



Payment Card Industry (PCI)- Datensicherheitsstandard für Zahlungsanwendungen (PA-DSS)

Programmleitfaden

Version 1.2

Oktober 2008

Dokumentänderungen

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

Inhalt

Dokumentänderungen	1
Einleitung	3
Zugehörige Veröffentlichungen.....	3
Updates für Dokumente und Sicherheitsanforderungen	3
Terminologie	3
Über PCI	4
PA-DSS – Angleichungsinitiative und Übersicht	4
Rollen und Verantwortlichkeiten	5
Überlegungen des Anbieters – Vorbereitung auf die Prüfung	8
Für welche Anwendungen gilt der PA-DSS?	8
Vor der Prüfung.....	9
Erforderliche Dokumentationen und Materialien	9
Zeitrahmen der PA-DSS-Prüfung	10
Qualifizierte Sicherheitsprüfer von Zahlungsanwendungen	10
Zugehörige PA-DSS-Dienste, die von PA-QSAs angeboten werden können.....	10
Technische Unterstützung beim Testen	11
Verzichtserklärung und Berichtübergabe	11
Gebühren	11
Übersicht über die PA-DSS-Prozesse	12
Abbildung 1: PA-DSS-Berichtannahmeprozess	13
Abbildung 2: PA-DSS – Änderungen an aufgelisteten Anwendungen	14
Abbildung 3: Übertragung und Übergang der PABP-Anwendungen zur PA-DSS-Liste	15
Abbildung 4: PA-DSS – Jährliche Neuvalidierung und Erneuerung abgelaufener Anwendungen	16
Abbildung 5: PA-QSA-Qualitätssicherungsprogramme für Berichtsprüfungen	17
PA-DSS-Berichtannahmeprozess – Übersicht	18
Änderungen an aufgelisteten Zahlungsanwendungen	19
Verlängerung abgelaufener Anwendungen	22
Übergang und Übertragung von PABP-validierten Zahlungsanwendungen	23
Qualitätssicherungsprogramm	25
PA-DSS-Berichterstellungsverfahren	27
Benachrichtigung nach einer Sicherheitsverletzung oder Sicherheitsgefährdung	28
Rechtliche Bestimmungen	30
Anhang A: Elemente für den Annahmepflicht und die <i>Liste PA-DSS-validierter Zahlungsanwendungen</i>	31
Anhang B: Identifizierung zertifizierter Zahlungsanwendungs-Builds	34
Anhang C: Selbstbescheinigung über kleine Versionsänderungen	35

Einleitung

Zugehörige Veröffentlichungen

Das folgende Dokument bildet die Grundlage für Beurteilungen der Zahlungsanwendung:

- *Payment Card Industry (PCI)-Datensicherheitsstandard für Zahlungsanwendungen – Anforderungen und Sicherheitsbeurteilungsverfahren*
- *Payment Card Industry (PCI)-Datensicherheitsstandard für Zahlungsanwendungen – Verfahrensweisen für den Übergang*

Die folgenden Dokumente werden zusätzlich zu den zuvor erwähnten Dokumenten verwendet:

- *Payment Card Industry (PCI)-Datensicherheitsstandard – Anforderungen und Sicherheitsbeurteilungsverfahren*
- *Payment Card Industry (PCI)-Datensicherheitsstandard und -Datensicherheitsstandard für Zahlungsanwendungen – Glossar für Begriffe, Abkürzungen und Akronyme*
- *Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements (Payment Card Industry (PCI)-Datensicherheitsstandard – QSA-Validierungsanforderungen)*
- *Payment Card Industry (PCI)-Datensicherheitsstandard – QSA-Validierungsanforderungen – Ergänzung für qualifizierte Sicherheitsprüfer von Zahlungsanwendungen (PA-QSAs)*

Hinweis:

Die PA-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren enthalten die spezifischen technischen Anforderungen und stellen die Beurteilungsverfahren und -vorlagen bereit, die zur Validierung der Konformität der Zahlungsanwendung und zur Dokumentierung der Prüfung verwendet werden. In den beiden Dokumenten für die QSA-Validierungsanforderungen werden die Anforderungen definiert, die ein PA-QSA erfüllen muss, um die Beurteilungen durchzuführen. Alle Dokumente stehen in elektronischer Form unter www.pcisecuritystandards.org zur Verfügung.

Updates für Dokumente und Sicherheitsanforderungen

Das Streben nach Sicherheit ist ein niemals endendes Rennen gegen mögliche Angreifer. Aus diesem Grund ist es erforderlich, die Sicherheitsanforderungen, die zur Beurteilung der Zahlungsanwendungen verwendet werden, regelmäßig zu prüfen, zu aktualisieren und zu verbessern. Der PCI SSC bemüht sich, die Sicherheitsanforderungen der Zahlungsanwendung alle 24 Monate zu aktualisieren.

Der PCI SSC behält sich außerdem das Recht vor, Sicherheitsanforderungen jederzeit zu ändern, zu ergänzen oder zurückzuziehen. Wenn eine solche Änderung erforderlich ist, arbeitet der PCI SSC eng mit den teilnehmenden Unternehmen und Softwareanbietern der PCI SSC-Community zusammen, damit die Änderungen so störungsfrei wie möglich verlaufen.

Terminologie

Die folgenden Begriffe werden in diesem Dokument verwendet:

- „PCI SSC“ steht für PCI Security Standards Council, LLC.
- „PABP“ bezieht sich auf das frühere Payment Application Best Practices-Programm von Visa, auf dem der Datensicherheitsstandard für Zahlungsanwendungen (Payment Application Data Security Standard, PA-DSS) basiert.
- Der Begriff „Zahlungsmarken“ bezeichnet die Kreditkartenunternehmen, die Mitglied des PCI SSC sind. Zurzeit sind das American Express, Discover, JCB, MasterCard und Visa.
- Mit „Zahlungsanwendungen“ werden im Allgemeinen alle an Dritte verkauften, vertriebenen oder lizenzierten Zahlungsanwendungen bezeichnet, bei denen Karteninhaberdaten im Zuge der Autorisierung oder Verrechnung gespeichert, verarbeitet oder weitergegeben werden.

Über PCI

Der PCI SSC spiegelt den Wunsch aller Beteiligten der Payment Card Industry (PCI) wider, Sicherheitsanforderungen, Sicherheitsbeurteilungsverfahren und Prozesse für die Anerkennung von Zahlungsanwendungen, die von einem PA-QSA validiert wurden, anzugleichen und zu standardisieren. Der PA-DSS und die damit verbundenen PCI SSC-Standards definieren einen gemeinsamen Sicherheitsbeurteilungsrahmen, der von allen Zahlungsmarken anerkannt wird.

Alle Beteiligten an der Zahlungswertschöpfungskette profitieren von den angeglichenen Anforderungen:

- Kunden haben den Vorteil, dass eine größere Auswahl an sicheren Zahlungsanwendungen bereitsteht.
- Kunden haben die Gewissheit, dass sie Produkte verwenden, die die Validierungsanforderungen erfüllen.
- Anbieter müssen nur eine einzelne Zahlungsanwendungsprüfung durchführen, die von allen Zahlungsmarken erkannt wird.

Weitere Informationen zum PCI SSC finden Sie auf der PCI SSC-Website unter www.pcisecuritystandards.org (die „Website“).

PA-DSS – Angleichungsinitiative und Übersicht

In diesem Payment Card Industry-PA-DSS-Programmeitfadens wird die Angleichung der Anforderungen der Zahlungsmarken an die folgenden Standards berücksichtigt:

- Sicherheitsanforderungen und -beurteilungsverfahren für Zahlungsanwendungen
- Prozesse für die Anerkennung von Zahlungsanwendungen, die von PA-QSAs validiert wurden
- Prozesse für den Übergang von PABP-validierten Zahlungsanwendungen zur PCI SSC-Liste
- Qualitätssicherungsprozesse für PA-QSAs

Hinweis:

PA-DSS-Berichte werden direkt vom PCI SSC geprüft und anerkannt.

Die übliche Einhaltung des PCI-DSS gilt unter Umständen nicht direkt für Anbieter von Zahlungsanwendungen, da die meisten von ihnen keine Karteninhaberdaten speichern, verarbeiten oder weitergeben. Da allerdings die betreffenden Zahlungsanwendungen von Kunden genutzt werden, um Karteninhaberdaten zu speichern, zu verarbeiten und weiterzugeben, und Kunden die PCI-DSS-Konformität sicherstellen müssen, sollten Zahlungsanwendungen die Einhaltung des Standards durch die Kunden begünstigen und nicht behindern. Zahlungsanwendungen können der PCI-DSS-Konformität z. B. aus den folgenden Gründen im Wege stehen:

1. Magnetstreifendaten, die nach der Autorisierung im Netzwerk des Kunden gespeichert werden
2. Anwendungen, die Kunden dazu auffordern, andere für den PCI-DSS erforderliche Funktionen, wie Antivirensoftware oder Firewalls, zu deaktivieren, um eine ordnungsgemäße Funktion der Zahlungsanwendung sicherzustellen
3. Nutzung ungesicherter Methoden zur Verbindung mit der Anwendung durch Anbieter zu Kundensupport-Zwecken

Sichere Zahlungsanwendungen minimieren *bei einer Implementierung in einer PCI-DSS-konformen Umgebung* das Potenzial von Sicherheitsverletzungen, die zu einer Kompromittierung von Magnetstreifendaten, von Kartvalidierungs-codes und -werten (CAV2, CID, CVC2, CVV2) sowie von PINs und PIN-Blöcken führen, und verhindern somit Schädigungen durch Betrug, der auf diese Sicherheitsverletzungen zurückzuführen ist.

Rollen und Verantwortlichkeiten

In der Branche für Zahlungsanwendungen gibt es mehrere wichtige Entscheidungsträger. Einige dieser Teilnehmer sind unmittelbar am PA-DSS-Beurteilungsverfahren beteiligt: Anbieter, PA-QSAs und der PCI SSC. Andere Mitglieder der Branche, die nicht direkt in Prüfverfahren involviert sind, sollten dennoch die allgemeinen Verfahrensweisen kennen, um Geschäftsentscheidungen in diesem Bereich leichter treffen zu können.

Im Folgenden werden die Rollen und Verantwortlichkeiten der Entscheidungsträger aus der Branche für Zahlungsanwendungen beschrieben. Für die Entscheidungsträger, die in Prüfverfahren involviert sind, sind entsprechende Verantwortlichkeiten aufgelistet.

Zahlungsmarken

American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa Inc. sind die Zahlungsmarken, die für die Gründung des PCI SSC verantwortlich zeichneten. Diese Marken sind für die Entwicklung und Durchsetzung sämtlicher Programme im Bezug auf PA-DSS-Konformität verantwortlich, darunter die folgenden:

- Sämtliche Anforderungen, Mandate oder Daten zur Verwendung von PA-DSS-konformen Zahlungsanwendungen
- Jegliche Gebühren oder Bußgelder, die bei der Verwendung nicht konformer Zahlungsanwendungen erhoben werden

Die Zahlungsmarken können Konformitätsprogramme, Mandate, Daten usw. unter Verwendung des PA-DSS und der validierten und durch den PCI SSC aufgelisteten Zahlungsanwendungen definieren. Über diese Konformitätsprogramme fördern die Zahlungsmarken die Nutzung der aufgelisteten, validierten Zahlungsanwendungen.

Der Payment Card Industry Security Standards Council (PCI SSC)

Der PCI SSC ist eine Normungsorganisation der Zahlungskartenbranche zur Überwachung der Branchenstandards, darunter des PCI-DSS und des PA-DSS. Im Bezug auf den PA-DSS übernimmt der PCI SSC folgende Aufgaben:

- Zentrale Archivierung von PA-DSS-Validierungsberichten („Reports of Validation“, kurz ROVs)
- Durchführung von Qualitätssicherungsprüfungen von PA-DSS-ROVs zur Sicherstellung der Konsistenz und Qualität von Berichten
- Auflistung PA-DSS-validierter Zahlungsanwendungen auf der Website
Hinweis: Diese Liste ist erst ab Oktober 2008 auf der Website verfügbar.
- Ausbildung und Schulung von PA-QSAs für die Durchführung von PA-DSS-Prüfungen
- Pflege und Aktualisierung des PA-DSS und den Standard betreffender Dokumentationen entsprechend einem Lebenszyklus-Management-Prozess für den Standard

Beachten Sie, dass die Bestätigung durch den PCI SSC nicht gleichbedeutend mit einer Validierung ist. Die Rolle der PA-QSAs besteht darin, die PA-DSS-Konformität von Zahlungsanwendungen am jeweiligen Prüfdatum zu dokumentieren. Darüber hinaus führt der PCI SSC Qualitätssicherungsmaßnahmen durch, um sicherzugehen, dass die PA-QSAs ihre PA-DSS-Beurteilungen akkurat und gründlich dokumentieren.

