



Payment Card Industry (PCI)- Datensicherheitsstandard **Selbstbeurteilungs-Fragebogen**

Anleitung und Richtlinien

Version 1.2

Oktober 2008

Dokumentänderungen

Datum	Version	Beschreibung
1. Oktober 2008	1.2	Angleichen von Inhalten mit dem neuen PCI-DSS v1.2 und Implementieren kleinerer Änderungen an der Ursprungsversion v1.1.

Inhalt

Dokumentänderungen	ii
Über dieses Dokument	1
Selbstbeurteilung zum PCI-Datensicherheitsstandard: Wie alles zusammenpasst	2
PCI-Datensicherheitsstandard: Damit verbundene Dokumente	3
SBF-Überblick	4
Warum ist die PCI-DSS-Konformität so wichtig?	5
Allgemeine Tipps und Strategien zur Konformitätsüberprüfung	6
Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind	8
<i>SBF Validierungstyp 1 / SBF A: Karte nicht vorliegend, alle Karteninhaber-Datenfunktionen extern vergeben.....</i>	<i>8</i>
<i>SBF Validierungstyp 2 / SBF B: Nur-Abdruck-Händler, kein elektronischer Karteninhaber-Datenspeicher</i>	<i>9</i>
<i>SBF Validierungstyp 3 / SBF B: Händler mit eigenständigen Terminals mit Dial-Out-Funktion, kein elektronischer Karteninhaber-Datenspeicher</i>	<i>9</i>
<i>SBF Validierungstyp 4 / SBF C: Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind.....</i>	<i>9</i>
<i>SBF Validierungstyp 5 / SBF D: Alle anderen Händler und alle Dienstleister, die von einer Zahlungsmarke als zum Ausfüllen eines SBF qualifiziert definiert werden.....</i>	<i>10</i>
<i>Anweisungen bezüglich der Ungültigkeit und zum Ausschluss bestimmter Anforderungen.....</i>	<i>10</i>
Anleitung zum Ausfüllen des SBF	11
SBF-Anleitung und Richtlinien — Wie lautet mein Validierungstyp?	12

Über dieses Dokument

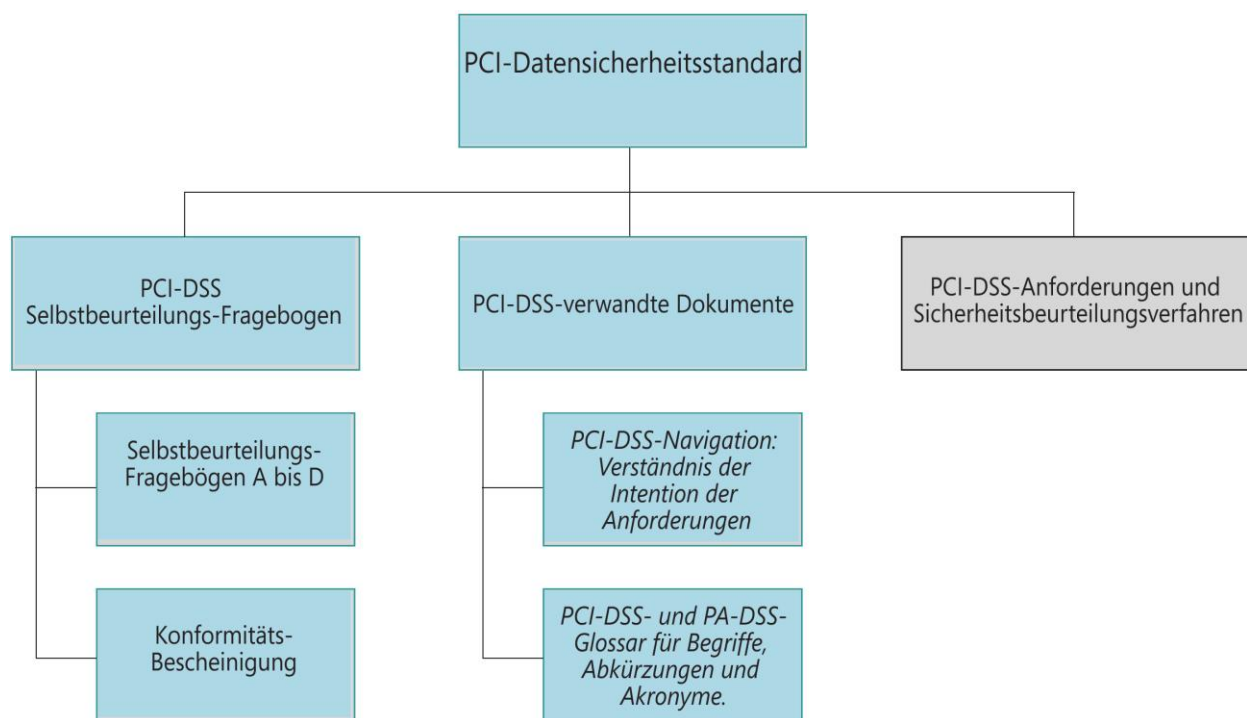
Dieses Dokument wurde als Hilfe für Händler und Dienstleister entwickelt, damit sie besser über den Selbstbeurteilungs-Fragebogen (SBF) zum PCI Datensicherheitsstandard (DSS) informiert sind. Lesen Sie diese Anleitung und Richtlinien gründlich durch, um sich darüber zu informieren, warum der PCI-DSS für Ihr Unternehmen wichtig ist, welche Strategien Ihr Unternehmen einsetzen kann, um die Konformitätsvalidierung zu erleichtern und ob Ihr Unternehmen qualifiziert ist, eine der kürzeren Versionen des SBF auszufüllen. In den folgenden Abschnitten wird umrissen, was Sie über den PCI-DSS-SBF wissen müssen.

