



Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS)

Guida al programma

Versione 1,2

Ottobre 2008

Modifiche del documento

Data	Versione	Descrizione
1 ottobre 2008	1.2	Allineare il contenuto ai nuovi standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.

Sommario

Modifiche del documento	1
Introduzione	3
Pubblicazioni correlate.....	3
Aggiornamenti dei documenti e dei requisiti di sicurezza.....	3
Terminologia.....	3
Informazioni su PCI.....	4
Iniziativa di allineamento PA-DSS e panoramica.....	4
Ruoli e responsabilità.....	5
Considerazioni per i fornitori – Preparazione per la revisione	8
A quali applicazione si riferisce il programma PA-DSS?.....	8
Prima della revisione.....	9
Documentazione e materiali richiesti.....	9
Tempi per la revisione PA-DSS.....	10
PA-QSA.....	10
Servizi PA-DSS correlati che possono essere offerti da PA-QSA.....	10
Supporto tecnico durante il test.....	11
Accordo di rilascio e consegna del rapporto.....	11
Tariffe.....	11
Panoramica dei processi PA-DSS	12
Figura 1: Processo di accettazione del rapporto PA-DSS.....	13
Figura 2: Modifiche PA-DSS ad applicazioni presenti in elenco.....	14
Figura 3: Grandfathering e trasferimento di applicazioni PABP nell'elenco PA-DSS.....	15
Figura 4: Riconvalida annuale PA-DSS e rinnovo delle applicazioni scadute.....	16
Figura 5: Programmi QA PA-QSA per revisioni dei rapporti.....	17
Panoramica del processo di accettazione del rapporto PA-DSS	18
Modifiche alle applicazioni di pagamento presenti in elenco	19
Rinnovo delle applicazioni scadute	22
Transizione e grandfathering di applicazioni di pagamento convalidate in base al programma PABP	23
Programma di controllo qualità (QA)	25
Processi di reporting PA-DSS	27
Notifica di una compromissione o violazione della sicurezza	28
Termini e condizioni legali	30
Appendice A: Elementi per la Lettera di accettazione e per l'Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS	31
Appendice B: Identificazione di build di applicazioni di pagamento certificate	34
Appendice C: Autocertificazione per modifica di versione minima	35

Introduzione

Pubblicazioni correlate

La documentazione seguente è la base per le valutazioni delle applicazioni di pagamento:

- *Payment Card Industry (PCI) Payment Application Data Security Standard – Procedure di audit della sicurezza*
- *Payment Card Industry (PCI) Payment Application Data Security Standard – Procedure di transizione*

Utilizzare i seguenti documenti aggiuntivi insieme ai documenti precedenti:

- *Standard di sicurezza dei dati PCI (Payment Card Industry) e procedure di valutazione della sicurezza*
- *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi*
- *Payment Card Industry (PCI) Data Security Standard - Requisiti di convalida per QSA*
- *Payment Card Industry (PCI) Data Security Standard - Requisiti di convalida per QSA - Supplemento per PA-QSA (Payment Application Qualified Security Assessor)*

Nota:

I requisiti PA-DSS e le procedure di valutazione della sicurezza elencano specifici requisiti tecnici e forniscono procedure e modelli di valutazione utilizzati per convalidare la conformità dell'applicazione di pagamento e documentare la revisione. I due documenti dei requisiti di convalida per QSA definiscono i requisiti che devono essere soddisfatti da un'azienda qualificata per valutare la sicurezza di un'applicazione di pagamento (PA-QSA).

Tutti i documenti sono disponibili in formato elettronico all'indirizzo www.pcisecuritystandards.org.

Aggiornamenti dei documenti e dei requisiti di sicurezza

Per garantire la sicurezza occorre lottare continuamente contro possibili intrusi. Di conseguenza, è necessario revisionare, aggiornare e migliorare costantemente i requisiti di sicurezza utilizzati per valutare le applicazioni di pagamento. In questo senso, PCI SSC si impegna ad aggiornare i requisiti di sicurezza delle applicazioni di pagamento ogni 24 mesi.

PCI SSC si riserva il diritto di modificare, correggere o eliminare determinati requisiti di sicurezza in qualsiasi momento. Se occorre apportare una modifica, PCI SSC collabora attivamente con la comunità di organizzazioni membri di PCI SSC e i fornitori del software per ridurre l'impatto di tale modifica.

Terminologia

Nel presente documento:

- "PCI SSC" si riferisce a PCI Security Standards Council, LLC.
- "PABP" è l'acronimo di Payment Application Best Practices, il programma Visa su cui si basa il programma PA-DSS (Payment Application Data Security Standard).
- "Marchi di pagamento" si riferisce ai marchi di carte di pagamento di organizzazioni membri di PCI SSC, attualmente American Express, Discover, JCB, MasterCard e Visa.
- "Applicazioni di pagamento" si riferisce in modo generale a tutte le applicazioni di pagamento che memorizzano, elaborano o trasmettono dati di titolari di carta nell'ambito del processo di autorizzazione o contabilizzazione, dove queste applicazioni di pagamento sono vendute, distribuite o concesse in licenza a terze parti.

