Zahlungskartenbranche (PCI)
Datensicherheitsstandard

Selbstbeurteilungsfragebogen P2PE und Konformitätsbescheinigung

---

Nur Händler, die Zahlungsterminal-Hardware in einer PCI-SSC-notierten P2PE-Lösung verwenden – keine elektronische Speicherung von Karteninhaberdaten

Zur Verwendung mit PCI DSS Version 3.2.1

Juni 2018

Dokumentänderungen

Datum	PCI DSS Version	SBF Revision	Beschreibung
Nicht zutr.	1.0		(findet keine Anwendung)
Mai 2012	2.0		Erstellung des SBF P2PE-HW für Händler, die ausschließlich Hardware-Terminals im Rahmen einer validierten, PCI-SSC-notierten P2PE-Lösung verwenden. Dieser SBF ist für die Nutzung mit PCI DSS v2.0. bestimmt.
Februar 2014	3.0		Anpassung der Inhalte an die Anforderungen und Testverfahren nach PCI DSS v3.0 sowie Integration weiterer Reaktionsmöglichkeiten.
April 2015	3.1		Aktualisiert im Sinne des PCI-DSS v3.1. Ausführliche Informationen finden Sie unter *PA-DSS – Änderungsübersicht von PA-DSS Version 3.0 auf 3.1*. Aus dem Titel des SBF wurde “HW” entfernt, wie es von Händlern verwendet werden kann, die entweder eine HW/HW oder HW/Hybrid P2PE-Lösung verwenden.
Juli 2015	3.1	1.1	Aktualisiert durch Entfernen von Bezügen auf „bewährte Verfahren” vor dem 30. Juni 2015.
April 2016	3.2	1.0	Aktualisiert zur Übereinstimmung mit PCI DSS v3.2. Ausführliche Informationen zu den Änderungen am PCI DSS finden Sie unter *PCI DSS – Änderungsübersicht von PCI DSS Version 3.1 auf 3.2*. Es wurden die PCI DSS-Anforderungen 3.3 und 4.2 entfernt, wie durch die Implementierung der PCI P2PE-Lösung und von PIM abgedeckt.
Januar 2017	3.2	1.1	Dokumentänderungen wurden aktualisiert, um die in der Aktualisierung von April 2016 entfernten Anforderungen zu verdeutlichen.
Juni 2018	3.2.1	1.0	Aktualisiert zur Übereinstimmung mit PCI DSS v3.2.1. Ausführliche Informationen zu den Änderungen am PCI DSS finden Sie unter *PCI DSS – Änderungsübersicht von PCI DSS Version 3.2 auf 3.2.1.*

DANKSAGUNG:

Die englische Textversion dieses Dokuments wie auf der PCI SSC-Website angezeigt gilt für alle Zwecke als offizielle Version dieses Dokuments. Für den Fall von Mehrdeutigkeit oder Unstimmigkeit zwischen diesem und dem englischen Text hat die englische Version Vorrang.

Inhalt

Vorbereitung

Qualifikationskriterien für Händler für SBF P2PE

SBF P2PE wurde entsprechend den Anforderungen an Händler entwickelt, die Karteninhaberdaten nur mithilfe von Zahlungsterminal-Hardware im Rahmen einer validierten und PCI-notierten P2PE-Lösung (Point-to-Point Encryption, Punkt-zu-Punkt-Verschlüsselung) verarbeiten.

SBF-P2PE-Händler haben auf keinem Computersystem Zugriff auf Klartext-Daten von Karteninhabern und geben Kontodaten nur über Zahlungsterminal-Hardware mithilfe einer PCI-SSC-bewährten P2PE-Lösung ein. SBF-P2PE-Händler sind entweder Händler mit stationären (Brick-and-Mortar-)Verkaufsstellen (mit Vorlage der Karte) oder Versand- oder Telefonhändler (ohne Kartenvorlage). So kann ein Händler, der Bestellprozesse per E-Mail oder Telefon abwickelt, für SBF P2PE in Frage kommen, wenn er Karteninhaberdaten auf Papier oder über Telefon erhält und diese umgehend mit einem validierten P2PE-Hardware-Gerät verschlüsselt.

SBF-P2PE-Händler bestätigen für diesen Zahlungskanal folgendes:

- Sämtliche Zahlungsvorgänge werden über die vom PCI SSC genehmigte validierte P2PE-Lösung getätigt;
- Die einzigen Systeme in der Umgebung des Händlers, mit denen Kontodaten gespeichert, übermittelt oder verarbeitet werden, sind die für die Nutzung mit der validierten und PCI-notierten P2PE-Lösung genehmigten POI-Geräte (Point of Interaction);
- Auf andere Art und Weise werden von Ihrem Unternehmen keine elektronischen Karteninhaberdaten übermittelt oder empfangen;
- Dass kein Legacy-Speicher an elektronischen Karteninhaberdaten in der Umgebung vorhanden ist.
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, sind in Papierform (zum Beispiel Papierdokumente und -quittungen), und diese Dokumente werden nicht elektronisch entgegengenommen; und
- hat Ihr Unternehmen alle Kontrollen in der vom P2PE-Lösungsanbieter bereitgestellten *P2PE-Betriebsanleitung (P2PE Instruction Manual, PIM)* implementiert.

Dieser SBF gilt ausschließlich für E-Commerce-Kanäle.

Diese gekürzte Version des SBF enthält Fragen, die sich auf eine bestimmte Kleinhändlerumgebung, wie in den oben beschriebenen Qualifikationskriterien beschrieben, beziehen. Sollten für Ihre Umgebung PCI-DSS-Anforderungen gelten, die nicht in diesem SBF behandelt werden, kann dies ein Hinweis darauf sein, dass dieser SBF nicht für Ihr Unternehmen geeignet ist.