- Selbstbeurteilung zum PCI-Datensicherheitsstandard: Wie alles zusammenpasst
- PCI-Datensicherheitsstandard: Damit verbundene Dokumente
- SBF-Überblick
- Warum ist die PCI-DSS-Konformität so wichtig?
- Allgemeine Tipps und Strategien
- Auswahl des SBF, der für Ihr Unternehmen am besten geeignet ist
- Anweisungen bezüglich der Ungültigkeit und zum Ausschluss bestimmter Anforderungen
- Ausfüllen des Fragebogens

Selbstbeurteilung zum PCI-Datensicherheitsstandard: Wie alles zusammenpasst

Der PCI-Datensicherheitsstandard und die begleitenden Dokumente stellen einen gemeinsamen Satz von Branchentools und -messdaten dar, die den sicheren Umgang mit vertraulichen Informationen gewährleisten sollen. Der Standard schafft einen Handlungsrahmen zur Entwicklung eines robusten Kontodatensicherheits-Prozesses einschließlich Vermeidung und Feststellung von Sicherheitsvorfällen und die Reaktion darauf. 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-Konformität zu erzielen und ihre Konformität selbst zu beurteilen.

Diese und andere Dokumente finden Sie unter: www.pcisecuritystandards.org.



PCI-Datensicherheitsstandard: Damit verbundene Dokumente

Die folgenden Dokumente wurden als Hilfe für Händler und Dienstanbieter entwickelt, damit sie besser über den PCI-Datensicherheitsstandard (DSS) und den PCI-DSS-SBF informiert werden.