Informazioni su PCI

PCI SSC risponde all'esigenza comune a tutti i livelli delle organizzazioni membri di PCI (Payment Card PCI) di allineare e standardizzare i requisiti di sicurezza, le procedure di valutazione della sicurezza e i processi per riconoscere applicazioni di pagamento convalidate da un PA-QSA, ossia un'azienda qualificata per valutare la sicurezza di questo tipo di applicazioni. Il programma PA-DSS e gli standard PCI SSC correlati definiscono una struttura comune per la valutazione della sicurezza riconosciuta da tutti i marchi di pagamento.

Tale allineamento dei requisiti di sicurezza è vantaggioso per tutti i partecipanti della catena del valore per le carte di pagamento:

- I clienti possono scegliere tra un numero più ampio di applicazioni di pagamento sicure.
- I clienti sono certi di utilizzare prodotti che soddisfano il livello di convalida richiesto.
- I fornitori dovranno completare solo una singola revisione dell'applicazione di pagamento che sarà riconosciuta da tutti i marchi di pagamento.

Per ulteriori informazioni su PCI SSC, fare riferimento al relativo sito Web all'indirizzo www.pcisecuritystandards.org (il "sito Web").

Iniziativa di allineamento PA-DSS e panoramica

Questa guida al programma PA-DSS di PCI riflette l'esigenza di allineamento dei requisiti dei marchi di pagamento a un set standard di:

- Requisiti di sicurezza delle applicazioni di pagamento e procedure di valutazione
- Processi per riconoscere le applicazioni di pagamento convalidate da PA-QSA
- Processi per inserire nell'elenco PCI SSC le applicazioni di pagamento convalidate in base al programma PABP
- Processi di controllo qualità (QA) per PA-QSA

Nota:

I rapporti PA-DSS vengono esaminati e riconosciuti direttamente da PCI SSC.

I requisiti di conformità tradizionali PCI DSS potrebbero non essere direttamente applicabili ai fornitori di applicazioni di pagamento, poiché la maggior parte dei fornitori non memorizza, elabora o trasmette dati di titolari di carta. Tuttavia, poiché queste applicazioni di pagamento sono utilizzate dai clienti per memorizzare, elaborare e trasmettere dati di titolari di carta e ai clienti viene richiesto di rispettare gli standard PCI DSS, le applicazioni di pagamento devono facilitare e non impedire la conformità a tali standard per i clienti. Di seguito alcuni esempi di come le applicazioni di pagamento possono impedire la conformità agli standard PCI DSS:

1. Dati della striscia magnetica memorizzati nella rete del cliente dopo l'autorizzazione;
2. Applicazioni che per un corretto funzionamento richiedono ai clienti di disattivare altre funzioni richieste dagli standard PCI DSS, quali software antivirus o firewall;
3. Uso di metodi non sicuri del fornitore per connettersi all'applicazione e fornire supporto al cliente.

Applicazioni di pagamento sicure, quando implementate in un ambiente conforme agli standard PCI DSS, riducono al minimo il rischio di violazioni della sicurezza che possono compromettere dati della striscia magnetica, valori e codici di validazione della carta (CAV2, CID, CVC2, CVV2), PIN e blocchi PIN e limitano i danni derivanti da tali violazioni.

Ruoli e responsabilità

La comunità delle applicazioni di pagamento è costituita da persone con ruoli diversi. Alcune di queste persone partecipano più direttamente al processo di valutazione della conformità agli standard PA-DSS, in particolare fornitori, PA-QSA e PCI SSC. Altre che non sono direttamente coinvolte nel processo di valutazione devono comunque conoscere l'intero processo per prendere decisioni a livello aziendale più appropriate.

Di seguito vengono definiti i ruoli e le responsabilità di tutti i membri della comunità delle applicazioni di pagamento. Le responsabilità elencate si riferiscono alle persone coinvolte nel processo di valutazione.

Marchi di pagamento

American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. sono i marchi di pagamento che hanno fondato PCI SSC. Questi marchi sono responsabili dello sviluppo e dell'applicazione di tutti i programmi correlati alla conformità agli standard PA-DSS, incluso, senza limitazione, quanto segue:

- Requisiti, mandati o date per l'uso di applicazioni di pagamento conformi agli standard PA-DSS
- Multe o sanzioni correlate all'uso di applicazioni di pagamento non conformi.

I marchi di pagamento possono definire programmi, mandati, date di conformità e altro utilizzando gli standard PA-DSS e le applicazioni di pagamento convalidate elencate da PCI SSC. Mediante questi programmi di conformità, tali marchi promuovono l'uso delle applicazioni di pagamento convalidate elencate.

