Security Standards Council

Zahlungskartenbranche (PCI)

Zahlungsanwendung Datensicherheitsstandard

Anforderungen und Sicherheitsbeurteilungsverfahren

Version 3.2

Mai 2016

Dokumentänderungen

Datum	Version	Beschreibung	Seiten
1. Oktober 2008	1.2	Anpassung der Inhalte an den neuen PCI DSS v1.2 und Implementieren kleinerer Änderungen nach der Ursprungsversion v1.1.	
Juli 2009	1.2.1	Angleichen von Inhalten an den PA-DSS-Programmleitfaden in „Umfang des PA-DSS“, v1.2.1, um zu verdeutlichen, für welche Anwendungen PA-DSS gilt.	v, vi
		Korrektur der Schreibweise von „OWASP“ in Laboranforderung 6.	30
		Aktualisieren der Funktionalität der Zahlungsanwendung in der Validierungsbestätigung, Teil 2a, um diese an die im PA-DSS-Programmleitfaden aufgeführten Anwendungsarten anzupassen und die Verfahren in Teil 3b für die jährlich erneute Validierungsbestätigung zu verdeutlichen.	32, 33
Oktober 2010	2.0	Aktualisieren und Implementieren kleinerer Änderungen seit der Version 1.2.1 und Angleichung an den neuen PCI-DSS v2.0. Ausführliche Informationen finden Sie unter *„PA-DSS – Änderungsübersicht von PA-DSS Version 1.2.1 auf 2.0.“*	
November 2013	3.0	Aktualisieren von PA-DSS v2. Ausführliche Informationen finden Sie unter *„PA-DSS – Änderungsübersicht von PA-DSS Version 2.0 auf 3.0.“*	
Mai 2015	3.1	Aktualisieren von PA-DSS v3.0. Einzelheiten zu den Änderungen finden Sie unter *PA-DSS – Übersicht der Änderungen PA-DSS Version 3.0 auf 3.1.*	
Mai 2016	3.2	Aktualisieren von PA-DSS v3.1. Einzelheiten zu den Änderungen finden Sie unter *PA-DSS – Übersicht der Ändrungen von PA-DSS Version 3.1 auf 3.2.*	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Inhalt

Dokumentänderungen ... 2
Einleitung ... 5
Zweck dieses Dokuments ... 5
Beziehung zwischen PCI-DSS und PA-DSS ... 5
Integratoren und Wiederverkäufer ... 7
Informationen zur PCI DSS-Anwendbarkeit ... 7
Umfang des PA-DSS ... 9
Anwendbarkeit des PA-DSS auf Zahlungsanwendungen in Hardware-Terminals ... 10
PA-DSS-Implementierungshandbuch ... 11
Anforderungen an PA-QSAs ... 12
Testlabor ... 12
Anweisungen und Inhalt für den Validierungsbericht ... 12
PA-DSS-Schritte zur Fertigstellung ... 13
PA-DSS-Programmleitfaden ... 13
PA-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren ... 14
Anforderung 1: *Kein Aufbewahren von vollständigen Verfolgungsdaten, Kartenüberprüfungscodes oder -werten (CAV2, CID, CVC2, CVV2) sowie PIN-Block-Daten* ... 15
Anforderung 2: *Schutz gespeicherter Karteninhaberdaten* ... 21
Anforderung 3: *Bereitstellen sicherer Authentifizierungsfunktionen* ... 31
Anforderung 4: *Protokollieren der Aktivität von Zahlungsanwendungen* ... 42
Anforderung 5: *Entwickeln sicherer Zahlungsanwendungen* ... 46
Anforderung 6: *Schutz von drahtlosen Übertragungen* ... 69
Anforderung 7: *Testen von Zahlungsanwendungen in Bezug auf die Ermittlung von Sicherheitsrisiken und Implementierung von Updates für die Zahlungsanwendung* ... 74
Anforderung 8: *Unterstützung einer sicheren Netzwerkimplementierung* ... 79
Anforderung 9: *Karteninhaberdaten dürfen nie auf einem mit dem Internet verbundenen Server gespeichert werden* ... 81
Anforderung 10: *Ermöglichen eines sicheren Remotezugriffs auf Zahlungsanwendungen* ... 83
Anforderung 11: *Verschlüsseln von sensiblem Datenverkehr in öffentlichen Netzwerken* ... 87
Anforderung 12: *Sichern des gesamten Nichtkonsolen-Verwaltungszugriffs* ... 90
Anforderung 13: *Pflegen eines PA-DSS-Implementierungshandbuchs für Kunden, Wiederverkäufer und Integratoren* ... 92

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 14: Zuweisen von PA-DSS-Verantwortlichkeiten an Mitarbeiter und Pflegen von Schulungsprogrammen für Mitarbeiter, Kunden, Wiederverkäufer und Integratoren 94
Anhang A: Inhaltszusammenfassung für das *PA-DSS-Implementierungshandbuch* 97
Anhang B: Testlabor-Konfiguration für PA-DSS-Bewertungen 117

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Einleitung

Zweck dieses Dokuments

Die PA-DSS (Payment Application Data Security Standard, Zahlungsanwendung Datensicherheitsstandard)-Anforderungen und Sicherheitsbeurteilungsverfahren der PCI definieren die Sicherheitsanforderungen und Beurteilungsverfahren für Anbieter von Zahlungsanwendungen. Dieses Dokument wurde für PA-QSAs (Payment Application Qualified Security Assessors, Akkreditierte Sicherheitsgutachter für Zahlungsanwendungen) entwickelt, die Zahlungsanwendungen bewerten, um sicherzustellen, dass die Zahlungsanwendungen den PA-DSS-Standard erfüllen. In der *PA-DSS-ROV-Berichtsvorlage,* die auf der PCI SSC-Website (PCI Security Standards Council) – www.pcisecuritystandards.org – *verfügbar ist, finden PA-QSAs Informationen zum Dokumentieren einer PA-DSS-Bewertung und zum Erstellen eines ROV (Report on Validation, Validierungsbericht).*

Weitere Ressourcen, einschließlich Validierungsbestätigungen, Häufig gestellte Fragen (FAQs) und der *PCI-DSS sowie dem PA-DSS-Glossar, Abkürzungen und Akronyme* sind auf der Website des PCI Security Standards Council (PCI SSC) verfügbar—www.pcisecuritystandards.org.

Beziehung zwischen PCI-DSS und PA-DSS

Allein durch die Nutzung einer PA-DSS-konformen Anwendung wird eine Einheit noch nicht PCI-DSS-konform, da diese Anwendung in einer PCI-DSS-konformen Umgebung und im Sinne des von dem Zahlungsanwendungsanbieter bereitgestellten *PA-DSS-Implementierungshandbuchs* implementiert werden muss (gemäß PA-DSS-Anforderung 13). Die PA-DSS-Anforderungen leiten sich aus den *PCI-DSS (Payment Card Industry Data Security Standard, PCI-Datensicherheitsstandard)-Anforderungen und Sicherheitsbeurteilungsverfahren* ab, in denen angegeben ist, welche Anforderungen erfüllt sein müssen, um als PCI-DSS-konform angesehen zu werden (und welche Elemente von einer Zahlungsanwendung unterstützt werden müssen, um Kunden die Einhaltung des PCI-DSS zu ermöglichen). Sie finden den PCI-DSS unter www.pcisecuritystandards.org.

Die PCI-DSS-Bewertung einer Einheit umfasst alle Anwendungen, in denen Karteninhaberdaten gespeichert, verarbeitet oder weitergegeben werden – einschließlich der Anwendungen, für die eine PA-DSS-Validierung durchgeführt wurde. Bei der PCI-DSS-Bewertung sollte geprüft werden, ob die PA-DSS-Zahlungsanwendung ordnungsgemäß konfiguriert und gemäß den PCI-DSS-Anforderungen sicher implementiert wurde. Wenn die Zahlungsanwendung individuell angepasst wurde, ist bei der PCI-DSS-Bewertung eine gründlichere Überprüfung erforderlich, da die Anwendung möglicherweise nicht mehr der Version entspricht, für die eine PA-DSS-Validierung durchgeführt wurde.

Der PCI-DSS gilt unter Umständen nicht direkt für einen Anbieter von Zahlungsanwendungen, wenn dieser Karteninhaberdaten nicht speichert, verarbeitet oder weitergibt bzw. Zugriff auf die Karteninhaberdaten der Kunden hat. Da allerdings die betreffenden Zahlungsanwendungen von Kunden des Anwendungsanbieters genutzt werden, um Karteninhaberdaten zu speichern, zu verarbeiten und zu übertragen, und die Kunden den PCI-DSS-Standard einhalten müssen, sollten Zahlungsanwendungen die Einhaltung des PCI-DSS-Standards durch die Kunden begünstigen und nicht behindern. Hier einige Beispiele dafür, wie unsichere Zahlungsanwendungen der Einhaltung des Standards im Wege stehen können:

1. Speicherung von Magnetstreifendaten und/oder gleichwertige Daten auf dem Chip im Kundennetzwerk nach der Autorisierung;
2. Anwendungen, die Kunden dazu auffordern, andere laut PCI-Datensicherheitsstandard erforderliche Funktionen, wie Antivirensoftware oder Firewalls, zu deaktivieren, um eine ordnungsgemäße Funktion der Zahlungsanwendung sicherzustellen; und

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

3. die Nutzung unsicherer Methoden durch den Anbieter, um den Kunden einen Online-Support für die Anwendung anzubieten.

Sichere Zahlungsanwendungen minimieren bei einer Implementierung in einer PCI-DSS-konformen Umgebung das Potenzial von Sicherheitsverletzungen, die zu einer Kompromittierung der PAN (Primary Account Number, Primäre Kontonummer), vollständigen Verfolgungsdaten, Kartenüberprüfungscodes und -werte (CAV2, CID, CVC2, CVV2) sowie PINs und PIN-Blöcke führen, und verhindern somit Schädigungen durch Betrug, der auf diese Sicherheitsverletzungen zurückzuführen ist.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Integratoren und Wiederverkäufer

Anwendungsanbieter können Integratoren und Wiederverkäufer beauftragen, Zahlungsanwendungen in ihrem Namen zu verkaufen, zu installieren und/oder zu warten. Integratoren/Wiederverkäufer sind an der Sicherstellung einer sicheren Installation und Ausführung der Zahlungsanwendungen beteiligt, da sie Services oft am Standort der Kunden eines Anbieters bereitstellen und sie die Kunden bei der Installation von validierten PA-DSS-Zahlungsanwendungen unterstützen. Wenn eine Anwendung nicht ordnungsgemäß konfiguriert, gewartet und unterstützt wird, kann dies Sicherheitsrisiken in der Karteninhaberdaten-Umgebung des Kunden verursachen, die dann für Angriffe ausgenutzt werden können. Anwendungsanbieter sollten ihre Kunden, Integratoren und Wiederverkäufer darüber informieren, wie die Installation und Konfiguration von Zahlungsanwendungen auf PCI-DSS-konforme Art und Weise durchgeführt wird.

QIRs (Qualified Integrators and Resellers, Integratoren und Wiederverkäufer mit PCI-Qualifizierung) werden vom Security Standards Council in PCI-DSS und PA-DSS, d. h. in der sicheren Implementierung von Zahlungsanwendungen, geschult. Weitere Informationen zum PCI-QIR-Programm finden Sie unter www.pcisecuritystandards.org.

Informationen zur PCI DSS-Anwendbarkeit

Der PCI-DSS gilt für alle Einrichtungen, die an der Verarbeitung von Zahlungskarten beteiligt sind – einschließlich Vertragsunternehmen, EDV-Dienstleistern, abrechnenden Stellen, Kartenemittenten und Dienstleistern. Der PCI-DSS gilt außerdem für ***alle*** anderen Einrichtungen, die Karteninhaberdaten und/oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder übertragen.

Karteninhaberdaten und vertrauliche Authentifizierungsdaten sind wie folgt definiert:

Kontodaten	
Zu den Karteninhaberdaten zählen:	**Zu den vertraulichen Authentifizierungsdaten zählen:**
▪ Primary Account Number (PAN) ▪ Name des Karteninhabers ▪ Ablaufdatum ▪ Servicecode	▪ Vollständige Verfolgungsdaten (Magnetstreifendaten oder gleichwertige Daten auf einem Chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN-Blöcke

***Die PAN (Primary Account Number, Primäre Kontonummer) ist der ausschlaggebende Faktor für die Karteninhaberdaten*.** Wenn der Name des Inhabers, der Servicecode und/oder das Ablaufdatum zusammen mit der PAN gespeichert, verarbeitet oder übertragen werden oder anderweitig innerhalb der Karteninhaberdaten-Umgebung (CDE) gegenwärtig sind, müssen diese Daten im Sinne der PCI-DSS-Anforderungen geschützt werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

In der Tabelle auf der folgenden Seite sind häufig verwendete Elemente von Karteninhaberdaten und vertraulichen Authentifizierungsdaten aufgeführt. Außerdem wird angegeben, ob die Speicherung dieser Daten zulässig oder verboten ist und ob diese Daten geschützt werden müssen. Diese Tabelle erhebt keinen Anspruch auf Vollständigkeit, sondern dient dazu, die verschiedenen Arten von Anforderungen darzustellen, die für jedes Datenelement gelten.

		Datenelement	Speichern zulässig	Gespeicherte Daten werden gemäß der PA-DSS-Anforderung 2.3 unleserlich gemacht.
Kontodaten	**Karteninhaberdaten**	Primary Account Number (PAN)	Ja	Ja
		Name des Karteninhabers	Ja	Nein
		Servicecode	Ja	Nein
		Ablaufdatum	Ja	Nein
	Vertrauliche Authentifizierungsdaten[1]	Vollständige Verfolgungsdaten [2]	Nein	Die Speicherung ist gemäß der PA-DSS-Anforderung 1.1 nicht zulässig.
		CAV2/CVC2/CVV2/CID[3]	Nein	Die Speicherung ist gemäß der PA-DSS-Anforderung 1.1 nicht zulässig.
		PIN/PIN-Block[4]	Nein	Die Speicherung ist gemäß der PA-DSS-Anforderung 1.1 nicht zulässig.

Die PA-DSS-Anforderungen 2.2 und 2.3 finden nur bezüglich der PAN Anwendung. Wenn die PAN zusammen mit anderen Elementen der Karteninhaberdaten gespeichert wird, muss nur die PAN gemäß der PA-DSS-Anforderung 2.3 unleserlich gemacht werden.

Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung (auch im verschlüsselten Zustand) nicht gespeichert werden. Dies gilt auch dann, wenn keine PAN in der Umgebung vorliegt.

---

1 *Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung (auch im verschlüsselten Zustand) nicht gespeichert werden.*

2 *Vollständige Verfolgungsdaten vom Magnetstreifen, gleichwertige Daten auf dem Chip oder einem anderen Speicherort*

3 *Die drei- bzw. vierstellige Zahl auf der Vorder- bzw. Rückseite der Zahlungskarte*

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

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Umfang des PA-DSS

Der PA-DSS gilt für Softwareanbieter und andere Entwickler von Zahlungsanwendungen, mit denen Karteninhaberdaten und/oder vertrauliche Authentifizierungsdaten gespeichert, verarbeitet oder übertragen werden. Informationen bezüglich der Qualifikation verschiedener Anwendungstypen finden Sie im *PA-DSS-Programmleitfaden*.

Die PA-DSS-Bewertung sollte Folgendes umfassen:

- Untersuchung aller Funktionen von Zahlungsanwendungen, darunter:
  1) End-to-End-Zahlungsfunktionen (Autorisierung und Verrechnung),
  2) Eingabe und Ausgabe,
  3) Fehlerzustände,
  4) Schnittstellen und Verbindungen zu anderen Dateien, Systemen, Zahlungsanwendungen oder Anwendungskomponenten,
  5) den vollständigen Verkehr von Karteninhaberdaten,
  6) Verschlüsselungsmechanismen und
  7) Authentifizierungsmechanismen.
- Untersuchung der Anleitungen, die der Anbieter der Zahlungsanwendung an Kunden und Integratoren/Wiederverkäufer weitergeben sollte (siehe auch das *PA-DSS-Implementierungshandbuch* an späterer Stelle), um Folgendes sicherzustellen:
  1) Der Kunde weiß, wie die Zahlungsanwendung auf PCI-DSS-konforme Weise implementiert wird
  2) Dem Kunden wird klar gemacht, dass gewisse Einstellungen der Zahlungsanwendung bzw. deren Umgebung die PCI-DSS-Konformität beeinträchtigen können.

  Beachten Sie, dass vom Anbieter der Zahlungsanwendung eventuell selbst dann erwartet wird, solche Hilfestellungen anzubieten, wenn die jeweilige Einstellung:
  1) nicht vom Anbieter der Zahlungsanwendung nach erfolgter Installation beim Kunden kontrolliert werden kann oder
  2) in der Verantwortung des Kunden und nicht des Anbieters der Zahlungsanwendung liegt.
- Prüfung aller ausgewählten Plattformen für die zu prüfende Version der Zahlungsanwendung (die geprüften Plattformen sollten dokumentiert werden)
- Prüfung der Tools, die von oder innerhalb der Zahlungsanwendung genutzt werden, um Karteninhaberdaten abzurufen und/oder anzuzeigen (Reportingtools, Protokollierungstools usw.)
- Prüfung aller mit der Zahlungsanwendung in Zusammenhang stehenden Softwarekomponenten, inklusive der Anforderungen und Abhängigkeiten von Drittanbieter-Software

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

- Prüfung aller anderen Arten von Zahlungsanwendungen, die für eine vollständige Implementierung erforderlich sind
- Prüfung der Versionierungsmethode des Anbieters

Anwendbarkeit des PA-DSS auf Zahlungsanwendungen in Hardware-Terminals

Dieser Abschnitt bietet einen Leitfaden für Anbieter, die eine PA-DSS-Validierung für eigene Zahlungsanwendungen auf Hardware-Terminals (auch bekannt als eigenständige oder spezielle Zahlungs-Terminals) anstreben.

Es gibt zwei Wege, die PA-PSS-Validierung für eine eigene Zahlungsanwendung auf einem Hardware-Terminal zu erreichen:

1. Die eigene Zahlungsanwendung erfüllt direkt alle PA-DSS-Anforderungen und wird entsprechend den Standard-PA-DSS-Verfahren validiert.

2. Die eigene Zahlungsanwendung erfüllt nicht alle PA-DSS-Anforderungen, doch die Hardware, auf der die Anwendung gespeichert ist, ist auf der Liste zugelassener PTS-Geräte (PIN Transaction Security, zu deutsch „PIN-Transaktionssicherheit“) des PCI-SSC als ein aktuell PCI-PTS-zugelassenes POI-Gerät (Point of Interaction, zu deutsch „Interaktionspunkt“) gelistet. In diesem Szenario wäre es möglich, dass die Anwendung die PA-DSS-Anforderungen mittels einer Kombination aus den PA-DSS und PTS-validierten Kontrollen erfüllt.

Der restliche Teil dieses Abschnitts gilt ausschließlich für Zahlungsanwendungen, die auf einem validierten PCI-PTS-zugelassenen POI-Gerät gespeichert sind.

Falls die Zahlungsanwendung einer oder mehreren PA-DSS-Anforderungen nicht direkt entspricht, können diese indirekt im Zuge von Kontrollen der PCI-PTS-Validierung erfüllt werden. Damit eine Hardwareeinheit in einer PS-DSS-Überprüfung einbezogen werden kann, MUSS die Hardwarereinheit als ein PCI-PTS-zugelassenes POI-Gerät validiert und auf der Liste zugelassener PTS-Geräte des PCI-SSC gelistet sein. Das PTS-validierte POI-Gerät, das eine sichere Datenverarbeitungsumgebung darstellt, wird zu einer „***benötigten Abhängigkeit***“ für die Zahlungsanwendung und die Kombination aus Anwendung und Hardware werden zusammen in der Liste der PA-DSS-validierten Zahlungsanwendungen erfasst.

Während der PA-DSS-Bewertung muss der PA-QSA die Zahlungsanwendung sowie die ihr zugrunde liegende Hardware vollständig auf alle PA-DSS-Anforderungen überprüfen. Sollte der PS-QSA zu dem Schluss kommen, dass eine oder mehrere PA-DSS-Anforderungen von der eigenen Zahlungsanwendung nicht erfüllt werden können, sie jedoch PCI-PTS-validierten Kontrollen entsprechen, muss der PA-QSA Folgendes tun:

1. Klar dokumentieren, welche PS-DSS-Anforderungen erfüllt werden (wie gewöhnlich);

2. Klar dokumentieren, welche PCI-PTS-Anforderung im „Implementiert“-Feld für diese Anforderung erfüllt wurde;

3. Angabe einer ausführlichen Erklärung, warum die Zahlungsanwendung der PA-DSS-Anforderung nicht entsprach;

4. Dokumentation der angewandten Verfahren, um zu bestimmen, wie diese Anforderung über eine PCI-PTS-validierte Kontrolle optimal erfüllt wurde;

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

5. Erfassen des PCI-PTS-validierten Hardware Terminals als eine erforderliche Abhängigkeit in der Zusammenfassung für die Geschäftsleitung des Validierungsberichts.

Sobald die Validierung der Zahlungsanwendung durch den PA-QSA abgeschlossen und durch den PCI-SSC akzeptiert wurde, wird die PTS-validierte Hardwareeinheit als eine Abhängigkeit der Zahlungsanwendung in den PA-DSS-validierten Anwendungen erfasst.

Eigene Zahlungsanwendungen auf Hardware Terminals, die mittels einer Kombination aus PS-DSS und PCI-PTS-Kontrollen validiert werden, müssen folgende Kriterien erfüllen:

1. Beide Elemente müssen dem Kunden zusammen geliefert werden (d. h. Hardware Terminal und Anwendung) ODER, wenn sie getrennt geliefert werden, muss der Anwendungsanbieter und/oder der Integrator/Wiederverkäufer die Anwendung für den Vertrieb so zusammenstellen, dass sie ausschließlich auf dem Hardware-Terminal läuft, für das sie validiert wurde.
2. Sie müssen standardmäßig aktiviert sein, um die PCI-Konformität eines Kunden zu unterstützen.
3. Sie müssen einen laufenden Support sowie Updates zur Aufrechterhaltung der PCI-DSS-Konformität bieten.
4. Wenn die Anwendung separat an Kunden verkauft, vertrieben oder lizenziert wird, muss der Anbieter in Übereinstimmung mit der PA-DSS-Validierungsliste der Anwendung detaillierte Informationen zu der zugehörigen Hardware liefern.

PA-DSS-Implementierungshandbuch

Validierte Zahlungsanwendungen müssen auf PCI-DSS-konforme Art und Weise implementiert werden können. Softwareanbieter sind verpflichtet, ein *PA-DSS-Implementierungshandbuch* bereitzustellen, das ihre Kunden und Integratoren/Wiederverkäufer über eine sichere Produktimplementierung informiert. In diesem Dokument müssen die individuellen Hinweise zur sicheren Konfiguration enthalten sein, außerdem muss der Anbieter die eigenen Verantwortlichkeiten ebenso wie die des Integrators/Wiederverkäufers und des Kunden zur Einhaltung der PCI-DSS-Anforderungen klar erläutern. Es sollte detailliert erklärt werden, wie der Kunde und/oder der Integrator/Wiederverkäufer Sicherheitseinstellungen innerhalb des Kundennetzwerks einzurichten hat. Beispielsweise sollten im *PA-DSS-Implementierungshandbuch* die Verantwortlichkeiten und grundlegenden Merkmale zur PCI-DSS-Kennwortsicherheit angesprochen werden, selbst wenn diese nicht durch die Zahlungsanwendung gesteuert wird. Der Grund: Der Kunde oder Integrator/Wiederverkäufer soll verstehen, wie sichere Kennwörter für eine PCI-DSS-Konformität implementiert werden.

Das *PA-DSS-Implementierungshandbuch* soll nicht einfach nur die Anforderungen des PCI-DSS oder PA-DSS wiederholen, sondern es muss detailliert beschreiben, wie die Zahlungsanwendung zu konfigurieren ist, damit sie den Anforderungen entspricht. Während einer Bewertung muss der PA-QSA überprüfen, ob die Anweisungen präzise und effektiv sind. Der PA-QSA muss außerdem überprüfen, ob das *PA-DSS-Implementierungshandbuch* an die Kunden und Integratoren/Wiederverkäufer verteilt wurde.

Zahlungsanwendungen, die entsprechend dem *PA-DSS-Implementierungshandbuch* und in einer PCI-DSS-konformen Umgebung implementiert werden, sollten die PCI-DSS-Konformität beim Kunden fördern und unterstützen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Siehe *Anhang A: Inhaltszusammenfassung für das PA-DSS-Implementierungshandbuch* für einen Vergleich der Verantwortungsbereiche für die Implementierung der im *PA-DSS-Implementierungshandbuch* spezifizierten Kontrollen.

Anforderungen an PA-QSAs

Nur PA-QSAs (Payment Application Qualified Security Assessors, Akkreditierte Sicherheitsgutachter für Zahlungsanwendungen), die von PA-QSA-Unternehmen beschäftigt werden, sind berechtigt, PA-DSS-Bewertungen durchzuführen. Eine Liste aller Unternehmen, die für die Durchführung von PA-DSS-Bewertungen qualifiziert sind, finden Sie in der PA-QSA-Liste unter www.pcisecuritystandards.org.

- Der PA-QSA muss die in diesem PA-DSS-Dokument genannten Testverfahren nutzen.
- Der PA-QSA muss Zugriff auf ein Labor haben, in dem der Validierungsprozess abläuft.

Testlabor

- Testlabore sind an zwei Orten vorzufinden: an einem PA-QSA-Standort oder in den Einrichtungen des Softwareanbieters.
- Das Testlabor sollte reale Nutzungen der Zahlungsanwendung simulieren können.
- Der PA-QSA muss die korrekte Installation der Laboreinrichtung bestätigen, um sicherzustellen, dass die Umgebung tatsächlich eine reale Situation simuliert und dass der Anbieter die Umgebung nicht auf irgendeine Weise modifiziert oder verfälscht hat.
- Weitere Informationen finden Sie in *Anhang B: Bestätigung der Testlabor-Konfiguration für die PA-DSS-Auswertung* in diesem Dokument mit detaillierten Anforderungen für Labor- und verwandte Prozesse.
- Der PA-QSA muss *Anhang B* für das zur Prüfung der jeweiligen Zahlungsanwendung genutzte Labor ausfüllen und als Teil des vollständigen PA-DSS-ROV (Report on Validation, Validierungsbericht) einreichen.

Anweisungen und Inhalt für den Validierungsbericht

Anweisungen und Inhalt für den PA-DSS-ROV (Report on Validation, Validierungsbericht) werden jetzt in der *PA-DSS-ROV-Berichtsvorlage bereitgestellt.* Die *PA-DSS-ROV-Berichtsvorlage* muss für die Erstellung des Validierungsberichts verwendet werden. An den PCI-SSC sollten nur konforme Zahlungsanwendungs-ROVs eingereicht werden. Ausführliche Informationen zum Einreichverfahren für ROVs finden Sie im *PA-DSS-Programmleitfaden*.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Schritte zur Fertigstellung

Dieses Dokument enthält die Tabelle zu den Anforderungen und Sicherheitsbeurteilungsverfahren sowie den *Anhang B: Testlabor-Konfiguration für PA-DSS-Bewertungen*. Die Anforderungen und Sicherheitsbeurteilungsverfahren enthalten detaillierte Informationen zu den Vorgehensweisen, die der PA-QSA durchzuführen hat.

Der PA-QSA muss die folgenden Schritte durchführen:

1. Bestätigen des Umfangs der PA-DSS-Bewertung
2. Durchführen der PA-DSS-Bewertung
3. Ausfüllen des ROV (Report on Validation, Validierungsbericht) mithilfe der *PA-DSS-ROV-Berichtsvorlage*, einschließlich der Bestätigung der für PA-DSS-Bewertungen verwendeten Testlabor-Konfiguration
4. Ausfüllen und Unterzeichnen einer Validierungsbestätigung (sowohl durch den PA-QSA als auch den Softwareanbieter) Die Validierungsbestätigung ist verfügbar auf der PCI-SSC-Website (www.pcisecuritystandards.org).
5. Einreichen sämtlicher oben aufgeführter Dokumente und des *PA-DSS-Implementierungshandbuchs* nach Fertigstellung an den PCI-SSC, entsprechend dem *PA-DSS-Programmleitfaden.*

Hinweis:

PA-DSS-Einreichungen sollten erst durchgeführt werden, nachdem bestätigt wurde, dass alle PA-DSS-Anforderungen erfüllt sind.

PA-DSS-Programmleitfaden

Im *PA-DSS-Programmleitfaden* finden Sie Informationen über das PA-DSS-Programmmanagement, einschließlich der folgenden Themen:

- Einzelheiten von verschiedenen PA-DSS-Versionen und deren Gültigkeitsdaten
- PA-DSS-Anwendbarkeit für verschiedene Arten von Anwendungen
- Einreich- und Annahmeverfahren für PA-DSS-Berichte
- Jährliche Aktualisierung von Zahlungsanwendungen auf der Liste validierter Zahlungsanwendungen
- Verantwortlichkeiten zur Benachrichtigung im Fall, dass eine Zahlungsanwendung sich als fehlerhaft herausstellt.

Der PCI SSC behält sich das Recht vor, bei wichtigen Änderungen am PA-DSS und/oder aufgrund festgestellter Verletzungen in einer aufgelisteten Zahlungsanwendung eine Neuvalidierung zu fordern.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren

Die Spaltentitel in der Tabelle für die PA-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren haben folgende Bedeutung:

- **PA-DSS-Anforderungen** – Diese Spalte definiert die Sicherheitsanforderungen für Zahlungsanwendungen, die überprüft werden.
- **Prüfverfahren** – Diese Spalte definiert die Prüfverfahren, anhand derer der PA-QSA die Einhaltung der PA-DSS-Anforderungen überprüft.
- **Leitfaden** – Diese Spalte beschreibt den Zweck bzw. das Sicherheitsziel hinter jeder PA-DSS-Anforderung und dient somit zum Verständnis der Anforderungen. Die Angaben in dieser Spalte ersetzen bzw. erweitern nicht die PA-DSS-Anforderungen und Prüfverfahren.

Hinweis:

Wenn Kontrollen noch nicht implementiert sind oder wenn ihre Implementierung für ein späteres Datum geplant ist, dürfen PA-DSS-Anforderungen nicht als erfüllt angesehen werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 1: Kein Aufbewahren von vollständigen Verfolgungsdaten, Kartenüberprüfungscodes oder -werten (CAV2, CID, CVC2, CVV2) sowie PIN-Block-Daten

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
1.1 Speichern Sie keine vertraulichen Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind). Falls vertrauliche Authentifizierungsdaten empfangen werden, müssen sämtliche Daten nach Abschluss des Autorisierungsprozesses so gelöscht werden, dass sie nicht wiederhergestellt werden können. Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 1.1.1 bis 1.1.3 aufgeführt sind. ***Im Sinne der PCI-DSS-Anforderung 3.2***	**1.1.a** Wenn diese Zahlungsanwendung vertrauliche Authentifizierungsdaten speichert, stellen Sie sicher, dass die Anwendung nur für Kartenemittenten und/oder Unternehmen, die Ausstellungsdienste unterstützen, gedacht ist.	Vertrauliche Authentifizierungsdaten umfassen vollständige Verfolgungsdaten, Kartenvalidierungscodes oder -werte und PIN-Daten. Die Speicherung vertraulicher Authentifizierungsdaten nach der Autorisierung ist nicht zulässig. Diese Daten sind für Personen mit böswilligen Absichten von großem Wert, zumal sie ihnen ermöglichen, gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen zu erstellen. Einheiten, die Zahlungskarten ausstellen bzw. Ausstellungsdienste erbringen oder unterstützen, erstellen und kontrollieren im Rahmen der Ausstellung häufig vertrauliche Authentifizierungsdaten. Kartenemittenten und Unternehmen, die Ausstellungsdienste unterstützen, dürfen vertrauliche Authentifizierungsdaten speichern, wenn dafür eine Begründung vorliegt und die Daten sicher gespeichert werden. Für Einheiten, die keine Zahlungskarten ausstellen, ist das Speichern vertraulicher Authentifizierungsdaten nach der Autorisierung nicht zulässig, und die Anwendungen müssen einen Mechanismus aufweisen, mit dem Daten in einer Art und Weise sicher gelöscht werden, die eine Wiederherstellung der Daten unmöglich macht.
	1.1.b Nutzen und prüfen Sie im Falle aller anderen Zahlungsanwendungen, wenn vertrauliche Authentifizierungsdaten (siehe nachfolgend 1.1.1 bis 1.1.3) vor der Autorisierung gespeichert werden, die Methode zum sicheren Löschen der Daten, um sicherzustellen, dass die Daten nicht wiederhergestellt werden können.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
1.1.1 Speichern Sie nicht den gesamten Inhalt einer Spur auf dem Magnetstreifen (auf der Kartenrückseite, in einem Chip oder an anderer Stelle). Diese Daten werden auch als Spurdaten, Full-Track-Daten, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet. ***Hinweis:*** *Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:* • *Der Name des Kontoinhabers,* • *Primäre Kontonummer (PAN),* • *Ablaufdatum und* • *Servicecode* *Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.* ***Im Sinne der PCI-DSS-Anforderung 3.2.1***	**1.1.1** Installieren Sie die Zahlungsanwendung, und führen Sie zahlreiche Testtransaktionen durch, die alle Funktionen der Zahlungsanwendung simulieren, einschließlich der Erzeugung von Fehlerbedingungen und Protokolleinträgen. Nutzen Sie forensische Tools und/oder Methoden (kommerziell vertriebene Tools, Skripte usw.),[5] um sämtliche von der Zahlungsanwendung ausgegebenen Informationen zu untersuchen und sicherzustellen, dass der gesamte Inhalt sämtlicher Spuren des Magnetstreifens auf der Kartenrückseite oder gleichwertige Daten auf einem Chip nach der Autorisierung nicht gespeichert werden. Nehmen Sie mindestens die folgenden Dateitypen auf (ebenso wie sämtliche anderen von der Zahlungsanwendung ausgegebenen Informationen): • Eingehende Transaktionsdaten • Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) • Verlaufsdateien • Trace-Dateien • Nicht flüchtige Arbeitsspeicherdaten inklusive nicht flüchtiger Cache-Inhalte • Datenbankschemata • Datenbankinhalte	Wenn vollständige Verfolgungsdaten gespeichert werden, sind Angreifer, die auf diese Daten zugreifen können, in der Lage, Zahlungskarten zu reproduzieren und betrügerische Transaktionen durchzuführen.

