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

Questionario di autovalutazione

Istruzioni e linee guida

Versione 3.2.1

Giugno 2018

Modifiche al documento

Data	Versione	Descrizione
1 ottobre 2008	1.2	Allineamento del contenuto con il nuovo standard PCI DSS v1.2 e implementazione di modifiche minori apportate dopo la versione originale v1.1.
28 ottobre 2010	2.0	Allineamento del contenuto al nuovo PCI DSS v2.0 e chiarimento dei tipi di ambienti SAQ e dei criteri di idoneità. Aggiunta di SAQ C-VT per gli esercenti con terminal di pagamento virtuali
Giugno 2012	2.1	Aggiunta di SAQ P2PE-HW per gli esercenti che elaborano i dati dei titolari di carta solo tramite terminali di pagamento hardware compresi in una soluzione PCI Point-to-Point Encryption (P2PE) inclusa nell'elenco PCI SSC. Il presente documento è da utilizzarsi solo con PCI DSS versione 2.0.
Aprile 2015	3.1	Allineamento del contenuto con PCI DSS v3.1, con aggiunta dei SAQ A-EP e B-IP, e chiarimento dei criteri di idoneità per i SAQ esistenti.
Maggio 2016	3.2	Aggiornamento per allinearsi con PCI DSS v3.2 e chiarire i criteri di idoneità per i SAQ esistenti.
Giugno 2018	3.2.1	Aggiornamenti minori per l'allineamento con PCI DSS v3.2.1.

ATTESTAZIONE: La versione testuale in lingua inglese di questo documento, nella forma in cui quest'ultima è stata pubblicata sul sito Internet PCI SSC, verrà, a tutti gli effetti, considerata la versione ufficiale di questi documenti. Qualora dovessero insorgere ambiguità o incongruenze fra questo testo e il testo in lingua inglese, prevarrà in tal sede la versione anglofona.

Sommario

Informazioni sul documento

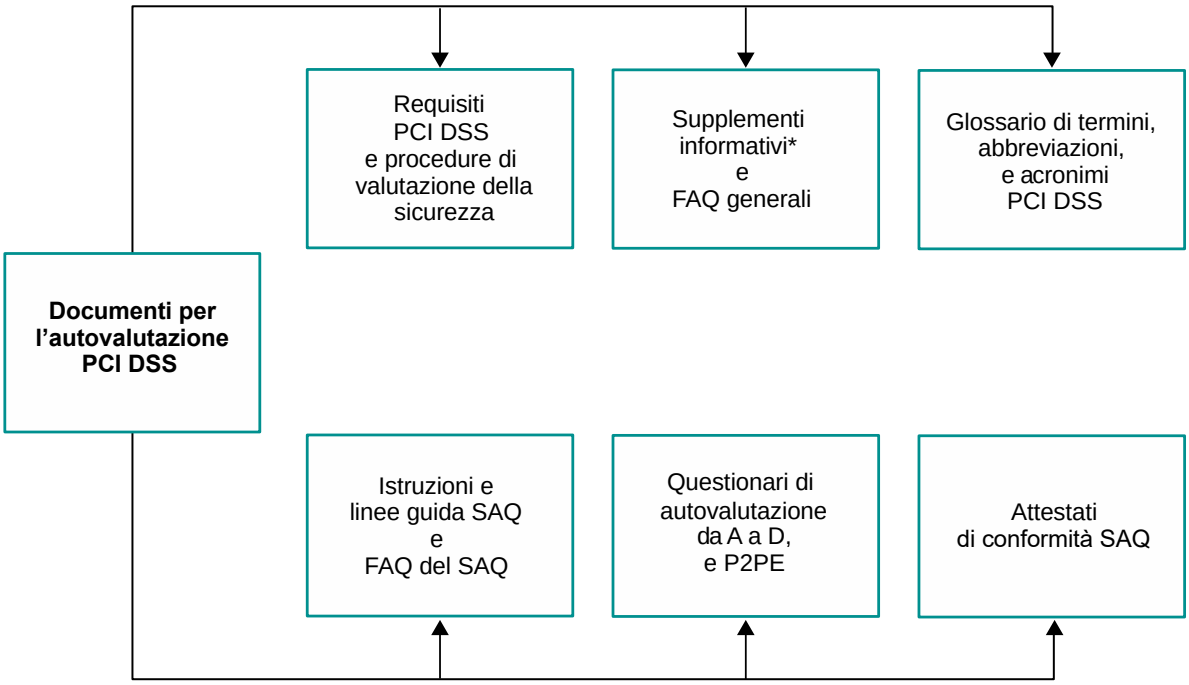
Il presente documento è stato sviluppato per aiutare esercenti e provider di servizi a comprendere il funzionamento dei questionari di autovalutazione (SAQ) per lo standard di protezione dei dati nel settore delle carte di pagamento (PCI DSS). Per capire perché il PCI DSS è importante per la propria organizzazione, quali strategie si possono adottare per favorire la conformità al PCI DSS e sapere se l'organizzazione è idonea a completare uno dei SAQ più brevi, si consiglia di leggere le istruzioni e le linee guida ivi contenute nella loro interezza.

Autovalutazione PCI DSS: in cosa consiste

Il PCI DSS e i documenti correlati rappresentano uno standard comune di strumenti del settore per garantire che i dati dei titolari di carta vengano gestiti in tutta sicurezza. Lo standard, di per sé, fornisce una struttura utile per sviluppare una procedura di sicurezza valida, che includa la prevenzione, il rilevamento e la capacità di reagire a violazioni di sicurezza. Per ridurre il rischio di problemi e limitare i danni in caso dovessero verificarsene, è importante che tutte le entità che archiviano, elaborano o trasmettono i dati dei titolari di carta siano conformi.