PCI SSC (Payment Card Industry Security Standards Council)

PCI SSC è l'organismo che gestisce gli standard per le carte di pagamento, inclusi gli standard PCI DSS e PA-DSS. Relativamente al programma PA-DSS, PCI SSC:

- È un repository centralizzato per i rapporti di convalida (ROV, Reports of Validation) PA-DSS
- Esegue controlli di qualità (QA) sui rapporti di convalida PA-DSS per confermare la congruenza e la qualità di tali rapporti
- Crea e gestisce un elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS sul sito Web *Tenere presente che questo elenco sarà disponibile sul sito Web a partire da ottobre 2008.*
- Qualifica e forma i PA-QSA per eseguire le revisioni PA-DSS
- Gestisce e aggiorna gli standard PA-DSS e la documentazione correlata in base a un processo specifico.

Tenere presente che PCI SSC non approva i rapporti da un punto di vista di convalida. Il ruolo del PA-QSA consiste nel documentare la conformità dell'applicazione di pagamento agli standard PA-DSS a partire dalla data di valutazione. Inoltre, PCI SSC esegue i controlli di qualità necessari per accertarsi che i PA-QSA documentino in modo accurato e completo le valutazioni PA-DSS.

Fornitori di software

I fornitori di software ("fornitori") sviluppano le applicazioni di pagamento che memorizzano, elaborano o trasmettono dati di titolari di carta nell'ambito del processo di autorizzazione o contabilizzazione e, quindi, vendono, distribuiscono e concedono in licenza queste applicazioni di pagamento a terze parti (clienti o rivenditori/responsabili dell'integrazione). I fornitori sono responsabili di:

- Creare applicazioni di pagamento conformi agli standard PA-DSS che facilitano e non impediscono la conformità agli standard PCI DSS per i clienti. L'applicazione non può richiedere un'impostazione di implementazione o configurazione che viola un requisito PCI DSS.

- Seguire i requisiti PCI DSS ogni volta che memorizzano, elaborano o trasmettono i dati di titolari di carta (ad esempio, durante la risoluzione dei problemi dei clienti).
- Creare una *Guida per l'implementazione del programma PA-DSS* specifica per ciascuna applicazione, in base ai requisiti del programma *Payment Application Data Security Standard (PA-DSS)*
- Formare clienti, rivenditori e responsabili dell'integrazione su come installare e configurare le applicazioni di pagamento in modo conforme agli standard PCI DSS.
- Assicurare che le applicazioni di pagamento soddisfino i requisiti PA-DSS superando una revisione PA-DSS come specificato nel documento *Requisiti PCI PA-DSS e procedure di valutazione della sicurezza*.

I fornitori inviano le relative applicazioni di pagamento e la documentazione di supporto al PA-QSA per la revisione. Qualsiasi accordo e costo associato alla valutazione viene negoziato tra fornitore e PA-QSA. I fornitori autorizzano i PA-QSA a inviare i rapporti di conformità agli standard PA-DSS completati a PCI SSC.

PA-QSA

I PA-QSA sono aziende qualificate e formate da PCI SSC per eseguire le revisioni PA-DSS, ossia per valutare la sicurezza delle applicazioni di pagamento. *Tenere presente che non tutte le aziende qualificate per la valutazione della sicurezza (QSA) sono PA-QSA, ossia aziende qualificate per valutare la sicurezza delle applicazioni di pagamento. Per diventare un PA-QSA, esistono ulteriori requisiti di qualifica che devono essere soddisfatti.*

I PA-QSA sono responsabili di:

- Eseguire le valutazioni delle applicazioni di pagamento in base alle Procedure di valutazione della sicurezza e ai Requisiti di convalida per PA-QSA.
- Fornire un feedback sulla conformità dell'applicazione di pagamento ai requisiti PA-DSS.
- Fornire una documentazione adeguata all'interno del rapporto di convalida (ROV) per dimostrare la conformità dell'applicazione di pagamento agli standard PA-DSS.
- Inviare il rapporto di convalida a PCI SSC, insieme all'attestato di convalida (firmato da entrambi, PA-QSA e fornitore).
- Gestire un processo di controllo qualità interno per le proprie attività.

È responsabilità del PA-QSA indicare se l'applicazione di pagamento è conforme. PCI SSC non approva i rapporti di convalida (ROV) da un punto di vista di conformità tecnica, ma sottopone a controlli di qualità tali rapporti per assicurare che documentino adeguatamente la dimostrazione della conformità.