[5] *Forensisches Werkzeug oder Methode: Ein Werkzeug oder eine Methode zur Erkennung, Analyse und Präsentation forensischer Daten, mit dem bzw. der Hinweise auf Computern schnell und gründlich authentifiziert, durchsucht und wiederhergestellt werden können. Im Fall, dass forensische Werkzeuge oder Methoden von PA-QSAs verwendet werden, sollten diese Werkzeuge oder Methoden jegliche sensiblen Authentifizierungsdaten, die von der Zahlungsanwendung geschrieben wurden, präzise lokalisieren können. Bei den Tools kann es sich um kommerziell vertriebene, Open-Source- oder intern durch den PA-QSA entwickelte Tools handeln.*

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
1.1.2 Speichern Sie nach der Autorisierung nicht den Kartenüberprüfungswert oder -code (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite einer Zahlungskarte), der zur Verifizierung bei Transaktionen verwendet wird, bei denen die Karte nicht physisch vorliegt). ***Im Sinne der PCI-DSS-Anforderung 3.2.2***	**1.1.2** Installieren Sie die Zahlungsanwendung, und führen Sie zahlreiche Testtransaktionen durch, die alle Funktionen der Zahlungsanwendung simulieren, einschließlich der Erzeugung von Fehlerbedingungen und Protokolleinträgen. Nutzen Sie forensische Tools und/oder Methoden (kommerziell vertriebene Tools, Skripte usw.), um sämtliche von der Zahlungsanwendung ausgegebenen Informationen zu untersuchen und sicherzustellen, dass der drei- oder vierstellige Kartenüberprüfungscode auf der Kartenvorderseite oder im Unterschriftenfeld (CVV2-, CVC2-, CID-, CAV2-Daten) nach der Autorisierung nicht gespeichert wird. Nehmen Sie mindestens die folgenden Dateitypen auf (ebenso wie sämtliche anderen von der Zahlungsanwendung ausgegebenen Informationen): • Eingehende Transaktionsdaten • Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) • Verlaufsdateien • Trace-Dateien • Nicht flüchtige Arbeitsspeicherdaten inklusive nicht flüchtiger Cache-Inhalte • Datenbankschemata • Datenbankinhalte	Der Zweck des Kartenvalidierungscodes liegt im Schutz von Transaktionen, bei denen weder der Kunde anwesend ist noch die Karte vorliegt – Auftragsabwicklungen über das Internet oder per E-Mail/Telefon. Wenn diese Daten entwendet werden, sind Betrüger in der Lage, Transaktionen über das Internet und per Post/Telefon abzuwickeln.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
1.1.3 Speichern Sie nach der Autorisierung keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blöcke. ***Im Sinne der PCI-DSS-Anforderung 3.2.3***	**1.1.3** Installieren Sie die Zahlungsanwendung, und führen Sie zahlreiche Testtransaktionen durch, die alle Funktionen der Zahlungsanwendung simulieren, einschließlich der Erzeugung von Fehlerbedingungen und Protokolleinträgen. Nutzen Sie forensische Tools und/oder Methoden (kommerziell vertriebene Tools, Skripte usw.), um sämtliche von der Zahlungsanwendung ausgegebenen Informationen zu untersuchen und sicherzustellen, dass PINs und verschlüsselte PIN-Blöcke nach der Autorisierung nicht gespeichert werden. Nehmen Sie mindestens die folgenden Dateitypen auf (ebenso wie sämtliche anderen von der Zahlungsanwendung ausgegebenen Informationen). • Eingehende Transaktionsdaten • Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) • Verlaufsdateien • Trace-Dateien • Nicht flüchtige Arbeitsspeicherdaten inklusive nicht flüchtiger Cache-Inhalte • Datenbankschemata • Datenbankinhalte	Diese Werte sollten ausschließlich dem Karteninhaber und der Bank, die die Karte ausgestellt hat, bekannt sein. Wenn diese Daten entwendet werden, sind Betrüger in der Lage, PIN-basierte Lastschriften auszuführen (z. B. Abhebungen an Geldautomaten).

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
1.1.4 Löschen Sie sicher sämtliche Verfolgungsdaten (auf dem Magnetstreifen oder gleichwertige Daten auf einem Chip), Kartenüberprüfungswerte oder -codes sowie PINs oder PIN-Block-Daten, die von vorherigen Versionen der Zahlungsanwendung gespeichert wurden, in Übereinstimmung mit den branchenweit geltenden Standards für sicheres Löschen, wie sie beispielsweise in der Liste genehmigter Produkte der National Security Agency oder anderen staatlichen oder nationalen Standards oder Regelungen vorgegeben werden. ***Hinweis:*** *Diese Anforderung gilt nur, wenn vorherige Versionen der Zahlungsanwendung vertrauliche Authentifizierungsdaten speicherten.* ***Im Sinne der PCI-DSS-Anforderung 3.2***	**1.1.4.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Verlaufsdaten müssen entfernt werden (Verfolgungsdaten, Kartenüberprüfungscodes, PINs oder PIN-Blöcke, die von vorherigen Versionen der Zahlungsanwendung gespeichert wurden). • Anweisungen zum Löschen von Verlaufsdaten • Hinweis, dass das Entfernen für die PCI-DSS-Konformität absolut erforderlich ist	Alle diese Elemente vertraulicher Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden. Wenn ältere Versionen von Zahlungsanwendungen diese Informationen gespeichert haben, ist der Anbieter der Zahlungsanwendungen dazu verpflichtet, entsprechende Anweisungen im *PA-DSS-Implementierungshandbuch* sowie ein Tool oder Verfahren für Secure Wipes (sichere Löschverfahren) bereitzustellen. Wenn diese Daten nicht sicher gelöscht werden, können sie versteckt auf den Systemen der Kunden verbleiben, und Angreifer, die Zugriff zu diesen Daten haben, können sie verwenden, um gefälschte Zahlungskarten zu generieren und/oder betrügerische Transaktionen durchzuführen.
	1.1.4.b Überprüfen Sie die Softwaredateien von Zahlungsanwendungen und die Konfigurationsdokumentation, um sicherzustellen, dass der Anbieter ein Tool oder Verfahren für Secure Wipes bereitstellt.	
	1.1.4.c Stellen Sie mithilfe forensischer Tools und/oder Methoden sicher, dass das Secure-Wipe-Tool bzw. Verfahren, das vom Anbieter bereitgestellt wurde, Daten auch wirklich entsprechend den Branchenstandards löscht.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
1.1.5 Speichern Sie keine vertraulichen Authentifizierungsdaten auf Systemen des Anbieters. Wenn vertrauliche Authentifizierungsdaten (Daten vor der Autorisierung) zu Debugging- oder Fehlerbehebungszwecken verwendet werden müssen, stellen Sie Folgendes sicher: • Vertrauliche Authentifizierungsdaten werden nur zur Lösung spezifischer Probleme erhoben. • Diese Daten werden an speziellen, bekannten Speicherorten mit eingeschränktem Zugriff aufbewahrt. • Es werden lediglich begrenzte Datenmengen, die zur Lösung eines spezifischen Problems benötigt werden, erhoben. • Vertrauliche Authentifizierungsdaten sind während der Speicherung mit starker Kryptographie verschlüsselt. • Die Daten werden sofort nach der Verwendung sicher gelöscht. Das schließt folgende Stellen ein: - Protokolldateien - Debugging-Dateien - Andere von Kunden erhaltene Datenquellen ***Im Sinne der PCI-DSS-Anforderung 3.2***	**1.1.5.a** Überprüfen Sie die Verfahrensweisen des *Softwareanbieters* bei der Fehlerbehebung beim Kunden, und stellen Sie sicher, dass die Verfahrensweisen folgende Punkte enthalten: • Erhebung vertraulicher Authentifizierungsdaten nur zur Lösung spezifischer Probleme • Speicherung dieser Daten an speziellen, bekannten Speicherorten mit eingeschränktem Zugriff • Erhebung lediglich begrenzter Datenmengen, die zur Lösung eines spezifischen Problems benötigt werden • Verschlüsselung vertraulicher Authentifizierungsdaten während der Speicherung • Sicheres Löschen der Daten unmittelbar nach der Verwendung **1.1.5.b** Machen Sie eine Stichprobe einer kürzlich erfolgten Fehlerbehebungsanfrage von Kunden, und überprüfen Sie, ob die unter 1.1.5.a aufgeführten Punkte eingehalten wurden. **1.1.5.c** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Erhebung sensibler Authentifizierungsdaten nur zur Lösung spezifischer Probleme • Speicherung dieser Daten an speziellen, bekannten Speicherorten mit eingeschränktem Zugriff • Erhebung lediglich begrenzter Datenmengen, die zur Lösung eines spezifischen Problems benötigt werden • Verschlüsselung sensibler Authentifizierungsdaten während der Speicherung • Sicheres Löschen der Daten unmittelbar nach der Verwendung	Wenn der Anbieter Dienste für den Kunden erbringt, die zur Erhebung von vertraulichen Authentifizierungsdaten führen können (beispielsweise zu Fehlerbehebungs- oder Debugging-Zwecken), muss der Anbieter die Datenerhebung auf ein Minimum beschränken und sicherstellen, dass die Daten sicher aufbewahrt und sicher gelöscht werden, sobald sie nicht mehr benötigt werden. Wenn zur Fehlerbehebung eine vorübergehende Konfiguration der Anwendung erforderlich ist, die die Erfassung von SAD (Sensitive Authentication Data, vertrauliche Authentifizierungsdaten) zulässt, sollte die Anwendung sofort nach Fertigstellung der erforderlichen Datenerhebung wieder auf die üblichen sicheren Konfigurationseinstellungen zurückgesetzt werden (d. h. die Erhebung von SAD wird deaktiviert). Sobald die SAD nicht mehr benötigt werden, sollten sie gemäß den branchenüblichen Standards gelöscht werden (beispielsweise mit einem Secure-Wipe-Programm, mit dem sichergestellt wird, dass die Daten unter keinen Umständen wiederhergestellt werden können.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 2: Schutz gespeicherter Karteninhaberdaten

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.1 Der Softwareanbieter muss Kunden Anweisungen zum sicheren Löschen von Karteninhaberdaten nach Ende der vom Kunden festgelegten Aufbewahrungsphase zur Verfügung stellen. ***Im Sinne der PCI-DSS-Anforderung 3.1***	**2.1** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Anweisungen, dass Karteninhaberdaten, die die vom Kunden festgelegte Aufbewahrungsfrist überschritten haben, gelöscht werden müssen • Eine Liste aller Speicherorte, an denen die Zahlungsanwendung Karteninhaberdaten aufbewahrt (sodass der Kunde weiß, wo die zu löschenden Daten sich befinden) • Erforderliche Anweisungen für die Kunden, damit sie Karteninhaberdaten sicher löschen können, wenn sie nicht länger zu juristischen, gesetzlichen oder geschäftlichen Zwecken benötigt werden • Anweisungen zum sicheren Löschen der von der Zahlungsanwendung gespeicherten Karteninhaberdaten, einschließlich der Daten, die in zugrunde liegenden Softwareanwendungen oder Systemen (z. B. Betriebssysteme, Datenbanken usw.) gespeichert werden • Anweisungen zur Konfiguration der zugrunde liegenden Software oder Systeme (z. B. Betriebssysteme, Datenbanken usw.), um einer unbeabsichtigten Erfassung oder Aufbewahrung der Karteninhaberdaten vorzubeugen – beispielsweise durch System-Backups oder Wiederherstellungspunkte	Zur Unterstützung der PCI-DSS-Anforderung 3.1 muss der Anbieter Folgendes bereitstellen: Details zu allen Speicherorten, an denen die Zahlungsanwendung Karteninhaberdaten speichern kann, einschließlich der zugrunde liegenden Software oder Systeme (z. B. Betriebssysteme, Datenbanken usw.), sowie Anweisungen zum sicheren Löschen der Daten aus diesen Speicherorten, sobald die Daten die vom Kunden festgelegte Aufbewahrungsphase überschritten haben. Kunden und Integratoren/Wiederverkäufer müssen außerdem Konfigurationsdetails zu den zugrunde liegenden Systemen und Softwareanwendungen, auf denen die Anwendung ausgeführt wird, erhalten, damit sie sicherstellen können, dass die zugrunde liegenden Systeme keine Karteninhaberdaten ohne ihr Wissen erfassen. Kunden müssen wissen, auf welche Weise die zugrunde liegenden Systeme Daten aus der Anwendung erfassen können, damit sie dies entweder verhindern oder einen ordnungsgemäßen Schutz der Daten sicherstellen können.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.2 Wird die PAN zum Teil verborgen (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), sodass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können? ***Hinweis:*** *Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. bei juristischen Anforderungen und Anforderungen der Kreditkartenunternehmen an POS-Belege.* ***Im Sinne der PCI-DSS-Anforderung 3.3***	**2.2.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Details zu allen Einzelfällen, in denen die PAN abgebildet wird, darunter POS-Geräte, Bildschirme, Protokolle und Belege • Bestätigung, dass die Zahlungsanwendung die PAN standardmäßig in allen Anzeigen maskiert • Anweisungen dazu, wie die Zahlungsanwendung zu konfigurieren ist, damit nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können (umfasst auch die Anzeige der vollständigen PAN).	Die Abbildung der vollständigen PAN beispielsweise auf Computerbildschirmen, Zahlungsbestätigungen, Faxmitteilungen oder Berichten in Papierform kann dazu führen, dass diese Daten in die Hände von unbefugten Personen gelangen, die diese dann in betrügerischer Absicht nutzen. Der Ansatz zur Maskierung sollte immer sicherstellen, dass nur die Mindestanzahl der zum Durchführen einer bestimmten Geschäftsfunktion notwendigen Ziffern dargestellt wird. Wenn beispielsweise nur die letzten vier Ziffern zum Durchführen einer Geschäftsfunktion benötigt werden, maskieren Sie die PAN so, dass die Person, die die Funktion durchführt, nur die letzten vier Ziffern sehen kann. *(Fortsetzung auf der nächsten Seite)*
	2.2.b Installieren Sie die Zahlungsanwendung, und überprüfen Sie alle Instanzen, in denen PAN-Daten abgebildet werden, darunter POS-Geräte, Bildschirme, Protokolle und Belege. Stellen Sie für jeden Fall, in dem die PAN abgebildet wird, sicher, dass die abgebildete PAN maskiert wird.	Ein weiteres Beispiel: Wenn eine Funktion zu Routing-Zwecken Zugriff auf die Bankleitzahl (bank identification number, BIN) benötigt, decken Sie während dieser Funktion nur die BIN-Ziffern (üblicherweise die ersten sechs) auf. Diese Anforderung bezieht sich auf den Schutz von PANs, die auf Bildschirmen, Papierbelegen usw. abgebildet sind, und darf nicht mit der PA-DSS-Anforderung 2.3 zum Schutz der in Dateien, Datenbanken usw. gespeicherten PANs verwechselt werden.
	2.2.c Konfigurieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, so dass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können. Prüfen Sie für jeden Fall, in dem die PAN abgebildet wird, die Anwendungskonfigurationen und die PAN-Anzeige, um sicherzustellen, dass die Anweisungen zum Maskieren der PAN richtig sind und dass nur Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund die mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.3 Machen Sie die PAN überall dort unleserlich, wo sie gespeichert wird (auch auf tragbaren digitalen Medien, Sicherungsmedien und in Protokollen). Setzen Sie dazu eines der folgenden Verfahren ein: • Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden); • Abkürzung (Hashing kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen); • Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden); • Starke Kryptographie mit entsprechenden Schlüsselverwaltungsprozessen und -verfahren. *(Fortsetzung auf der nächsten Seite)*	**2.3.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Details zu allen konfigurierbaren Optionen für jede Methode, die von der Anwendung verwendet wird, um Karteninhaberdaten unleserlich zu machen, und Anweisungen dazu, wie jede Methode für alle Speicherorte zu konfigurieren ist, an denen Karteninhaberdaten von der Zahlungsanwendung gespeichert werden (gemäß der PA-DSS-Anforderung 2.1). • Eine Liste aller Fälle, in denen Karteninhaberdaten für den Kunden ausgegeben werden können, um außerhalb der Zahlungsanwendung gespeichert zu werden, und die Information, dass der Kunde dafür verantwortlich ist, die PAN in solchen Fällen unleserlich zu machen. • Eine Anleitung, für den Fall, dass Debugging-Protokolle aktiviert werden (beipielsweise für Fehlerbehebungszwecke), und die Protokolle eine PAN enthalten, müssen diese in Übereinstimmung mit PCI DSS geschützt werden, deaktiviert werden, sobald die Fehlerbehebung abgeschlossen ist und sicher gelöscht werden, wenn sie nicht mehr benötigt werden.	Mangelnder Schutz der PANs ermöglicht es böswilligen Personen, diese Daten anzuzeigen oder gar herunterzuladen. Karteninhaberdaten können mit unidirektionalen Hash-Funktionen, die auf einer starken Kryptographie basieren, unleserlich gemacht werden. Hash-Funktionen eignen sich, wenn die ursprüngliche Nummer nicht mehr abgerufen werden muss (unidirektionale Hashes können nicht rückgängig gemacht werden). Das Ziel der Abkürzung liegt darin, nur einen Teil (nicht mehr als die ersten sechs und die letzten vier Ziffern) der PAN zu speichern. Ein Index-Token ist ein kryptographisches Token, das die PAN anhand eines bestimmten Index für einen unvorhersehbaren Wert ersetzt. Ein One-Time-Pad ist ein System, bei dem ein per Zufallsgenerator erstellter privater Schlüssel nur einmal benutzt wird, um eine Nachricht zu verschlüsseln, welche anschließend mit einem entsprechenden One-Time-Pad und Schlüssel wieder entschlüsselt wird. *(Fortsetzung auf der nächsten Seite)*
Hinweise: • Für eine Person mit böswilligen Absichten ist es eine relativ einfache Übung, die originalen PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die abgekürzte als auch auf die Hash-Version einer PAN hat. Wenn die gehashte und die abgekürzte Version derselben PAN von einer Zahlungsanwendung generiert wird, müssen zusätzliche Kontrollen eingesetzt werden, um sicherzustellen, dass gehashte und abgekürzte Versionen nicht verglichen werden können, um die originale PAN zu rekonstruieren.	**2.3.b** Überprüfen Sie die zum Schutz der PAN eingesetzte Methode, einschließlich Verschlüsselungsalgorithmen (falls vorhanden). Überprüfen Sie, ob die PAN mit einer der folgenden Methoden unleserlich gemacht wurde: • Unidirektionale Hashes, die auf einer starken Kryptographie basieren • Abkürzung • Index-Token und -Pads (Pads müssen sicher aufbewahrt werden) • Starke Kryptographie mit entsprechenden Schlüsselverwaltungsprozessen und -verfahren	Das Ziel der starken Kryptographie (gemäß der Definition im *PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*) liegt darin, dass die Verschlüsselung auf der Grundlage branchenbewährter und akzeptierter Algorithmen (keine firmeneigenen oder gar individuellen Algorithmen) mit starken kryptographischen Schlüsseln erfolgt.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
• Die PAN muss an jedem Speicherort unleserlich gemacht werden, auch außerhalb der Zahlungsanwendung (z. B. in Protokolldateien, die von der Anwendung ausgegeben werden, um in der Kundenumgebung gespeichert zu werden). ***Im Sinne der PCI-DSS-Anforderung 3.4***	**2.3.c** Wenn die Anwendung sowohl gehashte und abgekürzte Versionen derselben PAN erstellt, prüfen Sie die eingerichteten Methoden darauf hin, dass gehashte und abgekürzte Versionen nicht verglichen werden können, um die originale PAN zu rekonstruieren.	
	2.3.d Überprüfen Sie mehrere Tabellen oder Dateien aus von der Anwendung erstellten oder generierten Datenablagen, um sicherzustellen, dass die PAN unleserlich gemacht wurde.	
	2.3.e Wenn die Anwendung Dateien zur Nutzung außerhalb der Anwendung erstellt oder generiert (z. B. Dateien zum Exportieren oder Backups), einschließlich zum Speichern auf austauschbaren Datenträgern, überprüfen Sie eine Stichprobe dieser Dateien, einschließlich solcher, die auf austauschbaren Dateien erstellt wurden (z. B. Sicherungsbänder), um zu bestätigen, dass die PAN unleserlich gemacht wurde.	
	2.3.f Überprüfen Sie eine Stichprobe von Audit-Protokollen, die von der Anwendung erstellt oder generiert wurden, um zu bestätigen, dass die PAN unleserlich gemacht oder aus den Protokollen entfernt wurde.	
	2.3.g Wenn der Softwareanbieter die PAN speichert (etwa, weil Protokoll- und Debugging-Dateien und andere Datenquellen vom Kunden zu Debugging- oder Fehlerbehebungszwecken bereitgestellt werden), stellen Sie sicher, dass die PAN entsprechend den Anforderungen 2.3.b bis 2.3.f oben unleserlich gemacht wurde.	
2.4 Die Zahlungsanwendung muss sämtliche Schlüssel, die für den Schutz der Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch schützen.	**2.4.a** Überprüfen Sie die Produktdokumentation, und befragen Sie die zuständigen Mitarbeiter, um sicherzustellen, dass Kontrollen implementiert sind, die den Zugriff auf die von der Anwendung verwendeten kryptographischen Schlüssel einschränken.	Kryptographische Schlüssel müssen mittels strenger Sicherheitsvorkehrungen geschützt werden, da Personen, die in deren Besitz gelangen, in der Lage sind, Daten zu entschlüsseln.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
Hinweis: *Diese Anforderung gilt für Schlüssel, die zum Verschlüsseln gespeicherter Karteninhaberdaten verwendet werden, und für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von Schlüsseln zum Verschlüsseln von Daten verwendet werden. Diese Schlüssel zum Verschlüsseln von Schlüsseln müssen mindestens so sicher wie der Schlüssel zum Verschlüsseln von Daten sein.* ***Im Sinne der PCI-DSS-Anforderung 3.5***	**2.4.b** Überprüfen Sie die Systemkonfigurationsdateien, um Folgendes sicherzustellen: • Schlüssel werden im verschlüsselten Format gespeichert. • Schlüssel zum Verschlüsseln von Schlüsseln werden getrennt von Schlüsseln zum Verschlüsseln von Daten aufbewahrt. • Die Schlüssel zum Verschlüsseln von Schlüsseln sind mindestens so sicher wie die Schlüssel zum Verschlüsseln von Daten, zu deren Schutz sie eingesetzt werden.	Die Anforderung an Zahlungsanwendungen, Schlüssel vor Weitergabe und Missbrauch zu schützen, gilt sowohl für Schlüssel zum Verschlüsseln von Daten als auch für Schlüssel zum Verschlüsseln von Schlüsseln. Zwar ist es nicht vorgesehen, dass Schlüssel zum Verschlüsseln von Schlüsseln selbst verschlüsselt werden, allerdings müssen sie gemäß Anforderung 2.4 vor Weitergabe und Missbrauch geschützt werden. Es sollten möglichst wenige Personen Zugriff auf die kryptographischen Schlüssel haben, und vorzugsweise ausschließlich Personen, die als Schlüsselwächter eingesetzt wurden.
	2.4.c Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass Kunden und Integratoren/Wiederverkäufer ausdrücklich auf Folgendes hingewiesen werden: • Schränken Sie den Zugriff auf Schlüssel auf die unbedingt notwendige Anzahl von Wächtern ein. • Bewahren Sie Schlüssel sicher und an so wenigen Orten und in so wenigen Formen wie möglich auf.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.5 Die Zahlungsanwendung muss mindestens folgende Schlüsselverwaltungsprozesse und Verfahrensweisen für zur Verschlüsselung von Karteninhaberdaten verwendete kryptographische Schlüssel implementieren: ***Im Sinne der PCI-DSS-Anforderung 3.6***	**2.5** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Anleitungen zum sicheren Generieren, Verteilen, Schützen, Ändern, Speichern und Zurückziehen/Ersetzen von kryptografischen Schlüsseln, wenn Kunden oder Integratoren/Wiederverkäufer in diesen Schlüsselverwaltungsaktivitäten involviert sind • Ein Beispiel-Schlüsselwächterformular für Schlüsselwächter, das besagt, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen	Die Art und Weise, in der kryptographische Schlüssel verwaltet werden, spielt eine wichtige Rolle für die kontinuierliche Sicherheit der Zahlungsanwendung. Ein guter Schlüsselverwaltungsprozess, ganz gleich, ob als Teil des Verschlüsselungsprodukts manueller oder automatischer Natur, basiert auf Branchenstandards und spricht alle in 2.5.1 bis 2.5.7 aufgeführten Schlüsselelemente an. Durch die Bereitstellung von Anweisungen für Kunden zur sicheren Weitergabe, Speicherung und Aktualisierung von kryptographischen Schlüsseln wird dazu beigetragen, dass Schlüssel ordnungsgemäß verwaltet und nicht an Unbefugte weitergegeben werden. Diese Anforderung gilt für Schlüssel, die zur Verschlüsselung gespeicherter Karteninhaberdaten dienen, sowie für sämtliche zugehörigen Schlüsselverschlüsselungsschlüssel.
2.5.1 Generierung starker kryptographischer Schlüssel	**2.5.1.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass für Kunden und Integratoren/Wiederverkäufer Anweisungen zum sicheren Generieren von kryptographischen Schlüsseln enthalten sind.	Die Zahlungsanwendung muss, so wie unter dem Begriff „starke Kryptographie“ im *PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme* definiert, in der Lage sein, starke Schlüssel zu generieren.
	2.5.1.b Testen Sie die Anwendung, einschließlich der zum Generieren von kryptographischen Schlüsseln verwendeten Methoden, um sicherzustellen, dass mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* starke kryptographische Schlüssel generiert werden.	
2.5.2 Sichere Verteilung kryptographischer Schlüssel	**2.5.2.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass für Kunden und Integratoren/Wiederverkäufer Anweisungen zum sicheren Verteilen kryptographischer Schlüssel enthalten sind.	Die Zahlungsanwendung muss Schlüssel sicher verteilen können, d. h. dass Schlüssel nicht im Klartext und nur mithilfe von autorisierten Prozessen verteilt werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	2.5.2.b Testen Sie die Anwendung, einschließlich der zum Verteilen von kryptographischen Schlüsseln verwendeten Methoden, um sicherzustellen, dass kryptographische Schlüssel mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* sicher verteilt werden.	
2.5.3 Sicheres Speichern kryptographischer Schlüssel	**2.5.3.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass für Kunden und Integratoren/Wiederverkäufer Anweisungen zum sicheren Speichern kryptographischer Schlüssel enthalten sind.	Die Zahlungsanwendung muss Schlüssel sicher speichern können (z. B. indem diese mit einem Schlüssel zum Verschlüsseln von Schlüsseln verschlüsselt werden).
	2.5.3.b Testen Sie die Anwendung, einschließlich der zum Speichern von kryptographischen Schlüsseln verwendeten Methoden, um sicherzustellen, dass kryptographische Schlüssel mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* sicher gespeichert werden.	
2.5.4 Änderungen kryptographischer Schlüssel für Schlüssel, die das Ende ihrer Schlüssellebensdauer erreicht haben (z. B. nach Ablauf einer festgelegten Zeitspanne und/oder nachdem von einem bestimmten Schlüssel eine gegebene Menge an Geheimtext generiert wurde), so wie von dem entsprechenden Anwendungsanbieter oder Schlüsselinhaber definiert und entsprechend bewährter Branchenverfahren und -richtlinien (z. B. *NIST Special Publication 800-57*.	**2.5.4.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Definierte Schlüssellebensdauer für jeden von der Anwendung verwendeten Schlüsseltyp • Verfahren zum Durchsetzen von Schlüsseländerungen am Ende der definierten Schlüssellebensdauer	Die Schlüssellebensdauer beschreibt die Zeitspanne, in der ein bestimmter kryptographischer Schlüssel für den ihm vorbestimmten Zweck eingesetzt werden kann. Bei der Bestimmung der Schlüssellebensdauer müssen unter anderem die Stärke des zugrundeliegenden Algorithmus, die Größe oder Länge des Schlüssels, das Risiko für eine Kompromittierung des Schlüssels und die Vertraulichkeit der zu verschlüsselnden Daten berücksichtigt werden. Das regelmäßige Ändern der Verschlüsselungsschlüssel nach Ablauf der Schlüssellebensdauer ist von zentraler Bedeutung zur Minimierung des Risikos, dass sich Unbefugte Zugriff auf Verschlüsselungsschlüssel verschaffen und damit Daten entschlüsseln.
	2.5.4.b Testen Sie die Anwendung, einschließlich der zum Ändern von kryptographischen Schlüsseln verwendeten Methoden, um sicherzustellen, dass mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* am Ende der definierten Schlüssellebensdauer Schlüsseländerungen durchgeführt werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.5.5 Gegebenenfalls Entfernung oder Austausch von Schlüsseln (z. B. – je nach Bedarf – mittels Archivierung, Vernichtung und/oder Rückruf), wenn die Integrität des Schlüssels gefährdet ist (z. B. Ausscheiden eines Mitarbeiters, der einen Bestandteil des Klartext-Schlüssels kennt, usw.) oder der Verdacht besteht, dass bestimmte Schlüssel kompromittiert wurden. ***Hinweis:*** *Wenn entfernte oder ausgetauschte kryptographische Schlüssel aufbewahrt werden müssen, sind diese Schlüssel auf eine sichere Art und Weise zu archivieren (z. B. mittels Schlüssel zum Verschlüsseln von Schlüsseln) Archivierte kryptographische Schlüssel dürfen nur zu Entschlüsselungs-/Überprüfungszwecken verwendet werden.*	**2.5.5.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Anweisungen, dass Schlüssel entfernt oder ersetzt werden müssen, wenn die Integrität eines Schlüssels gefährdet ist oder wenn bekannt ist bzw. der Verdacht besteht, dass ein Schlüssel kompromittiert wurde. • Verfahren zum Entfernen oder Ersetzen von Schlüsseln (z. B. – je nach Bedarf – mittels Archivierung, Vernichtung und/oder Rückruf) • Verfahren zum Sicherstellen, dass entfernte oder ersetzte kryptographische Schlüssel nicht für Verschlüsselungsvorgänge eingesetzt werden	Schlüssel, die nicht länger genutzt oder gebraucht werden bzw. bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, dass sie kompromittiert wurden, sollten zurückgerufen und/oder vernichtet werden, um sicherzustellen, dass sie nicht mehr eingesetzt werden. Falls solche Schlüssel aufbewahrt werden müssen (z. B. zur Unterstützung archivierter, verschlüsselter Daten), sind sie mittels strenger Sicherheitsvorkehrungen zu schützen. Die Zahlungsanwendung sollte einen Prozess bereitstellen und unterstützen, mit dem Schlüssel ersetzt werden können, deren Ersetzung fällig ist bzw. bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden.
	2.5.5.b Testen Sie die Anwendung, einschließlich der zum Entfernen oder Ersetzen von kryptographischen Schlüsseln verwendeten Methoden, um sicherzustellen, dass die Schlüssel mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* entfernt oder ersetzt werden (z. B. – je nach Bedarf – mittels Archivierung, Vernichtung und/oder Rückruf).	
	2.5.5.c Testen Sie die Anwendung mit den entfernten/ersetzten Schlüsseln, um zu überprüfen, ob durch Befolgung der Anweisungen im *PA-DSS-Implementierungshandbuch* sichergestellt wird, dass die Anwendung keine entfernten oder ersetzten Schlüssel für Verschlüsselungsvorgänge einsetzt.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.5.6 Wenn die Zahlungsanwendung manuelle Verwaltungsvorgänge kryptographischer Klartext-Schlüssel unterstützt, müssen diese Vorgänge eine geteilte Kenntnis und duale Kontrollen durchsetzen. ***Hinweis:*** *Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen das Generieren, Übertragen, Laden, Speichern und Vernichten von Schlüsseln.*	**2.5.6.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Details zu allen manuellen Verwaltungsvorgängen kryptographischer Klartext-Schlüssel, die von der Anwendung unterstützt werden • Anweisungen zum Durchsetzen von geteilter Kenntnis und dualer Kontrolle für solche Vorgänge	Geteiltes Wissen und duale Schlüsselkontrollen werden genutzt, um zu verhindern, dass eine Person Zugriff auf den vollständigen Schlüssel hat. Diese Kontrolle gilt für manuelle Schlüsselverwaltungsverfahren. Geteiltes Wissen bedeutet, dass die Bestandteile eines Schlüssels auf mindestens zwei Personen aufgeteilt werden. Jede Person kennt nur den eigenen Bestandteil, und der ursprüngliche kryptographische Schlüssel kann nicht mithilfe der einzelnen Bestandteile rekonstruiert werden. Nach dem Prinzip der doppelten Kontrolle sind mindestens zwei Personen für die Durchführung einer Aufgabe erforderlich, und keine Person kann die Authentifizierungsunterlagen einer anderen Person aufrufen oder verwenden.
	2.5.6.b Testen Sie die Anwendung einschließlich aller manuellen Verwaltungsvorgänge kryptographischer Klartext-Schlüssel, um sicherzustellen, dass mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* festgelegt wird, dass für alle manuellen Verwaltungsvorgänge der kryptographischen Klartext-Schlüssel geteiltes Wissen und duale Schlüsselkontrolle erforderlich sind.	
2.5.7 Verhindern der unbefugten Ersetzung kryptographischer Schlüssel	**2.5.7.a** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass für Kunden und Integratoren/Wiederverkäufer Anweisungen zum Verhindern der unbefugten Ersetzung kryptographischer Schlüssel enthalten sind.	In der Zahlungsanwendung sollten Methoden für Benutzer der Anwendung definiert werden, um sicherzustellen, dass Schlüssel nur von autorisierten Personen ersetzt werden können. Die Anwendungskonfiguration sollte keinen Ersatz von Schlüsseln autorisieren, die aus nicht zugelassenen Quellen oder unerwarteten Prozessen stammen.
	2.5.7.b Testen Sie die Anwendung einschließlich aller Methoden zum Ersatz von Schlüsseln, um sicherzustellen, dass mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* die unbefugte Ersetzung kryptographischer Schlüssel verhindert wird.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
2.6 Stellen Sie einen Mechanismus bereit, mit dem alle kryptographischen Schlüsselmaterialien oder Kryptogramme, die von der Zahlungsanwendung gespeichert wurden, unwiderruflich und gemäß den Branchenstandards gelöscht werden. Hierbei handelt es sich um kryptographische Schlüssel, die zur Verschlüsselung oder Verifizierung von Karteninhaberdaten verwendet werden. ***Hinweis:*** *Diese Anforderung gilt nur, wenn die Zahlungsanwendung oder vorherige Versionen der Zahlungsanwendung kryptographische Schlüsselmaterialien oder Kryptogramme zur Verschlüsselung von Karteninhaberdaten verwendet bzw. verwendet haben.* ***Im Sinne der PCI-DSS-Anforderung 3.6***	**2.6.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer in der Dokumentation enthalten sind: • Verfahren, die Details zur Verwendung der Anwendung enthalten, oder mit der Anwendung bereitgestellte Verfahrensweisen zum unwiderruflichen Löschen kryptographischen Materials • Die Angabe, dass kryptographische Schlüsselmaterialien unwiderruflich gelöscht werden sollten, wenn Schlüssel nicht mehr verwendet werden – und gemäß den Schlüsselverwaltungsanforderungen in PCI-DSS • Verfahren zum erneuten Verschlüsseln von Verlaufsdaten mit neuen Schlüsseln, einschließlich Verfahren zum Aufrechterhalten der Sicherheit von Daten im Klartext während des Entschlüsselungs-/Neuverschlüsselungsvorgangs	Anbieter sollten einen Mechanismus für ihre Kunden bereitstellen, mit dem sie alte kryptographische Materialien sicher löschen können, wenn diese nicht mehr benötigt werden. Hinweis: Das Löschen alter kryptographischer Materialien liegt im Ermessen des Kunden. Kryptographische Schlüsselmaterialien und/oder Kryptogramme können unter anderen mithilfe folgender Tools oder Verfahren unwiderruflich gelöscht werden: • Sicheres Löschen, wie es beispielsweise in der Liste zugelassener Produkte der National Security Agency oder anderen staatlichen oder nationalen Standards oder Regelungen vorgegeben wird. • Löschen von Schlüsseln zum Verschlüsseln von Schlüsseln (Englisch: key-encrypting key, KEK), vorausgesetzt, dass Schlüssel zum Verschlüsseln von Schlüsseln unter den gelöschten KEK nur in verschlüsselter Form existieren.
	2.6.b Überprüfen Sie die fertige Anwendung, und stellen Sie sicher, dass der Anbieter mit der Anwendung ein Tool und/oder Verfahren zum unwiderruflichen Löschen kryptographischer Materialien bereitstellt.	
	2.6.c Testen Sie die Anwendung, einschließlich der bereitgestellten Methoden zum unwiderruflichen Löschen kryptographischer Schlüsselmaterialien. Stellen Sie mithilfe forensischer Tools und/oder Methoden sicher, dass das vom Anbieter bereitgestellte Secure-Wipe-Tool bzw. -Verfahren das verschlüsselte Material gemäß den Branchenstandards tatsächlich unwiderruflich löscht.	
	2.6.d Testen Sie die Methoden zum erneuten Verschlüsseln von Verlaufsdaten mit neuen Schlüsseln, um sicherzustellen, dass Verlaufsdaten mithilfe der Anweisungen im *PA-DSS-Implementierungshandbuch* mit neuen Schlüsseln erfolgreich erneut verschlüsselt werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 3: Bereitstellen sicherer Authentifizierungsfunktionen