Dokument	Publikum
<i>PCI-Datensicherheitsstandard: Anforderungen und Sicherheitsbeurteilungsverfahren</i>	Alle Händler und Dienstanbieter
<i>PCI-DSS-Navigation: Verständnis der Intention der Anforderungen</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen A und Bescheinigung</i>	Händler ¹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen B und Bescheinigung</i>	Händler ¹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen C und Bescheinigung</i>	Händler ¹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen D und Bescheinigung</i>	Händler ¹ und alle Dienstanbieter
<i>PCI-DSS- und PCI-PA-Glossar für Begriffe, Abkürzungen und Akronyme (PCI Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms)</i>	Alle Händler und Dienstanbieter

¹ Informationen zum Bestimmen des angemessenen Selbstbeurteilungs-Fragebogen finden Sie unter *PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung*, „Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind“

SBF-Überblick

Der Selbstbeurteilungs-Fragebogen zum PCI-Datensicherheitsstandard ist ein Validierungstool mit dem Ziel, Händlern und Dienstanietern bei der Selbstbeurteilung ihrer Einhaltung des 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 Dienstanieter, die keine Datensicherheitsbeurteilung vor Ort im Rahmen der PCI-DSS -Anforderungen und Sicherheitsbeurteilungsverfahren durchführen müssen, das von Ihrem Acquirer oder von ihrer Zahlungsmarke evtl. 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 Dienstanieter 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 der jeweiligen 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 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)
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 Hacker auf für POS-Händler vorgesehenen Wegen 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 entfernt oder korrigiert wurden, als das System eingerichtet wurde (Anforderung 2.2.2)
- 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 Sicherheits-Patches (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)
- Mangelnde Netzwerksegmentierung, wodurch über Schwachstellen in anderen Teilen des Netzwerks (z. B. Wireless-Zugriffspunkte, Mitarbeiter-E-Mail und Webbrowsing) leicht auf Karteninhaberdaten zugegriffen werden kann (Anforderungen 1.3 und 1.4)

Allgemeine Tipps und Strategien zur Konformitätsüberprüfung

Es folgen einige allgemeine Tipps und Strategien für den Beginn Ihrer PCI-DSS-Konformitätsüberprüfungsmaßnahmen. 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-Konformitätsüberprüfungsmaßnahmen eingrenzen. Wenn Sie z. B. Daten eliminieren, die Sie nicht benötigen, bzw. diese Daten in definierten und kontrollierten Bereichen isolieren, können Sie Systeme und Netzwerke, die keine Karteninhaberdaten mehr speichern, verarbeiten oder übertragen, aus Ihrer Selbstbeurteilung ausschließen.

1. Empfindliche Authentifizierungsdaten (umfasst gesamten Inhalt des Magnetstreifens, Kartvalidierungs-codes und -werte sowie PIN-Blöcke):

- a. Sie dürfen **diese Daten nie 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. Ist meine POS-Software gemäß dem Datensicherheitsstandard für Zahlungsanwendungen validiert (beziehen Sie sich auf die Liste validierter Zahlungsanwendungen des PCI SSC)?
- 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. 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?
- d. Erfordert Ihr POS-System, dass ich eine Firewall installiere, um meine Systeme vor unberechtigtem Zugriff zu schützen?
- e. 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?
- f. Wurden die Standardeinstellungen und -kennwörter auf den Systemen und in den Datenbanken, die Teil des POS-Systems sind, geändert?
- g. Wurden alle unnötigen und unsicheren Dienste von den Systemen und Datenbanken, die Teil des POS-Systems sind, entfernt?
- h. Greifen Sie dezentral 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 dezentral auf mein POS-System zu und warum? Wer ist berechtigt, dezentral auf mein POS-System zuzugreifen?
- i. Wurden alle Systeme und Datenbanken, die Teil des POS-Systems sind, mit allen geltenden Sicherheitsupdates aktualisiert?
- j. Wurde die Protokollfunktion für die Systeme und Datenbanken, die Teil des POS-Systems sind, aktiviert?
- k. 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 wertvollen Geschäftszweck, sollten Sie sie löschen.
- c. Überlegen Sie sich, ob das Speichern dieser Daten und der dadurch unterstützte Geschäftsprozess Folgendes wert sind:
 - i. Risiko, dass von Unberechtigten darauf zugegriffen wird
 - ii. Zusätzliche PCI-DSS-Bemühungen zum Schutz dieser Daten
 - iii. Kontinuierliche Pflegebemühungen, um die PCI-DSS-Kompatibilität aufrecht zu erhalten

4. Karteninhaberdaten – falls benötigt, konsolidieren und isolieren!

- a. Sie können den Umfang einer PCI-DSS-Beurteilung durch Konsolidieren des Datenspeichers in einer genau definierten Umgebung und Isolieren der Daten mittels korrekter Netzwerksegmentierung beschränken. Wenn Ihre Mitarbeiter z. B. im Internet browsen und E-Mail auf dem gleichen Rechner oder im gleichen 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, statt all Ihre Rechner überprüfen zu müssen.