Rivenditori/Responsabili dell'integrazione

I rivenditori e i responsabili dell'integrazione sono le entità che si occupano della vendita, dell'installazione e/o dell'assistenza delle applicazioni di pagamento per conto dei fornitori del software o di altri. I rivenditori e i responsabili dell'integrazione che svolgono servizi relativi alle applicazioni di pagamento conformi agli standard PA-DSS sono responsabili di:

- Implementare solo le applicazioni di pagamento conformi agli standard PA-DSS in un ambiente conforme agli standard PCI DSS (o fornire le istruzioni necessarie all' esercente).
- Configurare le applicazioni di pagamento (nel caso in cui sono fornite opzioni di configurazione) in base alla *Guida per l'implementazione del programma PA-DSS* del fornitore.
- Configurare le applicazioni di pagamento (o fornire le istruzioni necessarie all' esercente) in modo conforme agli standard PCI DSS.
- Fornire assistenza per le applicazioni di pagamento (ad esempio, risoluzione di problemi, aggiornamenti in remoto e assistenza in remoto) in base alla *Guida per l'implementazione del programma PA-DSS* e agli standard PCI DSS.

I rivenditori e i responsabili dell'integrazione non inviano applicazioni di pagamento per la valutazione. I prodotti possono essere inviati solo dal fornitore.

Clienti

I clienti sono esercenti, provider di servizi o altre persone che acquistano o ricevono un'applicazione di pagamento di terza parte per memorizzare, elaborare o trasmettere dati di titolari di carta nell'ambito del processo di autorizzazione o contabilizzazione delle transazioni. I clienti che desiderano utilizzare applicazioni conformi agli standard PA-DSS sono responsabili di:

- Implementare un'applicazione di pagamento conforme agli standard PA-DSS in un ambiente conforme agli standard PCI DSS.
- Configurare le applicazioni di pagamento (nel caso in cui sono fornite opzioni di configurazione) in base alla *Guida per l'implementazione del programma PA-DSS* del fornitore.
- Configurare l'applicazione di pagamento in modo conforme agli standard PCI DSS.
- Mantenere lo stato di conformità agli standard PCI DSS per l'ambiente e la configurazione dell'applicazione.

Nota:

Un'applicazione di pagamento conforme agli standard PA-DSS da sola non garantisce la conformità agli standard PCI DSS.

Dopo che PCI SSC avrà pubblicato l'elenco nella seconda metà del 2008, sul sito Web sarà disponibile per i clienti un elenco di applicazioni di pagamento convalidate insieme ad altro materiale di riferimento.

Considerazioni per i fornitori – Preparazione per la revisione

A quali applicazione si riferisce il programma PA-DSS?

Ai fini del programma PA-DSS, un'applicazione di pagamento è un'applicazione che memorizza, elabora o trasmette dati di titolari di carta nell'ambito del processo di autorizzazione o contabilizzazione delle transazioni, dove questa applicazione viene venduta, distribuita o concessa in licenza a terze parti.

La Guida seguente può essere utilizzata per determinare se il programma PA-DSS è valido per una determinata applicazione di pagamento:

- Il programma PA-DSS si riferisce ad applicazioni di pagamento che solitamente sono vendute e installate come "prodotti standard", senza alcuna personalizzazione da parte dei fornitori del software.
- Il programma PA-DSS è valido per applicazioni di pagamento fornite in moduli, che in genere includono un modulo "base" e altri moduli specifici dei tipi o delle funzioni dei clienti oppure personalizzati su richiesta dei clienti. Tale programma può essere applicato solo al modulo base se tale modulo è l'unico che esegue funzioni di pagamento (una volta ottenuta la conferma da un PA-QSA). Se anche altri moduli eseguono funzioni di pagamento, gli standard PA-DSS si applicano anche a tali moduli. Tenere presente che è consigliabile per i fornitori del software isolare le funzioni di pagamento in un singolo modulo o in un numero limitato di moduli base, riservando agli altri moduli funzioni non di pagamento. Questa strategia consigliata (non obbligatoria) consente di ridurre il numero di moduli che devono essere sottoposti alla revisione PA-DSS.
- Il programma PA-DSS NON è valido per un'applicazione di pagamento sviluppata e venduta per un solo cliente, poiché questa applicazione verrà esaminata nell'ambito della normale revisione per la valutazione della conformità agli standard PCI DSS del cliente. Tenere presente che un'applicazione di questo tipo (che può essere definita anche applicazione "su misura") è venduta a un solo cliente (in genere, un esercente o un provider di servizi importante) ed è progettata e sviluppata in base alle specifiche fornite dal cliente.
- Il programma PA-DSS NON si è valido per applicazioni di pagamento sviluppate da esercenti e provider di servizi se utilizzate solo in-house (non vendute, distribuite o concesse in licenza a terze parti), poiché le applicazioni di pagamento sviluppate in-house rientrano nella normale revisione per la valutazione della conformità agli standard PCI DSS dell'esercente o del provider di servizi.

