Payment Card Industry (PCI)

Standard di protezione dei dati

Attestato di conformità per valutazioni in sede - Provider di servizi

Versione 3.2.1

Giugno 2018

Sezione 1 - Informazioni sulla valutazione

Istruzioni per l'invio

Il presente attestato di conformità deve essere compilato come dichiarazione dei risultati della valutazione del provider di servizi unitamente a *Requisiti e procedure di valutazione della sicurezza PCI DSS.* Completare tutte le sezioni. Il provider di servizi è tenuto a garantire che ogni sezione sia stata completata dalle parti interessate, come applicabile. Contattare il marchio di pagamento richiedente per le procedure di reporting e invio.

Parte 1. Informazioni per provider di servizi ed azienda qualificata per la valutazione (QSA)					
Parte 1a. Informazioni su società provider di servizi					
Ragione sociale:			DBA (doing business as):		
Nome referente:			Mansione:		
Telefono:			E-mail:		
Indirizzo ufficio:			Città:		
Stato/Provincia:		Paese:		CAP:	
URL:					

Parte 1b. Informazioni sull'azienda qualificata per la valutazione (se applicabile)					
Ragione sociale:					
Nome referente QSA principale:			Mansione:		
Telefono:			E-mail:		
Indirizzo ufficio:			Città:		
Stato/Provincia:		Paese:		CAP:	
URL:					

Parte 2. Riepilogo esecutivo

Parte 2a. Verifica dell'ambito

Servizi che erano COMPRESI nell'ambito della valutazione PCI DSS (selezionare tutte le risposte pertinenti):

Nome del servizio valutato:		
Tipo di servizio valutato:		
Provider di hosting: ☐ Applicazione/Software ☐ Hardware ☐ Infrastruttura/Rete ☐ Spazio fisico (co-location) ☐ Memorizzazione ☐ Web ☐ Servizi di sicurezza ☐ Provider di hosting sicuro 3-D ☐ Provider di hosting condiviso ☐ Altro hosting (specificare):	**Servizi gestiti (specificare):** ☐ Servizi di sicurezza dei sistemi ☐ Supporto IT ☐ Sicurezza fisica ☐ Sistema di gestione terminale ☐ Altri servizi (specificare):	**Elaborazione pagamento:** ☐ POS/Con carta presente ☐ Internet/E-Commerce ☐ MOTO/Call center ☐ ATM ☐ Altra elaborazione (specificare):
☐ Gestione account	☐ Storno di addebito e frode	☐ Gateway/Switch di pagamento
☐ Servizi di back-office	☐ Elaborazione emittente	☐ Servizi prepagati
☐ Gestione fatturazione	☐ Programmi di fedeltà	☐ Gestione registrazioni
☐ Compensazione e contabilizzazione	☐ Servizi esercenti	☐ Pagamenti pubblici/fiscali
☐ Provider di rete		
☐ Altri (specificare):		

***Nota**: queste categorie vengono fornite solo per l'assistenza e non vogliono limitare o predeterminare la descrizione dei servizi di un'entità. Se si ritiene che tali categorie non siano valide per il proprio servizio, completare l'opzione "Altri". Se non si è certi se una categoria è valida per il proprio servizio, consultare il marchio di pagamento applicabile.*

Parte 2a. Verifica dell'ambito *(continua)*

Servizi forniti dal provider di servizi NON INCLUSI nell'ambito della valutazione PCI DSS (selezionare tutte le risposte pertinenti):

Nome del servizio non valutato:	

Tipo di servizio non valutato:

Provider di hosting:	**Servizi gestiti (specificare):**	**Elaborazione pagamento:**
☐ Applicazione/Software ☐ Hardware ☐ Infrastruttura/Rete ☐ Spazio fisico (co-location) ☐ Memorizzazione ☐ Web ☐ Servizi di sicurezza ☐ Provider di hosting sicuro 3-D ☐ Provider di hosting condiviso ☐ Altro hosting (specificare):	☐ Servizi di sicurezza dei sistemi ☐ Supporto IT ☐ Sicurezza fisica ☐ Sistema di gestione terminale ☐ Altri servizi (specificare):	☐ POS/Con carta presente ☐ Internet/E-Commerce ☐ MOTO/Call center ☐ ATM ☐ Altra elaborazione (specificare):
☐ Gestione account	☐ Storno di addebito e frode	☐ Gateway/Switch di pagamento
☐ Servizi di back-office	☐ Elaborazione emittente	☐ Servizi prepagati
☐ Gestione fatturazione	☐ Programmi di fedeltà	☐ Gestione registrazioni
☐ Compensazione e contabilizzazione	☐ Servizi esercenti	☐ Pagamenti pubblici/fiscali
☐ Provider di rete		
☐ Altri (specificare):		

Fornire una breve spiegazione del perché i servizi selezionati non sono stati inclusi nella valutazione:	

Parte 2b. Descrizione delle attività relative alla carta di pagamento

Descrivere come e in quale misura la propria azienda memorizza, elabora e/o trasmette i dati dei titolari di carta.	
Descrivere come e in quale misura la propria azienda è in altro modo coinvolta o ha la capacità di incidere sui dati dei titolari di carta.	

Parte 2c. Sedi

Indicare i tipi di struttura (ad esempio, punti vendita, uffici, centri dati, call center ecc.) e un riepilogo delle sedi incluse nella revisione PCI DSS.

Tipo di struttura:	**Numero di strutture di questo tipo**	**Posizione della struttura (città, paese):**
Esempio: punti vendita	*3*	*Boston, MA, Stati Uniti*

Parte 2d. Applicazioni di pagamento

L'azienda utilizza una o più applicazioni di pagamento? ☐ Sì ☐ No

Fornire le seguenti informazioni in ordine alle Applicazioni di pagamento utilizzate dalla propria azienda:

Nome applicazione di pagamento	Versione numero	Fornitore dell'applicazione	L'applicazione è inclusa nell'elenco PA-DSS?	Data di scadenza dell'elenco PA-DSS (se applicabile)
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	

Parte 2e. Descrizione dell'ambiente

Fornire una descrizione ***di alto livello*** dell'ambiente coperto da questa valutazione. *Ad esempio:* • *Connessioni interne ed esterne all'ambiente dei dati dei titolari di carta.* • *Componenti di sistema critici interni all'ambiente dei dati dei titolari di carta, ai database, ai server Web ecc. e qualsiasi altro componente di pagamento necessario, come applicabile.*	
L'azienda utilizza la segmentazione di rete per definire l'ambito del proprio ambiente PCI DSS? *(Consultare la sezione "Segmentazione di rete" di PCI DSS per indicazioni sulla segmentazione di rete.)*	☐ Sì ☐ No

Parte 2f. Provider di servizi di terzi	
L'azienda azienda ha rapporti con un responsabile dell'integrazione e rivenditore qualificati (QIR) per i servizi sottoposti a convalida? Se sì: Nome dell'azienda QIR: Singolo nome QIR: Descrizione dei servizi forniti dal QIR:	☐ Sì ☐ No
La società ha rapporti con uno o più provider di servizi terzi (ad esempio responsabili dell'integrazione e rivenditori qualificati (Qualified Integrator & Resellers, QIR), gateway, elaboratori di pagamento, provider di servizi di pagamento (Payment Service Providers, PSP), società di hosting Web, agenti per la prenotazione di voli aerei, agenti del programma fedeltà ecc.) ai fini della convalida dei servizi?	☐ Sì ☐ No

Se sì:

Nome del provider di servizi:	**Descrizione dei servizi forniti:**

Nota: *il Requisito 12.8 si applica a tutte le entità presenti in questo elenco.*

Parte 2g. Riepilogo dei requisiti testati

Per ogni requisito PCI DSS, selezionare una delle seguenti opzioni:

- **Completo**: il requisito e tutti i requisiti secondari sono stati valutati per quel requisito e nessun requisito secondario è stato contrassegnato come "Non testato" o "Non applicabile" nel ROC.
- **Parziale**: uno o più requisiti secondari di quel requisito sono stati contrassegnati come "Non testato" o "Non applicabile" nel ROC.
- **Nessuno**: tutti i requisiti secondari di quel requisito sono stati contrassegnati come "Non testato" e/o "Non applicabile" nel ROC.

