Beurteilung durch die Konsolidierung des Datenspeichers in einer genau definierten Umgebung und durch Isolieren der Daten mit einer korrekten Netzwerksegmentierung beschränken. Wenn Ihre Mitarbeiter z. B. im Internet browsen und E-Mails auf demselben Rechner oder im selben Netzwerksegment empfangen, in dem sich Karteninhaberdaten befinden, sollten Sie die Karteninhaberdaten auf einem eigenen Rechner oder in einem separaten Netzwerksegment (mithilfe von Routern oder Firewalls) segmentieren (isolieren). Wenn Sie die Karteninhaberdaten effektiv isolieren können, können Sie Ihre PCI-DSS-Bemühungen evtl. auf den isolierten Teil konzentrieren, anstatt all Ihre Rechner überprüfen zu müssen.

### 5. Kompensationskontrollen

Kompensationskontrollen können für die meisten PCI-DSS-Anforderungen in Erwägung gezogen werden, wenn ein Unternehmen die technische Spezifikation einer Anforderung nicht erfüllen kann, das damit verbundene Risiko aber ausreichend durch alternative Kontrollen gemindert hat. Falls Ihr Unternehmen nicht genau die Kontrolle gemäß PCI-DSS-Spezifikation einsetzt, dafür andere Kontrollen implementiert hat, die der PCI-DSS-Definition für Kompensationskontrollen entsprechen (siehe „Kompensationskontrollen“ im Anhang des jeweiligen SBF und im *Glossar, Abkürzungen und Akronyme* zum PCI-DSS unter [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)), sollte Ihr Unternehmen wie folgt vorgehen:

- a. Antworten Sie auf die SBF-Frage mit „JA“ und notieren Sie in der Spalte „Spezial“ die Verwendung aller Kompensationskontrollen, die zur Erfüllung einer Anforderung eingesetzt werden.
- b. Gehen Sie die Punkte unter „Kompensationskontrollen“ im Anhang B des jeweiligen SBF durch und dokumentieren Sie die Verwendung von Kompensationskontrollen, indem Sie das Arbeitsblatt C des SBF zu den Kompensationskontrollen ausfüllen.
- c. Füllen Sie für jede Anforderung, die durch eine Kompensationskontrolle erfüllt wird, ein Arbeitsblatt zu Kompensationskontrollen aus.
- d. Reichen Sie alle ausgefüllten Arbeitsblätter zu Kompensationskontrollen mit Ihrem SBF bzw. Ihrer Bescheinigung ein. Gehen Sie dabei gemäß der Anweisungen Ihres Acquirers oder der Zahlungsmarke vor.

## 6. Fachmännische Unterstützung und Schulungen

- a. Falls Sie Hilfe von einem Sicherheitsexperten benötigen, um die Richtlinien zu erfüllen und den SBF auszufüllen, können Sie gerne fachmännische Unterstützung in Anspruch nehmen. Sie können zwar einen Sicherheitsexperten Ihrer Wahl einsetzen, doch werden nur die auf der PCI-SSC-Liste der qualifizierten Sicherheitsprüfer (Qualified Security Assessors oder QSAs) als QSAs anerkannt und von PCI-SSC geschult. Diese Liste können Sie unter <https://www.pcisecuritystandards.org> abrufen.
- b. Der PCI-Security Standards Council (SSC) bietet eine Vielzahl von Schulungsmaterialien, um in der Zahlungskartenindustrie weiter das Bewusstsein für Sicherheit zu fördern. Zu diesen Ressourcen gehören auch die PCI-DSS-Schulung für Interne Sicherheitsberater (Internal Security Assessors, ISAs) und Schulungen zu Standards. Auch die Internetseite des PCI-DSS bietet erstklassige zusätzliche Materialien, darunter:
- Der *PCI-DSS-Navigationsleitfaden*
  - Das *PCI-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*
  - Häufig gestellte Fragen (FAQs)
  - Webinare
  - Ergänzungen und Richtlinien
  - Konformitätsbescheinigungen

Für weitere Informationen besuchen Sie bitte [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Hinweis:** Die Ergänzungen komplementieren den PCI-DSS und bestimmen zusätzliche Aspekte und Empfehlungen zur Einhaltung der PCI-DSS-Anforderungen – sie ändern, eliminieren oder ersetzen nicht den PCI-DSS oder dessen Anforderungen.

## Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind.

Je nach den Regeln der Zahlungsmarke müssen alle Händler und Dienstanbieter den gesamten PCI-DSS erfüllen. Es gibt fünf SBF-Kategorien, die in der nachstehenden Tabelle kurz vorgestellt und in den folgenden Abschnitten ausführlicher erläutert werden. Mit der Tabelle können Sie beurteilen, welcher SBF für Ihr Unternehmen zutrifft. Lesen Sie dann die ausführlichen Beschreibungen, um zu gewährleisten, dass Sie alle Anforderungen für diesen SBF erfüllen.

SBF	Beschreibung
A	Händler, bei denen die Karte nicht vorliegt (E-Commerce oder Versandhandel), alle Karteninhaberdaten-Funktionen wurden ausgegliedert. <i>Dies gilt nicht für Händler mit physischer Präsenz.</i>
B	Händler, die ausschließlich Abdruckgeräte ohne elektronischen Karteninhaberdaten-Speicher verwenden, oder Händler mit eigenständigen Terminals mit Dial-Out-Funktion ohne elektronischen Karteninhaberdaten-Speicher.
C-VT	Händler ausschließlich mit webbasierten virtuellen Terminals ohne elektronischen Karteninhaberdaten-Speicher
C	Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind, kein elektronischer Karteninhaberdaten-Speicher
D	Alle anderen Händler, die nicht in den Beschreibungen für SBF A bis C oben enthalten sind, und <b>alle Dienstanbieter</b> , die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden.

### SBF A – Händler, bei denen die Karte nicht vorliegt, alle Karteninhaberdaten-Funktionen wurden ausgegliedert.

*SBF A wurde entwickelt, um die Anforderungen an Händler anzusprechen, die nur Papierdokumente oder -quittungen mit Karteninhaberdaten aufbewahren, keine Karteninhaberdaten in elektronischer Form speichern und vor Ort oder auf ihren Systemen keine Karteninhaberdaten verarbeiten oder übertragen.*

*Für eine grafische Anleitung zur Auswahl des geeigneten SBF-Typs siehe „Welcher SBF eignet sich am besten für meine Umgebung?“ auf Seite 17.*

SBF A-Händler speichern keine Karteninhaberdaten in elektronischem Format und verarbeiten oder übertragen weder vor Ort noch auf ihren Systemen Karteninhaberdaten; sie müssen die Einhaltung der Anforderungen validieren, indem sie den SBF A und die zugehörige Konformitätsbescheinigung ausfüllen und folgende Punkte bestätigen:

- Ihr Unternehmen akzeptiert nur Transaktionen, bei denen die Karte nicht physisch vorliegt (E-Commerce oder Versandhandel);
- Ihr Unternehmen speichert, verarbeitet oder überträgt Karteninhaberdaten weder vor Ort noch auf Ihren Systemen, sondern verlässt sich voll und ganz auf einen oder mehrere Drittunternehmen, die diese Funktionen übernehmen;
- Ihr Unternehmen hat bestätigt, dass die Handhabung, Speicherung, Verarbeitung bzw. Übertragung der Karteninhaberdaten durch das oder die Drittunternehmen den PCI-DSS erfüllen.

- Ihr Unternehmen bewahrt ausschließlich Papierdokumente oder -quittungen mit Karteninhaberdaten auf und diese Dokumente werden nicht elektronisch entgegengenommen;  
**und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

**Diese Option würde nie für Händler in einer physischen POS-Umgebung (persönlicher Publikumsverkehr) gelten.**

## **SBF B – Händler, die ausschließlich Abdruckgeräte oder eigenständige Terminals mit Dial-Out-Funktion verwenden. Kein elektronischer Karteninhaberdaten-Speicher.**

*SBF B wurde entwickelt, um die Anforderungen an Händler anzusprechen, die Karteninhaberdaten nur mithilfe von Abdruckgeräten oder eigenständigen Terminals mit Dial-Out-Funktion verarbeiten.*