Ad esempio, per gli ultimi due punti precedenti, se l'applicazione di pagamento sviluppata in-house o "su misura" memorizza dati sensibili di autenticazione vietati o consente l'uso di password complesse, tale applicazione verrà controllata nell'ambito della valutazione della conformità agli standard PCI DSS dell'esercente o del provider di servizi e non richiederà una valutazione di conformità agli standard PA-DSS separata.

Il seguente elenco, sebbene non completo, indica le applicazioni che NON sono applicazioni di pagamento valide per il programma PA-DSS (e che, quindi, non devono essere sottoposte alle valutazioni di conformità agli standard PA-DSS):

- Sistemi operativi su cui è installata un'applicazione di pagamento (ad esempio, Windows, Unix)
- Sistemi di database che memorizzano dati di titolari di carta (ad esempio, Oracle)
- Sistemi back-office che memorizzano dati di titolari di carta (ad esempio, per scopi di reporting o assistenza clienti)

Nota:

PCI SSC inserirà nell'elenco SOLO le applicazioni che sono applicazioni di pagamento.

Prima della revisione

- Rivedere entrambi i requisiti, PCI DSS e PA-DSS, e la documentazione correlata disponibili sul sito Web all'indirizzo <http://www.pcisecuritystandards.org/>.
- Determinare/valutare lo stato di conformità agli standard PA-DSS dell'applicazione di pagamento:
 - Eseguire un'analisi dei "gap" per verificare lo stato dell'applicazione di pagamento rispetto ai requisiti PA-DSS.
 - Correggere eventuali gap.
 - Se si desidera, il PA-QSA può eseguire una pre-valutazione o analisi dei "gap" di un'applicazione di pagamento di un fornitore. In questo modo, se rileva dei problemi, può indicare preventivamente al fornitore del software le caratteristiche dell'applicazione di pagamento da correggere prima di iniziare il processo di revisione formale.
- Determinare se la *Guida per l'Implementazione del programma PA-DSS* soddisfa i requisiti PA-DSS.

Documentazione e materiali richiesti

Come requisito per la valutazione, il PA-QSA deve ricevere dal fornitore del software documentazione e software appropriati.

Tutte le informazioni e i documenti rilevanti per la valutazione di conformità agli standard PA-DSS possono essere scaricati dal sito Web. Tutti i materiali correlati all'applicazione di pagamento disponibili, quali CD di installazione, manuali, *Guida per l'implementazione del programma PA-DSS* e altro, necessari per la revisione devono essere consegnati a un'azienda qualificata (PA-QSA) tra quelle elencate sul sito Web, non a PCI SSC. Informazioni specifiche sulla revisione devono essere richieste direttamente dal PA-QSA.

Di seguito alcuni esempi di documenti e materiali da inviare al PA-QSA:

1. L'applicazione di pagamento con il manuale o le istruzioni dell'operatore
2. Gli accessori hardware e software necessari per eseguire transazioni di pagamento simulate
3. La documentazione che descrive tutte le funzioni per l'input e l'output dei dati che possono essere utilizzate dagli sviluppatori di applicazioni di terze parti. In modo specifico, devono essere descritte le funzioni associate ai flussi di acquisizione, autorizzazione, contabilizzazione e rettifica (se validi per l'applicazione). Un manuale è un esempio di documento che può soddisfare questo requisito.
4. La documentazione relativa all'installazione e alla configurazione dell'applicazione o che fornisce informazioni sull'applicazione. Di seguito alcuni esempi di tale documentazione:
 - *Guida per l'implementazione del programma PA-DSS*
 - Guida o istruzioni per l'installazione del software (fornita ai clienti)
 - Schema della numerazione delle versioni del fornitore
 - Documentazione di controllo delle modifiche che mostra come le modifiche vengono illustrate ai clienti
5. Ulteriore documentazione, quali diagrammi e diagrammi di flusso, di supporto durante la revisione dell'applicazione di pagamento (il PA-QSA può richiedere ulteriore materiale, se necessario).

Tempi per la revisione PA-DSS

La quantità di tempo necessaria per una revisione PA-DSS completa, il cui esito è un'applicazione convalidata con tutte le voci contrassegnate come "presenti", può variare molto. I fattori che determinano la durata della revisione sono:

- Il livello di conformità agli standard PA-DSS dell'applicazione all'inizio della revisione
 - Le correzioni all'applicazione di pagamento necessarie per raggiungere il livello di conformità necessario
- Il livello di preparazione della *Guida per l'implementazione del programma PA-DSS* all'inizio della revisione
 - Ampie riscritture della *Guida* aumentano la quantità di tempo richiesta per la revisione
- Se il PA-QSA prepara e invia un rapporto di convalida PA-DSS di alta qualità a PCI SSC
 - Se PCI SSC rivede il rapporto più di una volta, fornendo commenti al PA-QSA su caratteristiche da correggere ogni volta. In tal caso, la quantità di tempo necessario aumenta.