5. Erwägung von Kompensationskontrollen

- a. 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 gemindert hat. Falls Ihr Unternehmen nicht die genaue Kontrolle gemäß PCI-DSS-Spezifikation einsetzt, dafür andere Kontrollen implementiert hat, die der PCI-DSS-Definition für Kompensationskontrollen entsprechen (siehe „Kompensationskontrollen“ im Anhang zu SBF und das PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme unter www.pcisecuritystandards.org), sollte Ihr Unternehmen wie folgt vorgehen:
 - i. Beantworten Sie die SBF-Frage mit „JA“ und geben Sie in der Spalte „Spezial“ die Verwendung jeder Kompensationskontrolle an, die zur Erfüllung der Anforderung eingesetzt wird.
 - ii. Gehen Sie die Punkte unter „Kompensationskontrollen“ im Anhang durch und dokumentieren Sie die Verwendung von Kompensationskontrollen, indem Sie das Arbeitsblatt zu Kompensationskontrollen ausfüllen.
 - a) Füllen Sie für jede Anforderung, die durch eine Kompensationskontrolle erfüllt wird, ein Arbeitsblatt zu Kompensationskontrollen aus.
 - iii. Reichen Sie alle ausgefüllten Arbeitsblätter zu Kompensationskontrollen mit Ihrem SBF bzw. Ihrer Bescheinigung ein. Gehen Sie dabei gemäß der Anweisungen Ihres Acquirers oder der Bezahlungsmarke vor.

6. Fachmännische Unterstützung

- a. Wir empfehlen, einen Sicherheitsexperten zu Rate zu ziehen, wenn Sie Unterstützung benötigen, um die Konformität zu erzielen und den SBF auszufüllen, werden Sie dazu ermutigt. 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 vom PCI SSC geschult. Diese Liste finden Sie unter https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

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 dem PCI-Datensicherheitsstandard in seiner Gesamtheit entsprechen. Es gibt fünf SBF-Validierungskategorien, 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-Validierungstyp	Beschreibung	SBF
1	Händler, bei denen Karte nicht vorliegt (E-Commerce oder Bestellung per Post/Telefon), alle Karteninhaber-Datenfunktionen extern vergeben <i>Dies würde für Händler mit physischer Präsenz nie gelten.</i>	A
2	Nur-Abdruck-Händler ohne Karteninhaber-Datenspeicher	B
3	Händler mit eigenständigen Terminals mit Dial-Out-Funktion, kein Karteninhaber-Datenspeicher	B
4	Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind, kein Karteninhaber-Datenspeicher	C
5	Alle anderen Händler (nicht in den Beschreibungen für SBF A-C oben enthalten) und alle Dienstanbieter , die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden	D

SBF Validierungstyp 1 / SBF A: *Karte nicht vorliegend, alle Karteninhaber-Datenfunktionen extern vergeben*

SBF A wurde entwickelt, um die Anforderungen an Händler anzusprechen, die nur Papierdokumente oder -quittungen mit Karteninhaberdaten führen, Karteninhaberdaten nicht in elektronischem Format speichern und vor Ort keine Karteninhaberdaten verarbeiten oder übertragen.

