Settore delle carte di pagamento (PCI)

Standard di protezione dei dati delle applicazioni di pagamento

Requisiti e procedure di valutazione della sicurezza

Versione 3.2

Maggio 2016

Modifiche del documento

Data	Versione	Descrizione	Pagine
1 ottobre 2008	1.2	Allineare il contenuto con il nuovo standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.	
Luglio 2009	1.2.1	In “Ambito del programma PA-DSS” allineare il contenuto con la Guida del programma PA-DSS, v1.2.1, per chiarire con quali applicazioni utilizzare lo standard PA-DSS.	v, vi
		In Requisito laboratorio 6, correggere lo spelling di “OWASP”.	30
		In Attestato di convalida Parte 2a aggiornare la sezione “Funzionalità dell’applicazione di pagamento” affinché sia in linea con i tipi di applicazione elencati nella Guida del programma PA-DSS e chiarire le procedure di riconvalida annuale nella Parte 3b.	32, 33
Ottobre 2010	2.0	Aggiornare e implementare modifiche minori rispetto alla v1.2.1 ed allineare con il nuovo PCI DSS v2.0. Per informazioni dettagliate, fare riferimento a *PA-DSS - Riepilogo delle modifiche dalla Versione PA-DSS 1.2.1 alla 2.0.*	
Novembre 2013	3.0	Aggiornamento da PA-DSS v2. Per informazioni dettagliate, fare riferimento a *PA-DSS - Riepilogo delle modifiche dalla Versione PA-DSS 2.0 alla 3.0.*	
Maggio 2015	3.1	Aggiornamento da PA-DSS v3.0. Per informazioni sulle modifiche, fare riferimento a *PA-DSS - Riepilogo delle modifiche di PA-DSS dalla versione 3.0 alla 3.1*.	
Maggio 2016	3.2	Aggiornamento da PA-DSS v3.1. Per informazioni sulle modifiche, fare riferimento a *PA-DSS – - Riepilogo delle modifiche di PA-DSS dalla versione 3.1 alla 3.2*.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Sommario

Modifiche del documento 2
Introduzione 5
Scopo del documento 5
Relazione tra PCI DSS e PA-DSS 5
Responsabili dell'integrazione e rivenditori 7
Informazioni sull'applicabilità dello standard PCI DSS 7
Ambito del programma PA-DSS 10
Guida per l'implementazione del programma PA-DSS 14
Requisiti per PA-QSA 15
Laboratorio di test 15
Istruzioni e contenuto per il rapporto di convalida 15
Operazioni di completamento del programma PA-DSS 16
Guida del programma PA-DSS 16
Requisiti PCI DSS e procedure di valutazione della sicurezza 17
Requisito 1 - Non conservare i dati della traccia completa, il valore o il codice di verifica della carta (CAV2, CID, CVC2, CVV2) o i dati del blocco PIN 18
Requisito 2 - Proteggere i dati dei titolari di carta memorizzati 24
Requisito 3 - Fornire funzioni di autenticazione sicura 33
Requisito 4 - Registrare l'attività dell'applicazione di pagamento 42
Requisito 5 - Sviluppare applicazioni di pagamento sicure 46
Requisito 6 - Proteggere le trasmissioni wireless 65
Requisito 7 - Sottoporre a test le applicazioni di pagamento per identificare le vulnerabilità e gestire gli aggiornamenti delle applicazioni di pagamento 69
Requisito 8 - Facilitare l'implementazione sicura in rete 73
Requisito 9 - I dati dei titolari di carta non devono mai essere memorizzati su un server connesso a Internet 75
Requisito 10 - Facilitare l'accesso remoto sicuro all'applicazione di pagamento 76
Requisito 11 - Cifratura dei dati sensibili trasmessi su reti pubbliche 80
Requisito 12 - Sicurezza di tutto l'accesso amministrativo non da console 82
Requisito 13 - Gestire una Guida per l'implementazione del programma PA-DSS per clienti, rivenditori e responsabili dell'integrazione 84

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 14 - Assegnare responsabilità PA-DSS al personale e gestire programmi di formazione per personale, clienti, rivenditori e responsabili dell'integrazione 86
Appendice A: Riepilogo del contenuto della *Guida per l'implementazione del programma PA-DSS* 89
Appendice B - Configurazione del laboratorio di test per valutazioni PA-DSS 105

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Introduzione

Scopo del documento

I requisiti e le procedure di valutazione della sicurezza definiscono i requisiti di sicurezza e le procedure di valutazione per i fornitori del software delle applicazioni di pagamento. Questo documento è destinato ai PA-QSA, ossia ai valutatori qualificati delle applicazioni di pagamento, che eseguono le valutazioni delle applicazioni di pagamento per convalidarne la conformità allo standard PA-DSS. Per dettagli su come documentare una valutazione PA-DSS e creare il ROV (Report on Validation, rapporto di convalida), il PA-QSA deve fare riferimento al *modello di reporting ROV PA-DSS*, disponibile sul sito Web dell'Ente responsabile degli standard di protezione PCI (PCI SSC) www.pcisecuritystandards.org.

Ulteriori risorse inclusi Attestati di convalida, Frequently Asked Questions (FAQ) e *Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS* sono disponibili sul sito Web dell'Ente responsabile degli standard di protezione PCI (PCI SSC) www.pcisecuritystandards.org.

Relazione tra PCI DSS e PA-DSS

L'uso di un'applicazione conforme allo standard PA-DSS di per se stesso non rende l'entità conforme allo standard PCI DSS, poiché l'applicazione in questione deve essere implementata in un ambiente conforme allo standard PCI DSS e in conformità alla *Guida per l'implementazione del programma PA-DSS* messa a disposizione dal fornitore di applicazioni di pagamento (in base al Requisito 13 PA-DSS). I requisiti PA-DSS sono ricavati dai *Requisiti PCI DSS e procedure di valutazione della sicurezza*, che descrivono nel dettaglio i punti da rispettare per risultare conformi allo standard PCI DSS (e, di conseguenza, cosa un'applicazione di pagamento deve supportare per facilitare la conformità PCI DSS di un cliente). Lo standard PCI DSS è reperibile su www.pcisecuritystandards.org.

Tutte le applicazioni che memorizzano, elaborano o trasmettono i dati dei titolari di carta rientrano nella valutazione PCI DSS di un'entità, comprese le applicazioni convalidate in base allo standard PA-DSS. La valutazione PCI DSS deve verificare che l'applicazione di pagamento PA-DSS sia configurata correttamente e implementata in modo sicuro nel rispetto dei requisiti PCI DSS. Se l'applicazione di pagamento è stata sottoposta a una qualsiasi personalizzazione, sarà necessario un esame più approfondito durante la valutazione PCI DSS, perché l'applicazione potrebbe non rappresentare più la versione convalidata in base allo standard PA-DSS.

Il PCI DSS potrebbe non applicarsi direttamente ai fornitori di applicazioni di pagamento, a meno che il fornitore non memorizzi, elabori o trasmetta i dati dei titolari di carta o abbia accesso ai dati dei titolari di carta dei clienti. Tuttavia, poiché queste applicazioni di pagamento sono utilizzate dai clienti del fornitore di applicazioni per memorizzare, elaborare e trasmettere dati dei titolari di carta e ai clienti viene richiesto di rispettare lo standard PCI DSS, le applicazioni di pagamento devono facilitare e non impedire la conformità PCI DSS dei clienti. Di seguito alcuni esempi di come le applicazioni di pagamento non sicure possono impedire di rispettare la conformità:

1. memorizzazione di dati su striscia magnetica e/o dati equivalenti sul chip nella rete del cliente a seguito dell'autorizzazione;
2. applicazioni che per un corretto funzionamento richiedono ai clienti di disattivare altre funzioni richieste dallo standard PCI DSS, quali software antivirus o firewall;
3. uso di metodi non sicuri del fornitore per connettersi all'applicazione e fornire supporto al cliente.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Applicazioni di pagamento sicure, quando implementate in un ambiente conforme allo standard PCI DSS, riducono al minimo il rischio di violazioni della sicurezza che possono compromettere numero PAN (Primary Account Number), dati della traccia completa, codici e valori di verifica della carta (CAV2, CID, CVC2, CVV2), PIN e blocchi PIN e limitano i danni derivanti da tali violazioni.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Responsabili dell'integrazione e rivenditori

I fornitori di applicazioni possono rivolgersi a responsabili dell'integrazione e rivenditori per vendere, installare e/o mantenere le applicazioni di pagamento per loro conto. Considerato che spesso forniscono servizi in sede ai clienti del fornitore e collaborano all'installazione di applicazioni di pagamento PA-DSS convalidate, i responsabili dell'integrazione e i rivenditori hanno un ruolo importante nel garantire l'installazione e il funzionamento sicuri delle applicazioni di pagamento. Configurazione, manutenzione o supporto errati di un'applicazione possono determinare la comparsa di vulnerabilità della sicurezza nell'ambiente dei dati dei titolari di carta del cliente, che potrebbero essere sfruttate dagli aggressori. I fornitori di applicazioni devono educare i propri clienti, responsabili dell'integrazione e rivenditori a installare e configurare le applicazioni di pagamento in modo conforme allo standard PCI DSS.

I responsabili dell'integrazione e i rivenditori PCI qualificati (QIR) vengono formati sullo standard PCI DSS e PA-DSS dall'ente responsabile per garantire la corretta implementazione delle applicazioni di pagamento. Per ulteriori informazioni sul programma PCI QIR, consultare la pagina www.pcisecuritystandards.org.

Informazioni sull'applicabilità dello standard PCI DSS

Gli standard PCI DSS si applicano a tutte le entità coinvolte nell'elaborazione di carte di pagamento, con l'inclusione di esercenti, elaboratori, acquirenti, emittenti e provider di servizi, nonché di ***tutte*** le altre entità che si occupano di memorizzare, elaborare o trasmettere dati dei titolari di carta e/o dati sensibili di autenticazione.

Di seguito sono elencati i dati dei titolari di carta e i dati sensibili di autenticazione:

Dati di account	
I dati dei titolari di carta comprendono:	**I dati sensibili di autenticazione comprendono:**
▪ PAN (Primary Account Number) ▪ Nome titolare di carta ▪ Data di scadenza ▪ Codice di servizio	▪ Dati della traccia completa (dati della striscia magnetica o dati equivalenti in un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Blocchi PIN

Il PAN è il fattore determinante per i dati dei titolari di carta. Se il nome del titolare di carta, il codice di servizio e/o la data di scadenza sono memorizzati, elaborati o trasmessi con il PAN, oppure sono presenti in altro modo nell'ambiente di dati dei titolari di carta (CDE), tali dati devono essere protetti in conformità a tutti i requisiti PCI DSS applicabili.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

La tabella riportata nella pagina seguente illustra elementi comunemente utilizzati dei dati dei titolari di carta e dei dati sensibili di autenticazione, indica se la memorizzazione di tali dati è consentita o proibita e se i dati devono essere protetti. Questa tabella non intende essere completa, ma illustra i diversi tipi di requisiti che si applicano a ciascun elemento di dati.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

		Elemento di dati	Memorizzazione consentita	Rendere i dati memorizzati illeggibili per PA-DSS in base al Requisito 2.3
Dati di account	**Dati dei titolari di carta**	PAN (Primary Account Number)	Sì	Sì
		Nome titolare di carta	Sì	No
		Codice di servizio	Sì	No
		Data di scadenza	Sì	No
	Dati sensibili di autenticazione[1]	Dati della traccia completa [2]	No	Impossibile memorizzare in base al Requisito PA-DSS 1.1
		CAV2/CVC2/CVV2/CID[3]	No	Impossibile memorizzare in base al Requisito PA-DSS 1.1
		PIN/Blocco PIN[4]	No	Impossibile memorizzare in base al Requisito PA-DSS 1.1

I Requisiti PA-DSS 2.2 e 2.3 si applicano solo al PAN. In caso di memorizzazione del PAN con altri elementi dei dati dei titolari di carta, è solo il PAN che va reso illeggibile in conformità al Requisito PA-DSS 2.3.

I dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione, anche se cifrati. Questo vale anche se l'ambiente non prevede PAN.

1 *I dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione (anche se cifrati).*

2 *Dati della traccia completa dalla striscia magnetica, dati equivalenti in un chip o in altro luogo.*

3 *Il valore di tre o quattro cifre stampato nella parte anteriore o posteriore di una carta di pagamento.*

4 *Numero di identificazione personale inserito dal titolare della carta durante una transazione con carta presente e/o blocco PIN cifrato presente all'interno del messaggio di transazione.*

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Ambito del programma PA-DSS

Lo standard PA-DSS si applica a fornitori di software e a coloro che sviluppano applicazioni di pagamento che memorizzano, elaborano o trasmettono dati dei titolari di carta e/o dati sensibili di autenticazione. Per informazioni relative all'idoneità dei diversi tipi di applicazioni, consultare la *Guida del programma PA-DSS*.

Nell'ambito della valutazione PA-DSS deve essere verificato quanto segue:

- Ogni funzionalità dell'applicazione di pagamento, compresi senza limitazioni:
    1) funzioni di pagamento end-to-end (autorizzazione e contabilizzazione)
    2) input e output
    3) condizioni di errore
    4) interfacce e collegamenti ad altri file, sistemi e/o applicazioni di pagamento o componenti di applicazioni
    5) tutti i flussi dei dati dei titolari di carta
    6) meccanismi di cifratura
    7) meccanismi di autenticazione
- Istruzioni che il fornitore di applicazioni di pagamento deve fornire a clienti e responsabili dell'integrazione/rivenditori (vedere la *Guida per l'implementazione del programma PA-DSS* più avanti in questo documento) per accertarsi che:
    1) il cliente sia in grado di implementare l'applicazione di pagamento in modo conforme allo standard PCI DSS;
    2) il cliente sia consapevole che determinate impostazioni dell'applicazione di pagamento e dell'ambiente possono impedire la conformità allo standard PCI DSS.

  Tenere presente che il fornitore di applicazioni di pagamento può essere tenuto a fornire tali istruzioni anche quando la specifica impostazione:
    1) non può essere controllata dal fornitore di applicazioni di pagamento una volta installata dal cliente;
    2) è di responsabilità del cliente e non del fornitore di applicazioni di pagamento.
- Tutte le piattaforme selezionate per la versione dell'applicazione di pagamento sottoposta a revisione (specificare le piattaforme incluse)
- Gli strumenti utilizzati da o all'interno dell'applicazione di pagamento per accedere e/o visualizzare i dati dei titolari di carta (strumenti di reporting, registrazione, ecc.)
- Tutti i componenti software correlati all'applicazione di pagamento, inclusi requisiti e dipendenze di software di terzi
- Qualsiasi altro tipo di applicazione di pagamento necessaria per un'implementazione completa
- Metodologia di versioning del fornitore

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Applicabilità dello standard PA-DSS alle applicazioni di pagamento a terminali hardware

In questa sezione sono fornite le istruzioni per i fornitori che intendono ottenere la convalida PA-DSS per applicazioni di pagamento residenti su terminali hardware (detti anche terminali indipendenti o terminali di pagamento dedicati).

La convalida PA-DSS per un'applicazione di pagamento residente su un terminale hardware può essere ottenuta in due modi:

1. l'applicazione di pagamento residente soddisfa direttamente tutti i requisiti PA-DSS ed è convalidata in base alle procedure dello standard PA-DSS;

2. l'applicazione di pagamento residente non soddisfa tutti i requisiti PA-DSS, ma l'hardware su cui l'applicazione è residente è inserito nell'Elenco PCI SCC di dispositivi di sicurezza delle transazioni PIN (PTS) come come dispositivo di punto di interazione (POI) approvato PCI PTS attuale. In questo scenario, potrebbe essere possibile per l'applicazione soddisfare i requisiti PA-DSS attraverso una combinazione di controlli convalidati PTS e PA-DSS.

La restante parte di questa sezione si riferisce solo alle applicazioni di pagamento residenti su un dispositivo POI approvato PCI PTS convalidato.

Se non è possibile per l'applicazione di pagamento soddisfare direttamente uno o più requisiti PA-DSS, questi possono essere soddisfatti in modo indiretto attraverso controlli sottoposti a test come parte della convalida PCI PTS. Per un dispositivo hardware da prendere in esame per l'inserimento in una revisione PA-DSS, il dispositivo hardware DEVE essere convalidato come dispositivo POI approvato PCI PTS ed essere inserito nell'Elenco di dispositivi PTS approvati PCI SSC. Il dispositivo POI convalidato PTS, che mette a disposizione un ambiente informatico affidabile, diventerà una "***dipendenza necessaria***" per l'applicazione di pagamento e la combinazione di applicazione ed hardware sarà inserita insieme nell'Elenco PA-DSS di Convalida applicazioni di pagamento.

In sede di valutazione PA-DSS, il PA-QSA deve sottoporre a un test completo l'applicazione di pagamento con l'annesso hardware in base a tutti i requisiti PA-DSS. Se il PA-QSA ritiene che l'applicazione di pagamento residente non sia in grado di soddisfare uno o più requisiti PA-DSS, ma che questi siano soddisfatti dai controlli convalidati in base allo standard PCI PTS, il PA-QSA è tenuto a:

1. documentare in modo chiaro quali requisiti sono soddisfatti come indicato nel PA-DSS (come di consueto);

2. documentare in modo chiaro quale requisito sia stato soddisfatto mediante PCI PTS nella casella "Presente" per il requisito in questione;

3. inserire un'esauriente spiegazione in merito alle motivazioni in base alle quali l'applicazione di pagamento non era in grado di soddisfare il requisito PA-DSS;

4. documentare le procedure eseguite per stabilire in che modo il requisito in questione veniva soddisfatto completamente attraverso un controllo convalidato PCI PTS;

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

5. elencare il terminale hardware convalidato PCI PTS come dipendenza necessaria nel Riepilogo esecutivo del Rapporto di convalida.

A seguito del completamento della convalida PA-QSA dell'applicazione di pagamento e della successiva accettazione da parte del PCI SSC, il dispositivo hardware convalidato PTS sarà inserito come dipendenza per l'applicazione di pagamento nell'Elenco di applicazioni convalidate PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Le applicazioni di pagamento residenti su terminali hardware che sono convalidate attraverso una combinazione di controlli PA-DSS e PCI PTS devono soddisfare i seguenti criteri:

1. essere forniti insieme al cliente (terminale hardware ed applicazione); se vengono forniti separatamente, il fornitore dell'applicazione e/o il responsabile dell'integrazione/rivenditore deve inviare l'applicazione per la distribuzione in modo che funzioni esclusivamente sul terminale hardware per il quale ha ricevuto la convalida;
2. consentire per impostazione predefinita di supportare la conformità allo standard PCI DSS del cliente;
3. comprendere assistenza ed aggiornamenti continui per conservare la conformità allo standard PCI DSS;
4. in caso di vendita, distribuzione o concessione in licenza separata dell'applicazione ai clienti, il fornitore è tenuto a fornire informazioni dettagliate sull'hardware dipendente necessario per l'utilizzo con l'applicazione, in conformità al suo elenco di convalida PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Guida per l’implementazione del programma PA-DSS

Le applicazioni di pagamento convalidate devono poter essere implementate in modo conforme allo standard PCI DSS. Ai fornitori di software viene richiesto di fornire una *Guida per l’implementazione del programma PA-DSS* per istruire i relativi clienti e responsabili dell’integrazione/rivenditori a implementare il prodotto in modo sicuro, per documentare le specifiche di configurazione sicure menzionate nel presente documento e per delineare chiaramente le responsabilità di fornitori, responsabili dell’integrazione/rivenditori e clienti relativamente ai requisiti PCI DSS. In tale Guida deve essere descritto dettagliatamente come il cliente e/o il responsabile dell’integrazione/rivenditore deve abilitare le impostazioni di sicurezza all’interno della rete del cliente. Ad esempio, la *Guida per l’implementazione del programma PA-DSS* deve fornire tutte le informazioni rilevanti sulle responsabilità e sulle funzionalità di base della sicurezza delle password PCI DSS anche se non controllate dall’applicazione di pagamento, in modo che il cliente o il responsabile dell’integrazione/rivenditore comprenda come implementare password sicure per la conformità allo standard PCI DSS.

La *Guida per l’implementazione del programma PA-DSS* deve fornire dettagli su come configurare l’applicazione di pagamento per soddisfare i requisiti e non semplicemente ribadire i requisiti PCI DSS o PA-DSS. Durante una valutazione, il PA-QSA deve verificare che le istruzioni siano precise ed efficaci. Il PA-QSA deve inoltre verificare che la *Guida per l’implementazione del programma PA-DSS* venga distribuita a clienti e responsabili dell’integrazione/rivenditori.

Le applicazioni di pagamento, quando implementate in base alla *Guida per l’implementazione del programma PA-DSS* e quando implementate in un ambiente conforme allo standard PCI DSS, devono facilitare e supportare la conformità a tale standard del cliente.

Fare riferimento all’*Appendice A. Riepilogo del contenuto della Guida per l’implementazione del programma PA-DSS* per un confronto delle responsabilità di implementazione dei controlli specificati nella *Guida per l’implementazione del programma PA-DSS*.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti per PA-QSA

Solo i PA-QSA (Payment Application Qualified Security Assessor) assunti da società PA-QSA sono autorizzati a eseguire valutazioni di conformità allo standard PA-DSS. Fare riferimento all'elenco di PA-QSA all'indirizzo www.pcisecuritystandards.org per un elenco delle società qualificate a eseguire valutazioni di conformità allo standard PA-DSS.

- Il PA-QSA deve utilizzare le procedure di test descritte nel presente documento.
- Il PA-QSA deve avere accesso a un laboratorio in cui eseguire il processo di convalida.

Laboratorio di test

- I laboratori di test possono essere presenti in una delle due seguenti posizioni: in sede presso il PA-QSA, oppure in sede presso il fornitore del software.
- Il laboratorio deve essere in grado di simulare l'uso nel mondo reale dell'applicazione di pagamento.
- Il PA-QSA deve validare l'installazione completa dell'ambiente del laboratorio per assicurare l'effettiva simulazione da parte dell'ambiente di una situazione nel mondo reale e la mancata modifica o alterazione dell'ambiente in alcun modo da parte del fornitore.
- Fare riferimento all'*Appendice B. Conferma della configurazione del laboratorio di test specifica per la valutazione PA-DSS* in questo documento per verificare i requisiti dettagliati per il laboratorio e i processi correlati.
- Il PA-QSA deve completare e inviare l'*Appendice B* per il laboratorio specifico utilizzato per la revisione dell'applicazione di pagamento, insieme al ROV PA-DSS completato.

Istruzioni e contenuto per il rapporto di convalida

Le istruzioni e i contenuti per il ROV PA-DSS ora vengono forniti nel *modello di reporting ROV PA-DSS.* Il *modello di reporting ROV PA-DSS* deve essere utilizzato per creare il ROV. Solo i ROV delle applicazioni di pagamento conformi devono essere inoltrati al PCI SSC. Per dettagli sul processo di inoltro dei ROV, fare riferimento alla *Guida del programma PA-DSS*.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Operazioni di completamento del programma PA-DSS

Questo documento contiene la tabella dei requisiti e delle Procedure di valutazione della sicurezza, nonché *l'Appendice B - Configurazione del laboratorio di test per valutazioni PA-DSS*. I requisiti e le procedure di valutazione della sicurezza descrivono dettagliatamente le procedure che deve eseguire il PA-QSA.

Il PA-QSA deve effettuare le seguenti operazioni:

1. confermare l'ambito della valutazione PA-DSS;
2. eseguire la valutazione PA-DSS;
3. completare il ROV utilizzando il *modello di reporting ROV PA-DSS*, compresa la conferma della configurazione del laboratorio di test utilizzata per la valutazione PA-DSS;
4. completare e firmare un Attestato di convalida (entrambi, PA-QSA e fornitore del software); l'Attestato di convalida è disponibile sul sito Web PCI SSC (www.pcisecuritystandards.org);
5. dopo il completamento, inviare tutti i documenti precedenti e la *Guida per l'implementazione del programma PA-DSS* a PCI SSC in base alle istruzioni fornite nella *Guida del programma PA-DSS.*

Nota:

gli inoltri PA-DSS non devono avvenire a meno che tutti i requisiti PA-DSS non abbiano ricevuto la convalida.

Guida del programma PA-DSS

Fare riferimento alla *Guida del programma PA-DSS* per informazioni sulla gestione del programma PA-DSS, inclusi i seguenti argomenti:

- Dettagli di versioni PA-DSS differenti e le relative date di validità
- Applicabilità dello standard PA-DSS a diversi tipi di applicazioni
- Processi di invio e accettazione del rapporto PA-DSS
- Processo di rinnovo annuale delle applicazioni di pagamento incluse nell'Elenco di applicazioni di pagamento convalidate
- Responsabilità di notifica nel caso in cui un'applicazione presente in elenco venga compromessa

PCI SSC si riserva il diritto di richiedere la riconvalida in seguito a modifiche significative dello standard PA-DSS e/o in seguito all'identificazione di vulnerabilità specifiche di una delle applicazioni di pagamento presenti in elenco.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PCI DSS e procedure di valutazione della sicurezza

I seguenti sono gli elementi che costituiscono le intestazioni delle colonne dalla tabella per i requisiti PA-DSS e le procedure di valutazione della sicurezza:

- **Requisiti PA-DSS:** questa colonna illustra i requisiti di sicurezza in base ai quali vengono convalidate le applicazioni di pagamento.
- **Procedure di test:** questa colonna chiarisce i processi di test che il PA-QSA deve seguire per convalidare il rispetto dei requisiti PA-DSS
- **Istruzioni:** questa colonna descrive lo scopo o l'obiettivo di sicurezza di ogni requisito PA-DSS e mira a facilitare la comprensione dei requisiti. Le istruzioni di questa colonna non sostituiscono né estendono i requisiti PA-DSS e le procedure di test.

Nota:

i requisiti PA-DSS non devono essere convalidati se i controlli non sono stati ancora implementati o se sono programmati per una data futura.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 1 - Non conservare i dati della traccia completa, il valore o il codice di verifica della carta (CAV2, CID, CVC2, CVV2) o i dati del blocco PIN

Requisiti PA-DSS	Procedure di test	Istruzioni
1.1 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati). Se si ricevono dati sensibili di autenticazione, dopo il completamento del processo di autorizzazione rendere tutti i dati non recuperabili. I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti da 1.1.1 a 1.1.3. ***In linea con il Requisito 3.2 PCI DSS***	**1.1.a** Se questa applicazione di pagamento memorizza dati sensibili di autenticazione, verificare che l'applicazione sia destinata solo a emittenti e/o a società che supportano servizi di emissione.	I dati sensibili di autenticazione sono costituiti da dati della traccia completa, valore o codice di convalida della carta e dati PIN. La memorizzazione dei dati sensibili di autenticazione dopo l'autorizzazione è vietata. Questi dati sono particolarmente preziosi per gli utenti non autorizzati, in quanto consentono loro di generare carte di pagamento contraffatte e conseguenti transazioni fraudolente. Le entità che emettono carte di pagamento o che eseguono o supportano servizi di emissione spesso creano e controllano dati sensibili di autenticazione durante il processo di emissione. Gli emittenti e le società che supportano servizi di emissione sono autorizzati a memorizzare i dati sensibili di autenticazione in presenza di una giustificazione aziendale, a patto che utilizzino metodi sicuri. Per le entità che non emettono direttamente, la conservazione di dati sensibili di autenticazione dopo l'autorizzazione non è consentita e l'applicazione deve prevedere un meccanismo per l'eliminazione sicura dei dati, in modo che diventino non recuperabili.
	1.1.b Per tutte le altre applicazioni di pagamento, se i dati sensibili di autenticazione (vedere i successivi punti da 1.1.1 a 1.1.3) vengono memorizzati prima dell'autorizzazione, è necessario ottenere e riesaminare la metodologia per l'eliminazione sicura dei dati per verificare che i dati siano non recuperabili.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
1.1.1 Dopo l'autorizzazione, non memorizzare l'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, dati equivalenti contenuti in un chip o in altro luogo). Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati della striscia magnetica. ***Nota:*** *nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:* • *Nome del titolare del conto* • *PAN (Primary Account Number)* • *Data di scadenza* • *Codice di servizio* *Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari.* ***In linea con il Requisito 3.2.1 PCI DSS***	**1.1.1** Installare l'applicazione di pagamento ed eseguire varie transazioni di test che simulino tutte le funzioni dell'applicazione di pagamento, compresa la generazione di condizioni di errore e voci di registro. Utilizzare strumenti e/o metodi forensi (strumenti commerciali, script, ecc.)[5] per esaminare tutto l'output creato dall'applicazione di pagamento e verificare che non venga memorizzato, dopo l'autorizzazione, l'intero contenuto di ogni traccia dalla striscia magnetica della carta o i dati equivalenti in un chip. Includere almeno i seguenti tipi di file (nonché altro output generato dall'applicazione di pagamento): • Dati di transazioni in entrata • Tutti i registri (ad esempio, transazioni, cronologia, debug o errori) • File di cronologia • File di traccia • Memoria non volatile, inclusa la cache non volatile • Schemi di database • Contenuto di database	Se vengono memorizzati dati della traccia completa, gli utenti non autorizzati che otterranno tali dati potranno riprodurre carte di pagamento e completare transazioni fraudolente.

