Payment Card Industry (PCI)
Data Security Standard

Fragebogen zur Selbsteinschätzung

Hinweise und Richtlinien

Version 3.2.1

Juni 2018

Änderungen am Dokument

Datum	Version	Beschreibung
1. Oktober 2008	1.2	Anpassung der Inhalte an die neue PCI DSS v1.2 und zur Umsetzung kleiner Änderungen seit der ursprünglichen Version 1.1.
28. Oktober 2010	2.0	Anpassung der Inhalte an die neue PCI DSS v2.0 und Klarstellung der SAQ-Umgebungstypen und Qualifikationskriterien. Hinzufügen des SAQ C-VT für Händler mit webbasierten virtuellen Terminals
Juni 2012	2.1	Hinzufügen von SAQ P2PE-HW für Händler, die Karteninhaberdaten nur über Hardware-Zahlungsterminals verarbeiten, die in einer geprüften und in der PCI SSC geführten PCI-P2PE-Lösung (Punkt-zu-Punkt-Verschlüsselung) enthalten sind. Dieses Dokument ist zur Verwendung mit der PCI DSS Version 2.0 bestimmt.
April 2015	3.1	Anpassung der Inhalte an die PCI DSS v3.1, einschließlich Hinzufügen der SAQs A-EP und B-IP und Klarstellung der Qualifikationskriterien für bestehende SAQs.
Mai 2016	3.2	Aktualisierung zur Anpassung an die PCI DSS v3.2 und zur Klarstellung der Qualifikationskriterien für bestehende SAQs.
Juni 2018	3.2.1	Kleinere Aktualisierungen zur Anpassung an die PCI DSS v3.2.1.

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.

Inhaltsverzeichnis

Änderungen am Dokument ..... **i**

Über dieses Dokument **1**

PCI DSS Selbsteinschätzung: So funktioniert die Methode **2**

SAQ-Übersicht **3**

Darum ist die PCI DSS wichtig **4**

Der Unterschied zwischen Compliance und Sicherheit 6

Allgemeine Tipps und Strategien für die PCI-DSS-Compliance 6

So finden Sie den SAQ und die Bescheinigung, die am besten zu Ihrem Unternehmen passen **9**

SAQ A – Händler ohne Kartenpräsenz, alle Funktionen für Karteninhaberdaten vollständig ausgelagert 11

SAQ-A-EP – teilweise ausgelagert E-Commerce-Händler, die eine Drittanbieter-Website für die Zahlungsabwicklung nutzen 12

SAQ B – Händler mit ausschließlich Druckgeräten oder unabhängigen Dial-Out-Terminals. Keine elektronische Speicherung von Karteninhaberdaten 13

SAQ-B-IP – Händler mit unabhängigen PTS-POI-Terminals (Point of Interaction) mit IP-Anbindung, keine elektronische Speicherung von Karteninhaberdaten 14

SAQ C-VT – Händler mit webbasierten virtuellen Terminals, keine elektronische Speicherung von Karteninhaberdaten 15

SAQ C – Händler mit Zahlungsanwendungssystemen mit Internetverbindung, keine elektronische Speicherung von Karteninhaberdaten 17

SAQ P2PE – Händler, die nur Hardware-Zahlungsterminals in einer vom PCI SSC geführten P2PE-Lösung verwenden, keine elektronische Speicherung von Karteninhaberdaten 18

SAQ D für Händler – Alle sonstigen Händler mit SAQ-Qualifikation 19

SAQ D für Dienstleister – Dienstleister mit SAQ-Qualifikation 19

Welcher SAQ passt am besten zu meiner Umgebung? **20**

Über dieses Dokument

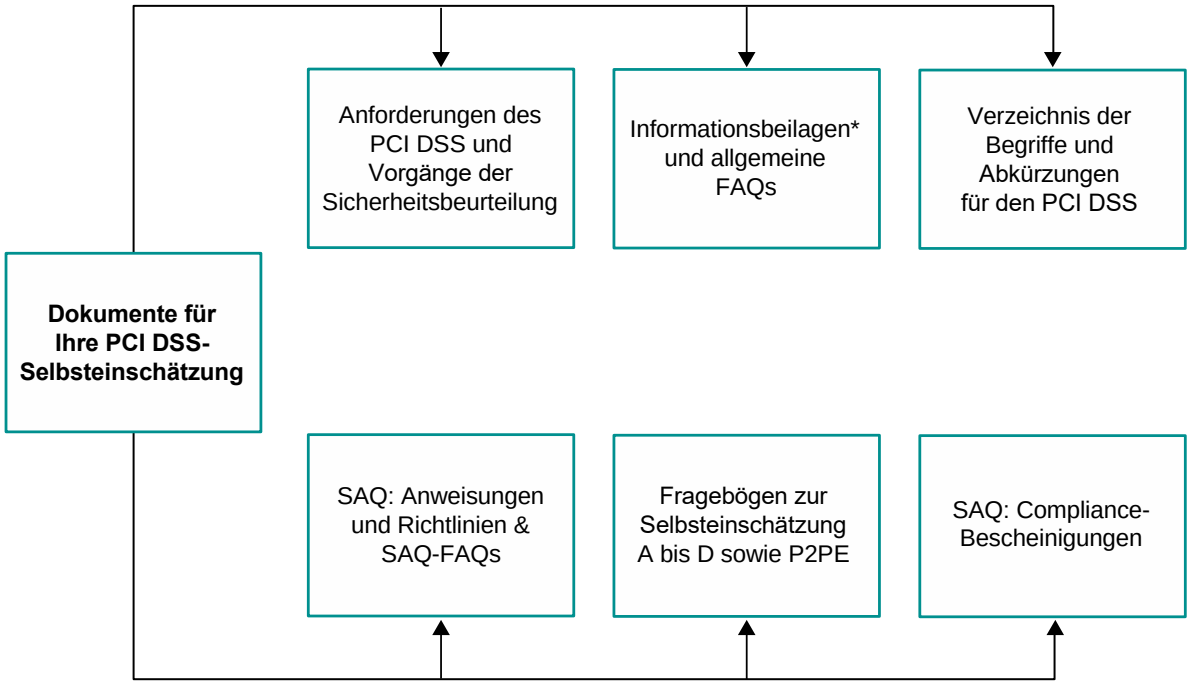
Dieses Dokument wurde erstellt, um Händlern und Dienstleistern dabei zu helfen, die Fragebögen zur Selbsteinschätzung (SAQs) für den Payment Card Industry Data Security Standard (PCI DSS) zu verstehen. Für ein besseres Verständnis, warum der PCI DSS für Ihr Unternehmen wichtig ist, mit welchen Strategien Ihr Unternehmen die PCI-DSS-Compliance-Bescheinigung erleichtern kann und ob Ihr Unternehmen die nötige Qualifikation zum Ausfüllen eines der kürzeren SAQs hat, empfehlen wir Ihnen, dies Hinweise und Richtlinien vollständig durchzulesen.

