

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 3.0 alla 3.1

Giugno 2015

Introduzione

Il presente documento contiene un riepilogo delle modifiche apportate da PA-DSS v3.0 a PA-DSS v3.1. La Tabella 1 fornisce una panoramica dei tipi di modifiche. La Tabella 2 fornisce un riepilogo delle modifiche effettive rilevate in PA-DSS v3.1.

Tabella 1 - Tipi di modifiche

¹ 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 ¹
PA-DSS v3.0	PA-DSS v3.1		
Tutte	Tutte	Corretti errori tipografici minori (grammatica, punteggiatura, formattazione, ecc.) e integrati aggiornamenti minimi per una migliore leggibilità del documento.	Chiarimento
Tutte	Tutte	Modificati i riferimenti da “esercente” a “cliente” quando si fa riferimento a entità che utilizzano applicazioni di pagamento.	Chiarimento
Informazioni sull'applicabilità dello standard PCI DSS	Informazioni sull'applicabilità dello standard PCI DSS	Modificato il riferimento da “istituzioni finanziarie” a “acquirenti, emittenti”. Chiarito che PCI DSS si applica a qualsiasi entità in grado di memorizzare, elaborare o trasmettere i dati degli account.	Chiarimento
2.3	2.3	Chiarito nella nota dei requisiti che sono richiesti controlli aggiuntivi se in uno stesso ambiente sono presenti entrambe le versioni troncata e hash dello stesso PAN. Aggiunta la procedura di test 2.3.c per la convalida della nota e rinumerate di conseguenza le procedure di test successive.	Chiarimento

2.4	2.4	Aggiornate le istruzioni per chiarire che le KEK (key-encrypting keys) non devono essere cifrate. Tuttavia, devono essere protette secondo quanto riportato nel Requisito 2.4.	Ulteriori istruzioni
2.5	2.5	Modificato il termine “cifratura” in “crittografico” nella procedura di test in modo da essere allineati con il requisito.	Chiarimento
3.1.a	3.1.a	Aggiornata la procedura di test per chiarire che le istruzioni riportate nel manuale <i>Guida per l'implementazione del programma PA-DSS</i> includono che l'assegnazione dell'autenticazione sicura a tutti gli account predefiniti che non saranno utilizzati deve essere disabilitata o non utilizzata.	Chiarimento
3.1.7	3.1.7	Chiarito che le password devono essere modificate almeno <i>una volta</i> ogni 90 giorni.	Chiarimento
5.1.d	5.1.d	Aggiornata la procedura di test per allinearla al requisito.	Chiarimento
5.3.3.a 5.4.1.c	5.3.3.a 5.4.1.c	Aggiornati termini nelle procedure di test per garantire l'uniformità.	Chiarimento
5.4.3.a	5.4.3.a	Sono stati combinati gli elenchi puntati nelle procedure di test per eliminare la ridondanza	Chiarimento
5.4.5.b	5.4.5.b	Aggiornata procedura di test per allinearla al requisito.	Chiarimento
6.3	6.3	Rimossi i termini ridondanti nella procedura di test.	Chiarimento
8.2	8.2	Rimosso SSL come esempio di tecnologia sicura. Aggiunta una nota che indica che SSL e TLS iniziale non sono più considerati una cifratura avanzata e le applicazioni di pagamento non li dovranno più utilizzare né supportarne l'uso. Interessa anche Requisiti 11.1 e 12.1 - 12.2.	Requisito in evoluzione
8.3	8.3	Aggiornato per garantire conformità con PCI DSS.	Chiarimento
10.2.2	10.2.2	Chiarito che per ogni cliente deve essere utilizzata una credenziale di autenticazione univoca.	Chiarimento
11.1	11.1	Rimosso SSL come esempio di tecnologia sicura e aggiunta una nota al requisito. Vedere la spiegazione precedente al punto 8.2.	Requisito in evoluzione
12.1 – 12.2	12.1 – 12.2	Rimosso SSL come esempio di tecnologia sicura e aggiunta una nota al requisito. Vedere la spiegazione precedente al punto 8.2.	Requisito in evoluzione

Appendice A: Riepilogo del contenuto della Guida per l'implementazione del programma PA-DSS	Appendice A: Riepilogo del contenuto della Guida per l'implementazione del programma PA-DSS	Aggiornamento effettuato per riflettere le modifiche apportate ai requisiti, come applicabile.	Chiarimento
---	---	--	-------------