Per tutti i requisiti identificati come "Parziale" o "Nessuno", fornire i dettagli nella colonna "Giustificazione all'approccio", compresi:

- Dettagli su requisiti secondari specifici che sono stati contrassegnati come "Non testato" e/o "Non applicabile" nel ROC
- Motivo per cui il requisito secondario non è stato testato o non è applicabile

Nota: *è necessario compilare una tabella per ogni servizio coperto da questo AOC. Copie aggiuntive di questa sezione sono disponibili sul sito Web PCI SSC*.

Nome del servizio valutato:	

Requisito PCI DSS	**Dettagli dei requisiti di valutati**			
	Completo	**Parziale**	**Nessuno**	**Giustificazione all'approccio** (Necessario per tutte le risposte "Parziale" e "Nessuno". Identificare quali tra i sotto-requisiti non sono stati verificati e per quale ragione.)
Requisito 1 :	☐	☐	☐	
Requisito 2 :	☐	☐	☐	
Requisito 3 :	☐	☐	☐	
Requisito 4 :	☐	☐	☐	
Requisito 5 :	☐	☐	☐	
Requisito 6 :	☐	☐	☐	
Requisito 7 :	☐	☐	☐	
Requisito 8 :	☐	☐	☐	
Requisito 9 :	☐	☐	☐	
Requisito 10 :	☐	☐	☐	
Requisito 11 :	☐	☐	☐	
Requisito 12 :	☐	☐	☐	
Appendice A1:	☐	☐	☐	
Appendice A2:	☐	☐	☐	

Sezione 2 - Rapporto sulla conformità

Questo attestato di conformità riflette i risultati di una valutazione in sede, documentata nel rapporto sulla conformità (ROC) allegato.

La valutazione illustrata in questo attestato e nel ROC è stata completata il:		
Sono stati utilizzati controlli di compensazione per soddisfare i requisiti del ROC?	☐ Sì	☐ No
Qualche requisito del ROC è stato identificato come non applicabile (N/A)?	☐ Sì	☐ No
Qualche requisito non è stato testato?	☐ Sì	☐ No
Qualche requisito del ROC è stato impossibile da soddisfare a causa di un vincolo legale?	☐ Sì	☐ No

Sezione 3 - Dettagli su convalida e attestato

Parte 3. Convalida PCI DSS

Questo AOC si basa sui risultati annotati nel ROC, datato *(data di completamento ROC).*

In base ai risultati documentati nel ROC indicato sopra, i firmatari di cui alle Parti 3b-3d, come applicabile, dichiarano il seguente stato di conformità dell'entità identificata nella Parte 2 di questo documento (***selezionare un'opzione):***

☐	**Conforme:** tutte le sezioni del ROC PCI DSS sono state completate e a tutte le domande è stato risposto in modo affermativo, determinando una valutazione di **CONFORMITÀ** globale; pertanto *(Ragione sociale provider di servizi)* ha dimostrato la massima conformità agli standard PCI DSS.
☐	**Non conforme:** non tutte le sezioni del ROC PCI DSS sono state completate o non a tutte le domande è stata fornita una risposta affermativa, determinando una valutazione di **NON CONFORMITÀ** globale; pertanto *(Ragione sociale provider di servizi)* non ha dimostrato la massima conformità agli standard PCI DSS. **Data di destinazione** per conformità: è possibile che a un'entità che invia questo modulo con lo stato "Non conforme" venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. *Consultare il marchio di pagamento prima di completare la Parte 4.*
☐	**Conforme ma con eccezione legale:** uno o più requisiti sono stati contrassegnati con "Non presente" a causa di una restrizione legale che impedisce di rispondere al requisito. Questa opzione richiede un'ulteriore revisione da parte dell'acquirente o del marchio di pagamento. *Se selezionata, completare quanto segue:*

Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti

Parte 3a. Riconoscimento dello stato

I firmatari confermano:

(Selezionare tutte le risposte pertinenti)

☐	Il ROC è stato completato in base al documento *Requisiti e procedure di valutazione della sicurezza PCI DSS*, versione *(inserire numero di versione)*, e alle istruzioni ivi fornite.
☐	Tutte le informazioni contenute nel ROC e in questo attestato rappresentano in modo onesto i risultati della mia valutazione sotto tutti gli aspetti.
☐	Ho verificato con il fornitore dell'applicazione di pagamento che il mio sistema di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
☐	Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard in ogni momento, in base a quanto applicabile al mio ambiente.
☐	Se il mio ambiente cambia, accetto di dover rivalutare l'ambiente e implementare eventuali requisiti PCI DSS in base alle necessità.

Parte 3a. Riconoscimento dello stato (continua)	
☐	Nessuna prova della memorizzazione dei dati della traccia completa[1], dei dati CAV2, CVC2, CID o CVV2[2] oppure dei dati PIN[3] dopo che l'autorizzazione alla transazione è stata individuata su QUALSIASI sistema esaminato durante questa valutazione.
☐	Le scansioni ASV vengono completate dal Fornitore di prodotti di scansione approvato (ASV) PCI SSC *(Nome ASV)*

Parte 3b. Attestato per provider di servizi	
Firma del funzionario esecutivo del provider di servizi ↑	*Data:*
Nome funzionario esecutivo del provider di servizi:	*Mansione:*

Parte 3c. Riconoscimento dell'azienda qualificata per la valutazione (QSA) (se applicabile)	
Se un QSA è stato coinvolto o aiutato durante questa valutazione, descrivere il ruolo ricoperto:	

Firma del funzionario espressamente autorizzato dell'azienda QSA ↑	*Data:*
Nome del funzionario espressamente autorizzato:	*Azienda QSA:*

Parte 3d. Coinvolgimento dell'azienda interna per la valutazione (ISA) (se applicabile)	
Se un ISA è stato coinvolto o aiutato durante questa valutazione, identificare il personale ISA e descrivere il ruolo ricoperto:	

[1] Dati codificati nella striscia magnetica o dati equivalenti su un chip utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare i dati della traccia completa dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il PAN, la data di scadenza e il nome del titolare della carta.

[2] Il valore di tre o quattro cifre stampato nel riquadro della firma o nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

[3] 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.

Parte 4. Piano d'azione per i requisiti non conformi

Selezionare la risposta appropriata per "Conforme ai requisiti PCI DSS" per ogni requisito. In caso di risposta negativa a uno dei requisiti, è necessario fornire la data in cui si prevede che la Società sarà conforme al requisito e una breve descrizione delle azioni che verranno intraprese per soddisfare il requisito.

Verificare con il marchio di pagamento applicabile prima di completare la Parte 4.

Requisito PCI DSS	Descrizione del requisito	Conforme ai requisiti PCI DSS *(Selezionarne uno)*		Data della soluzione e azioni (Se è stata selezionata l'opzione "NO" per un qualsiasi requisito)
		SÌ	NO	
1	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta	☐	☐	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	☐	☐	
3	Proteggere i dati dei titolari di carta memorizzati	☐	☐	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	☐	☐	
5	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus	☐	☐	
6	Sviluppare e gestire sistemi e applicazioni protette	☐	☐	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	☐	☐	
8	Individuare e autenticare l'accesso ai componenti di sistema	☐	☐	
9	Limitare l'accesso fisico ai dati dei titolari di carta	☐	☐	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta	☐	☐	
11	Eseguire regolarmente test dei sistemi e processi di protezione	☐	☐	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	☐	☐	
Appendice A1	Requisiti PCI DSS aggiuntivi per provider di hosting condiviso	☐	☐	
Appendice A2	Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale per connessioni a terminale POI POS con carta presente	☐	☐