PCI DSS Selbsteinschätzung: So funktioniert die Methode

Der PCI DSS und die Anhänge sind gängige Mittel der Branche, um den sicheren Umgang mit Karteninhaberdaten sicherzustellen. Der Standard selbst bietet einen umsetzbaren Rahmen zur Ausarbeitung eines robusten Sicherheitsprozesses – einschließlich Prävention, Erkennung und Reaktion auf Sicherheitsvorfälle. Um die Gefahr von Kompromittierungen zu reduzieren und deren potenzielle Auswirkungen aufzufangen, müssen alle juristischen Personen, die Karteninhaberdaten speichern, verarbeiten oder übertragen, den Standard erfüllen.

In der folgenden Tabelle finden Sie verfügbaren Werkzeuge, mit denen Unternehmen die Compliance und Selbsteinschätzung in Verbindung mit dem PCI DSS erleichtert wird.

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



** Beachten Sie, dass die Informationsbeilagen nur er gänzende Informationen und Hinweise liefern und keine Anforderungen im PCI DSS ersetzen.*

* ***Hinweis:*** *Informationsbeilagen liefern nur ergänzende Informationen und Hinweise und ersetzen keine Anforderungen im PCI DSS.*

SAQ-Übersicht

Die *PCI DSS Fragebögen zur Selbsteinschätzung* (SAQs) sind Validierungswerkzeuge, die Händler und Dienstleister bei der Selbsteinschätzung ihrer PCI-DSS-Compliance unterstützen sollen. Es gibt mehrere Versionen der PCI-DSS-SAQs für verschiedene Szenarien. Dieses Dokument wurde erstellt, um Ihrem Unternehmen die Entscheidung zu erleichtern, welche(r) SAQ(s) am ehesten auf Ihre Umgebung zutrifft/zutreffen.

Der PCI-DSS-SAQ ist ein Validierungswerkzeug für Händler und Dienstleister, die durch ihre Acquirers oder Zahlungsmarke(n) nicht verpflichtet sind, einen PCI-DSS-Compliance-Bericht (ROC) vorzulegen. Einzelheiten zu den PCI-DSS-Validierungsanforderungen erfahren Sie von Ihrem Acquirer oder Ihrer Zahlungsmarke.

Jeder PCI-DSS-SAQ enthält folgende Bestandteile:

1. Fragen zu den PCI-DSS-Anforderungen, angepasst für die jeweiligen Umgebungen: Siehe „So finden Sie den SAQ und die Bescheinigung, die am besten zu Ihrem Unternehmen passen“ in diesem Dokument. Dieser Abschnitt umfasst auch eine Spalte für „Vorausgesetzte Tests“, die auf den Testverfahren im PCI DSS basieren.
2. Compliance-Bescheinigung: Die Bescheinigung umfasst Ihre Qualifikation zum Ausfüllen des zutreffenden SAQ und die entsprechenden Ergebnisse einer PCI-DSS-Selbsteinschätzung.

Darum ist die PCI DSS wichtig

Die Gründungsmitglieder des PCI Security Standards Council (American Express, Discover, JCB, Mastercard und Visa) überwachen stetig Vorfälle, bei denen Kontodaten kompromittiert werden. Diese Kompromittierungen werden für das gesamte Unternehmensspektrum von Kleinstunternehmen bis hin zu großen Händlern und Dienstleistern überwacht.

Ein Sicherheitsvorfall und die folgende Kompromittierung von Zahlungskartendaten hat weitreichende Konsequenzen für die betroffenen Unternehmen, darunter:

1. Behördliche Mitteilungsanforderungen,
2. Reputationsverlust,
3. Kundenverlust,
4. Potenzielle finanzielle Verbindlichkeiten (beispielsweise Behördengebühren, sonstige Bußgelder) und
5. Rechtsstreitigkeiten.

Forensische Analysen der Kompromittierungen haben gezeigt, dass gängige Sicherheitsschwachstellen, die in den PCI-DSS-Kontrollen berücksichtigt werden, oft ausgenutzt werden, da die PCI-DSS-Kontrollen entweder nicht oder mangelhaft umgesetzt wurden, als die Kompromittierung passierte. Der PCI DSS wurde genau aus diesem Grund erstellt und enthält genau deswegen so detaillierte Anforderungen – um die Wahrscheinlichkeit einer Kompromittierung und die Auswirkungen einer potenziellen Kompromittierung zu minimieren.