Il grafico mostrato di seguito illustra gli strumenti in uso per aiutare le organizzazioni con la conformità e l'autovalutazione PCI DSS.

Questi e altri documenti correlati si trovano all'indirizzo https://it.pcisecuritystandards.org/minisite/env2/.



** Nota: i supplementi informavivi forniscono solo inform azioni e indicazioni aggiuntive, ma non sostituiscono né soppiantano alcun requisito PCI DSS.*

* ***Nota:*** *i Supplementi informativi forniscono solo informazioni e indicazioni supplementari, senza sostituire o sovrapporsi ai requisiti PCI DSS.*

Panoramica sul questionario SAQ

I *questionari di autovalutazione PCI DSS* (SAQ) sono strumenti di convalida destinati ad assistere esercenti e provider di servizi nell'autovalutazione della propria conformità a PCI DSS. I questionari SAQ PCI DSS sono stati elaborati in diverse versioni per adattarsi a differenti scenari. Questo documento è stato sviluppato per aiutare l'organizzazione a determinare quali SAQ sono più adeguati al proprio ambiente.

Il SAQ PCI DSS è uno strumento di convalida per esercenti e provider di servizi a cui gli acquirenti o marchi di pagamento non richiedono di presentare un rapporto sulla conformità PCI DSS (ROC). Per informazioni dettagliate sui requisiti di convalida PCI DSS, consultare il proprio acquirente o il marchio di pagamento.

Ogni SAQ PCI DSS contiene quanto segue:

1. Domande sui requisiti PCI DSS per i diversi ambienti: vedere “Selezione del SAQ e dell'attestato più adatti per la propria organizzazione” in questo documento. La sezione include anche una colonna di “Test attesi” che si basa sulle procedure di test dello standard PCI DSS.
2. Attestato di conformità: l'attestazione include la dichiarazione di idoneità per il completamento del SAQ applicabile e i successivi risultati dell'autovalutazione PCI DSS.

Perché PCI DSS è importante

I membri fondatori dell'Ente responsabile degli standard di protezione PCI (American Express, Discover, JCB, Mastercard e Visa) controllano costantemente che non si verifichino violazioni dei dati degli account. Il rischio che i dati vengano compromessi interessa tutte le organizzazioni, dalle più piccole agli esercenti e provider di servizi più grossi.

Una violazione di sicurezza con conseguente compromissione dei dati delle carte di pagamento ha conseguenze di vasta portata per le aziende interessate, come per esempio:

1. Requisiti normativi di notifica
2. Perdita della reputazione
3. Perdita di clienti
4. Potenziali sanzioni finanziarie (es. penali o sanzioni di altro tipo)
5. Contenziosi

L'analisi forense delle compromissioni ha dimostrato che le falle più comuni in materia di sicurezza individuate dai controlli PCI DSS in genere vengono sfruttate per la mancanza o la scarsa presenza di controlli PCI DSS in vigore al momento della violazione. Lo standard PCI DSS è stato progettato a questo scopo e prevede requisiti dettagliati proprio per minimizzare le possibilità di una violazione o gli effetti qualora dovesse verificarsene una.

Esempi di falle comuni nei controlli PCI DSS includono, tra gli altri:

- Archiviazione di dati sensibili di autenticazione (SAD) come i dati di traccia dopo l'autorizzazione (Requisito 3.2). Molte organizzazioni che hanno subito violazioni non sapevano che i loro sistemi archiviassero questo tipo di dati.
- Controllo degli accessi inadeguato a causa di sistemi POS installati in modo non corretto, che consentono agli utenti malintenzionati di accedere tramite i percorsi intesi per i fornitori POS (Requisiti 7.1, 7.2, 8.2 e 8.3).
- Impostazioni di sistema e password predefinite non modificate al momento dell'installazione del sistema (Requisito 2.1).
- Servizi non necessari e non sicuri non rimossi o resi sicuri durante l'installazione del sistema (Requisiti 2.2.2 e 2.2.3).
- Applicazioni web mal codificate con conseguente SQL injection e altre vulnerabilità, che consentono l'accesso al database in cui sono archiviati i dati dei titolari di carta direttamente dal sito web (Requisito 6.5).
- Patch di protezione mancanti o obsolete (Requisito 6.2).
- Mancanza di registri (Requisito 10).
- Scarso monitoraggio (tramite revisioni dei registri, rilevazione/prevenzione delle intrusioni, scansioni trimestrali delle vulnerabilità e meccanismi di rilevamento delle modifiche) (Requisiti 10.6, 11.2, 11.4 e 11.5).

- Determinazione dell'ambito scorretta, per esempio a causa dell'esclusione di parte della rete dall'ambito PCI DSS, dovuta a una segmentazione inadeguata di cui non è stata verificata l'efficacia (Requisito 11.3.4). Così facendo, l'ambiente dei dati dei titolari di carta viene inconsapevolmente esposto a falle di altre parti della rete che non sono state protette secondo PCI DSS (ad esempio, da punti di accesso wireless non protetti e vulnerabilità introdotte tramite e-mail e navigazione web dei dipendenti) (Requisiti 1.2, 1.3 e 1.4).