Softwareanbieter

Softwareanbieter („Anbieter“) entwickeln Zahlungsanwendungen, die Karteninhaberdaten im Zuge einer Autorisierung oder Verrechnung speichern, verarbeiten oder weitergeben, und verkaufen, vertreiben oder lizenzieren diese Zahlungsanwendungen dann an Dritte (Kunden oder Wiederverkäufer/Integratoren). Anbieter sind verantwortlich für:

- Die Erstellung PA-DSS-konformer Zahlungsanwendungen, die die PCI-DSS-Konformität ihrer Kunden fördern und nicht behindern (Die Anwendung darf keine Implementierung oder Konfiguration erfordern, die gegen die PCI-DSS-Anforderungen verstößt.)
- Einhaltung der PCI-DSS-Anforderungen, wenn der Anbieter Karteninhaberdaten speichert, verarbeitet oder weitergibt (z. B. bei der Fehlerbehandlung beim Kunden)
- Erstellung eines *PA-DSS-Implementierungshandbuchs* für jede Anwendung – gemäß den Anforderungen des *Datensicherheitsstandards für Zahlungsanwendungen*
- Schulung der Kunden, Wiederverkäufer und Integratoren im Hinblick auf die Installation und Konfiguration der Zahlungsanwendungen auf PCI-DSS-konforme Weise
- Sicherstellung, dass die Zahlungsanwendungen die PA-DSS-Anforderungen erfüllen, indem eine PA-DSS-Prüfung gemäß den *PCI-PA-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren* erfolgreich absolviert wird

Anbieter reichen ihre Zahlungsanwendungen und unterstützenden Dokumentationen zur Prüfung durch den PA-QSA ein. Alle Vereinbarungen und Kosten im Zusammenhang mit der Beurteilung werden zwischen dem Anbieter und dem PA-QSA verhandelt. Die Anbieter erteilen ihrem PA-QSA die Genehmigung, die resultierenden PA-DSS-Konformitätsberichte dem PCI SSC vorzulegen.

PA-QSAs

PA-QSAs sind QSAs, die vom PCI SSC für die Durchführung von PA-DSS-Überprüfungen qualifiziert und geschult worden sind. *Beachten Sie, dass nicht alle QSAs auch PA-QSAs sind. Ein PA-QSA verfügt gegenüber einem QSA über zusätzliche Qualifikationen.*

PA-QSAs sind verantwortlich für:

- Die Durchführung von Beurteilungen zu Zahlungsanwendungen in Übereinstimmung mit den Sicherheitsbeurteilungsverfahren und den PA-QSA-Validierungsanforderungen
- Die Abgabe einer Beurteilung, ob eine Zahlungsanwendung die PA-DSS-Anforderungen erfüllt
- Die Bereitstellung geeigneter Dokumentationen innerhalb der ROVs, die die PA-DSS-Konformität der Zahlungsanwendung demonstrieren
- Das Einreichen der ROVs beim PCI SSC, zusammen mit der Validierungsbestätigung (unterzeichnet vom PA-QSA und vom Anbieter)
- Die Pflege eigener Qualitätssicherungsmaßnahmen

Der PA-QSA ist dafür verantwortlich, zu bestätigen, ob die Zahlungsanwendung konform ist oder nicht. Der PCI SSC bestätigt ROVs nicht hinsichtlich der technischen Konformität, sondern führt Qualitätssicherungsprüfungen an den ROVs durch, um sicherzustellen, dass die Konformität in den Berichten ordnungsgemäß demonstriert wird.

Wiederverkäufer und Integratoren

Wiederverkäufer und Integratoren verkaufen, installieren und/oder bieten Service für Zahlungsanwendungen im Namen von Softwareanbietern oder anderen an. Wiederverkäufer und Integratoren, die Dienste im Zusammenhang mit PA-DSS-konformen Zahlungsanwendungen anbieten, sind verantwortlich für:

- Die Implementierung von ausschließlich PA-DSS-konformen Zahlungsanwendungen in eine PCI-DSS-konforme Umgebung (bzw. entsprechende Anweisung für den Händler)
- Die Konfiguration dieser Zahlungsanwendungen (wenn Konfigurationsoptionen vorhanden sind) gemäß dem *PA-DSS-Implementierungshandbuch*, das vom Anbieter bereitgestellt wird
- Die Konfiguration dieser Zahlungsanwendungen (oder die entsprechende Anweisung für den Händler) auf PCI-DSS-konforme Weise
- Die Wartung dieser Zahlungsanwendungen (z. B. Fehlerbehebung, Bereitstellung von Remote-Updates und Remote-Unterstützung) gemäß dem *PA-DSS-Implementierungshandbuch* und dem PCI-DSS.

Wiederverkäufer und Integratoren sind nicht dafür zuständig, Zahlungsanwendungen zur Überprüfung einzureichen. Produkte können nur vom Anbieter eingereicht werden.

Kunden

Kunden sind Großhändler, Dienstleister und andere Käufer oder Nutzer von Drittanbieter-Zahlungsanwendungen zum Speichern, Verarbeiten oder Weitergeben von Karteninhaberdaten im Zuge einer Autorisierung oder der Verrechnung bei Zahlungstransaktionen. Kunden, die PA-DSS-konforme Anwendungen nutzen möchten, sind für Folgendes verantwortlich:

Hinweis:

Eine PA-DSS-konforme Zahlungsanwendung allein ist noch keine Garantie für PCI-DSS-Konformität.

- Implementierung einer PA-DSS-konformen Zahlungsanwendung in einer PCI-DSS-konformen Umgebung
- Konfigurieren der Zahlungsanwendung (sofern Konfigurationsoptionen bereitstehen) entsprechend dem vom Anbieter bereitgestellten *PA-DSS-Implementierungshandbuch*
- Konfigurieren der Zahlungsanwendung auf PCI-DSS-konforme Art und Weise
- Aufrechterhalten des PCI-DSS-Konformitätsstatus sowohl für die Umgebung als auch für die Konfiguration der Zahlungsanwendung

Wenn die Liste vom PCI SSC in der zweiten Hälfte des Jahres 2008 veröffentlicht wird, finden Kunden die validierten Zahlungsanwendungen zusammen mit anderen Referenzmaterialien auf der Website.

Überlegungen des Anbieters – Vorbereitung auf die Prüfung

Für welche Anwendungen gilt der PA-DSS?

Im Hinblick auf den PA-DSS werden Zahlungsanwendungen als an Dritte verkaufte, vertriebene oder lizenzierte Anwendungen definiert, bei denen Karteninhaberdaten im Zuge der Autorisierung oder Verrechnung gespeichert, verarbeitet oder weitergegeben werden.

Die folgende Anleitung hilft bei der Bestimmung, ob der PA-DSS für eine gegebene Zahlungsanwendung gilt:

- Der PA-DSS gilt für Zahlungsanwendungen, die üblicherweise „vom Regal“ verkauft und installiert werden, also ohne individuelle Anpassung durch Softwareanbieter.
- Der PA-DSS gilt für Zahlungsanwendungen, die in Modulen bereitgestellt werden, zu deren Lieferumfang üblicherweise ein „Basis“-Modul und weitere spezifisch auf Kundentypen oder -anforderungen zugeschnittene Module gehören. Der PA-DSS gilt eventuell lediglich für das Basis-Modul, wenn dieses als einziges Modul Zahlungsfunktionen durchführt (nach Bestätigung durch einen PA-QSA). Wenn weitere Module Zahlungsfunktionen übernehmen, gilt der PA-DSS auch für diese Module. Beachten Sie, dass es sich für Softwareanbieter bewährt hat, Zahlungsfunktionen isoliert auf einem einzigen oder einer geringen Anzahl von Basis-Modulen anzubieten und andere Module für andere Funktionen vorzubehalten. Diese bewährte Methode kann (wenngleich sie kein unbedingtes Muss ist) dabei helfen, die Anzahl der Module, für die der PA-DSS Gültigkeit hat, zu begrenzen.
- Der PA-DSS gilt NICHT für Zahlungsanwendungen, die ausschließlich für einen Kunden entwickelt und verkauft wurden, da diese Anwendungen im Rahmen der üblichen Überprüfung zur Einhaltung des PCI-DSS beim Kunden abgedeckt sind. Beachten Sie, dass solche Anwendungen (oft auch als „Maßanfertigungen“ bezeichnet) nur an einen einzigen Kunden verkauft werden (für gewöhnlich ein Großhändler oder Dienstleister) und entsprechend der vom Kunden bereitgestellten Spezifikationen entworfen und entwickelt werden.
- Der PA-DSS gilt NICHT für Zahlungsanwendungen, die von Großhändlern und Dienstleistern ausschließlich zur internen Verwendung entwickelt wurden (und nicht an Dritte verkauft, vertrieben oder lizenziert werden), da diese intern entwickelten Zahlungsanwendungen im Rahmen der normalen Prüfung hinsichtlich der PCI-DSS-Einhaltung beim betreffenden Großhändler oder Dienstleister ebenfalls geprüft werden.

Beispiel für die letzten beiden Punkte: Unabhängig davon, ob die intern entwickelte oder „maßgefertigte“ Zahlungsanwendung verbotenerweise sensible Authentifizierungsdaten speichert oder komplexe Kennwörter zulässt, wäre sie im Rahmen der üblichen Verfahrensweise des Großhändlers bzw. Dienstleisters zur Einhaltung des PCI-DSS abgedeckt, sodass keine separate PA-DSS-Prüfung erforderlich ist.

In der folgenden Liste werden einige Anwendungen aufgeführt, die KEINE Zahlungsanwendungen gemäß PA-DSS sind (und deshalb auch nicht hinsichtlich einer PA-DSS-Einhaltung geprüft werden müssen):

- Betriebssysteme, unter denen eine Zahlungsanwendung installiert wird (z. B. Windows, Unix)
- Datenbanksysteme, in denen Karteninhaberdaten gespeichert sind (z. B. Oracle)
- Back-Office-Systeme, in denen Karteninhaberdaten gespeichert sind (z. B. zur Berichterstellung oder für den Kundenservice)

Hinweis:

Der PCI SSC listet AUSSCHLIESSLICH Zahlungsanwendungen auf.

Vor der Prüfung

- Prüfen Sie die PCI-DSS- und die PA-DSS-Anforderungen sowie die damit verbundenen Dokumentationen, die sich auf der Website befinden.
- Bestimmen und beurteilen Sie die PA-DSS-Konformität der Zahlungsanwendung:
 - Stellen Sie in einer „Lückenanalyse“ fest, welche Unterschiede zwischen der Zahlungsanwendung, die den PA-DSS-Funktionen unterliegt, und den PA-DSS-Anforderungen bestehen.
 - Schließen Sie jegliche Lücken.
 - Auf Wunsch kann der PA-QSA eine Vorbeurteilung oder „Lückenanalyse“ der Zahlungsanwendung eines Anbieters durchführen. Wenn der PA-QSA Mängel feststellt, die eine klare Stellungnahme verhindern würden, stellt er für den Softwareanbieter eine Liste der Zahlungsanwendungsfunktionen zusammen, auf die vor der offiziellen Prüfung eingegangen werden muss.
- Stellen Sie fest, ob das *PA-DSS-Implementierungshandbuch* die PA-DSS-Anforderungen erfüllt.

Erforderliche Dokumentationen und Materialien

Eine Beurteilung ist nur unter der Voraussetzung möglich, dass der Softwareanbieter die entsprechenden Dokumentationen und Softwareanwendungen für den PA-QSA bereitstellt.

Alle für den PA-DSS relevanten Informationen und Dokumente können von der Website heruntergeladen werden. Alle vollständigen Materialien in Bezug auf die Zahlungsanwendung, z. B. Installations-CDs, Handbücher, das *PA-DSS-Implementierungshandbuch* usw., die für die Prüfung relevant sind, müssen an einen auf der Website aufgeführten PA-QSA weitergeleitet werden, nicht an den PCI SSC. Prüfungsspezifische Informationen sollten direkt beim PA-QSA angefordert werden.

Beispiele für Dokumente und Komponenten, die dem PA-QSA vorzulegen sind:

1. Die Zahlungsanwendung mit Bedienungshandbuch oder Anweisungen
2. Das erforderliche Hardware- und Softwarezubehör, um eine Zahlungstransaktion simulieren zu können
3. Dokumentationen, die alle Funktionen für die Datenein- und -ausgabe beschreiben, können von Entwicklern von Drittanbieteranwendungen verwendet werden. Insbesondere müssen Funktionen in Zusammenhang mit Erfassung, Autorisierung, Verrechnung und Ausgleichsbuchungsabläufen (wenn für die Anwendung zutreffend) beschrieben werden. (Diese Anforderung könnte z. B. durch ein Handbuch erfüllt werden.)
4. Dokumentation, die sich auf die Installation und Konfiguration der Anwendung bezieht oder Informationen über die Anwendung bereitstellt. Beispiele für solche Dokumentationen:
 - *PA-DSS-Implementierungshandbuch*
 - Softwareinstallationshandbuch oder -anweisungen (gemäß Vorlage an die Kunden)
 - Versionsnummerierungsschema des Anbieters
 - Änderungskontrolldokumentation, die zeigt, wie Kunden über Änderungen informiert werden
5. Zusätzliche Dokumentation – z. B. Flussdiagramme und andere Diagramme –, die bei der Prüfung der Zahlungsanwendung behilflich ist (der PA-QSA kann ggf. zusätzliche Materialien anfordern)

Zeitrahmen der PA-DSS-Prüfung

Es dauert unterschiedlich lange, eine PA-DSS-Prüfung von Anfang bis Ende auszuführen, bis eine vollständig validierte Anwendung vorliegt, für die angegeben werden kann, dass alle Komponenten implementiert sind. Die folgenden Faktoren bestimmen die Zeitdauer:

- Wie weit die Anwendung zu Beginn der Prüfung von der PA-DSS-Konformität entfernt ist
 - Korrekturen an der Zahlungsanwendung, um Konformität zu erreichen, verlängern die Zeitdauer.
- Wie fortgeschritten das *PA-DSS-Implementierungshandbuch* zu Beginn der Prüfung ist
 - Viele nachträgliche Änderungen am Text des *Handbuchs* verlängern die Zeitdauer.
- Ob der PA-QSA einen hochwertigen PA-DSS-ROV vorbereitet und dem PCI SSC vorlegt
 - Wenn der PCI SSC den Bericht mehrmals prüft und Anmerkungen macht, auf die der PA-QSA jedes Mal eingehen muss, verlängert dies die Zeitdauer.