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.1 Die Zahlungsanwendung muss die Verwendung einmaliger Benutzer-IDs und einer sicheren Authentifizierung für sämtliche Verwaltungszugriffe sowie Zugriffe auf Karteninhaberdaten unterstützen und durchsetzen. Bei Abschluss der Installation sowie bei nachträglichen Änderungen nach der Installation muss eine sichere Authentifizierung für alle Konten durchgesetzt werden, die von der Anwendung generiert oder verwaltet werden. Die Anwendung muss die nachfolgenden Punkte 3.1.1 bis 3.1.11 durchsetzen: ***Hinweis:*** *Der in der gesamten Anforderung 3 verwendete Begriff „nachträgliche Änderungen" bezieht sich auf alle Anwendungsänderungen, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt werden, auf Änderungen an bestehenden Kontokonfigurationen und auf Änderungen, durch die neue Konten generiert oder bestehende Konten neu erstellt werden.* ***Hinweis:*** *Diese Kennwortkontrollen sind nicht zur Anwendung durch Mitarbeiter vorgesehen, die immer nur auf eine Kartennummer für eine einzige Transaktion Zugriff haben. Diese Kontrollen gelten für Zugriffe durch Personal mit administrativen Funktionen, für den Zugriff auf Systeme mit Karteninhaberdaten und für einen durch die Zahlungsanwendung kontrollierten Zugriff.* *Diese Anforderung findet Anwendung bei der Zahlungsanwendung und allen damit in Zusammenhang stehenden Tools zur Anzeige von oder zum Zugriff auf Karteninhaberdaten.* ***Im Sinne der PCI-DSS-Anforderungen 8.1 und 8.2***	**3.1.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, um Folgendes für Kunden und Integratoren/Wiederverkäufer sicherzustellen: • Es wird klar und unmissverständlich beschrieben, wie die Zahlungsanwendung eine starke Authentifizierung für alle Authentifizierungsinformationen durchsetzt, die die Anwendung generiert oder verwaltet, indem: - Sichere Änderungen der Authentifizierungsinformationen bei Abschluss der Installation entsprechend den Anforderungen 3.1.1 bis 3.1.11 durchgesetzt werden - Sichere Änderungen an den Authentifizierungsinformationen für sämtliche nachträgliche Änderungen (nach der Installation) entsprechend den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 durchgesetzt werden • Es wird darauf hingewiesen, dass zur Aufrechterhaltung der PCI-DSS-Konformität für alle Änderungen, die an Authentifizierungskonfigurationen vorgenommen werden, überprüft werden muss, dass sie Authentifizierungsmethoden bereitstellen, die mindestens so streng wie die PCI-DSS-Anforderungen sind. • Es wird empfohlen, eine sichere Authentifizierung für alle Standdardkonten in der Umgebung zu nutzen. • Jeglichen Standardkonten, die nicht verwendet werden, wird eine sichere Authentifizierung zugewiesen, und die Konten werden dann deaktiviert oder nicht verwendet. • Für alle Authentifizierungsinformationen, die von der Zahlungsanwendung verwendet werden (jedoch nicht von der Anwendung generiert oder verwaltet werden), sind klare und unmissverständliche Anweisungen dazu enthalten, wie bei Abschluss der Installation und für sämtliche Änderungen nach der Installation die Authentifizierungsinformationen geändert und starke Authentifizierungen gemäß den Anforderungen 3.1.1 bis 3.1.11 unten für alle Konten auf Anwendungsebene und alle Benutzerkonten mit administrativem Zugriff sowie für jegliche Konten mit Zugriff auf Karteninhaberdaten generiert werden. • Es werden alle Rollen und Standardkonten mit Verwaltungszugriff innerhalb der Anwendung ermittelt.	Indem sichergestellt wird, dass jeder Benutzer eindeutig identifiziert ist – anstatt eine Benutzer-ID für mehrere Mitarbeiter zu verwenden –, werden von der Anwendung die PCI-DSS-Anforderungen erfüllt, die vorgeben, dass Einzelne für ihre Handlungen zur Rechenschaft gezogen werden können und pro Mitarbeiter ein effektiver Audit-Trail erstellt wird. Hierdurch können die Problembewältigung sowie der Einsatz von Vorbeugungsmaßnahmen im Falle von Missbrauch oder böswilligen Absichten beschleunigt werden. Wenn die sichere Authentifizierung zusammen mit eindeutigen IDs eingesetzt wird, hilft sie dabei, die Benutzer-IDs vor Angriffen zu schützen, da der Angreifer sowohl die eindeutige ID als auch das Kennwort (oder andere verwendete Authentifizierungselemente) kennen muss.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.1.1 Die Zahlungsanwendung nutzt keine Standard-Administratorkonten für andere notwendige Software (oder erfordert deren Verwendung). (Beispielsweise darf die Zahlungsanwendungen nicht das Standard-Administratorkonto für die Datenbank nutzen.) ***Im Sinne der PCI-DSS-Anforderung 2.1***	**3.1.1** Installieren und konfigurieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*. Dazu gehört auch das Konfigurieren sämtlicher Administratorkonten für die gesamte erforderliche Software. Testen Sie die Zahlungsanwendung, um sicherzustellen, dass die Zahlungsanwendung keine Standard-Administratorkonten für benötigte Software verwendet (oder deren Verwendung erfordert).	Standard-Administratorkonten (und Standardkennwörter) sind öffentliches Wissen und jedem bekannt, der mit der Zahlungsanwendung oder den zugrunde liegenden Systemkomponenten vertraut ist. Wenn Standard-Administratorkonten und -kennwörter verwendet werden, können unbefugte Personen auf die Anwendung und Daten zugreifen, indem sie sich einfach mit allgemein bekannten Anmeldeinformationen anmelden.
3.1.2 Die Anwendung muss durchsetzen, dass alle Standardkennwörter der Anwendung für alle Konten, die von der Anwendung generiert oder verwaltet werden, bei Abschluss der Installation oder im Fall von nachträglichen Änderungen nach der Installation geändert werden. Dies gilt für alle Konten, einschließlich Benutzerkonten, Anwendungs- und Servicekonten und Konten, die vom Anbieter für den Support verwendet werden. ***Hinweis:*** *Diese Anforderung kann nicht durch das Festlegen eines Benutzerprozesses oder mithilfe von Anweisungen im PA-DSS-Implementierungshandbuch erfüllt werden. Bei Abschluss der Installation und nach nachträglichen Änderungen muss die Anwendung rigoros verhindern, dass Standard- oder integrierte Konten verwendet werden, bevor das Standardkennwort geändert wurde.* ***Im Sinne der PCI-DSS-Anforderung 2.1***	**3.1.2** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt: **3.1.2.a** Installieren Sie die Anwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, überprüfen Sie die Konto- und Kennworteinstellungen, und versuchen Sie, sämtliche Standardkennwörter zu verwenden, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs das Ändern aller Standardkennwörter der Zahlungsanwendung durchsetzt. **3.1.2.b** Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Konto- und Kennworteinstellungen, und versuchen Sie, sämtliche Standardkennwörter zu verwenden, um sicherzustellen, dass die Anwendung das Ändern der Standardkennwörter nach Abschluss einer Änderung durchsetzt.	Wenn die Anwendung das Ändern von Standardkennwörtern nicht durchsetzt, kann jede Person, die die Standardeinstellungen kennt, darauf zugreifen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.1.3 Die Zahlungsanwendung weist Benutzerkonten eine eindeutige ID zu. ***Im Sinne der PCI-DSS-Anforderung 8.1.1***	**3.1.3** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn jedem Benutzer eine eindeutige Benutzer-ID zugewiesen wird, ist es möglich, Zugriffe und Aktivitäten innerhalb der Zahlungsanwendung zu der Person zurückzuverfolgen, die sie durchgeführt hat.
	3.1.3.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und versuchen Sie, verschiedene Anwendungskonten mit derselben Benutzer-ID zu erstellen, um sicherzustellen, dass die Zahlungsanwendung bei Abschluss des Installationsvorgangs nur eindeutige Benutzer-IDs zuweist.	
	3.1.3.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass nach Abschluss einer Änderung eindeutige Benutzer-IDs für alle Konten zugewiesen werden.	
3.1.4 Die Zahlungsanwendung setzt mindestens eine der folgenden Methoden zur Authentifizierung aller Benutzer ein: ▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; ▪ etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; ▪ Etwas, das Sie sind, wie zum Beispiel biometrische Daten. ***Im Sinne der PCI-DSS-Anforderungen 8.2***	**3.1.4** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn diese Authentifizierungsmethoden zusammen mit eindeutigen IDs eingesetzt werden, helfen sie dabei, die Benutzer-IDs vor Angriffen zu schützen, da der Angreifer sowohl die eindeutige ID als auch das Kennwort (oder andere verwendete Authentifizierungselemente) kennen muss.
	3.1.4.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und testen Sie die Authentifizierungsmethoden, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs für alle Konten mindestens eine der definierten Authentifizierungsmethoden erfordert.	
	3.1.4.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Testen Sie für alle Änderungstypen, die vorgenommen wurden, die Authentifizierungsmethoden, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung für alle Konten mindestens eine der definierten Authentifizierungsmethoden erfordert.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.1.5 Die Zahlungsanwendung erfordert oder verwendet **keine** Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung. ***Im Sinne der PCI-DSS-Anforderung 8.5***	**3.1.5** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn mehrere Benutzer gemeinsam dieselben Authentifizierungsinformationen benutzen (z. B. Benutzerkonto und Kennwort), ist es nicht mehr möglich, Einzelne für ihre Aktionen zur Rechenschaft zu ziehen oder effektive Protokolle darüber zu führen, da die Aktion von jeder Person, die die Authentifizierungsinformationen kennt, hätte durchgeführt werden können.
	3.1.5.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, überprüfen Sie die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs keine Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung erfordert oder verwendet.	
	3.1.5.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung keine Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung erfordert oder verwendet.	
3.1.6 Die Zahlungsanwendung setzt für Kennwörter Folgendes voraus: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden. Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.	**3.1.6** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Angreifer versuchen häufig, Konten mit schwachen oder fehlenden Kennwörtern zu finden, um sich Zugriff auf eine Anwendung oder ein System zu verschaffen. Wenn Kennwörter kurz oder leicht zu erraten sind, ist es für einen Angreifer relativ einfach, diese schwachen Konten zu finden und sich unter dem Deckmantel einer gültigen Benutzer-ID unbefugten Zugriff auf eine Anwendung oder ein System zu verschaffen. *(Fortsetzung auf der nächsten Seite)*
	3.1.6.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Kontoeinstellungen, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs voraussetzt, dass Kennwörter mindestens die folgende Komplexität und Stärke aufweisen: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	3.1.6.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung voraussetzt, dass Kennwörter mindestens die folgende Komplexität und Stärke aufweisen: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.	Diese Anforderung legt fest, dass die Mindestlänge für Kennwörter sieben Zeichen ist, und dass sowohl numerische als auch alphabetische Zeichen verwendet werden sollten. Wenn diese Mindestanforderung aufgrund technischer Beschränkungen nicht erfüllt werden kann, können Einheiten zur Evaluierung der Alternative auf „gleichwertige Stärke“ setzen. In NIST SP 800-63-1 ist „Entropie“ als „ein Maß der Schwierigkeit, ein Kennwort oder einen Schlüssel zu erraten oder zu bestimmen“ definiert. Dieses Dokument und andere, in denen die „Entropie von Kennwörtern“ behandelt wird, bieten zusätzliche Informationen zum Entropiewert und zu gleichwertiger Kennwortstärke für Kennwörter mit unterschiedlichen Mindestformaten.
	3.1.6.c Wenn die Anwendung andere Mindestanforderungen an den Zeichensatz und die Länge eines Kennworts stellt, berechnen Sie die Entropie der Kennwörter, die die Anwendung erfordert, und stellen Sie sicher, dass sie mindestens den oben angegebenen Parametern entspricht (d. h. Mindestlänge von sieben Zeichen mit sowohl numerischen als auch alphabetischen Zeichen).	
3.1.7 Die Zahlungsanwendung setzt voraus, dass die Benutzerkennwörter mindestens einmal alle 90 Tage geändert werden. ***Im Sinne der PCI-DSS-Anforderung 8.2.4***	**3.1.7** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn Kennwörter/Kennsätzeüber einen langen Zeitraum hinweg gültig sind, ohne geändert werden zu müssen, haben Angreifer länger Zeit, das Kennwort/den Kennsatzherauszufinden.
	3.1.7.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Kontoeinstellungen, um sicherzustellen, dass die Zahlungsanwendung bei Abschluss des Installationsvorgangs voraussetzt, dass die Benutzerkennwörter mindestens einmal alle 90 Tage geändert werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	3.1.7.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung voraussetzt, dass die Benutzerkennwörter mindestens einmal alle 90 Tage geändert werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.1.8 Die Zahlungsanwendung speichert den Kennwortverlauf und setzt voraus, dass sich ein neues Kennwort mindestens von den letzten vier verwendeten Kennwörtern unterscheidet. ***Im Sinne der PCI-DSS-Anforderung 8.2.5***	**3.1.8** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn der Kennwortverlauf nicht aufgezeichnet wird, sinkt die Wirksamkeit der erzwungenen Kennwortänderungen, da alte Kennwörter immer wieder neu verwendet werden können. Wenn Kennwörter über einen bestimmten Zeitraum hinweg nicht wiederverwendet werden dürfen, sinkt die Wahrscheinlichkeit, dass Kennwörter, die erraten oder mithilfe der Brute-Force-Methode ermittelt wurden, in der Zukunft wiederverwendet werden.
	3.1.8.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Kontoeinstellungen, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs den Kennwortverlauf aufzeichnet und voraussetzt, dass sich ein neues Kennwort mindestens von den letzten vier verwendeten Kennwörtern unterscheidet.	
	3.1.8.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung den Kennwortverlauf aufzeichnet und voraussetzt, dass sich ein neues Kennwort mindestens von den letzten vier verwendeten Kennwörtern unterscheidet.	
3.1.9 Die Zahlungsanwendung begrenzt die wiederholten Zugriffsversuche durch Sperren des Benutzerkontos nach spätestens sechs ungültigen Anmeldeversuchen. ***Im Sinne der PCI-DSS-Anforderung 8.1.6***	**3.1.9** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Ohne implementierte Mechanismen für Kontosperrungen kann ein Angreifer fortwährend versuchen, ein Kennwort über manuelle oder automatisierte Tools zu erraten (z. B. Kennwort-Cracking-Tools), bis er letztendlich Erfolg hatte und sich Zugriff auf das Konto eines Benutzers verschafft hat.
	3.1.9.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Kontoeinstellungen, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs Benutzerkonten nach spätestens sechs ungültigen Anmeldeversuchen sperrt.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	3.1.9.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung Benutzerkonten nach spätestens sechs ungültigen Anmeldeversuchen sperrt.	
3.1.10 Die Zahlungsanwendung legt die Aussperrdauer auf mindestens 30 Minuten fest, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann. ***Im Sinne der PCI-DSS-Anforderung 8.1.7***	**3.1.10** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn ein Konto gesperrt wurde, weil eine Person versucht hat, ein Kennwort zu erraten, unterbinden Steuerungen zur Hinauszögerung der Reaktivierung dieser gesperrten Konten, dass ein Angreifer weiter versucht, das Kennwort zu erraten (während eines Zeitraums von mindestens 30 Minuten können sie keine weiteren Eingaben tätigen, bis das Konto erneut aktiviert wird.) Darüber hinaus kann der Administrator, sollte die erneute Aktivierung beantragt werden müssen, nachprüfen, ob die Reaktivierung tatsächlich vom Kontoinhaber beantragt wird.
	3.1.10.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Kontoeinstellungen, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs die Aussperrdauer auf mindestens 30 Minuten festlegt, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.	
	3.1.10.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung die Aussperrdauer auf mindestens 30 Minuten festlegt, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.1.11 Die Anwendung erfordert, dass sich die Benutzer nach einer mehr als 15-minütigen Inaktivität innerhalb einer Sitzung in der Zahlungsanwendung erneut authentifizieren und die Sitzung reaktivieren. ***Im Sinne der PCI-DSS-Anforderung 8.1.8***	**3.1.11** Testen Sie die Anwendung für alle von der Anwendung generierten oder verwalteten Konten wie folgt:	Wenn sich ein Benutzer von seiner Sitzung mit Zugriff auf die Kartenanwendung entfernt, kann die Verbindung von anderen in Abwesenheit des Benutzers dazu verwendet werden, sich unbefugten Zugriff auf dessen Konto zu verschaffen und/oder es missbräuchlich einzusetzen.
	3.1.11.a Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Kontoeinstellungen, um sicherzustellen, dass die Anwendung bei Abschluss des Installationsvorgangs die Inaktivitätszeit auf 15 Minuten oder weniger begrenzt.	
	3.1.11.b Testen Sie alle Funktionen der Anwendung, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontokonfigurationen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Kontoeinstellungen, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass die Anwendung nach Abschluss einer Änderung die Inaktivitätszeit auf 15 Minuten oder weniger begrenzt.	
3.2 Der Softwareanbieter muss die Kunden, die Zugriff auf PCs, Server und Datenbanken mit Zahlungsanwendungen haben, anweisen, dass eine eindeutige Benutzer-ID und sichere Authentifizierung erforderlich ist. ***Im Sinne der PCI-DSS-Anforderungen 8.1 und 8.2***	**3.2** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, um sicherzugehen, dass Kunden und Integratoren/Wiederverkäufer darauf hingewiesen werden, den Zugriff über eindeutige Benutzer-IDs und PCI-DSS-konforme, sichere Authentifizierungsmethoden für sämtliche PCs, Server und Datenbanken mit Zahlungsanwendungen und Karteninhaberdaten zu steuern.	Wenn die Anwendung auf Systemen installiert wird bzw. wenn Systeme auf die Anwendung zugreifen, die keine starken Identifizierungs- und Authentifizierungskontrollen durchsetzen, könnte die von der Anwendung bereitgestellte Methode zur starken Authentifizierung umgangen werden, wodurch unsicherer Zugriff ermöglicht wird.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.3 Sichern Sie alle Kennwörter der Zahlungsanwendung (einschließlich der Kennwörter für Benutzer- und Anwendungskonten) während der Übertragungs- und Speichervorgänge. ***Im Sinne der PCI-DSS-Anforderung 8.2.1***	**3.**3 Führen Sie die folgenden Schritte aus:	Wenn die Kennwörter der Zahlungsanwendung innerhalb des Netzwerks unverschlüsselt gespeichert oder übertragen werden, kann ein Angreifer Kennwörter mithilfe eines „Sniffers“ leicht abfangen oder direkt auf die Kennwörter in den Dateien zugreifen, in denen sie gespeichert werden, und diese gestohlenen Daten verwenden, um sich unbefugten Zugriff zu verschaffen. Durch die Verknüpfung einer eindeutigen Eingabevariablen mit jedem Kennwort, bevor der Hashing-Algorithmus angewendet wird, wird die Effektivität von Brute-Force-Angriffen verringert. Starke unidirektionale kryptographische Algorithmen, die für das Kennwort-Hashing geeignet sind, umfassen z. B. PBKDF2 und Bcrypt.
3.3.1 Machen Sie alle Kennwörter von Zahlungsanwendungen während der Übertragung mithilfe starker Kryptographie unleserlich.	**3.3.1.a** Überprüfen Sie die Dokumentation und die Anwendungskonfigurationen des Anbieters, um sicherzustellen, dass alle Kennwörter bei jeder Übertragung mithilfe starker Kryptographie unleserlich gemacht werden.	
	3.3.1.b Überprüfen Sie für alle Arten von Anwendungskennwörtern die Übertragung von Kennwörtern (beispielsweise, indem Sie sich von einem anderem System bei der Anwendung anmelden und die Anwendung auf anderen Systemen authentifizieren), um sicherzustellen, dass alle Kennwörter bei jeder Übertragung mithilfe starker Kryptographie unleserlich gemacht werden.	
3.3.2 Verwenden Sie einen starken, unidirektionalen kryptographischen Algorithmus, der auf bewährten Standards basiert, um alle Kennwörter der Zahlungsanwendung während der Speicherung unleserlich zu machen. Für jedes Kennwort muss eine eindeutige Eingabevariable mit dem Kennwort verknüpft werden, bevor der kryptographische Algorithmus angewendet wird. ***Hinweis:*** *Für die Eingabevariable muss kein unvorhersehbarer oder geheimer Wert verwendet werden.*	**3.3.2.a** Überprüfen Sie die Dokumentation und die Anwendungskonfigurationen des Anbieters, um Folgendes sicherzustellen**:** • Gespeicherte Kennwörter werden mit einem starken, unidirektionalen kryptographischen Algorithmus, der auf bewährten Standards basiert, unleserlich gemacht. • Eine eindeutige Eingabevariable wird mit jedem Kennwort verknüpft, bevor der kryptographische Algorithmus angewendet wird.	
	3.3.2.b Identifizieren Sie für alle Arten von Anwendungskennwörtern die Speicherorte, an denen die Anwendung Kennwörter aufbewahren kann, einschließlich Speicherorten innerhalb der Anwendung, in zugrunde liegenden Systemen, Protokolldateien, Registrierungseinstellungen usw. Überprüfen Sie für alle Speicherorte und Arten von Kennwörtern die gespeicherten Kennwortdateien, um sicherzustellen, dass die Kennwörter während der Speicherung stets mit einem starken, unidirektionalen kryptographischen Algorithmus und einer eindeutigen Eingabevariable unleserlich gemacht werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
3.4 Die Zahlungsanwendung muss den Zugriff auf erforderliche Funktionen/Ressourcen einschränken und das Prinzip der Mindestberechtigungen für integrierte Konten durchsetzen: • Standardmäßig haben alle Anwendungs-/Servicekonten nur Zugriff auf die Funktionen/Ressourcen, die für die Zwecke des Anwendungs-/Servicekontos speziell erforderlich sind. • Standardmäßig ist allen Anwendungs-/Servicekonten die minimale Berechtigungsstufe für jede Funktion/Ressource zugewiesen, die für das Anwendungs-/Servicekonto erforderlich ist. ***Im Sinne der PCI-DSS-Anforderung 7***	**3.4.a** Installieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und überprüfen Sie die Einstellungen für die integrierten Konten, um sicherzustellen, dass bei Abschluss des Installationsvorgangs Folgendes zutrifft: • Alle Anwendungs-/Servicekonten haben nur auf die Funktionen/Ressourcen Zugriff, die für die Zwecke des Anwendungs-/Servicekontos speziell erforderlich sind. • Allen Anwendungs-/Servicekonten ist die minimale Berechtigungsstufe für jede Funktion/Ressource zugewiesen, die für das Anwendungs-/Servicekonto erforderlich ist.	Um Zugriff auf Karteninhaberdaten und vertrauliche Funktionen auf die Konten zu beschränken, die ihn benötigen, müssen die Zugriffsanforderungen und die erforderliche Berechtigungsstufe für jedes integrierte Konto so festgelegt werden, dass die zugewiesenen Funktionen ausgeführt werden können, ohne dass zusätzliche, unnötige Zugriffsrechte oder Berechtigungsstufen gewährt werden. Das Zuweisen von Mindestberechtigungen trägt dazu bei zu verhindern, dass Benutzer ohne ausreichende Anwendungskenntnisse fälschlicherweise oder versehentlich die Anwendungskonfiguration oder ihre Sicherheitseinstellungen ändern. Durch die Durchsetzung der Mindestberechtigung wird auch das Ausmaß des Schadens minimiert, der entsteht, wenn eine nicht autorisierte Person Zugriff auf eine Benutzer-ID erhält.
	3.4.b Testen Sie alle Funktionen der Anwendung, die zu Änderungen an integrierten Konten führen – einschließlich Änderungen, die dazu führen, dass Benutzerkonten auf die Standardeinstellungen zurückgesetzt, bestehende Kontoeinstellungen geändert, neue Konten generiert und bestehende Konten neu erstellt werden. Überprüfen Sie für alle Änderungstypen, die vorgenommen wurden, die Einstellungen der integrierten Konten, und testen Sie die Anwendungsfunktionalität, um sicherzustellen, dass nach Abschluss einer Änderung Folgendes zutrifft: • Alle Anwendungs-/Servicekonten haben nur auf die Funktionen/Ressourcen Zugriff, die für die Zwecke des Anwendungs-/Servicekontos speziell erforderlich sind. • Allen Anwendungs-/Servicekonten ist die minimale Berechtigungsstufe für jede Funktion/Ressource zugewiesen, die für das Anwendungs-/Servicekonto erforderlich ist.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 4: Protokollieren der Aktivität von Zahlungsanwendungen

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
4.1 Nach Abschluss des Installationsvorgangs muss die Standardinstallation der Zahlungsanwendung den gesamten Benutzerzugriff protokollieren und in der Lage sein, sämtliche Aktivitäten den einzelnen Benutzern zuzuweisen. ***Im Sinne der PCI-DSS-Anforderung 10.1***	**4.1.a** Installieren Sie die Zahlungsanwendung. Testen Sie die Anwendung, und stellen Sie sicher, dass die Audit-Trails der Zahlungsanwendung nach der Installation automatisch aktiviert werden.	Es ist von entscheidender Bedeutung, dass die Zahlungsanwendung über einen Prozess oder Mechanismus verfügt, der die Anwendungsressourcen, auf die zugriffen wurde, den Benutzern zuordnet, der Prüfprotokolle generiert und die Möglichkeit bietet, verdächtige Aktivitäten auf einen bestimmten Benutzer zurückzuverfolgen. Ursachenanalyseteams eines Vorfalls verlassen sich stark auf diese Protokolle zur Einleitung der Untersuchung.
	4.1.b Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, um sicherzustellen, dass die folgenden Anweisungen enthalten sind: • Wie die Anwendung zu installieren ist, damit die Protokolle nach Abschluss des Installationsvorgangs automatisch konfiguriert und aktiviert werden • Wie PCI-DSS-konforme Protokolleinstellungen gemäß den nachstehenden PA-DSS-Anforderungen 4.2, 4.3 und 4.4 für sämtliche Protokollierungsoptionen einzurichten sind, die vom Kunden nach der Installation konfiguriert werden können • Die Anweisung, dass Protokolle nicht deaktiviert werden sollten, da es andernfalls zu einer Nichtkonformität mit dem PCI-DSS kommt • Wie PCI-DSS-konforme Protokolleinstellungen von Drittanbieter-Softwarekomponenten, die zusammen mit der Zahlungsanwendung bereitgestellt werden oder die für die Zahlungsanwendung erforderlich sind, für sämtliche Protokollierungsoptionen einzurichten sind, die vom Kunden nach der Installation konfiguriert werden können	
4.2 Die Zahlungsanwendung muss über Audit-Trail-Daten verfügen, mit denen folgende Ereignisse zurückverfolgt werden können: ***Im Sinne der PCI-DSS-Anforderung 10.2***	**4.2** Testen Sie die Zahlungsanwendung, indem Sie die Prüfprotokolleinstellungen und Prüfprotokollausgabe der Zahlungsanwendung überprüfen und Folgendes durchführen:	Die Protokollierung der Ereignisse unter 4.2.1 – 4.2.7 versetzt ein Unternehmen in die Lage, potenziell schädliche Aktivitäten zu erkennen und nachzuverfolgen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
4.2.1 Alle individuellen Benutzerzugriffe auf Karteninhaberdaten über die Anwendung	**4.2.1** Prüfen Sie, ob alle individuellen Zugriffe auf Karteninhaberdaten über die Zahlungsanwendung protokolliert werden.	Angreifer könnten über die Anwendung von einem Benutzerkonto mit Zugriff auf Karteninhaberdaten erfahren oder sie könnten ein neues, nicht genehmigtes Konto einrichten, um sich Zugriff auf die Karteninhaberdaten zu verschaffen. Einträge über alle einzelnen Zugriffe auf Karteninhaberdaten können Aufschluss darauf geben, welche Konten möglicherweise gefährdet oder missbräuchlich eingesetzt worden sind.
4.2.2 Alle von einer Person mit administrativen Rechten vorgenommen Aktionen, wie von der Anwendung vorgesehen	**4.2.2** Überprüfen Sie, ob alle von Personen mit administrativen Rechten an der Zahlungsanwendung vorgenommen Aktionen protokolliert werden.	Konten mit erweiterten Rechten, wie etwa das Administratorkonto, können die Sicherheit und die betriebliche Funktionalität der Anwendung ernstlich gefährden. Ohne ein Protokoll über die durchgeführten Aktivitäten kann ein Unternehmen Probleme, die durch einen Fehler des Administrators oder durch den Missbrauch von Rechten entstanden sind, nicht bis zu der entsprechenden Aktion oder der verantwortlichen Person zurückverfolgen.
4.2.3 Zugriff auf die Audit-Trails der Anwendung, die von oder innerhalb der Anwendung verwaltet werden	**4.2.3** Überprüfen Sie, ob der Zugriff auf die Audit-Trails der Anwendung, die von oder innerhalb der Anwendung verwaltet werden, protokolliert werden.	Angreifer versuchen häufig, Prüfprotokolle zu verfälschen, um ihre Aktionen zu verbergen. Doch mittels Einträgen zu allen Zugriffen kann ein Unternehmen sämtliche Widersprüche oder potenzielle Manipulationen der Protokolle bis zu einem einzelnen Konto zurückverfolgen.
4.2.4 Ungültige logische Zugriffsversuche	**4.2.4** Prüfen Sie, ob ungültige logische Zugriffsversuche protokolliert werden.	Angreifer werden häufig mehrere Versuche unternehmen, um auf die gewünschten Systeme zuzugreifen. Mehrere ungültige Anmeldeversuche können ein Hinweis darauf sein, dass ein unbefugter Benutzer versucht, das Kennwort über einen „Brute Force“-Angriff herauszufinden oder zu erraten.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
4.2.5 Verwendung der sowie Änderungen an Identifizierungs- und Authentifizierungsmechanismen der Anwendung (u. a. bei der Erstellung neuer Konten, Heraufstufung von Rechten usw.) und sämtliche Änderungen, Ergänzungen und Löschungen an bzw. von Anwendungskonten mit „root“- oder Administratorrechten	**4.2.5** Überprüfen Sie, dass die Verwendung der sowie Änderungen an Identifizierungs- und Authentifizierungsmechanismen der Zahlungsanwendung (u. a. bei der Erstellung neuer Konten, Heraufstufung von Rechten usw.) und sämtliche Änderungen, Ergänzungen und Löschungen an bzw. von Anwendungskonten mit „root“- oder Administratorrechten protokolliert werden.	Wenn nicht bekannt ist, wer zu dem Zeitpunkt eines Vorfalls angemeldet war, ist es unmöglich, die verwendeten Konten zu identifizieren. Außerdem könnten Angreifer versuchen, die Authentifizierungskontrollen zu manipulieren, um sie entweder zu umgehen oder um sich als der Benutzer eines bestimmten gültigen Kontos auszugeben. Aktivitäten wie unter anderem die Erstellung neuer Konten, Rechteeskalationen oder Änderungen an den Zugriffsberechtigungen können ein Hinweis auf eine nicht genehmigte Nutzung der Authentifizierungsmechanismen eines Systems sein.
4.2.6 Initialisieren, Beenden oder Anhalten der Prüfprotokolle der Anwendung	**4.2.6** Überprüfen Sie, ob Folgendes protokolliert wird: • Initialisierung der Prüfprotokolle der Anwendung • Beendung bzw. das Anhalten der Prüfprotokolle der Anwendung	Das Ausschalten (oder Anhalten) der Prüfprotokolle vor der Ausführung illegaler Aktivitäten ist eine beliebte Methode von Angreifern, die nicht entdeckt werden möchten. Die Initialisierung von Prüfprotokollen könnte darauf hinweisen, dass eine Protokollfunktion von einem Benutzer deaktiviert wurde, um seine Aktivitäten zu verbergen.
4.2.7 Erstellen und Löschen von Objekten auf Systemebene innerhalb oder von der Anwendung	**4.2.7** Prüfen Sie, ob die Erstellung und Löschung von Objekten auf Systemebene innerhalb oder von der Anwendung protokolliert werden.	Angreifer erstellen oder ersetzen oft Objekte auf Systemebene auf dem Zielsystem, um eine bestimmte Funktion oder einen Vorgang auf diesem System zu kontrollieren. Wenn der Zeitpunkt der Erstellung oder Löschung von Objekten auf Systemebene, z. B. Datenbanktabellen oder gespeicherte Verfahren, protokolliert wird, kann einfacher festgestellt werden, ob solche Änderungen genehmigt waren.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
4.3 Die Zahlungsanwendung muss mindestens die folgenden Audit-Trail-Einträge zu jedem Ereignis aufzeichnen: ***Im Sinne der PCI-DSS-Anforderung 10.3***	**4.3** Testen Sie die Zahlungsanwendung, indem Sie die Prüfprotokolleinstellungen und Prüfprotokollausgabe der Zahlungsanwendung überprüfen und für jedes zu protokollierende Ereignis (aus 4.2) Folgendes durchführen:	Durch die Aufzeichnung der Details unter 4.3.1 – 4.3.6 für die zu protokollierenden Ereignisse unter 4.2 kann eine potenzielle Gefährdung schnell und mit Informationen zu dem Wer, Was, Wo, Wann und Wie erkannt werden.
4.3.1 Benutzeridentifizierung	**4.3.1** Prüfen Sie, ob die Benutzer-ID in den Protokolleinträgen enthalten ist.	
4.3.2 Ereignistyp	**4.3.2** Prüfen Sie, ob die Art des Ereignisses in den Protokolleinträgen enthalten ist.	
4.3.3 Datum und Uhrzeit	**4.3.3** Prüfen Sie, ob die Datums- und Zeitangabe in den Protokolleinträgen enthalten ist.	
4.3.4 Angabe von Erfolgen oder Fehlschlägen	**4.3.4** Prüfen Sie, ob ein Hinweis auf die erfolgreiche oder fehlgeschlagene Ausführung in den Protokolleinträgen enthalten ist.	
4.3.5 Ereignisursprung	**4.3.5** Prüfen Sie, ob der Ursprung des Ereignisses in den Protokolleinträgen enthalten ist.	
4.3.6 Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen	**4.3.6** Überprüfen Sie, ob die Identität oder der Name der betroffenen Daten, Systemkomponenten oder Ressourcen in den Protokolleinträgen enthalten ist.	
4.4. Die Zahlungsanwendung muss eine zentralisierte Protokollierung ermöglichen. ***Hinweis:*** *Beispiele für diese Funktion sind unter anderem:* • Protokollierung mittels branchenüblicher Standard-Protokollmechanismen wie Common Log File System (CLFS), Syslog, tabulatorgetrennter Text, usw. • Bereitstellung von Funktionen und Dokumentation, um das Protokollformat der Anwendung in branchenübliche Protokollformate für ein schnelles, zentralisiertes Protokollieren umzuwandeln. ***Im Sinne der PCI-DSS-Anforderung 10.5.3***	**4.4.**a Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, um sicherzustellen, dass Folgendes für Kunden und Integratoren/Wiederverkäufer enthalten ist: • Angabe, welche zentralisierten Protokollierungsmechanismen unterstützt werden • Anweisungen und Verfahren zur Integration der Protokolle der Zahlungsanwendung in einer zentralen Protokollierungsumgebung **4.4.b** Installieren und konfigurieren Sie die Zahlungsanwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, um sicherzustellen, dass die Anweisungen präzise sind und dass Funktionen bereitgestellt werden, die es dem Kunden ermöglichen, Protokolle in den eigenen zentralisierten Protokollserver zu integrieren.	Ohne entsprechende Schutzmaßnahmen für die Prüfprotokolle kann deren Vollständigkeit, Genauigkeit und Integrität nicht garantiert werden, und darüber hinaus können die Prüfprotokolle nach einem Vorfall als Überprüfungstool unbrauchbar gemacht werden. Durch die Einbindung der Protokolle der Zahlungsanwendung in ein zentrales Protokollierungssystem kann der Kunde seine Protokolle integrieren und zuordnen und die Protokolle in seiner Umgebung konsistent sichern.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 5: Entwickeln sicherer Zahlungsanwendungen