Qualsiasi indicazione del tempo necessario per la revisione fornita da un PA-QSA deve essere considerata una stima, poiché potrebbe essere basata sul presupposto che l'applicazione di pagamento soddisfi completamente e rapidamente i requisiti PA-DSS. In caso di problemi durante il processo di revisione o accettazione, tali problemi devono essere esaminati dal PA-QSA, dal fornitore del software e/o da PCI SSC. Queste discussioni possono avere un impatto sul tempo di revisione e causare ritardi e/o anche una fine prematura della revisione (se, ad esempio, il fornitore decide che non desidera apportare all'applicazione di pagamento le modifiche necessarie per raggiungere il livello di conformità richiesto).

PA-QSA

PCI SSC qualifica e forma i PA-QSA, ossia le aziende qualificate per valutare la conformità delle applicazioni di pagamento agli standard PA-DSS. Sul sito Web è disponibile un elenco di PA-QSA riconosciuti. Tali aziende sono le sole aziende autorizzate da PCI SSC ad eseguire valutazioni PA-DSS.

I prezzi e le tariffe addebitate dai PA-QSA non sono definiti da PCI SSC, ma sono negoziate tra il PA-QSA e il cliente. Prima di decidere il PA-QSA appropriato, si consiglia di consultare diverse aziende PA-QSA e seguire i processi di selezione dei fornitori della propria società.

Servizi PA-DSS correlati che possono essere offerti da PA-QSA

Nessuno di questi servizi è richiesto o consigliato da PCI SSC. Il presente elenco è incluso per fornire alcuni esempi dei tipi di servizi che possono essere offerti dai PA-QSA. Per informazioni sulla disponibilità e sui prezzi di tali servizi, contattare direttamente i PA-QSA. Di seguito alcuni esempi di servizi correlati al programma PA-DSS:

- Istruzioni sulla progettazione di applicazioni di pagamento conformi agli standard PA-DSS
- Revisione del software di un fornitore, risposta a domande via e-mail o telefono e partecipazione a chiamate in conferenza per chiarire i requisiti
- Istruzioni sulla preparazione della *Guida per l'implementazione del programma PA-DSS*
- Servizi di pre-valutazione (analisi dei "gap") prima di iniziare la valutazione formale della conformità agli standard PA-DSS
- Istruzioni per rendere l'applicazione di pagamento conforme agli standard PA-DSS se vengono rilevati gap o aree di non conformità durante la valutazione

Supporto tecnico durante il test

È consigliabile che un tecnico del fornitore sia disponibile per eventuali domande durante la valutazione. Durante la revisione e per accelerare il processo, un contatto del fornitore deve essere "disponibile" per fornire chiarimenti e rispondere a domande del PA-QSA.

Accordo di rilascio e consegna del rapporto

Affinché il PA-QSA possa inviare il rapporto PA-DSS a PCI SSC, il fornitore deve prima firmare l'*Accordo di rilascio del fornitore PA-DSS PCI* ("Accordo di rilascio"), che autorizza l'invio del rapporto a PCI SSC per la revisione. Tale accordo deve essere consegnato direttamente a PCI SSC dal PA-QSA, insieme ai rapporti PA-DSS.

Tariffe

Tutte le tariffe e le date correlate alla valutazione della conformità agli standard PA-DSS del PA-QSA sono negoziate tra il PA-QSA e il fornitore dell'applicazione di pagamento. Il fornitore effettua il pagamento direttamente al PA-QSA.

Ai fornitori verrà addebitato un costo annuale di \$1.250 per ogni applicazione di pagamento presente nell'elenco di applicazioni convalidate di PCI SSC.

Nell'ambito del processo di riconvalida annuale (vedere la sezione specifica più avanti nel documento), tale tariffa verrà fatturata annualmente da PCI SSC ai fornitori di software per tutte le applicazioni di pagamento incluse nell'elenco PCI SSC per tale fornitore in corrispondenza della data di fatturazione. La data di fatturazione sarà trimestrale, in base al trimestre dell'elenco originale. Ad esempio, l'1 aprile verrà addebitato ai fornitori di software l'importo di \$1.250 per applicazione di pagamento elencata a partire dal trimestre che termina il 31 marzo. Non verranno addebitate le applicazioni convalidate ma non incluse nell'elenco sul sito Web per richiesta del fornitore del software. Tenere presente che ai fornitori non sarà consentito modificare gli elenchi per evitare l'addebito. Ciò significa che i fornitori non possono rimuovere dall'elenco un'applicazione e quindi richiederne nuovamente l'inserimento dopo la fatturazione.

Nota:

Il fornitore paga tutte le spese della valutazione di conformità agli standard PA-DSS direttamente al PA-QSA (queste tariffe sono negoziate tra il fornitore e il PA-QSA).