Beispiele für gängige PCI-DSS-Kontrollmängel umfassen unter anderem:

- Speicherung sensibler Autorisierungsdaten (SAD), beispielsweise Spurdaten, nach der Autorisierung (Anforderung 3.2). Viele kompromittierte juristische Personen waren sich nicht bewusst, dass ihre Systeme diese Daten speichern.
- Unzureichende Zugriffskontrollen aufgrund mangelhaft installierter POS-Systeme (Point of Sale), die es böswilligen Benutzern erlauben, über Pfade einzudringen, die für die POS-Anbieter gedacht sind (Anforderungen 7.1, 7.2, 8.2 und 8.3).
- Standard-Systemeinstellungen und -Passwörter, die bei der Systeminstallation nicht geändert wurden (Anforderung 2.1).
- Unnötige und unsichere Dienste, die bei der Systeminstallation nicht entfernt oder gesichert wurden (Anforderungen 2.2.2 und 2.2.3).
- Schlecht programmierte Webanwendungen, die zu SQL Injections und anderen Schwachstellen führen, wodurch direkt von der Website auf die Daten zugegriffen werden kann, die die Karteninhaberdaten enthält (Anforderung 6.5).
- Fehlende und veraltete Sicherheits-Patches (Anforderung 6.2).
- Mangelnde Protokollierung (Anforderung 10).
- Mangelndes Monitoring (mittels Protokollprüfungen, Eindringungserkennung/-bekämpfung, vierteljährliche Schwachstellen-Scans und Mechanismen zur Erkennung von Änderungen) (Anforderungen 10.6, 11.2, 11.4 und 11.5).

- Schlechte Scoping-Entscheidungen – beispielsweise Ausschluss eines Teils vom Netzwerk aus dem PCI-DSS-Rahmen aufgrund unzureichender Netzwerksegmentierung, deren Effektivität nicht bestätigt wurde (Anforderung 11.3.4). Das führt dazu, dass die Umgebung mit den Karteninhaberdaten unwissentlich Schwachstellen in anderen Teilen des Netzwerks ausgesetzt wird, die nicht nach PCI DSS gesichert wurden (beispielsweise von ungesicherten kabellosen Zugangspunkten und über Schwachstellen durch E-Mails und Webbrowsing von Angestellten) (Anforderungen 1.2, 1.3 und 1.4).

Der Unterschied zwischen Compliance und Sicherheit

Es ist wichtig, den Unterschied zwischen Compliance und Sicherheit zu verstehen. Die Konformität mit dem PCI DSS zu einem bestimmten Zeitpunkt verhindert nicht, dass sich Dinge in Ihrer Umgebung ändern, was sich – wenn keine entsprechenden Kontrollen eingeführt werden – auf Ihre Sicherheit auswirken kann. Sie sollten daher sicherstellen, dass weiterhin PCI-DSS-Kontrollen im Rahmen von Aktivitäten des Geschäftsalltags (Business as Usual, BAU) ordnungsgemäß und nach den Spezifikationen Ihrer Gesamtsicherheitsstrategie umgesetzt werden. So können Sie die Wirksamkeit der Sicherheitskontrollen Ihres Unternehmens fortlaufend überwachen und auch zwischen den PCI-DSS-Beurteilungen für eine PCI-DSS-konforme Umgebung sorgen. Beispiele für die Einbindung des PCI DSS in BAU-Aktivitäten finden Sie im Abschnitt „Best Practices für die Umsetzung des PCI DSS in gängige Geschäftsprozesse“ im PCI DSS.

Zudem sind die PCI-DSS-Sicherheitsanforderungen auf den Schutz der Zahlungskartendaten ausgelegt und Ihr Unternehmen hat möglicherweise weitere sensible Daten und Assets, die geschützt werden müssen, jedoch außerhalb des Rahmens des PCI DSS liegen. Daher kann die PCI-DSS-Compliance zwar zur Gesamtsicherheit beitragen (wenn Sie diese wahren); sie sollte jedoch nicht als Ersatz für ein solides, unternehmensweites Sicherheitsprogramm betrachtet werden.

Allgemeine Tipps und Strategien für die PCI-DSS-Compliance

Im Folgenden erhalten Sie allgemeine Tipps und Strategien für den Anfang Ihrer PCI-DSS-Compliance-Maßnahmen. Diese Tipps sollen Ihnen dabei helfen, die Speicherung von Karteninhaberdaten abzuschaffen, die Sie nicht benötigen, die benötigten Daten auf festgelegte und kontrollierte zentrale Bereiche einzuschränken und Ihnen die Eingrenzung des Rahmens Ihrer PCI-DSS-Compliance-Validierungsmaßnahmen ermöglichen. Wenn Sie beispielsweise Karteninhaberdaten eliminieren, die Sie nicht benötigen, und/oder die benötigten Daten auf festgelegte und kontrollierte Bereiche einschränken, können Sie Systeme und Netzwerke, die keine Karteninhaberdaten speichern, verarbeiten oder übertragen – und die nicht mit solchen Systemen verbunden sind – aus dem Rahmen Ihrer Selbsteinschätzung streichen.

1. **Sensible Authentifizierungsdaten (umfasst die gesamten Spurinhalte des Magnetstreifens oder gleichwertiger Daten auf einem Chip, Kartenprüfcodes und -werte, PINs und PIN-Blöcke):**

   Diese Daten ***sollten Sie niemals*** nach der Autorisierung speichern:

2. **Stellen Sie Ihrem POS-Anbieter Fragen zur Sicherheit Ihres Systems. Unsere Empfehlungen:**

   a. Wurden für die Systeme und Datenbanken, die Teil des POS-Systems sind, Standardeinstellungen und -Passwörter geändert?

   b. Greifen Sie aus der Ferne auf mein POS-System zu? Falls ja, haben Sie entsprechende Kontrollen implementiert, um zu verhindern, dass andere auf mein POS-System zugreifen – beispielsweise durch sichere Fernzugriffsmethoden und die Vermeidung gängiger oder Standardpasswörter? Wie oft greifen Sie aus der Ferne auf mein POS-Gerät zu und warum? Wer ist für den Fernzugriff auf mein POS befugt?