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.1 Der Softwareanbieter hat einen offiziellen Prozess für die sichere Bereitstellung von Zahlungsanwendungen definiert und implementiert, der Folgendes umfasst: • Zahlungsanwendungen werden gemäß dem PCI-DSS und dem PA-DSS entwickelt (z. B. sichere Authentifizierung und Protokollierung). • Entwicklungsprozesse basieren auf Branchenstandards und/oder Best Practices. • Informationssicherheit ist über den gesamten Softwareentwicklungszyklus hinweg integriert. • Vor der Freigabe einer Anwendung oder eines Updates für eine Anwendung werden Sicherheitsprüfungen durchgeführt. ***Im Sinne der PCI-DSS-Anforderung 6.3***	**5.1.a** Überprüfen Sie dokumentierte Softwareentwicklungsprozesse, um sicherzustellen, dass die Prozesse auf Branchenstandards und/oder Best Practices basieren.	Ohne die Einbindung von Sicherheitsmaßnahmen während der Definition der Anforderungen sowie der Design-, Analyse- und Testphasen im Softwareentwicklungsprozess können Sicherheitsrisiken ungewollt oder in böser Absicht in den Anwendungscode eingebaut werden.
	5.1.b Überprüfen Sie, ob die dokumentierten Softwareentwicklungsprozesse Verfahren für Folgendes enthalten: • Integration von Informationssicherheit über den gesamten Softwareentwicklungszyklus hinweg • Entwicklung der Zahlungsanwendungen gemäß den PCI-DSS- und PA-DSS-Anforderungen	
	5.1.c Überprüfen Sie, ob die dokumentierten Softwareentwicklungsprozesse Folgendes enthalten: • Definierte Sicherheitsprüfungen vor der Freigabe einer Anwendung oder eines Updates für eine Anwendung • Verfahren für durchzuführende Sicherheitsprüfungen, um sicherzustellen, dass die Sicherheitsziele von PCI-DSS und PA-DSS erfüllt werden	
	5.1.d Bestätigen Sie durch Befragung der Softwareentwickler, dass dokumentierte Prozesse befolgt werden und dass Folgendes zutrifft: • Informationssicherheit ist über den gesamten Softwareentwicklungszyklus hinweg integriert. • Zahlungsanwendungen werden gemäß den PCI-DSS- und PA-DSS-Anforderungen entwickelt. • Sicherheitsprüfungen werden vor der Freigabe durchgeführt, um sicherzustellen, dass die Sicherheitsziele, einschließlich PCI-DSS- und PA-DSS-Anforderungen, erreicht werden.	
5.1.1 Live-PANs werden nicht zum Testen oder zur Entwicklung verwendet. ***Im Sinne der PCI-DSS-Anforderung 6.4.3***	**5.1.1.a** Überprüfen Sie die Softwareentwicklungsprozesse dahingehend, ob sie Verfahren enthalten, mit denen sichergestellt wird, dass Live-PANs nicht zum Testen oder zur Entwicklung verwendet werden.	Kreditkartenunternehmen und eine Vielzahl von Acquirern sind in der Lage, für Tests geeignete Kontonummern bereitzustellen, falls vor der Veröffentlichung realistische PANs zum Testen der Anwendungsfunktionalität benötigt werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	5.1.1.b Stellen Sie durch Beobachtung der Prüfverfahren und Befragung der Mitarbeiter sicher, dass keine Live-PANs zum Testen oder zur Entwicklung verwendet werden.	
	5.1.1.c Überprüfen Sie Stichproben von Testdaten, um sicherzustellen, dass keine Live-PANs zum Testen oder zur Entwicklung verwendet werden.	
5.1.2 Testdaten und -konten werden vor der Freigabe an den Kunden entfernt. ***Im Sinne der PCI-DSS-Anforderung 6.4.4***	**5.1.2.a** Überprüfen Sie die Softwareentwicklungsprozesse dahingehend, ob sie Verfahren enthalten, mit denen sichergestellt wird, dass Testdaten und -konten vor der Freigabe der Zahlungsanwendung an Kunden entfernt werden.	Testdaten und -konten sollten aus der Anwendung vor der Freigabe an Kunden entfernt werden, da diese Elemente Aufschluss über den Aufbau von Schlüsseln in der Anwendung geben können.
	5.1.2.b Stellen Sie durch Beobachtung der Prüfverfahren und Befragung der Mitarbeiter sicher, dass Testdaten und -konten vor der Freigabe an Kunden entfernt werden.	
	5.1.2.c Überprüfen Sie die fertige Zahlungsanwendung, um sicherzustellen, dass Testdaten und -konten vor der Freigabe an Kunden entfernt werden.	
5.1.3 Benutzerdefinierte Zahlungsanwendungskonten, Benutzer-IDs und Kennwörter werden entfernt, bevor Zahlungsanwendungen an Kunden freigegeben werden. ***Im Sinne der PCI-DSS-Anforderung 6.3.1***	**5.1.3.a** Überprüfen Sie die Softwareentwicklungsprozesse dahingehend, ob sie Verfahren enthalten, mit denen sichergestellt wird, dass benutzerdefinierte Zahlungsanwendungskonten, Benutzer-IDs und Kennwörter vor der Freigabe der Zahlungsanwendung an Kunden entfernt werden.	Benutzerdefinierte Zahlungsanwendungskonten, Benutzer-IDs und Kennwörter der Vorabversion können von Entwicklern oder anderen Personen mit Kenntnis dieser Konten als Hintertür verwendet werden, um sich Zugriff auf die Anwendung zu verschaffen, wodurch die Anwendung sowie zugehörige Karteninhaberdaten gefährdet werden.
	5.1.3.b Stellen Sie durch Beobachtung der Prüfverfahren und Befragung der Mitarbeiter sicher, dass benutzerdefinierte Zahlungsanwendungskonten, Benutzer-IDs und Kennwörter entfernt werden, bevor die Zahlungsanwendung an Kunden freigegeben wird.	
	5.1.3.c Überprüfen Sie die fertige Zahlungsanwendung, um sicherzustellen, dass benutzerdefinierte Zahlungsanwendungskonten, Benutzer-IDs und Kennwörter entfernt werden, bevor die Zahlungsanwendung an Kunden freigegeben wird.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.1.4 Der Code der Zahlungsanwendung wird nach jeder wesentlichen Änderung überprüft, bevor die Anwendung an Kunden freigegeben wird, um alle potenziellen Programmanfälligkeiten zu identifizieren (mit manuellen oder automatischen Prozessen). Dabei wird mindestens Folgendes geprüft: • Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes sowie von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind. • Codeprüfungen gewährleisten, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird. (Siehe PA-DSS-Anforderung 5.2.) • Vor der Freigabe werden entsprechende Korrekturen implementiert. • Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt. • Die dokumentierten Ergebnisse der Codeprüfung schließen die Genehmigung des Managements, den Ersteller und den Prüfer des Codes ein und enthalten Angaben zu den Korrekturen, die vor der Freigabe implementiert wurden. ***Hinweis:*** *Diese Anforderung für Codeprüfungen gilt für sämtliche Zahlungsanwendungskomponenten (sowohl für interne als auch für öffentliche Webanwendungen) als Teil des Systementwicklungszyklus. Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden.* ***Im Sinne der PCI-DSS-Anforderung 6.3.2***	**5.1.4.a** Überprüfen Sie die dokumentierten Softwareentwicklungsverfahren, und befragen Sie die zuständigen Mitarbeiter, um sicherzustellen, dass der Anbieter bei allen wesentlichen Änderungen des Anwendungscodes (mit manuellen oder automatischen Prozessen) Codeprüfungen wie folgt durchführt: • Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes sowie von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind. • Codeprüfungen gewährleisten, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird. (Siehe PA-DSS-Anforderung 5.2.) • Vor der Freigabe werden entsprechende Korrekturen implementiert. • Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt. • Die Ergebnisse der Codeprüfung – u. a. die Genehmigung des Managements, der Ersteller und der Prüfer des Codes und Angaben zu den Korrekturen, die vor der Freigabe implementiert wurden – werden dokumentiert. **5.1.4.b** Überprüfen Sie die Ergebnisse der Codeprüfung für eine Stichprobe von Codeänderungen, um Folgendes sicherzustellen: • Codeprüfungen wurden von einer anderen Person geprüft als dem Ersteller des Codes, die mit dem Verfahren vertraut ist. • Codeprüfungen wurden gemäß sicheren Codierungsrichtlinien erstellt. • Vor der Freigabe wurden entsprechende Korrekturen implementiert. • Die Ergebnisse der Codeprüfung wurden vor der Freigabe vom Management geprüft und genehmigt.	Sicherheitsrisiken im Anwendungscode werden von Angreifern häufig ausgenutzt, um sich Zugriff auf ein Netzwerk zu verschaffen und Karteninhaberdaten zu kompromittieren. Zum Schutz gegen diese Art von Angriffen sollten geeignete Codeprüfungsverfahren verwendet werden. Die Codeprüfungsverfahren sollten sicherstellen, dass während des gesamten Entwicklungsprozesses Best Practices für sicheres Codieren eingesetzt wurden. Der Anwendungsanbieter sollte relevante Verfahren für sicheres Codieren einschließen, die den jeweils verwendeten Technologien entsprechen. Prüfungen sollten von Personen durchgeführt werden, die mit der Technologie vertraut sind und Erfahrung mit Verfahren zur Codeprüfung haben, sodass potenzielle Codierungsprobleme identifiziert werden. Indem die Codeprüfungen einer anderen Person als dem Entwickler des Codes aufgetragen werden, wird eine unabhängige und objektive Überprüfung gewährleistet. Durch die Behebung von Codierungsfehlern vor der Freigabe des Codes wird verhindert, dass Kundenumgebungen aufgrund von Codefehlern gefährdet werden. Nach der Bereitstellung des Codes ist es außerdem viel schwieriger und kostspieliger, Codefehler zu beheben. Eine offizielle Prüfung und die Abzeichnung durch das Management vor der Freigabe dienen zur Sicherstellung, dass der Code genehmigt und in Übereinstimmung mit den Richtlinien und Verfahren entwickelt wurde.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.1.5 Es wurden sichere Methoden zur Quellcodeverwaltung implementiert, mit denen die Integrität des Quellcodes während des Entwicklungsprozesses überprüft wird.	**5.1.5.a** Überprüfen Sie die dokumentierten Softwareentwicklungsverfahren, und befragen Sie die zuständigen Mitarbeiter, um sicherzustellen, dass der Anbieter sichere Methoden zur Quellcodeverwaltung einsetzt, um die Integrität des Quellcodes während des Entwicklungsprozesses zu überprüfen.	Mithilfe geeigneter Methoden zur Quellcodeverwaltung kann sichergestellt werden, dass alle Codeänderungen beabsichtigt sind und autorisiert wurden und nur von Personen mit einem berechtigten Grund für eine Codeänderung durchgeführt wurden. Beispiele dieser Methoden umfassen Eincheck- und Auscheckverfahren für Code mit strengen Zugriffskontrollen sowie ein Vergleich, der unmittelbar vor dem Aktualisieren des Codes durchgeführt wird, um zu bestätigen, dass die letzte genehmigte Version nicht geändert wurde (z. B. mit dem Prüfsummenverfahren).
	5.1.5.b Stellen Sie durch Überprüfung der Mechanismen zum Sichern des Quellcodes und Beobachtung der entsprechenden Verfahren sicher, dass die Integrität des Quellcodes während des Entwicklungsprozesses aufrechterhalten wird.	
5.1.6 Zahlungsanwendungen werden gemäß den Best Practices der Branche für sichere Codierungsverfahren entwickelt. Hierzu zählen: • Entwicklung gemäß dem Prinzip der Mindestberechtigungen für die Anwendungsumgebung • Entwicklung mit ausfallsicheren Standards (standardmäßig wird jegliche Ausführung verweigert, wenn dies nicht innerhalb des ursprünglichen Designs angegeben wurde) • Entwicklung unter Berücksichtigung aller Zugriffspunkte, einschließlich Eingabeformen wie Anwendungseingaben über mehrere Kanäle	**5.1.6.a** Stellen Sie durch Überprüfung der Softwareentwicklungsprozesse sicher, dass sichere Codierungsverfahren definiert sind, die Folgendes umfassen: • Entwicklung gemäß dem Prinzip der Mindestberechtigungen für die Anwendungsumgebung • Entwicklung mit ausfallsicheren Standards (standardmäßig wird jegliche Ausführung verweigert, wenn dies nicht innerhalb des ursprünglichen Designs angegeben wurde) • Entwicklung unter Berücksichtigung aller Zugriffspunkte, einschließlich Eingabeformen wie Anwendungseingaben über mehrere Kanäle	Die Entwicklung von Anwendungen mit Mindestberechtigungen ist die effektivste Methode, um sicherzustellen, dass keine unsicheren Annahmen in die Anwendung einfließen. Durch die Einbeziehung von ausfallsicheren Standards wird möglicherweise verhindert, dass sich ein Angreifer vertrauliche Informationen über einen Anwendungsfehler verschafft, die zur Vorbereitung späterer Angriffe verwendet werden könnten. Durch die Sicherstellung, dass Sicherheitsmaßnahmen für alle Zugriffs- und Eingabemöglichkeiten der Anwendung implementiert werden, wird

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	5.1.6.b Überprüfen Sie durch Befragung der Entwickler, ob Anwendungen gemäß den Best Practices der Branche für sichere Codierungsverfahren entwickelt werden, einschließlich: • Entwicklung gemäß dem Prinzip der Mindestberechtigungen für die Anwendungsumgebung • Entwicklung mit ausfallsicheren Standards (standardmäßig wird jegliche Ausführung verweigert, wenn dies nicht innerhalb des ursprünglichen Designs angegeben wurde) • Entwicklung unter Berücksichtigung aller Zugriffspunkte, einschließlich Eingabeformen wie Anwendungseingaben über mehrere Kanäle	die Wahrscheinlichkeit verringert, dass ein Eingabekanal für eine Kompromittierung verwendet werden kann. Wenn diese Konzepte während der Entwicklung des Codes nicht berücksichtigt werden, könnte dies dazu führen, dass eine unsichere Anwendung freigegeben wird und zu einem späteren Zeitpunkt möglicherweise übermäßig viele Nachbesserungen erforderlich sind.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.1.6.1 Die Codierungsverfahren umfassen Angaben zur Handhabung der PAN und/oder SAD im Arbeitsspeicher.	**5.1.6.1.a** Überprüfen Sie die Codierungsverfahren dahingehend, ob sie Angaben zur Handhabung der PAN und/oder SAD im Arbeitsspeicher umfassen.	Angreifer setzen Malware ein, um vertrauliche Daten aus dem Arbeitsspeicher zu erfassen. Durch Minimierung des Gefahrenpotenzials während des Zeitraums, in dem die PAN/SAD sich im Arbeitsspeicher befinden, wird die Wahrscheinlichkeit reduziert, dass die Daten von Angreifern erfasst werden oder unwissentlich in einer Speicherdatei auf der Festplatte gespeichert werden und nicht geschützt sind. Diese Anforderung soll sicherstellen, dass berücksichtigt wird, wie die PAN und SAD im Arbeitsspeicher gehandhabt werden. Wenn Anwendungsanbieter wissen, wann und wie lange vertrauliche Daten sich im Arbeitsspeicher befinden – und in welchem Format –, können sie potenziell unsichere Stellen in ihren Anwendungen identifizieren und feststellen, ob zusätzliche Schutzmaßnahmen erforderlich sind. Ob Codierungsverfahren aus dieser Aktivität entstehen, hängt von der jeweils entwickelten Software und den verwendeten Technologien ab.
	5.1.6.1.b Überprüfen Sie durch Befragung der Entwickler, ob sie während der Anwendungsentwicklung berücksichtigen, wie die PAN/SAD im Arbeitsspeicher gehandhabt werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.1.7 Bieten Sie mindestens jährlich aktuelle Schulungen an, in denen sichere Entwicklungsmethoden für Anwendungsentwickler vermittelt werden, die der Tätigkeitsfunktion des Entwicklers und der verwendeten Technologie entsprechen: • Sicheres Anwendungsdesign • Sichere Codierungsverfahren zur Vermeidung häufiger Sicherheitsrisiken beim Programmieren (beispielsweise Richtlinien für Anbieter, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding usw.) • Verwaltung vertraulicher Daten im Arbeitsspeicher • Codeprüfungen • Sicherheitstests (beispielsweise Durchdringungstestverfahren) • Verfahren zur Risikobewertung ***Hinweis:*** *Schulungen für Anwendungsentwickler können intern oder von Drittanbietern bereitgestellt werden. Die Schulungen können beispielsweise am Arbeitsplatz, mit Kursleitern oder am Computer durchgeführt werden.*	**5.1.7a** Überprüfen Sie, ob die dokumentierten Softwareentwicklungsprozesse aktuelle Schulungen voraussetzen, in denen sichere Entwicklungsmethoden für Anwendungsentwickler mindestens jährlich vermittelt werden, die der Tätigkeitsfunktion des Entwicklers und der verwendeten Technologie entsprechen.	Indem sichergestellt wird, dass die Entwickler mit sicheren Entwicklungsmethoden vertraut sind, kann die Anzahl der Sicherheitsrisiken, die durch unzulängliche Codierungsverfahren eingeschleust werden, auf ein Minimum reduziert werden. Geschulte Mitarbeiter können mit größerer Wahrscheinlichkeit potenzielle Sicherheitsprobleme im Anwendungsdesign und -code identifizieren. Plattformen und Methoden für die Softwareentwicklung ändern sich häufig. Das Gleiche gilt für Bedrohungen und Risiken für Softwareanwendungen. Schulungen zu sicheren Entwicklungsmethoden sollten immer auf dem gleichen Stand wie die sich ändernden Entwicklungsmethoden sein.
	5.1.7.b Überprüfen Sie durch die Befragung einiger stichprobenartig ausgewählter Entwickler, ob sie mit sicheren Entwicklungsmethoden und Codierungsverfahren vertraut sind, die für die verwendeten Technologien relevant sind.	
	5.1.7.c Überprüfen Sie Schulungsunterlagen, um sicherzustellen, dass alle Anwendungsentwickler die entsprechenden Schulungen für ihre Tätigkeitsfunktion und die verwendete Technologie mindestens jährlich erhalten.	
5.1.7.1 Aktualisieren Sie Schulungen gegebenenfalls, um neue Entwicklungstechnologien und -methoden zu berücksichtigen.	**5.1.7.1** Überprüfen Sie das Schulungsmaterial, und führen Sie Gespräche mit stichprobenartig ausgewählten Entwicklern, um sicherzustellen, dass die Schulungen auf neue Entwicklungstechnologien und -methoden eingehen.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.2 Achten Sie bei der Entwicklung aller Zahlungsanwendungen darauf, dass häufige Sicherheitsrisiken bie der Programmierung in Softwareentwicklungsprozessen vermieden werden. ***Hinweis:*** *Die unter den PA-DSS-Anforderungen 5.2.1 bis 5.2.10 und im PCI-DSS unter 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken entsprachen zum Zeitpunkt der Veröffentlichung dieser Version des PA-DSS den Best Practices der Branche Entsprechend den Aktualisierungen der Best Practices der Branche im Anfälligkeits-Management (z. B. die OWASP Top 10, SANS CWE Top 25, CERT Secure Coding usw.) müssen jedoch die aktuellen Best Practices für diese Anforderungen verwendet werden.* ***Im Sinne der PCI-DSS-Anforderung 6.5***	**5.2.** Stellen Sie für Zahlungsanwendungen sicher, dass diese nicht anfällig für häufige Programmierfehler sind, indem Sie manuelle oder automatisierte Durchdringungstests durchführen, mit denen gezielt versucht wird, folgende Fehler zu untersuchen:	Die Anwendungsschicht ist einem hohen Risiko ausgesetzt und ist sowohl durch interne als auch externe Bedrohungen gefährdet. Ohne eine geeignete Sicherheitslösung sind Karteninhaberdaten und andere vertrauliche Unternehmensinformationen gefährdet. Bei den Anforderungen 5.2.1 bis 5.2.9 handelt es sich um die Mindestkontrollen, die implementiert sein sollten. Diese Liste umfasst die häufigsten Sicherheitsrisiken bei der Programmierung zum Zeitpunkt der Veröffentlichung dieser PA-DSS-Version. Codierungsverfahren sollten den Änderungen der in der Branche bekannten häufigen Sicherheitsrisiken bei der Programmierung entsprechend aktualisiert werden.
Hinweis: *Die nachstehenden Anforderungen 5.2.1 bis 5.2.6 gelten für alle Zahlungsanwendungen (intern oder extern):*		

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.2.1 Injektionsfehler, insbesondere bei der SQL-Injektion. Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.	**5.2.1** Beispiele für Codierungsverfahren, die auf Injektionsfehler, insbesondere bei der SQL-Injektion, eingehen: • Validierung der Eingabe, um sicherzustellen, dass Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern können • Verwendung von parametrisierten Abfragen	Injektionsfehler, insbesondere die SQL-Injektion, sind eine häufige Methode zur Beschädigung von Anwendungen. Injektionen treten auf, wenn vom Benutzer übermittelte Daten als Teil eines Befehls oder einer Anfrage an einen Interpreter gesendet werden. Die schädlichen Daten des Angreifers verleiten den Interpreter unwissentlich dazu, Befehle auszuführen oder Daten zu ändern, wodurch Komponenten innerhalb der Anwendung Angriffen wie beispielsweise Pufferüberläufen ausgesetzt werden. Alle Eingabedaten sollten von der Anwendung vor der Verarbeitung validiert werden – beispielsweise indem alle alphabetischen, eine Kombination aus alphabetischen und numerischen Zeichen usw. überprüft werden.
5.2.2 Pufferüberlauf	**5.2.2** Beispiele für Codierungsverfahren, die auf Pufferüberläufe eingehen: • Validierung von Puffergrenzen • Kürzung der eingegebenen Zeichenfolgen	Pufferüberläufe treten auf, wenn eine Anwendung auf ihrem Pufferspeicherplatz nicht über eine geeignete Bereichsüberprüfung verfügt. Das kann dazu führen, dass die Informationen in dem Puffer aus dem Pufferspeicherplatz auf einen ausführbaren Speicherbereich verdrängt werden. In diesem Fall ist der Angreifer in der Lage, schädliche Codes an das Ende eines Puffers zu hängen und diesen Code anschließend, indem der Puffer zum Überlaufen gebracht wird, in einen ausführbaren Speicherbereich einzuschleusen. Der schädliche Code wird dann ausgeführt und gewährt dem Angreifer den rechnerfernen Zugriff auf die Anwendung und/oder das betroffene System.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.2.3 Unsicherer kryptographischer Speicher	**5.2.3** Codierungsverfahren gehen wie folgt auf unsicheren kryptographischen Speicher ein: • Durch die Verhinderung von kryptographischen Fehlern • Nutzung starker kryptographischer Algorithmen und Schlüssel	Anwendungen, die beim Speichern der Daten die starken kryptographischen Funktionen nicht richtig einsetzen, sind einem erhöhten Risiko der Kompromittierung und der Gefährdung der Authentifizierungsinformationen und/oder Karteninhaberdaten ausgesetzt.
5.2.4 Unsichere Mitteilungen	**5.2.4** Auf unsichere Mitteilungen gehen Codierungsverfahren ein, die alle vertraulichen Mitteilungen ordnungsgemäß authentifizieren und verschlüsseln.	Anwendungen, die vertraulichen Netzwerkdatenverkehr nicht mithilfe einer starken Kryptographie angemessen verschlüsseln, sind einem erhöhten Risiko der Kompromittierung und der Gefährdung der Karteninhaberdaten ausgesetzt.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.2.5 Inkorrekte Fehlerhandhabung	**5.2.5** Auf inkorrekte Fehlerhandhabung gehen Codierungsverfahren ein, die keine Informationen über Fehlermeldungen preisgeben (indem beispielsweise keine spezifischen Fehlerdetails, sondern nur allgemeine Angaben zum Fehler zurückgegeben werden).	Anwendungen, die durch unangemessene Methoden zur Fehlerhandhabung Informationen über ihre Konfiguration oder internen Abläufe bzw. vertrauliche Informationen preisgeben, unterliegen dem Risiko einer Kompromittierung. Angreifer nutzen diese Schwachstellen aus, um vertrauliche Informationen zu entwenden oder das gesamte System zu kompromittieren. Wenn ein Angreifer Fehler einbauen kann, die von der Anwendung nicht richtig gehandhabt werden, kann er an ausführliche Informationen über das System gelangen, Denial-of-Service-Unterbrechungen hervorrufen, oder erreichen, dass die Sicherheitsmaßnahmen fehlschlagen bzw. die Anwendung oder das System abstürzt. Durch die Meldung „falsches Kennwort“ erfährt ein Angreifer beispielsweise, dass die Benutzer-ID korrekt war, sodass er seine Anstrengungen auf das Kennwort konzentrieren kann. Es wird empfohlen, allgemeinere Fehlermeldungen zu verwenden, zum Beispiel „die Daten konnten nicht bestätigt werden“.
5.2.6 Alle „hohen“ Sicherheitsrisiken gemäß dem Identifikationsprozess von Sicherheitsrisiken in der PA-DSS-Anforderung 7.1	**5.2.6** Codierungsverfahren gehen auf alle „hohen“ Sicherheitsrisiken ein, die die Anwendung beeinträchtigen könnten – entsprechend der PA-DSS-Anforderung 7.1.	Alle Schwächen, die von dem Prozess des Anbieters zur Risikobewertung von Sicherheitsrisiken (in der PA-DSS-Anforderung 7.1 definiert) als „hohes Risiko“ eingestuft werden und die die Anwendung beeinträchtigen könnten, sollten während der Anwendungsentwicklung identifiziert und behoben werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
Hinweis: *Die nachstehenden Anforderungen 5.2.7 bis 5.2.10 gelten für webbasierte Anwendungen und Anwendungsschnittstellen (intern oder extern):*		Web-Anwendungen sind aufgrund ihrer Architektur sowie der relativ einfachen Durchführung und der Häufigkeit von Angriffen einmaligen Sicherheitsrisiken ausgesetzt.
5.2.7 Site-übergreifendes Scripting (XSS)	**5.2.7** Auf Site-übergreifendes Scripting (XSS) gehen beispielsweise folgende Codierungsverfahren ein: • Validierung aller Parameter vor der Einbindung • Nutzung einer kontextabhängigen Außerkraftsetzungsfunktion	XSS-Fehler treten auf, wenn eine Anwendung vom Benutzer übermittelte Daten an einen Webbrowser sendet, ohne diese zuvor zu überprüfen oder deren Inhalt zu verschlüsseln. XSS ermöglicht es Angreifern im Browser eines betroffenen Benutzers Skripts auszuführen, wodurch unter anderem Benutzer-Sitzungen entführt, Websites unleserlich gemacht und Würmer eingeschleust werden können.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.2.8 Ungenügende Zugriffskontrolle, beispielsweise unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal	**5.2.8** Auf eine ungenügende Zugriffskontrolle, beispielsweise unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal, gehen beispielsweise folgende Codierungsverfahren ein: • Ordnungsgemäße Benutzerauthentifizierung • Bereinigung der Eingaben • Keine Preisgabe interner Objektverweise an Benutzer • Benutzeroberflächen, die keinen Zugriff auf nicht autorisierte Funktionen zulassen	Ein direkter Objektverweis liegt vor, wenn ein Entwickler einen Verweis einem internen Implementierungsobjekt, wie etwa einer Datei, einem Verzeichnis, einem Datensatz in einer Datenbank oder einem Schlüssel, in Form einer URL oder eines Formularparameters zugänglich macht. Angreifer können diese Verweise manipulieren, um unerlaubt auch auf andere Objekte zuzugreifen. Ein Angreifer, der in der Lage ist, die Verzeichnisstruktur einer Website aufzulisten und zu durchsuchen (Directory Traversal), könnte sich dadurch Zugriff auf vertrauliche Informationen verschaffen und tiefere Einblicke in die Funktionsweise der Site für spätere Angriffe gewinnen. Über Benutzeroberflächen, die Zugriff auf nicht autorisierte Funktionen zulassen, könnten sich unbefugte Personen Zugriff auf vertrauliche Anmeldeinformationen oder Karteninhaberdaten verschaffen. Die Einschränkung des Zugriffs auf Datenressourcen trägt dazu bei, dass Karteninhaberdaten nicht von Unbefugten aufgerufen werden können.
5.2.9 CSRF (Cross-site Request Forgery, Websiteübergreifende Anfragenfälschung)	**5.2.9** Auf CSRF (Cross-site Request Forgery, Websiteübergreifende Anfragenfälschung) gehen Codierungsverfahren ein, die sicherstellen, dass Anwendungen sich nicht auf Autorisierungsinformationen und Token verlassen, die automatisch von Browsern gesendet werden.	Ein CSRF-Angriff zwingt den Browser eines angemeldeten Benutzers, eine noch nicht authentifizierte Anfrage an eine gefährdete Webanwendung zu senden, wodurch der Angreifer beliebige statusverändernde Vorgänge ausführen kann, zu denen der Benutzer autorisiert ist (beispielsweise das Aktualisieren von Kontodetails, Einkäufe oder sogar die Authentifizierung der Anwendung).