PCI SSC invierà una fattura al fornitore ogni tre mesi per tutte le applicazioni incluse nell'elenco e il fornitore effettuerà il pagamento direttamente a PCI SSC.

Panoramica dei processi PA-DSS

Il processo di revisione PA-DSS viene avviato dal fornitore. Sul sito Web sono disponibili tutti i documenti associati necessari al fornitore per completare il processo di revisione della conformità agli standard PA-DSS. Il fornitore seleziona un PA-QSA dall'elenco di PCI SSC e discute costi e NDA con il PA-QSA. Quindi, fornisce al PA-QSA il software dell'applicazione di pagamento, i manuali e altra documentazione richiesta. PCI SSC invia una lettera di accettazione, confermando il corretto completamento del processo per ciascuna applicazione di pagamento ("Lettera di accettazione PA-DSS"). Una volta accettata l'applicazione di pagamento, il prodotto viene inserito nell'elenco sul sito Web.

Le illustrazioni e le descrizioni nelle pagine seguenti spiegano dettagliatamente i componenti del programma PA-DSS:

Processo	Illustrazione	N. Pagina
Processo di accettazione del rapporto PA-DSS	Figura 1	13
Modifiche PA-DSS ad applicazioni presenti in elenco	Figura 2	14
Grandfathering e trasferimento di applicazioni PABP nell'elenco PA-DSS	Figura 3	15
Riconvalida annuale PA-DSS e rinnovo delle applicazioni scadute	Figura 4	16
Programma QA PA-QSA per revisioni dei rapporti	Figura 5	17