PCI-DSS-Selbstbeurteilung – Schritte zum Ausfüllen

1. Stellen Sie fest, welcher SBF für Ihre Umgebung relevant ist—Nähere Informationen finden Sie im Dokument *Anleitung und Richtlinien zum Selbstbeurteilungsfragebogen* auf der PCI-SSC-Website.
2. Bestätigen Sie, dass Ihre Umgebung dem Umfang/Geltungsbereich entspricht und die Qualifikationskriterien für den von Ihnen verwendeten SBF erfüllt (gemäß Definition in Teil 2g der Konformitätsbescheinigung).
3. Bestätigen Sie, dass Sie alle Elemente des PIMs implementiert haben.
4. Beurteilen Sie Ihre Umgebung hinsichtlich der Konformität mit den entsprechenden PCI-DSS-Anforderungen.
5. Füllen Sie alle Abschnitte des Dokuments aus:

- Abschnitt 1 (Teil 1 und 2 der Konformitätsbescheinigung) – Informationen zur Beurteilung und Executive Summary)
- Abschnitt 2 – PCI-DSS-Selbstbeurteilungsfragebogen (SBF P2PE)
- Abschnitt 3 (Teil 3 und 4 der Konformitätsbescheinigung) – Validierungs- und Bescheinigungsdetails sowie Aktionsplan für nicht konforme Anforderungen (falls zutreffend)

6. Senden Sie den SBF und die Konformitätsbescheinigung (AOC) zusammen mit allen anderen erforderlichen Dokumenten an Ihren Acquirer, Ihre Zahlungsmarke oder eine andere Anforderungsstelle.

Erklärungen zum Selbstbeurteilungsfragebogen

Die Fragen in der Spalte „PCI-DSS-Frage“ in diesem Selbstbeurteilungsfragebogen basieren auf den PCI-DSS-Anforderungen.

Als Hilfe beim Beurteilungsprozess stehen weitere Ressourcen mit Hinweisen zu den PCI-DSS-Anforderungen und zum Ausfüllen des Selbsbeurteilungsfragebogens zur Verfügung. Ein Teil dieser Ressourcen ist unten aufgeführt:

Dokument	enthält:
PCI DSS *(Anforderungen und Sicherheitsbeurteilungsverfahren des PCI-Datensicherheitsstandards)*	▪ Leitfaden zum Umfang/Geltungsbereich ▪ Leitfaden zum Zweck der PCI-DSS-Anforderungen ▪ Detaillierte Informationen zu Testverfahren ▪ Leitfaden zu Kompensationskontrollen
Anleitung und Richtlinien zum SBF	▪ Informationen zu allen SBF und ihren Qualifikationskriterien ▪ Bestimmung des passenden SBF für Ihr Unternehmen
PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme	▪ Beschreibungen und Definitionen von Begriffen, die im PCI DSS und in den Selbstbeurteilungsfragebögen vorkommen

Diese und weitere Ressourcen sind auf der PCI-SSC-Website *(www.pcisecuritystandards.org)* zu finden. Unternehmen sollten vor jeder Beurteilung den PCI DSS und weitere zugehörige Dokumente durchlesen.

Erwartete Tests

Die Anweisungen in der Spalte „Erwartete Tests “ basieren auf den Testverfahren im PCI DSS und beschreiben in allgemeiner Form die Testaktivitäten, mit denen die Erfüllung der Anforderungen überprüft werden sollte. Eine ausführliche Beschreibung der Testverfahren zu jeder Anforderung ist im PCI DSS zu finden.

Ausfüllen des Selbstbeurteilungsfragebogens

Zu jeder Frage gibt es mehrere Antwortmöglichkeiten. Die Antworten spiegeln den Status Ihres Unternehmens in Bezug auf die jeweilige Anforderung wider. ***Pro Frage ist nur eine Antwort auszuwählen.***

Die Bedeutung der jeweiligen Antworten ist in der Tabelle unten beschrieben:

Antwort	Wann trifft diese Antwort zu?
Ja	Die erwarteten Tests wurden durchgeführt und alle Elemente der Anforderung wurden wie angegeben erfüllt.
Ja, mit CCW (Compensating Control Worksheet, Arbeitsblatt zu Kompensationskontrollen)	Die erwarteten Tests wurden durchgeführt, und die Anforderung wurde unter Zuhilfenahme einer Kompensationskontrolle erfüllt. Für alle Antworten in dieser Spalte ist ein Arbeitsblatt zu Kompensationskontrollen (Compensating Control Worksheet, CCW) in Anhang B des SBF auszufüllen. Informationen zu Kompensationskontrollen und Hinweise zum Ausfüllen des Arbeitsblatts sind im PCI DSS enthalten.
Nein	Einige oder alle Elemente der Anforderung wurden nicht erfüllt, werden gerade implementiert oder müssen weiteren Tests unterzogen werden, ehe bekannt ist, ob sie vorhanden sind.
Nicht zutr. (Nicht zutreffend)	Die Anforderung gilt nicht für die Umgebung des Unternehmens. (Beispiele sind im *Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen* zu finden. Siehe unten.) Bei allen Antworten in dieser Spalte ist eine zusätzliche Erklärung in Anhang C des SBF erforderlich.

Leitfaden für die Nichtanwendbarkeit bestimmter Anforderungen

Gelten einzelne Anforderungen als nicht anwendbar in Ihrer Umgebung, wählen Sie für die betreffenden Anforderungen die Option „Nicht zutr.“ und füllen Sie zu jedem „Nicht zutr.“-Eintrag das Arbeitsblatt „Erklärung der Nichtanwendbarkeit“ in Anhang C aus.