Alle Zeitrahmen, die von einem PA-QSA genannt werden, sollten als Schätzwerte angesehen werden, da sie auf der Annahme basieren können, dass die Zahlungsanwendung alle PA-DSS-Anforderungen schnell erfüllt. Wenn während des Prüf- oder des Annahmeverfahrens Probleme festgestellt werden, müssen der PA-QSA, der Softwareanbieter und/oder der PCI SSC diese besprechen. Solche Diskussionen können eine Auswirkung auf die Prüfzeiten haben, Verzögerungen verursachen und/oder dazu führen, dass die Prüfung verfrüht endet (wenn der Anbieter z. B. entscheidet, dass er die Änderungen nicht vornehmen möchte, die zum Erreichen der Konformität erforderlich sind).

Qualifizierte Sicherheitsprüfer von Zahlungsanwendungen

Der PCI SSC qualifiziert und schult Sicherheitsprüfer von Zahlungsanwendungen (Payment Application-Qualified Security Assessors, kurz PA-QSAs) für die Durchführung von PA-DSS-Beurteilungen. Die PA-QSAs sind auf der Website aufgelistet. Sie sind die einzigen Prüfer, die vom PCI SSC für die Durchführung von PA-DSS-Beurteilungen anerkannt werden.

Die Preise und Gebühren der PA-QSAs werden nicht vom PCI SSC festgelegt. Diese Gebühren werden zwischen dem PA-QSA und dem Kunden verhandelt. Es wird empfohlen, mit verschiedenen PA-QSA-Unternehmen zu sprechen und die unternehmenseigenen Prozesse zur Anbieterauswahl zu befolgen, um einen PA-QSA auszuwählen.

Zugehörige PA-DSS-Dienste, die von PA-QSAs angeboten werden können

Der PCI SSC verlangt oder empfiehlt keinen dieser Dienste. Diese Liste dient nur als Beispiel für die Art von Diensten, die von PA-QSAs angeboten werden können. Wenn diese Dienste für Ihr Unternehmen interessant sind, wenden Sie sich bitte an die PA-QSAs, um sich über die Verfügbarkeit und die Preise zu informieren. Beispiele für Dienste im Zusammenhang mit dem PA-DSS:

- Anleitung für die Entwicklung von Zahlungsanwendungen gemäß PA-DSS
- Prüfung des Softwaredesigns eines Softwareanbieters, Beantwortung von Fragen per E-Mail oder auf telefonischem Weg und Teilnahme an Konferenzgesprächen, um die Anforderungen zu klären
- Anweisungen für die Vorbereitung des *PA-DSS-Implementierungshandbuchs*
- Vorbeurteilungsdienste („Lückenanalyse“) vor der offiziellen PA-DSS-Beurteilung
- Anweisungen, wie die Zahlungsanwendung PA-DSS-konform gemacht werden kann, wenn während der Beurteilung Lücken oder nicht konforme Bereiche festgestellt werden

Technische Unterstützung beim Testen

Es wird empfohlen, dass ein technischer Mitarbeiter des Anbieters bereitsteht, um Fragen zu beantworten, die während der Beurteilung auftreten. Während der Prüfung – und um den Prozess zu beschleunigen – sollte ein Ansprechpartner des Anbieters immer erreichbar sein, um Probleme zu besprechen und Fragen des PA-QSAs zu beantworten.

Verzichtserklärung und Berichtübergabe

Bevor der PA-QSA den PA-DSS-Bericht an den PCI SSC freigeben kann, muss der Anbieter die Freigabe des Berichts zur Prüfung durch den PCI SSC genehmigen und aus diesem Grund eine *Payment Card Industry PA-DSS Vendor Release Agreement* des PCI SSC („Verzichtserklärung“) unterschreiben. Der PA-QSA muss die Verzichtserklärung zusammen mit den PA-DSS-Berichten **direkt** an den PCI SSC weiterleiten.

Gebühren

Alle Gebühren und Termine, die in Zusammenhang mit der PA-DSS-Beurteilung des PA-QSAs stehen, werden zwischen dem PA-QSA und dem Zahlungsanwendungsanbieter vereinbart. Der Anbieter begleicht alle anfallenden Gebühren direkt beim PA-QSA.

Für Anbieter fällt eine Jahresgebühr in Höhe von 1.250 USD für jede Zahlungsanwendung an, die auf der Zahlungsanwendungsliste des PCI SSC eingetragen ist.

Im Rahmen des jährlichen Neuvalidierungsprozesses (siehe Abschnitt „Jährliche Neuvalidierung“ weiter unten im Dokument) wird die Gebühr für den Eintrag den Softwareanbietern jährlich vom PCI SSC in Rechnung gestellt. Die Rechnung umfasst alle Zahlungsanwendungen dieses Anbieters, die am Rechnungsdatum in der Liste des PCI SSC enthalten sind. Die Rechnung wird vierteljährlich gestellt, abhängig vom Quartal des ersten Eintrags. Beispiel: Am 1. April werden Softwareanbietern 1.250 USD pro Zahlungsanwendung in Rechnung gestellt, die im am 31. März endenden Quartal in der Liste eingetragen sind. Anwendungen, die zwar validiert sind, die aber auf Wunsch des Softwareanbieters nicht auf der Website aufgelistet sind, werden dem Anbieter nicht in Rechnung gestellt. Hinweis: Anbieter können die Einträge nicht manipulieren, um Gebühren zu vermeiden. Das bedeutet, dass es nicht möglich ist, dass Anbieter eine Anwendung aus der Liste entfernen lassen und nach der Rechnungsstellung die erneute Eintragung beantragen.

Hinweis:

Der Anbieter zahlt alle PA-DSS-Beurteilungsgebühren direkt an den PA-QSA (diese Gebühren werden zwischen dem Anbieter und dem PA-QSA verhandelt).

Der PCI SSC stellt dem Anbieter alle Gebühren für den Listeneintrag vierteljährlich in Rechnung, und der Anbieter zahlt diese Gebühren direkt an den PCI SSC.

Übersicht über die PA-DSS-Prozesse

Der PA-DSS-Prüfprozess wird vom Anbieter initiiert. Auf der Website sind alle damit verbundenen Dokumente enthalten, die der Anbieter benötigt, um den PA-DSS-Prüfprozess durchzuführen. Der Anbieter wählt einen PA-QSA aus der Liste des PCI SSC aus und vereinbart die Kosten und das Geheimhaltungsabkommen mit dem PA-QSA. Der Anbieter leitet anschließend die Zahlungsanwendungssoftware, Handbücher und andere erforderliche Dokumentationen an den PA-QSA weiter. Der PCI SSC stellt einen Annahmepflicht aus, der für jede Zahlungsanwendung den erfolgreichen Abschluss des Prozesses bestätigt („PA-DSS-Annahmepflicht“). Nach der Annahme der Zahlungsanwendung wird das Produkt auf der Website aufgelistet.

Die Abbildungen und Beschreibungen auf den folgenden Seiten erklären die nachfolgenden Komponenten des PA-DSS-Programms im Detail:

Prozess	Abbildung	Seite
PA-DSS-Berichtannahmeprozess	Abbildung 1	12
PA-DSS-Änderungen an aufgelisteten Anwendungen	Abbildung 2	13
Übertragung und Übergang der PABP-Anwendungen zur PA-DSS-Liste	Abbildung 3	14
PA-DSS-Jährliche Neuvalidierung und Erneuerung abgelaufener Anwendungen	Abbildung 4	15
PA-QSA-Qualitätssicherungsprogramm für Berichtsprüfungen	Abbildung 5	16