Capire la differenza tra conformità e sicurezza

È importante sapere che differenza c'è tra essere conformi ed essere sicuri: la conformità a PCI DSS in un dato momento, infatti, non impedisce che la situazione in un ambiente possa cambiare, cosa che, se non vengono implementati i controlli appropriati, potrebbe minarne la sicurezza. Pertanto, è bene garantire che i controlli PCI DSS continuino ad essere attuati correttamente nell'ambito della normale attività quotidiana (BAU) e come definito dalla strategia di sicurezza globale. Ciò consente di monitorare l'efficacia dei controlli di sicurezza dell'organizzazione su base continuativa e di mantenere l'ambiente conforme a PCI DSS tra una valutazione PCI DSS e l'altra. Esempi di come incorporare PCI DSS nelle attività BAU sono forniti nella sezione “Migliori prassi per l'implementazione del PCI DSS nei processi aziendali consueti” del PCI DSS.

Inoltre, i requisiti di sicurezza PCI DSS sono mirati alla protezione dei dati delle carte di pagamento, ma la propria organizzazione potrebbe disporre di altri dati sensibili e risorse da proteggere che ricadono al di fuori dell'ambito PCI DSS. Pertanto, sebbene la conformità PCI DSS, se correttamente mantenuta, possa certamente contribuire alla sicurezza generale, non può andare a sostituire un programma di sicurezza solido a livello di organizzazione.

Suggerimenti generali e strategie per la conformità PCI DSS

Di seguito sono riportati alcuni suggerimenti generali e strategie per adeguarsi alla conformità PCI DSS. Questi suggerimenti possono aiutarvi a eliminare l'archiviazione dei dati dei titolari di carta di cui non avete bisogno, a isolare i dati necessari per aree centralizzate definite e controllate e a limitare l'ambito delle attività di convalida della conformità PCI DSS. Eliminando i dati dei titolari di carta non necessari e/o isolando i dati relativi ad aree definite e controllate, per esempio, è possibile rimuovere i sistemi e le reti che non memorizzano, elaborano o trasmettono i dati dei titolari di carta (e che non si connettono a sistemi che lo fanno) dall'ambito dell'autovalutazione.

1. **Dati sensibili di autenticazione (comprendenti dati della traccia completa della banda magnetica o del chip, codici e valori di convalida della carta, PIN e blocchi PIN):**

   Assicuratevi di non ***memorizzare mai questi dati*** dopo l'autorizzazione:

2. **Informatevi dal fornitore POS riguardo alla sicurezza del vostro sistema, ponendogli le seguenti domande:**

   a. Le impostazioni e le password predefinite dei sistemi e dei database che fanno parte del sistema POS sono state modificate?

   b. È possibile accedere al mio sistema POS da remoto? In caso affermativo, sono stati implementati controlli adeguati per impedire ad altri di accedere al mio sistema POS, ad esempio tramite metodi di accesso remoto sicuro e non mediante l'uso di password comuni o predefinite? Con quale frequenza viene effettuato l'accesso al mio dispositivo POS da remoto e perché? Chi è autorizzato ad accedere al mio POS da remoto?

   c. Tutti i servizi inutili e poco sicuri sono stati rimossi dai sistemi e dai database che fanno parte del sistema POS?

   d. Il mio software POS è convalidato secondo lo standard PA-DSS (Payment Application Data Security Standard)? (Consultare l'elenco delle applicazioni di pagamento convalidate di PCI SSC.)

   e. Il mio software POS memorizza dati sensibili di autenticazione, come i dati di traccia o i blocchi PIN? Questi dati non possono essere memorizzati: quanto tempo ci vuole a rimuoverli?

f. Il mio software POS memorizza i numeri di conto univoci (PAN)? In caso affermativo, questi dati devono essere protetti: cosa fa il POS in questo senso?

g. È possibile inserire nell'elenco dei file scritti dall'applicazione un riepilogo dei contenuti di ciascun file, per verificare che i dati non archiviabili menzionati sopra non siano memorizzati?

h. Il mio software POS applica password complesse e univoche per l'accesso a tutti gli utenti?

i. Ho la garanzia che non vengono utilizzate password comuni o predefinite per accedere al mio sistema e ad altri sistemi per esercenti supportati?

j. I sistemi e i database parte del sistema POS sono stati soggetti a patch con tutti gli aggiornamenti di sicurezza applicabili?

k. La funzionalità di registro è attiva per tutti i sistemi e i database che fanno parte del sistema POS?

l. Se le versioni precedenti del software POS memorizzano dati sensibili di autenticazione, questa funzione è stata rimossa durante gli aggiornamenti correnti al software POS? Per rimuovere questi dati è stata usata un'utility di cancellazione sicura?

3. Dati del titolare della carta: se non ne avete bisogno, non conservarteli!

a. Le regole del marchio di pagamento consentono di memorizzare il numero di conto univoco (PAN), la data di scadenza, il nome del titolare della carta e il codice di servizio.

b. Fate un riepilogo dei luoghi in cui conservate questi dati e perché. Se non hanno uno scopo commerciale preciso, valutate se eliminarli.

c. Valutate se l'archiviazione di tali dati e il processo aziendale che la supporta valgono quanto segue:

   i. Il rischio che vengano compromessi.

   ii. I controlli PCI DSS aggiuntivi che vanno applicati per proteggere tali dati.

   iii. Le attività di manutenzione continua necessarie a mantenere la conformità a PCI DSS nel tempo.