Gesetzliche Ausnahme

Unterliegt Ihr Unternehmen einer gesetzlichen Beschränkung, welche die Erfüllung einer PCI-DSS-Anforderung unmöglich macht, markieren Sie für diese Anforderung die Spalte „Nein“ und füllen Sie die zugehörige Bescheinigung in Teil 3 aus.

1. Abschnitt: Informationen zur Beurteilung

Anleitung zum Einreichen

Dieses Dokument muss zur Bestätigung der Ergebnisse der Händler-Selbstbeurteilung gemäß dem *Datensicherheitsstandard der Zahlungskartenbranche (Payment Card Industry Data Security Standard, kurz PCI DSS) und den Sicherheitsbeurteilungsverfahren* ausgefüllt werden. Füllen Sie alle Abschnitte aus: Der Händler ist dafür verantwortlich, dass alle Abschnitte von den betreffenden Parteien ausgefüllt werden. Wenden Sie sich an Ihren Acquirer (Handelsbank) oder die Kartenunternehmen, um Berichts- und Sendeverfahren zu bestimmen.

Teil 1. Informationen zum Qualified Security Assessor und Händler

Teil 1a. Händlerinformationen

Firma:			DBA (Geschäftstätigkeit als):		
Name des Ansprechpartners:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 1b. Informationen zur Firma des Qualified Security Assessors (falls vorhanden)

Firma:					
QSA-Leiter:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 2. Zusammenfassung für die Geschäftsleitung

Teil 2a. Handelstätigkeit (alle zutreffenden Optionen auswählen)

☐ Einzelhändler ☐ Telekommunikation ☐ Lebensmitteleinzelhandel und Supermärkte

☐ Erdöl ☐ Bestellung über E-Mailoder Telefon (MOTO) ☐ Sonstige (bitte angeben):

Welche Arten von Zahlungskanälen werden von Ihrem Unternehmen bedient?	Welche Zahlungskanäle sind durch diesen SBF abgedeckt?
☐ Schriftliche/Telefonische Bestellung (MOTO)	☐ Schriftliche/Telefonische Bestellung (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Vorlage der Karte (persönlich)	☐ Vorlage der Karte (persönlich)

Hinweis: *Wird einer Ihrer Zahlungskanäle oder -prozesse durch diesen SBF nicht abgedeckt, wenden Sie sich bezüglich der Validierung für die anderen Kanäle an Ihren Acquirer oder Ihr Kartenunternehmen.*

Teil 2. Zusammenfassung für die Geschäftsleitung *(Fortsetzung)*

Teil 2b. Beschreibung des Zahlungskartengeschäfts

Wie und in welcher Kapazität speichert, verarbeitet bzw. überträgt Ihr Unternehmen Karteninhaberdaten?	

Teil 2c. Standorte

Listen Sie alle Einrichtungen (beispielsweise Einzelhandelsgeschäfte, Büroräume, Rechenzentren, Callcenter usw.) sowie eine Zusammenfassung der Standorte auf, die in der PCI-DSS-Prüfung berücksichtigt wurden.

Art der Einrichtung	Anzahl der Einrichtungen dieser Art	Standort(e) der Einrichtung (Ort, Land)
Beispiel: Einzelhandelsgeschäfte	*3*	*Boston, MA, USA*

Teil 2d. P2PE-Lösung

Geben Sie folgende Informationen zur validierten PCI P2PE-Lösung an, die in Ihrem Unternehmen verwendet wird:

Name des P2PE-Lösungsanbieters:	
Name der P2PE-Lösung:	
PCI-SSC-Referenznummer	
Vom Händler genutzte eingetragene P2PE-POI-Geräte (PTS Geräteabhängigkeiten):	

Teil 2e. Beschreibung der Umgebung

Beschreiben Sie ***in allgemeiner Form*** die in dieser Beurteilung berücksichtigte Umgebung. *Beispiel:* • *Ein- und ausgehende Verbindungen zur/von der CDE (cardholder data environment, Karteninhaberdaten-Umgebung).* • *Wichtige Systemkomponenten in der CDE, etwa POS-Geräte, Datenbanken und Webserver sowie weitere notwendige Zahlungskomponenten (falls zutreffend).*	
Nutzt Ihr Unternehmen die Netzwerksegmentierung auf eine Weise, dass der Umfang Ihrer PCI-DSS-Umgebung davon betroffen ist? *(Hinweise zur Netzwerksegmentierung finden Sie im PCI DSS im Abschnitt „Netzwerksegmentierung“.)*	☐ Ja ☐ Nein

Teil 2. Zusammenfassung für die Geschäftsleitung *(Fortsetzung)*

Teil 2f. Externe Dienstanbieter

Verwendet Ihr Unternehmen einen Qualified Integrator & Reseller (QIR)?	☐ Ja ☐ Nein

Falls ja:

Name des QIR-Unternehmens:	
Individuelle Bezeichnung des QIR:	
Beschreibung der vom QIR erbrachten Dienstleistungen:	

Werden Karteninhaberdaten von Ihrem Unternehmen an externe Dienstanbieter (beispielsweise Qualified Integrator & Resellers (QIR), Gateways, Flugreiseagenturen, Vertreter von Kundenbindungsprogrammen usw.) weitergegeben?	☐ Ja ☐ Nein

Falls ja:

Name des Dienstanbieters:	**Beschreibung der erbrachten Dienstleistungen:**

Hinweis: *Anforderung 12.8 gilt für alle Stellen in dieser Liste.*

Teil 2g. Qualifikation zum Ausfüllen des SBF P2PE

Der Händler bestätigt die Qualifikation zum Ausfüllen dieser Kurzfassung des Selbstbeurteilungsfragebogens (in Bezug auf diesen Zahlungskanal) aus folgenden Gründen:

☐	Sämtliche Zahlungsabwicklungen werden über die vom PCI SSC genehmigte und gelistete validierte P2PE-Lösung (wie oben beschrieben) getätigt.
☐	Die einzigen Systeme in der Umgebung des Händlers, mit denen Kontodaten gespeichert, übermittelt oder verarbeitet werden, sind die für die Nutzung mit der validierten und PCI-notierten P2PE-Lösung genehmigten POI-Geräte (Point of Interaction).
☐	Auf andere Art und Weise werden vom Händler keine elektronischen Karteninhaberdaten übermittelt oder empfangen.
☐	Der Händler stellt sicher, dass kein Legacy-Speicher an elektronischen Karteninhaberdaten in der Umgebung vorhanden ist.
☐	Wenn der Händler Karteninhaberdaten speichert, befinden sich diese nur in Berichten oder Kopien von Quittungen auf Papier und werden nicht elektronisch empfangen. **Außerdem**
☐	hat der Händler alle Kontrollen in der vom P2PE-Lösungsanbieter bereitgestellten P2PE-Betriebsanleitung (P2PE Instruction Manual, PIM) implementiert.

2. Abschnitt: Selbstbeurteilungsfragebogen P2PE

Hinweis: *Die folgenden Fragen wurden entsprechend den PCI-DSS-Anforderungen und Testverfahren nummeriert, so wie in den* PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren *beschrieben. Da nur eine Teilmenge der PCI-DSS-Anforderungen im Selbstbeurteilungsfragebogen P2PE aufgeführt ist, ist die Nummerierung der Fragen unter Umständen nicht konsekutiv.*

Selbstbeurteilung abgeschlossen am:

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Hinweis*: Die Anforderung 3 bezieht sich nur auf SBF-P2PE-Händler, die über Papierunterlagen (zum Beispiel Quittungen, gedruckte Berichte usw.) mit Kontodaten, einschließlich Kontonummern (Primary Account Numbers, PANs), verfügen.*

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
3.1	Umfassen die Richtlinien, Verfahren und Prozesse zur Datenaufbewahrung und zum Löschen von Daten folgende Punkte?					
	(a) Sind die Speichermenge und die Aufbewahrungszeit der Daten auf die für rechtliche, gesetzliche und/oder geschäftliche Zwecke festgelegten Vorgaben begrenzt?	▪ Richtlinien und Verfahren zum Aufbewahren und Löschen von Daten überprüfen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐
	(b) Wurden Prozesse für das sichere Löschen von Karteninhaberdaten festgelegt, wenn diese Daten nicht mehr für rechtliche, gesetzliche und/oder geschäftliche Zwecke benötigt werden?	▪ Richtlinien und Verfahren durchgehen. ▪ Mitarbeiter befragen. ▪ Verfahren zum Löschen von Daten untersuchen.	☐	☐	☐	☐
	(c) Gelten spezifische Anforderungen für die Aufbewahrung von Karteninhaberdaten? *Karteninhaberdaten müssen z. B. für den Zeitraum X aus den Geschäftsgründen Y aufbewahrt werden.*	▪ Richtlinien und Verfahren durchgehen. ▪ Mitarbeiter befragen. ▪ Aufbewahrungsanforderungen untersuchen.	☐	☐	☐	☐
	(d) Wurde ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten eingeführt, die den festgelegten Aufbewahrungszeitraum überschritten haben	▪ Richtlinien und Verfahren durchgehen. ▪ Mitarbeiter befragen. ▪ Löschprozesse verfolgen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
	(e) Erfüllen alle gespeicherten Karteninhaberdaten die in der Datenaufbewahrungsrichtlinie beschriebenen Anforderungen?	▪ Dateien und Systemdatensätze überprüfen.	☐	☐	☐	☐
Anweisung: *Werden die Punkte für die Anforderungen unter 3.1 mit „Ja“ beantwortet, bedeutet dies, dass der Händler Papierunterlagen (zum Beispiel Quittungen oder Papierberichte), die Kontodaten enthalten, nur so lange aufbewahrt, wie es für geschäftliche, rechtliche oder vorschriftsmäßige Zwecke erforderlich ist. Anschließend vernichtet er die Unterlagen .* *Wenn ein Händler niemals Papierunterlagen mit Kontodaten druckt oder aufbewahrt, kreuzt er die Spalte „Nicht zutreffend“ an und füllt das Arbeitsblatt „Erklärung der Nichtanwendbarkeit” im Anhang C aus.*						
3.2.2	Wird der Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte) für alle aufbewahrten Papierdokumente nach der Autorisierung tatsächlich nicht gespeichert?	▪ Papierdatenquellen überprüfen.	☐	☐	☐	☐
Anweisung: *Wird der Punkt für die Anforderung 3.2.2 mit „Ja“ beantwortet, bedeutet dies Folgendes: Sollte der Händler während der Durchführung einer Transaktion den Sicherheitscode einer Karte notieren, vernichtet er das entsprechende Papier entweder direkt nach Abschluss der Transaktion (zum Beispiel mit einem Schredder) oder macht den Code vor der Ablage des Papiers (zum Beispiel durch Ausschwärzen) unkenntlich.* *Wenn der Händler die drei- oder vierstellige Nummer auf der Vorder- oder Rückseite der Zahlungskarte (Kartensicherheitscode) niemals anfordert, sollte er die Spalte „Nicht zutreffend“ markieren und das Arbeitsblatt „Erklärung der Nichtanwendbarkeit” im Anhang C ausfüllen.*						
3.7	Sind Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren durchgehen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐
Anweisung: *Wird der Punkt für die Anforderung 3.7 mit „Ja“ beantwortet, bedeutet dies, dass der Händler über Richtlinien und Verfahren für die Anforderungen 3.1, 3.2.2 und 3.3 verfügt, sollte er Kontodaten in Papierform aufbewahren. Auf diese Weise kann sichergestellt werden, dass das Personal die Sicherheitsrichtlinien und dokumentierten betrieblichen Verfahren kennt und befolgt, so dass Karteninhaberdaten dauerhaft sicher gespeichert werden können.*						