SBF B-Händler verarbeiten Karteninhaberdaten über eigenständige Terminals mit Dial-Out-Funktion. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder E-Commerce- bzw. Versandhändler (Karte liegt nicht vor) handeln. Diese Händler validieren die Konformität, indem sie den SBF B und die zugehörige Konformitätsbescheinigung ausfüllen, in der sie Folgendes bestätigen:

- Ihr Unternehmen verwendet ausschließlich ein Abdruckgerät und/oder eigenständige Terminals mit Dial-Out-Funktion (über eine Telefonleitung mit Ihrem Prozessor verbunden), um die Zahlungskarteninformationen Ihrer Kunden zu erfassen;
- Die eigenständigen Terminals mit Dial-Out-Funktion sind nicht mit anderen Systemen in Ihrer Umgebung verbunden;
- Die eigenständigen Terminals mit Dial-Out-Funktion sind nicht mit dem Internet verbunden;
- Ihr Unternehmen überträgt keine Karteninhaberdaten über Netzwerke (weder interne Netzwerke noch über das Internet);
- Ihr Unternehmen bewahrt ausschließlich Papierdokumente oder Kopien von Quittungen mit Karteninhaberdaten auf und diese Dokumente werden nicht elektronisch entgegengenommen;  
**und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

*Für eine grafische Anleitung zur Auswahl des geeigneten SBF-Typs siehe „Welcher SBF eignet sich am besten für meine Umgebung?“ auf Seite 17.*

## **SBF C-VT – Händler mit webbasierten virtuellen Terminals ohne elektronische Karteninhaberdaten-Speicher**

*Der SBF C-VT wurde entwickelt, um die Anforderungen an Händler anzusprechen, die Karteninhaberdaten nur mithilfe eigenständiger virtueller Terminals auf PCs mit Internetanschluss verarbeiten.*

Ein virtuelles Terminal ist ein Webbrowser-basierter Zugriffspunkt auf die Website eines Acquirers, eines Verarbeitungsunternehmens oder eines Drittanbieters zur Autorisierung von Transaktionen mit Zahlungskarten; auf dieser Website gibt ein Händler manuell Karteninhaberdaten über einen sicher verbundenen Webbrowser ein. Anders als physische Terminals lesen virtuelle Terminals Daten nicht direkt von Zahlungskarten. Da die Transaktionen mit Zahlungskarten manuell eingegeben werden, werden in Händlerumgebungen mit niedrigen Transaktionsvolumen virtuelle Terminals häufig anstatt physischer Terminals eingesetzt.

*Für eine grafische Anleitung zur Auswahl des geeigneten SBF-Typs siehe „Welcher SBF eignet sich am besten für meine Umgebung?“ auf Seite 17.*

Diese Händler verarbeiten Karteninhaberdaten nur über ein virtuelles Terminal und speichern keine Karteninhaberdaten auf Computersystemen. Diese virtuellen Terminals sind mit dem Internet verbunden, um sich mit dem Drittanbieter in Kontakt zu setzen, der die Zahlungsabwicklungsfunktion auf dem virtuellen Terminal hostet. Dieser Drittanbieter kann entweder ein Verarbeitungsunternehmen, ein Acquirer oder ein anderer Drittdienstleister sein, der Karteninhaberdaten speichert, verarbeitet und/oder überträgt, um die Zahlungstransaktionen auf virtuellen Terminals von Händlern zu autorisieren und/oder abzuwickeln.

Diese SBF-Option gilt nur für Händler, die gleichzeitig immer nur eine Transaktion manuell über eine Tastatur einer internetbasierten virtuellen Terminallösung eingeben.

