

Settore delle carte di pagamento (PCI) Standard di protezione dei dati per le applicazioni di pagamento (PA-DSS)

**Riepilogo delle modifiche di PA-DSS
dalla versione 2.0 alla 3.0**

Novembre 2013

Introduzione

Il presente documento contiene un riepilogo delle modifiche apportate da PA-DSS v2.0 a PA-DSS v3.0. La tabella 1 fornisce una panoramica dei tipi di modifiche incluse in PA-DSS v3.0. La tabella 2 riportata nelle pagine seguenti fornisce un riepilogo delle modifiche materiali presenti in PA-DSS v3.0.

Tabella 1 - Tipi di modifiche

Tipo di modifica	Definizione
Chiarimento	Maggiori informazioni sullo scopo del requisito. Assicura che la formulazione sintetica nello standard presenti lo scopo desiderato dei requisiti.
Ulteriori istruzioni	Spiegazioni, definizioni e/o istruzioni per favorire la comprensione di o fornire ulteriori informazioni o istruzioni su un determinato argomento.
Requisito in evoluzione	Modifiche per assicurare che gli standard siano aggiornati alle minacce emergenti ed ai cambiamenti del mercato.

Tabella 2 - Riepilogo delle modifiche

Sezione		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
Introduzione	Introduzione	Scopo del documento Chiariti scopo e utilizzo del documento e incluso il riferimento al modello di reporting ROV PA-DSS.	Chiarimento
		Relazione tra PCI DSS e PA-DSS Chiarito che le applicazioni PA-DSS rientrano nella valutazione PCI DSS di un'organizzazione.	Chiarimento
Informazioni sull'applicabilità dello standard PCI DSS	Informazioni sull'applicabilità dello standard PCI DSS	Sezione riposizionata e aggiornata per allinearla alle modifiche applicate a PCI DSS. Rimossi alcuni termini di PCI DSS che non sono applicabili a PA-DSS.	Chiarimento
Ambito del programma PA-DSS	Ambito del programma PA-DSS	Rimosse le informazioni relative alle applicazioni di pagamento adatte per PA-DSS. Le informazioni sull'idoneità a PA-DSS sono incluse nella <i>Guida del programma PA-DSS</i> .	Chiarimento
Ruoli e responsabilità		Le informazioni riguardanti le persone interessate e i loro ruoli e responsabilità PA-DSS sono state rimosse poiché già incluse nella <i>Guida del programma PA-DSS</i> .	Chiarimento
Guida per l'implementazione del programma PA-DSS	Guida per l'implementazione del programma PA-DSS	Fornite ulteriori istruzioni sulla <i>Guida per l'implementazione del programma PA-DSS</i> e chiarito il ruolo di PA-QSA.	Ulteriori istruzioni
Istruzioni e contenuto per il rapporto di convalida	Istruzioni e contenuto per il rapporto di convalida	Contenuto riposizionato per separare il <i>modello di reporting ROV</i> .	Chiarimento
Operazioni di completamento del programma PA-DSS	Operazioni di completamento del programma PA-DSS	Sezione aggiornata per mettere in evidenza il processo di valutazione più che la documentazione (i dettagli sulla documentazione sono stati spostati nel <i>modello di reporting ROV</i>).	Chiarimento
Guida del programma PA-DSS	Guida del programma PA-DSS	Rimosso riferimento alla transizione PABP, poiché non esiste più un processo di transizione.	Chiarimento

Requisiti PCI DSS e procedure di valutazione della sicurezza	Requisiti PCI DSS e procedure di valutazione della sicurezza	Termini aggiunti per definire le intestazioni delle colonne in questa sezione e rimossi i riferimenti alle colonne "Presente", "Non presente" e "Data di destinazione/Commenti".	Chiarimento
--	--	--	-------------