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

Hinweis: *Die Anforderungen 9.5 und 9.8 beziehen sich nur auf SBF-P2PE-Händler, die über Papierunterlagen (zum Beispiel Quittungen, gedruckte Berichte usw.) mit Kontodaten, einschließlich PANs (Primary Account Numbers), verfügen.*

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
9.5	Wird die physische Sicherheit aller Medien gewährleistet (insbesondere Computer, elektronische Wechselmedien, Quittungen, Berichte und Faxe)? *Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Medien" auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.*	▪ Richtlinien und Verfahren zur physischen Sicherung von Medien durchgehen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐
9.8	(f) Werden alle Medien vernichtet, wenn sie nicht mehr zu geschäftlichen oder rechtlichen Zwecken benötigt werden?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen.	☐	☐	☐	☐
	(c) Erfolgt die Vernichtung von Medien wie nachstehend beschrieben?					
9.8.1	(g) Werden Ausdrucke Aktenvernichtern zugeführt, verbrannt oder aufgelöst, damit keine Karteninhaberdaten wiederhergestellt werden können?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen. ▪ Mitarbeiter befragen. ▪ Prozesse überprüfen.	☐	☐	☐	☐
	(b) Werden Container zur Aufbewahrung von zu vernichtenden Informationen so geschützt, dass Zugriffe auf diese Inhalte vermieden werden?	▪ Richtlinien und Verfahren zur regelmäßigen Vernichtung von Medien durchgehen. ▪ Sicherheit von Containern überprüfen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort (je Frage eine Antwort markieren)			
			Ja	Ja, mit CCW	Nein	Nicht zutr.
Anweisung: *Werden die Punkte für die Anforderungen unter 9.5 und 9.8 mit „Ja“ beantwortet, bedeutet dies, dass der Händler Papierdokumente mit Kontoinformationen sicher aufbewahrt (zum Beispiel in einem verriegelten Fach, Schrank oder Safe) und er diese zerstört, sobald sie nicht mehr für geschäftliche Zwecke erforderlich sind. Dies schließt ein schriftliches Dokument bzw. schriftliche Richtlinien für Mitarbeiter mit ein, in denen festgehalten ist, wie Papierdokumente mit Kontodaten zu sichern sind und wie diese zerstört werden, wenn sie nicht mehr benötigt werden.* *Wenn der Händler niemals Papierdokumente mit Kontoinformationen aufbewahrt, sollte er die Spalte „Nicht zutreffend“ markieren und das Arbeitsblatt „Erklärung der Nichtanwendbarkeit” im Anhang C ausfüllen.*						
9.9	Sind die Geräte, die Zahlungskartendaten über eine direkte physische Interaktion mit der Karte erfassen, vor Manipulation und Austausch geschützt? ***Hinweis:*** *Diese Anforderung gilt für Kartenlesegeräte, die bei Transaktionen eingesetzt werden, bei denen die Karte am Point-of-Sale vorliegt und durch das Gerät gezogen oder in das Gerät eingesteckt werden muss. Diese Anforderung gilt nicht für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke.*						
	(a) Sehen Richtlinien und Verfahren das Führen einer Liste solcher Geräte vor?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
	(b) Sehen Richtlinien und Verfahren vor, dass Geräte regelmäßig auf Manipulations- oder Austauschversuche untersucht werden?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
	(c) Sehen Richtlinien und Verfahren vor, dass das Bewusstsein der Mitarbeiter für verdächtiges Verhalten und das Melden der Manipulation bzw. des Austauschs von Geräten gefördert werden?	▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
9.9.1	(a) Enthält die Geräteliste folgende Angaben? - Fabrikat und Modell des Geräts - Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet) - Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung	▪ Geräteliste überprüfen.	☐	☐	☐	☐
	(b) Ist die Liste korrekt, vollständig und aktuell?	▪ Geräte und Gerätestandorte prüfen und mit der Liste vergleichen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
	(c) Wird die Geräteliste aktualisiert, sobald Geräte hinzugefügt, an einen anderen Standort gebracht, außer Betrieb genommen werden usw.?	▪ Mitarbeiter befragen.	☐	☐	☐	☐
9.9.2	(a) Werden Geräteoberflächen regelmäßig auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch untersucht (stimmen beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht)? ***Hinweis:*** *Anzeichen für eine Manipulation oder den Austausch von Geräten sind zum Beispiel unerwartete Anbauten oder Kabel, fehlende oder geänderte Sicherheitssiegel, beschädigte oder andersfarbige Gehäuse bzw. Änderungen bei der Seriennummer oder anderen externen Kennzeichen.*	▪ Mitarbeiter befragen. ▪ Untersuchungsprozesse beobachten und mit festgelegten Prozessen vergleichen.	☐	☐	☐	☐
	(b) Kennen die Mitarbeiter die Verfahren zur Untersuchung von Geräten?	▪ Mitarbeiter befragen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
9.9.3	Wurde das Bewusstsein der Mitarbeiter für Manipulations- oder Austauschversuche insbesondere durch die nachfolgenden Punkte gefördert?					
	(a) Umfasst das Schulungsmaterial für die Mitarbeiter an POS-Standorten die folgenden Punkte? - Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten). - Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe. - Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen). - Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter).	▪ Schulungsmaterialien überprüfen.	☐	☐	☐	☐
	(b) Wurden die Mitarbeiter an POS-Standorten geschult und haben sie die Verfahren zur Erkennung und Meldung von Versuchen der Manipulation oder des Austauschs von Geräten verinnerlicht?	▪ Mitarbeiter an POS-Standorten befragen.	☐	☐	☐	☐
Anweisung: *Werden die Punkte für die Anforderungen unter 9.9 mit „Ja" beantwortet, bedeutet dies, dass der Händler über Richtlinien und Verfahren für die Anforderungen 9.9.1 bis 9.9.3 verfügt und dass er eine Liste aller aktuellen Geräte führt, regelmäßige Geräteprüfungen durchführt und Mitarbeiter hinsichtlich der Erkennung von Manipulationen oder Geräteaustausch schult.*						
9.10	Sind Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des physischen Zugriffs auf Karteninhaberdaten …? ▪ dokumentiert ▪ derzeit in Verwendung ▪ allen Beteiligten bekannt	▪ Sicherheitsrichtlinien und betriebliche Verfahren überprüfen. ▪ Mitarbeiter befragen.	☐	☐	☐	☐