[5] *Strumento o metodo forense: uno strumento o un metodo per rilevare, analizzare e presentare dati forensi, che consentono di autenticare, ricercare e recuperare una prova su computer in modo rapido ed esauriente. Nel caso di strumenti o metodi forensi utilizzati dai PA-QSA, questi strumenti o metodi devono individuare accuratamente eventuali dati sensibili di autenticazione scritti dall'applicazione di pagamento. Tali strumenti possono essere commerciali, open-source o sviluppati in-house dal PA-QSA.*

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
1.1.2 Dopo l'autorizzazione, non memorizzare il Card Validation Code or Value (numero di tre o quattro cifre stampato sulla parte anteriore o posteriore della carta di pagamento utilizzato per verificare le transazioni con carta non presente). ***In linea con il Requisito 3.2.2 PCI DSS***	**1.1.2** Installare l'applicazione di pagamento ed eseguire varie transazioni di test che simulino tutte le funzioni dell'applicazione di pagamento, compresa la generazione di condizioni di errore e voci di registro. Utilizzare strumenti e/o metodi forensi (strumenti commerciali, script, ecc.) per esaminare tutto l'output creato dall'applicazione di pagamento e verificare che il codice di validazione della carta a tre o quattro cifre stampato sulla parte anteriore della carta o nel riquadro della firma (dati CVV2, CVC2, CID, CAV2) non sia memorizzato dopo l'autorizzazione. Includere almeno i seguenti tipi di file (nonché altro output generato dall'applicazione di pagamento): • Dati di transazioni in entrata • Tutti i registri (ad esempio, transazioni, cronologia, debug o errori) • File di cronologia • File di traccia • Memoria non volatile, inclusa la cache non volatile • Schemi di database • Contenuto di database	Lo scopo del codice di validazione della carta è proteggere le transazioni in cui il consumatore e la carta non sono presenti, ad esempio ordini via Internet oppure ordini via posta/telefono (MO/TO). Se questi dati vengono sottratti, gli individui non autorizzati possono eseguire transazioni Internet e MO/TO fraudolente.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
1.1.3 Dopo l'autorizzazione, non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato. ***In linea con il Requisito 3.2.3 PCI DSS***	**1.1.3** Installare l'applicazione di pagamento ed eseguire varie transazioni di test che simulino tutte le funzioni dell'applicazione di pagamento, compresa la generazione di condizioni di errore e voci di registro. Utilizzare strumenti e/o metodi forensi (strumenti commerciali, script, ecc.) per esaminare tutto l'output creato dall'applicazione di pagamento e verificare che i PIN e i blocchi PIN cifrati non siano memorizzati dopo l'autorizzazione. Includere almeno i seguenti tipi di file (nonché altro output generato dall'applicazione di pagamento): • Dati di transazioni in entrata • Tutti i registri (ad esempio, transazioni, cronologia, debug o errori) • File di cronologia • File di traccia • Memoria non volatile, inclusa la cache non volatile • Schemi di database • Contenuto di database	Questi valori dovrebbero essere noti soltanto al proprietario della carta o alla banca che ha emesso la carta. Se questi dati vengono sottratti, gli individui non autorizzati possono eseguire transazioni fraudolente di addebito basate su PIN (ad esempio, prelievi Bancomat).

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
1.1.4 Eliminare in modo sicuro i dati delle tracce (dalla striscia magnetica o i dati equivalenti in un chip), i codici o valori di verifica della carta, i PIN e i blocchi PIN memorizzati da precedenti versioni dell'applicazione di pagamento, in conformità con lo standard per l'eliminazione sicura accettati dal settore, come definito, ad esempio, dall'elenco dei prodotti approvati gestito dalla National Security Agency (NSA) o da qualsiasi altro ente che gestisce standard o normative a livello statale o nazionale. ***Nota:*** *questo requisito è valido solo se le precedenti versioni dell'applicazione di pagamento prevedevano la memorizzazione di dati sensibili di autenticazione.* ***In linea con il Requisito 3.2 PCI DSS***	**1.1.4.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti istruzioni per i clienti e i responsabili dell'integrazione/rivenditori: • i dati cronologici devono essere rimossi (dati delle tracce, codici di verifica della carta, PIN o blocchi PIN memorizzati da precedenti versioni dell'applicazione di pagamento); • modalità di rimozione dei dati cronologici; • tale rimozione è assolutamente necessaria per garantire la conformità allo standard PCI DSS. **1.1.4.b** Esaminare i file del software dell'applicazione di pagamento e la documentazione di configurazione per verificare che il fornitore metta a disposizione uno strumento o una procedura per la pulizia che elimini i dati. **1.1.4.c** Verificare, mediante l'uso di strumenti e metodi forensi, che lo strumento o la procedura di pulizia sicura rimuova in modo appropriato i dati, in base agli standard per l'eliminazione sicura dei dati accettati dal settore.	La memorizzazione di tutti questi elementi dei dati sensibili di autenticazione dopo l'autorizzazione è vietata. Se le precedenti versioni delle applicazioni di pagamento memorizzavano queste informazioni, il fornitore di applicazioni di pagamento è tenuto a fornire le istruzioni nella *Guida per l'implementazione del programma PA-DSS* e uno strumento o una procedura per la pulizia sicuri. Se non vengono eliminati in modo sicuro, questi dati potrebbero restare nascosti nei sistemi di clienti e individui non autorizzati potrebbero accedere a queste informazioni e utilizzarle per generare carte di pagamento contraffatte e/o eseguire transazioni fraudolente.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
1.1.5 Non memorizzare dati sensibili di autenticazione sui sistemi del fornitore. Se i dati sensibili di autenticazione (prima dell'autorizzazione) devono essere utilizzati per operazioni di debug o risoluzione dei problemi, verificare che: • i dati sensibili di autenticazione vengano raccolti solo quando necessario per risolvere un problema specifico; • i dati siano memorizzati in posizioni specifiche e note con accesso limitato; • vengano raccolti solo i dati indispensabili per risolvere un problema specifico; • i dati sensibili di autenticazione siano cifrati con crittografia avanzata al momento della memorizzazione; • i dati siano eliminati in modo sicuro immediatamente dopo l'uso anche da: – file di registro – file di debug – altre origini dati ricevute dai clienti. ***In linea con il Requisito 3.2 PCI DSS***	**1.1.5.a** Esaminare le procedure del *fornitore del software* per risolvere eventuali problemi dei clienti e verificare che le procedure includano: • raccolta di dati sensibili di autenticazione solo quando necessario per risolvere un problema specifico; • memorizzazione di tali dati solo in posizioni specifiche e note con accesso limitato; • raccolta solo della quantità di dati limitata necessaria per risolvere un problema specifico; • cifratura dei dati sensibili di autenticazione al momento della memorizzazione; • eliminazione sicura di tali dati immediatamente dopo l'uso. **1.1.5.b** Selezionare un campione di recenti richieste di risoluzione di problemi inviate dai clienti e verificare che ciascun evento abbia seguito la procedura descritta al punto 1.1.5.a. **1.1.5.c** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • raccogliere dati sensibili di autenticazione solo quando necessario per risolvere un problema specifico; • memorizzare tali dati solo in posizioni specifiche e note con accesso limitato; • raccogliere solo la quantità di dati limitata necessaria per risolvere un problema specifico; • cifrare i dati sensibili di autenticazione al momento della memorizzazione; • eliminare in modo sicuro tali dati immediatamente dopo l'uso.	Se il fornitore offre ai clienti servizi che potrebbero prevedere la raccolta di dati sensibili di autenticazione (ad esempio per operazioni di debug o risoluzione dei problemi), il fornitore deve limitare al minimo la raccolta dei dati e garantire che tali dati vengano protetti ed eliminati in modo sicuro non appena non sono più necessari. Se la risoluzione di un problema richiede che l'applicazione venga temporaneamente configurata per l'acquisizione di dati sensibili di autenticazione, si dovrà poi ripristinare la solita configurazione sicura (disabilitando la raccolta dei dati sensibili di autenticazione) immediatamente dopo il completamento dell'acquisizione dati necessaria. Se non sono più necessari, i dati sensibili di autenticazione devono essere eliminati in conformità agli standard accettati dal settore (ad esempio utilizzando un programma per la pulizia sicura che elimini la possibilità di recupero dei dati).

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 2 - Proteggere i dati dei titolari di carta memorizzati

Requisiti PA-DSS	Procedure di test	Istruzioni
2.1 Il fornitore del software deve fornire ai clienti istruzioni per l'eliminazione sicura dei dati dei titolari di carta dopo la scadenza del periodo di conservazione definito dal cliente. ***In linea con il Requisito 3.1. PCI DSS***	**2.1.** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • i dati dei titolari di carta che superano il periodo di conservazione definito dal cliente devono essere eliminati; • un elenco di tutte le posizioni in cui l'applicazione di pagamento memorizza i dati dei titolari di carta (in modo che il cliente conosca le posizioni dei dati da eliminare); • istruzioni necessarie affinché i clienti eliminino in modo sicuro i dati dei titolari di carta quando non sono più utili a fini legali, normativi o commerciali; • istruzioni per eliminare in modo sicuro i dati dei titolari di carta memorizzati dall'applicazione di pagamento, compresi i dati memorizzati nei sistemi o nel software sottostanti (come sistema operativo, database, ecc.); • istruzioni per configurare i sistemi o il software sottostanti (come sistema operativo, database, ecc.) per impedire l'acquisizione o la conservazione involontaria di dati dei titolari di carta (ad esempio backup di sistema o punti di ripristino).	Per supportare il Requisito 3.1 PCI DSS, il fornitore deve comunicare i dettagli di tutte le posizioni in cui l'applicazione di pagamento può memorizzare i dati dei titolari di carta, compresi i software o sistemi sottostanti (come sistema operativo, database, ecc.), e le istruzioni per l'eliminazione sicura dei dati da tali posizioni una volta che è stato superato il periodo di conservazione dei dati definito dal cliente. I clienti e i responsabili dell'integrazione/rivenditori devono ricevere dettagli anche sulla configurazione dei sistemi e dei software sottostanti all'applicazione in esecuzione, per sapere con certezza che tali sistemi non acquisiscono dati dei titolari di carta all'insaputa del cliente. Il cliente deve essere a conoscenza del modo in cui i sistemi sottostanti acquisiscono i dati dall'applicazione per evitarne l'acquisizione o per garantirne un'adeguata protezione.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
2.2 Mascherare il PAN quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) in modo che il PAN completo sia visibile solo al personale con un'esigenza aziendale legittima. ***Nota:*** *questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati dei titolari di carta, ad esempio requisiti legali o del marchio di carta di pagamento per ricevute di punti di vendita (POS).* ***In linea con il Requisito 3.3 PCI DSS***	**2.2.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • dettagli di tutte le istanze in cui il PAN viene visualizzato, compresi, a titolo di esempio, dispositivi POS, schermi, registri e ricevute; • conferma che, per impostazione predefinita, l'applicazione di pagamento maschera il PAN in tutte le visualizzazioni; • istruzioni per la configurazione dell'applicazione di pagamento in modo che solo il personale con un'esigenza aziendale legittima possa vedere più di sei cifre all'inizio/quattro cifre alla fine del PAN (include la visualizzazione dell'intero numero PAN).	La visualizzazione dell'intero numero PAN su elementi quali monitor di computer, ricevute di carte di pagamento, fax o rendicontazioni cartacee può comportare il recupero di tali dati da parte di utenti non autorizzati e il loro utilizzo fraudolento. L'approccio di mascheratura deve sempre garantire che venga visualizzato solo il numero minimo di cifre secondo necessità per eseguire una funzione aziendale specifica. Ad esempio, se per eseguire una funzione aziendale sono necessarie solo le ultime quattro cifre, mascherare il PAN in modo che singoli utenti che eseguono tale funzione possano visualizzare solo le ultime quattro cifre. *(continua alla pagina successiva)*
	2.2.b Installare l'applicazione di pagamento ed esaminare tutte le visualizzazioni dei dati PAN, compresi, a titolo di esempio, dispositivi POS, schermi, registri e ricevute. Per ogni istanza in cui viene visualizzato il PAN, verificare che il PAN sia mascherato quando viene visualizzato.	Come altro esempio, se una funzione deve accedere al numero di identificazione bancaria (BIN) per finalità di routing, disabilitare la mascheratura solo delle cifre BIN (in genere le prime sei cifre) durante tale funzione. Questo requisito si riferisce anche alla protezione del PAN visualizzato su schermi, ricevute cartacee, stampe ecc. e non deve essere confuso con il Requisito 2.3 PA-DSS per la protezione del PAN quando viene memorizzato in file, database, ecc.
	2.2.c Configurare l'applicazione di pagamento secondo la *Guida per l'implementazione del programma PA-DSS* per consentire la visualizzazione di più di sei cifre all'inizio/quattro cifre alla fine del PAN solo al personale con un'esigenza aziendale legittima. Per ogni istanza in cui viene visualizzato il PAN, esaminare le configurazioni dell'applicazione e le visualizzazioni del PAN per verificare che le istruzioni per il mascheramento del PAN siano accurate e che solo il personale con un'esigenza aziendale legittima possa visualizzare più di sei cifre all'inizio/quattro cifre alla fine del PAN.	
2.3 Rendere illeggibile il numero PAN ovunque sia memorizzato (inclusi i dati su supporti digitali	**2.3.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per	La mancanza di protezione dei numeri PAN può consentire agli utenti non autorizzati di

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
portatili, supporti di backup, registri) utilizzando uno dei seguenti approcci: • Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN) • Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN) • Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro) • crittografia avanzata con relativi processi e procedure di gestione delle chiavi. *(continua alla pagina successiva)*	verificare che la documentazione includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • dettagli di tutte le opzioni configurabili per ogni metodo utilizzato dall'applicazione per rendere i dati dei titolari di carta illeggibili e istruzioni su come configurare ogni metodo per tutte le posizioni in cui i dati dei titolari di carta vengono memorizzati dall'applicazione di pagamento (per Requisito 2.1 PA-DSS); • un elenco di tutte le istanze in cui i dati dei titolari di carta possono rappresentare un output che il cliente memorizza al di fuori dell'applicazione di pagamento e istruzioni che spiegano che il cliente è responsabile dell'illeggibilità del PAN in tutte le istanze di questo tipo; • istruzioni per cui se i log di debugging sono sempre abilitati (ad esempio, per le finalità della risoluzione dei problemi) e i log includono il PAN, devono essere protetti in base a PCI DSS, disabilitati non appena viene completata la risoluzione dei problemi ed eliminati in modo sicuro quando non sono più necessari.	visualizzare o scaricare questi dati. Le funzioni di hash one-way basate sulla crittografia avanzata possono essere utilizzate per rendere illeggibili i dati dei titolari di carta. Le funzioni di hash sono adatte all'uso quando non è necessario recuperare il numero originale (l'hash one-way è irreversibile). Lo scopo della troncatura è memorizzare solo una parte del PAN (non oltre le prime sei e le ultime quattro cifre). Un token indicizzato è un token crittografico che sostituisce il PAN in base a un determinato indice per un valore imprevedibile. Un pad one-time è un sistema in cui una chiave privata, generata in modo casuale, viene utilizzata una sola volta per cifrare un messaggio, che successivamente sarà decifrato utilizzando una chiave e un pad one-time corrispondente. *(continua alla pagina successiva)*
Note: • per un utente non autorizzato è relativamente facile ricostruire i dati PAN originali se ha accesso alla versione troncata e hash del PAN. Nel caso in cui versione troncata e hash dello stesso PAN siano generate da un'applicazione di pagamento, ulteriori controlli andrebbero predisposti per verificare che non sia possibile correlare la versione troncata e hash per ricostruire il PAN originale. • Il PAN deve essere reso illeggibile ovunque è memorizzato, anche al di fuori dell'applicazione di pagamento (ad esempio output dei file di log dell'applicazione per la memorizzazione nell'ambiente del cliente).	**2.3.b** Esaminare il metodo adottato per proteggere il PAN, inclusi gli algoritmi di cifratura (se applicabili). Verificare che il PAN sia stato reso illeggibile tramite uno dei seguenti metodi: • hash one-way basati su crittografia avanzata; • troncatura; • token e pad indicizzati, con pad custoditi in un luogo sicuro; • crittografia avanzata con relativi processi e procedure di gestione delle chiavi. **2.3.c** Se l'applicazione crea versione troncata e hash dello stesso PAN, esaminare metodi per la creazione della versione troncata e hash per verificare che entrambe le versioni non possano essere correlate per ricostruire il PAN originale.	Lo scopo della crittografia avanzata (come chiarito in *Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS*) è basare la cifratura su un algoritmo accettato e collaudato nel settore (non un algoritmo proprietario o personale) con chiavi di crittografia avanzata.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
In linea con il Requisito 3.4 PCI DSS	**2.3.d** Esaminare diverse tabelle o file dei repository dei dati creati o generati dall'applicazione per verificare che il PAN sia reso illeggibile.	
	2.3.e Se l'applicazione crea o genera file da utilizzare al di fuori della stessa (ad esempio, file generati per l'esportazione o il backup), compresa la memorizzazione su supporti rimovibili, esaminare un campione dei file generati, compresi quelli generati su supporti rimovibili (ad esempio, nastri di back-up), per confermare che il PAN è reso illeggibile.	
	2.3.f Esaminare un campione di log di audit creati o generati da un'applicazione per confermare che il PAN è reso illeggibile oppure eliminato dai log.	
	2.3.g Se il fornitore del software memorizza il PAN per qualsiasi motivo (ad esempio, per eseguire operazioni di debug o risoluzione di problemi segnalati dai clienti mediante file di log, file di debug o altre origini dei dati), verificare che il PAN sia reso illeggibile in base ai Requisiti da 2.3.b a 2.3.f riportati sopra.	
2.4 L'applicazione di pagamento deve proteggere ogni chiave utilizzata per proteggere i dati dei titolari di carta da divulgazione e uso improprio. ***Nota:*** *questo requisito si applica alle chiavi utilizzate per cifrare i dati dei titolari di carta memorizzati e alle chiavi di cifratura delle chiavi (KEK) utilizzate per proteggere le chiavi di cifratura dei dati. Tali KEK devono essere avanzate almeno quanto la chiave di cifratura dei dati.* ***In linea con il Requisito 3.5 PCI DSS***	**2.4.a** Esaminare la documentazione del prodotto e consultare il personale responsabile per verificare che vengano eseguiti controlli che limitano l'accesso alle chiavi di crittografia utilizzate dall'applicazione.	Le chiavi di crittografia devono essere protette in modo avanzato, perché chiunque le ottenga sarà in grado di decifrare i dati. Il requisito che le applicazioni di pagamento devono rispettare per proteggere le chiavi da divulgazione e uso improprio si applica sia alle chiavi di cifratura dei dati che alle KEK. Non si prevede la cifratura delle KEK, ad ogni modo queste chiavi devono essere protette da divulgazione e uso improprio come indicato al Requisito 2.4.
	2.4.b Esaminare i file di configurazione del sistema per verificare che: • le chiavi vengano memorizzate in un formato cifrato; • le KEK siano memorizzate separatamente dalle chiavi di cifratura dei dati; • le KEK siano avanzate almeno quanto le chiavi di cifratura dei dati che devono proteggere.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	2.4.c Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che contenga istruzioni per clienti e responsabili dell'integrazione/rivenditori per: • limitare l'accesso alle chiavi al minor numero possibile di persone necessarie; • memorizzare le chiavi in modo sicuro nel minor numero possibile di posizioni e moduli.	Dovrebbe essere molto limitato il numero di persone che ha accesso alle chiavi di crittografia, di solito solo coloro che hanno responsabilità di custodia delle chiavi.
2.5 L'applicazione di pagamento deve implementare processi e procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati dei titolari di carta, incluso almeno quanto segue: ***In linea con il Requisito 3.6 PCI DSS***	**2.5** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti istruzioni per i clienti e i responsabili dell'integrazione/rivenditori: • in che modo generare, distribuire, proteggere, modificare, memorizzare e ritirare/sostituire in modo sicuro le chiavi di crittografia, nei casi in cui i clienti o i responsabili dell'integrazione/rivenditori siano coinvolti in queste attività di gestione delle chiavi; • un modulo campione per i custodi delle chiavi con cui accettano e confermano di conoscere le proprie responsabilità.	La gestione delle chiavi di crittografia è una parte fondamentale della sicurezza continua dell'applicazione di pagamento. Un valido processo di gestione delle chiavi, sia esso manuale o automatico, come parte del prodotto di cifratura, è basato sugli standard di settore e gestisce tutti gli elementi chiave da 2.5.1 a 2.5.7. Fornire ai clienti istruzioni su come trasmettere, memorizzare e aggiornare le chiavi di crittografia in modo sicuro contribuisce a prevenire l'errata gestione delle chiavi o la loro divulgazione a entità non autorizzate. Lo scopo di questo requisito riguarda le chiavi utilizzate per cifrare i dati dei titolari di carta memorizzati e ogni rispettiva KEK.
2.5.1 Generazione di chiavi di crittografia avanzata	**2.5.1.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che comprenda le istruzioni per i clienti e i responsabili dell'integrazione/rivenditori su come generare in modo sicuro le chiavi di crittografia.	L'applicazione di pagamento deve generare chiavi avanzate, come definito in *Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS* alla sezione "Crittografia avanzata".
	2.5.1.b Sottoporre a test l'applicazione, compreso il metodo utilizzato per generare le chiavi di crittografia, per verificare che le istruzioni riportate nella *Guida per l'implementazione del programma PA-DSS* portino alla generazione di chiavi di crittografia avanzate.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
2.5.2 Distribuzione di chiavi di crittografia sicure	**2.5.2.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che comprenda le istruzioni per i clienti e i responsabili dell'integrazione/rivenditori su come distribuire in modo sicuro le chiavi di crittografia.	L'applicazione di pagamento deve distribuire le chiavi in modo sicuro, vale a dire che le chiavi non vengono distribuite in chiaro e attraverso processi autorizzati.
	2.5.2.b Sottoporre a test l'applicazione, compreso il metodo utilizzato per distribuire le chiavi di crittografia, per verificare che le istruzioni riportate nella *Guida per l'implementazione del programma PA-DSS* portino alla distribuzione sicura delle chiavi di crittografia.	
2.5.3 Memorizzazione di chiavi di crittografia sicure	**2.5.3.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che comprenda le istruzioni per i clienti e i responsabili dell'integrazione/rivenditori su come memorizzare in modo sicuro le chiavi di crittografia.	L'applicazione di pagamento deve memorizzare le chiave in modo sicuro (ad esempio, applicando una cifratura con una KEK).
	2.5.3.b Sottoporre a test l'applicazione, compreso il metodo utilizzato per memorizzare le chiavi di crittografia, per verificare che le istruzioni riportate nella *Guida per l'implementazione del programma PA-DSS* portino alla memorizzazione sicura delle chiavi di crittografia.	
2.5.4 Modifiche delle chiavi di crittografia per le chiavi giunte al termine del loro periodo di validità (ad esempio, una volta trascorso un periodo di tempo definito e/o dopo la produzione da parte di una determinata chiave di una quantità definita di testo di cifratura), come specificato dal fornitore dell'applicazione associato o dal proprietario delle chiavi, ed in base alle linee guida e alle migliori pratiche di settore (ad esempio, *NIST Special*	**2.5.4.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che comprenda le seguenti istruzioni per i clienti e i responsabili dell'integrazione/rivenditori: • periodo di validità definito per ogni tipo di chiave utilizzato dall'applicazione; • procedure per l'applicazione delle modifiche alle chiavi una volta raggiunto il periodo di validità definito.	Il periodo di validità è il periodo durante il quale una determinata chiave di crittografia può essere usata per uno scopo preciso. Le considerazioni per la definizione del periodo di validità includono, senza limitazioni, la solidità dell'algoritmo sottostante, le dimensioni o la lunghezza della chiave, il rischio che la chiave possa essere compromessa e la sensibilità dei dati che vengono cifrati.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
Publication 800-57).	**2.5.4.b** Sottoporre a test l'applicazione, compresi i metodi di modifica delle chiavi di crittografia, per verificare che le istruzioni riportate nella *Guida per l'implementazione del programma PA-DSS* portino alla modifica delle chiavi giunte al termine del periodo di validità definito.	La modifica periodica delle chiavi di cifratura che sono giunte al termine del loro periodo di validità è fondamentale per ridurre al minimo il rischio che qualcuno ottenga le chiavi e le utilizzi per decifrare i dati.
2.5.5 Ritiro o sostituzione delle chiavi (ad esempio, mediante archiviazione, distruzione e/o revoca, come applicabile) come ritenuto necessario in caso di indebolimento dell'integrità della chiave (ad esempio, partenza di un dipendente a conoscenza di chiavi con testo in chiaro, ecc.) o chiavi per le quali esista il sospetto che siano state compromesse. ***Nota:*** *se le chiavi di crittografia ritirate o sostituite devono essere conservate, queste chiavi devono essere archiviate in modo sicuro (ad esempio, usando una KEK). Le chiavi di crittografia archiviate dovrebbero essere usate solo per scopi di decifratura/verifica.*	**2.5.5.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • istruzioni relative alla necessità di ritirare o sostituire le chiavi in caso di indebolimento dell'integrità o di compromissione nota o sospetta di una chiave; • procedure per il ritiro o la sostituzione delle chiavi (ad esempio, mediante archiviazione, distruzione e/o revoca, come applicabile); • procedure che garantiscano che le chiavi di crittografia ritirate o sostituite non vengano utilizzate per le operazioni di cifratura.	Le chiavi che non sono più necessarie o in uso, o le chiavi di cui si conosce o si sospetta la compromissione, vanno ritirate e/o distrutte per garantire che non possano essere più utilizzate. Se è necessario conservare tali chiavi (ad esempio, per supportare i dati cifrati in archivio), si deve applicare loro una protezione avanzata. L'applicazione di pagamento dovrebbe fornire o favorire un processo di sostituzione delle chiavi che devono essere sostituite o di cui si conosce o si sospetta la compromissione.
	2.5.5.b Sottoporre a test l'applicazione, compresi i metodi per il ritiro o la sostituzione delle chiavi di crittografia, per verificare che le istruzioni riportate nella *Guida per l'implementazione del programma PA-DSS* portino al ritiro o alla sostituzione delle chiavi (ad esempio, mediante archiviazione, distruzione e/o revoca, come applicabile).	
	2.5.5.c Sottoporre a test l'applicazione con le chiavi ritirate/sostituite per verificare che le istruzioni contenute nella *Guida per l'implementazione del programma PA-DSS* assicurino che l'applicazione non riutilizzi le chiavi ritirate o sostituite per le operazioni di cifratura.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
2.5.6 Se l'applicazione di pagamento supporta le operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro, tali operazioni devono applicare i principi di "split knowledge" e controllo duale. ***Nota:*** *esempi di operazioni manuali di gestione delle chiavi includono, senza limitazioni, la generazione, la trasmissione, il caricamento, la memorizzazione e la distruzione delle chiavi.*	**2.5.6.a.** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • dettagli relativi a qualsiasi operazione manuale di gestione delle chiavi di crittografia con testo in chiaro supportata dall'applicazione; • istruzioni per l'applicazione dei principi di "split knowledge" e controllo duale per tutte le operazioni.	La tecnica "split knowledge" e il controllo duale delle chiavi vengono utilizzati per eliminare la possibilità che una singola persona abbia accesso all'intera chiave. Questo controllo è applicabile alle operazioni manuali di gestione delle chiavi. "Split knowledge" è un metodo secondo cui due o più persone dispongono separatamente di componenti chiave che singolarmente non trasmettono alcuna conoscenza della chiave di crittografia originale; ogni persona conosce solo il proprio componente chiave e i singoli componenti chiave non trasmettono alcuna informazione sulla chiavi di crittografia originale. Il controllo duale richiede che due o più persone eseguano una funzione e che una persona sola non possa consultare o utilizzare i materiali di autenticazione di un'altra.
	2.5.6.b Sottoporre a test l'applicazione, comprese tutte le operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro, per verificare che le istruzioni contenute nella *Guida per l'implementazione del programma PA-DSS* portino a "split knowledge" e controllo duale delle chiavi come richiesto per tutte le procedure manuali di gestione delle chiavi con testo in chiaro.	
2.5.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia	**2.5.7.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* e verificare che comprenda le istruzioni per i clienti e i responsabili dell'integrazione/rivenditori su come prevenire la sostituzione non autorizzata delle chiavi di crittografia.	L'applicazione di pagamento dovrebbe definire metodi per i suoi utenti per garantire che vengano effettuate solo sostituzioni autorizzate delle chiavi. La configurazione dell'applicazione non dovrebbe consentire o accettare la sostituzione delle chiavi provenienti da fonti non autorizzate o processi imprevisti.
	2.5.7.b Sottoporre a test l'applicazione, compresi tutti i metodi utilizzati per la sostituzione delle chiavi, per verificare che le istruzioni contenute nella *Guida per l'implementazione del programma PA-DSS* impediscano la sostituzione non autorizzata delle chiavi di crittografia.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
2.6 Fornire un meccanismo per rendere impossibile il recupero del materiale di chiavi di crittografia o crittogrammi memorizzati dall'applicazione di pagamento, in conformità agli standard accettati dal settore. Queste sono le chiavi di crittografia utilizzate per cifrare o verificare i dati dei titolari di carta. ***Nota:*** *questo requisito è valido solo se l'applicazione di pagamento o versioni precedenti dell'applicazione di pagamento prevedono l'uso di materiali di chiavi di crittografia o crittogrammi per cifrare i dati dei titolari di carta.* ***In linea con il Requisito 3.6 PCI DSS***	**2.6.a** Rivedere la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti istruzioni per i clienti e i responsabili dell'integrazione/rivenditori: • procedure che spiegano in modo dettagliato come usare lo strumento o la procedura fornita con l'applicazione per rendere impossibile il recupero del materiale crittografico; • chiarimento della necessità di rendere irrecuperabile il materiale delle chiavi di crittografia ogni volta che le chiavi non vengono più utilizzate e in conformità ai requisiti di gestione delle chiavi illustrati nello standard PCI DSS; • procedure per la ricifratura dei dati cronologici con chiavi nuove, comprese le procedure per garantire la sicurezza dei dati con testo in chiaro durante il processo di decifratura/ricifratura.	I fornitori dovrebbero garantire un meccanismo che consenta ai clienti di eliminare in modo sicuro il vecchio materiale crittografico quando il cliente non ne ha più bisogno. L'eliminazione del vecchio materiale crittografico è a discrezione dei clienti. I materiali di chiavi di crittografia e/o i crittogrammi possono essere resi impossibili da recuperare facendo ricorso a strumenti o processi, inclusi, senza limitazioni: • eliminazione sicura, come definito, ad esempio, nell'elenco di prodotti approvati gestito dalla National Security Agency (NSA) o da qualsiasi altro Ente che gestisce standard o normative statale o nazionale; • cancellazione della chiave KEK (key-encrypting key) a condizione che le rimanenti chiavi di cifratura dei dati esistano solo in forma cifrata sotto la KEK cancellata.
	2.6.b Esaminare l'applicazione finale per verificare che il fornitore abbia predisposto uno strumento e/o una procedura con l'applicazione per rendere irrecuperabile il materiale crittografico.	
	2.6.c Sottoporre a test l'applicazione, compresi i metodi forniti per rendere irrecuperabile il materiale delle chiavi di crittografia. Verificare, mediante l'uso di strumenti e/o metodi forensi, che lo strumento o la procedura di pulizia sicura renda il materiale crittografico impossibile da recuperare, in conformità agli standard accettati dal settore.	
	2.6.d Sottoporre a test i metodi per la ricifratura dei dati cronologici con le chiavi nuove, per verificare che istruzioni contenute nella *Guida per l'implementazione del programma PA-DSS* portino a una corretta ricifratura dei dati cronologici con le chiavi nuove.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 3 - Fornire funzioni di autenticazione sicura

