



*Your complimentary
use period has ended.
Thank you for using
PDF Complete.*

[Click Here to upgrade to
Unlimited Pages and Expanded Features](#)



Settore delle carte di pagamento (PCI) Standard di protezione dei dati

Attestato di conformità per questionario di autovalutazione D - Versione provider di servizi

Versione 1.2

Ottobre 2008

D - Versione provider di servizi

Istruzioni per l'invio

Il provider di servizi deve completare questo Attestato di conformità come una dichiarazione del proprio stato di conformità agli *Standard di protezione dei dati per il settore delle carte di pagamento (PCI DSS)* e alle procedure di valutazione della sicurezza. Completare tutte le sezioni applicabili e fare riferimento alle istruzioni per l'invio nella sezione "Conformità agli standard PCI DSS - Operazioni" nel presente documento.

Parte 1. 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. Informazioni su società provider di servizi

Ragione sociale:					
Nome referente:		Mansione:			
Telefono:		E-mail:			
Indirizzo ufficio:		Città:			
Stato/Provincia:		Paese:		CAP:	
URL:					

Parte 2a. Servizi

Servizi forniti (selezionare tutte le risposte appropriate):

- | | | |
|---|---|---|
| <input type="checkbox"/> Autorizzazione Secure | <input type="checkbox"/> Programmi fedeltà | <input type="checkbox"/> Server di controllo dell'accesso 3-D |
| <input type="checkbox"/> Switching magnetica | <input type="checkbox"/> IPSP (E-commerce) | <input type="checkbox"/> Elaborazione transazioni su striscia |
| <input type="checkbox"/> Gateway di pagamento MO/TO | <input type="checkbox"/> Compensazione e liquidazione | <input type="checkbox"/> Elaborazione transazioni |
| <input type="checkbox"/> Hosting | <input type="checkbox"/> Elaborazione emissioni | <input type="checkbox"/> Altro (specificare): |

Elencare le strutture e le posizioni incluse nella valutazione della conformità agli standard PCI DSS:

Parte 2b. Rapporti

La società ha rapporti con uno o più provider di servizi di terze parti (per esempio gateway, società di hosting Web, agenti per la prenotazione di voli aerei, agenti di programmi fedeltà, eccetera)? Sì No

Parte 2c. Elaborazione delle transazioni

In che modo e con quale titolo la società memorizza, elabora e/o trasmette dati dei titolari di carta?

ell'ambito del servizio:

Versione applicazione di pagamento:

Parte 3. Convalida PCI DSS

In base ai risultati del questionario SAQ D datato (*data di compilazione SAQ*), (*ragione sociale provider di servizi*) dichiara il seguente stato di conformità (selezionare una risposta):

Conforme: Tutte le sezioni del questionario SAQ PCI sono state completate e a tutte le domande è stato risposto "sì", determinando una valutazione di **CONFORMITÀ** globale e un fornitore di scansioni approvato (ASV) da PCI SSC ha eseguito una scansione di sicurezza; pertanto (*ragione sociale provider di servizi*) ha dimostrato la massima conformità agli standard PCI DSS.

Non conforme: Non tutte le sezioni del questionario SAQ PCI sono state completate e ad alcune domande è stato risposto "no", determinando una valutazione di **NON CONFORMITÀ** globale o non è stata eseguita una scansione di sicurezza da un fornitore di scansioni approvato (ASV) da PCI SSC; pertanto (*ragione sociale provider di servizi*) non ha dimostrato la massima conformità agli standard PCI DSS.

Data di scadenza 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, perché non tutti i marchi di pagamento richiedono questa sezione.*

Parte 3a. Conferma dello stato di conformità

Il provider di servizi conferma che:

- Il questionario di autovalutazione D, versione (*indicare numero di versione*), è stato completato in base alle istruzioni qui fornite.
- Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione.
- Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard.
- Nessuna prova di memorizzazione dei dati della striscia magnetica (traccia)¹, CAV2, CVC2, CID o CVV2² oppure dei dati PIN³ dopo l'autorizzazione della transazione è stata trovata sui sistemi controllati durante questa valutazione.

Parte 3b. Accettazione da parte del provider di servizi

Firma del funzionario esecutivo del provider di servizi ↑

Data ↑

Nome funzionario esecutivo del provider di servizi ↑

Mansione ↑

Società rappresentata dal provider di servizi ↑

¹ Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare tutti i dati completi della striscia magnetica dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il numero cliente, la data di scadenza e il nome.

² Il valore di tre o quattro cifre stampato nel riquadro della firma o a destra di questo riquadro oppure 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.

on conformità

Selezionare lo "Stato di conformità" appropriato per ciascun requisito. In caso di risposta negativa a uno dei requisiti, occorre specificare la data in cui 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, perché non tutti i marchi di pagamento richiedono questa sezione.*

Requisito PCI DSS	Descrizione del requisito	Stato di conformità (selezionare una risposta)		Data e azioni di correzione (in caso di non conformità)
		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	Utilizzare e aggiornare regolarmente 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	Assegnare un ID univoco a chiunque abbia accesso a un computer	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eeguire regolarmente test dei sistemi e processi di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni	<input type="checkbox"/>	<input type="checkbox"/>	