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.2.10 Geknackte Authentifizierungs- und Sitzungsverwaltung	**5.2.10** Auf geknackte Authentifizierungs- und Sitzungsverwaltung gehen Codierungsverfahren ein, die gewöhnlich Folgendes umfassen: • Kennzeichnung von Sitzungstoken (zum Beispiel Cookies) als „sicher“ • Keine Anzeige von Sitzungs-IDs in der URL • Berücksichtigung angemessener Timeouts und Rotation der Sitzungs-IDs nach erfolgreicher Anmeldung	Eine sichere Authentifizierungs- und Sitzungsverwaltung verhindert, dass unbefugte Personen zulässige Kontoanmeldeinformationen, Schlüssel oder Sitzungstoken gefährden, mit denen ein Angreifer die Identität eines autorisierten Benutzers annehmen könnte.
5.3 Der Softwareanbieter muss die Verfahrensweisen zur Änderungskontrolle für sämtliche Änderungen an der Anwendung befolgen. Für Verfahrensweisen zur Änderungskontrolle müssen dieselben Softwareentwicklungsprozesse wie bei neuen Freigaben befolgt werden (gemäß der PA-DSS-Anforderung 5.1), darunter: ***Im Sinne der PCI-DSS-Anforderung 6.4.5***	**5.3.a** Überprüfen Sie die Verfahrensweisen des Anbieters zur Änderungskontrolle bei Softwareänderungen, und stellen Sie Folgendes sicher: • Die Verfahrensweisen stimmen mit den dokumentierten Softwareentwicklungsprozessen überein, die in der Anforderung 5.1 definiert sind. • Die Verfahrensweisen setzen die nachstehenden Elemente 5.3.1 bis 5.3.4 voraus. **5.3.b** Stellen Sie durch Befragung der Entwickler fest, welche Änderungen in der letzten Zeit an der Zahlungsanwendung vorgenommen wurden. Überprüfen Sie kürzlich vorgenommene Änderungen an der Zahlungsanwendung, und verfolgen Sie diese zurück zur entsprechenden Dokumentation der Änderungskontrolle. Stellen Sie sicher, dass für jede überprüfte Änderung die folgenden Punkte entsprechend den Verfahrensweisen zur Änderungskontrolle dokumentiert wurden:	Wird die Verwaltung nicht ordnungsgemäß durchgeführt, sind die Auswirkungen von Softwareupdates und Sicherheitspatches möglicherweise nicht vollständig bekannt, und sie könnten unbeabsichtigte Folgen nach sich ziehen.
5.3.1 Dokumentation der Auswirkungen	**5.3.1** Überprüfen Sie, ob die Dokumentation der Kundenauswirkungen in der Änderungskontrolldokumentation für jede Änderung enthalten ist.	Die Auswirkungen der Änderung sollten dokumentiert werden, sodass alle betroffenen Parteien Prozessänderungen entsprechend vorausplanen können.
5.3.2 Dokumentierte Bestätigung von Änderungen durch autorisierte Parteien	**5.3.2** Bestätigen Sie, dass für jede Änderung eine dokumentierte Genehmigung durch eine autorisierte Partei vorhanden ist.	Die Genehmigung durch eine autorisierte Partei deutet darauf hin, dass es sich um eine zulässige und von dem Management gebilligte Änderung handelt.
5.3.3 Testen der Funktionalität, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt	**5.3.3.a** Stellen Sie sicher, dass Funktionalitätstests durchgeführt wurden, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.	Es sollten eingehende Tests durchgeführt werden, um sicherzustellen, dass die Sicherheit der Zahlungsanwendung durch

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	5.3.3.b Überprüfen Sie, ob alle Änderungen (einschließlich Patches) vor der Freigabe auf ihre Konformität mit Punkt 5.2 getestet wurden.	diese Änderung nicht herabgesetzt wird. Die Tests sollten überprüfen, ob alle vorhandenen Sicherheitsvorkehrungen bestehen bleiben, durch ebenso starke Kontrollen ersetzt werden oder nach jeglichen Änderungen an der Anwendung intensiviert werden.
5.3.4 Back-Out- oder Produktdeinstallationsverfahren	**5.3.4** Stellen Sie sicher, dass Back-Out- oder Produktdeinstallationsverfahren für jede Änderung erstellt werden.	Für alle Änderungen müssen Verfahren etabliert sein, um die Änderung – für den Fall, dass sie fehlschlägt oder die Sicherheit der Anwendung herabsetzt – rückgängig zu machen und den vorherigen Zustand wiederherzustellen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.4 Der Anbieter der Zahlungsanwendung muss im Rahmen des Systementwicklungszyklus eine Software-Versionierungsmethode dokumentieren und befolgen. Die Methoden müssen mit den für Änderungen an Zahlungsanwendungen geltenden Verfahrensweisen im *PA-DSS-Programmleitfaden* übereinstimmen und mindestens Folgendes umfassen:	**5.4** Überprüfen Sie dokumentierte Softwareentwicklungsprozesse, um sicherzustellen, dass sie die Versionierungsmethode des Softwareanbieters enthalten und dass die Versionierungsmethode dem PA-DSS-Programmleitfaden entsprechen muss. Stellen Sie sicher, dass die dokumentierte Versionierungsmethode für die Zahlungsanwendung, einschließlich aller Änderungen an der Zahlungsanwendung, eingehalten werden muss.	Ohne eine sorgfältig definierte Versionierungsmethode werden Anwendungsänderungen möglicherweise nicht richtig identifiziert, und Integratoren/Wiederverkäufer verstehen unter Umständen nicht, welche Auswirkungen Versionsänderungen von Anwendungen mit sich bringen.
5.4.1 Die Versionierungsmethode muss die spezifischen verwendeten Versionselemente wie folgt definieren: • Details zur Übereinstimmung der Elemente des Versionsschemas mit den im *PA-DSS-Programmleitfaden* angegebenen Anforderungen • Format des Versionsschemas, einschließlich Anzahl der Elemente, Trennzeichen, Zeichensatz usw. (bestehend aus alphabetischen, numerischen und/oder alphanumerischen Zeichen). • Definition, wofür jedes Element im Versionsnummernschema steht (beispielsweise Änderungstyp, große Änderung, kleine Änderung, Wartungsversion, Platzhalter usw.) • Definition der Elemente, die auf die Verwendung von Platzhaltern hinweisen	**5.4.1.a** Überprüfen Sie die dokumentierte Versionierungsmethode, um Folgendes sicherzustellen: • Es sind Details dazu angegeben, wie die Elemente des Versionsschemas mit den im *PA-DSS-Programmleitfaden angegebenen Anforderungen übereinstimmen.* • Das Format des Versionsschemas ist angegeben und enthält Details zu der Anzahl der Elemente, Trennzeichen, zum Zeichensatz usw. (zum Beispiel 1.1.1.N, bestehend aus alphabetischen, numerischen und/oder alphanumerischen Zeichen). • Es wird definiert, wofür jedes Element im Versionsnummernschema steht (beispielsweise Änderungstyp, große Änderung, kleine Änderung, Wartungsversion, Platzhalter usw.). • Definition der Elemente, die auf die Verwendung von Platzhaltern hinweisen **5.4.1.b** Überprüfen Sie, ob die Elemente des Versionsschemas den im PA-DSS-Programmleitfaden angegebenen Änderungstypen entsprechen.	Die Versionierungsmethode für die Zahlungsanwendung sollte ein bestimmtes Versionsschema enthalten, in dem die verwendeten Elemente, das Versionsformat, die Hierarchie der verschiedenen Versionselemente usw. für die spezifische Zahlungsanwendung ausdrücklich identifiziert sind. Das Versionsschema sollte klar angeben, wie jedes einzelne Element in der Versionsnummer verwendet wird. Es gibt verschiedene Möglichkeiten zur Angabe des Versionsschemas – zum Beispiel N.NN.NNA, wobei „N“ ein numerisches Element und „A“ ein alphabetisches Element darstellt. Im Versionsschema sollte der Zeichensatz (zum Beispiel 0-9, A-Z usw.) identifiziert werden, der für jedes Versionselement verwendet werden kann.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
Hinweis: *Platzhalter dürfen nur Elemente der Versionsnummer ersetzen, die Änderungen ohne Auswirkungen auf die Sicherheit darstellen. Unter Anforderung 5.4.3 finden Sie weitere Anforderungen hinsichtlich der Verwendung von Platzhaltern.*	**5.4.1.c** Wählen Sie ein Beispiel kürzlich vorgenommener Änderungen an der Zahlungsanwendung, die zugewiesenen Versionsnummern und die Änderungskontrolldokumentation, in der der Typ der Anwendungsänderung angegeben ist, und stellen Sie sicher, dass die Elemente der Versionsnummer mit der entsprechenden Änderung und den in der dokumentierten Versionierungsmethode definierten Parametern übereinstimmen.	Ohne ein sorgfältig definiertes Versionsschema stellt das Versionsnummernformat Änderungen an der Anwendung unter Umständen nicht richtig dar.
	5.4.1.d Überprüfen Sie durch Befragung von stichprobenartig ausgewählten Entwicklern, ob diese mit dem Versionsschema – beispielsweise mit der zulässigen Verwendung von Platzhaltern in der Versionsnummer – vertraut sind.	
5.4.2 Gemäß dem *PA-DSS-Programmleitfaden* muss die Versionierungsmethode den Typ und die Auswirkungen aller Anwendungsänderungen angeben. Dazu gehören: • Beschreibungen aller Typen und Auswirkungen von Anwendungsänderungen • Spezifische Identifizierung und Definition der Änderungen, für die Folgendes gilt: - Die Änderungen haben keine Auswirkungen auf die Funktionalität oder Abhängigkeiten der Anwendung. - Die Änderungen haben Auswirkungen auf die Funktionalität der Anwendung, aber keine Auswirkungen auf die Sicherheit oder PA-DSS-Anforderungen. - Die Änderungen haben Auswirkungen auf Sicherheitsfunktionen oder PA-DSS-Anforderungen. • Angaben zur Zuordnung jedes Änderungstyps zu einer bestimmten	**5.4.2.a** Überprüfen Sie die dokumentierte Versionierungsmethode des Softwareanbieters, um sicherzustellen, dass die Versionierungsmethode Folgendes umfasst: • Beschreibung aller Typen und Auswirkungen von Anwendungsänderungen (beispielsweise Änderungen ohne Auswirkungen, mit geringen Auswirkungen oder hohen Auswirkungen auf die Anwendung) • Spezifische Identifizierung und Definition der Änderungen, für die Folgendes gilt: - Die Änderungen haben keine Auswirkungen auf die Funktionalität oder Abhängigkeiten der Anwendung. - Die Änderungen haben Auswirkungen auf die Funktionalität der Anwendung, aber keine Auswirkungen auf die Sicherheit oder PA-DSS-Anforderungen. - Die Änderungen haben Auswirkungen auf Sicherheitsfunktionen oder PA-DSS-Anforderungen. • Angaben zur Zuordnung jedes Änderungstyps zu einer bestimmten Versionsnummer	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	5.4.2.b Überprüfen Sie, ob die Versionierungsmethode dem *PA-DSS-Programmleitfaden* entspricht.	
	5.4.2.c Überprüfen Sie durch Befragung der Mitarbeiter und durch Beobachtung der Prozesse für jeden Änderungstyp, ob die dokumentierten Methoden für alle Änderungstypen eingehalten werden.	
	5.4.2.d Wählen Sie eine Stichprobe aus kürzlich vorgenommenen Änderungen an der Zahlungsanwendung aus, und überprüfen Sie die Änderungskontrolldokumentation, um sicherzustellen, dass die Version, die der Änderung zugewiesen wurde, mit dem Änderungstyp gemäß den dokumentierten Methoden übereinstimmt.	
5.4.3 In der Versionierungsmethode muss ausdrücklich angegeben sein, ob Platzhalter verwendet werden und, falls ja, wie sie verwendet werden. Folgende Angaben müssen enthalten sein: • Details zur Verwendung von Platzhaltern in der Versionierungsmethode • Platzhalter werden nie für Änderungen verwendet, die Auswirkungen auf die Sicherheit oder PA-DSS-Anforderungen haben. • Ein Element der Versionsnummer, das zur Darstellung einer Änderung ohne Auswirkungen auf die Sicherheit verwendet wird (einschließlich eines Platzhalterelements), darf auf keinen Fall für die Darstellung einer Änderung mit Auswirkungen auf die Sicherheit verwendet werden. • Platzhalterelemente dürfen nicht vor Versionselementen stehen, die für die	**5.4.3.a** Überprüfen Sie die dokumentierte Versionierungsmethode des Softwareanbieters, um sicherzustellen, dass spezifische Angaben zur Verwendung von Platzhaltern enthalten sind. Dazu gehören: • Details zur Verwendung von Platzhaltern in der Versionierungsmethode • Platzhalter werden nie für Änderungen verwendet, die Auswirkungen auf die Sicherheit oder PA-DSS-Anforderungen haben. • Ein Element der Versionsnummer, das zur Darstellung einer Änderung ohne Auswirkungen auf die Sicherheit verwendet wird (einschließlich eines Platzhalterelements), darf auf keinen Fall für die Darstellung einer Änderung mit Auswirkungen auf die Sicherheit verwendet werden. • Jedes Element, das rechts von einem Platzhalter steht, darf nicht für die Darstellung einer Änderung mit Auswirkungen auf die Sicherheit verwendet werden. Alle Versionselemente, ide eine Änderung mit Auswirkungen auf die Sicherheit wiederspielgen, müssen „links“ neben dem ersten Platzhalterelement stehen.	Ein „Platzhalter“-Element gemäß dem PA-DSS kann im Versionsschema optional zur Darstellung mehrerer Änderungen ohne Auswirkungen auf die Sicherheit verwendet werden. Ein Platzhalter ist das einzige variable Element des Versionsschemas des Anbieters und er wird als Hinweis darauf verwendet, dass in jeder Version, die durch das Platzhalterelement dargestellt wird, nur kleine Änderungen ohne Auswirkungen auf die Sicherheit vorgenommen wurden. Die Versionsnummer 1.1.x würde beispielsweise die spezifischen Versionen 1.1.2, 1.1.3 usw. abdecken und den Kunden darauf hinweisen, dass die Codebasis zwischen den einzelnen Versionen abgesehen von kosmetischen oder anderen geringfügigen Änderungen praktisch unverändert ist.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
Darstellung von Änderungen mit Auswirkungen auf die Sicherheit verwendet werden könnten. Alle Versionselemente, die nach einem Platzhalterelement kommen, dürfen nicht für die Darstellung von Änderungen mit Auswirkungen auf die Sicherheit verwendet werden. ***Hinweis:*** *Platzhalter dürfen nur im Einklang mit den Angaben im PA-DSS-Programmleitfaden verwendet werden.*	**5.4.3.b** Überprüfen Sie, ob Platzhalter gemäß den Angaben im *PA-DSS-Programmleitfaden* verwendet werden. Zum Beispiel dürfen Elemente, die nach einem Platzhalterelement stehen, nicht für Änderungen mit Auswirkungen auf die Sicherheit verwendet werden.	Die Verwendung von Platzhaltern muss in der Versionierungsmethode des Anbieters vordefiniert sein, und die Platzhalter dürfen nur gemäß den Angaben im *PA-DSS-Programmleitfaden* verwendet werden. ***Hinweis:*** *Die Verwendung von Platzhaltern ist optional und stellt keine Voraussetzung dar.*
	5.4.3.c Stellen Sie durch Befragung der Mitarbeiter und durch Beobachtung der Prozesse für jeden Änderungstyp Folgendes sicher: • Platzhalter werden nie für Änderungen verwendet, die Auswirkungen auf die Sicherheit oder PA-DSS-Anforderungen haben. • Elemente der Versionsnummer, die zur Darstellung von Änderungen ohne Auswirkungen auf die Sicherheit verwendet werden (einschließlich eines Platzhalterelements), werden nie für die Darstellung einer Änderung mit Auswirkungen auf die Sicherheit verwendet.	
	5.4.3.d Wählen Sie eine Stichprobe aus kürzlich vorgenommenen Änderungen an der Zahlungsanwendung aus, und überprüfen Sie die Änderungskontrolldokumentation, in der der Typ der Anwendungsänderung angegeben ist. Überprüfen Sie Folgendes: • Platzhalter werden nicht für Änderungen verwendet, die Auswirkungen auf die Sicherheit oder PA-DSS-Anforderungen haben. • Elemente der Versionsnummer, die zur Darstellung von Änderungen ohne Auswirkungen auf die Sicherheit verwendet werden (einschließlich eines Platzhalterelements), werden nicht für die Darstellung einer Änderung mit Auswirkungen auf die Sicherheit verwendet.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.4.4 Die veröffentlichte Versionierungsmethode des Anbieters muss den Kunden und Integratoren/Wiederverkäufern mitgeteilt werden.	**5.4.4** Überprüfen Sie, ob das *PA-DSS-Implementierungshandbuch* eine Beschreibung der veröffentlichten Versionierungsmethode des Anbieters für Kunden und Integratoren/Wiederverkäufer enthält und Folgendes einschließt: • Details des Versionsschemas, einschließlich des Versionsschemaformats (Anzahl der Elemente, Trennzeichen, Zeichensatz usw.) • Details dazu, wie Änderungen mit Auswirkungen auf die Sicherheit vom Versionsschema angegeben werden • Details dazu, wie sich andere Änderungstypen auf die Version auswirken • Details zu verwendeten Platzhalterelementen, einschließlich der Bestätigung, dass diese nie zur Darstellung von Änderungen mit Auswirkungen auf die Sicherheit verwendet werden	Die Sicherstellung, dass die Versionierungsmethode des Anbieters im *PA-DSS-Implementierungshandbuch* enthalten ist, sorgt dafür, dass die Kunden und Integratoren/Wiederverkäufer die erforderlichen Angaben erhalten, die verdeutlichen, welche Version der Zahlungsanwendung sie verwenden und welche Arten von Änderungen an jeder Version der Zahlungsanwendung vorgenommen wurden.
5.4.5 Wenn interne Versionen dem veröffentlichten Versionsschema zugeordnet werden, muss die Versionierungsmethode die Zuordnung der internen Versionen zu den externen Versionen umfassen.	**5.4.5.a** Überprüfen Sie die dokumentierte Versionierungsmethode dahingehend, ob sie eine Zuordnung der internen Versionen zu den veröffentlichten externen Versionen umfasst. **5.4.5.b** Überprüfen Sie kürzlich vorgenommene Änderungen, um zu bestätigen, dass die Zuordnung der internen Version zum veröffentlichten Versionsschema in Übereinstimmung mit dem Änderungstyp, wie in der dokumentierten Methode festgelegt, aktualisiert wurde.	Einige Anbieter von Zahlungsanwendungen verwenden intern oder als Referenz andere Versionierungsmethoden als die Versionierungsmethode, die für externe (oder öffentliche) Freigaben verwendet wird. In solchen Fällen ist es wichtig, dass beide Versionierungsmethoden genau definiert und dokumentiert werden und die Beziehung zwischen den Methoden sorgfältig dokumentiert wird.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.4.6 Der Softwareanbieter muss einen Prozess implementiert haben, mit dem vor der Freigabe die Konformität von Anwendungsupdates mit der Versionierungsmethode überprüft werden kann.	**5.4.6.a** Überprüfen Sie die dokumentierten Softwareentwicklungsprozesse und die Versionierungsmethode dahingehend, ob ein Prozess implementiert ist, mit dem vor der Freigabe die Konformität von Anwendungsupdates mit der Versionierungsmethode überprüft werden kann.	Es ist von entscheidender Bedeutung, dass Anwendungsanbieter einen Prozess implementiert haben, mit dem sie sicherstellen können, dass Produktupdates dem Zweck und Umfang der geplanten Version entsprechen und dass diese Änderungen den Kunden korrekt mitgeteilt werden. Andernfalls könnten Änderungen an einer Anwendung vorgenommen werden, die die Sicherheit einer Kundenanwendung beeinträchtigen, ohne dass der Kunde davon weiß.
	5.4.6.b Überprüfen Sie durch Befragung der Softwareentwickler und durch Beobachtung der Prozesse, ob vor der Freigabe die Konformität von Anwendungsupdates mit der Versionierungsmethode überprüft wird.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.5 Verfahren zur Risikobewertung (beispielsweise die Erstellung von Bedrohungsmodellen für Anwendungen) werden eingesetzt, um potenzielle Fehler im Anwendungssicherheitsdesign und Sicherheitsrisiken während des Softwareentwicklungsprozesses zu identifizieren. Die Verfahren zur Risikobewertung umfassen Folgendes: • Abdeckung aller Funktionen der Zahlungsanwendung, darunter Funktionen mit Auswirkungen auf die Sicherheit und Funktionen, die Vertrauensgrenzen überschreiten • Bewertung der Entscheidungspunkte der Anwendung, der Prozessabläufe, der Datenflüsse, der Datenspeicherung und der Vertrauensgrenzen • Identifizierung aller Bereiche innerhalb der Zahlungsanwendung, die mit der PAN und/oder SAD oder der CDE (Cardholder Data Environment, Karteninhaberdaten-Umgebung) interagieren, sowie aller prozessorientierter Ergebnisse, die zur Preisgabe von Karteninhaberdaten führen könnten • Liste der potenziellen Bedrohungen und Sicherheitsrisiken aufgrund von Analysen der Flüsse von Karteninhaberdaten und die jeweilige Einteilung in Sicherheitsstufen (beispielsweise hohe, mittlere oder niedrige Priorität) • Implementierung geeigneter Korrektur- und Gegenmaßnahmen während des Entwicklungsprozesses • Dokumentation der Ergebnisse der Risikobewertung für die Überprüfung und Genehmigung durch das Management	**5.5** Überprüfen Sie die dokumentierten Softwareentwicklungsverfahren, und befragen Sie die zuständigen Mitarbeiter, um sicherzustellen, dass der Anbieter während des Softwareentwicklungsprozesses Verfahren zur Risikobewertung einsetzt und dass die Verfahren Folgendes umfassen: • Abdeckung aller Funktionen der Zahlungsanwendung, darunter Funktionen mit Auswirkungen auf die Sicherheit und Funktionen, die Vertrauensgrenzen überschreiten • Bewertung der Entscheidungspunkte der Anwendung, der Prozessabläufe, der Datenflüsse, der Datenspeicherung und der Vertrauensgrenzen • Identifizierung aller Bereiche innerhalb der Zahlungsanwendung, die mit der PAN/SAD oder der CDE (Cardholder Data Environment, Karteninhaberdaten-Umgebung) interagieren, sowie aller prozessorientierter Ergebnisse, die zur Preisgabe von Karteninhaberdaten führen könnten • Liste der potenziellen Bedrohungen und Sicherheitsrisiken aufgrund von Analysen der Flüsse von Karteninhaberdaten und die jeweilige Einteilung in Sicherheitsstufen (beispielsweise hohe, mittlere oder niedrige Priorität) • Implementierung geeigneter Korrektur- und Gegenmaßnahmen während des Entwicklungsprozesses • Dokumentation der Ergebnisse der Risikobewertung für die Überprüfung und Genehmigung durch das Management	Zur Aufrechterhaltung der Qualität und Sicherheit von Zahlungsanwendungen sollten Anwendungsanbieter Verfahren zur Risikobewertung während des Softwareentwicklungsprozesses einsetzen. Die Erstellung von Bedrohungsmodellen ist eine Form der Risikobewertung, die zur Analyse von Konstrukten und Datenflüssen einer Anwendung verwendet werden kann, um Gelegenheiten aufzudecken, bei denen vertrauliche Informationen nicht autorisierten Anwendungsbenutzern preisgegeben werden können. Mithilfe dieser Verfahren können Softwareentwickler und -architekten in der Anfangsphase des Entwicklungsprozesses potenzielle Sicherheitsprobleme identifizieren und beheben, die Anwendungssicherheit verbessern und Entwicklungskosten reduzieren.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
5.6 Der Softwareanbieter muss einen Prozess implementieren, mit dem die endgültige Freigabe der Anwendung und der Anwendungsupdates dokumentiert und autorisiert wird. Die Dokumentation umfasst Folgendes: • Unterschrift einer autorisierten Partei, mit der die Freigabe der Anwendung oder des Anwendungsupdates offiziell genehmigt wird • Bestätigung, dass sich der Anbieter an sichere Entwicklungsprozesse gehalten hat	**5.6.a** Überprüfen Sie die dokumentierten Prozesse, um sicherzustellen, dass die endgültige Freigabe der Anwendung und der Anwendungsupdates genehmigt und dokumentiert werden muss – einschließlich der Unterschrift einer autorisierten Partei, mit der die Freigabe offiziell genehmigt wird, und der Bestätigung, dass alle SDLC-Prozesse eingehalten wurden.	Ein Mitarbeiter im Unternehmen des Zahlungsanwendungsanbieters sollte dafür verantwortlich sein, alle Aspekte der sicheren Entwicklungsprozesse (gemäß den Anforderungen 5.1 bis 5.5) zu überprüfen und sicherzustellen, dass sie eingehalten wurden. Ohne die offizielle Prüfung und Bestätigung durch eine verantwortliche Stelle könnten kritische Sicherheitsprozesse übersehen oder ausgeschlossen werden, was zu Anwendungsfehlern oder einer Beeinträchtigung der Anwendungssicherheit führen könnte.
	5.6.b Überprüfen Sie für eine Stichprobe aus neuen Freigaben der Anwendung oder Anwendungsupdates die Genehmigungsdokumentation, um sicherzustellen, dass Folgendes enthalten ist: • Offizielle Genehmigung und Unterschrift einer autorisierten Partei • Bestätigung, dass alle sicheren Entwicklungsprozesse eingehalten wurden	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 6: Schutz von drahtlosen Übertragungen

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
6.1 Für Zahlungsanwendungen, die Funktechnologien einsetzen, ändern Sie die Anbieterstandardeinstellungen, einschließlich, aber nicht beschränkt auf drahtlose Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen. Die	**6.1** Bei Zahlungsanwendungen, die zur Nutzung von Drahtlostechnologie entwickelt wurden, sowie sonstigen Drahtlosanwendungen im Lieferumfang der Zahlungsanwendung stellen Sie wie folgt sicher, dass die Drahtlosanwendungen nicht die Standardeinstellungen des Anbieters verwenden:	Die Ausnutzung von Drahtlostechnologie ist eine altbewährte Methode für böswillige Personen, um sich Zugriff zu einem Netzwerk und Karteninhaberdaten zu verschaffen. Wenn keine Drahtlosnetzwerke mit ausreichenden

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
Funktechnologie muss sicher implementiert werden. ***Im Sinne der PCI-DSS-Anforderungen 1.2.3 und 2.1.1***	**6.1.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Die Zahlungsanwendung setzt bei der Installation Änderungen der standardmäßigen Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen für alle von der Anwendung gesteuerten drahtlosen Komponenten durch. • Verfahrensweisen für die Änderung von drahtlosen Verschlüsselungsschlüsseln und Kennwörtern, einschließlich SNMP-Zeichenfolgen, die jedes Mal angewendet werden, wenn jemand mit Kenntnis der Schlüssel/Kennwörter das Unternehmen verlässt oder eine andere Position antritt • Anweisungen zum Ändern der standardmäßigen Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen für alle drahtlosen Komponenten, die mit der Zahlungsanwendung bereitgestellt, von ihr aber nicht gesteuert werden • Anweisungen zum Installieren einer Firewall zwischen allen drahtlosen Netzwerken und Systemen, die Karteninhaberdaten speichern • Details zum gesamten drahtlosen Datenverkehr (einschließlich spezifischer Portinformationen), die die Drahtlosfunktion der Zahlungsanwendung verwenden würde • Anweisungen zum Konfigurieren der Firewalls, sodass der gesamte Verkehr zwischen der drahtlosen Umgebung und der Karteninhaberdaten-Umgebung abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt	Sicherheitskonfigurationen (einschließlich der Änderung von Standardeinstellungen) implementiert sind, können Wireless-Sniffer den Datenverkehr belauschen, im Handumdrehen Daten und Kennwörter erfassen und sich Zugriff auf das Netzwerk verschaffen und es schädigen. Aus diesen Gründen dürfen Zahlungsanwendungen nicht die Verwendung von standardmäßigen oder unsicheren Drahtloseinstellungen voraussetzen. Wenn Firewalls nicht den Zugriff von drahtlosen Netzwerken auf die CDE einschränken, könnten sich böswillige Individuen, die sich unerlaubten Zugang zum drahtlosen Netzwerk verschafft haben, mit der CDE verbinden und Kontoinformationen gefährden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	6.1.b Installieren Sie die Anwendung entsprechend dem *PA-DSS-Implementierungshandbuch*, und testen Sie die Anwendung sowie die Drahtloseinstellungen, um für alle Drahtlosfunktionen, die von der Zahlungsanwendung verwaltet werden, Folgendes sicherzustellen: • Die Standardwerte der Verschlüsselungsschlüssel wurden zum Zeitpunkt der Installation geändert. • Standard-SNMP-Community-Zeichenfolgen auf drahtlosen Geräten wurden bei der Installation geändert. • Standardkennwörter/-sätze auf Zugriffspunkten wurden bei der Installation geändert. • Die Firmware auf drahtlosen Geräten wurde aktualisiert, um eine starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen. • Andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen wurden gegebenenfalls geändert.	
	6.1.c Befolgen Sie für alle Drahtlosfunktionen, die von der Zahlungsanwendung verwaltet werden, die Anweisungen im *PA-DSS-Implementierungshandbuch* zum Ändern drahtloser Verschlüsselungsschlüssel, Kennwörter/-sätze und SNMP-Zeichenfolgen. Stellen Sie sicher, dass die Anweisungen im *PA-DSS-Implementierungshandbuch* präzise sind und zur Änderung der drahtlosen Verschlüsselungsschlüssel, Kennwörter und SNMP-Zeichenfolgen führen.	
	6.1.d Befolgen Sie für alle drahtlosen Komponenten, die mit der Zahlungsanwendung bereitgestellt, von ihr aber nicht gesteuert werden, die Anweisungen im *PA-DSS-Implementierungshandbuch* zum Ändern standardmäßiger Verschlüsselungsschlüssel, Kennwörter/-sätze und SNMP-Zeichenfolgen. Stellen Sie sicher, dass die Anweisungen im *PA-DSS-Implementierungshandbuch* präzise sind und zur Änderung der drahtlosen Verschlüsselungsschlüssel, Kennwörter und SNMP-Zeichenfolgen führen.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	6.1.e Installieren Sie die Anwendung, und testen Sie die Drahtlosfunktionen, um sicherzustellen, dass der drahtlose Datenverkehr und die von der Anwendung verwendeten Ports den Angaben im *PA-DSS-Implementierungshandbuch* entsprechen.	
6.2 Zahlungsanwendungen, die Drahtlostechnologie nutzen, müssen die Umsetzung bewährter Branchenverfahren (z. B. IEEE 802.11i) ermöglichen, um die starke Verschlüsselung für die Authentifizierung und Übertragung zu implementieren. ***Hinweis:*** *Die Nutzung von WEP als Sicherheitskontrolle ist verboten.* ***Im Sinne der PCI-DSS-Anforderung 4.1.1***	**6.2.a** Testen Sie für die Zahlungsanwendungen, die zur Nutzung von Drahtlostechnologie entwickelt wurden, alle Drahtlosfunktionen, um sicherzustellen, dass die Anwendung die Best Practices der Branche (zum Beispiel IEEE 802.11.i) einsetzt, um starke Verschlüsselung für die Authentifizierung und Übertragung zu erreichen.	Böswillige Personen verwenden kostenlose und allseits verfügbare Tools, um Drahtloskommunikationen zu belauschen. Durch eine starke Kryptographie kann die Weitergabe vertraulicher Informationen über Drahtlosnetzwerke eingeschränkt werden. Um zu vermeiden, dass sich böswillige Benutzer Zugriff auf Daten in einem Drahtlosnetzwerk verschaffen oder über die Drahtlosnetzwerke andere Systeme oder Daten erreichen, muss eine starke Kryptographie zur Authentifizierung und Übertragung von Karteninhaberdaten eingesetzt werden.
	6.2.b Testen Sie für alle Drahtlosanwendungen im Lieferumfang der Zahlungsanwendung die Drahtlosfunktionen, um sicherzustellen, dass die Best Practices der Branche (zum Beispiel IEEE 802.11.i) eingesetzt werden, um starke Verschlüsselung für die Authentifizierung und Übertragung zu erreichen.	
	6.2.c Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Anweisungen zum Konfigurieren der Anwendung, um für die Authentifizierung und Übertragung Best Practices der Branche (zum Beispiel IEEE 802.11.i) für starke Verschlüsselung einzusetzen, und/oder • Anweisungen zum Konfigurieren aller Drahtlosanwendungen im Lieferumfang der Zahlungsanwendung, um für die Authentifizierung und Übertragung Best Practices der Branche für starke Verschlüsselung einzusetzen	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
6.3 Stellen Sie für die Kunden Anweisungen zur sicheren Nutzung von Drahtlostechnologie bereit. ***Hinweis:*** *Diese Anforderung gilt für alle Zahlungsanwendungen, unabhängig davon, ob die Anwendung zur Nutzung von Drahtlostechnologie entwickelt wurde.* **Im Sinne der *PCI-DSS-Anforderungen 1.2.3, 2.1.1 und 4.1.1***	**6.3** Untersuchen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, um sicherzustellen, dass darin Kunden und Wiederverkäufer/Integratoren bei der Nutzung von Drahtlostechnologie auf PCI-DSS-konforme Art und Weise angewiesen werden, folgende Punkte zu beachten: • Anweisungen zum Ändern aller drahtlosen standardmäßigen Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen bei der Installation • Anweisungen zum Ändern der drahtlosen Verschlüsselungsschlüssel, Kennwörter und SNMP-Zeichenfolgen, die jedes Mal anzuwenden sind, wenn jemand mit Kenntnis der Schlüssel/Kennwörter das Unternehmen verlässt oder eine andere Position antritt • Anweisungen zum Installieren von Firewalls zwischen allen drahtlosen Netzwerken und Systemen, die Karteninhaberdaten speichern, und zum Konfigurieren der Firewalls, sodass der gesamte Verkehr zwischen der drahtlosen Umgebung und der Karteninhaberdaten-Umgebung abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt • Anweisungen zum Einsatz von Best Practices der Branche (zum Beispiel IEEE 802.11i), um eine starke Verschlüsselung bei der Authentifizierung und Übertragung zu erreichen	Anbieter von Zahlungsanwendungen müssen Anweisungen für die Kunden bereitstellen, die beschreiben, wie die Anwendung zu konfigurieren ist, damit die Nutzung von Drahtlostechnologien unterstützt wird, auch wenn die Anwendung nicht ausdrücklich auf die Verwendung in einer drahtlosen Umgebungen ausgelegt ist. Drahtlose Netzwerke sind etwas Alltägliches, und die Kunden sollten über die üblichen drahtlosen Sicherheitseinstellungen informiert werden, die zur Sicherstellung der Zahlungsanwendungssicherheit implementiert werden sollten.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 7: Testen von Zahlungsanwendungen in Bezug auf die Ermittlung von Sicherheitsrisiken und Implementierung von Updates für die Zahlungsanwendung