Requisiti PA-DSS	Procedure di test	Istruzioni
3.1 L'applicazione di pagamento deve supportare ed applicare l'uso di ID utente univoci e di autenticazione sicura per l'accesso amministrativo e l'accesso ai dati dei titolari di carta. L'autenticazione sicura deve essere applicata a tutti gli account, generati o gestiti dall'applicazione, al completamento dell'installazione e per le sue successive modifiche. L'applicazione deve applicare i requisiti da 3.1.1 a 3.1.11 riportati di seguito. ***Nota:*** *il termine "modifiche successive" utilizzato per tutto il Requisito 3 si riferisce a qualsiasi modifica all'applicazione che causa il ripristino delle impostazioni predefinite dell'account utente, a modifiche alle configurazioni account esistenti e a modifiche che generano account nuovi o ricreano quelli esistenti.* ***Nota:*** *questi controlli delle password non sono validi per il personale che accede a un solo numero di carta alla volta per facilitare una singola transazione. Tali controlli sono applicabili per l'accesso del personale con mansioni amministrative, per l'accesso a sistemi con dati dei titolari di carta e per l'accesso controllato dall'applicazione di pagamento.* *Questo requisito si applica all'applicazione di pagamento e a tutti gli strumenti associati utilizzati per visualizzare o accedere ai dati dei titolari di carta.* ***In linea con i Requisiti 8.1 e 8.2 PCI DSS***	**3.1.a** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che clienti e responsabili dell'integrazione/rivenditori: • abbiano ricevuto indicazioni chiare e inequivocabili su come l'applicazione di pagamento applichi un'autenticazione avanzata per tutte le credenziali di autenticazione che l'applicazione genera o gestisce: – applicando modifiche sicure alle credenziali di autenticazione al completamento dell'installazione (come da requisiti da 3.1.1 a 3.1.11); – applicando modifiche sicure per qualsiasi modifica successiva (all'installazione) alle credenziali di autenticazione (come da requisiti da 3.1.1 a 3.1.11); • sanno che, per garantire la conformità allo standard PCI DSS, qualsiasi modifica apportata alle configurazioni di autenticazione deve essere verificata per accertarsi che fornisca metodi di autenticazione che siano rigidi almeno quanto i requisiti PCI DSS; • abbiano ricevuto indicazioni su come assegnare metodi di autenticazione sicura agli account predefiniti nell'ambiente; • abbiano ricevuto indicazioni su come assegnare metodi di autenticazione sicura agli account predefiniti (anche se non verranno utilizzati) e disabilitare o non utilizzare gli account; • hanno ricevuto direttive chiare e inequivocabili per tutte le credenziali di autenticazione utilizzate dall'applicazione di pagamento (ma non generate o gestite dalla stessa), su come, al termine dell'installazione e per qualsiasi modifica successiva, modificare le credenziali di autenticazione e creare un'autenticazione avanzata in base ai Requisiti da 3.1.1 a 3.1.11 di seguito, per tutti gli account a livello di applicazione e utente con accesso amministrativo e per tutti gli account con accesso ai dati dei titolari di carta. • abbiano ricevuto indicazioni sull'identificazione tutti i ruoli e account predefiniti all'interno dell'applicazione con accesso amministrativo.	Garantendo l'identificazione univoca di ogni utente, invece di utilizzare un solo ID per diversi dipendenti, un'applicazione supporta i requisiti PCI DSS per garantire la responsabilità singola delle azioni e disporre di un effettivo audit trail per ogni dipendente. In questo modo i problemi vengono risolti più velocemente ed è possibile attuare un contenimento quando si rilevano abusi o cattive intenzioni. L'autenticazione sicura, se usata in aggiunta agli ID univoci, aiuta a proteggere gli ID degli utenti dalla compromissione, in quanto per un tentativo di compromissione è necessario conoscere sia l'ID univoco che la password (o l'altro elemento di autenticazione utilizzato).

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
3.1.1 L'applicazione non utilizza (o richiede di utilizzare) account amministrativi predefiniti per altro software necessario (ad esempio, l'applicazione di pagamento non deve utilizzare l'account amministrativo predefinito del database). ***In linea con il Requisito 2.1 PCI DSS***	**3.1.1** Installare e configurare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS*, compresa la configurazione degli account amministrativi per tutto il software necessario. Sottoporre a test l'applicazione di pagamento per verificare che non utilizzi (o richieda di utilizzare) account amministrativi predefiniti per il software necessario.	Gli account amministrativi predefiniti (e le password) sono di pubblico dominio, quindi noti a chiunque conosca l'applicazione di pagamento o i componenti di sistema sottostanti. Se si utilizzano gli account e le password amministrativi predefiniti, una persona non autorizzata potrebbe accedere all'applicazione e ai dati utilizzando semplicemente le credenziali di pubblico dominio.
3.1.2 L'applicazione deve imporre la modifica di tutte le sue password predefinite per tutti gli account generati o gestiti dall'applicazione stessa al completamento dell'installazione e per le modifiche successive all'installazione. Questa norma vale per tutti gli account, inclusi gli account utente, gli account di applicazione e servizio e gli account utilizzati dal fornitore per motivi di assistenza. ***Nota:*** *questo requisito non può essere soddisfatto specificando un processo utente o con le istruzioni contenute nella Guida per l'implementazione del programma PA-DSS. Al completamento dell'installazione e in caso di modifiche successive, l'applicazione deve impedire tecnicamente l'uso di qualsiasi account predefinito o integrato fino a che non si modifica la password predefinita.* ***In linea con il Requisito 2.1 PCI DSS***	**3.1.2** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test: **3.1.2.a** Installare l'applicazione in conformità alla *Guida per l'implementazione del programma PA-DSS*, esaminare le impostazioni di account e password e tentare di utilizzare tutte le password predefinite per verificare che l'applicazione attui le modifiche a qualsiasi password predefinita delle applicazioni di pagamento al completamente del processo di installazione. **3.1.2.b** Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni di account e password e tentare di utilizzare tutte le password predefinite per verificare che l'applicazione attui le modifiche a tutte le password predefinite al completamento della modifica.	Se l'applicazione non attua la modifica delle password predefinite, l'applicazione potrebbe essere esposta all'accesso non autorizzato di chiunque conosca le impostazioni predefinite.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
3.1.3 L'applicazione di pagamento assegna ID univoci per gli account utente. ***In linea con il Requisito 8.1.1 PCI DSS***	**3.1.3** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Quando ogni utente riceve un ID utente univoco, ogni accesso all'applicazione di pagamento e le attività svolte con essa possono associati alla persona che ne è responsabile.
	3.1.3.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* e tentare di creare diversi account dell'applicazione di pagamento con lo stesso ID utente per verificare che l'applicazione di pagamento assegni solo ID utenti univoci al completamento del processo di installazione.	
	3.1.3.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che ogni account riceva un ID utente univoco al completamento della modifica.	
3.1.4 L'applicazione di pagamento utilizza almeno uno dei seguenti metodi per autenticare tutti gli utenti: ▪ qualcosa che l'utente conosce, come una password o una passphrase; ▪ Qualcosa in possesso dell'utente, come un dispositivo token o una smart card ▪ qualcosa che l'utente è, come un elemento biometrico. ***In linea con i Requisiti 8.2 PCI DSS***	**3.1.4** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Questi metodi di autenticazione, se usati in aggiunta agli ID univoci, aiutano a proteggere gli ID univoci degli utenti dalla compromissione (in quanto per un tentativo di compromissione è necessario conoscere sia l'ID univoco che la password o l'altro metodo di autenticazione).
	3.1.4.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* e sottoporre a test i metodi di autenticazione per verificare che l'applicazione richieda almeno uno dei metodi di autenticazione definiti per tutti gli account al completamento del processo di installazione.	
	3.1.4.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, sottoporre a test i metodi di autenticazione per verificare che l'applicazione richieda almeno uno dei metodi di autenticazione definiti per tutti gli account, al completamento della modifica.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
3.1.5 L'applicazione di pagamento **non** richiede o usa alcun account o password di gruppo, condivisi o generici. ***In linea con il Requisito 8.5 PCI DSS***	**3.1.5** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Se più utenti condividono le medesime credenziali di autenticazione (ad esempio, account utente e password), diventa impossibile assegnare le responsabilità delle azioni o tenerne traccia in modo efficace, in quanto una determinata azione potrebbe essere stata eseguita da qualunque componente del gruppo a conoscenza delle credenziali di autenticazione.
	3.1.5.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS*, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che, al completamento del processo di installazione, l'applicazione non richieda o utilizzi account e password di gruppo, condivisi o generici.	
	3.1.5.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che l'applicazione non si avvalga di account e password di gruppo, condivisi o generici una volta completata la modifica.	
3.1.6 L'applicazione di pagamento richiede che le password rispondano ai seguenti criteri: • Lunghezza minima di almeno 7 caratteri • Presenza di caratteri numerici e alfabetici In alternativa, le password/passphrase devono presentare una complessità e solidità pari almeno ai parametri specificati sopra.	**3.1.6** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Gli utenti non autorizzati spesso tentano di trovare account con password deboli o non esistenti per accedere a un'applicazione o a un sistema. Se le password sono corte o facili da indovinare, è abbastanza semplice per un utente non autorizzato individuare account deboli e compromettere un'applicazione o un sistema utilizzando un ID utente valido. *(continua alla pagina successiva)*
	3.1.6.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni account per verificare che, al completamento dell'installazione, l'applicazione richieda un livello minimo di complessità e solidità indicate di seguito: • Lunghezza minima di almeno 7 caratteri • Presenza di caratteri numerici e alfabetici	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	3.1.6.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che, al completamento della modifica, l'applicazione richieda password in grado di soddisfare un livello minimo della complessità e solidità indicate di seguito: • Lunghezza minima di almeno 7 caratteri • Presenza di caratteri numerici e alfabetici	Questo requisito indica che la password deve contenere almeno sette caratteri e che deve essere composta sia da caratteri numerici che alfabetici. Nei casi in cui questi requisiti minimi non possono essere soddisfatti a causa di limiti tecnici, le entità possono utilizzare la "potenza equivalente" per valutare la propria alternativa. NIST SP 800-63-1 definisce "entropia" come "una misura della difficoltà di indovinare o determinare una password o una chiave". È possibile consultare questo e altri documenti che trattano di "entropia delle password" per ulteriori informazioni sul valore dell'entropia e sulla solidità password equivalente per le password con formati minimi diversi.
	3.1.6.c Se l'applicazione utilizza un set e una lunghezza minimi di caratteri per le password, calcolare l'entropia delle password richiesta dall'applicazione e verificare che sia quanto meno equivalente ai parametri specificati sopra (ossia che contenga almeno 7 caratteri sia numerici che alfabetici).	
3.1.7 L'applicazione di pagamento richiede modifiche alle password utente almeno ogni 90 giorni. ***In linea con il Requisito 8.2.4 PCI DSS***	**3.1.7** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Password/passphrase in uso da lungo tempo senza essere state modificate forniscono agli utenti non autorizzati più tempo per tentare di violarle.
	3.1.7.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni account per verificare che, al completamento del processo di installazione, l'applicazione richieda la modifica delle password utente almeno ogni 90 giorni.	
	3.1.7.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che, al completamento della modifica, l'applicazione richieda la modifica delle password utente almeno ogni 90 giorni.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
3.1.8 L'applicazione di pagamento mantiene la cronologia delle password e richiede che una nuova password sia diversa rispetto a ciascuna delle ultime quattro password utilizzate. ***In linea con il Requisito 8.2.5 PCI DSS***	**3.1.8** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Se non si conserva la cronologia password, si riduce l'efficacia della modifica della password, poiché le password precedenti possono essere riutilizzate in continuazione. La richiesta di non riutilizzare le password per un periodo di tempo riduce il rischio di adottare in futuro password individuate o violate.
	3.1.8.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni account per verificare che, al completamento del processo di installazione, l'applicazione conservi la cronologia delle password e richieda che una nuova password sia diversa dalle ultime quattro utilizzate.	
	3.1.8.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità account per verificare che, al completamento della modifica, l'applicazione conservi la cronologia delle password e richieda che una nuova password sia diversa dalle ultime quattro utilizzate.	
3.1.9 L'applicazione di pagamento limita i tentativi di accesso ripetuti bloccando l'account utente dopo un massimo di sei tentativi di accesso. ***In linea con il Requisito 8.1.6 PCI DSS***	**3.1.9** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Senza i meccanismi di blocco dell'account, un aggressore può tentare in modo continuo di indovinare una password mediante strumenti manuali o automatici (cracking delle password), fino ad avere successo e accedere all'account di un utente.
	3.1.9.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni account per verificare che, al completamento del processo di installazione, l'applicazione blocchi gli account utente dopo un massimo di sei tentativi di accesso non riusciti.	
	3.1.9.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che, al completamento della modifica, l'applicazione blocchi gli account utente dopo un massimo di sei tentativi di accesso non riusciti.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
3.1.10 L'applicazione di pagamento imposta la durata del blocco su un minimo di 30 minuti oppure fino a quando l'amministratore non abilita nuovamente l'ID utente. ***In linea con il Requisito 8.1.7 PCI DSS***	**3.1.10** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Se un account è bloccato a causa di un tentativo continuo di indovinare una password, i controlli per ritardare la riattivazione degli account bloccati impediscono all'utente non autorizzato di tentare continuamente di individuare una password (l'interruzione minima prima della riattivazione dell'account è di 30 minuti). Inoltre, se è necessario richiedere la riattivazione, l'amministratore può verificare che sia il proprietario dell'account a richiedere la riattivazione.
	3.1.10.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni account per verificare che, al completamento del processo di installazione, l'applicazione imposti la durata del blocco su un minimo di 30 minuti o fino a che l'amministratore non abilita l'ID utente.	
	3.1.10.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che, al completamento della modifica, l'applicazione imposti la durata del blocco su un minimo di 30 minuti o fino a che l'amministratore non abilità l'ID utente.	
3.1.11 Se una sessione dell'applicazione di pagamento è inattiva per più di 15 minuti, per riattivare la sessione, l'applicazione richiede di nuovo l'autenticazione all'utente. ***In linea con il Requisito 8.1.8 PCI DSS***	**3.1.11** Per tutti gli account generati o gestiti dall'applicazione, sottoporre l'applicazione al seguente test:	Quando gli utenti si allontanano da una sessione attiva con accesso all'applicazione di pagamento, la connessione può essere utilizzata da altri in loro assenza, dando luogo all'accesso non autorizzato all'account e/o all'abuso dell'account.
	3.1.11.a Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni account per verificare che, al completamento del processo di installazione, l'applicazione imposti un periodo di inattività della sessione non superiore ai 15 minuti.	
	3.1.11.b Sottoporre a test tutte le funzionalità dell'applicazione che portano al ripristino delle impostazioni predefinite degli account utente, a modifiche alle configurazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni account e testare la funzionalità dell'applicazione per verificare che, al completamento della modifica, l'applicazione imposti un tempo di inattività della sessione	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	non superiore ai 15 minuti.	
3.2 Il fornitore del software deve fornire ai clienti istruzioni relativamente al fatto che per ogni accesso a PC, server e database con applicazioni di pagamento è necessario un ID utente univoco e un'autenticazione sicura. ***In linea con i Requisiti 8.1 e 8.2 PCI DSS***	**3.2** Esaminare la *Guida per l'implementazione del programma PA-DSS* creata dal fornitore per verificare che contenga istruzioni per clienti e responsabili dell'integrazione/rivenditori relativa al controllo dell'accesso, mediante ID utente univoci e autenticazione sicura conforme allo standard PCI DSS, a qualsiasi PC, server e database con applicazioni di pagamento e dati dei titolari di carta.	Se l'applicazione è installa su, o viene aperta da, sistemi che non applicano controlli avanzati di identificazione e autenticazione, l'autenticazione avanzata fornita dall'applicazione potrebbe essere ignorata causando un accesso non sicuro.
3.3 proteggere le password di tutte le applicazioni di pagamento (comprese le password per gli account utente e applicazione) durante la trasmissione e l'archiviazione. ***In linea con il Requisito 8.2.1 PCI DSS***	**3.**3 Eseguire le seguenti operazioni:	Se le password dell'applicazione di pagamento vengono memorizzate o trasmesse sulla rete senza cifratura, un utente non autorizzato le può intercettare facilmente utilizzando uno "sniffer" oppure può accedere direttamente alle password nei file in cui sono memorizzate e utilizzare i dati sottratti per ottenere l'accesso non autorizzato. La concatenazione di una variabile di immissione esclusiva a ogni password prima di applicare l'algoritmo di hashing riduce l'efficacia degli attacchi violenti. Esempi di algoritmi di crittografia avanzata one-way adatti per le password hashing sono PBKDF2 e Bcrypt.
3.3.1 Utilizzare una crittografia avanzata per rendere tutte le password delle applicazioni di pagamento non leggibili durante la trasmissione.	**3.3.1.a** Esaminare la documentazione del fornitore e le configurazioni dell'applicazione per verificare che venga applicata una crittografia avanzata per rendere sempre tutte le password non leggibili durante la trasmissione.	
	3.3.1.b Per tutti i tipi di password delle applicazioni, esaminare le trasmissioni delle password (ad esempio, accedendo all'applicazione da un altro sistema e autenticando l'applicazione in altri sistemi) per verificare che venga applicata una crittografia avanzata per rendere sempre tutte le password non leggibili durante la trasmissione.	
3.3.2 Utilizzare un algoritmo di crittografia avanzata one-way in base agli standard approvati per rendere tutte le password dell'applicazione di pagamento non leggibili durante l'archiviazione. Ogni password deve disporre di una variabile di immissione esclusiva che viene concatenata alla password stessa prima che venga applicato	**3.3.2.a** Esaminare la documentazione del fornitore e le configurazioni dell'applicazione per verificare che**:** • le password memorizzate siano impossibili da leggere grazie all'uso di un algoritmo di crittografia avanzata basato su standard approvati; • una variabile di immissione esclusiva sia concatenata ad ogni password prima che venga applicato l'algoritmo di crittografia.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
l'algoritmo di crittografia. ***Nota:*** *non è necessario che la variabile di immissione sia imprevedibile o segreta.*	**3.3.2.b** Per tutti i tipi di password dell'applicazione, identificare tutte le posizioni in cui l'applicazione potrebbe memorizzare le password, tra cui all'interno dell'applicazione stessa, nei sistemi sottostanti, nei file di log, nelle impostazioni di registro, ecc. Per tutte le posizioni e i tipi di password, esaminare i file delle password memorizzate per verificare che tali password siano rese sempre illeggibili grazie a un algoritmo di crittografia avanzata one-way con una variabile di immissione esclusiva quando memorizzate.	
3.4 L'applicazione di pagamento deve limitare l'accesso a funzioni/risorse necessarie e applicare il privilegio più basso per gli account integrati: • per impostazione predefinita, tutti gli account di applicazioni/servizi hanno accesso solo alle funzioni/risorse specificatamente necessarie per rispondere allo scopo dell'account di applicazione/servizio; • per impostazione predefinita, tutti gli account di applicazione/servizio hanno un livello di privilegi minimo per ogni funzione/risorsa in base a quanto richiesto all'account di applicazione/servizio. ***In linea con il Requisito 7 PCI DSS***	**3.4.a** Installare l'applicazione di pagamento in conformità alla *Guida per l'implementazione del programma PA-DSS* ed esaminare le impostazioni relative agli account integrati per verificare che, al completamento del processo di installazione: • tutti gli account di applicazioni/servizi abbiano accesso solo alle funzioni/risorse specificatamente necessarie per rispondere allo scopo dell'account di applicazione/servizio; • tutti gli account di applicazione/servizio abbiano un livello di privilegio minimo per ogni funzione/risorsa in base a quanto richiesto all'account di applicazione/servizio.	Al fine di limitare l'accesso ai dati dei titolari di carta e alle funzioni sensibili solo a quegli account che necessitano di tale accesso, le esigenze di accesso e il livello di privilegio richiesto deve essere definito per ogni account integrato, in modo che l'account possa eseguire le funzioni assegnate ma che non gli venga concesso alcun accesso o privilegio aggiuntivo e superfluo. Assegnare il minor numero di privilegi possibile aiuta a prevenire che utenti con le giuste conoscenze sull'applicazione modifichino in modo errato o accidentale la configurazione dell'applicazione o alterino le sue impostazioni di sicurezza. L'applicazione del privilegio più limitato possibile contribuisce inoltre a ridurre al minimo la portata del danno nel caso in cui un utente non autorizzato riesca ad accedere a un ID utente.
	3.4.b Sottoporre a test tutte le funzionalità dell'applicazione che portano a modifiche agli account integrati, comprese quelle che causano il ripristino delle impostazioni predefinite degli account utente, a modifiche alle impostazioni account esistenti, alla generazione di nuovi account e alla ricreazione di account esistenti. Per tutti i tipi di modifica eseguiti, esaminare le impostazioni degli account integrati e testare la funzionalità dell'applicazione per verificare che, al completamento della modifica: • tutti gli account di applicazioni/servizi abbiano accesso solo alle funzioni/risorse specificatamente necessarie per rispondere allo scopo dell'account di applicazione/servizio; • tutti gli account di applicazione/servizio abbiano un livello di privilegio minimo per ogni funzione/risorsa in base a quanto richiesto all'account di applicazione/servizio.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 4 - Registrare l'attività dell'applicazione di pagamento

Requisiti PA-DSS	Procedure di test	Istruzioni
4.1 Al completamento del processo di installazione, l'installazione predefinita "pronta per l'uso" dell'applicazione di pagamento deve registrare ogni accesso degli utenti ed essere in grado di collegare tutte le attività ai singoli utenti. ***In linea con il Requisito 10.1 PCI DSS***	**4.1.a** Installare l'applicazione di pagamento. Sottoporre a test l'applicazione per verificare che gli audit trail dell'applicazione di pagamento vengano abilitati automaticamente al momento dell'installazione.	È importante che l'applicazione di pagamento disponga di un processo o un meccanismo che colleghi gli utenti alle risorse dell'applicazione consultate, generi i log di audit e fornisca la possibilità di ricondurre l'attività sospetta a un utente specifico. I team legali attivati dopo un incidente fanno affidamento su questi log per avviare le indagini.
	4.1.b Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che siano incluse le seguenti istruzioni: • come installare l'applicazione affinché i registri vengano configurati e abilitati per impostazione predefinita al completamento del processo di installazione; • come definire le impostazioni dei registri conformi a PCI DSS, in base ai Requisiti 4.2, 4.3 e 4.4 PA-DSS riportati di seguito, per qualsiasi opzione di registrazione che sia configurabile dal cliente dopo l'installazione; • la disattivazione dei registri non è consigliata in quanto può determinare una non conformità allo standard PCI DSS; • come configurare le impostazioni dei registri conformi a PCI DSS per qualsiasi componente software di terzi fornito con l'applicazione di pagamento o da essa richiesto, per qualsiasi opzione di registrazione che sia configurabile dal cliente dopo l'installazione.	
4.2 L'applicazione di pagamento deve fornire un audit trail automatico per ricostruire gli eventi seguenti: ***In linea con il Requisito 10.2 PCI DSS***	**4.2** Sottoporre a test l'applicazione di pagamento ed esaminare le impostazioni dei relativi log di audit e il risultato dei log di audit, quindi eseguire quanto segue:	La registrazione degli eventi illustrata in 4.2.1-4.2.7 consente a un'organizzazione di identificare e tenere traccia delle attività potenzialmente dannose.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
4.2.1 Tutti i singoli accessi utente ai dati dei titolari di carta dall'applicazione	**4.2.1** Verificare che siano registrati tutti i singoli accessi ai dati dei titolari di carta attraverso l'applicazione di pagamento.	Gli utenti non autorizzati potrebbero arrivare a conoscere un account utente con accesso ai dati dei titolari di carta attraverso l'applicazione oppure potrebbero creare un nuovo account non autorizzato per accedere ai dati dei titolari di carta. La registrazione di tutti gli accessi individuali ai dati dei titolari di carta può individuare quali account possono essere stati compromessi o usati in modo improprio.
4.2.2 Tutte le azioni intraprese da un utente con privilegi di amministratore come assegnati nell'applicazione	**4.2.2** Verificare che siano registrate tutte le azioni intraprese da un utente con privilegi di amministratore all'applicazione di pagamento.	Account con maggiori privilegi, come quello di "amministratore" o "root", hanno il potenziale di influire in modo significativo sulla sicurezza o sulla funzionalità operativa dell'applicazione. Senza un registro delle attività eseguite, un'organizzazione non è in grado di ricondurre ogni questione risultante da un errore amministrativo o dall'uso improprio di privilegi all'individuo o all'azione specifici.
4.2.3 Accesso agli audit trail gestiti dall'applicazione o all'interno della stessa	**4.2.3** Verificare che sia registrato l'accesso agli audit trail gestiti dall'applicazione o all'interno della stessa.	Gli utenti non autorizzati spesso cercano di modificare i log di audit per nascondere le loro azioni e con la registrazione degli accessi un'organizzazione può ricondurre eventuali incongruenze o potenziali manomissioni dei registri ad un singolo account.
4.2.4 Tentativi di accesso logico non validi	**4.2.4** Verificare che siano registrati i tentativi di accesso logico non riusciti.	Gli utenti non autorizzati sulla rete spesso eseguono più tentativi di accesso sui sistemi di destinazione. Vari tentativi di accesso non riusciti possono rappresentare un'indicazione dei tentativi di accesso di un utente non autorizzato facendo ricorso a "forza bruta" o cercando di indovinare una password.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
4.2.5 Uso e modifiche dei sistemi di identificazione e autenticazione dell'applicazione (compresi, a titolo esemplificativo, creazione di nuovi account, incremento dei privilegi, ecc.) e tutte le modifiche, le aggiunte e le eliminazioni agli account dell'applicazione con privilegi root o di amministratore	**4.2.5** Verificare che vengano registrati uso e modifiche dei sistemi di identificazione e autenticazione dell'applicazione di pagamento (compresi, senza limitazioni, creazione di nuovi account, incremento dei privilegi, ecc.) e tutte le modifiche, le aggiunte e le eliminazioni agli account dell'applicazione con privilegi root o di amministratore.	Se non è possibile sapere chi erano gli utenti presenti al momento in cui si è verificato un incidente, non è possibile identificare gli account utilizzati. Inoltre, gli utenti non autorizzati possono tentare di manipolare i controlli di autenticazione per cercare di superarli o di spacciarsi per un account valido. Le attività come, ad esempio, la creazione di nuovi account, l'incremento dei privilegi o le modifiche ai permessi di accesso possono segnalare l'uso non autorizzato dei meccanismi di autenticazione di un sistema.
4.2.6 Inizializzazione, blocco o sospensione dei log di audit dell'applicazione	**4.2.6** Verificare che vengano registrati i seguenti elementi: • Inizializzazione di log di audit dell'applicazione • Blocco o sospensione dei log di audit dell'applicazione	La disattivazione (o la sospensione) dei log di audit prima di eseguire delle attività illecite è una prassi comune degli utenti non autorizzati che non vogliono essere scoperti. L'inizializzazione dei log di audit potrebbe indicare che la funzione di registrazione è stata disattivata da un utente per nascondere le sue azioni.
4.2.7 Creazione ed eliminazione di oggetti a livello di sistema da parte dell'applicazione o all'interno della stessa	**4.2.7** Verificare che sia registrata la creazione e l'eliminazione di oggetti a livello di sistema da parte dell'applicazione o all'interno della stessa.	Gli utenti non autorizzati spesso creano o sostituiscono oggetti a livello di sistema sul sistema di destinazione per controllarne una determinata funzione o operazione. Grazie alla registrazione della creazione e dell'eliminazione degli oggetti a livello di sistema, come tabelle di database o procedure memorizzate, sarà più facile determinare se tali modifiche sono state autorizzate o meno.
4.3 L'applicazione di pagamento deve registrare almeno le seguenti voci di audit trail per ciascun evento: ***In linea con il Requisito 10.3 PCI DSS***	**4.3** Sottoporre a test l'applicazione di pagamento ed esaminare le impostazioni dei relativi log di audit e il risultato dei log di audit e, per ciascun evento registrabile (dal punto 4.2), eseguire quanto indicato di seguito:	Registrando queste voci in 4.3.1-4.3.6 per gli eventi registrabili nel punto 4.2, è possibile identificare rapidamente una potenziale compromissione e disporre di dettagli sufficienti per sapere chi, cosa, dove, come e