   c. Wurden alle unnötigen und unsicheren Dienste aus den Systemen und Datenbanken entfernt, die Teil des POS-Systems sind?

   d. Wird meine POS-Software nach dem PA-DSS (Payment Application Data Security Standard) validiert? (Siehe PCI-SSC-Liste der validierten Zahlungsanwendungen.)

e. Speichert meine POS-Software sensible Authentifizierungsdaten wie Spurdaten oder PIN-Blöcke? Falls ja, diese Speicherung ist untersagt: Wie schnell können Sie mir helfen, diese Funktion zu entfernen?

f. Speichert meine POS-Software primäre Kontonummern (PANs)? Falls ja, muss diese Speicherung abgesichert werden: Wie schützt das POS-System diese Daten?

g. Dokumentieren Sie die Liste der Dateien, die von der Anwendung geschrieben werden, mit einer Übersicht der Inhalte jeder Datei, um sicherzustellen, dass die oben genannten verbotenen Daten nicht gespeichert werden?

h. Erzwingt meine POS-Software komplexe und einzigartige Passwörter für den Zugriff aller Benutzer?

i. Können Sie bestätigen, dass Sie keine gängigen oder Standardpasswörter für den Zugriff auf mein System und andere von Ihnen unterstützte Händlersysteme verwenden?

j. Wurden alle Systeme und Datenbanken, die Teil des POS-Systems sind, mit den neuesten Sicherheits-Updates gepatcht?

k. Ist für die Systeme und Datenbanken, die Teil des POS-Systems sind, die Protokollierung aktiviert?

l. Falls vorige Versionen meiner POS-Software sensible Authentifizierungsdaten gespeichert haben, wurde diese Funktion durch aktuelle Updates der POS-Software entfernt? Wurde ein sicherer Löschvorgang zum Entfernen dieser Daten angewendet?

3. Karteninhaberdaten – was Sie nicht brauchen, sollten Sie auch nicht speichern!

a. Die Regeln von Zahlungsmarken erlauben die Speicherung von primären Kontonummern (PAN), Ablaufdatum, Karteninhabername und Servicecode.

b. Machen Sie eine Bestandsaufnahme aller Gründe und Orte, an und aus denen Sie diese Daten speichern. Wenn die Daten keinem rechtmäßigen Geschäftszweck dienen, sollten Sie sie vielleicht abschaffen.

c. Überlegen Sie sich, ob die Speicherung dieser Daten und die dadurch unterstützten Geschäftsprozesse folgende Risiken/Verpflichtungen wert sind:

   i. Die Gefahr einer Kompromittierung der Daten.

   ii. Die zusätzlichen PCI-DSS-Kontrollen, die zum Schutz der Daten eingeführt werden müssen.

   iii. Die laufende Wartungsarbeit, um die PCI-DSS-Compliance zu wahren.

4. Karteninhaberdaten – was Sie brauchen, sollten Sie konsolidieren und isolieren.

Sie können den Umfang einer PCI-DSS-Beurteilung eingrenzen, indem Sie die Datenspeicherung auf eine festgelegte Umgebung beschränken und die Daten mittels ordnungsgemäßer Netzwerksegmentierung isolieren. Wenn Ihre Mitarbeiter beispielsweise auf demselben Gerät oder im selben Netzwerksegment im Internet surfen und E-Mails empfangen, wo sich auch die Karteninhaberdaten befinden, sollten Sie die Karteninhaberdaten auf einen eigenen Rechner oder ein eigenes Netzwerksegment verlegen (isolieren) – beispielsweise über Router und Firewalls. Wenn Sie die Karteninhaberdaten effektiv isolieren können, können Sie sich mit Ihre PCI-DSS-Maßnahmen auf den isolierten Bereich konzentrieren und müssen nicht jeden Rechner unter die Lupe nehmen.

5. Ausgleichende Kontrollen

Ausgleichende Kontrollen können für die meisten PCI-DSS-Anforderungen in Erwägung gezogen werden, wenn ein Unternehmen die technische Spezifikation einer Anforderung nicht erfüllen kann, dass damit verbundene Risiko jedoch ausreichend durch alternative Kontrollen reduziert hat. Wenn Ihr Unternehmen nicht über die exakte, im PCI DSS angegebene Kontrolle verfügt, jedoch andere Kontrollen eingeführt hat, welche die Definition ausgleichender Kontrollen des PCI DSS erfüllen (siehe „Ausgleichende Kontrollen“ im PCI-DSS-Anhang B und im *PCI-DSS- und PA-DSS-Verzeichnis der Begriffe und Abkürzungen*), sollte Ihr Unternehmen Folgendes tun:

a. Befolgen Sie die Vorgehensweise für ausgleichende Kontrollen wie in PCI-DSS-Anhang B beschrieben.

b. Für alle Anforderungen, die mit Hilfe einer ausgleichenden Kontrolle erfüllt wurden, kreuzen Sie bei der jeweiligen SAQ-Frage die Spalte „YES with CCW“ an.

c. Dokumentieren Sie jede ausgleichende Kontrolle mit einem „Compensating Controls Worksheet“ (Arbeitsblatt ausgleichende Kontrollen) in Anhang B des SAQ.

   Ein Arbeitsblatt „Ausgleichende Kontrollen“ ist für jede Anforderung vorzulegen, die mit Hilfe einer ausgleichenden Kontrolle erfüllt wird.

d. Reichen Sie alle ausgefüllten „Ausgleichende Kontrollen“-Arbeitsblätter zusammen mit Ihrem ausgefüllten SAQ und/oder Ihrer Compliance-Bescheinigung nach den Anweisungen Ihres Acquirers oder Ihrer Zahlungsmarke ein.