Modifiche generali implementate per tutti i requisiti PA-DSS		Tipo
Nuova colonna "Istruzioni" per descrivere lo scopo o l'obiettivo di sicurezza di ogni requisito. Le istruzioni in questa colonna servono a comprendere i requisiti e non sostituiscono né estendono i requisiti PA-DSS e le procedure di test.		Ulteriori istruzioni
Requisiti e/o procedure di test aggiornati per riflettere le modifiche PCI DSS, dove un requisito PA-DSS si allinea a un requisito PCI DSS.		Come definito nello standard PCI DSS
Termini aggiornati nei requisiti e/o nelle procedure di test corrispondenti per motivi di allineamento e uniformità.		Chiarimento
Sono stati separati requisiti/procedure di test complessi per maggiore chiarezza e sono state rimosse le procedure di test ridondanti/sovrapposte.		Chiarimento
Procedure di test migliorate per chiarire il livello di convalida previsto per ogni requisito, comprese: <ul style="list-style-type: none"> informazioni richieste della Guida per l'implementazione del programma PA-DSS; installazione dell'applicazione in conformità alla <i>Guida per l'implementazione del programma PA-DSS</i> per verificare l'accuratezza delle istruzioni della <i>Guida per l'implementazione</i>. 		Chiarimento
Altre modifiche generali apportate includono: <ul style="list-style-type: none"> sono state rimosse le seguenti colonne: "Presente", "Non presente" e "Data di destinazione/Commenti"; requisiti e procedure di test sono stati rinumerati in base alle modifiche; requisiti e procedure di test sono stati riformattati per migliorarne la leggibilità, ad esempio contenuto di un paragrafo riformattato in elenco puntato, ecc.; sono state portate ovunque modifiche di formulazione minori per migliorare la leggibilità; sono stati corretti i refusi. 		Chiarimento

Requisito		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
Requisito 1			
Requisito 1 - Generale		Titolo aggiornato per motivi di uniformità, per sostituire “striscia magnetica” con “dati di traccia”.	Chiarimento
1.1.c	1.1.1-1.1.3	Procedura di test 1.1.c rimossa e aggiunta istruzione alle procedure di test correlate per i requisiti da 1.1.1 a 1.1.3.	Chiarimento
Requisito 2			

Requisito		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
2.x	2.x	Aggiunti i componenti <i>Guida per l'implementazione del programma PA-DSS</i> alle procedure di test in tutta la sezione.	Requisito in evoluzione
2.1	2.1	Termini modificati per fare riferimento alla rimozione sicura dei dati più che all'eliminazione.	Chiarimento
2.2	2.2	Procedure di test migliorate per richiedere la convalida delle funzioni di mascheramento PAN.	Chiarimento
2.4		Requisito rimosso relativo all'uso delle soluzioni di cifratura dell'intero disco. Requisiti successivi numerati di conseguenza.	Requisito in evoluzione
2.6.x	2.5.x	Procedure di test aggiornate per chiarire che le tecniche di gestione delle chiavi devono essere testate in modo corretto.	Chiarimento
2.7	2.6	Aggiornato per chiarire che il fornitore di applicazioni dovrebbe offrire un meccanismo di rimozione delle chiavi di crittografia, se le versioni attuali o precedenti utilizzavano chiavi di crittografia o crittogrammi.	Chiarimento
Requisito 3			
3.1	3.1	Nota spostata dalla procedura di test 3.1.d al Requisito 3.1.	Chiarimento
3.1.b-3.1.c	3.1.1-3.1.2	Nuovi requisiti creati da procedure di test precedenti 3.1.b-3.1.c per garantire che la modifica delle password predefinite sia attuata dall'applicazione e convalidata in modo appropriato.	Chiarimento
3.1.4	3.1.7	Requisito spostato in 3.1.7 per organizzare meglio i requisiti.	Chiarimento
3.1.6-3.1.7	3.1.6	Uniti i requisiti sulla complessità della password per allinearli a PCI DSS v3.0 e fornire la flessibilità necessaria per altre alternative di composizione password che rispondono al requisito minimo di solidità.	Chiarimento
3.3	3.3.1-3.3.2	Requisito 3.3 suddiviso in due requisiti per mettere in evidenza separatamente password <i>trasmesse</i> (3.3.1) e password <i>memorizzate</i> (3.3.2). Aggiornato 3.3.2 per richiedere l'uso di un algoritmo di crittografia avanzata one-way con una variabile di immissione esclusiva per rendere le password illeggibili.	Requisito in evoluzione