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
4.3.1 Identificazione utente	**4.3.1** Verificare che l'identificazione utente sia inclusa nelle voci di registro.	quando.
4.3.2 Tipo di evento	**4.3.2** Verificare che il tipo di evento sia incluso nelle voci di registro.	
4.3.3 Data e ora	**4.3.3** Verificare che l'indicazione di data e ora sia inclusa nelle voci di registro.	
4.3.4 Indicazione di successo o fallimento	**4.3.4**Verificare che l'indicazione di successo o fallimento sia inclusa nelle voci di registro.	
4.3.5 Origine dell'evento	**4.3.5**Verificare che l'origine dell'evento sia inclusa nelle voci di registro.	
4.3.6 Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa)	**4.3.6** Verificare che l'identità o il nome dei dati, del componente di sistema o delle risorse interessati siano inclusi nelle voci di registro.	
4.4. L'applicazione di pagamento deve facilitare la generazione centralizzata di registri. ***Nota:*** *esempi di questa funzionalità includono, senza limitazioni:* • generazione di registri mediante meccanismi di file di registro previsti dagli standard di settore come Common Log File System (CLFS), Syslog, testo delimitato, ecc.; • disponibilità di funzionalità e documentazione per convertire il formato di registro proprietario dell'applicazione in formati di registro previsti dagli standard di settore adatti ad una generazione di registri centralizzata ed immediata. ***In linea con il Requisito 10.5.3 PCI DSS***	**4.4** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che fornisca a clienti e responsabili dell'integrazione/rivenditori: • una descrizione dei meccanismi di registrazione centralizzati supportati; • istruzioni e procedure per l'inserimento dei registri dell'applicazione di pagamento nel server per la generazione centralizzata dei registri. **4.4.b** Installare e configurare l'applicazione di pagamento in base alla *Guida per l'implementazione del programma PA-DSS* per verificare che le istruzioni siano accurate e che venga fornita una funzionalità in grado di semplificare la capacità del cliente di assimilare i log nel proprio server log centralizzato.	Senza un'adeguata protezione dei log di audit non è possibile garantirne la completezza, la precisione e l'integrità; inoltre, i log di audit possono rivelarsi uno strumento di indagine inutile dopo una compromissione. Includere i registri dell'applicazione di pagamento in un sistema di registrazione centralizzato consente al cliente di integrare e relazionare tra loro i registri, oltre a proteggere i registri in modo omogeneo all'interno del proprio ambiente.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 5 - Sviluppare applicazioni di pagamento sicure

Requisiti PA-DSS	Procedure di test	Istruzioni
5.1 Il fornitore del software ha definito e implementato una procedura formale per proteggere lo sviluppo delle applicazioni di pagamento, che comprende i seguenti aspetti: • le applicazioni di pagamento vengono sviluppate in conformità agli standard PCI DSS e PA-DSS (ad esempio, autenticazione e registrazione sicure); • i processi di sviluppo si fondano su standard di settore e/o migliori pratiche; • la sicurezza delle informazioni è compresa per l'intera durata del ciclo di sviluppo del software; • le revisioni alla sicurezza vengono svolte prima di pubblicare un'applicazione o un aggiornamento all'applicazione. ***In linea con il Requisito 6.3 PCI DSS***	**5.1.a** Esaminare i processi di sviluppo del software documentati e verificare che si basino sugli standard e/o sulle migliori pratiche di settore.	Senza l'inclusione della sicurezza durante le fasi di definizione dei requisiti, progettazione, analisi e test del processo di sviluppo del software, le vulnerabilità di protezione possono essere introdotte inavvertitamente o con cattive intenzioni nel codice dell'applicazione.
	5.1.b Verificare che i processi di sviluppo del software documentati includano procedure per quanto segue: • integrazione della sicurezza delle informazioni per l'intera durata del ciclo di sviluppo del software; • sviluppo delle applicazioni di pagamento in conformità ai requisiti PCI DSS e PA-DSS.	
	5.1.c Verificare che i processi di sviluppo software includano: • revisioni alla sicurezza definite prima della release di un'applicazione o di un aggiornamento all'applicazione; • procedure per le revisioni alla sicurezza da eseguire per garantire che gli obiettivi in termini di sicurezza degli standard PCI DSS e PA-DSS siano rispettati.	
	5.1.d Consultare gli sviluppatori software per confermare che vengano seguiti processi documentati come: • la sicurezza delle informazioni è compresa per l'intera durata del ciclo di sviluppo del software; • le applicazioni di pagamento vengono sviluppate in base ai Requisiti PCI DSS e PA-DSS; • le revisioni alla sicurezza vengono eseguite prima della release per assicurarsi che gli obiettivi di sicurezza, compresi i requisiti PCI DSS e PA-DSS, vengano rispettati.	
5.1.1 Non utilizzare PAN attivi per le attività di test o sviluppo. ***In linea con il Requisito 6.4.3 PCI DSS***	**5.1.1.a** Rivedere i processi di sviluppo software per verificare che includano procedure volte a garantire che non si utilizzino PAN attivi per il test e lo sviluppo.	I marchi di carte di pagamento e molti acquirenti sono in grado di fornire numeri di conto adatti per i test qualora siano necessari PAN realistici per sottoporre a test la funzionalità dell'applicazione prima della release.
	5.1.1.b Osservare i processi di test e consultare il personale per verificare che non vengano utilizzati PAN attivi per le attività di test o sviluppo.	
	5.1.1.c Esaminare campioni di dati dei test per verificare che non vengano utilizzati PAN attivi per le attività di test o sviluppo.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.1.2 I dati e gli account di test vengono rimossi prima della release al cliente. ***In linea con il Requisito 6.4.4 PCI DSS***	**5.1.2.a** Rivedere i processi di sviluppo software per verificare che comprendano procedure per garantire che i dati e gli account di test siano rimossi prima della release dell'applicazione di pagamento ai clienti.	I dati e gli account di test devono essere rimossi dall'applicazione prima della release ai clienti, poiché l'inclusione di questi elementi può fornire informazioni sulla costruzione delle chiavi all'interno dell'applicazione.
	5.1.2.b Osservare i processi di test e consultare il personale per verificare che i dati e gli account di test vengano rimossi prima della release al cliente.	
	5.1.2.c Esaminare l'applicazione di pagamento finale per verificare che i dati e gli account di test vengano rimossi prima della release al cliente.	
5.1.3 Account, ID utente e password di applicazioni di pagamento personalizzate vengono rimossi prima della release delle applicazioni ai clienti. ***In linea con il Requisito 6.3.1 PCI DSS***	**5.1.3.a** Rivedere i processi di sviluppo software per verificare che includano le procedure per garantire che account, ID utente e password di applicazioni di pagamento personalizzate vengono rimossi prima della release delle applicazioni ai clienti.	Account, ID utente e password personalizzati precedenti alla release possono essere sfruttati come "back door" per sviluppatori e altri individui a conoscenza di tali account per accedere all'applicazione e potrebbero facilitare la compromissione dell'applicazione e i dati dei titolari di carta correlati.
	5.1.3b Osservare i processi di test e consultare il personale per verificare che account, ID utente e password di applicazioni di pagamento personalizzate vengono rimossi prima della release delle applicazioni ai clienti.	
	5.1.3c Esaminare l'applicazione di pagamento finale per verificare che account, ID utente e password di applicazioni di pagamento personalizzate vengono rimossi prima della release delle applicazioni ai clienti.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.1.4 Il codice dell'applicazione di pagamento viene rivisto prima della release ai clienti dopo eventuali modifiche significative, per identificare potenziali vulnerabilità di codifica (attraverso processi manuali o automatici) includendo almeno quanto segue: • le modifiche del codice vengono analizzate da utenti singoli diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure; • le analisi del codice garantiscono che il codice venga sviluppato in base a linee guida di codifica sicure (vedere Requisito 5.2. PA-DSS); • le correzioni appropriate vengono implementate prima della release; • i risultati dell'analisi del codice vengono esaminati e approvati dalla direzione prima della release; • risultati documentati dell'analisi del codice includono approvazione della direzione, autore e revisore del codice e quali correzioni sono state implementate prima della release. ***Nota:*** *questo requisito per le analisi del codice si applica a tutti i componenti delle applicazioni di pagamento (applicazioni Web interne ed esterne), come parte della durata del ciclo di sviluppo del sistema. Le analisi del codice possono essere condotte da personale interno preparato o da terze parti.* ***In linea con il Requisito 6.3.2 PCI DSS***	**5.1.4.a** Esaminare le procedure di sviluppo software scritte e consultare il personale per verificare che il fornitore esegua le analisi del codice per tutte le modifiche significative al codice dell'applicazione (attraverso processi manuali o automatici) come indicato di seguito: • le modifiche del codice vengono analizzate da utenti singoli diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure; • le analisi del codice garantiscono che il codice venga sviluppato in base a linee guida di codifica sicure (vedere Requisito 5.2. PA-DSS); • le correzioni appropriate vengono implementate prima della release; • i risultati dell'analisi del codice vengono esaminati e approvati dalla direzione prima della release; • i risultati dell'analisi del codice vengono documentati in modo da includere approvazione della direzione, autore e revisore del codice e quali correzioni sono state implementate prima della release. **5.1.4.b** Esaminare i risultati dell'analisi di codice alla ricerca di un campione di modifiche al codice per verificare che: • le analisi del codice siano state eseguite da una persona esperta diversa dall'autore; • le analisi del codice garantiscano che il codice venga sviluppato in base a linee guida di codifica sicure; • le correzioni appropriate vengano implementate prima della release; • i risultati dell'analisi del codice vengano esaminati e approvati dalla direzione prima della release.	Le vulnerabilità di protezione nel codice dell'applicazione vengono comunemente sfruttate da utenti non autorizzati per accedere a una rete e compromettere i dati dei titolari di carta. Al fine di tutelare contro questi tipi di attacchi, è necessario utilizzare tecniche di analisi del codice adeguate. Si dovrebbero adottare tecniche di analisi del codice per verificare che siano state applicate le migliori pratiche per una codifica sicura durante tutto il processo di sviluppo. Il fornitore dell'applicazione dovrebbe incorporare pratiche di codifica sicura rilevanti in base alle tecnologie particolari utilizzate. Le analisi dovrebbero essere eseguite da un utente esperto della tecnologia e delle tecniche di analisi del codice al fine di identificare i potenziali problemi di codifica. Assegnare le analisi del codice a una persona diversa dallo sviluppatore del codice consente di ottenere un'analisi indipendente e oggettiva. La correzione degli errori di codifica prima della release del codice impedisce che del codice errato esponga gli ambienti dei clienti a un potenziale sfruttamento. Il codice errato è più difficile e costoso da risolvere dopo essere stato implementato. L'analisi e l'approvazione formali da parte della direzione prima della release consentono di garantire che il codice è approvato ed è stato sviluppato in conformità alle politiche e alle procedure.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.1.5 Pratiche di controllo sorgente sicure vengono implementate per verificare l'integrità del codice sorgente durante il processo di sviluppo.	**5.1.5.a** Esaminare le procedure di sviluppo software scritte e consultare il personale responsabile per verificare che il fornitore mantenga pratiche di controllo sorgente sicure per verificare l'integrità del codice sorgente durante il processo di sviluppo.	Buone pratiche di controllo del codice sorgente consentono di garantire che tutte le modifiche al codice siano intenzionali e autorizzate, nonché eseguite solo da utenti con una motivazione legittima a modificare il codice. Esempi d queste pratiche includono procedure di archiviazione ed estrazione del codice con controlli di accesso rigidi, oltre a un confronto da eseguire immediatamente prima dell'aggiornamento del codice per confermare che l'ultima versione approvata non sia stata modificata (ad esempio, utilizzando un checksum).
	5.1.5.b Esaminare i meccanismo e osservare le procedure per la protezione del codice sorgente per verificare che la sua integrità sia mantenuta per tutto il processo di sviluppo.	
5.1.6 Le applicazioni di pagamento vengono sviluppate in base alle migliori pratiche di settore per le tecniche di codifica sicure, tra cui: • sviluppo con il privilegio più basso possibile per l'ambiente dell'applicazione; • sviluppo con opzioni predefinite in modalità provvisoria (ogni esecuzione è negata per impostazione predefinita a meno che non sia specificato nella progettazione iniziale); • sviluppo di tutti gli aspetti analizzati per i punti di accesso, comprese le variazioni di input come l'input multicanale	**5.1.6.a** Esaminare i processi di sviluppo software per verificare che siano state definite le tecniche di codifica sicure e che queste includano: • sviluppo con il privilegio più basso possibile per l'ambiente dell'applicazione; • sviluppo con opzione predefinita in modalità provvisoria (ogni esecuzione è negata per impostazione predefinita a meno che non sia specificato nella progettazione iniziale); • sviluppo di tutti gli aspetti analizzati per i punti di accesso, comprese le variazioni di input come l'input multicanale nell'applicazione.	Lo sviluppo delle applicazioni con il privilegio più basso è il modo più efficace per accertarsi che nessun presupposto non sicuro venga introdotto nell'applicazione. L'introduzione di opzioni predefinite in modalità provvisoria impedisce agli aggressori di ottenere informazioni sensibili su un errore dell'applicazione che potrebbero poi essere utilizzate per creare attacchi successivi. Assicurare che la sicurezza sia applicata a tutti gli accessi e ingressi all'applicazione evita il rischio di lasciare

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
nell'applicazione.	**5.1.6.b** Consultare gli sviluppatori per verificare che le applicazioni vengano sviluppate in base alle migliori pratiche di settore per le tecniche di codifica sicure, tra cui: • sviluppo con il privilegio più basso possibile per l'ambiente dell'applicazione; • sviluppo con opzioni predefinite in modalità provvisoria (ogni esecuzione è negata per impostazione predefinita a meno che non sia specificato nella progettazione iniziale); • sviluppo di tutti gli aspetti analizzati per i punti di accesso, comprese le variazioni di input come l'input multicanale nell'applicazione.	un canale di ingresso aperto a possibili compromissioni. Se non si prendono in considerazione questi aspetti durante lo sviluppo del codice, si rischia di distribuire un'applicazione non sicura e di incorrere in una correzione potenzialmente eccessiva in seguito.
5.1.6.1 Le tecniche di codifica comprendono la documentazione relativa a come PAN e/o SAD vengono gestiti in memoria.	**5.1.6.1.a** Esaminare le tecniche di codifica per verificare che includano la documentazione di come PAN e/o SAD vengano gestiti in memoria.	Gli aggressori utilizzano strumenti malware per acquisire informazioni sensibili dalla memoria. La riduzione dell'esposizione di PAN/dati sensibili di autenticazione in memoria aiuta a ridurre la probabilità che tali dati vengano acquisiti da un utente non autorizzato o che vengano inconsapevolmente salvati nel disco in un file di memoria e lasciati senza protezione. Questo requisito è inteso per garantire che si adottino le giuste misure per la gestione di PAN e dati sensibili di autenticazione in memoria. Comprendere quando e per quanto tempo i dati sensibili restano in memoria, oltre al relativo formato, aiuta i fornitori di applicazioni a identificare le potenziali insicurezze nelle proprie applicazioni e a determinare se sono necessarie protezioni aggiuntive. Se le tecniche di codifica derivino o meno da questa attività dipende dal software particolare che viene sviluppato e dalle tecniche in uso.
	5.1.6.1.b Consultare gli sviluppatori per verificare che prendano in considerazione la modalità di gestione di PAN/dati sensibili di autenticazione durante il processo di sviluppo delle applicazioni.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.1.7 Fornire la formazione aggiornata nelle pratiche di sviluppo sicuro per gli sviluppatori di applicazioni, come richiesto in base alla mansione dello sviluppatore e alla tecnologia utilizzata, ad esempio: • Strutturazione applicazione sicura • Tecniche di codifica sicure per evitare vulnerabilità di codifica comuni (come linee guida del fornitore, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, ecc.) • Gestione dati sensibili in memoria • Analisi del codice • Test di sicurezza (ad esempio, tecniche per test di penetrazione) • Tecniche di valutazione dei rischi ***Nota:*** *la formazione per gli sviluppatori di applicazioni può essere fornita dall'azienda o da terzi. Esempi di come la formazione può essere fornita presso la sede dell'azienda, da un istruttore e basata su computer.*	**5.1.7a** Verificare che i processi di sviluppo software documentati richiedano la formazione aggiornata nelle pratiche di sviluppo sicuro per gli sviluppatori di applicazione almeno una volta l'anno, come richiesto in base alla mansione dello sviluppatore e alla tecnologia utilizzata.	Garantire che gli sviluppatori conoscano le pratiche di sviluppo sicuro contribuisce a ridurre al minimo il numero di vulnerabilità alla sicurezza introdotte attraverso pratiche di codifica scarse. Il personale qualificato ha inoltre maggiori competenze per identificare i potenziali problemi alla sicurezza nella progettazione e nella codifica delle applicazioni. Le piattaforme e le metodologie di sviluppo software cambiano frequentemente, come anche le minacce e i rischi alle applicazioni software. La formazione nelle pratiche di sviluppo sicuro dovrebbe essere sempre aggiornata e al passo con le mutevoli pratiche di sviluppo.
	5.1.7.b Consultare alcuni sviluppatori per verificare che conoscano le pratiche di sviluppo sicuro e le tecniche di codifica, applicabili in base alla tecnologia utilizzata.	
	5.1.7.c Esaminare i record della formazione per verificare che tutti gli sviluppatori di applicazioni ricevano la formazione almeno una volta l'anno, come richiesto in base alla propria mansione e alla tecnologia utilizzata.	
5.1.7.1 Aggiornare la formazione come necessario per rispondere alle nuove tecnologie e metodologie di sviluppo utilizzate.	**5.1.7.1** Esaminare i materiali della formazione e consultare alcuni sviluppatori per verificare che la formazione sia aggiornata come richiesto per rispondere alle nuove tecnologie e metodologie utilizzate.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.2 Sviluppare tutte le applicazioni di pagamento per prevenire le vulnerabilità di codifica comuni nei processi di sviluppo software. ***Nota:*** *le vulnerabilità elencate dai Requisiti da 5.2.1 a 5.2.10 PA-DSS e da 6.5.1 a 6.5.10 PCI DSS erano presenti nelle migliori pratiche di settore al momento della pubblicazione della presente versione dello standard PA DSS. Tuttavia, poiché le migliori pratiche di settore per la gestione delle vulnerabilità sono state aggiornate (ad esempio, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, ecc.), per questi requisiti è necessario utilizzare le migliori pratiche più recenti.* ***In linea con il Requisito 6.5 PCI DSS***	**5.2.** Verificare che le applicazioni di pagamento non siano esposte a vulnerabilità di codifica comuni eseguendo un test di penetrazione manuale o automatico che tenta di sfruttare in modo specifico ciascuna delle seguenti vulnerabilità:	Lo strato applicazione è ad alto rischio e può divenire bersaglio di minacce interne ed esterne. Senza la corretta protezione, i dati dei titolari di carta e altre informazioni riservate dell'azienda possono essere esposte. I Requisiti da 5.2.1 a 5.2.10 rappresentano i controlli minimi da adottare. Questo elenco si compone delle vulnerabilità di codifica comuni al momento della pubblicazione di questa versione dello standard PA-DSS. Poiché le vulnerabilità di codifica comuni sono in continuo cambiamento, le pratiche di codifica del fornitore dovrebbero essere aggiornate di conseguenza.
Nota: *i requisiti da 5.2.1 a 5.2.6, riportati di seguito, si riferiscono a tutte le applicazioni di pagamento (interne o esterne).*		
5.2.1 Injection flaw, in particolare SQL injection. Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.	**5.2.1** Gli injection flaw, in particolare SQL injection, vengono risolti da tecniche di codifica che includono: • convalida dell'input per verificare che i dati dell'utente non possano modificare il significato di comandi e query; • utilizzo di query con parametri.	Injection flaw, in particolare SQL injection, rappresentano il metodo comunemente usato per compromettere le applicazioni. L'injection avviene quando i dati forniti dall'utente vengono inviati a un interprete durante un comando o una query. I dati ostili dell'aggressore inducono l'interprete a eseguire comandi indesiderati o a modificare i dati, esponendo quindi i componenti all'interno dell'applicazione ad attacchi di tipo buffer overflow. Tutti i dati di input devono essere convalidati dall'applicazione prima di essere elaborati, ad esempio controllando tutti i caratteri alfabetici, un insieme di caratteri alfabetici e numerici, ecc.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.2.2 Buffer overflow	**5.2.2** I buffer overflow vengono risolti da tecniche di codifica come: • Convalida dei limiti del buffer • Troncatura delle stringhe di input	I buffer overflow si verificano quando un'applicazione non dispone degli adeguati controlli di limite sul suo spazio buffer. Ciò può causare che le informazioni nel buffer vengano spinte fuori dallo spazio di memoria del buffer e collocate nello spazio di memoria eseguibile. Quando ciò si verifica, l'aggressore è in grado di inserire un codice dannoso alla fine del buffer e quindi spingere tale codice nello spazio di memoria eseguibile causando un buffer overflow. Questo codice dannoso viene quindi eseguito e spesso consente all'aggressore di accedere in remoto all'applicazione e/o al sistema infetto.
5.2.3 Memorizzazione di dati crittografici non sicura	**5.2.3** La memorizzazione di dati crittografici non sicura viene risolta da tecniche di codifica che: • evitano gli errori di crittografia; • utilizzano algoritmi e chiavi di crittografia avanzata.	Le applicazioni che non usano funzioni di crittografia avanzata in modo corretto per la memorizzazione dei dati sono esposte ad un maggiore rischio di essere compromesse e di esporre l credenziali di autenticazione e/o i dati dei titolari di carta.
5.2.4 Comunicazioni non sicure	**5.2.4** Le comunicazioni non sicure vengono risolte dalle tecniche di codifica che autenticano e cifrano tutte le comunicazioni sensibili.	Le applicazioni che non riescono a cifrare in modo appropriato il traffico di rete sensibile usando la crittografia avanzata sono esposte ad un rischio maggiore di compromissione e di esposizione dei dati dei titolari di carta.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.2.5 Gestione degli errori non corretta	**5.2.5** La gestione errata degli errori viene risolta con tecniche di codifica che non perdono informazioni mediante messaggi di errore (ad esempio, generando messaggi d'errore generici anziché specifici).	Le applicazioni che perdono informazioni sulla relativa configurazione e sulle procedure interne o espongono le informazioni con privilegi tramite metodi di errata gestione degli errori sono a rischio di compromissione. Gli aggressori utilizzano questi punti deboli per sottrarre dati sensibili o compromettere il sistema. Se un utente non autorizzato può creare errori che l'applicazione non è in grado di gestire correttamente, può ottenere informazioni dettagliate sul sistema, creare interruzioni denial-of-service, provocare il fallimento della protezione o causare l'arresto anomalo dell'applicazione o del server. Ad esempio, il messaggio "password non corretta" comunica che l'ID utente fornito è corretto e che l'attenzione deve essere concentrata solamente sulla password. Utilizzare messaggi d'errore più generici, come "Impossibile verificare i dati".
5.2.6 Tutte le vulnerabilità di livello elevato vengono individuate nel processo di identificazione delle vulnerabilità di cui al Requisito 7.1 PA-DSS	**5.2.6** Le tecniche di codifica risolvono eventuali vulnerabilità di livello elevato che possono incidere sull'applicazione, come identificato nel Requisito 7.1 PA-DSS.	Durante lo sviluppo dell'applicazione è necessario identificare e risolvere tutte le vulnerabilità che mediante il processo di classificazione dei rischi delle vulnerabilità del fornitore (definito nel Requisito 7.1 PA-DSS) risultano essere ad "alto rischio" e potrebbero incidere sull'applicazione.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
Nota: *i requisiti da 5.2.7 a 5.2.10, riportati di seguito, si riferiscono ad applicazioni basate su Web e interfacce di applicazioni (interne o esterne):*		Applicazioni Web presentano dei rischi di sicurezza univoci sulla base della loro architettura nonché della loro relativa facilità e del verificarsi di compromissioni.
5.2.7 Cross-site scripting (XSS)	**5.2.7** Il cross-site scripting (XSS) viene risolto da tecniche di codifica che prevedono: • convalida di tutti i parametri prima dell'inclusione; • utilizzo di escape sensibile al contesto.	Le falle XSS si verificano quando un'applicazione prende i dati forniti dall'utente e li invia a un browser Web senza prima convalidarli o codificarne il contenuto. XSS consente agli aggressori di eseguire script sul browser della vittima, che può dirottare le sessioni utente, alterare i siti Web, introdurre worm, ecc.
5.2.8 Controllo di accesso non corretto, come riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL e scansione trasversale directory	**5.2.8** Controllo di accesso non corretto, come riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL e scansione trasversale directory sono risolti da tecniche di codifica che includono: • corretta autenticazione degli utenti; • purificazione degli input; • mancata esposizione di riferimenti a oggetti interni agli utenti; • interfacce utente che non consentono l'accesso alle funzioni non autorizzate.	Un riferimento a oggetto diretto si verifica quando uno sviluppatore espone un riferimento a un oggetto di implementazione interno, come un file, una directory, un record di database o una chiave, sotto forma di parametro URL o di modulo. Gli aggressori possono manipolare questi riferimenti per accedere ad altri oggetti senza autorizzazione. Un aggressore può essere in grado di elencare e navigare la struttura della directory (scansione trasversale directory) di un sito Web e quindi ottenere accesso a informazioni non autorizzate ed anche acquisire un'ulteriore comprensione approfondita delle procedure interne del sito per un successivo sfruttamento. Le interfacce utente che consentono l'accesso a funzioni non autorizzate potrebbero determinare l'accesso da parte di utenti non autorizzati a credenziali con privilegi o dati dei titolari di carta. La limitazione dell'accesso alle risorse di dati consente di impedire che i dati dei titolari di carta vengano presentati a risorse non autorizzate.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.2.9 Cross-site request forgery (CSRF)	**5.2.9** Il cross-site request forgery (CSRF) è stato risolto con tecniche di codifica che garantiscono che le applicazioni non facciano affidamento su credenziali e token di autorizzazione inviati automaticamente dai browser.	Un attacco CSRF impone al browser di una vittima connessa di inviare una richiesta pre-autenticata a un'applicazione Web vulnerabile che permette all'aggressore di eseguire tutte le operazioni di modifica di stato che la vittima è autorizzata ad eseguire, quali l'aggiornamento dei dettagli dell'account, acquisti o l'autenticazione su un'applicazione.
5.2.10 Violazione dell'autenticazione e gestione delle sessioni	**5.2.10** La violazione dell'autenticazione e la gestione delle sessioni viene risolta con tecniche di codifica che in genere prevedono: • contrassegnare i token delle sessioni (ad esempio, i cookie) come "sicuri"; • non esporre gli ID sessione nell'URL; • incorporare timeout appropriati e rotazione di ID sessione dopo l'accesso.	L'autenticazione sicura e la gestione delle sessioni impediscono agli utenti non autorizzati di compromettere credenziali degli account, chiavi o token di sessione che altrimenti consentirebbero loro di impossessarsi dell'identità degli utenti autorizzati.
5.3 Il fornitore del software deve seguire le procedure di controllo delle modifiche per tutte le modifiche apportate all'applicazione. Le procedure di controllo delle modifiche devono seguire gli stessi processi di sviluppo software delle release nuove (come definito nel Requisiti 5.1 PA-DSS) e comprendono quanto segue: ***In linea con il Requisito 6.4.5 PCI DSS***	**5.3.a** Esaminare le procedure di controllo delle modifiche del fornitore per le modifiche software e: • verificare che le procedure seguano i processi di sviluppo software documentati come specificato nel Requisito 5.1; • verificare che le procedure richiedano gli elementi 5.3.1-5.3.4 di seguito.	Se non adeguatamente gestito, l'impatto degli aggiornamenti software e delle patch di sicurezza potrebbe non essere pienamente realizzato e potrebbe avere conseguenze non previste.
	5.3.b Consultare gli sviluppatori per determinare le modifiche all'applicazione di pagamento recenti. Esaminare le recenti modifiche dell'applicazione di pagamento e farle risalire alla documentazione di controllo delle modifiche correlata. Per ogni modifica esaminata, verificare che ogni aspetto indicato di seguito sia stato documentato in conformità alle procedure di controllo delle modifiche:	
5.3.1 Documentazione dell'impatto	**5.3.1** Verificare che la documentazione dell'impatto sul cliente sia inclusa nella documentazione di controllo delle modifiche per ciascuna modifica.	L'impatto della modifica dovrebbe essere documentato in modo che tutte le parti interessate siano in grado di pianificare accuratamente qualsiasi modifica di elaborazione.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.3.2 Approvazione documentata della modifica delle parti autorizzate competenti	**5.3.2** Verificare la presenza dell'approvazione documentata delle parti autorizzate competenti per ogni modifica.	L'approvazione delle parti autorizzate indica che una modifica è legittima e autorizzata dalla direzione.
5.3.3 Esecuzione del test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema.	**5.3.3.a** Verificare che sia stato eseguito il test della funzionalità per controllare che la modifica non influisca negativamente sulla sicurezza del sistema. **5.3.3.b** Verificare che tutte le modifiche (inclusi i patch) siano sottoposte a test per la conformità al punto 5.2 prima della loro release.	Un test approfondito consente di verificare che l'introduzione della modifica non comporti una riduzione della sicurezza dell'applicazione di pagamento. I test dovrebbero convalidare che, dopo ogni modifica apportata all'applicazione, tutti i controlli di sicurezza esistenti rimangano attivi, siano sostituiti con controlli ugualmente efficaci oppure siano intensificati.
5.3.4 Procedure di backout o disinstallazione del prodotto	**5.3.4** Verificare che vengano preparate procedure di backout o disinstallazione del prodotto per ogni modifica.	Per ogni modifica devono esistere procedure di back-out nel caso in cui la modifica non riesca o influisca negativamente sulla sicurezza dell'applicazione, in modo da consentire il ripristino dell'applicazione allo stato precedente.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.4 Il fornitore di applicazioni di pagamento deve documentare e seguire la metodologia di versioning del software all'interno del ciclo di vita di sviluppo del sistema. La metodologia deve rispettare le procedure riportate nella *Guida del programma PA-DSS* per le modifiche alle applicazioni di pagamento e includere almeno quanto segue:	**5.4** Esaminare i processi di sviluppo software documentati per verificare che includano la metodologia di versioning del fornitore del software e che la metodologia di versioning sia conforme alla Guida del programma PA-DSS. Verificare che sia richiesto di attenersi alla metodologia di versioning documentata per l'applicazione di pagamento, comprese tutte le modifiche all'applicazione di pagamento.	Senza una metodologia di versioning definita con attenzione, le modifiche alle applicazioni potrebbero non essere identificate correttamente e clienti e responsabili dell'integrazione/rivenditori potrebbero non comprendere l'impatto di una modifica a una versione dell'applicazione.
5.4.1 La metodologia di versioning deve definire gli elementi di versione specifici utilizzati, come indicato di seguito: • dettagli di come gli elementi dello schema di versione sono in conformità ai requisiti specifici indicati nella *Guida del programma PA-DSS*; • formato dello schema di versione, compresi numero di elementi, separatori, set di caratteri, ecc. (composti da caratteri alfabetici, numerici e/o alfanumerici); • definizione di cosa rappresenta ogni elemento nello schema di versione (ad esempio, tipo di modifica, release maggiore, minore o di manutenzione, carattere jolly, ecc.); • una definizione degli elementi che indicano l'uso dei caratteri jolly. ***Nota:*** *i caratteri jolly possono essere sostituiti solo per elementi del numero di versione che rappresentano modifiche senza effetti sulla sicurezza. Consultare il Requisito 5.4.3 per ulteriori requisiti sull'uso dei caratteri jolly.*	**5.4.1.a** Esaminare la metodologia di versioning documentata per verificare che includa quanto segue: • i dettagli di come gli elementi dello schema di numerazione della versione sono in conformità ai requisiti specifici indicati nella *Guida del programma PA-DSS;* • il formato dello schema di numerazione della versione è specificato e include i dettagli relativi a numero di elementi, separatori, set di caratteri, ecc. (ad esempio 1.1.1.N, composti da caratteri alfabetici, numerici e/o alfanumerici); • una definizione di cosa rappresenta ogni elemento nello schema di numerazione della versione (ad esempio tipo di modifica, release maggiore, minore o di manutenzione, carattere jolly, ecc.); • una definizione degli elementi che indicano l'uso dei caratteri jolly. **5.4.1.b** Verificare che gli elementi dello schema di versione siano conformi ai tipi di modifiche specificati nella Guida del programma PA-DSS. **5.4.1.c** Selezionare un campione di modifiche recenti all'applicazione di pagamento, i numeri di versione assegnati e la documentazione di controllo delle modifiche che specifica il tipo di modifica apportato all'applicazione e verificare che gli elementi nel numero di versione corrispondano alla modifica applicabile e ai parametri definiti nella metodologia di versioning documentata.	La metodologia di versioning del fornitore di applicazioni di pagamento dovrebbe includere uno schema di versione che identifica in modo specifico gli elementi in uso, il formato della versione, la gerarchia degli elementi di versioni diverse, ecc. per l'applicazione di pagamento in questione. Lo schema di versione deve specificare in modo chiaro come ciascuno dei vari elementi viene utilizzato nel numero di versione. Lo schema di versione può essere indicato in modi diversi, ad esempio N.NN.NNA, dove "N" rappresenta un elemento numerico e "A" un elemento alfabetico. Lo schema di versioning dovrebbe includere l'identificazione del set di caratteri (ad esempio, 0-9, A-Z, ecc.) che può essere utilizzato per ogni elemento della versione. Senza uno schema di versione definito in modo corretto, le modifiche apportate all'applicazione rischiano di non essere rappresentate in modo accurato dal formato del numero di versione.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	5.4.1.d Consultare alcuni sviluppatori e verificare che conoscano lo schema di versione, compreso l'uso accettabile di caratteri jolly nel numero di versione.	
5.4.2 La metodologia di versioning deve indicare il tipo e l'impatto di tutte le modifiche apportate all'applicazione in conformità alla *Guida del programma PA-DSS*, tra cui: • descrizioni di tutti i tipi e gli impatti delle modifiche apportate all'applicazione; • identificazione e definizione specifiche delle modifiche che: – non incidono sulla funzionalità dell'applicazione o sulle sue dipendenze; – incidono sulla funzionalità dell'applicazione ma non sulla sicurezza o sui requisiti PA-DSS; – incidono sulla funzionalità di sicurezza o sui requisiti PA-DSS; • descrizione di come ogni tipo di modifica è collegato a un numero di versione specifico.	**5.4.2.a** Esaminare la metodologia di versioning del fornitore dell'applicazione per verificare che tale metodologia includa: • descrizione di tutti i tipi e gli impatti delle modifiche dell'applicazione (ad esempio, modifiche che non hanno alcun impatto, hanno un impatto limitato o hanno un impatto elevato sull'applicazione; • identificazione e definizione specifiche delle modifiche che: – non incidono sulla funzionalità dell'applicazione o sulle sue dipendenze; – incidono sulla funzionalità dell'applicazione ma non sulla sicurezza o sui requisiti PA-DSS; – incidono sulla funzionalità di sicurezza o sui requisiti PA-DSS; • descrizione di come ogni tipo di modifica è collegato a un numero di versione specifico.	
	5.4.2.b Verificare che la metodologia di versioning sia conforme ai requisiti espressi nella *Guida del programma PA-DSS*.	
	5.4.2.c Consultare il personale e osservare i processi per ogni tipo di modifica per verificare che la metodologia documentata sia rispettata per tutti i tipi di modifiche.	
	5.4.2.d Selezionare un campione di modifiche recenti all'applicazione di pagamento e rivedere la documentazione di controllo delle modifiche che specifica il tipo di modifica all'applicazione per verificare che la versione assegnata alla modifica corrisponda al tipo di modifica in base alla metodologia documentata.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.4.3 La metodologia di versioning deve identificare in modo specifico se i caratteri jolly vengono utilizzati e, in tal caso, come vengono utilizzati. È necessario includere quanto segue: • dettagli sull'utilizzo dei caratteri jolly nella metodologia di versioning; • i caratteri jolly non vengono mai utilizzati per modifiche che incidono sulla sicurezza o sui requisiti PA-DSS; • gli elementi del numero di versione utilizzati per rappresentare una modifica senza effetti sulla sicurezza (inclusi i caratteri jolly) non devono mai essere usati per rappresentare una modifica con effetti sulla sicurezza; • i caratteri jolly non devono precedere gli elementi della versione che potrebbero rappresentare una modifica con effetti sulla sicurezza; qualsiasi elemento di versione visualizzato dopo un carattere jolly non può essere utilizzato per rappresentare modifiche con effetti sulla sicurezza. ***Nota:*** *i caratteri jolly possono essere utilizzati soltanto in conformità alla Guida del programma PA-DSS.*	**5.4.3.a** Esaminare la metodologia di versioning documentata per verificare che includa l'identificazione specifica di come vengono utilizzati i carattere jolly, tra cui: • dettagli sull'utilizzo dei caratteri jolly nella metodologia di versioning; • i caratteri jolly non vengono mai utilizzati per modifiche che incidono sulla sicurezza o sui requisiti PA-DSS; • gli elementi del numero di versione utilizzati per rappresentare una modifica senza effetti sulla sicurezza (inclusi i caratteri jolly) non devono mai essere usati per rappresentare una modifica con effetti sulla sicurezza; • qualsiasi elemento a destra di un carattere jolly non può essere utilizzato per una modifica con effetti sulla sicurezza. Elementi della versione che riflettono una modifica con effetti sulla sicurezza devono essere mostrati "a sinistra" del primo carattere jolly. **5.4.3.b** Verificare che qualsiasi utilizzo di caratteri jolly sia in conformità ai requisiti espressi nella *Guida del programma PA-DSS*. Ad esempio, gli elementi a destra di un carattere jolly non possono essere utilizzati per una modifica con effetti sulla sicurezza. **5.4.3.c** Consultare il personale e osservare i processi per ogni tipo di modifica per verificare quanto segue: • i caratteri jolly non vengono mai utilizzati per modifiche che incidono sulla sicurezza o sui requisiti PA-DSS; • gli elementi del numero di versione utilizzati per rappresentare una modifica senza effetti sulla sicurezza (inclusi i caratteri jolly) non vengono mai utilizzati per rappresentare una modifica con effetti sulla sicurezza.	Un elemento "carattere jolly" PA-DSS può, facoltativamente, essere utilizzato nello schema di versione per rappresentare modifiche senza effetti sulla sicurezza. Un carattere jolly è l'unico elemento variabile della versione del fornitore e viene utilizzato per indicare solo le modifiche minori senza effetti sulla sicurezza tra ogni versione rappresentata dal carattere jolly. Ad esempio, un numero di versione tipo 1.1.x copre le versioni specifiche 1.1.2 e 1.1.3, ecc., e informa il cliente che la base del codice tra versioni non è stata di fatto modificata, fatta eccezione per modifiche estetiche e di minore entità. Qualsiasi utilizzo dei caratteri jolly deve essere predefinito nella metodologia di versioning del fornitore e deve essere conforme alla *Guida del programma PA-DSS*. ***Nota:*** *l'utilizzo di un carattere jolly è facoltativo e non obbligatorio.*