Abbildung 1: PA-DSS-Berichtannahmeprozess

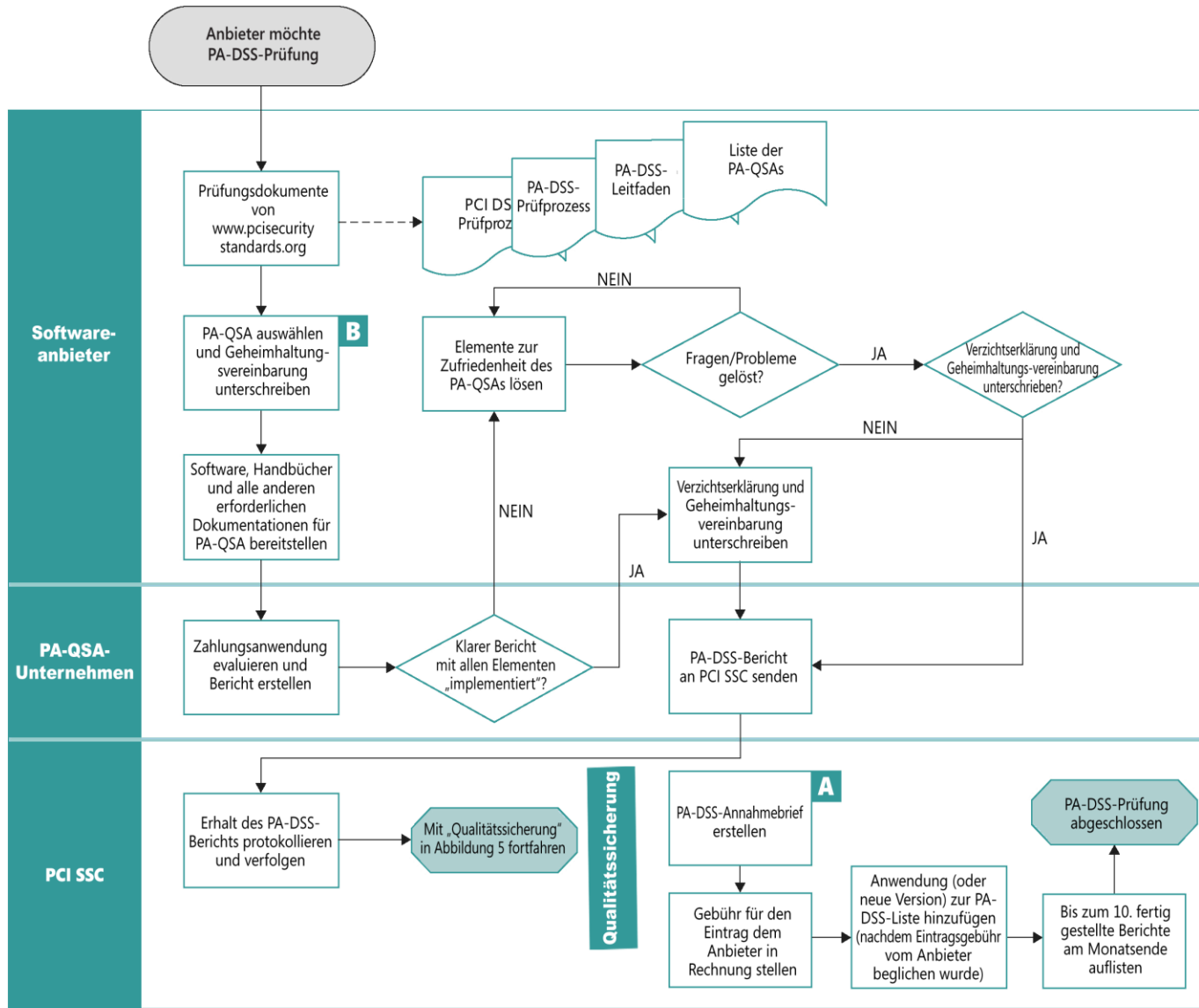


Abbildung 2: PA-DSS – Änderungen an aufgelisteten Anwendungen

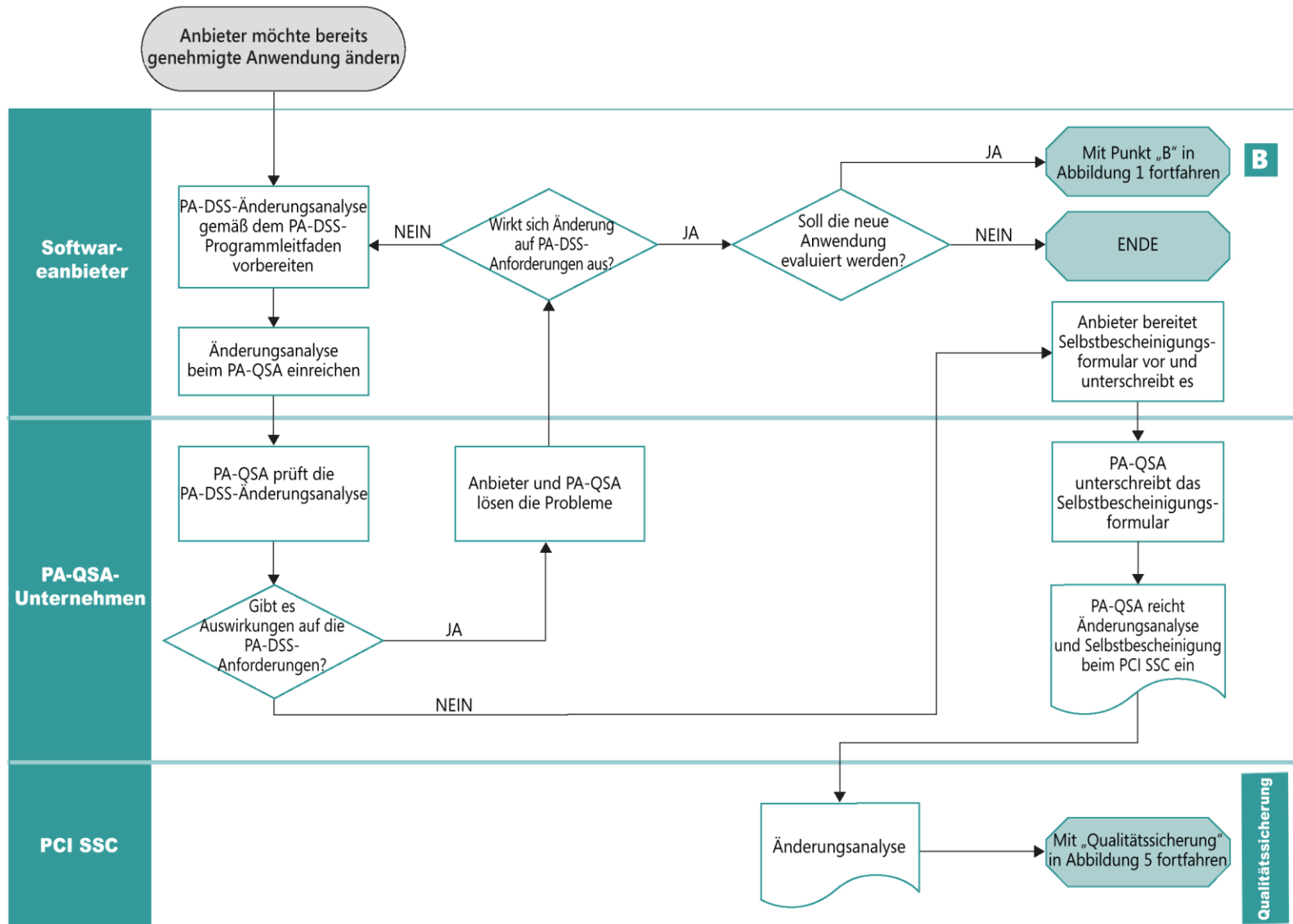


Abbildung 3: Übertragung und Übergang der PABP-Anwendungen zur PA-DSS-Liste

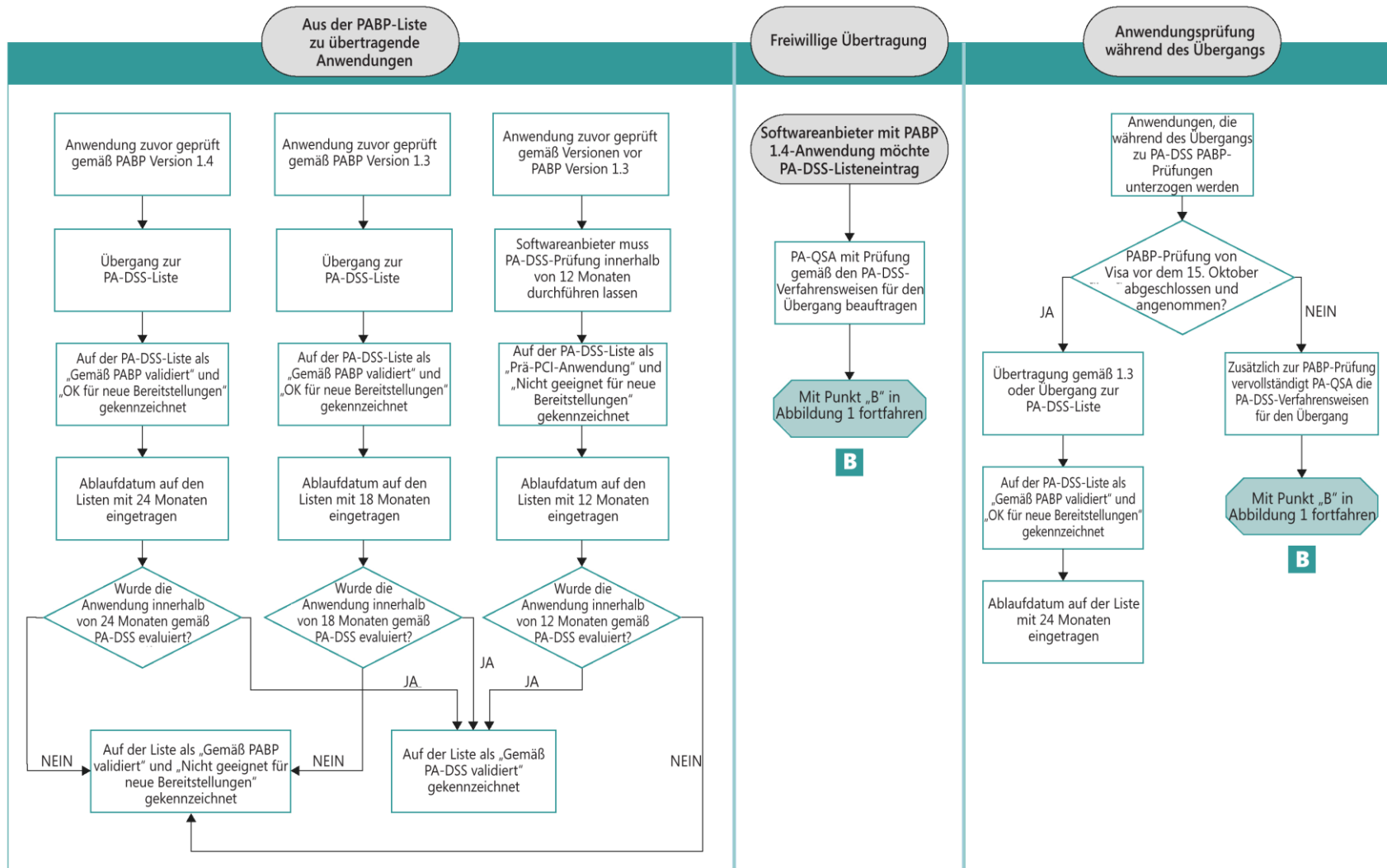


Abbildung 4: PA-DSS – Jährliche Neuvalidierung und Erneuerung abgelaufener Anwendungen

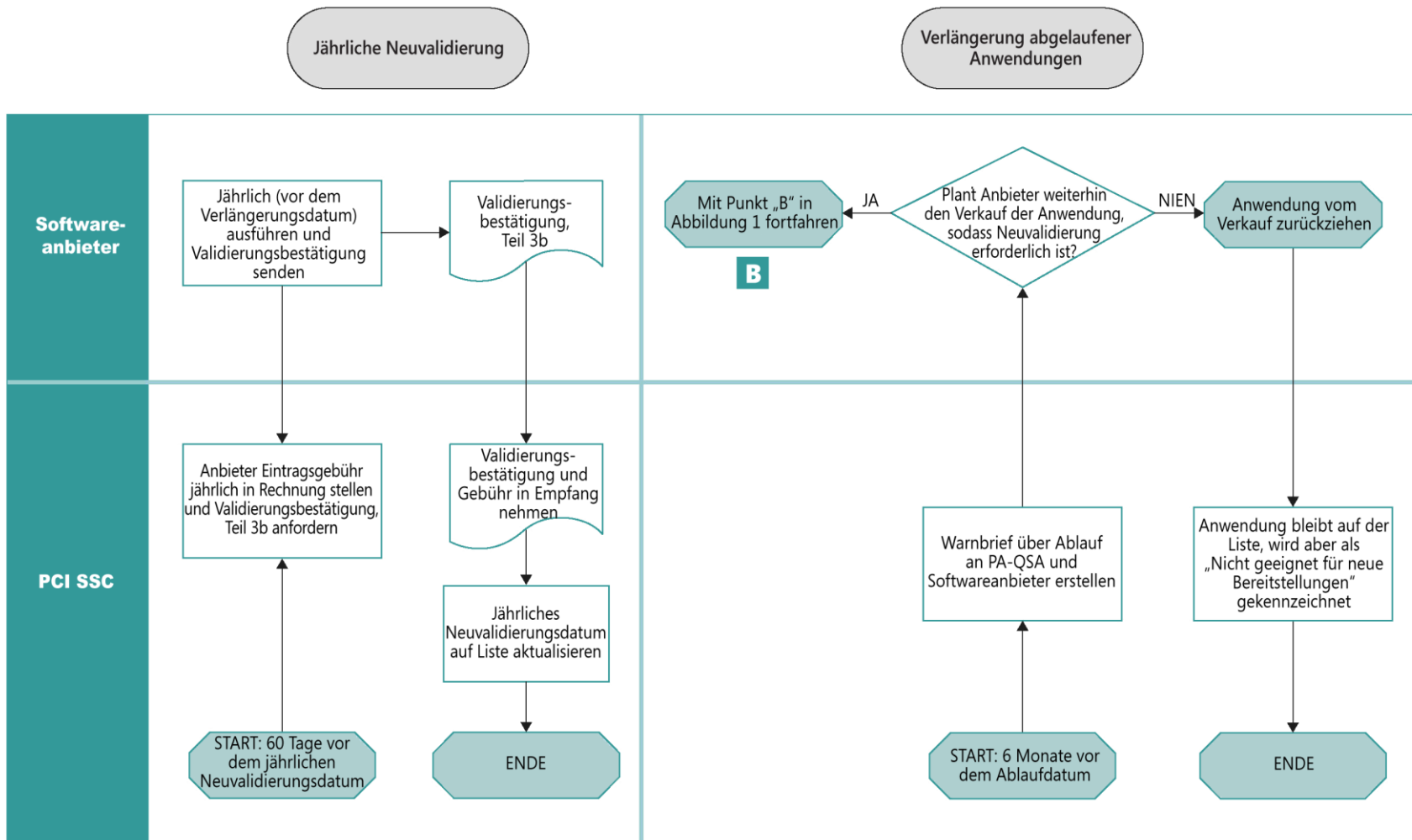
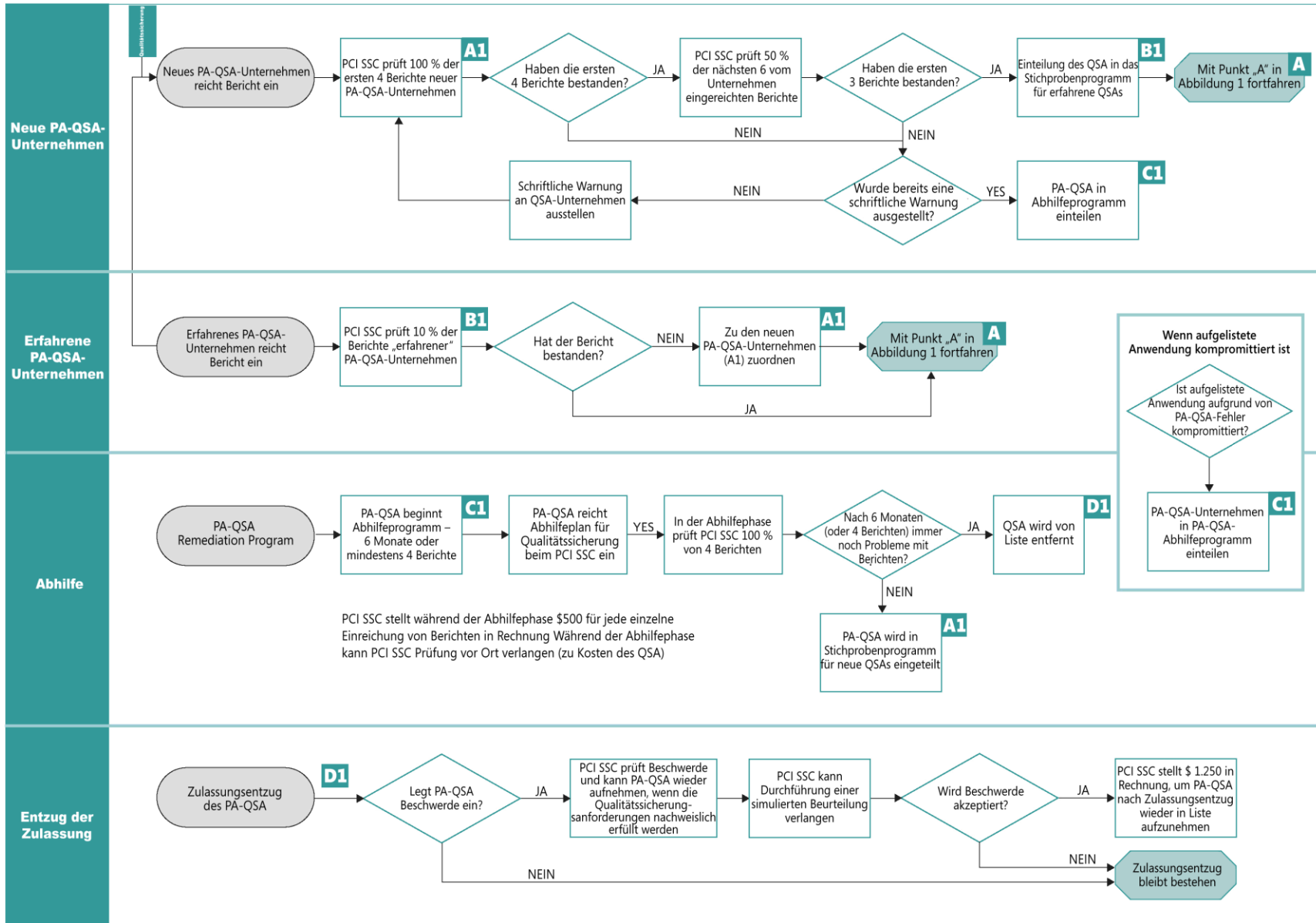


Abbildung 5: PA-QSA-Qualitätssicherungsprogramme für Berichtsprüfungen



PA-DSS-Berichtannahmeprozess – Übersicht

Der PA-QSA führt die Zahlungsanwendungsprüfung gemäß den *PA-DSS-Sicherheitsbeurteilungsverfahren* durch und erstellt einen Bericht, der an den Anbieter weitergegeben wird. Wenn im Bericht für alle Elemente „Implementiert“ angegeben ist, unterschreibt der Anbieter die *Verzichtserklärung*, und der Bericht wird vom PA-QSA an den PCI SSC gesendet. Wenn im Bericht nicht für alle Elemente „Implementiert“ angegeben ist, muss der Anbieter auf die Elemente eingehen, die im Bericht hervorgehoben sind. Das kann z. B. heißen, dass die Benutzerdokumentation oder die Software aktualisiert werden muss. Wenn der Anbieter alle Probleme zur Zufriedenheit des PA-QSA gelöst hat, unterschreibt er die *Verzichtserklärung*, und der Bericht wird vom PA-QSA an den PCI SSC gesendet.