SBF C-VT Händler verarbeiten Karteninhaberdaten über virtuelle Terminals auf PCs, die mit dem Internet verbunden sind, und sie speichern keine Karteninhaberdaten auf Computersystemen. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder Versandhändler (Karte liegt nicht vor) handeln. Diese Händler validieren Ihre Konformität, indem sie den SBF C-VT und die zugehörige Konformitätsbescheinigung ausfüllen, in der sie Folgendes bestätigen:

- Die Zahlungsvorgänge Ihres Unternehmens werden über ein virtuelles Terminal abgewickelt, auf das über einen mit dem Internet verbundenen Webbrowser zugegriffen wird;
- Die virtuelle Terminallösung Ihres Unternehmens wird von einem vom PCI-DSS validierten Drittdienstleister angeboten und gehostet;
- Ihr Unternehmen greift auf die PCI-DSS-konforme virtuelle Terminallösung über einen isolierten Computer einer einzelnen Stelle zu, der innerhalb Ihrer Umgebung weder mit anderen Stellen noch Systemen verbunden ist (diese Eigenschaft kann mithilfe einer Firewall- oder Netzwerksegmentierung erreicht werden, um den Computer von anderen Systemen zu trennen.);
- Auf dem Computer Ihres Unternehmens ist keine Software installiert, die bewirkt, dass Karteninhaberdaten gespeichert werden (z. B. gibt es keine Software zur Batchverarbeitung oder Store-and-Forward);
- Am Computer Ihres Unternehmens sind keine Hardware-Geräte angeschlossen, die zum Erfassen und Speichern von Karteninhaberdaten verwendet werden (z. B. Kartenlesegeräte);
- Ihr Unternehmen empfängt oder überträgt auch anderweitig über andere Kanäle keine Karteninhaberdaten (z. B. über ein internes Netzwerk oder das Internet);
- Ihr Unternehmen bewahrt nur Berichte oder Kopien der Quittungen auf Papier auf; **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

**Diese Option trifft nicht auf E-Commerce-Händler zu.**

## **SBF C – Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind, kein elektronischer Karteninhaberdaten-Speicher**

*SBF C wurde speziell für die Anforderungen entwickelt, die für Händler gelten, deren Zahlungsanwendungssysteme (z. B. Point-Of-Sale-Systeme) aus folgenden Gründen mit dem Internet verbunden sind (beispielsweise über DSL, Kabel, Modem usw.):*

1. *Das Zahlungsanwendungssystem befindet sich auf einem PC, der mit dem Internet verbunden ist (z. B. für E-Mails oder Webrowsing); oder*
2. *das Zahlungsanwendungssystem ist mit dem Internet verbunden, um Karteninhaberdaten zu übertragen.*

*Für eine grafische Anleitung zur Auswahl des geeigneten SBF-Typs siehe „Welcher SBF eignet sich am besten für meine Umgebung?“ auf Seite 17.*

SBF C-Händler verarbeiten Karteninhaberdaten über POS-Systeme oder andere Zahlungsanwendungssysteme, die mit dem Internet verbunden sind und keine Karteninhaberdaten auf Computersystemen speichern. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder E-Commerce- bzw. Versandhändler (Karte liegt nicht vor) handeln. SBF C-Händler bestätigen die Einhaltung der Anforderungen, indem sie den SBF C und die zugehörige Konformitätsbescheinigung ausfüllen und folgende Punkte bestätigen:

- Ihr Unternehmen verfügt über ein Zahlungsanwendungssystem und eine Internetverbindung auf demselben Gerät und/oder demselben Local Area Network (LAN);
- Das Zahlungsanwendungssystem/Internetgerät ist nicht mit anderen Systemen Ihrer Umgebung verbunden (dies kann mithilfe einer Netzwerksegmentierung zur Isolierung des Zahlungsanwendungssystems/Internetgeräts von allen anderen Systemen erreicht werden);
- Die Unternehmensverkaufsstelle ist nicht mit anderen Filialen verbunden und LANs werden immer jeweils nur für ein Geschäft eingerichtet;
- Ihr Unternehmen bewahrt nur Berichte oder Kopien der Quittungen auf Papier auf;
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format; **und**
- Der Anbieter der Zahlungsanwendungssoftware Ihres Unternehmens verwendet sichere Techniken zur Bereitstellung von Remote-Unterstützung für Ihr Zahlungsanwendungssystem.

### **SBF D – Alle anderen Händler und Dienstleister, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden.**

*Der SBF D wurde für alle Dienstleister entwickelt, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden, sowie für SBF-qualifizierte Händler, die nicht die Beschreibungen der SBFs des Typs A bis C oben erfüllen.*

SBF D Dienstleister und Händler müssen die Einhaltung der Anforderungen bestätigen, indem sie den SBF D und die zugehörige Konformitätsbescheinigung ausfüllen.