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	5.4.3.d Selezionare un campione di modifiche recenti all'applicazione di pagamento e rivedere la documentazione di controllo delle modifiche che specifica il tipo di modifica all'applicazione. Verificare quanto segue: • i caratteri jolly non vengono utilizzati per modifiche che incidono sulla sicurezza o sui requisiti PA-DSS; • gli elementi del numero di versione utilizzati per rappresentare una modifica senza effetti sulla sicurezza (inclusi i caratteri jolly) non vengono usati per rappresentare una modifica con effetti sulla sicurezza.	
5.4.4 La metodologia di versioning pubblicata del fornitore deve essere comunicata ai clienti e ai responsabili dell'integrazione/rivenditori.	**5.4.4** Verificare che la *Guida per l'implementazione del programma PA-DSS* contenga una descrizione della metodologia di versioning pubblicata del fornitore per clienti e responsabili dell'integrazione/rivenditori e che includa quanto segue: • dettagli dello schema di versioning, compreso il formato dello schema di versione (numero di elementi, separatori, set di caratteri, ecc.); • dettagli su come verranno indicate le modifiche con effetti sulla sicurezza nello schema di versioning; • dettagli su come altri tipi di modifiche avranno effetti sulla versione; • dettagli su eventuali caratteri jolly utilizzati, inclusa la conferma che non verranno mai utilizzati per rappresentare una modifica con effetti sulla sicurezza.	Garantire che la metodologia di versioning dei fornitori sia inclusa nella *Guida per l'implementazione del programma PA-DSS* fornisce ai clienti e ai responsabili dell'integrazione/rivenditori le informazioni necessarie per comprendere quale versione dell'applicazione di pagamento stanno utilizzando oltre ai tipi di modifiche che sono stati apportati a ogni versione dell'applicazione di pagamento.
5.4.5 Se si utilizza una mappatura interna delle versioni allo schema di versioning pubblicato, la metodologia di versioning deve comprendere la mappatura delle versioni interne alle versioni esterne.	**5.4.5.a** Esaminare la metodologia di versione documentata per verificare che comprenda una mappatura delle versioni interne alle versioni esterne pubblicate. **5.4.5.b** Esaminare le modifiche recenti per confermare che la mappatura interna delle versioni allo schema di versioning pubblicato è aggiornata in base al tipo di modifica, come definito nella metodologia documentata.	Alcuni fornitori di applicazioni di pagamento adottano metodologie di versioning per uso interno o di riferimento che risultano diverse dalla metodologia di versioning utilizzata per le release esterne (o pubbliche). In queste situazioni è importante che entrambe le metodologie di versioning siano definite e documentate in modo chiaro e che le relazioni tra loro siano documentate con accuratezza.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.4.6 Il fornitore software deve disporre di un processo finalizzato all'analisi degli aggiornamenti dell'applicazione per garantire la conformità alla metodologia di versioning prima della release.	**5.4.6.a** Esaminare i processi di sviluppo software documentati e la metodologia di versioning per verificare che sia stato adottato un processo finalizzato all'analisi degli aggiornamenti alle applicazioni per garantire la conformità alla metodologia di versioning prima della release.	È importante che i fornitori di applicazioni di pagamento adottino un processo in grado di assicurare che gli aggiornamenti al prodotto siano in linea con l'intento e lo scopo della release pianificata e che tali modifiche siano state comunicate con accuratezza ai clienti. In caso contrario, si rischia di apportare modifiche a un'applicazione che possono incidere negativamente sulla sicurezza dell'applicazione del cliente e a sua insaputa.
	5.4.6.b Consultare gli sviluppatori software e osservare i processi per verificare che venga eseguita l'analisi degli aggiornamenti all'applicazione con lo scopo di garantire la conformità alla metodologia di versioning prima della release.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.5 Vengono adottate tecniche di valutazione dei rischi (ad esempio, definizione modelli di minacce all'applicazione) per identificare le potenziali falle e vulnerabilità nella progettazione della sicurezza dell'applicazione durante il processo di sviluppo software. I processi di valutazione di rischi comprendono quanto segue: • copertura di tutte le funzioni dell'applicazione di pagamento, compresi, a titolo informatico, le funzioni con effetti sulla sicurezza e le funzioni che superano i limiti di affidabilità; • valutazione di stati decisionali dell'applicazione, flussi di processo, flussi di dati, memorizzazione dati e limiti di affidabilità; • identificazione di tutte le aree all'interno dell'applicazione di pagamento che interagiscono con il numero PAN e/o i dati dei titolari di carta o l'ambiente dei dati dei titolari di carta, oltre a qualsiasi risultato orientato al processo che potrebbe portare all'esposizione dei dati dei titolari di carta; • un elenco delle potenziali minacce e vulnerabilità derivanti dall'analisi del flusso dei dati dei titolari di carta e assegnazione di un livello di rischio a ciascuno (ad esempio, priorità alta, media o bassa) a ciascuno; • implementazione di correzioni e contromisure appropriate durante il processo di sviluppo; • documentazione dei risultati della valutazione dei rischi per l'analisi e l'approvazione da parte della direzione.	**5.5** Esaminare le procedure di sviluppo software scritte e consultare il personale responsabile per verificare che il fornitore utilizzi tecniche di valutazione dei rischi all'interno del proprio processo di sviluppo software e che i processi includano quanto segue: • copertura di tutte le funzioni dell'applicazione di pagamento, compresi, a titolo informatico, le funzioni con effetti sulla sicurezza e le funzioni che superano i limiti di affidabilità; • valutazione di stati decisionali dell'applicazione, flussi di processo, flussi di dati, memorizzazione dati e limiti di affidabilità; • identificazione di tutte le aree all'interno delle applicazioni di pagamento che interagiscono con numero PAN/dati dei titolari di carta o l'ambiente dei dati dei titolari di carta, oltre a qualsiasi risultato orientato al processo che potrebbe portare all'esposizione dei dati dei titolari di carta; • un elenco delle potenziali minacce e vulnerabilità derivanti dall'analisi del flusso dei dati dei titolari di carta e assegnazione di un livello di rischio a ciascuno (ad esempio, priorità alta, media o bassa) a ciascuno; • implementazione di correzioni e contromisure appropriate durante il processo di sviluppo; • documentazione dei risultati della valutazione dei rischi per l'analisi e l'approvazione da parte della direzione.	Per mantenere la qualità e la sicurezza delle applicazioni di pagamento, i fornitori di applicazioni devono adottare tecniche di valutazione dei rischi durante il processo di sviluppo software. La definizione di modelli delle minacce è una forma di valutazione dei rischi che può essere utilizzata per analizzare la struttura e il flusso di dati di un'applicazione alla ricerca di occasioni in cui le informazioni riservate possono essere esposte a utenti dell'applicazione non autorizzati. Questi processi consentono a sviluppatori e architetti software di identificare e risolvere i potenziali problemi nelle fasi iniziali del processo di sviluppo, migliorando la sicurezza dell'applicazione e riducendo al minimo i costi di sviluppo.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
5.6 Il fornitore software deve implementare un processo per documentare e autorizzare la release finale dell'applicazione e di qualsiasi aggiornamento all'applicazione. La documentazione include: • firma di un soggetto autorizzato ad approvare in modo formale la release dell'applicazione o dell'aggiornamento dell'applicazione; • conferma che il fornitore ha seguito i processi di sviluppo sicuro.	**5.6.a** Esaminare i processi documentati per verificare che la release finale dell'applicazione e gli aggiornamenti dell'applicazione siano approvati e documentati in modo formale, inclusa la firma da parte di un soggetto autorizzato ad approvare ufficialmente la release e la conferma che sono stati seguiti tutti i processi SDLC.	Qualcuno all'interno dell'organizzazione del fornitore deve essere responsabile di rivedere e garantire che siano stati applicati tutti gli aspetti del processo di sviluppo sicuro (come definito nei Requisiti da 5.1 a 5.5). Senza una revisione e un riconoscimento formali da parte di un soggetto responsabile, è possibile che vengano saltati o ignorati processi di sicurezza essenziali e che si ottenga un'applicazione guasta o meno sicura.
	5.6.b Per un campione di release recenti dell'applicazione e aggiornamenti dell'applicazione, analizzare la documentazione dell'approvazione e verificare che comprenda: • approvazione formale e forma di un soggetto autorizzato; • conferma che il fornitore ha seguito tutti i processi di sviluppo sicuro.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 6 - Proteggere le trasmissioni wireless

Requisiti PA-DSS	Procedure di test	Istruzioni
6.1 Per le applicazioni di pagamento che utilizzano la tecnologia wireless, modificare i valori wireless predefiniti del fornitore, compresi, senza limitazioni, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP. La tecnologia wireless deve essere implementata in modo sicuro. ***In linea con i Requisiti 1.2.3 e 2.1.1 PCI DSS***	**6.1** Per le applicazioni di pagamento sviluppate per essere utilizzate con tecnologia wireless e tutte le applicazioni wireless associate all'applicazione di pagamento, verificare che per le applicazioni wireless non vengano utilizzate le impostazioni predefinite del fornitore, come segue:	Lo sfruttamento della tecnologia wireless rappresenta un metodo noto agli utenti non autorizzati per ottenere l'accesso alla rete e ai dati dei titolari di carta. Se le reti wireless non vengono implementate con configurazioni di sicurezza sufficienti (che comprendono la modifica delle impostazioni predefinite), gli sniffer wireless possono ascoltare di nascosto il traffico, acquisire facilmente i dati e le password e accedere alla rete per l'attacco. Per queste ragioni, le applicazioni di pagamento non devono richiedere l'uso di impostazioni wireless predefinite o non sicure. Se i firewall non limitano l'accesso dalle reti wireless all'ambiente dei dati dei titolari di carta, gli utenti che ottengono accesso non autorizzato alla rete wireless possono facilmente connettersi a tale ambiente e compromettere le informazioni dei conti.
	6.1.a Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • l'applicazione di pagamento applica le modifiche a chiavi di cifratura predefinite, password e stringhe di comunità SNMP al momento dell'installazione per tutti i componenti wireless controllati dall'applicazione; • procedure per modificare le chiavi di cifratura e le password wireless, comprese le stringhe SNMP, ogni volta che un utente a conoscenza delle chiavi/password lascia l'azienda o cambia sede; • istruzioni per modificare chiavi di cifratura, password e stringhe di comunità SNMP predefinite per tutti i componenti wireless forniti con, ma non controllati da, l'applicazione di pagamento; • istruzioni per installare un firewall tra le reti wireless e i sistemi che memorizzano dati dei titolari di carta; • dettagli sull'eventuale traffico wireless (comprese informazioni su porte specifiche) che la funzione wireless dell'applicazione di pagamento utilizzerà; • istruzioni per configurare i firewall affinché impediscano o controllino il traffico (qualora sia necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	6.1.b Installare l'applicazione in conformità alla *Guida per l'implementazione del programma PA-DSS* e testare l'applicazione e le impostazioni wireless per verificare i punti seguenti per tutte le funzionalità wireless gestite dall'applicazione di pagamento: • le chiavi di cifratura sono state modificate al momento dell'installazione; • le stringhe di comunità SNMP predefinite sui dispositivi wireless sono state modificate al momento dell'installazione; • le password/passphrase predefinite sui punti di accesso sono state modificate al momento dell'installazione; • il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless; • sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili.	
	6.1.c Per tutte le funzionalità wireless gestite dall'applicazione di pagamento, seguire le istruzioni della *Guida per l'implementazione del programma PA-DSS* per modificare le chiavi di cifratura wireless, password/passphrase e stringhe SNMP. Verificare che le istruzioni della *Guida per l'implementazione del programma PA-DSS* siano accurate e abbiano assicurato la modifica delle chiavi di cifratura wireless, delle password e delle stringhe SNMP.	
	6.1.d Per tutti i componenti wireless forniti con, non controllati da, l'applicazione di pagamento, seguire le istruzioni della *Guida per l'implementazione del programma PA-DSS* per modificare le chiavi di cifratura wireless, password/passphrase e stringhe di comunità SNMP predefinite. Verificare che le istruzioni della *Guida per l'implementazione del programma PA-DSS* siano accurate e abbiano assicurato la modifica delle chiavi di cifratura wireless, delle password e delle stringhe SNMP.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	6.1.e Installare l'applicazione e testare le funzioni wireless per verificare che il traffico wireless e le porte utilizzate dall'applicazione coincidano con quelle documentate nella *Guida per l'implementazione del programma PA-DSS*.	
6.2 Per le applicazioni di pagamento che utilizzano la tecnologia wireless, tale applicazione deve facilitare l'uso delle migliori pratiche di settore (ad esempio, IEEE 802.11i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione. ***Nota:*** *l'utilizzo della tecnologia WEP per controllare la sicurezza è vietato.* ***In linea con il Requisito 4.1.1 PCI DSS***	**6.2.a** Per le applicazioni di pagamento sviluppate per l'uso con tecnologia wireless, testare tutte le funzionalità wireless per verificare che l'applicazione utilizzi le migliori pratiche di settore (ad esempio IEEE 802.11.i) per garantire una cifratura avanzata per l'autenticazione e la trasmissione.	Gli utenti non autorizzati utilizzano strumenti liberi e ampiamente disponibili per ascoltare le comunicazioni wireless. L'uso di crittografia avanzata può contribuire a limitare la divulgazione di informazioni sensibili attraverso le reti wireless. La crittografia avanzata per l'autenticazione e la trasmissione dei dati dei titolari di carta è necessaria per impedire agli utenti non autorizzati di ottenere accesso ai dati su una rete wireless o di utilizzare le reti wireless per accedere ad altri dati o sistemi.
	6.2.b Per tutte le applicazioni wireless associate all'applicazione di pagamento, eseguire il test della funzionalità wireless per verificare che siano state utilizzate le migliori pratiche di settore (ad esempio IEEE 802.11.i) per garantire una cifratura avanzata per l'autenticazione e la trasmissione.	
	6.2.c Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti istruzioni per clienti e responsabili dell'integrazione/rivenditori: • come configurare l'applicazione per utilizzare le migliori pratiche di settore (ad esempio IEEE 802.11.i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione; • come configurare tutte le applicazioni wireless associate all'applicazione per utilizzare le migliori pratiche di settore per implementare la cifratura avanzata per l'autenticazione e la trasmissione.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
6.3 Fornire istruzioni per i clienti sull'uso sicuro della tecnologia wireless. ***Nota:*** *questo requisito si applica a tutte le applicazioni di pagamento, a prescindere dal fatto che l'applicazione sia sviluppata per l'uso con tecnologie wireless o meno.* **In linea con i *Requisiti 1.2.3, 2.1.1 e 4.1.1 PCI DSS***	**6.3** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che contenga le istruzioni necessarie per clienti e rivenditori/responsabili dell'integrazione per le impostazioni wireless conformi agli standard PCI DSS come segue: • istruzioni per modificare tutte le chiavi, password e stringhe di comunità SNMP della cifratura wireless predefinita al momento dell'installazione; • istruzioni per modificare chiavi, password e stringhe di comunità SNMP della cifratura wireless ogni volta che un utente a conoscenza delle chiavi/password lascia l'azienda o cambia sede; • istruzioni per installare un firewall tra le reti wireless e i sistemi dove sono conservati i dati dei titolari di carta e configurare tali firewall per negare o consentire il traffico (se necessario per gli scopi aziendali) tra l'ambiente wireless e l'ambiente dei dati dei titolari di carta; • istruzioni per utilizzare le migliori pratiche di settore (ad esempio IEEE 802.11.i) per fornire una cifratura avanzata per l'autenticazione e la trasmissione.	I fornitori di applicazioni di pagamento devono comunicare ai clienti le istruzioni per la configurazione dell'applicazione in modo da garantire il supporto dell'uso di tecnologie wireless, anche se l'applicazione non è stata esplicitamente progettata per essere utilizzata in un ambiente wireless. Poiché le reti wireless sono ormai la norma, i clienti devono conoscere le impostazioni di sicurezza wireless più comuni da implementare per garantire la protezione dell'applicazione di pagamento.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 7 - Sottoporre a test le applicazioni di pagamento per identificare le vulnerabilità e gestire gli aggiornamenti delle applicazioni di pagamento