6. Professionelle Unterstützung und Schulung

a. Wenn Sie eine Sicherheitsfachkraft mit der Unterstützung bei Ihrer Selbsteinschätzung beauftragen möchten, empfehlen wir Ihnen, nach einem Qualified Security Assessor (QSA) Ausschau zu halten. QSAs sind vom PCI SSC für die Ausführung von PCI-DSS-Beurteilungen ausgebildet und werden auf der Website des PCI SSC geführt.

b. Die Website des PCI SSC ist eine Primärquelle für weitere Ressourcen, darunter:

   - Das *PCI-DSS-Verzeichnis der Begriffe und Abkürzungen*
   - Häufig gestellte Fragen (FAQs)
   - Webinare
   - Informationsbeilagen und Richtlinien
   - SAQ-Formulare und Compliance-Bescheinigungen

c. Das PCI SSC bietet zudem eine Reihe von Schulungsprogrammen, um das Bewusstsein der Angestellten von Unternehmen zu schärfen. Beispiele sind das PCI Awareness Program, das PCI Professional Program (PCIP) und das Internal Security Assessor Program (ISA).

   Weitere Informationen finden Sie unter www.pcisecuritystandards.org.

d. Schulungsprogramme und Ressourcen zum Thema Zahlungen finden Sie möglicherweise auch bei den Zahlungsmarken und/oder Ihrem Händler-Acquirer.

Hinweis: *Informationsbeilagen ergänzen den PCI DSS und nennen weitere Hinweise und Empfehlungen zur Erfüllung von PCI-DSS-Anforderungen – sie ändern oder ersetzen weder den PCI DSS noch darin enthaltene Anforderungen.*

So finden Sie den SAQ und die Bescheinigung, die am besten zu Ihrem Unternehmen passen

Alle Händler und Dienstleister müssen den PCI DSS in seinem Geltungsumfang für ihre Umgebung jederzeit einhalten. Es gibt verschiedene SAQ-Typen, die unten in der Tabelle kurz aufgeführt sind und auf den folgenden Seiten genauer beschrieben werden. Mit Hilfe der Tabelle können Sie feststellen, welcher SAQ auf Ihr Unternehmen zutrifft, und sich anschließend die detaillierten Beschreibungen ansehen, damit Sie alle Anforderungen für diesen SAQ erfüllen.

Hinweis für alle SAQs außer SAQ D: Diese SAQs umfassen Fragen, die für eine bestimmte Art von Händlerumgebung (Definition in den zugehörigen SAQ-Qualifikationskriterien) gelten. Wenn für Ihre Umgebung PCI-DSS-Anforderungen gelten, die nicht in einem bestimmten SAQ aufgeführt sind, bedeutet das möglicherweise, dass dieser SAQ nicht auf Ihre Umgebung zutrifft. Zudem müssen Sie alle geltenden PCI-DSS-Anforderungen erfüllen, um die PCI-DSS-Compliance zu erreichen.

SAQ	Beschreibung
A	Händler ohne Kartenpräsenz (E-Commerce oder Versand- bzw. Telefonbestellung), die alle Funktionen für Karteninhaberdaten vollständig an externe Dienstleister mit PCI-DSS-Compliance ausgelagert haben, ohne elektronische Speicherung, Verarbeitung oder Übertragung jeglicher Karteninhaberdaten auf den Systemen oder am Standort des Händlers. *Gilt nicht für Kanäle mit persönlichem Kundenkontakt.*
A-EP	E-Commerce-Händler, die die gesamte Zahlungsabwicklung an nach PCI DSS validierte externe Dienstleister ausgelagert haben und (eine) Website(s) haben, die nicht direkt Karteninhaberdaten erhält/erhalten, die jedoch die Sicherheit der Zahlungstransaktion beeinflussen kann/können. Keine elektronische Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten auf den Systemen oder am Standort des Händlers. *Gilt nur für E-Commerce-Kanäle.*
B	Händler, die nur Folgendes nutzen: ▪ Druckmaschinen ohne elektronische Speicherung von Karteninhaberdaten, und/oder ▪ unabhängige Dial-Out-Terminals ohne elektronische Speicherung von Karteninhaberdaten. *Gilt nicht für E-Commerce-Kanäle.*
B-IP	Händler, die nur unabhängige, PTS-geprüfte Zahlungsterminals mit einer IP-Anbindung an den Zahlungsabwickler nutzen, ohne elektronische Speicherung von Karteninhaberdaten. *Gilt nicht für E-Commerce-Kanäle.*
C-VT	Händler, die manuell jeweils einzelne Transaktionen in eine internetbasierte Lösung mit virtuellem Zahlungsterminal eingeben, welche von einem nach PCI DSS validierten externen Dienstleister bereitgestellt wird. Keine elektronische Speicherung von Karteninhaberdaten. *Gilt nicht für E-Commerce-Kanäle.*
C	Händler mit Zahlungsanwendungssystemen mit Internetverbindung, keine elektronische Speicherung von Karteninhaberdaten.

SAQ	Beschreibung
	Gilt nicht für E-Commerce-Kanäle.
P2PE	Händler, die nur Hardware-Zahlungsterminals nutzen, die in einer validierten, vom PCI SSC geführten P2PE-Lösung (Punkt-zu-Punkt-Verschlüsselung) enthalten sind und verwaltet werden, ohne elektronische Speicherung von Karteninhaberdaten. *Gilt nicht für E-Commerce-Kanäle.*
D	***SAQ D für Händler:*** Alle Händler, die nicht in Beschreibungen für die obigen SAQ-Typen enthalten sind.
	SAQ D für Dienstleister: Alle Dienstleister, die von einer Zahlungsmarke als qualifiziert zum Ausfüllen eines SAQ eingestuft werden.