4. Dati del titolare della carta: se ne avete bisogno, rendeteli sicuri!

È possibile limitare l'ambito di una valutazione PCI DSS limitando l'archiviazione dei dati a un ambiente definito e isolandoli attraverso l'uso di una corretta segmentazione di rete. Ad esempio, se i dipendenti navigano su Internet e ricevono messaggi di posta elettronica sulla stessa macchina o sullo stesso segmento di rete usati per i dati dei titolari di carta, valutate se segmentare (isolare) i dati dei titolari di carta su una macchina o segmento di rete a sé (ad esempio tramite router o firewall). Isolando in modo efficace i dati dei titolari di carta, sarà possibile concentrare le attività PCI DSS solo sulla parte isolata, anziché includere tutte le macchine.

5. Controlli compensativi

I controlli compensativi possono essere presi in considerazione per la maggior parte dei requisiti PCI DSS quando un'organizzazione non è in grado di soddisfare le specifiche tecniche di un requisito, ma ha posto in essere altri controlli sufficienti a mitigare il rischio associato. Se l'organizzazione non dispone esattamente del controllo specificato in PCI DSS, ma ha posto in essere altri controlli che soddisfano la definizione PCI DSS di controlli compensativi (vedere “Controlli compensativi” nell'Appendice B e anche in *Glossario, abbreviazioni e acronimi*), dovrà effettuare le seguenti operazioni:

a. Seguire le procedure per i controlli compensativi descritte nell'Appendice B.

b. Per tutti i requisiti soddisfatti tramite controllo compensativo, rispondere alla domanda SAQ mettendo la spunta nella colonna “Sì con CCW”.

c. Documentare ogni controllo compensativo compilando il Foglio di lavoro sui controlli compensativi nell'Appendice B del SAQ.

   Per ogni requisito soddisfatto con un controllo compensativo, è necessario compilare il relativo foglio di lavoro.

d. Inviare tutti i fogli di lavoro dei controlli compensativi compilati, insieme al SAQ e/o all'Attestato di conformità compilato, secondo le istruzioni del proprio acquirente o marchio di pagamento.

6. Assistenza e formazione professionale

a. Se desiderate rivolgervi a un professionista della sicurezza per ricevere assistenza con la vostra autovalutazione, vi invitiamo a prendere in considerazione la possibilità di contattare un responsabile della valutazione di sicurezza qualificato (QSA). I QSA sono stati formati da PCI SSC per condurre valutazioni PCI DSS e sono elencati sul sito web PCI SSC.

b. Il sito web PCI SSC è un'importante fonte di risorse aggiuntive, tra cui:

   - *Glossario, abbreviazioni e acronimi di PCI DSS*
   - Domande frequenti (FAQ)
   - Webinar
   - Supplementi informativi e linee guida
   - Moduli SAQ e attestati di conformità

c. PCI SSC offre anche una serie di programmi di formazione per il personale delle organizzazioni. Esempio: PCI Awareness, il programma PCI Professional (PCIP) e il programma per responsabili delle valutazioni di sicurezza interni (ISA).

   Per ulteriori informazioni, consultare https://it.pcisecuritystandards.org/minisite/env2/.

d. I programmi di formazione e le risorse relative ai pagamenti possono essere disponibili anche presso i marchi di pagamento o le entità acquirenti.

Nota: *i supplementi informativi integrano il PCI DSS, indicando considerazioni e consigli aggiuntivi per soddisfare i requisiti ivi contenuti, ma non modificano, eliminano o sostituiscono il PCI DSS o uno qualsiasi dei requisiti indicati.*

Selezione del SAQ e dell'attestato più adatti per la propria organizzazione

Esercenti e fornitori devono rispettare il PCI DSS applicabile al proprio ambiente in qualsiasi momento. I questionari SAQ sono disponibili in diverse varianti, presentate nella tabella sottostante e descritte più nel dettaglio nelle pagine che seguono. Usate la tabella per determinare quale SAQ sia più adatto per la vostra organizzazione e poi controllate le descrizioni dettagliate per essere sicuri di soddisfare tutti i requisiti del caso.

Nota per tutti i questionari tranne SAQ D: questi SAQ includono domande che si applicano a un tipo specifico di ambiente per esercenti, come definito nei criteri di idoneità SAQ correlati. Se esistono requisiti PCI DSS applicabili al vostro ambiente che non sono coperti dal SAQ selezionato, potrebbe voler dire che il questionario scelto non è adatto per l'ambiente in uso. Ricordate che è necessario rispettare tutti i requisiti PCI DSS applicabili per essere conformi a PCI DSS.

SAQ	Descrizione
A	Esercenti con carta non presente (e-commerce od ordine tramite posta/telefono), che hanno esternalizzato tutte le funzioni dei dati del titolare della carta a fornitori di servizi terzi conformi a PCI DSS, senza archiviare, elaborare o trasmettere per via elettronica i dati dei titolari di carta ai sistemi o nelle sedi degli esercenti. *Non applicabile ai canali che prevedono un contatto diretto con il cliente.*
A-EP	Esercenti di e-commerce che elaborano i pagamenti in outsourcing tramite terzi convalidati PCI DSS e che dispongono di siti web che non ricevono direttamente i dati dei titolari di carta, ma che possono influire sulla sicurezza delle transazioni di pagamento. Nessuna memorizzazione, elaborazione o trasmissione elettronica dei dati dei titolari di carta ai sistemi o nelle sedi degli esercenti. *Applicabile solo ai canali e-commerce.*
B	Per esercenti che usano solo: ▪ Dispositivi di stampa privi di archiviazione elettronica dei dati dei titolari di carta; ▪ Terminali per connessione in uscita indipendenti, privi di archiviazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali e-commerce.*
B-IP	Esercenti che utilizzano solo terminali di pagamento autonomi e approvati PTS con connessione IP all'elaboratore di pagamenti e senza archiviazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali e-commerce.*
C-VT	Esercenti che inseriscono manualmente una singola transazione alla volta tramite tastiera, in una soluzione con terminali di pagamento virtuali basata su Internet, fornita e ospitata da un provider di servizi di terzi convalidato da PCI DSS. Nessuna memorizzazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali e-commerce.*
C	Esercenti con applicazioni di pagamento connesse a Internet. Nessuna memorizzazione elettronica dei dati dei titolari di carta. *Non applicabile ai canali e-commerce.*