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
7.1 Softwareanbieter müssen einen Prozess einrichten, mit dem Sicherheitsrisiken wie folgt identifiziert und verwaltet werden: ***Hinweis:*** *Sämtliche zugrunde liegenden Programme oder Systeme, die zusammen mit der Zahlungsanwendung angeboten oder von ihr benötigt werden (z. B. Webserver, Drittanbieterbibliotheken und -programme), müssen in diesem Prozess berücksichtigt werden.* ***Im Sinne der PCI-DSS-Anforderung 6.1***	**7.1.a** Überprüfen Sie die Dokumentation zum Prozess für die Verwaltung von Sicherheitsrisiken dahingehend, ob Verfahrensweisen für Folgendes definiert sind: • Identifizierung neuer Sicherheitsrisiken mithilfe von entsprechenden Informationen aus verlässlichen Quellen • Zuweisung von Risikostufen für alle identifizierten Sicherheitsrisiken • Prüfung der Zahlungsanwendungen und Updates bezüglich des Vorliegens von Sicherheitsrisiken vor der Freigabe **7.1.b** Stellen Sie sicher, dass Prozesse zur Identifizierung neuer Sicherheitsrisiken und zur Implementierung von Korrekturen in der Zahlungsanwendung für sämtliche Software, die mit der Zahlungsanwendung bereitgestellt oder von ihr erfordert wird (etwa Webserver, Drittanbieterbibliotheken und -programme), Anwendung finden.	Anbieter müssen die neuesten Sicherheitsrisiken kennen, die ihre Anwendungen beeinträchtigen können – einschließlich Sicherheitsrisiken in zugrunde liegenden Komponenten oder Softwareprodukten, die mit der Anwendung bereitgestellt werden oder für die Anwendung erforderlich sind. Anbieter von Zahlungsanwendungen, die die neuesten Sicherheitsrisiken in ihren eigenen Anwendungen oder in zugrunde liegenden Komponenten kennen, sollten diese Sicherheitsrisiken dann vor der Freigabe beheben können oder andere Mechanismen implementieren, um die Wahrscheinlichkeit zu verringern, dass das Sicherheitsrisiko ausgenutzt werden kann, falls ein Sicherheitspatch eines Drittanbieters nicht sofort verfügbar ist.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
7.1.1 Identifizieren Sie neue Sicherheitsrisiken mithilfe von entsprechenden Informationen aus verlässlichen Quellen.	**7.1.1** Überprüfen Sie durch Befragung der zuständigen Mitarbeiter und Beobachtung der Prozesse, ob neue Sicherheitsrisiken identifiziert werden: • Sowohl in der Zahlungsanwendung als auch in zugrunde liegenden Softwareprodukten oder Systemen, die mit der Zahlungsanwendung bereitgestellt oder von ihr erfordert werden • Über verlässliche Quellen (beispielsweise Websites des Software-/Systemanbieters sowie NVD (National Vulnerability Database, Nationale Datenbank der Sicherheitsrisiken) von NIST (National Institute of Standards and Technology, Nationales Institut für Standards und Technologie), CVE (Common Vulnerabilities and Exposures, Häufige Sicherheitsrisiken und Gefährdungen) von MITRE und US-CERT-Websites des DHS (Department of Homeland Security, Ministerium für Innere Sicherheit)	Informationen zu Sicherheitsrisiken und/oder Patches für Softwarekomponenten von Drittanbietern sollten aus verlässlichen Quellen bezogen werden. Die Quellen für Informationen zu Sicherheitsrisiken sollten vertrauenswürdig sein. Häufig zählen die Websites von Anbietern, Branchen-Newsgruppen, Mailinglisten und RSS-Feeds ebenso dazu. Branchenquellen sind beispielsweise die National Vulnerability Database von NIST, die Liste mit Common Vulnerabilities and Exposures von MITRE und die US-CERT-Websites des Ministeriums für Innere Sicherheit der Vereinigten Staaten.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
7.1.2 Weisen Sie allen identifizierten Sicherheitsrisiken Risikostufen zu. Dazu gehören auch Sicherheitsrisiken im Zusammenhang mit zugrunde liegenden Softwareprodukten oder Systemen, die mit der Zahlungsanwendung bereitgestellt oder von ihr erfordert werden. ***Hinweis:*** *Die Risikostufen sollten auf den bewährten Verfahren der Branche beruhen und die potenziellen Auswirkungen berücksichtigen. So könnten der CVSS-Basiswert und/oder die Klassifizierung durch den Anbieter und/oder Auswirkungen auf Anwendungsfunktionen als Kriterien für die Einteilung der Sicherheitsrisiken in verschiedene Stufen dienen.* *Bei der Risikoeinstufung müssen zumindest die Sicherheitsrisiken ermittelt werden, die als „hohes Risiko" für die Anwendung gelten. Zusätzlich zu der Risikoeinstufung können einzelne Sicherheitsrisiken als „kritisch" betrachtet werden, falls sie eine unmittelbare Bedrohung darstellen, sich auf wichtige Anwendungskomponenten auswirken oder eine potenzielle Gefährdung darstellen, wenn nicht auf sie eingegangen wird.*	**7.1.2** Überprüfen Sie durch Befragung der zuständigen Mitarbeiter und Beobachtung der Prozesse, ob neuen Sicherheitsrisiken – einschließlich Sicherheitsrisiken im Zusammenhang mit zugrunde liegenden Softwareprodukten oder Systemen, die mit der Zahlungsanwendung bereitgestellt oder von ihr erfordert werden – eine Risikostufe zugewiesen wird.	Sobald ein Anbieter ein Sicherheitsrisiko entdeckt, das seine Anwendung beeinträchtigen könnte, muss das Risiko bewertet und entsprechend eingestuft werden. Dies erfordert einen Prozess, mit dem die Branchenquellen hinsichtlich Informationen zu Sicherheitsrisiken aktiv überwacht werden. Durch die Risikoeinstufung (z. B. „hoch", „mittel" oder „niedrig") ist ein Anbieter in der Lage, die größten Risiken zu erkennen, zu priorisieren und zu beheben (beispielsweise durch die schnellere Freigabe von Patches mit hoher Priorität) und somit die Wahrscheinlichkeit zu reduzieren, dass Sicherheitsrisiken, die das größte Risiko für Kundenumgebungen darstellen, tatsächlich ausgenutzt werden können.
7.1.3 Prüfung der Zahlungsanwendungen und Updates bezüglich des Vorliegens von Sicherheitsrisiken vor der Freigabe	**7.1.3** Überprüfen Sie durch Befragung der zuständigen Mitarbeiter und Beobachtung der Prozesse, ob Zahlungsanwendungen vor der Freigabe dahingehend getestet werden, ob Sicherheitsrisiken vorliegen.	Alle Sicherheitsrisiken-Verwaltungsprozesse des Zahlungsanwendungsanbieters sollten angemessene Prüfverfahren enthalten, um sicherzustellen, dass sämtliche identifizierten Sicherheitsrisiken vor der Freigabe behoben wurden. *Zu den Testmethoden gehören beispielsweise Durchdringungstests und/oder Tests mit zufälligen Daten zur Ermittlung potenzieller Sicherheitsrisiken – indem z. B. falsch gebildete oder unerwartete Daten zugeführt werden oder die Datenbitgröße verändert wird.*

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
7.2 Softwareanbieter müssen einen Prozess für die zeitgerechte Entwicklung und Bereitstellung von Sicherheitspatches und -updates einrichten.	**7.2** Überprüfen Sie die Prozessdokumentation hinsichtlich der Entwicklung und Verteilung von Sicherheitspatches und -upgrades, um sicherzustellen, dass der Prozess Verfahrensweisen für die Punkte 7.2.1 bis 7.2.2 umfasst:	Softwareupdates, die auf Sicherheitsrisiken eingehen, sollten so schnell wie möglich entwickelt und für die Kunden freigegeben werden, nachdem ein kritisches Sicherheitsrisiko erkannt wurde, um den Zeitraum, in dem das Sicherheitsrisiko ausgenutzt werden könnte, sowie die Wahrscheinlichkeit auf ein Minimum zu beschränken.
7.2.1 Patches und Updates werden Kunden auf sichere und vertrauenswürdige Art und Weise zur Verfügung gestellt.	**7.2.1** Überprüfen Sie durch Befragung der zuständigen Mitarbeiter und Beobachtung der Prozesse, ob Patches und Updates Kunden auf sichere und vertrauenswürdige Art und Weise zur Verfügung gestellt werden.	Bei der Verteilung von Sicherheitspatches muss sichergestellt sein, dass böswillige Personen die Updates nicht während der Übertragung abfangen, verändern und anschließend an die nichtsahnenden Kunden weiterleiten können.
7.2.2 Patches und Updates werden Kunden auf eine Art und Weise zur Verfügung gestellt, die die Integrität des Patch- und Updatecodes bewahrt.	**7.2.2.a** Überprüfen Sie durch Befragung der zuständigen Mitarbeiter und Beobachtung der Prozesse, ob Patches und Updates Kunden auf eine Art und Weise zur Verfügung gestellt werden, die die Integrität des Patch- und Updatecodes bewahrt.	Sicherheitsupdates sollten einen Mechanismus im Updateprozess umfassen, mit dem sichergestellt wird, dass der Updatecode nicht ersetzt oder verfälscht wurde. Zu den Beispielen für Integritätsprüfungen gehören u. a. Prüfsummenverfahren und digital signierte Zertifikate.
	7.2.2.b Überprüfen Sie durch Befragung der zuständigen Mitarbeiter und Beobachtung der Updateprozesse für Anwendungen, ob die Integrität von Patches und Updates auf dem Zielsystem vor der Installation getestet wird.	
	7.2.2.c Stellen Sie sicher, dass die Integrität des Patch- und Updatecodes aufrechterhalten wird, indem Sie den Updateprozess mit einem willkürlichen Code durchführen und überprüfen, ob das System das Update zulässt.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
7.2.3 Stellen Sie Anweisungen für Kunden zur sicheren Installation von Patches und Updates zur Verfügung.	**7.2.3** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Wie der Anwender Benachrichtungen zu neuen Patches und Updates kommunizieren will. • Wie Patches und Updates auf sichere und vertrauenswürdige Art und Weise zur Verfügung gestellt werden. • Wie auf Patches und Updates auf eine Art und Weise zugegriffen werden kann, die die Integrität des Patch- und Updatecodes bewahrt.	Unterweisen Sie die Kunden und Integratoren/Wiederverkäufer hinsichtlich des Prozesses, wie man Patches sicher empfängt und installiert, da dies hilft, die Integrität es Update-Prozesses und der Anwendung zu schützen.
7.3 Schließen Sie Versionshinweise für alle Anwendungsupdates, einschließlich Details und Auswirkungen des Updates ein, und geben Sie an, inwiefern sich die Versionsnummer geändert hat, um das Anwendungsupdate widerzuspiegeln.	**7.3.a** Überprüfen Sie die Prozesse für die Freigabe von Updates, und stellen Sie durch Befragung der Mitarbeiter sicher, dass Versionshinweise für alle Updates erstellt werden und Details und Auswirkungen des Updates sowie Angaben dazu enthalten, inwiefern sich die Versionsnummer geändert hat, um das Anwendungsupdate widerzuspiegeln. **7.3.b** Überprüfen Sie für eine Stichprobe aus Anwendungsupdates die Versionshinweise, und stellen Sie sicher, dass sie mit dem Update bereitgestellt werden.	Die Versionshinweise informieren Kunden über Softwareupdates und enthalten Angaben dazu, welche Dateien sich möglicherweise geändert haben und welche Anwendungsfunktionen geändert wurden. Außerdem sind die sicherheitsbezogenen Funktionen angegeben, die betroffen sein können. Darüber hinaus sollte in den Versionshinweisen angegeben sein, wie sich ein bestimmter Patch oder ein bestimmtes Update auf die mit der Patchfreigabe verbundene Gesamtversionsnummer auswirkt.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 8: Unterstützung einer sicheren Netzwerkimplementierung

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
8.1 Die Zahlungsanwendung muss in einer sicheren Netzwerkumgebung implementiert werden können. Die Anwendung darf nicht mit der Nutzung von Geräten, Anwendungen oder Konfigurationen interferieren, die für die PCI-DSS-Konformität erforderlich sind. *Die Zahlungsanwendung darf beispielsweise nicht mit der Installation von Patches, Programmen zum Schutz vor Malware, Firewall-Konfigurationen oder anderen Geräten, Anwendungen oder Konfigurationen interferieren, die für die PCI-DSS-Konformität erforderlich sind.* ***Im Sinne der PCI-DSS-Anforderungen 1, 3, 4, 5, und 6***	**8.1.a** Installieren Sie die Anwendung in einer PCI-DSS-konformen Laborumgebung entsprechend dem *PA-DSS-Implementierungshandbuch.* Testen Sie die Zahlungsanwendung, um nachzuweisen, dass die Anwendung in einem Netzwerk ausgeführt werden kann, das vollkommen PCI-DSS-konform ist. **8.1.b** Testen Sie die Anwendung und die zugrunde liegenden Systeme, um sicherzustellen, dass die Zahlungsanwendung die Nutzung von PCI-DSS-Funktionen in zugrunde liegenden Systemen nicht verhindert oder damit interferiert – d. h. dass die Anwendung beispielsweise nicht die Installation von Patches oder Updates zum Schutz vor Malware verhindert oder mit dem Einsatz anderer PCI-DSS-Funktionen interferiert.	Zahlungsanwendungen sollten so ausgelegt und entwickelt sein, dass durch die Installation und den Einsatz der Anwendung nicht verhindert werden kann, dass ein Unternehmen andere für die PCI-DSS-Konformität erforderliche Kontrollen implementiert. Die Zahlungsanwendung muss beispielsweise in einer Umgebung eingesetzt werden können, in der Antivirenlösungen ausgeführt werden (sie darf z. B. nicht erfordern, dass diese Lösungen deaktiviert oder deinstalliert werden).
8.2 Die Zahlungsanwendung darf nur erforderliche und sichere Dienste, Protokolle, Daemons, Komponenten und zugehörige Software und Hardware nutzen bzw. deren Nutzung voraussetzen, einschließlich jener, die von Drittanbietern für Funktionen der Zahlungsanwendung bereitgestellt werden. *Hinweis: SSL und eine frühe Version von TLS werden nicht als starke Kryptographie betrachtet. Zahlungsanwendungen müssen nicht zwingend SSL oder frühere Versionen von TLS verwenden oder unterstützen. Anwendungen, die TLS verwenden oder unterstützen, müssen nicht zwingend einen Fallback zurück zu SSL zulassen.* ***Im Sinne der PCI-DSS-Anforderung 2.2.3***	**8.2.a** Überprüfen Sie Systemdienste, Protokolle, Daemons, Komponenten und zugehörige Software und Hardware, die von der Zahlungsanwendung aktiviert oder benötigt werden. Stellen Sie sicher, dass ausschließlich erforderliche und sichere Dienste, Protokolle, Daemons, Komponenten und zugehörige Software und Hardware standardmäßig aktiviert werden. **8.2.b** Installieren sie die Anwendung, und testen Sie die Anwendungsfunktionen, um sicherzustellen, dass unsichere Dienste, Daemons, Protokolle oder Komponenten standardmäßig sicher konfiguriert sind, wenn sie von der Anwendung unterstützt werden. **8.2.c** Prüfen Sie, ob das *PA-DSS-Implementierungshandbuch* alle für jegliche Funktionen der Zahlungsanwendung erforderlichen Protokolle, Dienste, Komponenten und zugehörige Software und Hardware, einschließlich solcher, die von Drittanbietern angeboten werden, dokumentiert.	Es gibt zahlreiche Protokolle, die ein Unternehmen unter Umständen benötigt (oder standardmäßig aktiviert hat) und die wiederholt von böswilligen Personen ausgenutzt werden, um ein System oder Netzwerk zu kompromittieren. Die Zahlungsanwendung sollte nicht die Nutzung unsicherer Protokolle, Dienste, Daemons usw. voraussetzen. Wenn die Anwendung die Nutzung unsicherer Dienste, Daemons, Protokolle oder Komponenten unterstützt, müssen diese standardmäßig sicher konfiguriert sein.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
8.3. Die Zahlungsanwendung muss die Nutzung von Diensten oder Protokollen nicht voraussetzen, die den üblichen Einsatz von Zwei-Faktor-Authentifizierungstechnologien verhindern oder damit interferieren. ***Hinweis:*** *Bei der Multi-Faktor-Authentifizierung müssen mindestens zwei der drei Authentifizierungsmethoden (siehe unten) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Multi-Faktor-Authentifizierung. Die Authentifizierungsmethoden, auch bekannt unter der Bezeichnung Faktoren, sind Folgende:* • Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; • etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; • etwas, das Sie sind, wie zum Beispiel biometrische Daten. ***Im Sinne der PCI-DSS-Anforderung 8.3***	**8.3.a** Überprüfen Sie die Funktionen der Zahlungsanwendung, um sicherzustellen, dass sie nicht die Nutzung von Diensten oder Protokollen voraussetzen, die den üblichen Einsatz von Multi-Faktor-Authentifizierungstechnologien verhindern oder damit interferieren. **8.3.b** Identifizieren Sie die von der Anwendung unterstützten Mechanismen für den Remotezugriff, und stellen Sie sicher, dass die Mechanismen nicht die Multi-Faktor-Authentifizierung verhindern.	Zahlungsanwendungen sollten so ausgelegt und entwickelt sein, dass für die Installation und den Einsatz der Anwendung nicht vorausgesetzt werden kann, dass ein Unternehmen Dienste oder Protokolle nutzt, die die Implementierung oder den Einsatz von Mullti-Faktor-Authentifizierungslösungen für einen sicheren Zugriff verhindern. Beispielsweise sollte die Anwendung standardmäßig nicht Port 1812 (der bekanntermaßen RADIUS von RFC 2865 zugewiesen wird) nutzen, wenn RADIUS als Authentifizierungs- und Autorisierungstechnologie unterstützt werden soll. *Beispiele für Multi-Faktor-Technologie sind RADIUS mit Token-Geräten, TACACS mit Token-Geräten oder andere Technologien, die eine Multi-Faktor-Authentifizierungstechnologie bieten.*

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 9: Karteninhaberdaten dürfen nie auf einem mit dem Internet verbundenen Server gespeichert werden

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
9.1 Die Zahlungsanwendung muss so entwickelt sein, dass Webserver und Komponenten für die Speicherung von Karteninhaberdaten (beispielsweise Datenbankserver) sich nicht auf ein und demselben Server befinden müssen und dass die Datenspeicherkomponente nicht in der gleichen Netzwerkzone (beispielsweise einer DMZ) wie der Webserver sein muss. ***Im Sinne der PCI-DSS-Anforderung 1.3.7***	**9.1.a** Identifizieren Sie alle Datenspeicherkomponenten der Zahlungsanwendung (beispielsweise Datenbanken) und alle Webserver. Installieren Sie die Datenspeicherkomponenten und Webserver auf mehreren Servern, und testen Sie die Anwendungsfunktionen auf den verschiedenen Servern. Stellen Sie sicher, dass die Zahlungsanwendung nicht voraussetzt, dass eine Datenspeicherkomponente (z. B. eine Datenbank) auf dem gleichen Server wie ein Webserver installiert ist, um zu funktionieren.	Jede Webserverkomponente einer Zahlungsanwendung ist angesichts der offenen Natur öffentlicher Netzwerke (Internet, öffentliches Drahtlosnetzwerk usw.) und der Natur und Menge der potenziellen Angriffe aus diesen Netzwerken einer beträchtlich höheren Gefährdung ausgesetzt. Komponenten zur Speicherung von Karteninhaberdaten erfordern höheren Schutz als öffentliche Anwendungskomponenten. Wenn sich Karteninhaberdaten innerhalb einer DMZ befinden, ist es aufgrund der geringeren Zahl an zu durchdringenden Schichten für einen externen Angreifer einfacher, auf diese Informationen zuzugreifen.
	9.1.b Installieren Sie Datenspeicherkomponenten und Webserver in unterschiedlichen Netzwerkzonen. Testen Sie alle Anwendungsfunktionen in sämtlichen Netzwerkzonen, um sicherzustellen, dass die Zahlungsanwendung nicht voraussetzt, dass eine Datenspeicherkomponente (beispielsweise eine Datenbank) in derselben Netzwerkzone wie ein Webserver installiert wird, um zu funktionieren.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

	9.1.c Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Anweisungen, dass Karteninhaberdaten nicht auf über das Internet zugänglichen Systemen gespeichert werden dürfen (beispielsweise dürfen Webserver und Datenbankserver sich nicht auf demselben Server befinden) • Anweisungen zum Konfigurieren der Zahlungsanwendung, sodass Systeme zum Speichern von Karteninhaberdaten mithilfe einer DMZ vom Internet abgetrennt werden (beispielsweise indem eine Webserverkomponente in einer DMZ und eine Datenspeicherkomponente in einer anderen internen Netzwerkzone installiert wird) • Eine Liste der Dienste/Ports, die die Anwendung zur Kommunikation zwischen zwei Netzwerkzonen benötigt (damit der Kunde seine Firewall so konfigurieren kann, dass nur die erforderlichen Ports geöffnet sind)	Aus diesem Grund sollten Webserver nie auf dem gleichen Server wie die Datenspeicherkomponente installiert werden. Wenn sich ein Angreifer unbefugten Zugriff auf ein Konto auf einem Webserver verschaffen kann, kann er sich auch ohne zusätzlichen Aufwand Zugriff auf die Datenbank mit Karteninhaberdaten verschaffen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 10: Ermöglichen eines sicheren Remotezugriffs auf Zahlungsanwendungen

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
10.1 Multi-Faktor-Authentifizierung muss für sämtlichen Remotezugriff auf die Zahlungsanwendung, der von außerhalb der Kundenumgebung erfolgt, genutzt werden. ***Hinweis:*** *Bei der Multi-Faktor-Authentifizierung müssen mindestens zwei der drei Authentifizierungsmethoden für die Authentifizierung eingesetzt werden (eine Beschreibung der Authentifizierungsmethoden finden Sie in der PA-DSS-Anforderung 3.1.4).* **Im Sinne der *PCI-DSS-Anforderung 8.3***	**10.1.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass die folgenden Informationen für Kunden und Integratoren/Wiederverkäufer enthalten sind: • Anweisungen, dass zur Einhaltung der PCI-DSS-Anforderungen Multi-Faktor-Authentifizierung für sämtlichen Remotezugriff auf die Zahlungsanwendung, der von außerhalb des Kundennetzwerks erfolgt, genutzt werden muss • Eine Beschreibung der von der Anwendung unterstützten Mechanismen für die Multi-Faktor-Authentifizierung • Anweisungen zum Konfigurieren der Anwendung, damit diese Multi-Faktor-Authentifizierung unterstützt (mindestens zwei der drei in der PA-DSS-Anforderung 3.1.4 beschriebenen Authentifizierungsmethoden)	Die Multi-Faktor-Authentifizierung erfordert mindestens zwei Authentifizierungsmethoden für Zugriffe, die von außerhalb des Netzwerks erfolgen. Anbieter von Zahlungsanwendungen müssen für die Kunden Anweisungen zum Konfigurieren der Anwendung bereitstellen, damit sie die beschriebenen Mechanismen zur Multi-Faktor-Authentifizierung unterstützt, um sicherzustellen, dass diese Mechanismen ordnungsgemäß implementiert werden können und anwendbare PCI-DSS-Anforderungen erfüllen. Die Anforderung hinsichtlich einer Multi-Faktor-Authentifizierung gilt für alle Mitarbeiter mit Remotezugriff, wenn dieser von außerhalb der Kundenumgebung erfolgt.
	10.1.b Wenn der Anwendungsanbieter von außerhalb der Kundenumgebung remote auf die Zahlungsanwendung eines Kunden zugreifen kann, überprüfen Sie die Anbieterrichtlinien, um sicherzustellen, dass der Anbieter die Kundenanforderungen hinsichtlich einer Multi-Faktor-Authentifizierung für alle diese Zugriffe befolgt.	
10.2 Sämtliche Remotezugriffe auf eine Zahlungsanwendung müssen auf eine sichere Art und Weise erfolgen. Das bedeutet Folgendes:	**10.2** Überprüfen Sie den Remotezugriff auf folgende Eigenschaften:	Sämtliche Mechanismen für Remotezugriff, die vom Anbieter der Zahlungsanwendung und/oder Integratoren/Wiederverkäufern

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
10.2.1 Wenn Updates der Zahlungsanwendung per Remotezugriff an Kundensysteme geliefert werden, müssen Softwareanbieter die Kunden auffordern, ihre Remotezugriffstechnologien nur für den Download vom Anbieter zu aktivieren und danach sofort wieder zu deaktivieren. Alternativ müssen Softwareanbieter bei einer Bereitstellung über VPN (Virtual Private Network, virtuelles privates Netzwerk) oder andere Hochgeschwindigkeitsverbindungen Kunden darauf hinweisen, dass ständig aktive Verbindungen durch die ordnungsgemäße Konfiguration einer Firewall oder einer persönlichen Firewall zu sichern sind. ***Im Sinne der PCI-DSS-Anforderungen 1 und 12.3.9***	**10.2.1.a** Wenn Updates einer Zahlungsanwendung per Remotezugriff für Kundennetzwerke bereitgestellt werden, überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass folgende Punkte enthalten sind: • Anweisungen für Kunden und Integratoren/Wiederverkäufer hinsichtlich der sicheren Nutzung von Remotezugriffstechnologien, mit dem Hinweis darauf, dass die von Anbietern und Geschäftspartnern verwendeten Remotezugriffstechnologien nur bei Bedarf aktiviert und nach der Nutzung umgehend wieder deaktiviert werden müssen • Empfehlung für Kunden und Integratoren/Wiederverkäufer, eine sicher konfigurierte Firewall oder persönliche Firewall zu verwenden, wenn der Computer über VPN oder andere Hochgeschwindigkeitsverbindungen verbunden ist, um diese ständig aktiven Verbindungen gemäß PCI-DSS-Anforderung 1 zu sichern	eingesetzt werden – beispielsweise, um von diesen Anbietern bereitstellte Supportdienste zu unterstützen –, sollten alle anwendbaren PCI-DSS-Anforderungen erfüllen.
	10.2.1.b Wenn der Anbieter die Zahlungsanwendung und/oder Updates per Remotezugriff auf die Kundennetzwerke bereitstellt, beobachten Sie, welche Methoden der Anbieter dafür einsetzt, um sicherzustellen, dass sie Folgendes umfassen: • Aktivierung von Technologien für Remotezugriff auf Kundennetzwerke nur im Bedarfsfall und mit sofortiger Deaktivierung nach der Verwendung • Wenn der Remotezugriff über VPN oder eine andere Hochgeschwindigkeitsverbindung erfolgt, muss die Verbindung gemäß PCI-DSS-Anforderung 1 gesichert sein.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
10.2.2 Wenn Anbieter oder Integratoren/Wiederverkäufer auf Zahlungsanwendungen des Kunden remote zugreifen können, müssen für jeden Kunden eindeutige Authentifizierungsinformationen (beispielsweise ein Kennwort/-satz) verwendet werden. ***Im Sinne der PCI-DSS-Anforderung 8.5.1***	**10.2.2** Wenn Anbieter oder Integratoren/Wiederverkäufer auf Zahlungsanwendungen des Kunden remote zugreifen können, stellen Sie durch Überprüfung der Anbieterprozesse und Befragung der Mitarbeiter sicher, dass für jeden Kunden eindeutige Authentifizierungsinformationen (beispielsweise ein Kennwort/-satz) verwendet wird, auf die sie Zugriff haben.	Um zu verhindern, dass mehrere Kundenumgebungen durch die Verwendung der gleichen Anmeldeinformationen kompromittiert werden, sollten Anbieter mit Konten für den Remotezugriff auf Kundenumgebungen unterschiedliche Authentifizierungsinformationen für jeden Kunden verwenden. Erzeugen Sie nicht mithilfe wiederholbarer Formeln Kennwörter, die einfach zu erraten sind. Solche Anmeldeinformationen werden im Laufe der Zeit allgemein bekannt und können von nicht autorisierten Personen verwendet werden, um sich unbefugten Zugriff auf Umgebungen von Kunden des Anbieters zu verschaffen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
10.2.3 Remotezugriff auf Zahlungsanwendungen von Kunden durch Anbieter, Integratoren/Wiederverkäufer oder Kunden muss sicher implementiert sein, beispielsweise folgendermaßen: • Ändern der Standardeinstellungen der Remotezugriffssoftware (beispielsweise die Änderung von Standardkennwörtern und Nutzung eindeutiger Kennwörter für jeden Kunden); • Zulassen von Verbindungen ausschließlich über bestimmte (bekannte) IP-/MAC-Adressen; • Verwendung einer starken Authentifizierung und komplexer Zugriffskennwörter (siehe PA-DSS-Anforderungen 3.1.1 bis 3.1.11); • Ermöglichen einer verschlüsselten Datenübertragung entsprechend der PA-DSS-Anforderung 12.1; • Aktivieren einer Kontosperrung nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche; (siehe PA-DSS-Anforderungen 3.1.9 bis 3.1.10); • Einrichten einer VPN-Verbindung mit einer Firewall, bevor der Zugriff zugelassen wird; • Aktivieren der Protokollfunktion. • Einschränken des Zugriffs auf Kundenumgebungen auf autorisierte Mitarbeiter von Integratoren/Wiederverkäufer. ***Im Sinne der PCI-DSS-Anforderungen 2, 8 und 10***	**10.2.3.a** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass Kunden und Integratoren/Wiederverkäufer darauf hingewiesen werden, dass sämtlicher Remotezugriff auf die Zahlungsanwendung sicher implementiert sein muss, beispielsweise folgendermaßen: • Ändern der Standardeinstellungen der Remotezugriffssoftware (beispielsweise die Änderung von Standardkennwörtern und Nutzung eindeutiger Kennwörter für jeden Kunden); • Zulassen von Verbindungen ausschließlich über bestimmte (bekannte) IP-/MAC-Adressen; • Verwendung einer starken Authentifizierung und komplexer Zugriffskennwörter (siehe PA-DSS-Anforderungen 3.1.1 bis 3.1.11); • Ermöglichen einer verschlüsselten Datenübertragung entsprechend der PA-DSS-Anforderung 12.1; • Aktivieren einer Kontosperrung nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche; (siehe PA-DSS-Anforderungen 3.1.9 bis 3.1.10); • Einrichten einer VPN-Verbindung mit einer Firewall, bevor der Zugriff zugelassen wird; • Aktivieren der Protokollfunktion. • Einschränken des Zugriffs auf Kundenumgebungen auf autorisierte Mitarbeiter. **10.2.3.b** Wenn der Softwareanbieter auf die Zahlungsanwendungen des Kunden remote zugreifen kann, überprüfen Sie durch Beobachtung der Remotezugriffsmethoden und durch Befragung der Mitarbeiter, ob der Remotezugriff sicher implementiert ist.	Anbieter von Zahlungsanwendungen müssen für die Kunden und Integratoren/Wiederverkäufer Anweisungen zum Konfigurieren der Anwendung bereitstellen, damit sie sicheren Remotezugriff unterstützt, um sicherzustellen, dass diese Mechanismen ordnungsgemäß implementiert werden können und PCI-DSS-Anforderungen erfüllen. Diese Anforderung gilt für alle Arten von Remotezugriff auf die Kundenumgebung.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 11: Verschlüsseln von sensiblem Datenverkehr in öffentlichen Netzwerken

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
11.1 Wenn die Zahlungsanwendung Karteninhaberdaten über öffentliche Netzwerke sendet oder eine Übermittlung dieser Daten zulässt, muss sie starke Verschlüsselungsmethoden und Sicherheitsprotokolle unterstützen, damit sensible Karteninhaberdaten während der Übertragung über offene und öffentliche Netzwerke geschützt sind, einschließlich zumindest der Folgenden: • Es werden ausschließlich vertrauenswürdige Schlüssel und Zertifikate akzeptiert. • Das verwendete Protokoll unterstützt ausschließlich sichere Versionen oder Konfigurationen. • Für die verwendete Verschlüsselungsmethode wird die richtige Verschlüsselungsstärke verwendet. ***Hinweis:*** *SSL und eine frühe Version von TLS werden nicht als starke Kryptographie. Zahlungsanwendungen müssen nicht zwingend SSL oder frühere Versionen von TLS verwenden oder unterstützen. Anwendungen, die TLS verwenden oder unterstützen, müssen nicht zwingend einen Fallback zurück zu SSL zulassen.* *Zu den offenen, öffentlichen Netzwerken zählen unter anderem:* • Das Internet • Drahtlostechnologien, darunter 802.11 und Bluetooth • Mobilfunktechnologien wie GSM (Global System for Mobile Communications) und CDMA (Code Division Multiple Access)	**11.1.a** Wenn eine Zahlungsanwendung Karteninhaberdaten über öffentliche Netzwerke sendet bzw. eine solche Übertragung zulässt, stellen Sie sicher, dass eine starke Kryptographie und Sicherheitsprotokolle mit der Anwendung bereitgestellt werden und die Verwendung dieser Technologien beschrieben wird. **11.1.b** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass der Anbieter Kunden oder Integratoren/Wiederverkäufern darin Anweisungen zur Nutzung der starken Kryptographie und der Sicherheitsprotokolle erteilt, die von der Anwendung bereitgestellt werden oder die für den Einsatz mit der Anwendung spezifiziert sind. Dazu gehören Folgende: • Anweisungen, dass starke Kryptographie und Sicherheitsprotokolle verwendet werden müssen, wenn die Karteninhaberdaten über öffentliche Netzwerke übertragen werden • Anweisungen zur Überprüfung, ob nur vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert werden • Anweisungen zum Konfigurieren der Zahlungsanwendung, damit ausschließlich sichere Versionen und sichere Implementierungen von Sicherheitsprotokollen verwendet werden • Anweisungen zum Konfigurieren der Zahlungsanwendung, um einen Fallback zurück zu einer unsicheren Version oder Konfiguration zu vermeiden (z. B., wenn TSS verwendet wird, darf die Anwendung keinen Fallback auf SSL zulassen). • Anweisungen zum Konfigurieren der Zahlungsanwendung, damit die richtige Verschlüsselungsstärke für die verwendete Verschlüsselungsmethode eingesetzt wird	Da böswillige Personen Daten während der Übertragung mühelos abfangen und/oder umleiten können, müssen vertrauliche Informationen während der Übertragung über öffentliche Netzwerke verschlüsselt werden. Eine sichere Übertragung von Karteninhaberdaten setzt die Verwendung vertrauenswürdiger Schlüssel/Zertifikate, eines sicheren Übertragungsprotokolls und eine angemessene Verschlüsselung der Karteninhaberdaten voraus. Beachten Sie, dass einige Protokollimplementierungen (z. B. SSL, SSH Version 1.0 und frühe TLS) dokumentierte Sicherheitsrisiken wie etwa Pufferüberlaufe aufweisen, welche von einem Angreifer ausgenutzt werden könnten, um die Kontrolle über das betroffene System zu erlangen. Ganz gleich, welche Sicherheitsprotokolle für die Zahlungsanwendung eingesetzt werden, stellen Sie sicher, dass sie standardmäßig so konfiguriert sind, ausschließlich sichere Konfigurationen und Versionen zu verwenden, um zu vermeiden, dass eine unsichere Verbindung verwendet wird.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
• General Packet Radio Service (GPRS) • Satellitenverbindungen ***Im Sinne der PCI-DSS-Anforderung 4.1***	**11.1.c** Wenn starke Kryptographie und Sicherheitsprotokolle mit der Zahlungsanwendung bereitgestellt werden, installieren Sie die Anwendung, und testen Sie sie gemäß den Anweisungen im *PA-DSS-Implementierungshandbuch*, um Folgendes sicherzustellen: • Das Protokoll wird standardmäßig so implementiert, dass nur vertrauenswürdige Schlüssel und/oder Zertifikate verwendet werden. • Das Protokoll wird standardmäßig so implementiert, dass ausschließlich sichere Konfigurationen verwendet und keine unsicheren Versionen oder Konfigurationen unterstützt werden. • Das Protokoll wird standardmäßig so installiert, dass ein Fallback zurück zu einer unsicheren Version oder Konfiguration nicht zugelassen wird (z. B., wenn TSS verwendet wird, darf die Anwendung keinen Fallback auf SSL zulassen). • Für die verwendete Verschlüsselungsmethode wird die richtige Verschlüsselungsstärke implementiert.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
11.2 Wenn die Zahlungsanwendung die Übermittlung von PANs über Messaging-Technologien für Endbenutzer zulässt (z. B. E-Mail, Instant Messaging, Chat), muss die Zahlungsanwendung eine Lösung bieten, die die PAN unleserlich macht oder eine starke Kryptographie implementiert oder die Verwendung einer starken Kryptographie zur Verschlüsselung von PANs spezifiziert. ***Im Sinne der PCI-DSS-Anforderung 4.2***	**11.2.a** Wenn die Zahlungsanwendung die Übermittlung von PANs mithilfe von Messaging-Technologien für Endbenutzer gestattet und/oder zulässt, stellen Sie sicher, dass eine Lösung bereitgestellt wird, die die PAN unleserlich macht oder eine starke Kryptographie implementiert oder dass Anweisungen zur Verwendung einer solchen gegeben werden.	E-Mail, Instant Messaging und Chats können in internen und öffentlichen Netzwerken während der Übertragung mithilfe von Paket-Sniffing leicht abgefangen werden. Verwenden Sie diese Messaging-Tools nicht zur Übermittlung von PANs, außer wenn die Zahlungsanwendung die Verwendung von starker Kryptographie bei diesen Technologien ermöglicht oder die PAN unleserlich macht.
	11.2.b Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass der Anbieter Kunden oder Integratoren/Wiederverkäufern darin Anweisungen zur Nutzung einer Lösung erteilt, die mit der Anwendung bereitgestellt oder die für den Einsatz mit der Anwendung spezifiziert wird. Dazu gehören Folgende: • Anweisungen zur Verwendung der definierten Lösung, um die PAN unleserlich zu machen oder die PAN mit starker Kryptographie zu sichern • Anweisung, dass die PAN immer unleserlich gemacht oder mittels einer starken Kryptographie gesichert werden muss, wenn sie über Messaging-Technologien für Endbenutzer übermittelt wird	
	11.2.c Wenn eine Lösung mit der Zahlungsanwendung bereitgestellt wird, installieren und testen Sie die Anwendung, um sicherzustellen, dass die Lösung die PAN unleserlich macht oder starke Kryptographie implementiert.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 12: Sichern des gesamten Nichtkonsolen-Verwaltungszugriffs