Händler des Validierungstyps 1 speichern keine Karteninhaberdaten in elektronischem Format und verarbeiten oder übertragen keine Karteninhaberdaten vor Ort; sie müssen die Konformität durch Ausfüllen von SBF A und der zugehörigen Konformitätsbescheinigung validieren und bestätigen, dass Folgendes zutrifft:

- Ihr Unternehmen führt nur Transaktionen durch, bei denen die Karte nicht physisch vorliegt (E-Commerce oder Bestellungen per Post/Telefon).
- Ihr Unternehmen speichert, verarbeitet oder überträgt keine Karteninhaberdaten vor Ort, sondern verlässt sich ganz auf einen Dritten, der diese Funktionen übernimmt.
- Ihr Unternehmen hat bestätigt, dass die Handhabung, Speicherung, Verarbeitung bzw. Übertragung der Karteninhaberdaten durch den Dritten den PCI-DSS erfüllt.
- Ihr Unternehmen bewahrt nur Papierdokumente oder -quittungen mit Karteninhaberdaten auf, und diese Dokumente werden nicht elektronisch empfangen **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Eine grafische Anleitung zur Auswahl des Validierungstyps finden Sie unter „SBF-Anleitung und Richtlinien – Wie lautet mein Validierungstyp“ auf Seite 12.

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

SBF Validierungstyp 2 / SBF B: *Nur-Abdruck-Händler, kein elektronischer Karteninhaber-Datenspeicher*

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

Händler des Validierungstyps 2 verarbeiten Karteninhaberdaten nur mithilfe von Abdruckmaschinen und müssen die Konformität durch Ausfüllen von SBF B und der damit verbundenen Konformitätsbescheinigung validieren, wodurch sie Folgendes bestätigen:

- Ihr Unternehmen verwendet nur Abdruckmaschinen, um die Zahlungskarteninformationen Ihrer Kunden entgegen zu nehmen.
- Ihr Unternehmen überträgt keine Karteninhaberdaten über eine Telefonleitung oder das Internet.
- Ihr Unternehmen bewahrt nur Kopien der Quittungen auf Papier auf und
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Eine grafische Anleitung zur Auswahl des Validierungstyps finden Sie unter „SBF-Anleitung und Richtlinien – Wie lautet mein Validierungstyp“ auf Seite 12.

SBF Validierungstyp 3 / SBF B: *Händler mit eigenständigen Terminals mit Dial-Out-Funktion, kein elektronischer Karteninhaber-Datenspeicher*

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

Händler des Validierungstyps 3 verarbeiten Karteninhaberdaten über eigenständige Terminals mit Dial-Out-Funktion. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder E-Commerce- bzw. Post-/Telefonbestellungshändler (Karte liegt nicht vor) handeln. Händler des Validierungstyps 3 müssen die Konformität durch Ausfüllen von SBF B und der damit verbundenen Konformitätsbescheinigung validieren, wodurch sie Folgendes bestätigen:

- Ihr Unternehmen verwendet nur eigenständige Terminals mit Dial-Out-Funktion (über eine Telefonleitung mit Ihrem Prozessor verbunden).
- 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 bewahrt nur Berichte oder Kopien der Quittungen auf Papier auf und
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

SBF Validierungstyp 4 / SBF C: *Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind*

SBF C wurde speziell für die Anforderungen entwickelt, die für Händler gelten, deren Zahlungsanwendungssysteme (z. B. Point-Of-Sale- oder Warenkorbsysteme) über Hochgeschwindigkeitsverbindung, DSL, Kabelmodem usw. aus folgenden Gründen mit dem Internet verbunden sind:

1. Das Zahlungsanwendungssystem befindet sich auf einem Computer, der mit dem Internet verbunden ist (z. B. für E-Mail oder Webbrowsing) oder
2. das Zahlungsanwendungssystem ist mit dem Internet verbunden, um Karteninhaberdaten zu übertragen.