Hinweis: Alle PA-DSS-Berichte und andere Materialien müssen dem PCI SSC in Englisch vorgelegt werden.

Nachdem der PCI SSC den Bericht erhalten hat, prüft er ihn im Hinblick auf die Qualitätssicherung. Wenn der Bericht die Anforderungen an die Qualitätssicherung gemäß den QSA-Validierungsanforderungen und begleitenden Dokumenten erfüllt, sendet der PCI SSC einen PA-DSS-Akzeptationsbrief an den Anbieter und fügt die Anwendung zur Liste des PCI SSC hinzu. Anwendungen werden bis zum Monatsende hinzugefügt, wenn sie bis zum 10. des Monats fertig gestellt wurden. Qualitätsmängel im Zusammenhang mit dem Bericht werden vom PCI SSC und dem PA-QSA besprochen. Der PA-QSA ist dafür verantwortlich, diese Probleme mit dem PCI SSC zu beheben. Die Probleme können sich darauf beschränken, dass der Bericht mit ausreichender Dokumentation aktualisiert werden muss, um die Entscheidungen des PA-QSA zu unterstützen. Wenn es jedoch erforderlich ist, dass der PA-QSA weitere Tests durchführt, muss der PA-QSA den Anbieter darüber informieren und diese Tests mit dem Anbieter koordinieren.

In Abbildung 1 wird der Prozessablauf für die Berichtsannahme detailliert dargestellt.

Änderungen an aufgelisteten Zahlungsanwendungen

Anbieter aktualisieren bereits aufgelistete Zahlungsanwendungen aus verschiedenen Gründen – z. B. um Hilfsfunktionen hinzuzufügen oder um die Basis- oder Kernanwendung zu aktualisieren.

Aus PA-DSS-Perspektive gibt es im Wesentlichen drei Änderungsszenarien:

1. Geringfügige Änderungen an der aufgelisteten Zahlungsanwendung, die keine Auswirkung auf die PA-DSS-Anforderungen haben. In diesem Fall dokumentiert der Softwareanbieter die Änderung für die Prüfung durch den PA-QSA, damit die neue Version aufgelistet werden kann – genauere Einzelheiten finden Sie im Abschnitt *Keine Auswirkung auf PA-DSS-Anforderungen*.
2. Änderungen an der aufgelisteten Zahlungsanwendung, die mögliche Auswirkungen auf die PA-DSS-Anforderungen haben. In diesem Fall reicht der Softwareanbieter die neue Version der Zahlungsanwendung zur vollständigen PA-DSS-Prüfung ein, damit die neue Version aufgelistet werden kann – genauere Einzelheiten finden Sie im Abschnitt *Mögliche Auswirkungen auf PA-DSS-Anforderungen*.
3. Keine Änderungen an der aufgelisteten Zahlungsanwendung. In diesem Fall muss nur ein jährliches Bescheinigungsformular ausgefüllt werden – genauere Einzelheiten finden Sie im Abschnitt *Keine Änderungen an der aufgelisteten Zahlungsanwendung*.

Wenn bereits aufgelistete Anwendungen aktualisiert wurden und der Anbieter möchte, dass die aktualisierten Zahlungsanwendungsinformationen in die Liste aufgenommen werden, muss der Anbieter die Änderungseinzelheiten an den PA-QSA weiterleiten – vorzugsweise an den PA-QSA, der die Zahlungsanwendung bereits geprüft hat.

Der PA-QSA überprüft daraufhin, ob eine erneute Evaluierung der Zahlungsanwendung erforderlich ist. Die Entscheidung kann davon abhängen, ob die an der Anwendung vorgenommenen Änderungen die Sicherheit der Anwendung beeinträchtigen. Der Umfang oder die Reichweite der vorgenommenen Änderungen können weitere Faktoren sein. Zum Beispiel könnte eine Änderung nur Auswirkungen auf die Hilfsfunktionen, aber nicht auf die Kernzahlungsanwendung haben.

Wenn an einer aufgelisteten Zahlungsanwendung Änderungen vorgenommen wurden, die sich möglicherweise auf die PA-DSS-Anforderungen auswirken, und/oder wenn der Anbieter möchte, dass diese Informationen im *PA-DSS-Annahmeprotokoll* und auf der Website überarbeitet werden, muss der Anbieter dem PA-QSA die entsprechende Änderungsdokumentation vorlegen, damit dieser feststellen kann, ob eine vollständige Evaluierung durchgeführt werden muss. Wenn der PA-QSA wie der Anbieter der Meinung ist, dass die dokumentierten Änderungen keine Auswirkung auf die PA-DSS-Anforderungen haben, teilt er dies dem Softwareanbieter mit. Der Softwareanbieter füllt ein Formular zur Selbstbescheinigung der Änderungen aus und unterschreibt es. Der PA-QSA unterschreibt das Formular ebenfalls und leitet es an den PCI SSC weiter. Anschließend beschreibt der PCI SSC die entsprechenden Aktualisierungen im überarbeiteten *PA-DSS-Annahmeprotokoll* und auf der Website. Weitere Informationen finden Sie nachfolgend unter *Keine Auswirkung auf PA-DSS-Anforderungen: Keine PA-DSS-Prüfung erforderlich*.

Hinweis:

Wenn Anbieter von Zahlungsanwendungen die Zahlungsfunktionen auf Module aufteilen, können dadurch erneute Evaluierungen aufgrund von Änderungen, die keine Auswirkung auf die Zahlungsfunktionen und Sicherheit haben, auf ein Minimum reduziert werden.

In Abbildung 2 wird der Prozessablauf für Änderungen an aufgelisteten Anwendungen detailliert dargestellt.

Keine Auswirkung auf PA-DSS-Anforderungen: Keine PA-DSS-Prüfung erforderlich

Wenn eine bereits aufgelistete Zahlungsanwendung überarbeitet wird, aber diese Überarbeitung als geringfügig eingestuft und die Sicherheit nicht beeinträchtigt wird, kann die Änderungsdokumentation („Änderungsanalyse“) dem PA-QSA zur Prüfung vorgelegt werden. Es wird dringend empfohlen, dass der Anbieter denselben PA-QSA auswählt, der auch die ursprüngliche Evaluierung durchgeführt hat.

Die Änderungsanalyse, die der Softwareanbieter dem PA-QSA vorlegt, sollte mindestens die folgenden Informationen enthalten:

- Name der Zahlungsanwendung
- Versionsnummer der Zahlungsanwendung
- Name und Versionsnummer zugehöriger Zahlungsanwendungen, die sich bereits in der Liste des PCI SSC befinden
- Beschreibung der Änderung
- Erklärung, warum die Änderung erforderlich ist
- Informationen darüber, ob Auswirkungen auf die Karteninhaberdaten und Zahlungsfunktionen vorhanden sind, und ggf. Beschreibung der Auswirkungen
- Beschreibung der Funktionsweise der Änderung
- Beschreibung der Tests, die der Anbieter durchgeführt hat, um zu validieren, dass die PA-DSS-Sicherheitsanforderungen nicht beeinträchtigt werden
- Erklärung der Gründe, warum PA-DSS-Anforderungen nicht beeinträchtigt werden
- Beschreibung der Änderung unter Verweis auf die Versionierungsmethoden des Anbieters und Erklärung, wie anhand dieser Versionsnummer ersichtlich ist, dass es sich nur um eine „geringfügige“ Änderung handelt
- Gegebenenfalls Beschreibung der Verwendung von Programmierverfahren/Modulansätzen und wie diese Verwendung negative Auswirkungen auf die Anforderungen verhindert

Wenn der PA-QSA zustimmt, dass die Änderung, wie in der Änderungsanalyse des Anbieters dokumentiert, keine negative Auswirkung auf die Sicherheit der Zahlungsanwendung hat, (i) informiert der PA-QSA den Softwareanbieter darüber, (ii) der Softwareanbieter füllt ein Formular zur Selbstbescheinigung der Änderungen aus, unterschreibt es und sendet es an den PA-QSA; daraufhin (iii) bestätigt der PA-QSA durch Unterschrift seine Zustimmung und leitet es zusammen mit der Änderungsanalyse an den PCI SSC weiter, und (iv) der PCI SSC überprüft das Formular und die Dokumentation aus Qualitätssicherungsgründen.

Wenn keine Auswirkungen auf die PA-DSS-Anforderungen vorhanden sind:

- Für den Anbieter wird ein überarbeiteter PA-DSS-Akzeptanzbrief ausgestellt.
- Die Liste der PA-DSS-validierten Zahlungsanwendungen wird auf der Website mit den neuen Informationen aktualisiert.
- Das Ablaufdatum dieser neu aufgelisteten Anwendung und die Versionsnummer sind dieselben wie bei der übergeordneten Zahlungsanwendung.

Qualitätsmängel in Zusammenhang mit der Selbstbescheinigung der Änderungen werden vom PCI SSC an den PA-QSA weitergeleitet. Diese Probleme werden gemäß dem weiter oben beschriebenen Prozess gelöst.

Mögliche Auswirkungen auf PA-DSS-Anforderungen: Neue PA-DSS-Prüfung erforderlich

Wenn die Änderungen an der Zahlungsanwendung eine Auswirkung auf die PA-DSS-Anforderungen haben, muss die Zahlungsanwendung einer weiteren PA-DSS-Beurteilung unterzogen werden. Der PA-QSA legt dem PCI SSC einen neuen PA-DSS-Bericht zur Genehmigung vor. In einer solchen Situation kann der Anbieter die Änderungsdokumentation zuerst dem PA-QSA vorlegen, der feststellt, ob die Art der Änderung unter Berücksichtigung der aktuellen PA-DSS-Anforderungen Auswirkungen auf die Sicherheit der Zahlungsanwendung hat.

Keine Änderungen an der aufgelisteten Zahlungsanwendung: Jährliche Neuvalidierung erforderlich

Der Softwareanbieter muss jedes Jahr bis zum in der Liste angegebenen Neuvalidierungsdatum ein Validierungsbestätigungsformular einreichen, in dem Abschnitt 3b ausgefüllt ist. Das Validierungsbestätigungsformular befindet sich im PA-DSS-Anhang C.

In Abbildung 4 wird der Prozessablauf für die jährliche Neuvalidierung detailliert dargestellt.

Verlängerung abgelaufener Anwendungen

Wenn sich eine Anwendung ihrem Ablaufdatum nähert, informiert der PCI SSC den Softwareanbieter über den bevorstehenden Ablauf. Es gibt zwei Optionen, die der Anbieter berücksichtigen muss:

1. Der Anbieter möchte die Anwendung weiterhin verkaufen. In diesem Fall beauftragt der Anbieter einen PA-QSA damit, die Zahlungsanwendung neu zu bewerten.
2. Der Anbieter möchte die Anwendung nicht mehr verkaufen. In diesem Fall ändert der PCI SSC nach dem Ablaufdatum den Status der aufgelisteten Zahlungsanwendung in „Not acceptable for new deployments“.

Hinweis: Wenn der Anbieter sich entscheidet, die Anwendung weiterhin zu verkaufen, wird der Status „acceptable for new deployments“ in der Liste des PCI SSC beibehalten, und es wird ein neues Ablaufdatum zugewiesen, sobald die Anwendung erneut das PA-DSS-Beurteilungsverfahren erfolgreich durchlaufen hat.

In Abbildung 4 wird der Prozessablauf für die Verlängerung abgelaufener Anwendungen detailliert dargestellt.