SAQ	Descrizione
P2PE	Esercenti che usano terminali di pagamento hardware compresi e gestiti tramite una soluzione PCI Point-to-Point Encryption (P2PE) inclusa nell'elenco PCI SSC, senza memorizzazione dei dati dei titolari di carta. *Non applicabile ai canali e-commerce.*
D	***SAQ D Esercenti:*** tutti gli esercenti non inclusi nelle descrizioni dei SAQ precedenti.
	SAQ D Provider di servizi: tutti i provider di servizi definiti da un marchio di pagamento come idonei a completare un SAQ.

SAQ A: esercenti con carta non presente, tutte le funzioni per i dati dei titolari di carta sono fornite dall'esterno

Il modulo SAQ A è stato sviluppato per rispondere ai requisiti applicabili agli esercenti le cui funzioni per i dati dei titolari di carta sono state completamente esternalizzate a terzi convalidati, per cui l'esercente conserva soltanto i resoconti cartacei o le ricevute con i dati dei titolari di carta.

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Gli esercenti SAQ A possono svolgere la propria attività sia mediante e-commerce sia tramite ordini per posta/telefono (con carta non presente) e non memorizzano, elaborano o trasmettono i dati dei titolari di carta in formato elettronico nei loro sistemi o presso le loro sedi.

Gli esercenti SAQ A confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

- L'azienda accetta solo transazioni con carta non presente (e-commerce o via posta/telefono);
- Tutte le operazioni di elaborazione dei dati dei titolari di carta vengono interamente esternalizzate a provider di servizi di terzi convalidati PCIDSS;
- L'azienda non memorizza, elabora o trasmette in formato elettronico i dati di titolari di carta nei propri sistemi o sedi, ma si affida interamente a provider di servizi di terzi per tutte queste operazioni;
- L'azienda ha confermato che la terza parte che si occupa della memorizzazione, dell'elaborazione e/o della trasmissione dei dati di titolari di carta è conforme agli standard PCI DSS;
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei).

Inoltre, per canali di e-commerce:

- Tutti gli elementi delle pagine di pagamento che vengono inviati al browser del consumatore provengono direttamente e soltanto da un provider di servizi di terzi PCI DSS convalidato.

Questo SAQ non è applicabile ai canali che prevedono un contatto diretto con il cliente.

SAQ A-EP – Outsourcing parziale Esercenti di e-commerce che usano siti web di terzi per l'elaborazione dei pagamenti

SAQ A-EP è stato sviluppato per rispondere ai requisiti applicabili agli esercenti di e-commerce con siti web che non ricevono i dati dei titolari di carta direttamente, ma che incidono sulla sicurezza della transazione di pagamento e/o sull'integrità della pagina che accetta i dati dei titolari di carta.

Gli esercenti SAQ A-EP sono esercenti di e-commerce che si avvalgono parzialmente di terzi convalidati PCI DSS per la gestione del proprio canale di pagamento di e-commerce e che non memorizzano, elaborano né trasmettono in formato elettronico i dati dei titolari di carta nei propri sistemi o sedi.

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Gli esercenti SAQ A-EP confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

- L'azienda accetta solo le transazioni di e-commerce;
- Tutte le operazioni di elaborazione dei dati dei titolari di carta, fatta eccezione per la pagina dei pagamenti, vengono esternalizzate a un terzo elaboratore di pagamenti convalidato PCI DSS;
- Il sito web non riceve i dati dei titolari di carta direttamente, ma verifica in che modo i consumatori o i relativi dati di titolari di carta vengono indirizzati a un elaboratore di pagamenti di terzi convalidato PCI DSS;
- Il sito web dell'esercente è ospitato da un provider di terzi convalidato in base a tutti i requisiti PCI DSS applicabili (ad es., inclusa l'Appendice A PCI DSS se il provider è un provider di hosting condiviso);
- Tutti gli elementi delle pagine di pagamento che vengono inviati al browser del consumatore provengono dal sito web dell'esercente o da un provider di servizi conforme agli standard PCI DSS;
- L'azienda non memorizza, elabora o trasmette in formato elettronico i dati di titolari di carta nei propri sistemi o sedi, ma si affida interamente a provider di servizi di terzi per tutte queste operazioni;
- L'azienda ha confermato che la terza parte che si occupa della memorizzazione, dell'elaborazione e/o della trasmissione dei dati di titolari di carta è conforme agli standard PCI DSS;
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei).

Questo SAQ è applicabile solo ai canali di e-commerce.