Händler des Validierungstyps 4 verarbeiten Karteninhaberdaten über Zahlungsanwendungssysteme, die mit dem Internet verbunden sind, und speichern Karteninhaberdaten nicht auf einem Computersystem. Dabei kann es sich um normale Ladengeschäfte (Karte liegt vor) oder E-Commerce- bzw. Post-/Telefonbestellungshändler (Karte liegt nicht vor) handeln. Händler des Validierungstyps 4 müssen die Konformität durch Ausfüllen von SBF C und der damit verbundenen Konformitätsbescheinigung validieren, wodurch sie Folgendes bestätigen:

- Ihr Unternehmen hat auf dem gleichen Gerät ein Zahlungsanwendungssystem und eine Internetverbindung.
- Das Gerät mit Zahlungsanwendungssystem/Internetverbindung ist nicht mit anderen Systemen in Ihrer Umgebung verbunden.
- 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.

Eine grafische Anleitung zur Auswahl des Validierungstyps finden Sie unter „SBF-Anleitung und Richtlinien – Wie lautet mein Validierungstyp“ auf Seite 12.

SBF Validierungstyp 5 / SBF D: Alle anderen Händler und alle Dienstleister, die von einer Zahlungsmarke als zum Ausfüllen eines SBF qualifiziert definiert werden

SBF D spricht die Anforderungen an, die für alle Dienstleister gelten, die von einer Zahlungsmarke als für einen SBF qualifiziert beurteilt wurden, sowie für Händler, die nicht zu den Validierungstypen 1 – 4 zu zählen sind.

Dienstleister und Händler des Validierungstyps 5 müssen die Konformität durch Ausfüllen von SBF D und der damit verbundenen Konformitätsbescheinigung validieren.

Während viele Unternehmen, die SBF D ausfüllen, die Konformität mit jeder PCI-DSS-Anforderung bestätigen müssen, 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 Konformität mit den Abschnitten des PCI-DSS, die sich speziell auf drahtlose Technologie beziehen, nicht validieren. In der nachstehenden Anleitung finden Sie Informationen über den Ausschluss drahtloser Technologie und bestimmte andere spezifische Anforderungen.

Anweisungen bezüglich der Ungültigkeit und zum Ausschluss bestimmter Anforderungen

Ausschluss: Wenn Sie SBF C oder D ausfüllen müssen, um Ihre PCI-DSS-Konformität zu bestätigen, können folgende Ausnahmen berücksichtigt werden. Die korrekte SBF-Antwort finden Sie weiter unten unter „Ungültigkeit“.

- Anforderungen 1.2.3 (SBF D), 2.1.1 (SBF C und D) und 4.1.1 (SBF D): Diese für drahtlose Technologie spezifischen Fragen müssen nur beantwortet werden, wenn drahtlose Technologie in Ihrem Netzwerk verwendet wird. Bitte beachten Sie, dass Anforderung 11.1 (Verwendung eines Analysators für drahtlose Netzwerke) auch beantwortet werden muss, wenn Sie in Ihrem Netzwerk keine drahtlose Technologie verwenden, weil der Analysator alle sicherheitsgefährdenden oder nicht berechtigten Geräte erfasst, die vielleicht ohne Ihr Wissen hinzugefügt wurden.
- Anforderungen 6.3 – 6.5 (SBF D): Diese Fragen zu benutzerdefinierten Anwendungen und Codes müssen nur beantwortet werden, wenn Ihr Unternehmen eigene benutzerdefinierte Webanwendungen programmiert.

- Anforderungen 9.1 – 9.4 (SBF D): Diese Fragen müssen nur für Einrichtungen beantwortet werden, die „zugangsbeschränkte Bereiche“ gemäß der nachfolgenden Definition aufweisen. „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassensbereich im Einzelhandel), zählen nicht hierzu.

Ungültigkeit: Diese und andere Anforderungen, die für Ihre Umgebung nicht gelten, müssen in allen SBFs in der Spalte „Spezial“ als „Nicht zutr.“ gekennzeichnet werden. Für jeden mit „Nicht zutr.“ gekennzeichneten Eintrag muss das Arbeitsblatt „Erläuterung der Nichtanwendbarkeit“ im Anhang ausgefüllt werden.

Anleitung zum Ausfüllen des SBF

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

SBF-Anleitung und Richtlinien — Wie lautet mein Validierungstyp?