Übergang und Übertragung von PABP-validierten Zahlungsanwendungen

Übertragung von PABP-Anwendungen zur PABP-Liste bis zum 15. Oktober 2008

Der PCI SSC überträgt vorhandene PABP-konforme Anwendungen zur PCI SSC-Liste. Diese Übertragung ermöglicht es, Anwendungen, die früher evaluiert und als PABP-konform eingestuft wurden, so lange einzusetzen, bis neuere, PA-DSS-konforme Zahlungsanwendungen verfügbar werden.

Die Ablaufdaten der PABP-Anwendungen unterliegen verschiedenen Phasen. Dieser Ansatz basiert auf der Version der Anforderungen, die zur Beurteilung der Anwendung verwendet wurde. Die PABP-konformen Anwendungen müssen innerhalb von vorgeschriebenen Zeitrahmen einer PA-DSS-Beurteilung unterzogen werden, um in der PCI SSC-Liste als „geeignet für neue Bereitstellungen“ aufgeführt zu bleiben. Wenn die PABP-konforme Anwendung nicht innerhalb der vorgeschriebenen Zeitrahmen einer PA-DSS-Beurteilung unterzogen wird, bleibt die Anwendung zwar in der PCI SSC-Liste, wird aber als „nicht geeignet für neue Bereitstellungen“ gekennzeichnet.

Hinweis:

In der PCI SSC-Liste wird zwischen „neuen Bereitstellungen“ und „vorhandenen Bereitstellungen“ unterschieden.

Zahlungsanwendungen weisen häufig eine lange Lebensdauer auf, nachdem sie bereitgestellt wurden – möglicherweise bis zu 10 – 15 Jahre. Der PCI SSC ist sich bewusst, dass die Bereitstellung einer Zahlungsanwendung ein komplexer und kostspieliger Vorgang sein kann und dass es häufig unrentabel für Händler und Käufer ist, ihre Zahlungsanwendungen alle paar Jahre zu aktualisieren.

Im folgenden Diagramm werden die jeweiligen Ablaufdaten und Hinweise angezeigt, die in der *Liste PA-DSS-validierter Zahlungsanwendungen* für die PABP-Versionen und für die PA-DSS-Prüfungen gemäß den aktuellen PA-DSS v1.1-Anforderungen enthalten sind.

Version	Ablaufdatum	Eintrag in der PCI SSC-Liste vor dem Ablauf		Eintrag in der PCI SSC-Liste nach dem Ablauf	
		Validierungshinweise	Bereitstellungshinweise	Validierungshinweise	Bereitstellungshinweise
PABP 1.4	24 Monate	Gemäß PABP validiert	Geeignet für neue Bereitstellungen	Gemäß PABP validiert	Nicht geeignet für neue Bereitstellungen
PABP 1.3	18 Monate	Gemäß PABP validiert	Geeignet für neue Bereitstellungen	Gemäß PABP validiert	Nicht geeignet für neue Bereitstellungen
Vor PABP 1.3	12 Monate	Prä-PCI-Anwendung	Nicht empfohlen für neue Bereitstellungen	Prä-PCI-Anwendung	Nicht geeignet für neue Bereitstellungen
PA-DSS 1.1	3 Jahre nach Änderung des Standards	Gemäß PA-DSS validiert	Geeignet für neue Bereitstellungen	Gemäß PA-DSS validiert	Nicht geeignet für neue Bereitstellungen

In Abbildung 3 wird der Prozessablauf für die Übertragung und den Übergang der PABP-Anwendungen detailliert dargestellt.

PABP-Prüfungen für Zahlungsanwendungen während des Übergangs

Nach der Veröffentlichung von Version 1.1 des PA-DSS begann eine Frist von ungefähr sechs Monaten, die es den PA-QSAs ermöglicht, sich mit dem neuen Standard vertraut zu machen, an Schulungen teilzunehmen und sich für die Durchführung von PA-DSS-Prüfungen zu qualifizieren. Während dieses Zeitrahmens können sich auch die Anbieter mit dem PA-DSS vertraut machen und die neuen PA-DSS-Anforderungen bei der Entwicklung ihrer neuen Zahlungsanwendungen berücksichtigen.

Während dieser Frist können Zahlungsanwendungen weiterhin gemäß PABP Version 1.4 evaluiert werden. Diese Frist läuft bis zum **15. Oktober 2008**. Berichte, die nach diesem Datum eingereicht werden, werden nicht für eine PABP-Konformitätsbeurteilung akzeptiert.¹

Berichte, die auf PABP Version 1.4 basieren und nach dem 15. Oktober 2008 eingereicht wurden, unterliegen den *PA-DSS-Verfahrensweisen für den Übergang*. Der PA-QSA kann die Ergebnisse des PABP-Berichts verwenden. Die Ergebnisse, die beim PCI SSC eingereicht werden, müssen aber auch eine Evaluierung der Veränderungen gemäß den *PA-DSS-Verfahrensweisen für den Übergang* enthalten.

Nachdem der neue Standard veröffentlicht wurde, kann der Anbieter die Zahlungsanwendung jederzeit einer PA-DSS-Beurteilung unterziehen.

PA-DSS-Verfahrensweisen für den Übergang

Die PA-DSS-Verfahrensweisen für den Übergang werden ggf. von den PA-QSAs (Payment Application Qualified Security Assessors) verwendet, um eine Anwendung aus der Liste PABP-validierter Zahlungsanwendungen von Visa² zur Liste PA-DSS-validierter Zahlungsanwendungen des PCI SSC zu übertragen³.

Hinweis: Der PCI SSC überträgt Zahlungsanwendungen, die gemäß den PABP-Versionen 1.3 und 1.4 validiert wurden, zur Liste der PA-DSS-validierten Anwendungen über einen Zeitraum von 18 bzw. 24 Monaten, bevor eine PA-DSS-Prüfung erforderlich wird.

Diese Übergangsverfahren sind für die folgenden Szenarien verfügbar:

Vorgeschriebener Abschluss der Übergangsverfahren: Wenn eine Zahlungsanwendung einer PABP-Prüfung unterzogen wird, die nicht bis zum 15. Oktober 2008 abgeschlossen ist und von VISA angenommen wird, **müssen** diese Übergangsverfahren abgeschlossen werden, damit der PCI SSC diese Anwendungen als gemäß PA-DSS validiert anerkennt. **Hinweis: Prüfungen, die nur gemäß PABP durchgeführt wurden, werden nach dem 15. Oktober 2008 nicht mehr angenommen.**

Hinweis:

Zur Durchführung der PA-DSS-Verfahrensweisen für den Übergang sollte dasselbe PA-QSA-Unternehmen beauftragt werden, das die PABP-Prüfung durchgeführt hat.

Freiwilliger Abschluss der Übergangsverfahren: Wie im oben stehenden *Hinweis* beschrieben, müssen diese Übergangsverfahren verwendet werden, wenn ein Zahlungsanwendungsanbieter über Anwendungen verfügt, die zur Übertragung berechtigt sind, die gemäß PABP Version 1.3 oder 1.4 validierten Anwendungen stattdessen jedoch als „Gemäß PA-DSS validiert“ aufgelistet werden sollen. Ein PA-QSA führt die Verfahren durch und leitet den Bericht gemäß dem PA-DSS-Programmleitfaden weiter, damit der PCI SSC die gemäß PABP Version 1.3 und 1.4 evaluierten Anwendungen als validiert anerkennt.

Weitere Informationen über die PA-DSS-Verfahrensweisen für den Übergang finden Sie auf der Website unter *PABP to PA-DSS Transition Procedures*.

¹ Wenn eine Zahlungsanwendung gemäß PABP Version 1.4 evaluiert und vor dem 15. Oktober 2008 eingereicht wird und der Bericht Qualitätsmängel aufzeigt, wird eine Ausnahme gemacht. Die Prüfung gemäß PABP Version 1.4 kann für diese Anwendung fortgesetzt werden, bis die Qualitätsmängel behoben sind. Ausnahmen dieser Art sind bis zum 15. April 2009 zulässig.

² Geprüft gemäß Payment Application Best Practices (PABP), Versionen 1.3 oder 1.4

³ Geprüft gemäß dem Datensicherheitsstandard für Zahlungsanwendungen (Payment Application Data Security Standard, PA-DSS), Version 1.1

Qualitätssicherungsprogramm

Der PCI SSC prüft Berichte vom PA-QSA aus Gründen der Qualitätssicherung. Wie in den *QSA-Validierungsanforderungen* und im *PA-QSA Agreement* angegeben ist, müssen PA-QSAs Qualitätssicherungsstandards einhalten, die vom PCI SSC vorgegeben werden. Die verschiedenen Phasen des Qualitätssicherungsprogramms werden weiter unten beschrieben.

In Abbildung 5 wird der Prozessablauf für das Qualitätssicherungsprogramm detailliert dargestellt.

Stichprobenprogramm für neue PA-QSAs

Der PCI SSC verwendet einen gestaffelten Stichprobenprozess, um die ROVs der PA-QSAs zu prüfen. In der Anfangsphase werden mehr Berichte geprüft, und wenn sich zeigt, dass der PA-QSA sorgfältig arbeitet, wird die Häufigkeit der Stichproben reduziert. Wenn der PA-QSA kontinuierlich die Qualitätsstandards einhält, wird er in das Stichprobenprogramm für erfahrene QSAs (mit einer noch geringeren Häufigkeit von Stichproben) eingeteilt. Solange der PA-QSA die Qualitätsstandards einhält, unterliegt er eingeschränkten Stichprobenprüfungen.

Wenn der PA-QSA die Qualitätsstandards jedoch nicht erfüllt, werden die folgenden Maßnahmen ergriffen:

- **Warnbrief:** Der PA-QSA erhält eine erste Benachrichtigung, dass er die Qualität steigern muss.
- **Abhilfe:** Wenn die Qualitätsstandards weiterhin nicht erfüllt werden, wird der PA-QSA in ein Abhilfeprogramm eingeteilt, und es können Strafmaßnahmen verordnet werden.
- **Entzug der Zulassung:** Wenn die Qualitätsstandards immer noch nicht erfüllt werden, wird dem PA-QSA die Zulassung entzogen, und er wird aus der PCI SSC-Liste der genehmigten PA-QSAs entfernt.

Stichprobenprogramm für erfahrene PA-QSAs

Wenn ein PA-QSA in das Stichprobenprogramm für erfahrene PA-QSAs eingeteilt wird, werden seine Berichte nur eingeschränkten Stichprobenprüfungen unterzogen. Wenn die Qualitätsstandards kontinuierlich eingehalten werden, werden Stichprobenprüfungen auch weiterhin nur eingeschränkt durchgeführt. Dieses Programm ist als „stabiler Zustand“ beabsichtigt, in dem die PA-QSAs ihre Arbeit erledigen.

Wenn Qualitätsmängel auftreten und Standards nicht eingehalten werden, wird der PA-QSA wieder in das Stichprobenprogramm für neue PA-QSAs eingeteilt.

Abhilfe

In dieser Phase dürfen PA-QSAs immer noch Prüfungen durchführen, aber alle Berichte werden vom PCI SSC aus Gründen der Qualitätssicherung geprüft. PCI SSC berechnet für jeden Bericht, der während der Abhilfephase mehrmals eingereicht wird, \$ 500.

Der PA-QSA muss dem PCI SSC außerdem einen Abhilfeplan vorlegen, der beschreibt, wie der PA-QSA die Qualität seiner Berichte verbessern möchte. Der PCI SSC kann auch verlangen, dass das Qualitätssicherungsprogramm des PA-QSA vor Ort geprüft wird. Die Kosten für den Besuch muss der PA-QSA übernehmen.

Wenn der PA-QSA während der Abhilfephase die Qualitätsstandards erfüllt, wird er wieder in das Stichprobenprogramm für neue PA-QSAs eingeteilt. Wenn der PA-QSA die Qualitätsstandards während der Abhilfephase nicht erfüllt, tritt für ihn die nächste Phase ein: Entzug der Zulassung.

Hinweis: Wenn eine Zahlungsanwendung, die in der *Liste PA-DSS-validierter Zahlungsanwendungen* des PCI SSC enthalten ist, aufgrund eines Fehlers des PA-QSA kompromittiert wird, wird dieser PA-QSA sofort in das Abhilfeprogramm eingeteilt. Der PA-QSA wird erst wieder in das Stichprobenprogramm für neue PA-QSAs eingeordnet, wenn er die Qualitätsstandards erfüllt.

Entzug der Zulassung

Wenn die Zulassung eines PA-QSA entzogen wird, wird dieser aus der PCI SSC-Liste der genehmigten PA-QSAs entfernt. Wenn einem PA-QSA die Zulassung entzogen wurde, kann er keine Zahlungen mehr prüfen. Der PA-QSA kann gegen den Entzug der Zulassung Beschwerde einlegen, aber er muss die Anforderungen gemäß den QSA-Validierungsanforderungen und begleitenden Dokumenten erfüllen. Der PCI SSC behält sich das Recht vor, die Durchführung einer simulierten Beurteilung zu verlangen.

Bevor der PA-QSA wieder in das Stichprobenprogramm für neue PA-QSAs aufgenommen wird, wird eine Gebühr von 1.250 USD für die erneute Eintragung berechnet.