PCI-DSS-Frage	Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
		Ja	Ja, mit CCW	Nein	Nicht zutr.
Anweisung: *Wird die Anforderung 9.10 mit „Ja“ beantwortet, bedeutet dies, dass der Händler entsprechend seiner Umgebung über Richtlinien und Verfahren für die Anforderungen 9.5, 9.8 und 9.9 verfügt. Dies hilft sicherzustellen, dass das Personal die Sicherheitsrichtlinien und dokumentierten betrieblichen Verfahren kennt und befolgt.*					

Befolgung einer Informationssicherheits-Richtlinie

Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.

Hinweis: *Die Anforderung 12 legt fest, dass Händler über Informationssicherheitsrichtlinien für ihr Personal verfügen müssen. Diese Richtlinien können sich in ihrer Ausarbeitung jedoch vollständig nach der Komplexität und dem Ausmaß der Geschäftsabläufe des Händlers richten und flexibel an diese angepasst werden. Das Richtliniendokument muss dem gesamten Personal zur Verfügung gestellt werden, sodass alle Mitarbeiter sich genauestens ihrer Verantwortung hinsichtlich des Schutzes von Zahlungsterminals und Papierdokumenten mit Karteninhaberdaten usw. bewusst sind. Wenn ein Händler keine Mitarbeiter beschäftigt, wird erwartet, dass er seine Verantwortung im Bezug auf Sicherheit in seinen Geschäften versteht und anerkennt.*

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
12.1	Wurde eine Sicherheitsrichtlinie festgelegt, veröffentlicht, gepflegt und an das betroffene Personal weitergeleitet?	▪ Informationssicherheitsrichtlinie überprüfen.	☐	☐	☐	☐
12.1.1	Wird die Sicherheitsrichtlinie mindestens einmal pro Jahr überarbeitet und bei Umgebungsänderungen aktualisiert?	▪ Informationssicherheitsrichtlinie überprüfen. ▪ Verantwortliche Mitarbeiter befragen.	☐	☐	☐	☐
Anweisung: *Werden die Anforderungen unter 12.1 mit „Ja“ beantwortet, bedeutet dies, dass der Händler über eine Sicherheitsrichtlinie verfügt, die dem Ausmaß und die Komplexität seiner Geschäftsabläufe entspricht. Außerdem wird die Richtlinie jährlich überprüft und, falls notwendig, entsprechend angepasst. Bei einer solchen Richtlinie könnte es sich zum Beispiel um ein einfaches Dokument handeln, in dem festgehalten ist, wie das Geschäft und die Zahlungsgeräte in Übereinstimmung mit* der P2PE-Betriebsanleitung *geschützt werden und wer in einem Notfall kontaktiert werden sollte.*						
12.4	Beinhalten die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeiten aller Mitarbeiter?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen. ▪ Per Stichprobe zuständige Mitarbeiter befragen.	☐	☐	☐	☐
Anweisung: *Wird der Punkt für die Anforderung 12.4 mit „Ja“ beantwortet, bedeutet dies, dass die Sicherheitsrichtlinie des Händlers grundlegende Sicherheitsverantwortlichkeiten für das gesamte Personal festlegt und diese mit dem Ausmaß und der Komplexität der Geschäftsabläufe des Händlers übereinstimmen. Sicherheitsverantwortlichkeiten können beispielsweise anhand grundlegender Verantwortlichkeiten auf Mitarbeiterebene definiert werden, z. B. die Verantwortlichkeiten eines Managers/Besitzers und die eines Angestellten.*						
12.5	Wurden die folgenden Verantwortungsbereiche im Informationssicherheitsmanagement einer Einzelperson oder einem Team zugewiesen?					