Nota: *ai fini di questo questionario SAQ, i requisiti PCI DSS che fanno riferimento all'"ambiente dei dati dei titolari di carta" sono applicabili ai siti web dell'esercente. Questo perché il sito dell'esercente influisce direttamente sulla modalità di trasmissione dei dati dei titolari di carta, anche se il sito web stesso non riceve alcun dato.*

SAQ B: esercenti dotati solo di dispositivi di stampa o solo di terminali per connessione in uscita indipendenti. Nessuna memorizzazione elettronica dei dati dei titolari di carta

Il questionario SAQ B è stato sviluppato per rispondere ai requisiti applicabili a esercenti che elaborano i dati di titolari di carta solo tramite dispositivi di stampa o terminali per connessione in uscita indipendenti.

Gli esercenti SAQ B possono essere punti vendita reali (con presenza fisica della carta) o società di vendita per posta/telefono (senza presenza fisica della carta) che non memorizzano i dati dei titolari di carta su alcun sistema informatico. Gli esercenti SAQ B confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

- L'azienda utilizza solo dispositivi di stampa e/o terminali per connessione in uscita indipendenti (connessi tramite la linea telefonica all'elaboratore di pagamenti) per acquisire i dati della carta di pagamento dei clienti;
- I terminali per connessione in uscita indipendenti non sono connessi ad altri sistemi all'interno dell'ambiente;
- I terminali per connessione in uscita indipendenti non sono connessi a Internet;
- L'azienda non trasmette i dati dei titolari di carta tramite una rete (né interna né Internet);
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei);
- L'azienda non memorizza i dati dei titolari di carta in formato elettronico.

Questo SAQ non è applicabile ai canali di e-commerce.

SAQ B-IP – Esercenti con terminali per punti di interazione (POI) indipendenti PTS connessi tramite IP, senza memorizzazione elettronica dei dati dei titolari di carta

SAQ B-IP è stato sviluppato per rispondere ai requisiti applicabili agli esercenti che elaborano i dati dei titolari di carta solo mediante dispositivi per punti di interazione (POI) autonomi e approvati PTS con una connessione IP all'elaboratore di pagamenti.

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Gli esercenti SAQ B-IP possono essere punti vendita reali (con presenza fisica della carta) o società di vendita per posta/telefono (senza presenza fisica della carta) che non memorizzano i dati dei titolari di carta su alcun sistema informatico.

Gli esercenti SAQ B-IP confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

- L'azienda utilizza solo dispositivi per punti di interazione (POI) autonomi e approvati PTS (esclusi gli SCR) connessi tramite IP all'elaboratore di pagamenti per acquisire i dati della carta di pagamento dei clienti;
- I dispositivi POI autonomi connessi mediante IP vengono convalidati in base al programma POI di PTS secondo quanto indicato sul sito web PCI SSC (esclusi gli SCR);
- I dispositivi POI autonomi connessi mediante IP non sono collegati ad altri sistemi all'interno dell'ambiente (risultato ottenibile tramite le segmentazione della rete per isolare i dispositivi POI dagli altri sistemi);
- L'unica trasmissione dei dati di titolari di carta avviene dai dispositivi POI approvati da PTS all'elaboratore di pagamenti;
- Il dispositivo POI non si basa su eventuali altri dispositivi (ad esempio computer, cellulari, tablet ecc.) per collegarsi all'elaboratore di pagamenti;
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei);
- L'azienda non memorizza i dati dei titolari di carta in formato elettronico.

Questo SAQ non è applicabile ai canali di e-commerce.

SAQ C-VT: esercenti con terminali di pagamento virtuali basati su web. Nessuna memorizzazione elettronica dei dati dei titolari di carta

Il questionario SAQ C-VT è stato sviluppato per rispondere ai requisiti applicabili a tutti gli esercenti che elaborano i dati dei titolari di carta solo mediante terminali virtuali isolati su computer connessi a Internet.

Un terminale virtuale è un accesso basato su browser web al sito di un acquirente, elaboratore o provider di servizi di terzi per autorizzare le transazioni della carta di pagamento, in cui l'esercente inserisce manualmente i dati della carta mediante un browser connesso in modo sicuro. A differenza dei terminali fisici, i terminali di pagamento virtuali non leggono i dati direttamente da una carta di pagamento, per cui i dati delle transazioni vanno inseriti manualmente.

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Gli esercenti SAQ C-VT elaborano i dati dei titolari di carta solo tramite un terminale virtuale e non memorizzano le informazioni su un computer. I terminali virtuali sono connessi a Internet per accedere a terze parti che ospitano la funzione di elaborazione del pagamento del terminale virtuale. Questa terza parte può essere un elaboratore, un acquirente o un altro provider di servizi di terzi che memorizza, elabora e/o trasmette i dati dei titolari di carta per autorizzare e/o contabilizzare le transazioni di pagamento del terminale virtuale dell'esercente.

L'applicazione di questa opzione SAQ riguarda solo gli esercenti che inseriscono manualmente una singola transazione per volta tramite tastiera in una soluzione di terminale virtuale basato su Web. Gli esercenti SAQ C-VT possono essere punti vendita reali (con presenza fisica della carta) o società di vendita per posta/telefono (senza presenza fisica della carta).

