



# **Payment Card Industry (PCI) Standard di protezione dei dati**

---

**Attestato di conformità per  
valutazioni in sede - Esercenti**

**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 dell'esercente unitamente a *Requisiti e procedure di valutazione della sicurezza PCI DSS*. Completare tutte le sezioni. L'esercente è tenuto a garantire che ogni sezione sia stata completata dalle parti interessate, come applicabile. Per le procedure di reporting e invio contattare l'acquirente (banca dell'esercente) o i marchi di pagamento.

### Parte 1. Informazioni Esercente e Azienda qualificata per la valutazione (QSA)

#### Parte 1a. Informazioni sull'organizzazione dell'esercente

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. Tipo di esercente (selezionare tutte le risposte pertinenti)

- Rivenditore
  Telecomunicazioni
  Negozi di alimentari e supermercati  
 Distributori di benzina
  E-Commerce
  Ordini via posta/telefono (MOTO)  
 Altro (specificare):

Quali tipi di canali di pagamento offre l'azienda?

- Ordini via posta/telefono (MOTO)  
 E-Commerce  
 Con carta presente (contatto diretto)

Quali sono i canali di pagamento coperti dalla presente valutazione?

- Ordini via posta/telefono (MOTO)  
 E-Commerce  
 Con carta presente (contatto diretto)

**Nota:** se la propria azienda dispone di un canale o una procedura di pagamento non inclusi nella presente valutazione, consultare l'acquirente o il marchio di pagamento in merito alla convalida degli altri canali.

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

In che modo e con quale titolo la società memorizza, elabora e/o trasmette i 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	Sedi della struttura (città, paese)
<i>Esempio: punti vendita</i>	3	<i>Boston, MA, Stati Uniti</i>

### Parte 2d. Applicazione 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)
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> 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? <i>(Consultare la sezione "Segmentazione di rete" di PCI DSS per indicazioni sulla segmentazione di rete.)</i>	<input type="checkbox"/> Sì <input type="checkbox"/> No
---	---

**Parte 2f. Provider di servizi di terzi**

L'azienda utilizza un responsabile dell'integrazione e rivenditore qualificati (QIR)? Se sì: Nome dell'azienda QIR: Singolo nome QIR: Descrizione dei servizi forniti dal QIR:	<input type="checkbox"/> Sì <input type="checkbox"/> No
--	---

L'azienda condivide i dati dei titolari di carta con provider di servizi di terzi (ad esempio responsabile dell'integrazione e rivenditore qualificati (QIR), gateway, elaboratori pagamenti, provider di servizi di pagamento (PSP), società di hosting Web, agenti per la prenotazione di voli aerei, agenti del programma fedeltà, ecc.)?	<input type="checkbox"/> Sì <input type="checkbox"/> 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.

## 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?	<input type="checkbox"/> Sì <input type="checkbox"/> No
Qualche requisito del ROC è stato identificato come non applicabile (N/A)?	<input type="checkbox"/> Sì <input type="checkbox"/> No
Qualche requisito non è stato testato?	<input type="checkbox"/> Sì <input type="checkbox"/> No
Qualche requisito del ROC è stato impossibile da soddisfare a causa di un vincolo legale?	<input type="checkbox"/> Sì <input type="checkbox"/> 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 esercente*) 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 CONFORME** globale; pertanto (*Ragione sociale esercente*) 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 proprio acquirente o 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)

- |                          |   |
|--------------------------|---|
| <input type="checkbox"/> | Nessuna prova della memorizzazione dei dati della traccia completa <sup>1</sup> , dei dati CAV2, CVC2, CID o CVV2 <sup>2</sup> oppure dei dati PIN <sup>3</sup> dopo che l'autorizzazione alla transazione è stata individuata su QUALSIASI sistema esaminato durante questa valutazione. |
| <input type="checkbox"/> | Le scansioni ASV vengono completate dal Fornitore di prodotti di scansione approvato (ASV) PCI SSC ( <i>Nome ASV</i> )  |

### Parte 3b. Attestato esercente

Firma del funzionario esecutivo dell'esercente ↑

Data:

Nome funzionario esecutivo dell'esercente:

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:

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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.

*Consultare il proprio acquirente o il marchio di pagamento 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati dei titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Sviluppare e gestire sistemi e applicazioni protette	<input type="checkbox"/>	<input type="checkbox"/>	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	<input type="checkbox"/>	<input type="checkbox"/>	
8	Individuare e autenticare l'accesso ai componenti di sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eseguire regolarmente test dei sistemi e processi di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	<input type="checkbox"/>	<input type="checkbox"/>	
Appendice A2	Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale per connessioni a terminale POI POS con carta presente	<input type="checkbox"/>	<input type="checkbox"/>	