Requisiti PA-DSS	Procedure di test	Istruzioni
7.1 I fornitori di software devono definire un processo per identificare e gestire le vulnerabilità, come descritto: ***Nota:*** *qualsiasi software o sistema sottostante fornito con l'applicazione di pagamento o richiesto dall'applicazione (ad esempio, server Web, librerie e programmi di terzi) deve essere incluso in questo processo.* ***In linea con il Requisito 6.1 PCI DSS***	**7.1.a** Esaminare la documentazione dei processi di gestione delle vulnerabilità per verificare che siano state definite procedure per: • individuare nuove vulnerabilità della sicurezza utilizzando fonti attendibili per ottenere informazioni sulle vulnerabilità della sicurezza; • assegnare una classificazione dei rischi a tutte le vulnerabilità identificate; • testare applicazioni di pagamento e aggiornamenti per verificare la presenza di vulnerabilità prima della release. **7.1.b** Verificare che i processi per identificare nuove vulnerabilità e implementare le correzioni nell'applicazione di pagamento siano applicati a tutto il software fornito con tale applicazione o richiesto dall'applicazione (ad esempio server Web, librerie e programmi di terzi).	I fornitori devono mantenersi aggiornati sulle nuove vulnerabilità che potrebbero avere un impatto sulle loro applicazioni, comprese le vulnerabilità dei componenti sottostanti o del software fornito con le applicazioni o da loro richiesti. Conoscendo le vulnerabilità insite nelle loro applicazioni o nei componenti sottostanti, i fornitori di applicazioni di pagamento dovrebbero quindi essere in grado di risolvere tali vulnerabilità prima della release o di implementare altri meccanismi per ridurre la probabilità che la vulnerabilità possa essere sfruttata nel caso in cui una patch di sicurezza di terzi non sia immediatamente disponibile.
7.1.1 individuare nuove vulnerabilità della sicurezza utilizzando fonti attendibili per ottenere informazioni sulle vulnerabilità della sicurezza.	**7.1.1** Consultare il personale responsabile e osservare i processi per verificare se vengono individuate nuove vulnerabilità della sicurezza: • sia nell'applicazione di pagamento che nel software o nei sistemi sottostanti forniti con l'applicazione di pagamento o richiesti dall'applicazione; • utilizzando fonti attendibili (come siti Web dei fornitori di software/sistemi, NVD del NIST, CVE del MITRE e siti Web US-CERT del DHS).	Nei componenti software di terzi è necessario utilizzare fonti attendibili per informazioni su vulnerabilità e/o patch. Le fonti di informazioni sulle vulnerabilità devono essere affidabili e spesso includono siti Web dei fornitori, newsgroup di settore, mailing list o feed RSS. Tra gli esempi di fonti del settore è possibile citare il National Vulnerability Database del NIST, il Common Vulnerabilities and Exposures List del MITRE e i siti Web US-CERT del DHS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
7.1.2 Assegnare una classificazione dei rischi a tutte le vulnerabilità identificate, comprese le vulnerabilità che riguardano software o sistemi sottostanti forniti con l'applicazione di pagamento o richiesti dall'applicazione. ***Nota:*** *le classificazioni dei rischi devono essere basate sulle migliori pratiche di settore nonché sulla valutazione del potenziale impatto. Ad esempio, i criteri per la classificazione delle vulnerabilità possono tenere in considerazione il punteggio base CVSS e/o la classificazione del fornitore e/o l'impatto sulla funzionalità dell'applicazione.* *Le classificazioni dei rischi devono almeno identificare tutte le vulnerabilità ad "alto rischio" per l'applicazione. Oltre alla classificazione dei rischi, le vulnerabilità possono essere considerate "critiche" se rappresentano una minaccia imminente, influiscono sui componenti critici dell'applicazione o comportano una potenziale compromissione se non risolte.*	**7.1.2** Consultare il personale responsabile e osservare i processi per verificare che venga assegnata una classificazione dei rischi alle nuove vulnerabilità della sicurezza, comprese le vulnerabilità che riguardano software o sistemi sottostanti forniti con l'applicazione di pagamento o richiesti dall'applicazione.	Una volta che il fornitore identifica una vulnerabilità che potrebbe incidere sulla sua applicazione, è necessario valutare e classificare il rischio che la vulnerabilità comporta. Per questo è utile un processo che monitori attivamente le fonti di informazione del settore sulle vulnerabilità. La classificazione dei rischi (ad esempio, come "alta", "media" o "bassa") consente ai fornitori di individuare, assegnare priorità e risolvere gli elementi a rischio (ad esempio, pubblicando con maggiore rapidità le patch ad alta priorità) e di ridurre la probabilità che vengano sfruttate le vulnerabilità che costituiscono i rischi più elevati per gli ambienti dei clienti.
7.1.3 Testare applicazioni di pagamento e aggiornamenti per verificare la presenza di vulnerabilità prima della release.	**7.1.3** Consultare il personale responsabile e osservare i processi per verificare che le applicazioni di pagamento vengano testate per verificare la presenza di vulnerabilità prima della release.	Per garantire la corretta risoluzione delle vulnerabilità identificate prima della release, è necessario includere test adeguati nel processo di gestione delle vulnerabilità del fornitore di applicazioni di pagamento. *I metodi di test possono includere test di penetrazione e/o tecniche di fuzz testing per l'identificazione di potenziali vulnerabilità, ad esempio attraverso l'inserimento di dati imprevisti o non corretti o la modifica della dimensione dei bit dei dati.*

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
7.2 I fornitori di software devono stabilire un processo per uno sviluppo e una distribuzione tempestivi delle patch di sicurezza e degli aggiornamenti.	**7.2** Esaminare la documentazione dei processi per lo sviluppo e la distribuzione delle patch di sicurezza e degli aggiornamenti per verificare che il processo includa le procedure per i punti 7.2.1 e 7.2.2.	Per ridurre al minimo la finestra temporale e la probabilità che la vulnerabilità possa essere sfruttata, una volta individuata una vulnerabilità critica gli aggiornamenti del software per risolvere le vulnerabilità della sicurezza devono essere sviluppati e distribuiti ai clienti il più rapidamente possibile.
7.2.1 Le patch e gli aggiornamenti vengono distribuiti ai clienti in modo sicuro mediante canali affidabili.	**7.2.1** Consultare il personale responsabile e osservare i processi per verificare che patch e aggiornamenti raggiungano i clienti in modo sicuro mediante canali affidabili.	Le patch di sicurezza devono essere distribuite in modo che gli utenti non autorizzati non possano intercettare, modificare e ridistribuire gli aggiornamenti in transito a ignari clienti.
7.2.2 Le patch e gli aggiornamenti vengono consegnati ai clienti in modo da garantire l'integrità del codice della patch e dell'aggiornamento.	**7.2.2.a** Consultare il personale responsabile e osservare i processi per verificare che patch e aggiornamenti vengano consegnati ai clienti in modo da garantire l'integrità del codice della patch e dell'aggiornamento.	Gli aggiornamenti della sicurezza devono includere un meccanismo interno al processo di aggiornamento che verifichi che il codice dell'aggiornamento non sia stato sostituito o alterato. Esempi di controlli dell'integrità includono, senza limitazioni, checksum, certificati con firma digitale, ecc.
	7.2.2.b Consultare il personale responsabile e osservare i processi di aggiornamento dell'applicazione per verificare che le patch e gli aggiornamenti vengano testati a livello di integrità nel sistema di destinazione prima dell'installazione.	
	7.2.2.c Verificare che l'integrità del codice di patch e aggiornamenti sia garantita eseguendo il processo di aggiornamento con codice arbitrario e controllando che il sistema non consenta l'esecuzione dell'aggiornamento.	
7.2.3 Fornire istruzioni per i clienti sull'installazione sicura di patch e aggiornamenti.	**7.2.3** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore per verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • comunicazione delle notifiche di nuovi patch e aggiornamenti da parte del fornitore; • consegna di patch e aggiornamenti in modo sicuro mediante "canali affidabili"; • accesso e installazione di patch e aggiornamenti in modo da mantenere l'integrità del relativo codice.	Fornendo istruzioni a clienti e responsabili dell'integrazione/rivenditori sul processo per la ricezione e l'installazione di patch in modo sicuro si contribuisce a proteggere l'integrità dell'applicazione e del processo di aggiornamento.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
7.3 Includere note sulla release per tutti gli aggiornamenti dell'applicazione, compresi dettagli e impatto dell'aggiornamento e modalità con cui è stato modificato il numero di versione affinché rifletta l'avvenuto aggiornamento.	**7.3.a** Esaminare i processi per la pubblicazione degli aggiornamenti e consultare il personale per verificare che per tutti gli aggiornamenti vengano preparate note sulla release, che contengono dettagli e impatto dell'aggiornamento e modalità con cui è stato modificato il numero di versione affinché rifletta l'avvenuto aggiornamento.	Le note sulla release forniscono ai clienti dettagli sugli aggiornamenti del software: quali sono i file che possono aver subito modifiche, quali funzionalità dell'applicazione sono state modificate ed eventuali funzioni relative alla sicurezza che possono essere state coinvolte. Le note sulla release devono inoltre indicare qual è l'impatto di una patch o di un aggiornamento particolari sul numero di versione complessivo associato alla release della patch.
	7.3.b Esaminare le note sulla release di un campione di aggiornamenti dell'applicazione e verificare che siano state fornite con l'aggiornamento.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 8 - Facilitare l'implementazione sicura in rete

Requisiti PA-DSS	Procedure di test	Istruzioni
8.1 L'applicazione di pagamento deve poter essere implementata in un ambiente di rete sicuro. L'applicazione non deve interferire con l'uso di dispositivi, applicazioni o configurazioni richieste per conformità allo standard PCI DSS *(ad esempio l'applicazione di pagamento non può interferire con l'installazione di patch, la protezione antivirus, le configurazioni del firewall o qualsiasi altro dispositivo, applicazione o configurazione richiesta per conformità allo standard PCI DSS).* ***In linea con i requisiti 1, 3, 4, 5 e 6 PCI DSS***	**8.1.a** Installare l'applicazione in un ambiente di laboratorio conforme allo standard PCI DSS in base alla *Guida per l'implementazione del programma PA-DSS.* Sottoporre a test l'applicazione di pagamento per ottenere la prova che possa essere eseguita in una rete in modo conforme allo standard PCI DSS. **8.1.b** Sottoporre a test l'applicazione e i sistemi sottostanti per verificare che l'applicazione di pagamento non precluda l'uso o non interferisca con le funzioni PCI DSS nei sistemi sottostanti (ad esempio che l'applicazione non impedisca l'installazione di patch o di aggiornamenti anti-malware o non interferisca con altre funzioni PCI DSS.	Le applicazioni di pagamento devono essere progettate e sviluppate in modo che l'installazione e il funzionamento delle applicazioni stesse non impediscano a un'organizzazione di implementare altri controlli necessari per garantire la conformità PCI DSS. Ad esempio, l'applicazione di pagamento deve essere in grado di operare in un ambiente che esegue soluzioni antivirus (ad esempio non richiede lo spegnimento o la disinstallazione di tali soluzioni).
8.2 L'applicazione di pagamento deve utilizzare o richiedere solo l'uso di servizi, protocolli, componenti, software e hardware dipendenti sicuri e necessari, compresi quelli forniti da terze parti, per qualsiasi funzionalità dell'applicazione di pagamento. *Nota: SSL e TLS iniziale non sono più considerati crittografia avanzata. Le applicazioni di pagamento non li devono utilizzare né supportarne l'uso. Le applicazioni che utilizzano o supportano TLS non devono consentire il fallback a SSL.* ***In linea con il Requisito 2.2.3 PCI DSS***	**8.2.a** Esaminare servizi di sistema, protocolli, daemon, componenti e software e hardware dipendenti abilitati o richiesti dall'applicazione di pagamento. Verificare che solo servizi, protocolli, daemon, componenti e software e hardware dipendenti sicuri e necessari siano abilitati per impostazione predefinita come "pronti per l'uso". **8.2.b** Installare l'applicazione e testarne le funzioni per verificare che, se l'applicazione supporta servizi, daemon, protocolli o componenti non sicuri, questi siano configurati in modo sicuro come "pronti per l'uso" per impostazione predefinita. **8.2.c** Verificare che la *Guida per l'implementazione del programma PA-DSS* documenti tutti i protocolli, servizi, componenti e software e hardware dipendenti che sono necessari per qualsiasi funzionalità dell'applicazione di pagamento, compresi quelli forniti da terze parti.	Esistono molti protocolli di cui un'azienda potrebbe avere bisogno (o che sono attivati per impostazione predefinita), e che sono comunemente utilizzati da utenti non autorizzati per compromettere un sistema o una rete. L'applicazione di pagamento non deve richiedere l'uso di protocolli, servizi, daemon, ecc. non sicuri. Se l'applicazione supporta l'uso di servizi, daemon, protocolli o componenti non sicuri, questi devono essere protetti per impostazione predefinita.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
8.3 L'applicazione di pagamento non deve richiedere l'uso di servizi o protocolli che precludono l'uso o interferiscono con il normale funzionamento delle tecnologie di autenticazione a più fattori. ***Nota:*** *l'autenticazione a più fattori richiede che siano utilizzati almeno due dei tre metodi di autenticazione (vedere di seguito). Utilizzare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a più fattori. I metodi di autenticazione, conosciuti anche come fattori, sono:* • qualcosa che l'utente conosce, come una password o una passphrase; • Qualcosa in possesso dell'utente, come un dispositivo token o una smart card • qualcosa che l'utente è, come un elemento biometrico. ***In linea con il Requisito 8.3 PCI DSS***	**8.3.a** Esaminare la funzionalità dell'applicazione di pagamento per verificare che non richieda l'uso di eventuali servizi o protocolli che precludono l'uso o interferiscono con il normale funzionamento delle tecnologie di autenticazione a più fattori. **8.3.b** Identificare i meccanismi di accesso remoto supportati dall'applicazione e verificare che tali meccanismi non impediscano l'autenticazione a più fattori.	Le applicazioni di pagamento devono essere progettate e sviluppate in modo che l'installazione e il funzionamento delle applicazioni stesse non richiedano a un'organizzazione l'uso di servizi o protocolli che impedirebbero all'organizzazione di implementare e utilizzare soluzioni di autenticazione a più fattori per la sicurezza dell'accesso. Ad esempio, l'applicazione non deve utilizzare per impostazione predefinita la porta 1812 (universalmente nota per essere assegnata a RADIUS da RFC 2865) se RADIUS deve essere una tecnologia di autenticazione e autorizzazione supportata. *Esempi di tecnologie a più fattori includono, senza limitazione, RADIUS con token, TACACS con token oppure altre tecnologie che facilitano l'autenticazione a più fattori.*

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 9 - I dati dei titolari di carta non devono mai essere memorizzati su un server connesso a Internet

Requisiti PA-DSS	Procedure di test	Istruzioni
9.1 L'applicazione di pagamento deve essere sviluppata in modo che qualsiasi server Web e componente della memorizzazione dei dati dei titolari di carta (ad esempio un database server) non debbano essere sullo stesso server e in modo che il componente della memorizzazione dei dati non debba essere nella stessa zona di rete (ad esempio nella stessa zona DMZ) del server Web. ***In linea con il Requisito 1.3.7 PCI DSS***	**9.1.a** Identificare tutti i componenti della memorizzazione dei dati dell'applicazione di pagamento (ad esempio i database) e tutti i server Web. Installare i componenti della memorizzazione dei dati e i server Web su server diversi e testare la funzionalità dell'applicazione sui diversi server. Verificare che, per funzionare, l'applicazione di pagamento non richieda l'installazione di componenti della memorizzazione dei dati (ad esempio database) sullo stesso server come server Web.	Ogni componente del server Web di un'applicazione di pagamento è sostanzialmente esposto a un maggior rischio di compromissione, considerata la natura aperta delle reti pubbliche (Internet, wireless pubbliche, ecc.) e la natura e il volume degli attacchi che possono originarsi da tali reti. I componenti della memorizzazione dei dati dei titolari di carta richiedono un livello di protezione più alto rispetto ai componenti delle applicazioni rivolti al pubblico. Se i dati dei titolari di carta sono all'interno della zona DMZ, un aggressore esterno può accedere più facilmente a queste informazioni, in quanto esistono meno strati da penetrare. Per lo stesso motivo, i server Web non devono mai essere conservati nello stesso server del componente della memorizzazione dei dati di titolari di carta. Se un utente non autorizzato fosse in grado di compromettere un account sul server Web, potrebbe, senza ulteriori sforzi, compromettere anche il database dei titolari di carta.
	9.1.b Installare i componenti della memorizzazione dei dati di titolari di carta e i server Web in zone diverse della rete. Testare tutte le funzioni delle applicazioni nelle zone di rete per verificare che l'applicazione di pagamento non richieda per funzionare l'installazione di un componente della memorizzazione dei dati (ad esempio un database) sulla stessa zona di rete di un server Web.	
	9.1.c Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • istruzioni per non memorizzare dati dei titolari di carta su sistemi rivolti al pubblico (ad esempio i server Web e i database server non devono trovarsi sullo stesso server); • istruzioni su come configurare l'applicazione di pagamento per utilizzare una zona DMZ per separare Internet dai sistemi che memorizzano dati dei titolari di carta (ad esempio installando un componente server Web in una zona DMZ e un componente della memorizzazione dei dati su una zona di rete interna diversa); • un elenco di servizi/porte che l'applicazione deve utilizzare per comunicare in due zone di rete (per consentire al cliente di configurare il firewall in modo che si aprano solo le porte necessarie).	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 10 - Facilitare l'accesso remoto sicuro all'applicazione di pagamento

Requisiti PA-DSS	Procedure di test	Istruzioni
10.1 Per tutto l'accesso remoto all'applicazione di pagamento originato al di fuori dell'ambiente del cliente è necessario utilizzare l'autenticazione a più fattori. ***Nota:*** *l'autenticazione a più fattori richiede l'utilizzo di almeno due dei tre metodi di autenticazione (fare riferimento al Requisito 3.1.4 PA-DSS per le descrizioni dei metodi di autenticazione).* **In linea con il *Requisito 8.3 PCI DSS*** **10.1.a** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che includa le seguenti informazioni per i clienti e i responsabili dell'integrazione/rivenditori: • istruzioni che stabiliscono che tutto l'accesso remoto all'applicazione di pagamento originato al di fuori della rete del cliente deve utilizzare l'autenticazione a più fattori per soddisfare i requisiti PCI DSS; • una descrizione dei meccanismi di autenticazione a più fattori supportati dall'applicazione; • istruzioni per la configurazione dell'applicazione affinché supporti l'autenticazione a più fattori (almeno due dei tre metodi di autenticazione descritti nel Requisito 3.1.4 PA DSS). **10.1.b** Se il fornitore dell'applicazione ha accesso remoto all'applicazione di pagamento di un cliente che ha origine al di fuori dell'ambiente del cliente, esaminare le politiche del fornitore per verificare che il fornitore supporti i requisiti del cliente per l'autenticazione a più fattori di tutto l'accesso.	L'autenticazione a più fattori richiede almeno due metodi di autenticazione per l'accesso originato al di fuori della rete. I fornitori di applicazioni di pagamento devono comunicare ai clienti le istruzioni per la configurazione dell'applicazione per supportare i meccanismi di autenticazione a più fattori specificati al fine di garantire la loro corretta implementazione e il rispetto dei requisiti PCI DSS applicabili. Il requisito dell'autenticazione a più fattori si applica a tutto il personale con accesso remoto che ha origine al di fuori dell'ambiente del cliente.
10.2 Ogni accesso remoto all'applicazione di pagamento deve essere effettuato in modo sicuro, come segue:	**10.2** Verificare che ogni accesso remoto sia effettuato come segue:	Qualsiasi meccanismo di accesso remoto utilizzato dal fornitore di applicazioni di pagamento e/o dai responsabili

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
10.2.1 Se gli aggiornamenti dell'applicazione di pagamento vengono inviati tramite l'accesso remoto ai sistemi dei clienti, i fornitori del software devono richiedere ai clienti di attivare le tecnologie di accesso remoto solo quando occorre eseguire i download e di disattivarle immediatamente una volta completata l'operazione. In alternativa, se consegnati tramite VPN o altra connessione ad alta velocità, i fornitori del software devono indicare ai clienti di configurare in modo appropriato un firewall o un prodotto firewall personale per proteggere le connessioni "sempre attive". ***In linea con i Requisiti 1 e 12.3.9 PCI DSS***	**10.2.1.a** Se gli aggiornamenti dell'applicazione di pagamento vengono consegnati tramite accesso remoto ai sistemi dei clienti, esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che contenga: • istruzioni per clienti e responsabili dell'integrazione/rivenditori relative all'uso sicuro delle tecnologie di accesso remoto, che specificano che tali tecnologie usate da fornitori e partner aziendali si dovrebbero attivare solo quando servono e disattivare immediatamente dopo l'uso; • consigli per clienti e responsabili dell'integrazione/rivenditori affinché utilizzino un firewall o un prodotto firewall personale configurati in modo sicuro se il computer è connesso tramite VPN o altra connessione ad alta velocità, per proteggere le connessioni "sempre attive", in conformità al Requisito 1 PCI DSS.	dell'integrazione/rivenditori (ad esempio per supportare servizi forniti dai fornitori) deve supportare tutti i requisiti PCI DSS applicabili.
	10.2.1.b Se il fornitore consegna l'applicazione di pagamento e/o gli aggiornamenti tramite accesso remoto alle reti dei clienti, esaminare i metodi del fornitore per la consegna dell'applicazione di pagamento e/o degli aggiornamenti tramite accesso remoto alle rete dei clienti e verificare che il metodo preveda: • attivazione di tecnologie di accesso remoto alle reti dei clienti solo quando richiesto, con disattivazione immediata dopo l'uso; • se l'accesso remoto avviene tramite VPN o altra connessione ad alta velocità, la connessione deve essere protetta in base al Requisito 1 PCI DSS.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
10.2.2 Se i fornitori o i responsabili dell'integrazione/rivenditori possono accedere alle applicazioni di pagamento dei clienti in remoto, è necessario utilizzare un'unica credenziale di autenticazione (ad esempio una password/passphrase) per ogni cliente. ***In linea con il Requisito 8.5.1 PCI DSS***	**10.2.2** Se i fornitori o i responsabili dell'integrazione/rivenditori possono accedere alle applicazioni di pagamento dei clienti in remoto, esaminare i processi del fornitore e consultare il personale per verificare che venga utilizzata un'unica credenziale di autenticazione (ad esempio una password/passphrase) per ogni cliente a cui accedono.	Per evitare il problema della gestione di più ambienti dei clienti con un unico gruppo di credenziali, i fornitori con account ad accesso remoto agli ambienti dei clienti devono utilizzare credenziali di autenticazione diverse per ogni cliente. Evitare l'uso di formule ripetibili per generare password facilmente individuabili. Le credenziali diventano note nel corso del tempo e possono essere utilizzate da persone non autorizzate per recar danno ai clienti del fornitore.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
10.2.3 L'accesso remoto alle applicazioni di pagamento da parte di fornitori, responsabili dell'integrazione/rivenditori o clienti deve essere implementato in modo sicuro, ad esempio con i metodi seguenti: • modifica delle impostazioni predefinite del software di accesso remoto (ad esempio, modifica delle password predefinite e uso di password univoche per ciascun cliente); • Possibilità di connessioni solo da indirizzi IP/MAC (noti) specifici. • uso di autenticazione di password avanzate e di password complesse per i login (vedere i Requisiti da 3.1.1 a 3.1.11 PA-DSS); • abilitazione della trasmissione di dati cifrati in conformità al Requisito 12.1 PA-DSS; • abilitazione del lockout dell'account dopo un determinato numero di login non riusciti (vedere i Requisiti da 3.1.9 a 3.1.10 PA-DSS); • attivazione di una connessione VPN tramite firewall prima che venga concesso l'accesso; • Abilitazione della funzione di registrazione in file di log. • limitazione dell'accesso agli ambienti dei clienti per responsabili dell'integrazione/rivenditori autorizzati. ***In linea con i Requisiti 2, 8 e 10 PCI DSS***	**10.2.3.a** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che clienti e responsabili dell'integrazione/rivenditori sappiano che ogni accesso remoto all'applicazione di pagamento deve essere implementato in modo sicuro, ad esempio con i metodi seguenti: • modifica delle impostazioni predefinite del software di accesso remoto (ad esempio, modifica delle password predefinite e uso di password univoche per ciascun cliente); • Possibilità di connessioni solo da indirizzi IP/MAC (noti) specifici. • uso di autenticazione di password avanzate e di password complesse per i login (vedere i Requisiti da 3.1.1 a 3.1.11 PA-DSS); • abilitazione della trasmissione di dati cifrati in conformità al Requisito 12.1 PA-DSS; • abilitazione del lockout dell'account dopo un determinato numero di login non riusciti (vedere i Requisiti da 3.1.9 a 3.1.10 PA-DSS); • attivazione di una connessione VPN tramite firewall prima che venga concesso l'accesso; • Abilitazione della funzione di registrazione in file di log. • limitazione dell'accesso agli ambienti dei clienti per il personale autorizzato. **10.2.3.b** Se il fornitore del software può accedere alle applicazioni di pagamento dei clienti in remoto, esaminare i metodi di accesso remoto del fornitore e consultare il personale per verificare che l'accesso remoto sia implementato in modo sicuro.	I fornitori di applicazioni di pagamento dovranno fornire a clienti e responsabili dell'integrazione/rivenditori le istruzioni per configurare l'applicazione affinché supporti l'accesso remoto sicuro e garantisca l'implementazione corretta dei meccanismi e il rispetto dei requisiti PCI DSS. Questo requisito si applica a qualsiasi tipo di accesso remoto utilizzato per accedere all'ambiente del cliente.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 11 - Cifratura dei dati sensibili trasmessi su reti pubbliche

Requisiti PA-DSS	Procedure di test	Istruzioni
11.1 Se l'applicazione di pagamento consente o facilita l'invio di dati dei titolari di carta su reti pubbliche, l'applicazione di pagamento deve supportare l'uso di protocolli di sicurezza e crittografia avanzata per proteggere i dati dei titolari di carta sensibili durante la trasmissione su reti pubbliche aperte, incluso almeno quanto segue: • vengono accettati solo certificati e chiavi affidabili; • il protocollo utilizzato supporta soltanto versioni o configurazioni sicure; • il livello di cifratura è corretto per la metodologia di cifratura in uso. ***Nota:*** *SSL e TLS iniziale non sono più considerati crittografia avanzata. Le applicazioni di pagamento non li devono utilizzare né supportarne l'uso. Le applicazioni che utilizzano o supportano TLS non devono consentire il fallback a SSL.* *Esempi di reti pubbliche aperte includono, senza limitazioni:* • Internet • Tecnologie wireless, incluso 802.11 e Bluetooth	**11.1.a** Se l'applicazione di pagamento consente o facilita l'invio di dati dei titolari di carta tramite reti pubbliche, verificare che con l'applicazione siano forniti protocolli di crittografia e sicurezza avanzati o che ne venga richiesto l'uso. **11.1.b** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che il fornitore abbia incluso istruzioni per clienti e responsabili dell'integrazione/rivenditori che richiedono l'uso dei protocolli di crittografia e sicurezza avanzati forniti con l'applicazione o specificati, comprese: • istruzioni che richiedono l'uso di protocolli di crittografia e sicurezza avanzati qualora i dati dei titolari di carta dovessero essere trasmessi su reti pubbliche; • istruzioni che spiegano quali sono i certificati e/o le chiavi affidabili accettati; • istruzioni per configurare l'applicazione di pagamento affinché utilizzi solo versioni e implementazioni sicure dei protocolli di sicurezza; • istruzioni per configurare l'applicazione di pagamento per impedire il fallback a una configurazione o una versione non sicura (ad es. se si utilizza TLS, l'applicazione non deve consentire il fallback a SSL); • istruzioni per configurare l'applicazione di pagamento affinché utilizzi il livello di cifratura corretto per la metodologia di cifratura in uso.	Poiché si verifica con facilità e frequenza che un utente non autorizzato intercetti e/o dirotti i dati in transito, le informazioni sensibili devono essere cifrate durante la trasmissione su reti pubbliche. La trasmissione sicura dei dati dei titolari di carta richiede l'uso di chiavi/certificati affidabili, un protocollo sicuro per il trasferimento e il livello di cifratura corretto per cifrare i dati dei titolari di carta. Tener presente che alcune implementazioni di protocolli (come SSL, SSH versione 1.0 e TLS iniziale) dispongono di vulnerabilità documentate, quali buffer overflow, che un aggressore può utilizzare per ottenere il controllo del sistema interessato. Qualunque sia il protocollo di sicurezza utilizzato dall'applicazione di pagamento, verificare che sia configurato per usare solo versioni e configurazioni sicure e non consenta l'utilizzo di una connessione non sicura.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
• Tecnologie mobili, ad esempio, comunicazioni GSM (Global System for Mobile), CDMA (Code Division Multiple Access) • GPRS (General Packet Radio Service) • Comunicazioni satellitari ***In linea con il Requisito 4.1 PCI DSS***	**11.1.c** Se con l'applicazione di pagamento vengono forniti protocolli di crittografia e sicurezza avanzati, installare e sottoporre a test l'applicazione seguendo le istruzioni della *Guida per l'implementazione del programma PA-DSS* e verificare che: • per impostazione predefinita, il protocollo sia implementato per utilizzare solo certificati e/o chiavi affidabili; • per impostazione predefinita, il protocollo sia implementato per utilizzare solo configurazioni sicure e non supporti versioni o configurazioni non sicure; • per impostazione predefinita, il protocollo sia implementato per non consentire il fallback a una configurazione o una versione non sicura (ad es. se si utilizza TLS, l'applicazione non deve consentire il fallback a SSL); • sia implementato il livello di cifratura corretto per la metodologia di cifratura in uso.	
11.2 Se l'applicazione di pagamento facilita l'invio di PAN mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea e chat), l'applicazione di pagamento deve fornire una soluzione che renda il PAN impossibile da leggere o implementi una crittografia avanzata, oppure specificare l'uso di una crittografia avanzata per cifrare i PAN. ***In linea con il Requisito 4.2 PCI DSS***	**11.2.a** Se l'applicazione di pagamento consente e/o facilita l'invio di PAN mediante tecnologie di messaggistica degli utenti finali, verificare che venga fornita o richiesta una soluzione che renda il PAN illeggibile o che implementi crittografia avanzata.	L'e-mail, la messaggistica istantanea e la chat possono essere facilmente intercettati mediante packet-sniffing durante il recapito attraverso reti interne e pubbliche. Non utilizzare questi strumenti di messaggistica per inviare numeri PAN, a meno che l'applicazione di pagamento non preveda l'uso di crittografia avanzata con queste tecnologie o non sia in grado di rendere il PAN illeggibile.
	11.2.b Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che il fornitore abbia incluso istruzioni per clienti e responsabili dell'integrazione/rivenditori che richiedono l'uso di una soluzione fornita con l'applicazione o specificata, comprese: • procedure per utilizzare la soluzione indicata in modo che renda il PAN illeggibile o protegga il PAN con crittografia avanzata; • istruzioni per far sì che il PAN sia reso illeggibile o sicuro con crittografia avanzata ogni volta che viene inviato mediante tecnologie di messaggistica degli utenti finali.	
	11.2.c Se viene fornita una soluzione con l'applicazione di pagamento, installare e sottoporre a test l'applicazione per verificare che la soluzione renda il PAN illeggibile o implementi crittografia avanzata.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 12 - Sicurezza di tutto l'accesso amministrativo non da console