Gli esercenti SAQ C-TV confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

- L'azienda elabora pagamenti solo ed esclusivamente mediante un terminale virtuale a cui si accede tramite un browser collegato a Internet;
- La soluzione di terminale virtuale dell'azienda è fornita e ospitata da un provider di servizi di terze parti convalidato PCI DSS;
- L'azienda accede alla soluzione di terminale di pagamento virtuale conforme a PCI DSS tramite un computer isolato in un unica sede e non collegato ad altre sedi o sistemi dell'ambiente aziendale (risultato ottenibile mediante segmentazione di rete o firewall per isolare il computer dagli altri sistemi);
- Il computer dell'azienda non ha software installati che determinino la memorizzazione dei dati dei titolari di carta (ad esempio, non ha software per l'elaborazione di batch o store-and-forward);
- Il computer dell'azienda non dispone di dispositivi hardware collegati usati per acquisire o memorizzare i dati dei titolari di carta (ad esempio non è collegato a un lettore di carte);
- L'azienda non riceve o trasmette in altro modo i dati dei titolari di carta per via elettronica tramite alcun canale (ad esempio mediante una rete interna o Internet);
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei);
- L'azienda non memorizza i dati dei titolari di carta in formato elettronico.

Questo SAQ non è applicabile ai canali di e-commerce.

SAQ C: esercenti con sistemi di pagamento connessi a Internet. Nessuna memorizzazione elettronica dei dati dei titolari di carta

Il questionario SAQ C è stato sviluppato per rispondere ai requisiti applicabili a esercenti i cui sistemi di pagamento (ad esempio, sistemi POS) sono connessi a Internet (ad esempio tramite DSL, modem via cavo, ecc.).

Gli esercenti SAQ C elaborano i dati dei titolari di carta mediante sistemi POS o altri sistemi di pagamento connessi a Internet, non memorizzano tali dati su un computer e possono essere aziende di e-commerce con punti vendita reali (carta presente) o società di vendita per posta/telefono (carta non presente).

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Gli esercenti SAQ C confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

- L'azienda dispone di un sistema di applicazione per i pagamenti e di una connessione Internet sul medesimo dispositivo e/o sulla stessa rete locale (LAN);
- Il sistema di applicazione di pagamento/dispositivo Internet non è connesso ad altri sistemi all'interno dell'ambiente (risultato ottenibile tramite la segmentazione della rete per isolare il sistema dell'applicazione di pagamento/dispositivo Internet da tutti gli altri sistemi);
- La sede fisica dell'ambiente POS non è connessa ad altre sedi o posizioni e la rete LAN è limitata a un singolo punto vendita;
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei);
- L'azienda non memorizza i dati dei titolari di carta in formato elettronico.

Questo SAQ non è applicabile ai canali di e-commerce.

SAQ P2PE – Esercenti che usano solo terminali di pagamento hardware in una soluzione P2PE inclusa nell'elenco PCI SSC, senza memorizzazione elettronica dei dati dei titolari di carta

Il questionario SAQ P2PE è stato sviluppato per rispondere ai requisiti applicabili agli esercenti che elaborano i dati dei titolari di carta esclusivamente tramite terminali di pagamento inclusi in una soluzione P2PE (Point-to-PointEncryption) convalidata e inclusa nell'elenco PCI SSC.

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Gli esercenti SAQ P2PE non dispongono dell'accesso ai dati dei titolari di carta con testo in chiaro su alcun sistema informatico e inseriscono i dati degli account tramite terminali di pagamento hardware presenti in una soluzione P2PE approvata PCI SSC. Gli esercenti SAQ P2PE possono essere punti vendita reali (con presenza fisica della carta) o società di vendita per posta/telefono (senza presenza fisica della carta). Ad esempio, una società di vendita per posta/telefono potrebbe essere idonea al SAQ P2PE se riceve i dati dei titolari di carta in formato cartaceo o per telefono e se attribuisce loro una chiave direttamente e solo su un dispositivo hardware convalidato PCI SSC.

Gli esercenti SAQ P2PE confermano di soddisfare i requisiti di idoneità per questo canale di pagamento:

- Tutte le operazioni di elaborazione dei pagamenti avvengono tramite una soluzione P2PE convalidata che è stata approvata e inclusa nell'elenco da PCI SSC;
- Gli unici sistemi presenti nell'ambiente dell'esercente che memorizzano, elaborano o trasmettono i dati degli account sono i dispositivi per punti di interazione (POI), approvati per essere utilizzati con la soluzione P2PE convalidata e inclusa nell'elenco PCI;
- L'azienda non riceve o trasmette in altro modo i dati dei titolari di carta in formato elettronico;
- L'azienda verifica che non sia presente alcuna memorizzazione precedente dei dati dei titolari di carta all'interno dell'ambiente;
- L'azienda conserva su carta eventuali dati dei titolari di carta ricevuti in formato diverso da quello elettronico (ad esempio, resoconti o ricevute cartacei);
- L'azienda ha implementato tutti i controlli presenti nel *Manuale di istruzioni per P2PE (PIM)* fornito dal provider della soluzione P2PE.

Questo SAQ non è applicabile ai canali di e-commerce.

SAQ D Esercente: tutti gli altri esercenti idonei per il questionario SAQ

Il modulo SAQ D per esercenti è valido per gli esercenti idonei al questionario SAQ che non rispondono ai criteri previsti per altri tipi di SAQ.

Esempi di ambienti di esercenti che potrebbero avvalersi di SAQ D sono, senza limitazioni:

- Esercenti di e-commerce che accettano i dati dei titolari di carta nel loro sito web;
- Esercenti che utilizzano la memorizzazione elettronica dei dati dei titolari di carta;
- Esercenti che non memorizzano i dati dei titolari di carta in formato elettronico ma che non rispondono ai criteri di un altro tipo di SAQ;
- Esercenti con ambienti che potrebbero rispondere ai requisiti di un altro tipo di SAQ ma con altri requisiti PCI DSS applicabili al proprio ambiente.