Requisito		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
	3.4	Nuovo requisito per le applicazioni per limitare l'accesso a funzioni/risorse richieste e applicare il privilegio più basso possibile per gli account di applicazioni integrate.	Requisito in evoluzione
Requisito 4			
4.2.5	4.2.5	Requisito aggiornato per chiarire i tipi di meccanismo di identificazione e autenticazione che devono essere registrati, inclusa la creazione di nuovi account.	Chiarimento
Requisito 5			
5.1	5.1	Requisito migliorato per includere le revisioni della sicurezza nei processi di sviluppo.	Requisito in evoluzione
	5.1.5	Nuovo requisito per gli sviluppatori di applicazioni di pagamento per verificare l'integrità del codice sorgente durante il processo di sviluppo.	Requisito in evoluzione
	5.1.6	Nuovo requisito per le applicazioni di pagamento da sviluppare in base alle migliori pratiche di settore per le tecniche di codifica sicure, tra cui: <ul style="list-style-type: none"> sviluppo con il privilegio più basso possibile per l'ambiente; sviluppo con opzioni predefinite in modalità provvisoria, ossia 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; documentazione che illustra come il numero PAN e/o i dati sensibili di autenticazione vengono gestiti in memoria. 	Requisito in evoluzione
	5.1.7	Nuovo requisito creato dalle precedenti procedure di test 5.2.a e 5.2.b per gli sviluppatori di applicazioni di pagamento che dovranno seguire una formazione sulle pratiche di sviluppo sicuro.	Chiarimento
5.2	5.2	Requisito aggiornato per mettere in evidenza la prevenzione delle vulnerabilità di codifica comuni.	Chiarimento
	5.2.10	Nuovo requisito per affrontare la questione della violazione dell'autenticazione e della gestione delle sessioni.	Requisito in evoluzione

Requisito		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
5.4	8.2	Requisito spostato in 8.2 per allinearlo ad altri requisiti che promuovono un ambiente PCI DSS sicuro e per mantenere il Requisito 5.x incentrato sulle pratiche di sviluppo software.	Chiarimento
	5.4	Nuovi requisiti per il fornitore di applicazioni di pagamento per definire e implementare una metodologia di versioning in conformità alla <i>Guida del programma PA-DSS</i> .	Requisito in evoluzione
	5.5	Nuovo requisito per i fornitori di applicazioni di pagamento che devono integrare le tecniche di valutazione dei rischi nel loro processo di sviluppo software.	Requisito in evoluzione
	5.6	Nuovo requisito per i fornitori di applicazioni di pagamento per implementare un processo di autorizzazione formale prima della release finale.	Requisito in evoluzione
Requisito 6			
6.1-6.2	6.1-6.3	Requisiti riorganizzati per chiarire i controlli validi per tutte le applicazioni e i controlli validi solo dove è fornito il servizio wireless o dove il servizio wireless è inteso per l'uso con l'applicazione di pagamento. Nuovo Requisito 6.3 creato dalla ex procedura di test 6.2.b.	Chiarimento
Requisito 7			
Requisito 7 - Generale		Titolo aggiornato per rispecchiare lo scopo del requisito (per affrontare le vulnerabilità e <i>gestire gli aggiornamenti delle applicazioni</i>).	Chiarimento
7.1	7.1.1-7.1.3	Suddiviso in requisiti separati e richiesto l'uso di fonti "attendibili" per le informazioni sulle vulnerabilità della sicurezza.	Chiarimento
7.2	7.2.1-7.2.2	Suddiviso in requisiti separati.	Chiarimento
	7.3	Nuovo requisito per il fornitore di applicazioni che deve fornire note sulla release per tutti gli aggiornamenti dell'applicazione.	Requisito in evoluzione
Requisito 8			
8.1	8.1	Esempio ampliato per chiarire lo scopo del requisito.	Chiarimento
5.4	8.2	Requisito spostato da 5.4 per allinearlo ad altri requisiti che promuovono un ambiente PCI DSS sicuro.	Chiarimento
10.1	8.3	Requisito spostato da 10.1 per allinearlo ad altri requisiti che promuovono un ambiente PCI DSS sicuro.	Chiarimento