Requisiti PA-DSS	Procedure di test	Istruzioni
12.1 Se l'applicazione di pagamento facilita l'accesso amministrativo non da console, eseguire la cifratura di tutto l'accesso con la crittografia avanzata. ***Note:*** • *non utilizzare mai protocolli con testo in chiaro come Telnet o rlogin per l'accesso amministrativo.* • *SSL e TLS iniziale non sono più considerati crittografia avanzata. Le applicazioni di pagamento non li devono utilizzare né supportarne l'uso. Le applicazioni che utilizzano o supportano TLS non devono consentire il fallback a SSL.* ***In linea con il Requisito 2.3 PCI DSS***	**12.1.a** Installare l'applicazione di pagamento in laboratorio e testare le connessioni di amministrazione non da console per verificare che venga richiamato un metodo di cifratura avanzata prima della richiesta della password dell'amministratore.	Se l'amministrazione remota non viene eseguita con l'autenticazione sicura e comunicazioni cifrate, un utente non autorizzato può rilevare informazioni sensibili a livello amministrativo e operativo (ad esempio le password degli amministratori). Un utente non autorizzato può utilizzare queste informazioni per accedere all'applicazione e/o alla rete, modificare le autorizzazioni e sottrarre i dati.
	12.1.b Esaminare le impostazioni della configurazione dell'applicazione di pagamento per verificare che l'applicazione di pagamento non utilizzi protocolli con testo in chiaro, come Telnet e rlogin, per accessi amministrativi non da console.	
	12.1.c Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che vengano fornite istruzioni ai clienti e ai responsabili dell'integrazione/rivenditori per configurare l'applicazione in modo che utilizzi la crittografia avanzata per la cifratura dell'accesso amministrativo non da console.	
12.1.1 Fornire istruzioni ai clienti per la cifratura di tutto l'accesso amministrativo non da console con crittografia avanzata per la gestione basata su Web e altre attività di accesso amministrativo non da console. ***Nota:*** *non utilizzare mai protocolli con testo in chiaro come Telnet o rlogin per l'accesso amministrativo.* ***In linea con il Requisito 2.3 PCI DSS***	**12.1.1** Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che vengano fornite istruzioni ai clienti e ai responsabili dell'integrazione/rivenditori per implementare la crittografia avanzata per la cifratura di tutto l'accesso amministrativo non da console.	I fornitori di applicazioni di pagamento dovranno fornire a clienti e responsabili dell'integrazione/rivenditori le istruzioni per configurare l'applicazione affinché utilizzi la crittografia avanzata per cifrare tutto l'accesso amministrativo non da console. In questo modo, si ha la certezza che i controlli di sicurezza vengono implementati in maniera corretta e che le linee guida PCI DSS e PA-DSS vengono rispettate.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
12.2 Utilizzare l'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console. ***Nota:*** *l'autenticazione a più fattori richiede l'utilizzo di almeno due dei tre metodi di autenticazione (fare riferimento al Requisito 3.1.4 PA-DSS per le descrizioni dei metodi di autenticazione).* ***In linea con il Requisito 8.3 PCI DSS***	**12.2.a** Verificare che l'autenticazione a più fattori sia fornita con l'applicazione o che ne venga richiesto l'uso.	L'accesso amministrativo richiede un maggiore livello di sicurezza garantendo l'identità dell'utente che tenta di ottenere l'accesso. Poiché l'autenticazione a più fattori può essere implementata a livello di applicazione, sistema o rete, non è necessario che tutte le applicazioni includano una soluzione di autenticazione a più fattori. I fornitori delle applicazioni possono fornire l'autenticazione a più fattori con la loro applicazione o includere istruzioni per utenti e responsabili dell'integrazione/rivenditori per installare l'autenticazione a più fattori per l'accesso amministrativo all'applicazione.
	12.2.b Esaminare la *Guida per l'implementazione del programma PA-DSS* preparata dal fornitore e verificare che vengano fornite istruzioni ai clienti e ai responsabili dell'integrazione/rivenditori per utilizzare l'autenticazione a più fattori, incluse: • istruzioni per l'uso dell'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console al CDE; • procedure per l'uso dell'autenticazione a più fattori fornita con l'eventuale applicazione.	
	12.2.c Se l'autenticazione a più fattori viene fornita con l'applicazione di pagamento, installare e testare l'applicazione per verificare che l'autenticazione a più fattori sia stata applicata prima che venga concesso l'accesso.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 13 - Gestire una Guida per l'implementazione del programma PA-DSS per clienti, rivenditori e responsabili dell'integrazione

Requisiti PA-DSS	Procedure di test	Istruzioni
13.1 Sviluppare, gestire e distribuire una *Guida per l'implementazione del programma PA-DSS* per clienti, rivenditori e responsabili dell'integrazione per:	**13.1** Esaminare la *Guida per l'implementazione del programma PA-DSS* e i relativi processi del fornitore e consultare il personale per verificare che: • la *Guida per l'implementazione del programma PA-DSS* venga distribuita a tutti i clienti, rivenditori e responsabili dell'integrazione insieme all'applicazione; • il fornitore abbia messo a punto un meccanismo per fornire la *Guida per l'implementazione del programma PA-DSS* a clienti, rivenditori e responsabili dell'integrazione su richiesta.	Una *Guida per l'implementazione del programma PA-DSS* ben concepita e molto dettagliata aiuta i clienti e i responsabili dell'integrazione/rivenditori a implementare le configurazioni e le misure di sicurezza adeguate nell'applicazione di pagamento e nei componenti sottostanti, per rispettare le linee guida PCI DSS e PA-DSS di protezione dei dati dei titolari di carta.
13.1.1 Fornire importanti informazioni specifiche per l'applicazione a clienti, rivenditori e responsabili dell'integrazione.	**13.1.1** Esaminare la *Guida per l'implementazione del programma PA-DSS* e verificare che: • indichi chiaramente il nome dell'applicazione di pagamento e la versione di riferimento; • fornisca dettagli su tutte le dipendenze dell'applicazione necessarie per configurare l'applicazione in conformità allo standard PCI DSS.	
13.1.2 Soddisfare tutti i requisiti descritti nel presente documento ovunque siano citati nella *Guida per l'implementazione del programma PA-DSS*.	**13.1.2** Esaminare la *Guida per l'implementazione del programma PA-DSS* e, utilizzando l'Appendice A come riferimento, verificare che la *Guida per l'implementazione del programma PA-DSS* contenga informazioni su tutti i requisiti descritti nel presente documento.	
13.1.3 Includere una revisione almeno annuale e successiva a eventuali modifiche all'applicazione o ai requisiti PA-DSS e garantire gli aggiornamenti necessari per mantenere la documentazione al passo con tutte le modifiche all'applicazione, oltre che con i requisiti del presente documento.	**13.1.3.a** Esaminare la *Guida per l'implementazione del programma PA-DSS* e consultare il personale per verificare che la *Guida per l'implementazione del programma PA-DSS* venga revisionata: • Almeno una volta all'anno • In caso di modifiche all'applicazione • In caso di modifiche ai requisiti PA-DSS	Per ogni modifica all'applicazione, possono essere modificati o introdotti funzioni di sistema e, in alcuni casi, meccanismi di sicurezza critici per l'applicazione. Se la *Guida per l'implementazione del programma PA-DSS* non viene mantenuta aggiornata con le versioni più recenti

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
	13.1.3.b Verificare che la *Guida per l'implementazione del programma PA-DSS* sia aggiornata in base alle ultime: • Modifiche ai requisiti PA-DSS • Modifiche all'applicazione o alle sue dipendenze	dell'applicazione di pagamento, i clienti e i responsabili dell'integrazione/rivenditori potrebbero ignorare o configurare in modo errato i controlli di sicurezza critici per l'applicazione, consentendo a un aggressore di bypassare i meccanismi di sicurezza e compromettere dati sensibili.
	13.1.3.c Esaminare la *Guida per l'implementazione del programma PA-DSS* e i relativi processi del fornitore e consultare il personale per verificare che il fornitore abbia messo a punto un meccanismo per comunicare gli aggiornamenti a clienti, rivenditori e responsabili dell'integrazione e fornisca le versioni aggiornate quando necessario.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito 14 - Assegnare responsabilità PA-DSS al personale e gestire programmi di formazione per personale, clienti, rivenditori e responsabili dell'integrazione

Requisiti PA-DSS	Procedure di test	Istruzioni
14.1 Garantire la formazione per la sicurezza delle informazioni e il rispetto dello standard PA-DSS per il personale del fornitore con responsabilità PA-DSS almeno una volta all'anno.	**14.1** Controllare i materiali di formazione e consultare il personale responsabile per verificare che tutto il personale del fornitore con responsabilità PA-DSS riceva la formazione per la sicurezza delle informazioni e il rispetto dello standard PA-DSS almeno una volta all'anno.	Per assicurare una progettazione dell'applicazione di pagamento efficiente, che rispetti le linee guida PA-DSS, il personale del fornitore di applicazioni di pagamento deve conoscere a fondo lo standard PA-DSS e le proprie responsabilità riguardo alle valutazioni PA-DSS in corso. È responsabilità del fornitore di applicazioni di pagamento garantire la corretta formazione del proprio personale in queste aree.
14.2 Assegnare ruoli e responsabilità al personale del fornitore, comprese le attività seguenti: • promuovere l'assunzione di responsabilità generali per soddisfare tutti i requisiti dello standard PA-DSS; • mantenersi aggiornati sulle modifiche apportate alla Guida del programma PA-DSS PCI SSC; • garantire il rispetto di pratiche di codifica sicure; • garantire la corretta formazione dei responsabili dell'integrazione/rivenditori e la diffusione dei materiali di supporto;	**14.2.a** Esaminare le responsabilità documentate per verificare che la responsabilità per i ruoli seguenti sia stata formalmente assegnata: • promuovere l'assunzione di responsabilità generali per soddisfare tutti i requisiti dello standard PA-DSS; • mantenersi aggiornati sulle modifiche apportate alla Guida del programma PA-DSS PCI SSC; • garantire il rispetto di pratiche di codifica sicure; • garantire la corretta formazione dei responsabili dell'integrazione/rivenditori e la diffusione dei materiali di supporto; • garantire la formazione di tutto il personale del fornitore con responsabilità PA-DSS, compresi gli sviluppatori.	All'interno di ogni organizzazione del fornitore di applicazioni di pagamento, a ogni figura responsabile (singola persona o team) deve essere assegnata una responsabilità PA-DSS formale, per garantire il rispetto di tutti i requisiti PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
• garantire la formazione di tutto il personale del fornitore con responsabilità PA-DSS, compresi gli sviluppatori.	**14.2.b** Consultare il personale a cui sono state assegnate le responsabilità per i ruoli seguenti per avere la conferma che ruoli e responsabilità sono stati definiti e compresi: • promuovere l'assunzione di responsabilità generali per soddisfare tutti i requisiti dello standard PA-DSS; • mantenersi aggiornati sulle modifiche apportate alla Guida del programma PA-DSS PCI SSC; • garantire il rispetto di pratiche di codifica sicure; • garantire la corretta formazione dei responsabili dell'integrazione/rivenditori e la diffusione dei materiali di supporto; • garantire la formazione di tutto il personale del fornitore con responsabilità PA-DSS, compresi gli sviluppatori.	
14.3 Sviluppare e implementare programmi di formazione e comunicazione per responsabili dell'integrazione e rivenditori dell'applicazione di pagamento. La formazione deve prevedere almeno i seguenti punti: • come implementare l'applicazione di pagamento e i sistemi e le reti correlati in modo conforme allo standard PCI DSS; • copertura di tutte le voci indicate per la *Guida per l'implementazione del programma PA-DSS* in questo documento (e nell'Appendice A).	**14.3.a** Esaminare i materiali di formazione per i responsabili dell'integrazione e i rivenditori e confermare che i materiali comprendono: • formazione su come implementare l'applicazione di pagamento e i sistemi e le reti correlati in modo conforme allo standard PCI DSS; • copertura di tutte le voci indicate per la *Guida per l'implementazione del programma PA-DSS* in questo documento (e nell'Appendice A).	Configurazione, gestione o supporto errati di un'applicazione possono determinare la comparsa di vulnerabilità della sicurezza nell'ambiente dei dati dei titolari di carta del cliente, che potrebbero essere sfruttate dagli aggressori. I fornitori di applicazioni devono garantire la formazione dei responsabili dell'integrazione/rivenditori per l'installazione e la configurazione sicure dell'applicazione, per assicurarsi che l'applicazione installata nell'ambiente del cliente faciliti il rispetto dello standard PCI DSS. È responsabilità del fornitore di applicazioni di pagamento garantire la formazione dei responsabili dell'integrazione e dei rivenditori in queste aree.
	14.3.b Esaminare i programmi di comunicazione del fornitore e i relativi processi e consultare il personale del fornitore per verificare che: • ai responsabili dell'integrazione e ai rivenditori vengano forniti i materiali di formazione; • il fornitore abbia messo a punto un meccanismo per fornire i materiali aggiornati ai responsabili dell'integrazione e ai rivenditori su richiesta.	
	14.3.c Consultare un campione di responsabili dell'integrazione e di rivenditori per verificare che abbiano ricevuto formazione e materiali per la formazione dal fornitore dell'applicazione.	
	14.3.d Esaminare le prove che responsabili dell'integrazione e rivenditori abbiano ricevuto i materiali di formazione dal fornitore del software.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Procedure di test	Istruzioni
14.3.1 Riesaminare i materiali di formazione almeno ogni anno e in caso di modifiche all'applicazione o ai requisiti PA-DSS. Aggiornare i materiali di formazione in base alle necessità per mantenere la documentazione al passo con le nuove versioni dell'applicazione di pagamento e le modifiche ai requisiti PA-DSS.	**14.3.1.a** Esaminare i materiali di formazione per i responsabili dell'integrazione e i rivenditori e verificare che i materiali vengano: • riesaminati almeno ogni anno e in caso di modifiche all'applicazione o ai requisiti PA-DSS; • aggiornati in base alle necessità per mantenere la documentazione al passo con le nuove versioni dell'applicazione di pagamento e le modifiche ai requisiti PA-DSS.	I materiali di formazione per il personale del fornitore di applicazioni di pagamento, i responsabili dell'integrazione e i rivenditori devono essere aggiornati almeno ogni anno per essere al passo con le ultime versioni delle applicazioni e dei requisiti PA-DSS. L'uso di materiali di formazione non aggiornati può rendere inefficaci i programmi di formazione e determinare un'inadeguata progettazione delle funzioni di sicurezza dell'applicazione o un'errata configurazione dell'applicazione da parte di responsabili dell'integrazione e rivenditori.
	14.3.1.b Esaminare il processo di distribuzione di nuove versioni di applicazioni di pagamento e verificare che la documentazione aggiornata sia stata distribuita a responsabili dell'integrazione e rivenditori con l'applicazione aggiornata.	
	14.3.1.c Consultare un campione di responsabili dell'integrazione e di rivenditori per verificare che abbiano ricevuto materiali di formazione aggiornati dal fornitore dell'applicazione.	

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Appendice A: Riepilogo del contenuto della *Guida per l'implementazione del programma PA-DSS*