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.1 Wenn die Zahlungsanwendung Nichtkonsolen-Verwaltungszugriff zulässt, verschlüsseln Sie diesen gesamten Zugriff mit einer starken Kryptographie. ***Hinweise:*** • *Klartextprotokolle wie Telnet oder rlogin dürfen grundsätzlich nicht für Verwaltungszugriff genutzt werden.* • *SSL und eine frühe Version von TLS werden nicht als starke Kryptographie betrachtet. Zahlungsanwendungen müssen nicht zwingend SSL oder frühere Versionen von TLS verwenden oder unterstützen. Anwendungen, die TLS verwenden oder unterstützen, müssen nicht zwingend einen Fallback zurück zu SSL zulassen.* ***Im Sinne der PCI-DSS-Anforderung 2.3***	**12.1.a** Installieren Sie die Zahlungsanwendung in einem Labor, und testen Sie Nichtkonsolen-Verwaltungsverbindungen, um sicherzustellen, dass eine starke Verschlüsselungsmethode aufgerufen wird, bevor das Administratorkennwort eingegeben werden muss. **12.1.b** Überprüfen Sie die Konfigurationseinstellungen der Zahlungsanwendung, um sicherzustellen, dass Klartextprotokolle wie Telnet und rlogin von der Zahlungsanwendung nicht für Nichtkonsolen-Verwaltungszugriff verwendet werden. **12.1.c** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass Anweisungen für Kunden und Integratoren/Wiederverkäufer enthalten sind, wie die Anwendung zu konfigurieren ist, damit eine starke Kryptographie für die Verschlüsselung von Nichtkonsolen-Verwaltungszugriff verwendet wird.	Wenn die Fernadministration nicht mit einer sicheren Authentifizierung und verschlüsselten Kommunikationen erfolgt, können vertrauliche administrative oder Informationen auf Betriebsebene (wie etwa Administrator-Kennwörter) Lauschangriffen ausgesetzt sein. Böswillige Personen könnten mithilfe dieser Informationen auf die Anwendung und/oder das Netzwerk zugreifen, Berechtigungen ändern und Daten entwenden.
12.1.1 Weisen Sie Kunden an, den gesamten Nichtkonsolen-Verwaltungszugriff mit einer starken Kryptographie für webbasierte Verwaltung und andere Nichtkonsolen-Verwaltungszugriffe zu verschlüsseln. ***Hinweis:*** *Klartextprotokolle wie Telnet oder rlogin dürfen grundsätzlich nicht für Verwaltungszugriff genutzt werden.* ***Im Sinne der PCI-DSS-Anforderung 2.3***	**12.1.1** Überprüfen Sie das vom Anbieter erstellte *PA-DSS-Implementierungshandbuch*, und stellen Sie sicher, dass Kunden und Integratoren/Wiederverkäufer darin angewiesen werden, eine starke Kryptographie für die Verschlüsselung des gesamten Nichtkonsolen-Verwaltungszugriffs zu implementieren.	Anbieter von Zahlungsanwendungen müssen Anweisungen für Kunden und Integratoren/Wiederverkäufer bereitstellen, wie die Anwendung für die Verwendung von starker Kryptographie für die Verschlüsselung des gesamten Nichtkonsolen-Verwaltungszugriffs konfiguriert wird. Auf diese Weise wird sichergestellt, dass Sicherheitskontrollen richtig implementiert werden und den PCI-DSS- und PA-DSS-Richtlinien entsprechen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.2 Verwenden Sie eine Multi-Faktor-Authentifizierung für alle Mitarbeiter mit Nichtkonsolen-Verwaltungszugriff. ***Hinweis:*** *Bei der Multi-Faktor-Authentifizierung müssen mindestens zwei der drei Authentifizierungsmethoden für die Authentifizierung eingesetzt werden (eine Beschreibung der Authentifizierungsmethoden finden Sie in der PA-DSS-Anforderung 3.1.4).* ***Im Sinne der PCI-DSS-Anforderung 8.3***	**12.2.a** Überprüfen Sie, ob eine Multi-Faktor-Authentifizierung mit der Anwendung bereitgestellt wird oder die Verwendung hiervon beschrieben wird.	Der Verwaltungszugriff erfordert ein höheres Maß an Gewissheit über die Idendität der Person, die versucht Zugriff zu erhalten. Da eine Multi-Faktor-Authentifizierung auf Anwendungs-, System- oder Netzwerkebene implementiert werden kann, ist es nicht erforderlich, dass alle Anwendungen über eine Mullti-Faktor-Authentifizierungslösung verfügen. Anbieter von Zahlungsanwendungen können entweder mit ihren Anwendungen Multi-Faktor-Authentifizierungen bereitstellen, oder Anweisungen für ihre Benutzer und Integratoren/Wiederverkäufer beifügen, um eine Multi-Faktor-Authentifizierung für den Verwaltungszugriff auf die Anwendung zu installieren.
	12.2.b Überprüfen Sie das vom Anbieter erstellte*PA-DSS-Implementierungshandbuch* und stellen Sie sicher, dass es Anweisungen zur Nutzung der Multi-Faktor-Authentifizierung für Kunden und Integratoren/Wiederverkäufer enthält, einschließlich: • Anweisungen, dass die Multi-Faktor-Authentifizierung für alle Mitarbeiter mit Nichtkonsolen-Verwaltungszugriff auf das CDE eingesetzt wird • Verfahren für die Nutzung der Multi-Faktor-Authentifizierung, die mit der Anwendung bereitgestellt werden (falls bereitgestellt).	
	12.2.c Falls die Multi-Faktor-Authentifizierung mit der Zahlungsanwendung bereitgestellt wird, installieren und testen Sie die Anwendung, um zu überprüfen, ob die Multi-Faktor-Authentifizierung angewandt wird, bevor der Zugriff gestattet wird.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 13: Pflegen eines PA-DSS-Implementierungshandbuchs für Kunden, Wiederverkäufer und Integratoren

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
13.1 Entwickeln, pflegen und verteilen Sie *PA-DSS-Implementierungshandbücher* für Kunden, Wiederverkäufer und Integratoren, die die folgenden Anforderungen erfüllen:	**13.1** Überprüfen Sie das *PA-DSS-Implementierungshandbuch* und zugehörige Prozesse des Anbieters, und befragen Sie die Mitarbeiter, um Folgendes sicherzustellen: • Das *PA-DSS-Implementierungshandbuch* wird mit der Anwendung an alle Kunden, Wiederverkäufer und Integratoren weitergeleitet. • Der Anbieter verfügt über einen Mechanismus, mit dem das *PA-DSS-Implementierungshandbuch* Kunden, Wiederverkäufern und Integratoren auf Anfrage bereitgestellt wird.	Ein gut konzipiertes und ausführliches *PA-DSS-Implementierungshandbuch* unterstützt Kunden und Integratoren/Wiederverkäufer bei der Implementierung der geeigneten Sicherheitsmaßnahmen und Konfigurationen innerhalb der Zahlungsanwendung und in den zugrunde liegenden Komponenten, sodass die relevanten PCI-DSS- und PA-DSS-Richtlinien zum Schutz vom Karteninhaberdaten erfüllt werden.
13.1.1 Bereitstellung relevanter und für die Anwendung spezifischer Informationen für Kunden, Wiederverkäufer und Integratoren	**13.1.1** Überprüfen Sie das *PA-DSS-Implementierungshandbuch*, und stellen Sie Folgendes sicher: • Der Name und die Version der Zahlungsanwendung, auf die sich das Handbuch bezieht, sind deutlich angegeben. • Es sind Details zu allen Abhängigkeiten der Anwendung angegeben, die für eine PCI-DSS-konforme Konfiguration der Anwendung erforderlich sind.	
13.1.2 Sämtliche Anforderungen in diesem Dokument werden behandelt, wann immer auf das *PA-DSS-Implementierungshandbuch* eingegangen wird.	**13.1.2** Überprüfen Sie das *PA-DSS-Implementierungshandbuch* , und stellen Sie mithilfe von Anhang A sicher, dass im *PA-DSS-Implementierungshandbuch* auf alle verwandten Anforderungen in diesem Dokument eingegangen wird.	
13.1.3 Eine Überprüfung wird mindestens jährlich und nach Änderungen an der Anwendung oder an PA-DSS-Anforderungen durchgeführt, und das Handbuch wird nach Bedarf aktualisiert, damit es immer dem aktuellen Stand aller Änderungen mit Auswirkungen auf die Anwendung und der	**13.1.3.a** Stellen Sie durch Überprüfung des *PA-DSS-Implementierungshandbuchs* und Befragung der Mitarbeiter sicher, dass das *PA-DSS-Implementierungshandbuch* gemäß den folgenden Anforderungen geprüft wird: • Mindestens jährlich • Nach Änderungen an der Anwendung • Nach Änderungen an den PA-DSS-Anforderungen	Bei jedem Anwendungsupdate werden Systemfunktionen und – in einigen Fällen – kritische Anwendungs-Sicherheitsmechanismen geändert oder eingeführt. Wenn das *PA-DSS-Implementierungshandbuch* nicht dem aktuellen Stand der neuesten Zahlungsanwendungsversionen

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
Anforderungen in diesem Dokument entspricht.	**13.1.3.b** Stellen Sie sicher, dass das *PA-DSS-Implementierungshandbuch* nach Bedarf aktualisiert wird, um auf dem gleichen Stand wie Folgendes zu bleiben: • Änderungen an den PA-DSS-Anforderungen • Änderungen an der Anwendung oder ihren Abhängigkeiten	entspricht, könnten Kunden und Integratoren/Wiederverkäufer kritische Anwendungs-Sicherheitskontrollen übersehen oder falsch konfigurieren, was zur Folge haben könnte, dass ein Angreifer solche Sicherheitsmechanismen umgehen und sich Zugriff auf vertrauliche Daten verschaffen kann.
	13.1.3.c Überprüfen Sie das *PA-DSS-Implementierungshandbuch* und verwandte Prozesse des Anbieters, und befragen Sie die Mitarbeiter, um sicherzustellen, dass der Anbieter einen Mechanismus implementiert hat, mit dem Kunden, Wiederverkäufer und Integratoren über Updates informiert werden und aktualisierte Versionen nach Bedarf bereitgestellt werden.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anforderung 14: Zuweisen von PA-DSS-Verantwortlichkeiten an Mitarbeiter und Pflegen von Schulungsprogrammen für Mitarbeiter, Kunden, Wiederverkäufer und Integratoren

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
14.1 Bereitstellung von Schulungen in Informationssicherheit und PA-DSS für Mitarbeiter des Anbieters mit PA-DSS-Verantwortlichkeiten – mindestens einmal jährlich	**14.1** Überprüfen Sie das Schulungsmaterial, und befragen Sie die zuständigen Mitarbeiter, um sicherzustellen, dass alle Mitarbeiter des Anbieters mit PA-DSS-Verantwortlichkeiten mindestens einmal jährlich eine Schulung in PA-DSS und Informationssicherheit erhalten.	Damit eine Zahlungsanwendung gemäß den PA-DSS-Richtlinien effektiv konzipiert werden kann, sollten die Mitarbeiter des Anbieters der Zahlungsanwendung mit PA-DSS und ihren Verantwortlichkeiten in Bezug auf laufende PA-DSS-Bewertungen vertraut sein. Es liegt in der Verantwortung des Anbieters der Zahlungsanwendung, sicherzustellen, dass seine Mitarbeiter eine angemessene Ausbildung in diesen Bereichen erhalten haben.
14.2 Zuweisung von Rollen und Verantwortlichkeiten an Mitarbeiter des Anbieters, einschließlich der Folgenden: • Gesamtverantwortung dafür, dass alle PA-DSS-Anforderungen eingehalten werden • Kenntnis aller neuen Änderungen im PA-DSS-Programmleitfaden des PCI SSC • Sicherstellung, dass sichere Codierungsverfahren eingehalten werden • Sicherstellung, dass Integratoren/Wiederverkäufer Schulungen und Begleitmaterial erhalten • Sicherstellung, dass alle Mitarbeiter der Anbieter mit PA-DSS-Verantwortlichkeiten, einschließlich Entwickler, Schulungen erhalten	**14.2.a** Überprüfen Sie die dokumentierten Verantwortlichkeiten dahingehend, ob die Verantwortung für folgende Rollen offiziell zugewiesen wurde: • Gesamtverantwortung dafür, dass alle PA-DSS-Anforderungen eingehalten werden • Kenntnis aller neuen Änderungen im PA-DSS-Programmleitfaden des PCI SSC • Sicherstellung, dass sichere Codierungsverfahren eingehalten werden • Sicherstellung, dass Integratoren/Wiederverkäufer Schulungen und Begleitmaterial erhalten • Sicherstellung, dass alle Mitarbeiter der Anbieter mit PA-DSS-Verantwortlichkeiten, einschließlich Entwickler, Schulungen erhalten	Im Unternehmen eines jeden Anbieters von Zahlungsanwendungen sollte einer verantwortlichen Partei (entweder einem Einzelnen oder einem Team) die Verantwortung für PA-DSS offiziell übertragen werden, um sicherzustellen, dass alle PA-DSS-Anforderungen eingehalten werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	14.2.b Befragen Sie die Mitarbeiter, denen die Verantwortung für die folgenden Rollen übertragen wurde, um zu bestätigen, dass die Rollen und Verantwortlichkeiten definiert sind und verstanden werden: • Gesamtverantwortung dafür, dass alle PA-DSS-Anforderungen eingehalten werden • Kenntnis aller neuen Änderungen im PA-DSS-Programmleitfaden des PCI SSC • Sicherstellung, dass sichere Codierungsverfahren eingehalten werden • Sicherstellung, dass Integratoren/Wiederverkäufer Schulungen und Begleitmaterial erhalten • Sicherstellung, dass alle Mitarbeiter der Anbieter mit PA-DSS-Verantwortlichkeiten, einschließlich Entwickler, Schulungen erhalten	
14.3 Entwicklung und Implementierung von Schulungs- und Kommunikationsprogrammen für Integratoren und Wiederverkäufer von Zahlungsanwendungen Die Schulungen sollten mindestens Folgendes umfassen: • PCI-DSS-konforme Implementierung der Zahlungsanwendung und verwandter Systeme und Netzwerke • Alle Elemente in diesem Dokument (und in Anhang A) mit Bezug auf das *PA-DSS-Implementierungshandbuch*	**14.3.a** Überprüfen Sie das Schulungsmaterial für Integratoren und Wiederverkäufer, und bestätigen Sie, dass das Material Folgendes umfasst: • Schulung in der PCI-DSS-konformen Implementierung der Zahlungsanwendung und verwandter Systeme und Netzwerke • Alle Elemente in diesem Dokument (und in Anhang A) mit Bezug auf das *PA-DSS-Implementierungshandbuch*	Wenn eine Anwendung nicht ordnungsgemäß konfiguriert, gewartet und unterstützt wird, kann dies zu Sicherheitsrisiken in der Karteninhaberdaten-Umgebung des Kunden führen, die dann für Angriffe ausgenutzt werden können. Anwendungsanbieter sollten für Integratoren/Wiederverkäufer eine Schulung in der sicheren Installation und Konfiguration der Anwendung bereitstellen, um sicherzustellen, dass die Anwendung PCI-DSS-Konformität fördert, wenn sie in der Kundenumgebung installiert ist. Es liegt in der Verantwortung des Anbieters der Zahlungsanwendung, Schulungen für Integratoren und Wiederverkäufer in diesen Bereichen bereitzustellen.
	14.3.b Überprüfen Sie die Kommunikationsprogramme und verwandte Prozesse des Anbieters, und befragen Sie die Mitarbeiter des Anbieters, um Folgendes sicherzustellen: • Schulungsmaterial wird für Integratoren und Wiederverkäufer bereitgestellt. • Der Anbieter hat einen Mechanismus implementiert, mit dem Integratoren und Wiederverkäufer auf Anfrage aktualisiertes Material bereitgestellt wird.	
	14.3.c Wählen Sie stichprobenartig Integratoren und Wiederverkäufer aus und befragen Sie sie, um zu überprüfen, ob sie die Schulung und das Schulungsmaterial vom Anwendungsanbieter erhalten haben.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderungen	Prüfverfahren	Leitfaden
	14.3.d Überprüfen Sie die Nachweise, dass Integratoren und Wiederverkäufer das Schulungsmaterial vom Softwareanbieter erhalten haben.	
14.3.1 Überprüfen Sie das Schulungsmaterial mindestens einmal jährlich und nach Änderungen an der Anwendung oder an den PA-DSS-Anforderungen. Aktualisieren Sie das Schulungsmaterial nach Bedarf, damit die Dokumentation immer dem aktuellen Stand der neuen Zahlungsanwendungsversionen und Änderungen an den PA-DSS-Anforderungen entspricht.	**14.3.1.a** Überprüfen Sie das Schulungsmaterial für Integratoren und Wiederverkäufer, und stellen Sie sicher, dass Folgendes zutrifft: • Das Schulungsmaterial wird mindestens einmal jährlich und nach Änderungen an der Anwendung oder an den PA-DSS-Anforderungen überprüft. • Das Schulungsmaterial wird nach Bedarf aktualisiert, damit die Dokumentation immer dem aktuellen Stand der neuen Zahlungsanwendungsversionen und Änderungen an den PA-DSS-Anforderungen entspricht.	Das Schulungsmaterial für Mitarbeiter des Anbieters der Zahlungsanwendung, Integratoren und Wiederverkäufer sollte mindestens einmal jährlich aktualisiert werden, um sicherzustellen, dass das Material immer dem aktuellsten Stand der neuesten Anwendungsversionen und PA-DSS-Anforderungen entspricht. Veraltetes Schulungsmaterial kann die Wirkung der Schulungsprogramme zunichte machen, was schlecht konzipierte Sicherheitsfunktionen in der Anwendung oder ungeeignete Anwendungskonfigurationen der Integratoren und Wiederverkäufer zur Folge haben kann.
	14.3.1.b Überprüfen Sie den Vertriebsprozess für neue Versionen von Zahlungsanwendungen, und stellen Sie sicher, dass die aktualisierte Dokumentation mit der aktualisierten Zahlungsanwendung an die Integratoren und Wiederverkäufer geliefert wird.	
	14.3.1.c Wählen Sie stichprobenartig Integratoren und Wiederverkäufer aus und befragen Sie sie, um zu überprüfen, ob sie das aktualisierte Schulungsmaterial vom Anwendungsanbieter erhalten haben.	

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anhang A: Inhaltszusammenfassung für das *PA-DSS-Implementierungshandbuch*

Mit diesem Anhang sollen die PA-DSS-Anforderungen, die in Themen im *PA-DSS-Implementierungshandbuch* behandelt werden, zusammengefasst werden, der Inhalt des *PA-DSS-Implementierungshandbuchs*, das Kunden und Integratoren/Wiederverkäufern bereitgestellt wird (siehe „PA-DSS-Implementierungshandbuch“ auf Seite 11), erläutert werden sowie auf die jeweiligen Verantwortlichkeiten für die Implementierung entsprechender Kontrollen eingegangen werden.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
1.1.4	Löschen sensibler Authentifizierungsdaten, die von vorherigen Versionen der Zahlungsanwendung gespeichert wurden.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Verlaufsdaten müssen entfernt werden (Verfolgungsdaten, Kartenüberprüfungscodes, PINs oder PIN-Blöcke, die von vorherigen Versionen der Zahlungsanwendung gespeichert wurden). ▪ Anweisungen zum Löschen von Verlaufsdaten ▪ Hinweis, dass das Entfernen für die PCI-DSS-Konformität absolut erforderlich ist	**Softwareanbieter**: Bereitstellen eines Tools oder einer Verfahrensweise, mit dem bzw. der Kunden von früheren Versionen gespeicherte vertrauliche Authentifizierungsdaten sicher entsprechend der PA-DSS-Anforderung 1.1.4 entfernen können **Kunden und Integratoren/Wiederverkäufer**: Löschen sämtlicher Verlaufsdaten entsprechend dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 1.1.4.
1.1.5	Löschen sämtlicher sensibler Authentifizierungsdaten (Prä-Autorisierung), die im Rahmen einer Fehlerbehebung bei der Zahlungsanwendung erhoben wurden.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Sensible Authentifizierungsdaten (Prä-Autorisierung) dürfen nur zur Lösung spezifischer Probleme erhoben werden. ▪ Diese Daten dürfen nur an speziellen, bekannten Speicherorten mit eingeschränktem Zugriff aufbewahrt werden. ▪ Es dürfen lediglich begrenzte Datenmengen, die zur Lösung eines spezifischen Problems benötigt werden, erhoben werden. ▪ Vertrauliche Authentifizierungsdaten müssen während der Speicherung verschlüsselt sein. ▪ Die Daten sind nach der Verwendung umgehend sicher zu löschen.	**Softwareanbieter**: Keine Speicherung von vertraulichen Authentifizierungsdaten; Beheben von Kundenproblemen entsprechend der PA-DSS-Anforderung 1.1.5.a **Kunden und Integratoren/Wiederverkäufer:** Keine Speicherung von vertraulichen Authentifizierungsdaten; Beheben sämtlicher Probleme entsprechend dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 1.1.5.a

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
2.1	Sicheres Löschen von Karteninhaberdaten nach einer vom Kunden festgelegten Aufbewahrungsphase	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Anweisungen, dass Karteninhaberdaten, die die vom Kunden festgelegte Aufbewahrungsfrist überschritten haben, gelöscht werden müssen ▪ Eine Liste aller Speicherorte, an denen die Zahlungsanwendung Karteninhaberdaten aufbewahrt (sodass der Kunde weiß, wo die zu löschenden Daten sich befinden) ▪ Erforderliche Anweisungen für die Kunden, damit sie Karteninhaberdaten sicher löschen können, wenn sie nicht länger zu juristischen, gesetzlichen oder geschäftlichen Zwecken benötigt werden ▪ Anweisungen zum sicheren Löschen der von der Zahlungsanwendung gespeicherten Karteninhaberdaten, einschließlich der Daten, die in zugrunde liegenden Softwareanwendungen oder Systemen (z. B. Betriebssysteme, Datenbanken usw.) aufbewahrt werden ▪ Anweisungen zur Konfiguration der zugrunde liegenden Software oder Systeme (z. B. Betriebssysteme, Datenbanken usw.), um einer unbeabsichtigten Erfassung oder Aufbewahrung der Karteninhaberdaten vorzubeugen.	**Softwareanbieter**: Information der Kunden, dass Karteninhaberdaten, die die vom Kunden festgelegte Aufbewahrungsphase überschritten haben, sicher gelöscht werden müssen – wenn Karteninhaberdaten von der Zahlungsanwendung und in zugrunde liegenden Softwareprodukten oder Systemen gespeichert werden –, und Anweisungen zum sicheren Löschen von Karteninhaberdaten, die von der Zahlungsanwendung gespeichert wurden **Kunden und Integratoren/Wiederverkäufer**: Sicheres Löschen von Karteninhaberdaten, die die vom Kunden festgelegte Aufbewahrungsphase überschritten haben, entsprechend dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 2.1

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
2.2	Maskieren Sie die PAN, wenn sie bei der Anzeige so maskiert ist, dass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Details zu allen Einzelfällen, in denen die PAN abgebildet wird, darunter POS-Geräte, Bildschirme, Protokolle und Belege ▪ Bestätigung, dass die Zahlungsanwendung die PAN standardmäßig in allen Anzeigen maskiert ▪ Anweisungen dazu, wie die Zahlungsanwendung zu konfigurieren ist, damit nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund die vollständige PAN einsehen können (umfasst auch die Anzeige der vollständigen PAN)	**Softwareanbieter**: Bereitstellung von Anweisungen für Kunden zum Maskieren der PAN, damit nur die Mitarbeiter mit einem geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können- **Kunden und Integratoren/Wiederverkäufer**: Maskieren von abgebildeten PANs, damit nur die Mitarbeiter mit einem geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können, entsprechend dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 2.2

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
2.3	Unleserlich machen der PAN an allen Speicherorten (auch auf tragbaren digitalen Medien, Sicherungsmedien und in Protokollen)	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Details zu allen konfigurierbaren Optionen für jede Methode, die von der Anwendung verwendet wird, um Karteninhaberdaten unleserlich zu machen, und Anweisungen dazu, wie jede Methode für alle Speicherorte zu konfigurieren ist, an denen Karteninhaberdaten von der Zahlungsanwendung gespeichert werden (gemäß der PA-DSS-Anforderung 2.1) ▪ Eine Liste aller Fälle, in denen Karteninhaberdaten für den Kunden ausgegeben werden können, um außerhalb der Zahlungsanwendung gespeichert zu werden, und die Information, dass der Kunde dafür verantwortlich ist, die PAN in solchen Fällen unleserlich zu machen. ▪ Eine Anleitung, für den Fall, dass Debugging-Protokolle aktiviert werden (beipielsweise für Fehlerbehebungszwecke), eine Anleitung aufzunehmen, und auch um eine PAN einzuschließen, müssen die Protokolle in Übereinstimmung mit PCI DSS geschützt werden, deaktiviert werden, sobald die Fehlerbehebung abgeschlossen ist und sicher gelöscht werden, wenn sie nicht mehr benötigt werden.	**Softwareanbieter**: Bereitstellung von Anweisungen für den Kunden, mit denen die PAN an allen Speicherorten und an allen Stellen, an denen sie von der Anwendung ausgegeben wird, unleserlich gemacht werden kann **Kunden und Integratoren/Wiederverkäufer**: Unleserlich machen der PAN an allen Speicherorten entsprechen dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 2.3

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
2.4	Schützen von Schlüsseln vor Weitergabe und Missbrauch, die für den Schutz der Karteninhaberdaten eingesetzt werden.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Schränken Sie den Zugriff auf Schlüssel auf die unbedingt notwendige Anzahl von Wächtern ein. ▪ Bewahren Sie Schlüssel sicher und an so wenigen Orten und in so wenigen Formen wie möglich auf.	**Softwareanbieter**: Anweisung der Kunden, dass zum Schutz von Karteninhaberdaten verwendete Schlüssel sicher an so wenigen Orten wie möglich aufbewahrt werden müssen und dass so wenig Schlüsselwächter wie möglich Zugriff auf diese Schlüssel haben dürfen **Kunden und Integratoren/Wiederverkäufer**: Sicheres Aufbewahren der Schlüssel an so wenigen Orten wie möglich und Beschränkung des Zugriffs auf diese Schlüssel auf so wenig Schlüsselwächter wie möglich entsprechend dem*PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 2.4
2.5	Implementieren von Schlüsselverwaltungsprozessen und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Anleitungen zum sicheren Generieren, Verteilen, Schützen, Ändern, Speichern und Zurückziehen/Ersetzen von kryptographischen Schlüsseln, wenn Kunden oder Integratoren/Wiederverkäufer in diesen Schlüsselverwaltungsaktivitäten involviert sind ▪ Ein Beispiel-Schlüsselwächterformular für Schlüsselwächter, das besagt, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen	**Softwareanbieter**: Bereitstellung von Anweisungen für Kunden, die auf kryptographische Schlüssel zugreifen, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, zur Implementierung von Schlüsselverwaltungsprozessen und -verfahren **Kunden und Integratoren/Wiederverkäufer**: Implementieren von Schlüsselverwaltungsprozessen und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 2.5

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
2.5.1 – 2.5.7	Implementieren sicherer Schlüsselverwaltungsfunktionen	Stellen Sie Anweisungen für Kunden und Integratoren/Wiederverkäufer zum Ausführen von Schlüsselverwaltungsfunktionen bereit: ▪ Erstellung starker kryptographischer Schlüssel ▪ Sichere Verteilung kryptographischer Schlüssel ▪ Sicheres Speichern kryptographischer Schlüssel ▪ Änderungen kryptographischer Schlüssel für Schlüssel, die das Ende ihrer Schlüssellebensdauer erreicht haben ▪ Entfernung oder Austausch von Schlüsseln je nach Notwendigkeit, wenn die Integrität des Schlüssels gefährdet ist oder Grund zur Annahme besteht, dass bestimmte Schlüssel beschädigt sind ▪ Geteilte Kenntnis und duale Kontrolle für alle manuellen Verwaltungsvorgänge kryptographischer Klartext-Schlüssel, die von der Zahlungsanwendung unterstützt werden ▪ Verhindern der unbefugten Ersetzung kryptographischer Schlüssel	**Softwareanbieter**: Bereitstellung von Anweisungen für Kunden zum Implementieren sicherer Schlüsselverwaltungsfunktionen **Kunden und Integratoren/Wiederverkäufer**: Implementieren sicherer Schlüsselverwaltungsfunktionen für kryptographische Schlüssel entsprechend dem *PA-DSS-Implementierungshandbuch* und den PA-DSS-Anforderungen 2.5.1 – 2.5.7

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
2.6	Bereitstellung eines Mechanismus, mit dem kryptographische Materialien oder Kryptogramme, die von der Zahlungsanwendung gespeichert wurden, unwiderruflich gelöscht werden können	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Verfahren, die Details zur Verwendung der Anwendung enthalten, oder mit der Anwendung bereitgestellte Verfahrensweisen zum unwiderruflichen Löschen kryptographischen Materials ▪ Die Angabe, dass kryptographische Schlüsselmaterialien unwiderruflich gelöscht werden sollten, wenn Schlüssel nicht mehr verwendet werden – und gemäß den Schlüsselverwaltungsanforderungen in PCI-DSS ▪ Anweisungen zum erneuten Verschlüsseln von Verlaufsdaten mit neuen Schlüsseln, einschließlich Verfahren zum Aufrechterhalten der Sicherheit von Daten im Klartext während des Entschlüsselungs-/Neuverschlüsselungsvorgangs	**Softwareanbieter**: Bereitstellung eines Tools oder einer Verfahrensweise zum sicheren Entfernen kryptographischer Schlüsselmaterialien oder von Kryptogrammen, die von der Anwendung gespeichert wurden, sowie die Bereitstellung eines Tools oder einer Verfahrensweise zur Neuverschlüsselung von Verlaufsdaten mit neuen Schlüsseln **Kunden und Integratoren/Wiederverkäufer**: Löschen sämtlichen historischen kryptographischen Materials entsprechend den Schlüsselverwaltungsanforderungen im *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 2.6

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
3.1	Nutzen eindeutiger Benutzer-IDs und sicherer Authentifizierung für den Verwaltungszugriff und den Zugriff auf Karteninhaberdaten.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Anleitungen dazu, wie die Zahlungsanwendung eine starke Authentifizierung für alle Authentifizierungsinformationen (z. B. Benutzer, Kennwörter) durchsetzt, die die Anwendung generiert oder verwaltet, indem: - Sichere Änderungen der Authentifizierungsinformationen bei Abschluss der Installation entsprechend den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 durchgesetzt werden - Sichere Änderungen an den Authentifizierungsinformationen für sämtliche nachträgliche Änderungen (nach der Installation) entsprechend den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 durchgesetzt werden ▪ Angabe, dass zur Aufrechterhaltung der PCI-DSS-Konformität für alle Änderungen, die an Authentifizierungskonfigurationen vorgenommen werden, überprüft werden muss, dass sie Authentifizierungsmethoden bereitstellen, die mindestens so streng wie die PCI-DSS-Anforderungen sind ▪ Zuweisung einer sicheren Authentifizierung für alle Standardkonten in der Umgebung ▪ Jeglichen Standardkonten, die nicht verwendet werden, wird eine sichere Authentifizierung zugewiesen, und die Konten werden dann deaktiviert oder nicht verwendet. ▪ Änderung und Erstellung von Authentifizierungsinformationen, wenn diese nicht von der Zahlungsanwendung generiert oder verwaltet werden, gemäß den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 bei Abschluss der Installation sowie für nachträgliche Änderungen nach der Installation für alle Konten auf Anwendungsebene mit administrativem Zugriff sowie für jegliche Zugriffe auf Karteninhaberdaten ▪ Es werden alle Rollen und Standardkonten mit Verwaltungszugriff innerhalb der Anwendung ermittelt.	**Softwareanbieter**: Sicherstellung, dass die Zahlungsanwendung für alle Authentifizierungsinformationen, die von der Anwendung generiert oder verwaltet werden, die Nutzung eindeutiger Benutzer-IDs und sicherer Authentifizierungsmethoden für Konten/Kennwörter entsprechend den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 durchsetzt. Sicherstellung, dass das *PA-DSS-Implementierungshandbuch* für Authentifizierungsinformationen, die von der Zahlungsanwendung nicht generiert oder verwaltet werden, eine klare und unmissverständliche Anleitung für Kunden und Integratoren/Wiederverkäufer dazu bietet, wie sichere Authentifizierungsinformationen gemäß den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 geändert und erstellt werden. **Kunden und Integratoren/Wiederverkäufer**: Einrichten und Pflegen eindeutiger Benutzer-IDs und sicherer Authentifizierungsmethoden entsprechend dem *PA-DSS-Implementierungshandbuch* und den PA-DSS-Anforderungen 3.1.1 bis 3.1.11