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
12.5.3	Wurden Sicherheitsvorfallreaktions- und Eskalationsverfahren festgelegt, dokumentiert und verteilt, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten?	▪ Informationssicherheitsrichtlinie und -verfahren überprüfen.	☐	☐	☐	☐
Anweisung: *Wird die Anforderung 12.5.3 mit „Ja“ beantwortet, bedeutet dies, dass der Händler einen Verantwortlichen für den unter 12.9 erforderlichen Reaktions- und Eskalationsplan für Sicherheitsvorfälle bestimmt hat.*						
12.6	(a) Wurde ein offizielles Sicherheitsbewusstseinsprogramm implementiert, um allen Mitarbeitern die Bedeutung der Sicherheitheitsrichtlinien und Verfahren der Karteninhaberdaten zu vermitteln?	▪ Sicherheitsbewusstseinsprogramm durchgehen.	☐	☐	☐	☐
Anweisung: *Wird der Punkt für die Anforderung 12.6 mit „Ja“ beantwortet, bedeutet dies, dass der Händler über ein Sicherheitsbewusstseinsprogramm verfügt, das dem Ausmaß und der Komplexität der Geschäftsabläufe des Händlers entspricht. Dabei kann es sich zum Beispiel um einen Flyer handeln, der im Backoffice ausgehängt wird, oder eine E-Mail, die regelmäßig an Mitarbeiter versendet wird. Beispiele eines Sicherheitsbewusstseinsprogramms können beispielsweise Sicherheitshinweise umfassen, die alle Mitarbeiter befolgen sollten (zum Beispiel wie Türen und Aufbewahrungsbehälter verschlossen werden sollen, wie festgestellt werden kann, ob ein Zahlungsterminal manipuliert wurde, und wie befugtes Personal erkannt werden kann, das unter Umständen Wartungsarbeiten an Zahlungsterminals durchführt).*						
12.8	Werden Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert und gepflegt?					
12.8.1	Wird eine Liste von Dienstanbietern mit Angabe einer Beschreibung der geleisteten Dienstleistung(en) gepflegt?	▪ Richtlinien und Verfahren durchgehen. ▪ Prozesse überprüfen. ▪ Liste der Dienstanbieter überprüfen.	☐	☐	☐	☐

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
12.8.2	Wird eine schriftliche Vereinbarung aufbewahrt, mit der bestätigt wird, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden bzw. die er für den Kunden speichert, verarbeitet oder überträgt, oder dass die Sicherheit der CDE betroffen sein könnte. ***Hinweis:*** *Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.*	▪ Schriftliche Vereinbarungen überprüfen. ▪ Richtlinien und Verfahren durchgehen.	☐	☐	☐	☐
12.8.3	Gibt es ein eindeutiges Verfahren für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht?	▪ Prozesse überprüfen. ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen.	☐	☐	☐	☐
12.8.4	Gibt es ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard?	▪ Prozesse überprüfen. ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen.	☐	☐	☐	☐
12.8.5	Werden Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden, aufbewahrt?	▪ Prozesse überprüfen. ▪ Richtlinien und Verfahren sowie die zugehörige Dokumentation durchgehen.	☐	☐	☐	☐

Anweisung: *Werden die Punkte für die Anforderungen unter 12.8 mit „Ja“ beantwortet, bedeutet dies, dass der Händler über eine Liste mit Dienstanbietern verfügt, an die er Karteninhaberdaten weitergibt, sowie Vereinbarungen mit diesen bestehen. Solche Vereinbarungen kämen beispielsweise zum Einsatz, wenn ein Händler mit einem Unternehmen zusammenarbeitet, das Papierdokumente für ihn aufbewahrt, die Kontodaten beinhalten.*

PCI-DSS-Frage		Erwartete Tests	Antwort *(je Frage eine Antwort markieren)*			
			Ja	**Ja, mit CCW**	**Nein**	**Nicht zutr.**
12.10.1	(a) Wurde ein Vorfallreaktionsplan erstellt, der im Falle einer Systemsicherheitsverletzung im System implementiert wird?	▪ Vorfallreaktionsplan überprüfen. ▪ Verfahren im Zusammenhang mit dem Vorfallreaktionsplan überprüfen.	☐	☐	☐	☐

Anweisung: *Werden die Anforderungen unter 12.10 mit „Ja“ beantwortet, bedeutet dies, dass der Händler einen Reaktions- und Eskalationsplan für Sicherheitsvorfälle dokumentiert hat, der bei Notfällen zum Einsatz kommt und mit dem Ausmaß und der Komplexität der Betriebsabläufe des Händlers übereinstimmt. Ein solcher Plan kann beispielsweise ein einfaches Dokument sein, das im Backoffice ausgehängt wird und Informationen darüber enthält, wer in verschiedensten Situationen kontaktiert werden sollte, sowie jährlich auf seine Richtigkeit überprüft wird. Dieses Dokument kann jedoch bis auf einen vollständigen Reaktionsplan für Sicherheitsvorfälle erweitert werden, der Backup-Einrichtungen (Hotsites) sowie sorgfältige Tests umfasst. Dieser Plan sollte sämtlichem Personal als Ressource im Falle eines Notfalls zur Verfügung stehen.*

Anhang A: Zusätzliche PCI DSS Anforderungen

Anhang A1: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsamem Hosting

Dieser Anhang wird nicht für Händlerbeurteilungen verwendet.

Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/frühe Versionen von TLS in POS-POI-Terminalverbindungen mit vorliegender Karte verwenden

Dieser Anhang wird nicht für SBF P2PE Händlerbeurteilungen verwendet.

Anhang A3: Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation, DESV)

Dieser Anhang gilt ausschließlich für Einheiten, welche von einem Kartenunternehmen oder Acquirer zu einer zusätzlichen Überprüfung der vorhandenen PCI-DSS-Anforderungen aufgefordert wurden. Einheiten, von denen eine Überprüfung verlangt wird, müssen die ergänzende DESV-Berichtsvorlage und die ergänzende Konformitätsbescheinigung für Berichterstattung verwenden, sowie sich an das entsprechende Kartenunternehmen bzw. Acquirer bezüglich der Einreichverfahren wenden.

Anhang B: Arbeitsblatt – Kompensationskontrollen

Bestimmen Sie anhand dieses Arbeitsblatts die Kompensationskontrollen für alle Anforderungen, bei denen „Ja, mit CCW“ markiert wurde.

Hinweis: *Nur Unternehmen, die eine Risikoanalyse vorgenommen und legitime technologische oder dokumentierte geschäftliche Hindernisse nachweisen können, können den Einsatz von Kompensationskontrollen zu Konformitätszwecken in Erwägung ziehen.*

Informationen zu Kompensationskontrollen sowie Hinweise zum Ausfüllen dieses Arbeitsblatts finden Sie in den PCI-DSS-Anhängen B, C und D.