SAQ A – Händler ohne Kartenpräsenz, alle Funktionen für Karteninhaberdaten vollständig ausgelagert

SAQ A wurde entwickelt, um Anforderungen für Händler zu berücksichtigen, deren Funktionen für Karteninhaberdaten vollständig an validierte Dritte ausgelagert sind und wo die Händler nur Papierberichte oder -belege mit Karteninhaberdaten behalten.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

SAQ-A-Händler können E-Commerce- oder (telefonischer) Versandhändler sein (keine Kartenpräsenz) und speichern, verarbeiten oder übertragen keine Karteninhaberdaten im elektronischen Format auf ihren Systemen oder an ihren Standorten.

SAQ-A-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

- Ihr Unternehmen akzeptiert nur Transaktionen ohne Kartenpräsenz (E-Commerce oder (telefonischer) Versandhandel);
- Sämtliche Verarbeitungstätigkeiten der Karteninhaberdaten sind vollständig an nach PCI DSS validierte externe Dienstleister ausgelagert;
- Ihr Unternehmen speichert, verarbeitet oder überträgt keine Karteninhaberdaten auf seinen Systemen oder an seinen Standorten elektronisch, sondern vergibt diese Funktionen vollständig an Dritte;
- Ihr Unternehmen hat sich vergewissert, dass (alle) Dritte(n), die für die Speicherung, Verarbeitung und/oder Übertragung von Karteninhaberdaten PCI-DSS-konform sind; **und**
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein.

Zudem gilt für E-Commerce-Kanäle:

- Alle Elemente aller Zahlungsseiten, die an den Browser des Verbrauchers ausgeliefert werden, stammen ausschließlich und direkt von (einem) nach PCI DSS validierten externen Dienstleister(n).

Dieser SAQ gilt nicht für Kanäle mit persönlichem Kundenkontakt.

SAQ-A-EP – teilweise ausgelagert E-Commerce-Händler, die eine Drittanbieter-Website für die Zahlungsabwicklung nutzen

SAQ-A-EP wurde für die Anforderungen entwickelt, die für E-Commerce-Händler mit (einer) Website(s) gelten, die selbst keine Karteninhaberdaten empfängt, jedoch die Sicherheit der Zahlungstransaktion und/oder die Integrität der Seite beeinflusst, welche die Karteninhaberdaten des Verbrauchers empfängt.

SAQ-A-EP-Händler sind E-Commerce-Händler, die ihren E-Commerce-Zahlungskanal an nach PCI DSS validierte Dritte ausgelagert haben und keine Karteninhaberdaten auf den Systemen oder an ihrem Standort elektronisch speichern, verarbeiten oder übertragen.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

SAQ-A-EP-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

- Ihr Unternehmen akzeptiert ausschließlich E-Commerce-Transaktionen;
- Sämtliche Verarbeitung von Karteninhaberdaten, mit Ausnahme der Zahlungsseite, ist vollständig an einen nach PCI DSS validierten externen Zahlungsabwickler ausgelagert;
- Ihre E-Commerce-Website empfängt keine Karteninhaberdaten, sondern steuert, wie Verbraucher oder ihre Karteninhaberdaten an einen nach PCI DSS validierten externen Zahlungsabwickler weitergeleitet werden;
- Wenn eine Händler-Website von einem Drittanbieter gehostet wird, muss der Anbieter nach allen geltenden Anforderungen des PCI DSS validiert sein (z. B. einschließlich PCI-DSS-Anhang A, wenn der Anbieter ein Shared-Hosting-Anbieter ist);
- Jedes Element der Zahlungsseite(n), das an den Browser des Verbrauchers ausgeliefert wird, stammt entweder von der Website des Händlers oder von (einem) PCI-DSS-konformen Dienstleister(n);
- Ihr Unternehmen speichert, verarbeitet oder überträgt keine Karteninhaberdaten auf seinen Systemen oder an seinen Standorten elektronisch, sondern vergibt diese Funktionen vollständig an Dritte;
- Ihr Unternehmen hat sich vergewissert, dass (alle) Dritte(n), die für die Speicherung, Verarbeitung und/oder Übertragung von Karteninhaberdaten PCI-DSS-konform sind; **und**
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein.

Dieser SAQ gilt nur für E-Commerce-Kanäle.

Hinweis: *Für die Zwecke des SAQ-A-EP gelten PCI-DSS-Anforderungen bezüglich der „Karteninhaberdaten-Umgebung“ für die Händler-Website(s). Dies hat den Grund, dass die Händler-Website direkte Auswirkungen auf die Übertragung der Zahlungskartendaten hat, auch wenn die Website selbst keine Karteninhaberdaten empfängt.*

SAQ B – Händler mit ausschließlich Druckgeräten oder unabhängigen Dial-Out-Terminals. Keine elektronische Speicherung von Karteninhaberdaten

SAQ B wurde für die Anforderungen entwickelt, die für Händler gelten, welche Karteninhaberdaten nur über Druckmaschinen oder unabhängige Dial-Out-Terminals verarbeiten.

SAQ-B-Händler können entweder Händler mit physischer Präsenz (Kartenpräsenz) oder (telefonische) Versandhändler (keine Kartenpräsenz) sein und speichern keine Karteninhaberdaten auf jeglichen Computersystemen. SAQ-B-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

- Ihr Unternehmen nutzt ausschließlich eine Druckmaschine und/oder unabhängige Dial-Out-Terminals (die über eine Telefonleitung mit Ihrem Zahlungsabwickler verbunden sind), um die Zahlungskartendaten Ihrer Kunden zu erfassen;
- Die unabhängigen Dial-Out-Terminals sind nicht mit anderen Systemen in Ihrer Umgebung verbunden;
- Die unabhängigen Dial-Out-Terminals sind nicht mit dem Internet verbunden;
- Ihr Unternehmen überträgt Karteninhaberdaten nicht über ein Netzwerk (egal ob internes Netzwerk oder das Internet);
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein; **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Dieser SAQ gilt nicht für E-Commerce-Kanäle.