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
3.2	Nutzen eindeutiger Benutzer-IDs und sicherer Authentifizierung für den Zugriff auf PCs, Server und Datenbanken mit Zahlungsanwendungen.	Anweisung der Kunden und Integratoren/Wiederverkäufer, dass eindeutige Benutzernamen und sichere Authentifizierungsmethoden für den Zugriff auf sämtliche PCs, Server und Datenbanken mit Zahlungsanwendungen und/oder Karteninhaberdaten entsprechend den PA-DSS-Anforderungen 3.1.1 bis 3.1.11 zu verwenden sind	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung die Nutzung eindeutiger Benutzer-IDs und sicherer Authentifizierungsmethoden für Konten/Kennwörter zum Zugriff auf PCs, Server und Datenbanken entsprechend den PA-DSS-Anforderungen 3.1.2 bis 3.1.9 unterstützt. **Kunden und Integratoren/Wiederverkäufer**: Einrichten und Pflegen eindeutiger Benutzer-IDs und sicherer Authentifizierungsmethoden entsprechend dem *PA-DSS-Implementierungshandbuch* und den PA-DSS-Anforderungen 3.1.1 bis 3.1.11.
4.1	Implementieren automatisierter Prüfverfahren.	Es müssen Anweisungen für das Implementieren automatisierter Audit-Trails bereitgestellt werden, die Folgendes umfassen: ▪ Wie die Anwendung zu installieren ist, damit die Protokolle nach Abschluss des Installationsvorgangs automatisch konfiguriert und aktiviert werden ▪ Wie PCI-DSS-konforme Protokolleinstellungen gemäß den PA-DSS-Anforderungen 4.2, 4.3 und 4.4 für sämtliche Protokollierungsoptionen einzurichten sind, die vom Kunden nach der Installation konfiguriert werden können ▪ Protokolle müssen aktiviert sein. Die Deaktivierung von Protokollen führt zur Nichteinhaltung des PCI-DSS. ▪ Wie PCI-konforme Protokolleinstellungen von Drittanbieter-Softwarekomponenten, die zusammen mit der Zahlungsanwendung bereitgestellt werden oder die für die Zahlungsanwendung erforderlich sind, für sämtliche Protokollierungsoptionen einzurichten sind, die vom Kunden nach der Installation konfiguriert werden können	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung Kunden bei der Nutzung konformer Protokolle gemäß den PA-DSS-Anforderungen 4.2, 4.3 und 4.4. unterstützt **Kunden und Integratoren/Wiederverkäufer:** Einrichten und Pflegen von PCI-DSS-konformen Protokollen entsprechend dem *PA-DSS-Implementierungshandbuch* und den PA-DSS-Anforderungen 4.2, 4.3 und 4.4

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
4.4	Ermöglichen einer zentralisierten Protokollierung.	Beschreibung, welche zentralisierten Protokollierungsmechanismen unterstützt werden, und Anweisungen sowie Verfahren zur Integration der Protokolle der Zahlungsanwendung in einem zentralen Protokollierungsserver	**Softwareanbieter**: Sicherstellung, dass die Zahlungsanwendung zentralisierte Protokolle in Kundenumgebungen gemäß der PA-DSS-Anforderung 4.4. unterstützt **Kunden und Integratoren/Wiederverkäufer:** Einrichten und Pflegen zentralisierter Protokolle entsprechend dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 4.4
5.4.4	Implementieren und Bekanntmachen der Anwendungs-Versionierungsmethode	Beschreibung der veröffentlichten Versionierungsmethode des Anbieters, einschließlich Anleitungen für folgende Punkte: ▪ Details des Versionsschemas, einschließlich des Versionsschemaformats (Anzahl der Elemente, Trennzeichen, Zeichensatz usw.) ▪ Details dazu, wie Änderungen mit Auswirkungen auf die Sicherheit vom Versionsschema angegeben werden ▪ Details dazu, wie sich andere Änderungstypen auf die Version auswirken ▪ Details zu verwendeten Platzhalterelementen, einschließlich der Anweisung, dass diese nie zur Darstellung von Änderungen mit Auswirkungen auf die Sicherheit verwendet werden	**Softwareanbieter**: Dokumentierung und Implementierung einer Software-Versionierungsmethode im Rahmen des Systementwicklungszyklus. Die Methode muss die Verfahrensweisen im *PA-DSS-Programmleitfaden* für Änderungen an Zahlungsanwendungen gemäß der PA-DSS-Anforderung 5.5 einhalten. **Kunden und Integratoren/Wiederverkäufer:** Kenntnis, welche Version der Zahlungsanwendung von ihnen verwendet wird, und Sicherstellung, dass nur validiertes Versionen verwendet werden

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
6.1	Sicheres Implementieren drahtloser Technologien.	Für Zahlungsanwendungen, die zur Nutzung von Drahtlostechnologie entwickelt wurden, müssen die folgenden Anweisungen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Anweisung, dass die Zahlungsanwendung bei der Installation Änderungen der standardmäßigen Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen für alle von der Anwendung gesteuerten drahtlosen Komponenten durchsetzt ▪ Verfahrensweisen für die Änderung von drahtlosen Verschlüsselungsschlüsseln und Kennwörtern, einschließlich SNMP-Zeichenfolgen, die jedes Mal angewendet werden, wenn jemand mit Kenntnis der Schlüssel/Kennwörter das Unternehmen verlässt oder eine andere Position antritt ▪ Anweisungen zum Ändern der standardmäßigen Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen für alle drahtlosen Komponenten, die mit der Zahlungsanwendung bereitgestellt, von ihr aber nicht gesteuert werden ▪ Anweisungen zum Installieren einer Firewall zwischen allen drahtlosen Netzwerken und Systemen, die Karteninhaberdaten speichern ▪ Details zum gesamten drahtlosen Datenverkehr (einschließlich spezifischer Portinformationen), die die Drahtlosfunktion der Zahlungsanwendung verwenden würde ▪ Anweisungen zum Konfigurieren der Firewalls, sodass der gesamte Verkehr zwischen der drahtlosen Umgebung und der Karteninhaberdaten-Umgebung abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten (und für die Geschäftszwecke notwendigen) Datenverkehr handelt	**Softwareanbieter**: Anweisen von Kunden und Integratoren/Wiederverkäufern, dass bei einer Verwendung von Drahtlostechnologie innerhalb der Zahlungsanwendung die Standardeinstellungen des Anbieters für Drahtlostechnologie entsprechend der PA-DSS-Anforderung 6.1 geändert werden müssen **Kunden und Integratoren/Wiederverkäufer**: Ändern der Anbieterstandardeinstellungen gemäß PA-DSS-Anforderung 6.1 und Installation einer Firewall gemäß dem *PA-DSS-Implementierungshandbuch* und der PCI-DSS-Anforderung 2.1.1 bei der Implementierung von Drahtlostechnologie in der Zahlungsanwendung durch Kunden oder Integratoren/Wiederverkäufern

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
6.2	Sichere Übertragung von Karteninhaberdaten über Drahtlosnetzwerke.	Anweisungen zum Implementieren von starker Verschlüsselung für die Authentifizierung und Übertragung von Karteninhaberdaten gemäß Best Practices der Branche (z. B. IEEE 802.11i) bei Zahlungsanwendungen, die zur Nutzung von Drahtlostechnologie entwickelt wurden Dazu gehören Folgende: ▪ Anweisungen zum Konfigurieren der Anwendung, um für die Authentifizierung und Übertragung Best Practices der Branche (zum Beispiel IEEE 802.11.i) für starke Verschlüsselung einzusetzen, und/oder ▪ Anweisungen zum Konfigurieren aller Drahtlosanwendungen im Lieferumfang der Zahlungsanwendung, um für die Authentifizierung und Übertragung Best Practices der Branche für starke Verschlüsselung einzusetzen	**Softwareanbieter**: Anweisen von Kunden und Integratoren/Wiederverkäufern, dass bei einer Verwendung von Drahtlostechnologie innerhalb der Zahlungsanwendung sichere verschlüsselte Übertragungen entsprechend der PA-DSS-Anforderung 6.2 implementiert werden müssen **Kunden und Integratoren/Wiederverkäufer**: Nutzung sicherer verschlüsselter Übertragungen gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 6.2 bei der Implementierung von Drahtlostechnologie in der Zahlungsanwendung durch Kunden oder Integratoren/Wiederverkäufer

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
6.3	Bereitstellung von Anweisungen zur sicheren Nutzung von Drahtlostechnologie	Die folgenden Anweisungen für PCI-DSS-konforme Drahtloseinstellungen müssen bereitgestellt werden: ▪ Anweisungen zum Ändern aller drahtlosen standardmäßigen Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen bei der Installation ▪ Anweisungen zum Ändern der drahtlosen Verschlüsselungsschlüssel, Kennwörter und SNMP-Zeichenfolgen, die jedes Mal anzuwenden sind, wenn jemand mit Kenntnis der Schlüssel/Kennwörter das Unternehmen verlässt oder eine andere Position antritt ▪ Anweisungen zum Installieren einer Firewall zwischen allen drahtlosen Netzwerken und Systemen, die Karteninhaberdaten speichern, und zum Konfigurieren von Firewalls, sodass der gesamte Verkehr aus der drahtlosen Umgebung in die Karteninhaberdaten-Umgebung abgelehnt oder (sofern dieser Verkehr für Geschäftszwecke notwendig ist) kontrolliert wird ▪ Anweisungen zum Einsatz von Best Practices der Branche (zum Beispiel IEEE 802.11i), um eine starke Verschlüsselung bei der Authentifizierung und Übertragung zu erreichen	**Softwareanbieter**: Anweisen der Kunden und Integratoren/Wiederverkäufer, drahtlose Technologien gemäß der PA-DSS-Anforderung 6.3 zu sichern **Kunden und Integratoren/Wiederverkäufer**: Sichern der drahtlosen Technologien gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 6.2

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
7.2.3	Stellen Sie Anweisungen für Kunden zur sicheren Installation von Patches und Updates zur Verfügung.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: • Wie der Anwender Benachrichtungen zu neuen Patches und Updates kommunizieren will. • Wie Patches und Updates auf sichere und vertrauenswürdige Art und Weise zur Verfügung gestellt werden. • Wie auf Patches und Updates auf eine Art und Weise zugegriffen werden kann, die die Integrität des Patch- und Updatecodes bewahrt.	**Softwareanbieter:** Prozesse für Kommunikation, Lieferung und sichere Installation von Patches und Updates dokumentieren und implementieren **Kunden und Integratoren/Wiederverkäufer:** Auf Patches und Updates auf sichere Art und Weise in Übereinstimmung mit dem *PA-DSS Implementierungshandbuch zugreifen und diese installieren*
8.2	Verwenden Sie ausschließlich erforderliche und sichere Dienste, Protokolle, Daemons, Komponenten und zugehörige Software und Hardware, einschließlich solcher, die von Drittanbietern stammt.	Dokumentieren Sie alle Protokolle, Dienste, Komponenten und zugehörige Software und Hardware, die für eine Funktion der Zahlungsanwendung erforderlich sind.	**Softwareanbieter:** Sicherstellen, dass die Zahlungsanwendung ausschließlich die Verwendung durch den Kunden von erforderlichen und sicheren Protokollen, Diensten usw. unterstützt, indem 1) sie standardmäßig nur über erforderliche Protokolle, Dienste usw. verfügt, 2) diese erforderlichen Protokolle, Dienste usw. standardmäßig sicher konfiguriert sind und 3) erforderliche Protokolle, Dienste usw. als Hinweis für Kunden und Integratoren/Wiederverkäufer dokumentiert werden **Kunden und Integratoren/Wiederverkäufer:** Verwenden der dokumentierten Liste im *PA-DSS-Implementierungshandbuch*, um sicherzustellen, dass ausschließlich erforderliche und sichere Protokolle, Dienste usw. auf dem System gemäß der PA-DSS-Anforderung 5.4 eingesetzt werden

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
9.1	Speichern von Karteninhaberdaten ausschließlich auf nicht mit dem Internet verbundenen Servern.	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Anweisungen, dass Karteninhaberdaten nicht auf über das Internet zugänglichen Systemen gespeichert werden dürfen (beispielsweise dürfen Webserver und Datenbankserver sich nicht auf demselben Server befinden) ▪ Anweisungen zum Konfigurieren der Zahlungsanwendung, sodass Systeme zum Speichern von Karteninhaberdaten mithilfe einer DMZ vom Internet abgetrennt werden ▪ Eine Liste der Dienste/Ports, die die Anwendung zur Kommunikation zwischen zwei Netzwerkzonen benötigt (damit der Kunde seine Firewall so konfigurieren kann, dass nur die erforderlichen Ports geöffnet sind)	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung keine Speicherung von Karteninhaberdaten in der DMZ oder auf über das Internet zugänglichen Systemen erfordert und eine DMZ entsprechend der PA-DSS-Anforderung 9 gestattet **Kunden und Integratoren/Wiederverkäufer**: Einrichten und Pflegen von Zahlungsanwendungen auf eine Weise, dass Karteninhaberdaten nicht auf über das Internet zugänglichen Systemen gespeichert werden, entsprechend dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 9.
10.1	Implementieren von Multi-Faktor-Authentifizierung für sämtlichen Remotezugriff auf die Zahlungsanwendung, der von außerhalb der Kundenumgebung erfolgt	Die folgenden Anweisungen müssen für Kunden und Integratoren/Wiederverkäufer bereitgestellt werden: ▪ Anweisung, dass zur Einhaltung der PCI-DSS-Anforderungen Multi-Faktor-Authentifizierung für sämtlichen Remotezugriff auf die Zahlungsanwendung, der von außerhalb des Kundennetzwerks erfolgt, genutzt werden muss ▪ Beschreibung der von der Anwendung unterstützten Mechanismen für die Multi-Faktor-Authentifizierung ▪ Anweisungen zum Konfigurieren der Anwendung, damit diese Multi-Faktor-Authentifizierung unterstützt (mindestens zwei der drei in der PA-DSS-Anforderung 3.1.4 beschriebenen Authentifizierungsmethoden)	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung die Nutzung von Multi-Faktor-Authentifizierung durch den Kunden für sämtlichen Remotezugriff auf die Zahlungsanwendung, der von außerhalb der Kundenumgebung erfolgt, gemäß der PA-DSS-Anforderung 10.2 unterstützt **Kunden und Integratoren/Wiederverkäufer**: Einrichten und Pflegen einer Multi-Faktor-Authentifizierung für sämtlichen Remotezugriff auf die Zahlungsanwendung, der von außerhalb der Kundenumgebung erfolgt, gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 10.2

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
10.2.1	Sichere Bereitstellung von Updates für Remote-Zahlungsanwendungen.	Wenn Updates für die Zahlungsanwendung per Remotezugriff auf Kundensysteme bereitgestellt werden, müssen folgende Anweisungen enthalten sein: ▪ Anweisungen zum Aktivieren von Technologien für den Remotezugriff auf Zahlungsanwendungen unter der Voraussetzung, dass diese für Downloads erforderlich sind, und zum umgehenden Deaktivieren gemäß der PCI-DSS-Anforderung 12.3.9, nachdem der Download abgeschlossen ist ▪ Anweisungen, dass im Fall, dass der Computer über VPN oder eine andere Hochgeschwindigkeitsverbindung angeschlossen ist, Updates für Remote-Zahlungsanwendungen gemäß der PCI-DSS-Anforderung 1 nur über eine sicher konfigurierte Firewall oder eine persönliche Firewall empfangen werden sollten	**Softwareanbieter**: Sichere Bereitstellung von Updates für Remote-Zahlungsanwendungen gemäß PA-DSS 10.3 **Kunden und Integratoren/Wiederverkäufer**: Empfangen von Updates für Remote-Zahlungsanwendungen von Anbietern gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 10.3 und PCI-DSS-Anforderung 1 nur auf sicherem Wege

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
10.2.3	Sichere Implementierung der Remotezugriffssoftware	Es müssen Anweisungen enthalten sein, dass sämtlicher Remotezugriff auf die Zahlungsanwendung sicher implementiert sein muss, zum Beispiel: ▪ Ändern der Standardeinstellungen der Remotezugriffssoftware (beispielsweise die Änderung von Standardkennwörtern und Nutzung eindeutiger Kennwörter für jeden Kunden); ▪ Zulassen von Verbindungen ausschließlich über bestimmte (bekannte) IP-/MAC-Adressen; ▪ Verwendung einer starken Authentifizierung und komplexer Zugriffskennwörter (siehe PA-DSS-Anforderungen 3.1.1 bis 3.1.11); ▪ Ermöglichen einer verschlüsselten Datenübertragung entsprechend der PA-DSS-Anforderung 12.1; ▪ Aktivieren einer Kontosperrung nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche (siehe PA-DSS-Anforderungen 3.1.9 bis 3.1.10); ▪ Einrichten einer VPN (Virtual Private Network)-Verbindung mit einer Firewall, bevor der Zugriff zugelassen wird; ▪ Aktivieren der Protokollfunktion. ▪ Einschränken des Zugriffs auf Kundenumgebungen auf autorisierte Mitarbeiter von Integratoren/Wiederverkäufer.	**Softwareanbieter**: (1) Wenn der Anbieter remote auf die Zahlungsanwendungen des Kunden zugreifen kann, muss der Remotezugriff gemäß den Anweisungen in der PA-DSS-Anforderung 10.3.2 sicher implementiert sein. (2) Sicherstellen, dass die Zahlungsanwendung Kunden bei der Verwendung der Sicherheitsfunktionen für den Remotezugriff unterstützt **Kunden und Integratoren/Wiederverkäufer**: Verwenden von Sicherheitsfunktionen für sämtlichen Remotezugriff auf Zahlungsanwendungen gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 10.3.2

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
11.1	Sichere Übertragung von Karteninhaberdaten über öffentliche Netzwerke.	Wenn die Zahlungsanwendung Karteninhaberdaten über öffentliche Netzwerke sendet oder eine Übermittlung dieser Daten zulässt, müssen Anweisungen zum Implementieren und Verwenden von starker Kryptographie und Sicherheitsprotokollen für die sichere Übertragung von Karteninhaberdaten über öffentliche Netzwerke bereitstellt werden, einschließlich: ▪ Anweisungen, dass starke Kryptographie und Sicherheitsprotokolle verwendet werden müssen, wenn die Karteninhaberdaten über öffentliche Netzwerke übertragen werden ▪ Anweisungen zur Überprüfung, ob nur vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert werden ▪ Anweisungen zum Konfigurieren der Zahlungsanwendung, damit ausschließlich sichere Versionen und sichere Implementierungen von Sicherheitsprotokollen verwendet werden ▪ Anweisungen zum Konfigurieren der Zahlungsanwendung, um einen Fallback zurück zu einer unsicheren Version oder Konfiguration zu vermeiden (z. B., wenn TSS verwendet wird, darf die Anwendung keinen Fallback auf SSL zulassen). ▪ Anweisungen zum Konfigurieren der Zahlungsanwendung, damit die richtige Verschlüsselungsstärke für die verwendete Verschlüsselungsmethode eingesetzt wird	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung Kunden bei der Nutzung einer starken Kryptographie und von Sicherheitsprotokollen bei der Übertragung von Karteninhaberdaten über öffentliche Netzwerke gemäß PA-DSS-Anforderung 11.1 unterstützt **Kunden und Integratoren/Wiederverkäufer**: Einrichten und Pflegen einer starken Kryptographie und von Sicherheitsprotokollen bei der Übertragung von Karteninhaberdaten gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 11.1

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
11.2	Verschlüsseln von über Messaging-Technologien für Endbenutzer gesendeten Karteninhaberdaten.	Wenn die Zahlungsanwendung die Übermittlung von PANs über Messaging-Technologien für Endbenutzer zulässt, müssen Anweisungen zum Implementieren und Verwenden einer Lösung, mit der die PAN unleserlich gemacht werden kann oder die starke Kryptographie implementiert, enthalten sein, einschließlich: ▪ Anweisungen zur Verwendung der definierten Lösung, um die PAN unleserlich zu machen oder die PAN mit starker Kryptographie zu sichern ▪ Anweisung, dass die PAN immer unleserlich gemacht oder mittels einer starken Kryptographie gesichert werden muss, wenn sie über Messaging-Technologien für Endbenutzer übermittelt wird	**Softwareanbieter**: Bereitstellung einer Lösung bzw. die Angabe, dass eine Lösung verwendet werden soll, die die PAN unleserlich macht oder eine starke Kryptographie implementiert, und Sicherstellung, dass die Zahlungsanwendung Funktionen unterstützt, mit denen die PANs verschlüsselt oder unleserlich gemacht werden, wenn sie über Messaging-Technologien für Endbenutzer übermittelt werden – gemäß der PA-DSS-Anforderung 11.2 **Kunden und Integratoren/Wiederverkäufer**: Unleserlich machen oder Verschlüsseln mit starker Kryptographie aller über Messaging-Technologien für Endbenutzer gesendeten PANs gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 11.2
12.1	Verschlüsseln des Nichtkonsolen-Verwaltungszugriffs.	Wenn die Zahlungsanwendung Nichtkonsolen-Verwaltungszugriff zulässt, müssen Anweisungen bereitgestellt werden, wie die Anwendung für die Nutzung starker Kryptographie für die Verschlüsselung des gesamten Nichtkonsolen-Verwaltungszugriffs auf die Zahlungsanwendung oder Server in der Karteninhaberdaten-Umgebung konfiguriert wird.	**Softwareanbieter**: Wenn die Zahlungsanwendung Nichtkonsolen-Verwaltungszugriff zulässt, muss sichergestellt werden, dass die Zahlungsanwendung starke Verschlüsselung für Nichtkonsolen-Verwaltungszugriff gemäß der PA-DSS-Anforderung 12.1 implementiert **Kunden und Integratoren/Wiederverkäufer**: Verschlüsseln des Nichtkonsolen-Verwaltungszugriffs gemäß *PA-DSS-Implementierungshandbuch* und PCI-DSS-Anforderung 12.1
12.1.1	Verschlüsseln des Nichtkonsolen-Verwaltungszugriffs.	Anweisungen für Kunden und Integratoren/Wiederverkäufer, eine starke Kryptographie für die Verschlüsselung des gesamten Nichtkonsolen-Verwaltungszugriffs zu implementieren	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung den Kunden bei der Verschlüsselung des Nichtkonsolen-Verwaltungszugriffs gemäß der PA-DSS-Anforderung 12.1.1 unterstützt **Kunden und Integratoren/Wiederverkäufer**: Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 12.1.1

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

PA-DSS-Anforderung	PA-DSS-Thema	Erforderlicher Inhalt des Implementierungshandbuchs	Verantwortlichkeit für die Implementierung der Kontrolle
12.2	Verwenden Sie eine Multi-Faktor-Authentifizierung für alle Mitarbeiter mit Nichtkonsolen-Verwaltungszugriff.	Anweisungen zur Nutzung der Multi-Faktor-Authentifizierung für Kunden und Integratoren/Wiederverkäufer hinzufügen, einschließlich: • Anweisungen, dass die Multi-Faktor-Authentifizierung für alle Mitarbeiter mit Nichtkonsolen-Verwaltungszugriff auf das CDE eingesetzt wird. • Verfahren für die Nutzung der Multi-Faktor-Authentifizierung, die mit der Anwendung bereitgestellt werden (falls bereitgestellt).	**Softwareanbieter**: Sicherstellen, dass die Zahlungsanwendung die Nutzung der Multi-Faktor-authentifizierung für alle Mitarbeiter mit Nichtkonsolen-Verwaltungszugriff gemäß der PA-DSS-Anforderung 12.2 vorsieht und festlegt **Kunden und Integratoren/Wiederverkäufer**: Einsatz einer Multi-Faktor-Authentifizierung für alle Mitarbeiter mit Nichtkonsolen-Verwaltungszugriff, gemäß dem *PA-DSS-Implementierungshandbuch* und der PA-DSS-Anforderung 12.2

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Anhang B: Testlabor-Konfiguration für PA-DSS-Bewertungen

Der PA-QSA muss für jede durchgeführte PA-DSS-Bewertung den Status und die Fähigkeiten des für die Durchführung dieser PA-DSS-Bewertung genutzten Testlabors bestätigen. Diese Bestätigung muss zusammen mit dem ausgefüllten *ROV (Report on Validation, Validierungsbericht)* eingereicht werden.

Der PA-QSA muss für jedes Laborvalidierungsverfahren angeben, ob es sich bei dem Labor, das für die Durchführung der Bewertung genutzt wurde und das diese Validierungsverfahren durchlaufen hat, um das Labor des PA-QSA oder das Labor des Softwareanbieters handelte. PA-QSAs müssen sicherstellen, dass das Testlabor alle der unten festgehaltenen Anforderungen erfüllt, und das eigene Labor für die Durchführung der Bewertungen nutzen, wenn dies möglich ist. Das Labor des Softwareanbieters darf nur eingesetzt werden, wenn dies erforderlich ist (z. B. wenn der PA-QSA nicht über den Mainframe, AS400 oder Tandem verfügt, auf dem die Zahlungsanwendung ausgeführt wird) und nachdem sichergestellt wurde, dass das Labor alle Anforderungen erfüllt.

Der PA-QSA muss außerdem alle Elemente in der nachstehenden Tabelle bestätigen:

- **Identifizierung des Standorts und Besitzers des Labors oder der Labore, das bzw. die für die PA-DSS-Bewertung eingesetzt wurde(n)**
- **Beschreibung der Labortestarchitektur und -umgebung für diese PA-DSS-Überprüfung**
- **Beschreibung, wie die reale Nutzung der Zahlungsanwendung in dem Labor für diese PA-DSS-Überprüfung simuliert wurde**

Die *PA-DSS-ROV-Berichtsvorlage* enthält Details zur Validierung des Labors, die bei jeder Bewertung durchgeführt werden muss.

Laboranforderung	Laborvalidierungsverfahren
1. Installieren der Zahlungsanwendung gemäß den Installationsanweisungen oder der Schulung des Anbieters, die der Kunde erhalten hat.	**1.** Überprüfen Sie, ob das Installationshandbuch oder die Schulung des Anbieters, das/die der Kunde erhalten hat, genutzt wurde, um die standardmäßige Installation der Zahlungsanwendung auf allen in dem PA-DSS-Bericht aufgeführten Plattformen zur Simulation der realen Kundenerfahrung durchzuführen.
2. Installieren und Testen aller im PA-DSS-Bericht aufgeführten Zahlungsanwendungsversionen.	**2.a** Überprüfen Sie, ob alle häufig genutzten Implementierungen (einschließlich regions-/landesspezifischer Versionen) der Zahlungsanwendung an dem Installationsort getestet wurden.
	2.b Überprüfen Sie, ob alle Versionen und Plattformen der Zahlungsanwendung, einschließlich aller erforderlichen Systemkomponenten und Abhängigkeiten, getestet wurden.
	2.c Überprüfen Sie, ob alle wichtigen Zahlungsanwendungsfunktionen für jede Version getestet wurden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Laboranforderung	Laborvalidierungsverfahren
3. Installieren und Implementieren aller gemäß PCI-DSS erforderlichen Sicherheitseinrichtungen.	**3.** Überprüfen Sie, ob alle gemäß PCI-DSS erforderlichen Sicherheitseinrichtungen (z. B. Firewalls und Antivirensoftware) in den Testsystemen implementiert wurden.
4. Installieren und/oder Konfigurieren aller gemäß PCI-DSS erforderlichen Sicherheitseinstellungen.	**4.** Überprüfen Sie, ob alle Systemeinstellungen, Patches usw. auf PCI-DSS-konforme Art und Weise in den Testsystemen für Betriebssysteme, Systemsoftware und Anwendungen, die von der Zahlungsanwendung genutzt werden, implementiert wurden.
5. Simulieren der realen Nutzung der Zahlungsanwendung.	**5.a** Das Labor simuliert die reale Nutzung der Zahlungsanwendung, einschließlich aller Systeme und Anwendungen, in denen die Zahlungsanwendung implementiert ist. So könnte beispielsweise eine Standardimplementierung einer Zahlungsanwendung Folgendes umfassen: eine Client-/Server-Umgebung in einer Ladenfront eines Einzelhändlers mit einem POS-Computer und ein Back-Office oder ein Unternehmensnetzwerk. In dem Labor wird die gesamte Implementierung simuliert.
	5.b Das Labor verwendet ausschließlich Testkartennummern für die Simulation/den Test – es werden keine echten PANs für die Tests verwendet. ***Hinweis:*** *Testkarten sind in der Regel über den Anbieter, einen EDV-Dienstleister oder einen Erwerber erhältlich.*
	5.c Das Labor führt die Autorisierungs- und/oder Verrechnungsfunktionen der Zahlungsanwendung durch. Außerdem werden alle ausgegebenen Informationen gemäß Punkt 6 überprüft.
	5.d Das Labor und/oder die Prozesse bilden alle von der Zahlungsanwendung ausgegebenen Informationen ab, und zwar für jedes mögliche Szenario, z. B. temporär, permanent, Fehlerbearbeitung, Fehlersuche und -behebung oder Protokolldateien.
	5.e Das Labor und/oder die Prozesse simulieren und validieren alle Funktionen der Zahlungsanwendung, um die Erzeugung von Fehlerbedingungen und Protokolleinträgen unter Verwendung von simulierten „echten“ Daten und ungültigen Daten mit einzubeziehen.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Laboranforderung	Laborvalidierungsverfahren
6. Bereitstellen von Funktionen und Tests unter Verwendung der folgenden Penetrationstestmethoden:	**6.a** Anwendung forensischer Werkzeuge/Methoden: Forensische Werkzeuge/Methoden werden dazu genutzt, um alle ermittelten ausgegebenen Informationen gemäß PA-DSS-Anforderung 1.1.1 bis 1.1.3 nach vertraulichen Authentifizierungsdaten zu durchsuchen (kommerziell vertriebene Tools, Skripte usw.).[6]
	6.b Versuch, Sicherheitsrisiken der Anwendung auszunutzen: Anhand aktueller Sicherheitsrisiken (z. B. die OWASP Top 10, SANS CWE Top 25, CERT Secure Coding usw.) wurde versucht, die Zahlungsanwendung(en) auszunutzen – gemäß PA-DSS-Anforderung 5.2.
	6.c Das Labor und/oder die Prozesse versuchten, den Update-Prozess für die Zahlungsanwendung mit einem beliebigen Code durchzuführen: Führen Sie den Update-Prozess mit einem beliebigen Code gemäß PA-DSS-Anforderung 7.2.2 durch.
7. Verwendung des Labors des Anbieters NUR, nachdem überprüft wurde, dass alle Anforderungen erfüllt sind.	Ist der Einsatz des Labors des Softwareanbieters erforderlich (z. B. wenn der PA-QSA nicht über den Mainframe, AS400 oder Tandem verfügt, auf dem die Zahlungsanwendung ausgeführt wird), kann der PA-QSA entweder (1) die vom Anbieter geliehene Ausrüstung verwenden oder (2) das Labor des Anbieters nutzen, vorausgesetzt, dies wird in dem Bericht zusammen mit dem Ort der Tests so angegeben. In beiden Fällen hat der PA-QSA zu überprüfen, ob die Ausrüstung und das Labor des Anbieters die folgenden Anforderungen erfüllen:
	7.a Der PA-QSA überprüft, ob das Labor des Anbieters alle oben genannten Anforderungen erfüllt, und dokumentiert die Informationen in dem Bericht.
	7.b Der PA-QSA muss die korrekte Installation der externen Laboreinrichtung bestätigen, um sicherzustellen, dass die Umgebung tatsächlich eine reale Situation simuliert und dass der Anbieter die Umgebung nicht auf irgendeine Weise modifiziert oder verfälscht hat.
	7.c Alle Tests werden von dem PA-QSA durchgeführt (der Anbieter darf bei seinen eigenen Anwendungen keine Tests durchführen).

[6] Forensisches Werkzeug oder Methode: Ein Werkzeug oder eine Methode zur Erkennung, Analyse und Präsentation forensischer Daten, mit dem bzw. der Hinweise auf Computern schnell und gründlich authentifiziert, durchsucht und wiederhergestellt werden können. Im Fall, dass forensische Werkzeuge oder Methoden von PA-QSAs verwendet werden, sollten diese Werkzeuge oder Methoden jegliche sensiblen Authentifizierungsdaten, die von der Zahlungsanwendung geschrieben wurden, präzise lokalisieren können. Bei den Tools kann es sich um kommerziell vertriebene, Open-Source- oder intern durch den PA-QSA entwickelte Tools handeln.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.

Laboranforderung	Laborvalidierungsverfahren
	7.d Alle Tests werden entweder (1) direkt vor Ort in den Einrichtungen des Anbieters oder (2) per Remotezugriff über eine Netzwerkverbindung unter Verwendung eines sicheren Links (zum Beispiel VPN) durchgeführt.
	7.e Verwenden Sie ausschließlich Testkartennummern für die Simulation/Tests. Verwenden Sie keine echten PANs für die Tests. Diese Testkarten sind in der Regel über den Anbieter, einen EDV-Dienstleister oder einen Erwerber erhältlich.
8. Pflegen eigener Qualitätssicherungsmaßnahmen	**8.a** Das für die Qualitätssicherung zuständige Personal des PA-QSA überprüft, ob alle im PA-DSS-Bericht ermittelten Plattformen im Test berücksichtigt wurden.
	8.b Das für die Qualitätssicherung zuständige Personal des PA-QSA überprüft, ob alle PA-DSS-Anforderungen beim Test berücksichtigt wurden.
	8.c Das für die Qualitätssicherung zuständige Personal des PA-QSA überprüft, ob die PA-QSA-Laborkonfigurationen und -prozesse die Anforderungen erfüllen und korrekt im Bericht dokumentiert wurden.
	8.d Das für die Qualitätssicherung zuständige Personal des PA-QSA überprüft, ob die Testergebnisse im Bericht korrekt dargestellt werden.

© 2006-2016 PCI Security Standards Council, LLC. Alle Rechte vorbehalten.