Während viele Unternehmen, die SBF D ausfüllen, um die Einhaltung aller PCI-DSS-Anforderungen zu bestätigen, werden einige Unternehmen mit sehr spezifischen Geschäftsmodellen evtl. feststellen, dass einige Anforderungen für sie nicht gelten. Ein Unternehmen, das z. B. überhaupt keine drahtlose Technologie verwendet, muss die Einhaltung der Abschnitte des PCI-DSS, die sich speziell auf die Verwaltung drahtloser Technologien beziehen, nicht validieren. In der nachstehenden Anleitung finden Sie Informationen über den Ausschluss drahtloser Technologie und anderer spezifischer Anforderungen.

## Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

---

**Ausschlusskriterien:** Wenn Sie SBF C oder D ausfüllen müssen, um Ihre PCI-DSS-Konformität zu bestätigen, können folgende Ausnahmen berücksichtigt werden: Lesen Sie unten den Abschnitt „Nichtanwendbarkeit“, um die jeweils zutreffende SBF-Antwort zu erfahren.

- Anforderungen 1.2.3, 2.1.1 und 4.1.1 (SBFs C und D): Die für drahtlose Technologien spezifischen Fragen müssen nur beantwortet werden, wenn in Ihrem Netzwerk drahtlose Technologien verwendet werden. Bitte beachten Sie, dass die Anforderung 11.1 (Verwendung eines Prozesses zur Erkennung unbefugter WLAN-Zugriffspunkte) auch beantwortet werden muss, wenn Sie in Ihrem Netzwerk keine drahtlose Technologie verwenden, weil der Prozess alle sicherheitsgefährdenden oder unerlaubten Geräte erfasst, die vielleicht ohne Ihr Wissen angeschlossen wurden.
- Anforderungen 6.3 bis 6.5 (SBF D): Diese Fragen beziehen sich auf benutzerspezifische Anwendungen und Codes und müssen nur beantwortet werden, wenn Ihr Unternehmen eigene benutzerdefinierte Anwendungen entwickelt.
- Anforderungen 9.1 bis 9.4 (SBF D): Die Fragen müssen nur von Stellen mit „zugangsbeschränkten Bereichen“ (siehe Definition) beantwortet werden. „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Dazu zählen nicht Bereiche, in denen ausschließlich Point-of-Sale-Terminals vorhanden sind, wie zum Beispiel der Kassensbereich in einem Einzelhandel. Hierin eingeschlossen sind jedoch Back-Office-Serverräume in Einzelhandelsgeschäften, in denen Karteninhaberdaten gespeichert werden, sowie Speicherbereiche für große Mengen an Karteninhaberdaten.

**Nichtanwendbarkeit:** In allen SBFs müssen diese und alle anderen Anforderungen, die nicht für Ihre Umgebung gelten, in der Spalte „Spezial“ mit „N/A“ gekennzeichnet werden. Dementsprechend müssen Sie das Arbeitsblatt „Erläuterung der Nichtanwendbarkeit“ im Anhang des SBF für jeden einzelnen Eintrag, der „N/A“ lautet, ausfüllen.

## Anleitung zum Ausfüllen des SBF

---

1. Verwenden Sie die hierin geschilderten Richtlinien, um zu ermitteln, welcher SBF sich für Ihr Unternehmen eignet.
2. Unter *PCI-DSS-Navigation: Verständnis des Zwecks der Anforderungen* finden Sie Informationen darüber, wie und warum die Anforderungen für Ihr Unternehmen relevant sind.
3. Bewerten Sie Ihre Umgebung auf die Einhaltung des PCI-DSS.
4. Verwenden Sie den jeweiligen Selbstbeurteilungsfragebogen als Hilfsmittel zur Validierung Ihrer PCI-DSS-Konformität.
5. Folgen Sie den Anleitungen im jeweiligen Selbstbeurteilungsfragebogen unter „PCI-DSS-Konformität – Schritte zum Ausfüllen“, und stellen Sie alle erforderlichen Dokumentationen für Ihren Acquirer oder Ihre Zahlungsmarke bereit.

# Welcher SBF eignet sich am besten für meine Umgebung?