PA-DSS-Berichterstellungsverfahren

Der PCI SSC legt für die Annahme eines Berichts ausschließlich die Ergebnisse zugrunde, die im ROV dokumentiert sind. Schritte nach dem Erhalt des Berichts:

- Der PCI SSC prüft den Bericht (im Allgemeinen innerhalb von 30 Kalendertagen nach Eingang) und stellt fest, ob er akzeptabel ist.
- Wenn keine Probleme oder Fragen an den PA-QSA identifiziert werden, stellt der PCI SSC dem Softwareanbieter die Gebühr für den Eintrag in Rechnung. Nach Erhalt der Gebühr stellt der PCI SSC einen PA-DSS-Annahmefrief aus und veröffentlicht die Zahlungsanwendung und die Anbieterinformationen auf der Website.
- Wenn Fragen oder Probleme identifiziert und an den PA-QSA weitergeleitet werden, beginnt der weiter oben beschriebene Prozess erneut, nachdem ein vollständiger und akzeptabler überarbeiteter Bericht oder eine Antwort („Überarbeiteter Bericht“) vom PA-QSA eingegangen ist. Der Prozess beginnt erst dann erneut, wenn ein akzeptabler überarbeiteter Bericht eingegangen ist, der auf alle zuvor identifizierten Elemente eingeht, die noch offen sind. Der PCI SSC prüft einen überarbeiteten Bericht i. d. R. innerhalb von 14 Kalendertagen nach Eingang.
- Wenn zusätzliche Fragen oder Probleme auftreten, werden die entsprechenden Schritte so lange wiederholt, bis die Antwort zufriedenstellend ist. Zu diesem Zeitpunkt stellt der PCI SSC den PA-DSS-Annahmefrief aus und veröffentlicht die Informationen auf der Website. Die zusätzlichen Probleme oder Fragen können jederzeit zur Sprache gebracht werden, solange noch kein **PA-DSS-Annahmefrief** ausgestellt ist.

Für Berichte, die sich auf Änderungen an bereits aufgelisteten Anwendungsversionen beziehen und auf der Selbstbescheinigung der Änderungen basieren, gilt dasselbe Annahmeverfahren für PA-DSS-Berichte wie oben beschrieben. Wenn keine Probleme oder Fragen auftreten, stellt der PCI SSC einen überarbeiteten PA-DSS-Annahmefrief aus und veröffentlicht die überarbeiteten Informationen auf der Website – in ähnlicher Weise wie zuvor beschrieben.

Der PCI SSC-Annahmefrief und der Eintrag auf der Website enthalten zumindest die nachfolgenden Informationen. Jedes Merkmal wird detailliert in „Anhang A: Anwendungselemente für die Liste PA-DSS-validierter Zahlungsanwendungen“ beschrieben.

- Anbieter der Zahlungsanwendung
- Identifikator der Zahlungsanwendung
- Genehmigungsnummer
- Validierungshinweise
- Bereitstellungshinweise
- Selbstbescheinigung über kleine Versionsänderungen, falls zutreffend
- Datum der jährlichen Neuvalidierung
- Ablaufdatum
- PA-QSA-Unternehmen
- Typ der Zahlungsanwendung
- Gegebenenfalls Zielmarkt der Zahlungsanwendung
- Gegebenenfalls eine bestimmte Region oder Ländereinstellung für die Zahlungsanwendung

Hinweis:

Der PCI SSC erteilt keine „Teilgenehmigungen“, wenn eine Zahlungsanwendung einige – aber nicht alle – Anforderungen erfüllt.

Benachrichtigung nach einer Sicherheitsverletzung oder Sicherheitsgefährdung

Die Anbieter müssen gemäß den in diesem Abschnitt beschriebenen Verfahren den PCI SSC über jede Sicherheitsverletzung oder -gefährdung informieren, die in Zusammenhang mit einer aufgelisteten Zahlungsanwendung auftritt.

Benachrichtigung und zeitlicher Ablauf

Unbeschadet anderer rechtlicher Verpflichtungen des Anbieters muss dieser den PCI SSC sofort informieren, wenn eine Sicherheitsverletzung oder -gefährdung in Zusammenhang mit einer Zahlungsanwendung von ihm auftritt, die in der Liste des PCI SSC aufgeführt ist.

Der Anbieter muss außerdem umgehend Feedback zu den (möglichen oder tatsächlichen) Auswirkungen geben, die aufgrund der Verletzung aufgetreten sind, auftreten können oder auftreten werden.

Hinweis:

Der Anbieter muss den PCI SSC spätestens 24 Stunden nach Entdeckung der Sicherheitsverletzung oder -gefährdung benachrichtigen.

Benachrichtigungsformat

Der Anbieter muss den PA-DSS-Koordinator des PCI SSC zunächst telefonisch über die Sicherheitsverletzung oder -gefährdung benachrichtigen. Anschließend müssen die gesamten Einzelheiten der Sicherheitsverletzung oder -gefährdung in einer E-Mail, einem Fax oder Brief ausführlich beschrieben werden.

Benachrichtigungseinzelheiten

Nach der Benachrichtigung über die Sicherheitsverletzung oder -gefährdung muss der Anbieter dem PA-DSS-Koordinator des PCI SSC alle relevanten Informationen in Zusammenhang mit der Sicherheitsverletzung oder -gefährdung bereitstellen. Dazu gehören u. a. die folgenden Informationen:

- Die Anzahl der gefährdeten Konten (wenn bekannt)
- Alle Berichte mit Einzelheiten über die Sicherheitsverletzung oder -gefährdung
- Alle Berichte oder Evaluierungen, die zur Untersuchung der Sicherheitsverletzung oder -gefährdung erstellt wurden

Wie in der Verzichtserklärung vereinbart, darf der PCI SSC diese und andere Informationen weitergeben, die eine Evaluierung der Sicherheitsverletzung oder -gefährdung unterstützen bzw. ermöglichen, um zukünftige Sicherheitsverletzungen oder -gefährdungen zu verhindern oder die Auswirkungen zu mindern.

Maßnahmen nach einer Sicherheitsverletzung oder -gefährdung

Wenn der PCI SSC über eine Sicherheitsschwäche oder tatsächliche Gefährdung in Zusammenhang mit einem bestimmten Produkt oder einer Gruppe von Produkten, das/die in der *Liste PA-DSS-validierter Zahlungsanwendungen* aufgeführt ist bzw. aufgeführt sind, informiert wird, kann er die folgenden Maßnahmen ergreifen:

- Benachrichtigung aller Zahlungsmarken, dass eine Sicherheitsschwäche oder -gefährdung aufgetreten ist
- Versuch, Einblick in den forensischen Bericht zu erhalten, um genau festzustellen, wie die Gefährdung entstanden ist
- Kontaktaufnahme mit dem Anbieter, um diesen darüber zu informieren, dass sein Produkt eine Sicherheitsschwäche aufweist oder kompromittiert wurde, und um Informationen über die tatsächliche Schwäche oder Gefährdung an den Anbieter weiterzugeben

- Unterstützung des Anbieters beim Versuch, zukünftige Gefährdungen zu verhindern oder die Auswirkungen zu mindern
- Unterstützung des Anbieters 1) beim Beheben der Sicherheitsschwächen und 2) bei der Erstellung eines Leitfadens, der die Kunden des Anbieters über mögliche Schwachstellen informiert und beschreibt, welche Maßnahmen zu ergreifen sind, um zukünftige Sicherheitsverletzungen oder -gefährdungen zu verhindern oder die Auswirkungen zu mindern
- Zusammenarbeit mit den entsprechenden Untersuchungsbehörden, um zukünftige Gefährdungen zu verhindern oder die Auswirkungen zu mindern
- Unterstützung und/oder Ermöglichung der Evaluierungen des gefährdeten Produkts – entweder intern oder im Rahmen der Verzichtserklärung – und Einsatz der PA-QSAs, um die Ursache der Gefährdung zu identifizieren

Rücknahme der Annahme

Der PCI SSC behält sich das Recht vor, die Annahme einer Zahlungsanwendung zurückzuziehen und die Zahlungsanwendung aus der *Liste PA-DSS-validierter Zahlungsanwendungen* zu entfernen, wenn es offensichtlich ist, dass die Zahlungsanwendung keinen ausreichenden Schutz gegen aktuelle Bedrohungen bietet und/oder die PA-DSS-Anforderungen nicht erfüllt. Wenn der PCI SSC feststellt, dass eine Zahlungsanwendung eine Sicherheitsschwäche aufweist oder gefährdet ist, benachrichtigt der PCI SSC den Anbieter schriftlich darüber, dass er beabsichtigt, die Annahme der Zahlungsanwendung zurückzuziehen.

Rechtliche Bestimmungen

Die Annahme durch den PCI SSC gilt nur für die Zahlungsanwendungen/-versionen, die mit der vom PA-QSA geprüften Zahlungsanwendung identisch sind. Wenn sich ein Aspekt der Zahlungsanwendung von der vom PA-QSA getesteten Anwendung unterscheidet – auch wenn die Zahlungsanwendung der grundlegenden Produktbeschreibung im Annahmefried entspricht –, sollte die Zahlungsanwendung nicht als vom PCI SSC angenommen betrachtet werden, und es sollte nicht damit geworben werden, dass die Anwendung vom PCI SSC angenommen wurde. Beispiel: Wenn eine Zahlungsanwendung denselben Namen oder dieselbe Versionsnummer aufweist wie die vom PA-QSA getestete Anwendung, aber nicht mit der Zahlungsanwendung identisch ist, die vom PA-QSA getestet wurde, dann sollte die Zahlungsanwendung nicht als angenommen betrachtet oder beworben werden.

Es ist Anbietern oder anderen Dritten nicht gestattet, eine Zahlungsanwendung als „PCI-genehmigt“ oder „PCI SSC-genehmigt“ zu bezeichnen oder anzugeben bzw. zu implizieren, dass der PCI SSC einen Aspekt des Anbieters oder seiner Zahlungsanwendung im Ganzen oder teilweise genehmigt hat, außer in dem Umfang und unter Einhaltung der Bestimmungen und Beschränkungen, die in einer schriftlichen Vereinbarung mit dem PCI SSC oder in einem PA-DSS-Annahmefried ausdrücklich festgelegt sind. Alle anderen Verweise auf die Annahme durch den PCI SSC sind durch den PCI SSC streng verboten.

Bei Genehmigung erteilt der PCI SSC eine Bestätigung der Annahme, um bestimmte sicherheitsbezogene und betriebliche Merkmale, die zur Erreichung der Ziele des PCI SSC wichtig sind, zu sichern, aber die Bestätigung stellt unter keinen Umständen eine Befürwortung oder Gewährleistung in Bezug auf die Funktionalität, Qualität oder Leistung eines bestimmten Produkts oder Dienstes dar. Der PCI SSC übernimmt keine Gewährleistungen für Produkte oder Dienste von Dritten. Die Annahme umfasst oder impliziert unter keinen Umständen Produktgewährleistungen des PCI SSC, einschließlich u. a. der stillschweigenden Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck und der Nichtverletzung von Rechten Dritter, die alle vom PCI ausdrücklich ausgeschlossen werden. Alle Rechte und Rechtsmittel in Bezug auf die Produkte und Dienste, die angenommen wurden, werden vom Anbieter dieser Produkte oder Dienste gewährt, nicht vom PCI SSC oder den Zahlungsmarken.

Vorbehaltlich anderslautender schriftlicher Verpflichtungen des PCI SSC werden alle Objekte und Dienste, die in diesem vom PCI SSC für Dritte erstellten Dokument einer eingehenden Betrachtung unterzogen werden, ohne Mängelgewähr, „mit allen Fehlern“ und ohne Gewährleistung jeglicher Art zur Verfügung gestellt.

Anhang A: Elemente für den Annahmepflicht und die Liste PA-DSS-validierter Zahlungsanwendungen

Anbieter der Zahlungsanwendung

Dieser Eintrag beschreibt den **Zahlungsanwendungsanbieter** für die validierte Zahlungsanwendung.

Identifikator der Zahlungsanwendung

Der **Identifikator der Zahlungsanwendung** wird vom PCI SSC für die Beschreibung der relevanten Informationen verwendet, die für eine validierte Zahlungsanwendung maßgeblich sind. Er besteht aus:

- Name der Zahlungsanwendung
- Versionsnummer der Zahlungsanwendung

Um sicherzustellen, dass eine validierte Zahlungsanwendung verwendet wird, wird Käufern bzw. ihren jeweiligen Beauftragten dringend empfohlen, nur solche Zahlungsanwendungen zu erwerben und bereitzustellen, deren Informationen genau mit den Informationen des Identifikators der Zahlungsanwendung übereinstimmen. Beispiel für einen **Identifikator einer Zahlungsanwendung** (zwei Komponenten):

Komponente	Beschreibung
Name der Anwendung	Acme Payment 600
Versionsnummer der Anwendung	PCI 4.53

Versionsnummer der Anwendung

Die **Versionsnummer der Anwendung** stellt die spezifische Anwendungsversion dar, die während der PA-DSS-Bewertung geprüft wurde. Die Felder, die die Versionsnummer der Anwendung ergeben, können aus einer Kombination aus festen und variablen alphanumerischen Zeichen bestehen.

Hinweis:

Im PA-DSS finden Sie im Abschnitt „Anweisungen und Inhalt des Validierungsberichts“ ausführliche Informationen über den Inhalt, der im PA-DSS-ROV für die Versionierungsmethoden des Anbieters aufgenommen werden soll.