Anforderungsnummer und -definition:

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	
2. Ziel	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
4. Definition der Kompensations-kontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. Validierung der Kompensations-kontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

Anhang C: Erläuterung der Nichtanwendbarkeit

Falls die Spalte „N/A“ (Nicht zutreffend) im Fragebogen markiert wurde, erläutern Sie bitte im Arbeitsblatt, warum die zugehörige Anforderung nicht für Ihr Unternehmen gilt.

Anforderung	Grund, warum die Anforderung nicht anwendbar ist.
Beispiel:	
12.8	Karteninhaberdaten werden niemals an Dienstanbieter weitergegeben.

3. Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

Diese Konformitätsbescheinigung basiert auf den Ergebnissen, welche im SBF P2PE (Abschnitt 2) mit Datum vom *(Abschlussdatum des SBF) notiert wurden.*

Aufgrund der obengenannten Ergebnisse des SBF P2PE stellen die in Teil 3b bis 3d angegebenen Unterzeichner den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (Datum) ermittelte Einheit fest: (***Zutreffendes ankreuzen):***

☐	**Konform:** Alle Abschnitte des PCI DSS SBF P2PE sind vollständig und alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung **KONFORM**. *(Name des Händlerunternehmens)* hat somit eine vollständige Konformität mit dem PCI DSS gezeigt.
☐	**Nicht konform:** Nicht alle Abschnitte des PCI DSS SBF P2PE sind vollständig beziehungsweise es wurden nicht alle Fragen mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung **NICHT KONFORM**. *(Name des Händlerunternehmens)* hat somit keine vollständige Konformität mit dem PCI DSS gezeigt. **Zieldatum** für Konformität: Von einer Einheit, die dieses Formular mit einem Status von „Nicht konform“ einreicht, kann verlangt werden, den Aktionsplan in Teil 4 dieses Dokuments auszufüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*
☐	**Konform, jedoch mit gesetzlicher Ausnahme:** Eine oder mehrere Anforderungen sind aufgrund einer gesetzlichen Einschränkung, die das Erfüllen der jeweiligen Anforderung(en) unmöglich macht, mit „Nein“ gekennzeichnet. Bei dieser Option ist eine zusätzliche Prüfung durch den Acquirer oder das Kartenunternehmen erforderlich. *Falls diese Option markiert ist, arbeiten Sie folgende Punkte ab:*

Betroffene Anforderung	Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern

Teil 3a. Feststellung des Status

Unterzeichner bestätigt:

(Zutreffendes ankreuzen)

☐	Der PCI-DSS Selbstbeurteilungsfragebogen P2PE, 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.
☐	Ich habe den PCI DSS gelesen und erkenne an, dass ich jederzeit die für meine Umgebung geltende PCI-DSS-Konformität aufrechterhalten muss.
☐	Für den Fall, dass sich meine Umgebung ändert, erkenne ich an, dass ich meine Umgebung erneut beurteilen und etwaige zusätzliche PCI-DSS-Anforderungen erfüllen muss.

Teil 3. PCI-DSS-Validierung *(Fortsetzung)*

Teil 3a. Feststellung des Status *(Fortsetzung)*

☐	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung vollständige Spurdaten („Full-Track-Daten“)[1], CAV2-, CVC2-, CID-, CVV2[2]- oder PIN-Daten[3] gespeichert wurden.

Teil 3b. Bescheinigung des Händlers

Unterschrift des Beauftragten des Händlers ↗	*Datum:*
Name des Beauftragten des Händlers:	*Titel:*

Teil 3c. Bestätigung durch den QSA (Qualified Security Assessor) (sofern zutreffend)

Falls ein QSA an dieser Beurteilung beteiligt war, beschreiben Sie bitte dessen Aufgabe:	

Unterschrift des ordnungsgemäß ermächtigten Vertreters des QSA-Unternehmens ↗	*Datum:*
Name des ordnungsgemäß ermächtigten Vertreters:	*Unternehmen des QSA:*

Teil 3d. Beteiligung eines ISA (Internal Security Assessor) (sofern zutreffend)

Falls ein ISA an dieser Beurteilung beteiligt war oder dabei geholfen hat, identifizieren Sie bitte den ISA-Mitarbeiter und beschreiben Sie dessen Aufgabe:	

[1] Im Magnetstreifen verschlüsselte Daten oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Spurdaten speichern. Die einzigen Spurdatenelemente, die aufbewahrt werden dürfen, sind die primäre Kontonummer (PAN), das Ablaufdatum und der Name des Karteninhabers.

[2] Der drei- oder vierstellige Wert, der 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“

Wählen Sie zu jeder Anforderung die zutreffende Antwort auf die Frage nach der Konformität mit PCI-DSS-Anforderungen aus. Wenn Sie einen der Punkte mit „Nein“ beantworten, müssen Sie möglicherweise das Datum angeben, an dem das Unternehmen die Anforderung voraussichtlich erfüllen wird. Geben Sie außerdem eine kurze Beschreibung der Maßnahmen an, die zur Erfüllung der Anforderung ergriffen werden.

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**	**Konform mit PCI-DSS-Anforderungen** (zutreffende Antwort auswählen)		**Datum bis zur Mängelbeseitigung und Abhilfemaßnahmen** (falls „Nein“ ausgewählt wurde)
		JA	**NEIN**	
3	Schutz gespeicherter Karteninhaberdaten	☐	☐	
9	Beschränkung des physischen Zugriffs auf Karteninhaberdaten	☐	☐	
12	Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal	☐	☐	

** Die hier angegebenen PCI-DSS-Anforderungen beziehen sich auf die Fragen in Abschnitt 2 des SBF.*