Lo scopo di questa Appendice è riepilogare i requisiti PA-DSS correlati agli argomenti della *Guida per l'implementazione del programma PA-DSS,* per spiegare il contenuto della *Guida per l'implementazione del programma PA-DSS* fornita ai clienti e ai responsabili dell'integrazione/rivenditori (vedere "Guida per l'implementazione del programma PA-DSS" a pagina 11) e assegnare le responsabilità per l'implementazione dei controlli correlati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
1.1.4	Eliminazione dati sensibili di autenticazione memorizzati da versioni precedenti dell'applicazione di pagamento.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ i dati cronologici devono essere rimossi (dati della striscia magnetica, codici di verifica della carta, PIN o blocchi PIN memorizzati da precedenti versioni dell'applicazione di pagamento); ▪ modalità di rimozione dei dati cronologici; ▪ tale rimozione è assolutamente necessaria per garantire la conformità allo standard PCI DSS.	**Fornitori di software**: fornire strumento o procedura ai clienti per rimuovere in modo sicuro i dati sensibili di autenticazione memorizzati da precedenti versioni, in conformità al Requisito 1.1.4 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: eliminare tutti i dati cronologici in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 1.1.4 PA-DSS.
1.1.5	Eliminazione dei dati sensibili di autenticazione (prima dell'autorizzazione) raccolti in seguito alla risoluzione di problemi con l'applicazione di pagamento.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ i dati sensibili di autenticazione (prima dell'autorizzazione) devono essere raccolti solo quando necessario per risolvere un problema specifico; ▪ tali dati devono essere memorizzati solo in posizioni specifiche e note con accesso limitato; ▪ raccogliere solo la quantità di dati limitata necessaria per risolvere un problema specifico; ▪ i dati sensibili di autenticazione devono essere cifrati al momento della memorizzazione; ▪ tali dati devono essere eliminati in modo sicuro immediatamente dopo l'uso.	**Fornitori di software**: non memorizzare dati sensibili di autenticazione ed eseguire le operazioni di risoluzione di problemi dei clienti in conformità al Requisito 1.1.5.a PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori:** non memorizzare dati sensibili di autenticazione e risolvere eventuali problemi in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 1.1.5.a PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
2.1	Rimozione sicura dei dati dei titolari di carta dopo il periodo di conservazione definito dal cliente.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ i dati dei titolari di carta che superano il periodo di conservazione definito dal cliente devono essere eliminati; ▪ un elenco di tutte le posizioni in cui l'applicazione di pagamento memorizza i dati dei titolari di carta (in modo che il cliente conosca le posizioni dei dati da eliminare); ▪ istruzioni necessarie affinché i clienti eliminino in modo sicuro i dati dei titolari di carta quando non sono più utili a fini legali, normativi o commerciali; ▪ istruzioni per eliminare in modo sicuro i dati dei titolari di carta memorizzati dall'applicazione di pagamento, compresi i dati memorizzati nei sistemi o nel software sottostanti (come sistema operativo, database, ecc.); ▪ istruzioni per configurare i sistemi o il software sottostante (quali OS, database, ecc.) per impedire l'acquisizione o la conservazione involontaria di dati dei titolari di carta.	**Fornitori di software**: fornire istruzioni ai clienti relativamente alla rimozione dei dati dei titolari di carta che superano i periodi di conservazione definiti dai clienti, alle posizioni in cui l'applicazione di pagamento e il software sottostante memorizzano tali dati e alla modalità con cui i dati dei titolari di carta memorizzati dall'applicazione di pagamento possono essere rimossi in modo sicuro. **Clienti e responsabili dell'integrazione/rivenditori**: rimuovere in modo sicuro i dati dei titolari di carta che superano i periodi di conservazione definiti dai clienti, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.1 PA-DSS.
2.2	Mascherare il PAN quando visualizzato in modo che solo il personale con un'esigenza aziendale legittima possa vedere più di sei cifre all'inizio/quattro cifre alla fine del PAN.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ dettagli di tutte le istanze in cui il PAN viene visualizzato, compresi, a titolo di esempio, dispositivi POS, schermi, registri e ricevute; ▪ conferma che, per impostazione predefinita, l'applicazione di pagamento maschera il PAN in tutte le visualizzazioni; ▪ istruzioni per la configurazione dell'applicazione di pagamento in modo che solo il personale con un'esigenza aziendale legittima possa vedere più di sei cifre all'inizio/quattro cifre alla fine del PAN (include la visualizzazione dell'intero numero PAN).	**Fornitori di software**: fornire istruzioni ai clienti per la mascheratura del PAN in modo che solo il personale con un'esigenza aziendale legittima possa vedere più di sei cifre all'inizio/quattro cifre alla fine del PAN. **Clienti e responsabili dell'integrazione/rivenditori**: mascherare il PAN in modo che solo il personale con un'esigenza aziendale legittima possa vedere più di sei cifre all'inizio/quattro cifre alla fine del PAN, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.2 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
2.3	Conservazione di un PAN illeggibile ovunque sia memorizzato (inclusi i dati su supporti digitali portatili, supporti di backup, registri).	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ dettagli di tutte le opzioni configurabili per ogni metodo utilizzato dall'applicazione per rendere i dati dei titolari di carta illeggibili e istruzioni su come configurare ogni metodo per tutte le posizioni in cui i dati dei titolari di carta vengono memorizzati dall'applicazione di pagamento (per Requisito 2.1 PA-DSS); ▪ un elenco di tutte le istanze in cui i dati dei titolari di carta possono rappresentare un output che il cliente memorizza al di fuori dell'applicazione di pagamento e istruzioni che spiegano che il cliente è responsabile dell'illeggibilità del PAN in tutte le istanze di questo tipo; ▪ istruzioni per cui se i log di debugging sono sempre abilitati (ad esempio, per le finalità della risoluzione dei problemi) e i log includono il PAN, devono essere protetti in base a PCI DSS, disabilitati non appena viene completata la risoluzione dei problemi ed eliminati in modo sicuro quando non sono più necessari.	**Fornitori di software**: fornire ai clienti istruzioni per rendere il PAN illeggibile ovunque sia memorizzato o generato come output dall'applicazione. **Clienti e responsabili dell'integrazione/rivenditori**: rendere il PAN illeggibile ovunque sia memorizzato, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.3 PA-DSS.
2.4	Proteggere le chiavi usate per rendere sicuri i dati dei titolari di carta da divulgazione e uso improprio.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ limitare l'accesso alle chiavi al minor numero possibile di persone necessarie; ▪ memorizzare le chiavi in modo sicuro nel minor numero possibile di posizioni e moduli.	**Fornitori di software**: fornire istruzioni ai clienti relativamente alle chiavi usate per proteggere i dati dei titolari di carta che dovrebbero essere memorizzate in modo sicuro nel minor numero possibile di posizioni, limitando inoltre l'accesso alle chiavi al minor numero possibile di persone necessarie. **Clienti e responsabili dell'integrazione/rivenditori**: memorizzare le chiavi in modo sicuro nel minor numero possibile di posizioni e limitare l'accesso alle chiavi al minor numero possibile di persone necessarie, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.4 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
2.5	Implementazione di processi e procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati dei titolari di carta.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ in che modo generare, distribuire, proteggere, modificare, memorizzare e ritirare/sostituire in modo sicuro le chiavi di crittografia, nei casi in cui i clienti o i responsabili dell'integrazione/rivenditori siano coinvolti in queste attività per la gestione delle chiavi; ▪ un modulo campione per i custodi delle chiavi con cui accettano e confermano di conoscere le proprie responsabilità.	**Fornitori di software**: fornire istruzioni ai clienti che hanno accesso alle chiavi di crittografia usate per cifrare i dati dei titolari di carta per implementare i processi e le procedure di gestione delle chiavi. **Clienti e responsabili dell'integrazione/rivenditori**: implementare i processi e le procedure di gestione delle chiavi per le chiavi di crittografia usate per cifrare i dati dei titolari di carta in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.5 PA-DSS.
2.5.1 - 2.5.7	Implementazione di funzioni sicure di gestione delle chiavi	Fornire istruzioni a clienti e responsabili dell'integrazione/rivenditori su come utilizzare le funzioni di gestione delle chiavi, comprese: ▪ generazione di chiavi di crittografia avanzata; ▪ distribuzione sicura delle chiavi di crittografia; ▪ memorizzazione sicura delle chiavi di crittografia; ▪ modifica delle chiavi di crittografia giunte al termine del periodo di validità definito; ▪ ritiro o sostituzione delle chiavi, in base alle necessità, in caso di indebolimento dell'integrità della chiave o di sospetta compromissione delle chiavi; ▪ split knowledge e controllo duale di tutte le operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro supportate dall'applicazione; ▪ prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia.	**Fornitori di software**: fornire ai clienti istruzioni per l'implementazione di funzioni sicure di gestione delle chiavi. **Clienti e responsabili dell'integrazione/rivenditori**: implementare funzioni sicure di gestione delle chiavi di crittografia in conformità alla *Guida per l'implementazione del programma PA-DSS* e ai Requisiti 2.5.1 - 2.5.7 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
2.6	Rendere impossibili da recuperare il materiale di chiavi di crittografia o i crittogrammi memorizzati da precedenti versioni dell'applicazione di pagamento.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ procedure che spiegano in modo dettagliato come usare lo strumento o la procedura fornita con l'applicazione per rendere impossibile il recupero del materiale crittografico; ▪ chiarimento della necessità di rendere irrecuperabile il materiale delle chiavi di crittografia ogni volta che le chiavi non vengono più utilizzate e in conformità ai requisiti di gestione delle chiavi illustrati nello standard PCI DSS; ▪ modalità di ricifratura dei dati cronologici con chiavi nuove, comprese le procedure per garantire la sicurezza dei dati con testo in chiaro durante il processo di decifratura/ricifratura.	**Fornitori di software**: fornire strumenti o procedure per rimuovere in modo sicuro chiavi di crittografia o crittogrammi memorizzati dall'applicazione e fornire strumenti o procedure per eseguire nuovamente la cifratura dei dati cronologici con nuove chiavi. **Clienti e responsabili dell'integrazione/rivenditori**: rimuovere tutti i dati crittografici cronologici in base ai requisiti di gestione delle chiavi conformemente alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.6 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
3.1	Uso di ID utente univoci e autenticazione sicura per l'accesso amministrativo e l'accesso ai dati dei titolari di carta.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ indicazioni su come l'applicazione di pagamento applica l'autenticazione sicura per tutte le credenziali di autenticazione (ad esempio utenti, password) generate o gestite dall'applicazione: – applicando modifiche sicure alle credenziali di autenticazione per il completamento dell'installazione in conformità ai requisiti da 3.1.1 a 3.1.11 PA-DSS – applicando modifiche sicure alle credenziali di autenticazione per qualsiasi modifica successiva (all'installazione) in conformità ai requisiti da 3.1.1 a 3.1.11 PA-DSS ▪ per garantire la conformità allo standard PCI DSS, qualsiasi modifica apportata alle configurazioni di autenticazione deve essere verificata per accertarsi che fornisca metodi di autenticazione che siano rigidi almeno quanto i requisiti PCI DSS; ▪ indicazioni su come assegnare metodi di autenticazione sicura agli account predefiniti nell'ambiente; ▪ indicazioni su come assegnare metodi di autenticazione sicura agli account predefiniti (anche se non verranno utilizzati) e disabilitare o non utilizzare gli account; ▪ modalità di modifica e creazione delle credenziali di autenticazione quando le stesse non sono generate o gestite dall'applicazione di pagamento, in conformità ai Requisiti da 3.1.1 a 3.1.11 PA DSS, al completamento dell'installazione e per modifiche successive all'installazione, per tutti gli account a livello di applicazione con accesso amministrativo o accesso ai dati dei titolari di carta. ▪ identificazione di tutti i ruoli e account predefiniti all'interno dell'applicazione con accesso amministrativo.	**Fornitori di software**: per tutte le credenziali di autenticazione generate o gestite dall'applicazione, assicurare che tale applicazione applichi l'uso del cliente di ID utente univoci e di autenticazione sicura per account/password, in conformità ai Requisiti da 3.1.1 a 3.1.11 PA-DSS. Quando le credenziali di autenticazione non sono generate o gestite dall'applicazione di pagamento, assicurare che la *Guida per l'implementazione del programma PA-DSS* fornisca istruzioni chiare ed univoche ai clienti e ai responsabili dell'integrazione/rivenditori relativamente alla modifica e alla creazione di credenziali di autenticazione sicure in conformità ai Requisiti da 3.1.1 a 3.1.11 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: definire e gestire autenticazione sicura e ID utenti univoci in conformità alla*Guida per l'implementazione del programma PA-DSS* e ai Requisiti da 3.1.1 a 3.1.11 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
3.2	Uso di nomi utente univoci e autenticazione sicura per l'accesso a PC, server e database con l'applicazione di pagamento.	Fornire a clienti e responsabili dell'integrazione/rivenditori le istruzioni per utilizzare nomi utente univoci e metodi di autenticazione sicura per l'accesso a PC, server e database con le applicazioni di pagamento e/o ai dati dei titolari di carta, in conformità ai Requisiti da 3.1.1 a 3.1.11 PA-DSS.	**Fornitori di software**: assicurare che l'applicazione di pagamento supporti l'uso di ID utente univoci e autenticazione sicura del cliente per gli account e le password se impostati dal fornitore per accedere a PC, server e database, in conformità ai Requisiti da 3.1.2 a 3.1.9 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: definire e gestire autenticazione sicura e ID utenti univoci in conformità alla*Guida per l'implementazione del programma PA-DSS* e ai Requisiti da 3.1.1 a 3.1.11 PA-DSS.
4.1	Implementazione di audit trail automatici.	Fornire istruzioni per l'implementazione di audit trail automatici che spieghino: ▪ come installare l'applicazione affinché i registri vengano configurati e abilitati per impostazione predefinita al completamento del processo di installazione; ▪ come definire le impostazioni dei registri conformi a PCI DSS, in base ai Requisiti 4.2, 4.3 e 4.4 PA-DSS, per qualsiasi opzione di registrazione che sia configurabile dal cliente dopo l'installazione; ▪ I registri devono essere attivati e la disattivazione dei registri determinerà una non conformità allo standard PCI DSS. ▪ come configurare le impostazioni dei registri conformi a PCI DSS per qualsiasi componente software di terzi fornito con l'applicazione di pagamento o da essa richiesto, per qualsiasi opzione di registrazione che sia configurabile dal cliente dopo l'installazione.	**Fornitori di software**: assicurare che l'applicazione di pagamento supporti l'uso del cliente di registri conformi ai Requisiti 4.2, 4.3 e 4.4 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori:** definire e gestire registri conformi allo standard PCI DSS in base alle indicazioni di cui alla *Guida per l'implementazione del programma PA-DSS* e ai Requisiti 4.2, 4.3 e 4.4 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
4.4	Facilitare la generazione centralizzata dei registri.	Fornire una descrizione dei meccanismi di registrazione centralizzata supportati e le istruzioni e le procedure per l'inserimento dei registri dell'applicazione di pagamento nel server per la generazione centralizzata dei registri.	**Fornitori di software**: assicurare che l'applicazione di pagamento supporti la generazione centralizzata di registri in ambienti del cliente in conformità al Requisito 4.4 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori:** definire e gestire registri centralizzati in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 4.4. PA-DSS.
5.4.4	Implementazione e comunicazione della metodologia di versioning dell'applicazione.	Fornire una descrizione della metodologia di versioning pubblicata dal fornitore e includere linee guida per: ▪ dettagli dello schema di versioning, compreso il formato dello schema di versione (numero di elementi, separatori, set di caratteri, ecc.); ▪ dettagli su come verranno indicate le modifiche con effetti sulla sicurezza nello schema di versioning; ▪ dettagli su come altri tipi di modifiche avranno effetti sulla versione; ▪ dettagli su eventuali caratteri jolly utilizzati, compreso il fatto che non verranno mai utilizzati per rappresentare una modifica con effetti sulla sicurezza.	**Fornitori di software**: documentare e implementare una metodologia di versioning del software durante il ciclo di sviluppo del sistema. La metodologia deve rispettare le procedure riportate nella *Guida del programma PA-DSS* per le modifiche alle applicazioni di pagamento, in conformità al Requisito 5.5 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori:** comprendere quale versione dell'applicazione di pagamento si sta utilizzando e verificare che si tratti di versioni convalidate.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
6.1	Implementazione sicura di tecnologia wireless.	Per le applicazioni di pagamento sviluppate per tecnologie wireless, i clienti e i responsabili dell'integrazione/rivenditori devono ricevere: ▪ istruzione che l'applicazione di pagamento applica le modifiche a chiavi di cifratura predefinite, password e stringhe di comunità SNMP al momento dell'installazione per tutti i componenti wireless controllati dall'applicazione; ▪ procedure per modificare le chiavi di cifratura e le password wireless, comprese le stringhe SNMP, ogni volta che un utente a conoscenza delle chiavi/password lascia l'azienda o cambia sede; ▪ istruzioni per modificare chiavi di cifratura, password e stringhe di comunità SNMP predefinite per tutti i componenti wireless forniti con, ma non controllati da, l'applicazione di pagamento; ▪ istruzioni per installare un firewall tra le reti wireless e i sistemi che memorizzano dati dei titolari di carta; ▪ dettagli sull'eventuale traffico wireless (comprese informazioni su porte specifiche) che la funzione wireless dell'applicazione di pagamento utilizzerà; ▪ istruzioni per configurare i firewall affinché impediscano o controllino il traffico (qualora sia necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta.	**Fornitori di software**: fornire istruzioni a clienti e responsabili dell'integrazione/rivenditori spiegando che se si utilizza la tecnologia wireless con l'applicazione di pagamento, le impostazioni predefinite del fornitore per tale tecnologia devono essere modificate in base al Requisito 6.1 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: per il wireless implementato nell'ambiente di pagamento da clienti o responsabili dell'integrazione/rivenditori, modificare le impostazioni predefinite del fornitore in conformità al Requisito 6.1 PA-DSS e installare un firewall in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 2.1.1 PCI DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
6.2	Protezione delle trasmissioni di dati dei titolari di carta su reti wireless	Per le applicazioni di pagamento sviluppate per l'uso con tecnologia wireless, includere istruzioni per l'uso delle migliori pratiche di settore (ad esempio, IEEE 802.11i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione dei dati dei titolari di carta. Le istruzioni spiegano: ▪ come configurare l'applicazione per utilizzare le migliori pratiche di settore (ad esempio IEEE 802.11.i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione; ▪ come configurare tutte le applicazioni wireless associate all'applicazione per utilizzare le migliori pratiche di settore per implementare la cifratura avanzata per l'autenticazione e la trasmissione.	**Fornitori di software**: fornire istruzioni a clienti e responsabili dell'integrazione/rivenditori spiegando che se si utilizza la tecnologia wireless con l'applicazione di pagamento, occorre eseguire la cifratura dei dati per la trasmissione in conformità al Requisito 6.2 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: per la tecnologia wireless implementata nell'ambiente di pagamento da clienti o responsabili dell'integrazione/rivenditori, utilizzare trasmissioni cifrate sicure in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 6.2 PA-DSS.
6.3	Fornitura di istruzioni per l'uso sicuro della tecnologia wireless.	Fornire istruzioni per configurare impostazioni wireless conformi allo standard PCI DSS, comprese: ▪ istruzioni per modificare tutte le chiavi, password e stringhe di comunità SNMP della cifratura wireless predefinita al momento dell'installazione; ▪ istruzioni per modificare chiavi, password e stringhe di comunità SNMP della cifratura wireless ogni volta che un utente a conoscenza delle chiavi/password lascia l'azienda o cambia sede; ▪ istruzioni per installare un firewall tra le reti wireless e i sistemi dove sono conservati i dati dei titolari di carta e configurare tali firewall per negare o controllare il traffico (se necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta; ▪ istruzioni per utilizzare le migliori pratiche di settore (ad esempio IEEE 802.11.i) per fornire una cifratura avanzata per l'autenticazione e la trasmissione.	**Fornitori di software**: fornire istruzioni a clienti e responsabili dell'integrazione/rivenditori per mettere in sicurezza le tecnologie wireless in base al Requisito 6.3 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: mettere in sicurezza le tecnologie wireless in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 6.2. PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
7.2.3	Fornire istruzioni per i clienti sull'installazione sicura di patch e aggiornamenti.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: • comunicazione delle notifiche di nuovi patch e aggiornamenti da parte del fornitore; • consegna di patch e aggiornamenti in modo sicuro mediante "canali affidabili"; • accesso e installazione di patch e aggiornamenti in modo da mantenere l'integrità del relativo codice.	**Fornitori di software:** documentare e implementare processi per la comunicazione, la distribuzione e l'installazione sicura di patch e aggiornamenti. **Clienti e responsabili dell'integrazione/rivenditori:** accedere e installare patch e aggiornamenti in maniera sicura, in base alla *Guida per l'implementazione del programma PA-DSS*.
8.2	Usare solo servizi, protocolli, componenti necessari e sicuri e software e hardware dipendenti, compresi quelli forniti da terze parti.	Documentare tutti i protocolli, servizi, componenti necessari e software e hardware dipendenti che servono per ogni funzionalità dell'applicazione di pagamento.	**Fornitori di software:** assicurare che l'applicazione di pagamento supporti l'uso del cliente solo dei protocolli, servizi, ecc. necessari e sicuri, 1) avendo solo i protocolli, servizi, ecc. necessari, stabiliti pronti per l'uso per impostazione predefinita, 2) avendo solo quei protocolli, servizi, ecc. necessari configurati in modo sicuro automaticamente e 3) documentando tutti protocolli, servizi, ecc. necessari, come riferimento per clienti e responsabili dell'integrazione/rivenditori. **Clienti e responsabili dell'integrazione/rivenditori:** utilizzare l'elenco documentato contenuto nella *Guida per l'implementazione del programma PA-DSS* per assicurare l'uso nel sistema solo di protocolli, servizi, ecc. necessari e sicuri, in conformità al Requisito 5.4 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
9.1	Memorizzazione di dati dei titolari di carta solo su server non connessi a Internet	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ istruzioni per non memorizzare dati dei titolari di carta su sistemi rivolti al pubblico (ad esempio i server Web e i database server non devono trovarsi sullo stesso server); ▪ istruzioni su come configurare l'applicazione di pagamento per utilizzare una zona DMZ per separare Internet dai sistemi che memorizzano dati dei titolari di carta; ▪ un elenco di servizi/porte che l'applicazione deve utilizzare per comunicare in due zone di rete (per consentire al cliente di configurare il firewall in modo che si aprano solo le porte necessarie).	**Fornitori di software**: assicurare che l'applicazione di pagamento non richieda la memorizzazione di dati dei titolari di carta nella zona DMZ o su sistemi accessibili via Internet e consenta di utilizzare un'area DMZ, in conformità al Requisito 9 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: definire e gestire applicazioni di pagamento in modo che i dati dei titolari di carta non vengano memorizzati su sistemi accessibili via Internet, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 9 PA-DSS
10.1	Implementazione dell'autenticazione a più fattori per tutto l'accesso remoto all'applicazione di pagamento originato al di fuori dell'ambiente del cliente.	I clienti e i responsabili dell'integrazione/rivenditori devono ricevere le istruzioni seguenti: ▪ istruzioni che stabiliscono che tutto l'accesso remoto all'applicazione di pagamento originato al di fuori della rete del cliente debba utilizzare l'autenticazione a più fattori per soddisfare i requisiti PCI DSS; ▪ descrizione dei meccanismi di autenticazione a più fattori supportati dall'applicazione; ▪ istruzioni per la configurazione dell'applicazione affinché supporti l'autenticazione a più fattori (almeno due dei tre metodi di autenticazione descritti nel Requisito 3.1.4 PA DSS).	**Fornitori di software**: assicurarsi che l'applicazione di pagamento supporti l'uso da parte dei clienti dell'autenticazione a più fattori per tutto l'accesso remoto all'applicazione di pagamento originato al di fuori dell'ambiente del cliente, in conformità al Requisito 10.2 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: definire e mantenere l'autenticazione a più fattori per tutto l'accesso remoto all'applicazione di pagamento originato al di fuori dell'ambiente del cliente, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 10.2 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
10.2.1	Consegna sicura di aggiornamenti in remoto di applicazioni di pagamento.	Se gli aggiornamenti dell'applicazione di pagamento vengono consegnati tramite accesso remoto ai sistemi dei clienti, fornire le istruzioni seguenti: ▪ istruzioni per attivare le tecnologie di accesso remoto per gli aggiornamenti dell'applicazione di pagamento solo quando necessario per scaricare gli aggiornamenti e spegnerle immediatamente una volta completata l'operazione, in conformità al Requisito 12.3.9 PCI DSS; ▪ se il computer è collegato tramite VPN o altra connessione ad alta velocità, istruzioni per ricevere gli aggiornamenti dell'applicazione di pagamento in remoto mediante un firewall configurato in modo sicuro o un firewall personale, in conformità al Requisito 1 PCI DSS.	**Fornitori di software**: consegnare in modo sicuro gli aggiornamenti in remoto dell'applicazione di pagamento in conformità allo standard 10.3 PA-DSS **Clienti e responsabili dell'integrazione/rivenditori**: ricevere in modo sicuro aggiornamenti in remoto dell'applicazione di pagamento dal fornitore, in conformità alla *Guida per l'implementazione del programma PA-DSS*, al Requisito 10.3 PA-DSS e al Requisito 1 PCI DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
10.2.3	Implementazione sicura del software di accesso remoto.	Includere istruzioni che spiegano che ogni accesso remoto all'applicazione di pagamento deve essere implementato in modo sicuro, ad esempio con i metodi seguenti: ▪ modifica delle impostazioni predefinite del software di accesso remoto (ad esempio, modifica delle password predefinite e uso di password univoche per ciascun cliente); ▪ Possibilità di connessioni solo da indirizzi IP/MAC (noti) specifici. ▪ uso di autenticazione di password avanzate e di password complesse per i login (vedere i Requisiti da 3.1.1 a 3.1.11 PA-DSS); ▪ abilitazione della trasmissione di dati cifrati in conformità al Requisito 12.1 PA-DSS; ▪ abilitazione del lockout dell'account dopo un determinato numero di login non riusciti (vedere il Requisito 3.1.9 e 3.1.10 PA-DSS); ▪ attivazione di una connessione VPN tramite firewall prima che venga concesso l'accesso; ▪ Abilitazione della funzione di registrazione in file di log. ▪ limitazione dell'accesso agli ambienti dei clienti per responsabili dell'integrazione/rivenditori autorizzati.	**Fornitori di software**: (1) se il fornitore può accedere alle applicazioni di pagamento dei clienti in remoto, implementare un accesso remoto sicuro come quello specificato nel Requisito 10.3.2 PA-DSS; (2) accertarsi che l'applicazione di pagamento supporti l'uso delle funzioni di sicurezza dell'accesso remoto dei clienti. **Clienti e responsabili dell'integrazione/rivenditori**: utilizzare le funzioni di sicurezza dell'accesso remoto per ogni accesso remoto alle applicazioni di pagamento, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 10.3.2 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
11.1	Protezione delle trasmissioni di dati dei titolari di carta su reti pubbliche	Se l'applicazione di pagamento consente o facilita l'invio di dati dei titolari di carta tramite reti pubbliche, includere le istruzioni per implementare e utilizzare protocolli di crittografia e sicurezza avanzati per la trasmissione di dati dei titolari di carta su reti pubbliche, comprese: ▪ istruzioni per utilizzare protocolli di crittografia e sicurezza avanzati se vengono trasmessi dati dei titolari di carta tramite reti pubbliche; ▪ istruzioni che spiegano quali sono i certificati e/o le chiavi affidabili accettati; ▪ istruzioni per configurare l'applicazione di pagamento affinché utilizzi solo versioni e implementazioni sicure dei protocolli di sicurezza; ▪ istruzioni per configurare l'applicazione di pagamento per impedire il fallback a una configurazione o una versione non sicura (ad es. se si utilizza TLS, l'applicazione non deve consentire il fallback a SSL); ▪ istruzioni per configurare l'applicazione di pagamento affinché utilizzi il livello di cifratura corretto per la metodologia di cifratura in uso.	**Fornitori di software**: assicurare che l'applicazione di pagamento supporti l'uso del cliente di protocolli di crittografia e sicurezza avanzati per la trasmissione di dati dei titolari di carta tramite reti pubbliche, in conformità al Requisito 11.1 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: definire e gestire protocolli di crittografia e sicurezza avanzati per la trasmissione di dati dei titolari di carta, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 11.1 PA-DSS.
11.2	Cifratura dei dati dei titolari di carta inviati mediante tecnologie di messaggistica degli utenti finali.	Se l'applicazione di pagamento facilita l'invio di PAN mediante tecnologie di messaggistica degli utenti finali, includere le istruzioni per implementare e utilizzare una soluzione che renda il PAN illeggibile o che implementi la crittografia avanzata, comprese: ▪ procedure per utilizzare la soluzione indicata in modo che renda il PAN illeggibile o protegga il PAN con crittografia avanzata; ▪ istruzioni per far sì che il PAN sia reso illeggibile o sicuro con crittografia avanzata ogni volta che viene inviato mediante tecnologie di messaggistica degli utenti finali.	**Fornitori di software**: fornire o specificare l'uso di una soluzione che renda il PAN illeggibile o implementi la crittografia avanzata e garantisca che l'applicazione di pagamento supporta la cifratura o l'illeggibilità dei numeri PAN, se inviati tramite tecnologie di messaggistica degli utenti finali, in conformità al Requisito 11.2 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: rendere i PAN illeggibili o eseguire la cifratura con crittografia avanzata di tutti i numeri PAN inviati tramite tecnologie di messaggistica degli utenti finali, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 11.2 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisiti PA-DSS	Argomento PA-DSS	Contenuto obbligatorio della Guida per l'implementazione	Responsabilità per l'implementazione dei controlli
12.1	Cifratura dell'accesso amministrativo non da console	Se l'applicazione di pagamento facilita l'accesso amministrativo non da console, includere istruzioni su come configurare l'applicazione affinché utilizzi la crittografia avanzata per la cifratura di tutto l'accesso amministrativo non da console all'applicazione di pagamento o ai server nell'ambiente dei dati dei titolari di carta.	**Fornitori di software**: se l'applicazione di pagamento facilita l'accesso amministrativo non da console, assicurarsi che l'applicazione di pagamento implementi la cifratura avanzata per l'accesso amministrativo non da console, in conformità al Requisito 12.1 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: eseguire la cifratura di tutto l'accesso amministrativo non da console, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 12.1 PA-DSS.
12.1.1	Cifratura dell'accesso amministrativo non da console	includere istruzioni per clienti e responsabili dell'integrazione/rivenditori per implementare la crittografia avanzata per la cifratura di tutto l'accesso amministrativo non da console.	**Fornitori di software**: assicurarsi che l'applicazione di pagamento supporti la cifratura dell'accesso amministrativo non da console del cliente, in conformità al Requisito 12.1.1 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: eseguire la cifratura di tutto l'accesso amministrativo non da console, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 12.1.1 PA-DSS.
12.2	Uso dell'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console.	Includere istruzioni per clienti e responsabili dell'integrazione/rivenditori per utilizzare l'autenticazione a più fattori, incluse: • istruzioni per l'uso dell'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console al CDE; • procedure per l'uso dell'autenticazione a più fattori fornita con l'eventuale applicazione.	**Fornitori di software**: assicurarsi che l'applicazione di pagamento fornisca o specifichi l'uso dell'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console, in conformità al Requisito 12.2 PA-DSS. **Clienti e responsabili dell'integrazione/rivenditori**: utilizzare l'autenticazione a più fattori per tutto l'accesso amministrativo non da console, in conformità alla *Guida per l'implementazione del programma PA-DSS* e al Requisito 12.2 PA-DSS.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Appendice B - Configurazione del laboratorio di test per valutazioni PA-DSS

Per ciascuna valutazione PA-DSS condotta, il PA-QSA deve confermare lo stato e le capacità del laboratorio utilizzato per eseguire il test per la valutazione PA-DSS. Questa conferma deve essere inviata insieme al *ROV (Report of Validation)*.

Per ogni procedura di convalida laboratorio, il PA-QSA deve indicare se il laboratorio utilizzato per la valutazione e soggetto alle presenti procedure di convalida era il laboratorio del PA-QSA o il laboratorio del fornitore del software. I PA-QSA sono essenziali per gestire il laboratorio di test in modo che soddisfi tutti i requisiti sotto riportati e utilizzare il loro laboratorio per eseguire valutazioni, quando possibile. Il laboratorio del fornitore di software può essere utilizzato solo quando strettamente necessario (ad esempio se il PA-QSA non dispone di mainframe, AS400 o Tandem su cui viene eseguita l'applicazione di pagamento) e dopo aver verificato il rispetto di tutti i requisiti di laboratorio.

Il PA-QSA deve confermare tutti gli elementi della tabella seguente, oltre a:

- **identificare il luogo e il proprietario del laboratorio utilizzato per la revisione PA-DSS;**
- **descrivere l'architettura e l'ambiente di test del laboratorio per questa revisione PA-DSS;**
- **descrivere come l'uso nel mondo reale dell'applicazione di pagamento era simulato nel laboratorio per questa revisione PA-DSS.**

Il *modello di reporting ROV PA-DSS* fornisce dettagli sulla convalida del laboratorio, prevista per ogni valutazione.

Requisito laboratorio	Procedura di convalida laboratorio
1. Installare l'applicazione di pagamento in base alle istruzioni di installazione del fornitore o alla formazione fornita al cliente	**1.** Verificare che il manuale di installazione del fornitore o la formazione fornita ai clienti sia stata utilizzata per eseguire l'installazione predefinita dell'applicazione di pagamento su tutte le piattaforme elencate nel rapporto PA-DSS per simulare l'esperienza del cliente in tempo reale.
2. Installare e sottoporre a test tutte le versioni dell'applicazione di pagamento elencate nel rapporto PA-DSS	**2.a** Verificare che tutte le implementazioni comuni (incluse versioni specifiche di aree e paesi) dell'applicazione di pagamento da sottoporre a test siano state installate.
	2.b Verificare che tutte le versioni dell'applicazione di pagamento e le piattaforme siano state sottoposte a test, compresi tutti i componenti e le dipendenze di sistema necessari.
	2.c Verificare che tutte le funzionalità critiche dell'applicazione di pagamento per ogni versione siano state sottoposte a test.
3. Installare e implementare tutti i dispositivi di sicurezza richiesti dallo standard PCI DSS	**3.** Verificare che tutti i dispositivi di sicurezza richiesti dallo standard PCI DSS (ad esempio, firewall e software antivirus) siano stati implementati sui sistemi di test.
4. Installare e/o configurare tutte le impostazioni di sicurezza richieste dallo standard PCI DSS	**4.** Verificare che tutte le impostazioni del sistema e le patch conformi allo standard PCI DSS siano state implementate sui sistemi di test per sistemi operativi, software di sistema e applicazioni utilizzate dall'applicazione di pagamento.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito laboratorio	Procedura di convalida laboratorio
5. Simulare l'uso nel mondo reale dell'applicazione di pagamento	**5.a** Il laboratorio simula l'uso nel 'mondo reale' dell'applicazione di pagamento, inclusi tutti i sistemi e tutte le applicazioni in cui l'applicazione di pagamento è implementata. Ad esempio, un'implementazione standard di un'applicazione di pagamento potrebbe includere un ambiente client/server in un negozio con un sistema POS, tecnologia backoffice o rete aziendale. Il laboratorio simula l'implementazione completa.
	5.b Il laboratorio utilizza solo numeri di carta di prova per la simulazione e i test. I PAN attivi non vengono utilizzati per i test. ***Nota:*** *è possibile ottenere le carte di prova in genere dal fornitore, da un elaboratore o un acquirente.*
	5.c Il laboratorio esegue le funzioni di autorizzazione e/o contabilizzazione dell'applicazione di pagamento e tutto l'output viene esaminato in base alle istruzioni fornite al punto 6 seguente.
	5.d Il laboratorio e/o i processi associano tutto l'output prodotto dall'applicazione di pagamento per ogni possibile scenario: temporaneo, permanente, di elaborazione degli errori, di debug, di file di registro, ecc.
	5.e Il laboratorio e/o i processi simulano e convalidano tutte le funzioni dell'applicazione di pagamento, per includere la generazione di tutte le condizioni di errore e le voci di registro utilizzando dati "attivi" e dati non validi simulati.
6. Fornire capacità per le seguenti metodologie di test di penetrazione:	**6.a** Utilizzare strumenti/metodi forensi: vengono utilizzati strumenti/metodi forensi per ricercare in tutto l'output identificato la prova di dati sensibili di autenticazione (strumenti commerciali, script, ecc.), in base al Requisito 1.1.1-1.1.3 PA-DSS.[6]
	6.b Tentare di sfruttare le vulnerabilità dell'applicazione: le vulnerabilità correnti (ad esempio OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, ecc.) sono state utilizzate per cercare di sfruttare le applicazioni di pagamento, in conformità al Requisito 5.2 PA-DSS.
	6.c Il laboratorio e/o i processi hanno tentato di eseguire codice arbitrario durante il processo di aggiornamento dell'applicazione di pagamento: Eseguire il processo di aggiornamento con codice arbitrario in base al Requisito 7.2.2 PA-DSS.

[6] Strumento o metodo forense: uno strumento o un metodo per rilevare, analizzare e presentare dati forensi, che consentono di autenticare, ricercare e recuperare una prova su computer in modo rapido ed esauriente. Nel caso di strumenti o metodi forensi utilizzati dai PA-QSA, questi strumenti o metodi devono individuare accuratamente eventuali dati sensibili di autenticazione scritti dall'applicazione di pagamento. Tali strumenti possono essere commerciali, open-source o sviluppati in-house dal PA-QSA.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.

Requisito laboratorio	Procedura di convalida laboratorio
7. Utilizzare il laboratorio del fornitore SOLO dopo aver verificato che tutti i requisiti sono stati soddisfatti	Se è necessario utilizzare il laboratorio del fornitore del software (ad esempio il PA-QSA non dispone di mainframe, AS400, o Tandem su cui viene eseguita l'applicazione di pagamento), il PA-QSA può (1) utilizzare apparecchiature in prestito del fornitore o (2) utilizzare le funzionalità del laboratorio del fornitore, indicando tale scelta dettagliatamente nel rapporto insieme al luogo dei test. Per entrambe le opzioni, il PA-QSA verifica che l'apparecchiatura e il laboratorio del fornitore soddisfino i seguenti requisiti:
	7.a Il PA-QSA verifica che il laboratorio del fornitore soddisfi tutti i requisiti specificati in questo documento e inserisca tutti i dettagli nel rapporto.
	7.b Il PA-QSA deve convalidare l'installazione completa dell'ambiente del laboratorio remoto per assicurare l'effettiva simulazione da parte dell'ambiente di una situazione nel mondo reale e la mancata modifica o alterazione dell'ambiente in alcun modo da parte del fornitore.
	7.c Tutti i test vengono eseguiti dal PA-QSA (il fornitore non può eseguire test sulla propria applicazione).
	7.d Tutti i test vengono (1) eseguiti presso la sede del fornitore o (2) eseguiti in remoto mediante una connessione di rete utilizzando un collegamento sicuro (ad esempio VPN).
	7.e Utilizzare solo numeri di carta di prova per la simulazione/test. Non utilizzare PAN attivi. È possibile ottenere le carte utilizzate per i test in genere dal fornitore, da un elaboratore o un acquirente.
8. Mantenere un processo di controllo qualità (QA) efficiente.	**8.a** Il personale addetto al controllo qualità (QA) del PA-QSA verifica che tutte le versioni e le piattaforme identificate nel rapporto PA-DSS siano incluse nei test.
	8.b Il personale addetto al controllo qualità (QA) del PA-QSA verifica che vengano eseguiti tutti i test in base ai requisiti PA-DSS.
	8.c Il personale addetto al controllo qualità (QA) del PA-QSA verifica che le configurazioni e i processi del laboratorio del PA-QSA soddisfino i requisiti e siano documentati in modo accurato nel rapporto.
	8.d Il personale addetto al controllo qualità (QA) del PA-QSA verifica che il rapporto riporti accuratamente tutti i risultati dei test.

© 2006-2016 PCI Security Standards Council (Ente responsabile degli standard di protezione PCI), LLC. Tutti i diritti riservati.