Kunden wird dringend empfohlen, Zahlungsanwendungen nur dann zu erwerben und bereitzustellen, wenn die alphanumerischen Zeichen der Anwendungsversionsnummer genau mit der Anwendungsversionsnummer übereinstimmen, die auf der Liste PA-DSS-validierter Zahlungsanwendungen oder im PA-DSS-Annahmepflicht vom PCI SSC aufgeführt ist.

Annahmepflicht

Der PCI SSC ordnet zum Zeitpunkt der Annahme eine **Annahmepflicht** zu. Diese Nummer bleibt dieselbe, solange die Anwendung in der Liste eingetragen ist.

Validierungshinweise

Validierungshinweise werden vom PCI SSC verwendet, um anzugeben, ob die Prüfung gemäß dem PABP-Programm von Visa oder gemäß dem PA-DSS-Programm vom PCI SSC durchgeführt wurde, und um die zutreffende PABP- oder PA-DSS-Version anzuzeigen. Beispiele dazu finden Sie in der Tabelle unter „Bereitstellungshinweise“.

Bereitstellungshinweise

Bereitstellungshinweise werden vom PCI SSC verwendet, um anzugeben, ob eine Zahlungsanwendung für neue Bereitstellungen akzeptabel oder nicht akzeptabel ist. Diese Hinweise beziehen sich auf das Ablaufdatum der Zahlungsanwendung (weiter unten angegeben). Weitere Einzelheiten finden Sie in der vollständigen Tabelle auf Seite 22.

Eintrag in der PCI SSC-Liste vor dem Ablauf		Eintrag in der PCI SSC-Liste nach dem Ablauf	
Validierungshinweise	Bereitstellungshinweise	Validierungshinweise	Bereitstellungshinweise
Gemäß PABP validiert	Geeignet für neue Bereitstellungen	Gemäß PABP validiert	Nicht geeignet für neue Bereitstellungen
Prä-PCI-Anwendung	Nicht empfohlen für neue Bereitstellungen	Prä-PCI-Anwendung	Nicht geeignet für neue Bereitstellungen
Gemäß PA-DSS validiert	Geeignet für neue Bereitstellungen	Gemäß PA-DSS validiert	Nicht geeignet für neue Bereitstellungen

Selbstbescheinigung über kleine Versionsänderungen, falls zutreffend

Die **Selbstbescheinigung über kleine Versionsänderungen** wird gegebenenfalls verwendet, um die Anwendungsversionen anzugeben, die das Verfahren für geringfügige Anwendungsänderungen durchlaufen, das in diesem Dokument im Abschnitt *Keine Auswirkung auf PA-DSS-Anforderungen* dokumentiert ist.

Datum der jährlichen Neuvalidierung

Über das **Datum der jährlichen Neuvalidierung** gibt der PCI SSC an, wann die jährliche Validierungsbestätigung des Softwareanbieters fällig ist. Die jährliche Neuvalidierung ist Bestandteil des Formulars für die Validierungsbestätigung, das sich in Anhang C zum PA-DSS, Teil 3b, befindet.

Ablaufdatum

Das **Ablaufdatum** für PA-DSS-validierte Zahlungsanwendungen ist das Datum, an dem eine Anwendung gemäß den aktuellen PA-DSS-Anforderungen erneut evaluiert worden sein muss, damit der Annahmestatus bestehen bleibt. Das Ablaufdatum bezieht sich auf die weiter oben beschriebenen Bereitstellungshinweise.

Der PCI SSC bemüht sich, den PA-DSS alle 24 Monate zusammen mit dem PCI-DSS zu aktualisieren. Die Annahme der PA-DSS-validierten Zahlungsanwendungen läuft drei Jahre nach dem Datum des Inkrafttretens einer nachfolgenden Aktualisierung der PA-DSS-Anforderungen ab. Das Ziel besteht darin, dass die Annahme mindestens drei Jahre gültig ist, vorausgesetzt, dass keine ernste Bedrohung sofortige Änderungen erfordert.

Hinweis:

Alle PA-DSS-Beurteilungen gemäß Version 1.1 weisen dasselbe Ablaufdatum wie Prüfungen gemäß PA-DSS Version 1.2 auf, wobei derselbe Prozess für den Ablauf gilt.

Beispiel: PA-DSS Version 1.1 und Version 1.2 weisen dasselbe Ablaufdatum auf. Die neue PA-DSS-Version (die Version nach 1.2) wird ungefähr im Oktober 2010 erwartet, und Prüfungen gemäß PA-DSS Version 1.1 und 1.2 werden im Oktober 2013 ablaufen.

Zurzeit gibt es noch kein Ablaufdatum für PA-DSS-validierte Zahlungsanwendungen, die sich zum Zeitpunkt der Bereitstellung auf der Annahmeliste befanden. Bereitgestellte Zahlungsanwendungen, deren Genehmigung abläuft, können weiterhin verwendet werden. Die Ablauffrist bezieht sich auf Neuanschaffungen oder neue Bereitstellungen, nicht auf vorhandene Bereitstellungen.

PA-QSA-Unternehmen

Dieser Eintrag bezeichnet den Namen des **Unternehmens für die qualifizierte Sicherheitsprüfung von Zahlungsanwendungen**, das die Validierung durchgeführt und festgestellt hat, dass die Zahlungsanwendung PA-DSS-konform ist.

Typ der Zahlungsanwendung

Der **Typ der Zahlungsanwendung** gibt einen der folgenden Punkte an:

- Point of Sale (POS)
- Middleware
- Automatische Tanksäule
- Warenkorb
- Verrechnung
- Karte liegt nicht physisch vor
- Gateway
- Sonstiges

Zielmarkt

Der **Zielmarkt** beschreibt gegebenenfalls einen Zielmarkt für die Zahlungsanwendung. Der Zielmarkt kann z. B. einer der folgenden Bereiche sein:

- Einzelhändler
- Kiosks an Parkplätzen
- Gas/Öl
- E-Commerce

Hinweis:

Dies dient zur Angabe, ob die Zahlungsanwendung für einen bestimmten Markt bestimmt ist, nicht für Marketingzwecke des Softwareanbieters.

Gegebenenfalls eine bestimmte Region oder Ländereinstellung für die Zahlungsanwendung

Die bestimmte Region oder Ländereinstellung für die Zahlungsanwendung bezeichnet Zahlungsanwendungen, die für spezifische geografische Regionen oder Ländereinstellungen entwickelt wurden und nur für diese Regionen und Einstellungen verwendet werden können.

Anhang B: Identifizierung zertifizierter Zahlungsanwendungs-Builds

Hinweis: Zur zukünftigen Berücksichtigung.

Zertifizierte Zahlungsanwendungs-Builds sind zu diesem Zeitpunkt zwar nicht erforderlich, aber Softwareanbietern und PA-QSAs wird empfohlen, in Zusammenarbeit Methoden für die Zertifizierung und digitale Unterzeichnung von Zahlungsanwendungs-Builds zu entwickeln. Der PCI SSC behält sich das Recht vor, zu einem zukünftigen Zeitpunkt zertifizierte Anwendungs-Builds zu verlangen.

Eine solche Methode könnte z. B. Folgendes beinhalten:

Anbieter identifizieren einen zertifizierten Build eindeutig zur allgemeinen Freigabe. Im Idealfall wird ein Build, der von einem PA-QSA als PA-DSS-konform zertifiziert wird, vom Softwareanbieter und dem QSA mit einem Fingerabdruck versehen – digital unterzeichnet (Code Signing) –, wenn er für die Lieferung verpackt wird. Zumindest sollte die Lieferung durch den Namen, die Version, die Build-Nummer und einen Datum-/Uhrzeitstempel eindeutig gekennzeichnet sein und mit einem MD5-Digest und der entsprechenden Build-Kopfzeile verifiziert werden können. Auf diese Weise wird die PA-DSS-Anforderung 7.2 zur Lieferungssicherung durch eine „vertrauenswürdige Basis“ verstärkt. Außerdem können dadurch PA-DSS-Programme im Zusammenhang mit den Zahlungsmarken unterstützt und das Sicherheitsbewusstsein sowie das Vertrauen der Kunden erhöht werden.

Anhang C: Selbstbescheinigung über kleine Versionsänderungen

Anleitung zum Einreichen

Der Zahlungsanwendungsanbieter und der PA-QSA (Payment Application Qualified Security Assessor) müssen dieses Dokument als Erklärung der Änderung der Zahlungsanwendung entsprechend dem Datensicherheitsstandard für Zahlungsanwendungen (PA-DSS) ausfüllen. Der Zahlungsanwendungsanbieter sollte alle zutreffenden Abschnitte ausfüllen und das Änderungsanalysedokument sowie diese Selbstbescheinigung an den PA-QSA weiterleiten.

Nach der Prüfung der bereitgestellten Dokumentation sollte der PA-QSA die zutreffenden Abschnitte ausfüllen und zusammen mit sämtlichen Kopien der gesamten benötigten Dokumentation gemäß den PCI SSC-Anweisungen zur Verschlüsselung und Einreichung von Berichten beim PCI SSC einreichen.

Teil 1. Informationen zum Anbieter der Zahlungsanwendung

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

Teil 1a. Informationen zur Zahlungsanwendung

Name und Versionsnummer der übergeordneten Zahlungsanwendung, die auf der aktuellen PCI SSC-Liste enthalten ist:

Name der vorhandenen Anwendung: _____ Versionsnummer der vorhandenen Anwendung: _____

PCI SSC-Annahmenummer: _____

Name und Versionsnummer der neuen Zahlungsanwendung, falls zutreffend:

Name der neuen Anwendung: _____ Versionsnummer der neuen Anwendung: _____

Beschreibung der Änderung, falls zutreffend: _____

Funktionen der Zahlungsanwendung (alle zutreffenden auswählen):

- | | | |
|---|---|---|
| <input type="checkbox"/> Point of Sale | <input type="checkbox"/> Warenkorb | <input type="checkbox"/> Karte liegt nicht physisch vor |
| <input type="checkbox"/> Middleware | <input type="checkbox"/> Verrechnung | <input type="checkbox"/> Gateway: |
| <input type="checkbox"/> Automatische Tanksäule | <input type="checkbox"/> Sonstiges (bitte angeben): _____ | |

Zielmarkt für die Anwendung: _____

Teil 2. Informationen über den qualifizierten Sicherheitsprüfer von Zahlungsanwendungen (PA QSA)

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

Teil 3. Bestätigung des Änderungsstatus

Teil 3a. Bescheinigung des Zahlungsanwendungsanbieters

Auf der Grundlage der internen Änderungsanalyse und der Änderungsanalyседokumentation stellt (*PA Vendor Name*) den folgenden Status für die in Teil 1a dieses Dokuments vom (*date*) ermittelte(n) Anwendung(en) und Version(en) fest (Zutreffendes ankreuzen):

<input type="checkbox"/>	Nur <i>geringfügige Änderungen</i> wurden an der weiter oben beschriebenen übergeordneten Anwendung vorgenommen, um die ebenfalls weiter oben beschriebene neue Anwendung zu erstellen, sodass sich Keine Auswirkung auf die PA-DSS-Anforderungen ergibt.
<input type="checkbox"/>	Alle Änderungen wurden im begleitenden Änderungsanalyседokument genau aufgezeichnet, das dem in Teil 2 angegebenen PA-QSA bereitgestellt wird.
<input type="checkbox"/>	Alle Informationen, die in dieser Selbstbescheinigung enthalten sind, stellen die Ergebnisse der Änderungsanalyse in allen materiellen Aspekten korrekt dar.
<input type="checkbox"/>	Für KEINE der von der Anwendung generierten Dateien oder Funktionen wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifendaten (aus einer Spur) ⁴ , CAV2-, CVC2-, CID- oder CVV2-Daten ⁵ oder PIN-Daten ⁶ gespeichert wurden.

Teil 3b. PA-QSA-Bescheinigung

Auf der Grundlage der Änderungsanalyседokumentation, die von dem in Teil 1 angegebenen Zahlungsanwendungsanbieter bereitgestellt wird, stellt (*PA-QSA Name*) den folgenden Status für die in Teil 1a dieses Dokuments vom (*date*) ermittelte(n) Anwendung(en) und Version(en) fest (Zutreffendes ankreuzen):

<input type="checkbox"/>	Auf der Grundlage unserer Prüfung der Änderungsanalyседokumentation sind wir der Meinung, dass die Dokumentation die Behauptung des Anbieters unterstützt, dass <i>nur geringfügige Änderungen</i> an der weiter oben beschriebenen Anwendung vorgenommen wurden, sodass sich Keine Auswirkung auf die PA-DSS-Anforderungen ergibt.
--------------------------	--

⁴ Magnetstreifendaten (Verfolgungsdaten): Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Stellen dürfen nach der Autorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Verfolgungsdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

⁵ Der drei- oder vierstellige Wert, der im oder rechts neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

⁶ PIN-Daten: Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Teil 3c. Bestätigungen des PA-QSA und Anwendungsanbieters

<i>Unterschrift des PA-QSA-Leiters</i> ↑	<i>Datum</i> ↑
<i>Name des PA-QSA-Leiters</i> ↑	<i>Titel</i> ↑
<i>Unterschrift des Beauftragten des Anwendungsanbieters</i> ↑	<i>Datum</i> ↑
<i>Name des Beauftragten des Anwendungsanbieters</i> ↑	<i>Titel</i> ↑

Vertretener Anwendungsanbieter ↑