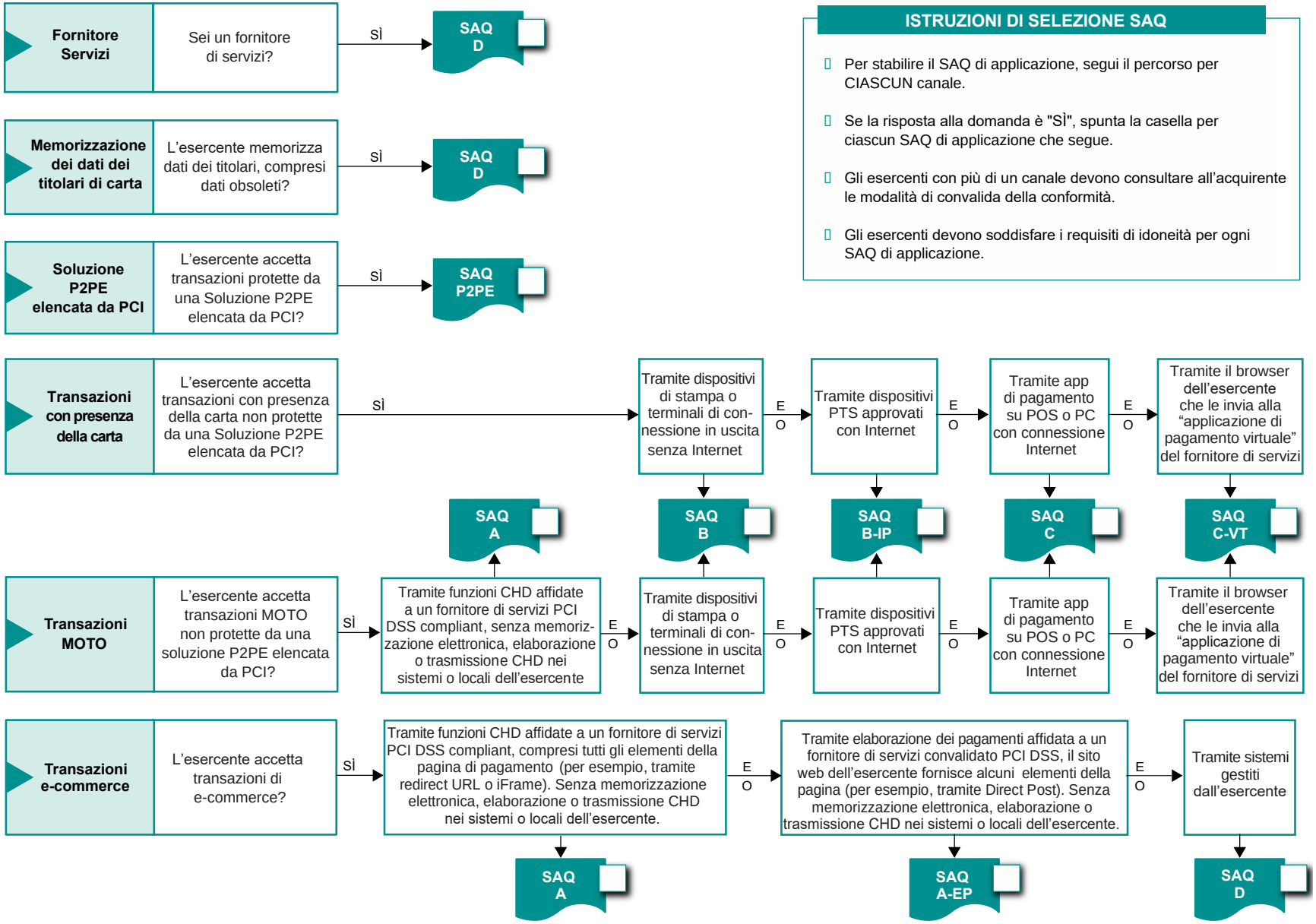
SAQ D Provider di servizi: provider di servizi idonei per il questionario SAQ

Il modulo SAQ D per i provider di servizi si applica a tutti i provider di servizi definiti da un marchio di pagamento come idonei per il questionario SAQ.

Nota sul SAQ D per Esercenti e Provider di servizi: sebbene molte aziende che completano il questionario SAQ D debbano convalidare la propria conformità a ogni requisito PCI DSS, alcune aziende con modelli di business molto specifici possono trovare non applicabili alcuni requisiti. Ad esempio, se un'azienda non usa la tecnologia wireless in nessuna sua forma, non dovrà rispettare i requisiti di conformità previsti dalle sezioni del PCI DSS che fanno riferimento a questa tecnologia. Per informazioni sull'esclusione di alcuni requisiti specifici, consultare la guida che segue.

Per una guida grafica alla scelta del tipo di questionario, vedere "Quale SAQ è più adatto al mio ambiente?" a pagina 19.

Quale SAQ è più adatto al mio ambiente?



ISTRUZIONI DI SELEZIONE SAQ

- Per stabilire il SAQ di applicazione, segui il percorso per CIASCUN canale.
- Se la risposta alla domanda è "SÌ", spunta la casella per ciascun SAQ di applicazione che segue.
- Gli esercenti con più di un canale devono consultare all'acquirente le modalità di convalida della conformità.
- Gli esercenti devono soddisfare i requisiti di idoneità per ogni SAQ di applicazione.