SAQ-B-IP – Händler mit unabhängigen PTS-POI-Terminals (Point of Interaction) mit IP-Anbindung, keine elektronische Speicherung von Karteninhaberdaten

SAQ-B-IP wurde für die Anforderungen entwickelt, die für Händler gelten, welche Karteninhaberdaten nur über unabhängige, PTS-geprüfte POI-Geräte (Point of Interaction) mit einer IP-Anbindung an den Zahlungsabwickler verarbeiten.

SAQ-B-IP-Händler können entweder Händler mit physischer Präsenz (Kartenpräsenz) oder (telefonische) Versandhändler (keine Kartenpräsenz) sein und speichern keine Karteninhaberdaten auf jeglichen Computersystemen.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

SAQ-B-IP-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

- Ihr Unternehmen nutzt nur unabhängige, PTS-geprüfte POI-Geräte (Point of Interaction) (ausgenommen SCRs) mit IP-Anbindung an Ihren Zahlungsabwickler, um die Zahlungskartendaten Ihrer Kunden zu erfassen;
- Die unabhängigen POI-Geräte mit IP-Anbindung sind nach dem PTS-POI-Programm validiert, wie auf der Website des PCI SSC aufgeführt (ausgenommen SCRs);
- Die unabhängigen POI-Geräte mit IP-Anbindung sind nicht mit anderen System in Ihrer Umgebung verbunden (dies lässt sich durch eine Netzwerksegmentierung zur Isolierung der POI-Geräte von anderen Systemen bewerkstelligen);
- Die einzige Übertragung der Karteninhaberdaten erfolgt von den PTS-geprüften POI-Geräten zum Zahlungsabwickler;
- Das POI-Gerät ist nicht von einem anderen Gerät (z. B. Computer, Mobiltelefon, Tablet etc.) abhängig, um die Verbindung zum Zahlungsabwickler herzustellen;
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein; **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Dieser SAQ gilt nicht für E-Commerce-Kanäle.

SAQ C-VT – Händler mit webbasierten virtuellen Terminals, keine elektronische Speicherung von Karteninhaberdaten

SAQ C-VT wurde für die Anforderungen entwickelt, die für Händler gelten, welche Karteninhaberdaten nur über isolierte virtuelle Zahlungsterminals auf einem PC verarbeiten, der mit dem Internet verbunden ist.

Ein virtuelles Zahlungsterminal ist ein Webbrowser-basierter Zugang zur Website eines Acquirers, Abwicklers oder externen Dienstleisters, um Zahlungskartentransaktionen zu autorisieren, wobei der Händler die Zahlungskartendaten manuell über einen sicher verbundenen Webbrowser eingibt. Anders als bei physischen Terminals lesen virtuelle Zahlungsterminal keine Daten direkt aus einer Zahlungskarte. Zahlungskartentransaktionen werden manuell eingegeben.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

SAQ-C-VT-Händler verarbeiten Karteninhaberdaten ausschließlich über ein virtuelles Zahlungsterminal und speichern keine Karteninhaberdaten auf Computersystemen. Diese virtuellen Terminals sind mit dem Internet verbunden, um auf einen Dritten zuzugreifen, der die Zahlungsabwicklungsfunktion des virtuellen Terminals bereitstellt. Dieser Dritte kann ein Abwickler, Acquirer oder sonstiger externer Dienstleister sein, der die Karteninhaberdaten speichert, verarbeitet und/oder überträgt, um die Zahlungstransaktionen vom virtuellen Terminal des Händlers zu autorisieren und/oder abzuwickeln.

Diese SAQ-Option richtet sich nur an Händler, die jeweils manuell eine Transaktion über eine Tastatur in eine internetbasierte virtuelle Terminal-Lösung eingeben. SAQ-C-VT-Händler können entweder Händler mit physischer Präsenz (Kartenpräsenz) oder (telefonische) Versandhändler (keine Kartenpräsenz) sein.

SAQ-C-VT-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

- Die einzige Zahlungsabwicklung Ihres Unternehmens erfolgt über ein virtuelles Zahlungsterminal, auf das von einem Webbrowser mit Internetverbindung zugegriffen wird;
- Die virtuelle Zahlungsterminal-Lösung Ihres Unternehmens wird von einem nach PCI DSS validierten externen Dienstleister bereitgestellt und gehostet;
- Ihr Unternehmen greift auf die PCI-DSS-konforme virtuelle Zahlungsterminal-Lösung über einen Computer zu, der auf einen einzigen Standort eingegrenzt ist und nicht mit anderen Standorten oder Systemen innerhalb Ihrer Umgebung verbunden ist (dies lässt sich über eine Firewall oder eine Netzwerksegmentierung bewerkstelligen, um den Computer von anderen Systemen zu isolieren);
- Auf dem Computer Ihres Unternehmens ist keine Software installiert, die für die Speicherung von Karteninhaberdaten sorgen würde (beispielsweise gibt es keine Software für die Sammelverarbeitung oder die Speicherung und Weiterleitung);
- Der Computer Ihres Unternehmens verfügt nicht über verbundene Hardware-Geräte, die zur Erfassung oder Speicherung von Karteninhaberdaten dienen (beispielsweise sind keine Kartenlesegeräte verbunden);
- Ihr Unternehmen empfängt oder überträgt anderweitig keine Karteninhaberdaten elektronisch (beispielsweise über ein internes Netzwerk oder das Internet);

- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein; **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Dieser SAQ gilt nicht für E-Commerce-Kanäle.

SAQ C – Händler mit Zahlungsanwendungssystemen mit Internetverbindung, keine elektronische Speicherung von Karteninhaberdaten

SAQ C wurde für die Anforderungen entwickelt, die für Händler gelten, deren Zahlungsanwendungssysteme (beispielsweise Point-of-Sale-Systeme) mit dem Internet verbunden sind (z. B. über DSL, Kabelmodem etc.).