Requisito		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
Requisito 9			
9.1	9.1	Termini aggiunti per chiarire lo scopo del requisito, ossia che i server Web e i componenti della memorizzazione dei dati dei titolari di carta non devono necessariamente essere nella stessa zona di rete, con database come esempio di un componente della memorizzazione dei dati di titolari di carta e DMZ come esempio di una zona di rete.	Chiarimento
Requisito 10			
10.1	8.3	Requisito spostato in 8.3 per allinearlo ad altri requisiti che promuovono un ambiente PCI DSS sicuro. Requisiti successivi rinumerati.	Chiarimento
10.2	10.1	Chiarito che il requisito si applica all'accesso remoto che ha origine al di fuori della rete del cliente.	Chiarimento
	10.2.2	Nuovo requisito per fornitori che offrono servizi di assistenza/manutenzione per gestire credenziali di autenticazione univoche per ogni cliente.	Requisito in evoluzione
10.3.2	10.2.3	Aggiornato per chiarire che i requisiti sono validi per tutti i tipi di accesso remoto.	Chiarimento
Requisito 11			
11.1	11.1	Aggiornamenti minori per fornire maggiore chiarezza e allinearsi allo standard PCI DSS.	Chiarimento
Requisito 12			
12.1	12.1 12.2	Requisiti riorganizzati per chiarire i controlli validi per tutte le applicazioni e i controlli validi solo dove è fornito il servizio wireless o dove il servizio wireless è inteso per l'uso con l'applicazione di pagamento.	Chiarimento
Requisito 13			
Requisito 13 - Generale		Titolo modificato per mettere in evidenza i requisiti della <i>Guida per l'implementazione del programma PA-DSS</i> . Requisiti relativi alla documentazione e ai programmi di formazione spostati nel nuovo Requisito 14.	Chiarimento
	13.1.1	Nuovo requisito per confermare che la <i>Guida per l'implementazione del programma PA-DSS</i> è specifica per l'applicazione e le versioni fase di valutazione.	Chiarimento

Requisito		Modifica	Tipo
PA-DSS v2.0	PA-DSS v3.0		
13.1.3	13.1.3	Chiarito che la <i>Guida per l'implementazione del programma PA-DSS</i> deve essere rivista e aggiornata ad ogni cambiamento dei requisiti di applicazione o PA-DSS.	Chiarimento
Requisito 14			
Requisito 14 - Generale		Vedere "Requisito 13 - Generale" sopra. Nuovo requisito per mettere in evidenza la documentazione e i programmi di formazione, compresa la formazione interna per il personale del fornitore con responsabilità PA-DSS.	Chiarimento
	14.1	Nuovo requisito per garantire la sicurezza delle informazioni e la formazione PA-DSS per il personale del fornitore con responsabilità PA-DSS almeno una volta all'anno.	Requisito in evoluzione
	14.2	Nuovo requisito per l'assegnazione delle responsabilità PA-DSS al personale del fornitore.	Requisito in evoluzione
13.2	14.3	Requisiti migliorati in precedenza inclusi in 13 per i programmi di formazione per responsabile dell'integrazione/rivenditore. Chiarito che i materiali di formazione devono essere rivisti e aggiornati ad ogni cambiamento dei requisiti di applicazione o PA-DSS.	Chiarimento
Appendice B			
Conferma della configurazione del laboratorio di test specifica per la valutazione PA-DSS	Configurazione del laboratorio di test per valutazioni PA-DSS	Appendice incentrato sulla fornitura di informazioni su aspettative e funzionalità del laboratorio utilizzato per condurre le valutazioni PA-DSS. Dettagli e modello per documentare la configurazione del laboratorio di test spostato per separare il <i>modello di reporting ROV PA-DSS</i> .	Chiarimento