SAQ-C-Händler verarbeiten Karteninhaberdaten über ein POS-System (Point of Sale) oder sonstige Zahlungsanwendungssysteme mit Internetverbindung, speichern keine Karteninhaberdaten auf Computersystemen und können sowohl Händler mit physischer Präsenz (Kartenpräsenz) oder (telefonische) Versandhändler (keine Kartenpräsenz) sein.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

SAQ-C-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

- Ihr Unternehmen hat ein Zahlungsanwendungssystem und eine Internetverbindung auf demselben Gerät und/oder im selben lokalen Netzwerk (LAN);
- Das Zahlungsanwendungssystem/Internetgerät ist nicht mit anderen Systemen in Ihrer Umgebung verbunden (dies lässt sich durch eine Netzwerksegmentierung zur Isolierung des Zahlungsanwendungssystems/Internetgeräts von anderen Systemen bewerkstelligen);
- Der physische Standort der POS-Umgebung ist nicht mit anderen Standorten verbunden und ein eventuell vorhandenes LAN ist ausschließlich für eine Filiale konfiguriert;
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein; **und**
- Ihr Unternehmen speichert keine Karteninhaberdaten in elektronischem Format.

Dieser SAQ gilt nicht für E-Commerce-Kanäle.

SAQ P2PE – Händler, die nur Hardware-Zahlungsterminals in einer vom PCI SSC geführten P2PE-Lösung verwenden, keine elektronische Speicherung von Karteninhaberdaten

SAQ P2PE wurde für die Anforderungen von Händlern entwickelt, die Karteninhaberdaten ausschließlich über Zahlungsterminals verarbeiten, welche in einer validierten und vom PCI SSC geführten P2PE-Lösung (Punkt-zu-Punkt-Verschlüsselung) enthalten sind.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

SAQ-P2PE-Händler haben auf keinem Computersystem Zugang zu Klartext-Kontodaten und geben Kundendaten nur über Hardware-Zahlungsterminals aus einer vom PCI SSC genehmigten P2PE-Lösung ein. SAQ-P2PE-Händler können entweder Händler mit physischer Präsenz (Kartenpräsenz) oder (telefonische) Versandhändler (keine Kartenpräsenz) sein. Beispielsweise kann ein (telefonischer) Versandhändler für SAQ P2PE qualifiziert sein, wenn er Karteninhaberdaten auf Papier oder telefonisch empfängt und diese direkt und ausschließlich in ein nach PCI DSS validiertes P2PE-Hardware-Gerät eingibt.

SAQ-P2PE-Händler bestätigen, dass sie die folgenden Qualifikationskriterien für diesen Zahlungskanal erfüllen:

- Sämtliche Zahlungsabwicklung erfolgt über eine validierte PCI-P2PE-Lösung, die vom PCI SSC genehmigt wurde und geführt wird;
- Die einzigen Systeme in der Händlerumgebung, die Kontodaten speichern, verarbeiten oder übertragen, sind die POI-Geräte (Point of Interaction), die für die Nutzung mit der validierten und PCI-geführten P2PE-Lösung freigegeben sind;
- Ihr Unternehmen empfängt oder überträgt sonst keine Karteninhaberdaten elektronisch;
- Es gibt keine ältere Speicherung elektronischer Karteninhaberdaten in der Umgebung;
- Alle Karteninhaberdaten, die Ihr Unternehmen aufbewahrt, liegen in Papierform vor (beispielsweise gedruckte Berichte oder Belege), und diese Dokumente gehen nicht elektronisch bei Ihnen ein; und
- Ihr Unternehmen hat alle Kontrollen im *P2PE-Handbuch (PIM)* umgesetzt, das vom P2PE-Lösungsanbieter bereitgestellt wurde.

Dieser SAQ gilt nicht für E-Commerce-Kanäle.

SAQ D für Händler – Alle sonstigen Händler mit SAQ-Qualifikation

SAQ D für Händler gilt für SAQ-qualifizierte Händler, die Kriterien anderer SAQ-Typen nicht erfüllen.

Beispiele für Händlerumgebungen, die SAQ D nutzen, umfassen unter anderem:

- E-Commerce-Händler, die Karteninhaberdaten auf ihrer Website entgegennehmen;
- Händler mit elektronischer Speicherung von Karteninhaberdaten;
- Händler, die Karteninhaberdaten nicht elektronisch speichern, aber die Kriterien anderer SAQ-Typen nicht erfüllen;
- Händler mit Umgebungen, die möglicherweise die Kriterien anderer SAQ-Typen erfüllen, jedoch zusätzliche PCI-DSS-Anforderungen aufgrund ihrer Umgebung erfüllen müssen.

SAQ D für Dienstleister – Dienstleister mit SAQ-Qualifikation

SAQ D für Dienstleister gilt für alle Dienstleister, die von einer Zahlungsmarke als SAQ-qualifiziert definiert wurden.

Hinweis zu SAQ D für Händler und SAQ D für Dienstleister: Obwohl viele Unternehmen die SAQ D ausfüllen, die Compliance für alle PCI-DSS-Anforderungen nachweisen müssen, stellen Unternehmen mit sehr speziellen Geschäftsmodellen möglicherweise fest, dass einige Anforderungen für sie nicht gelten. Ein Unternehmen, das bei keiner Funktion Funktechnologie einsetzt, müsste zum Beispiel keine Compliance für Abschnitte des PCI DSS nachweisen, die speziell für die Handhabung von Funktechnologie gelten. Im jeweiligen SAQ D finden Sie spezielle Hinweise zum Ausschluss anderer spezifischer Anforderungen.

Einen grafischen Leitfaden zur Auswahl Ihres SAQ-Typs finden Sie auf Seite 20 in „Welcher SAQ-Typ trifft am ehesten auf meine Umgebung zu?“.

Welcher SAQ passt am besten zu meiner Umgebung?