Figura 1: Processo di accettazione del rapporto PA-DSS

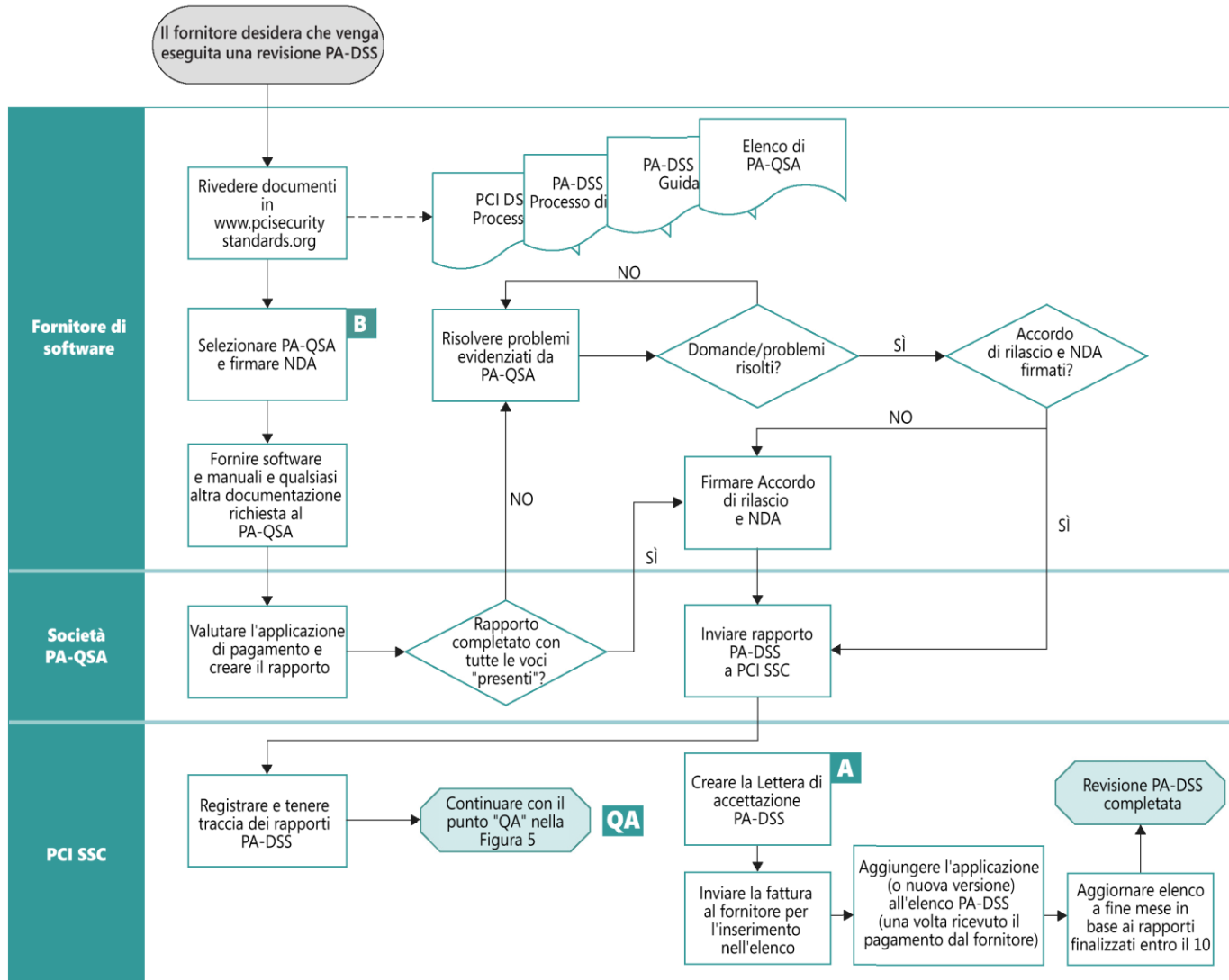


Figura 2: Modifiche PA-DSS ad applicazioni presenti in elenco

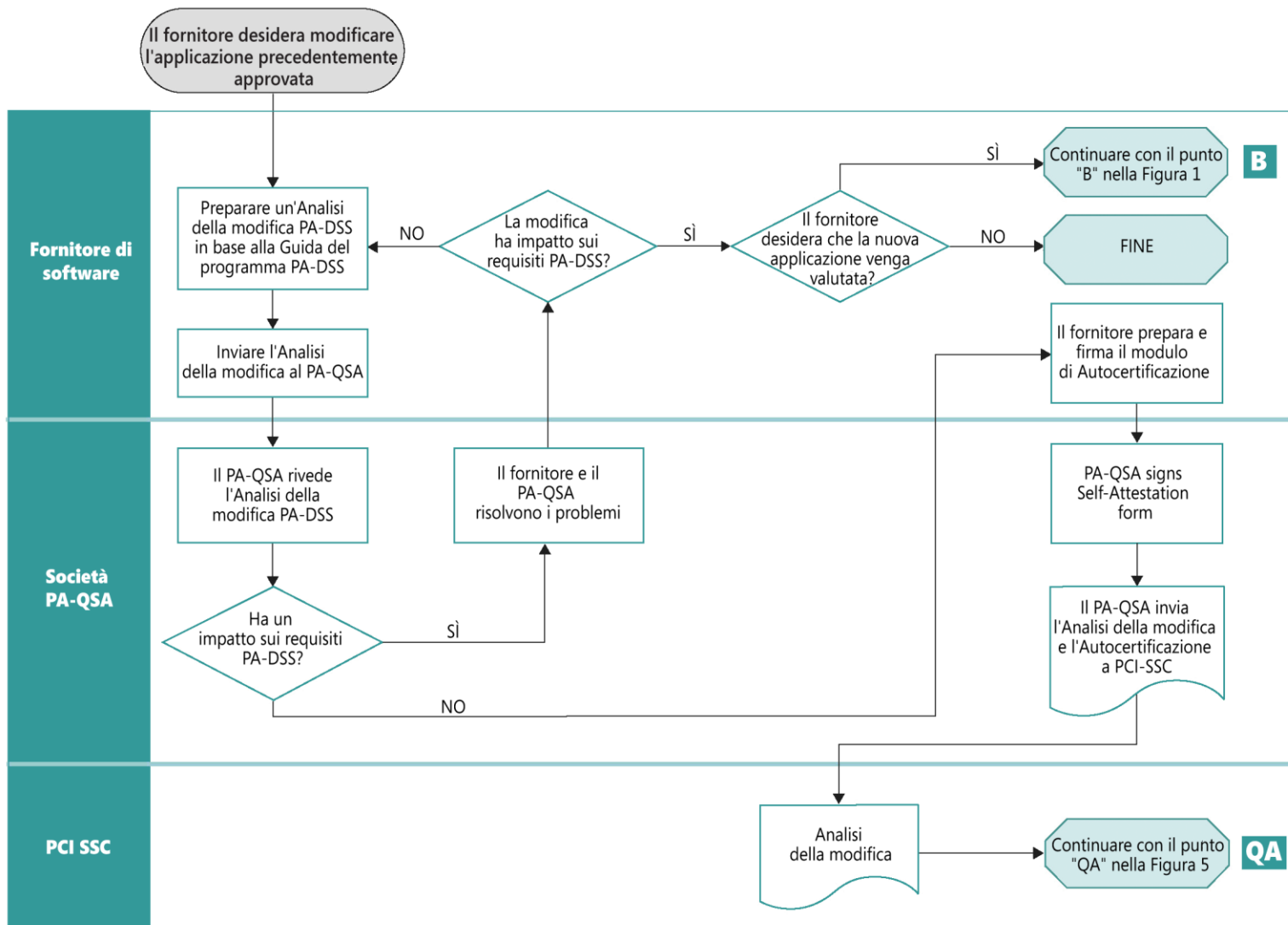


Figura 3: Grandfathering e trasferimento di applicazioni PABP nell'elenco PA-DSS

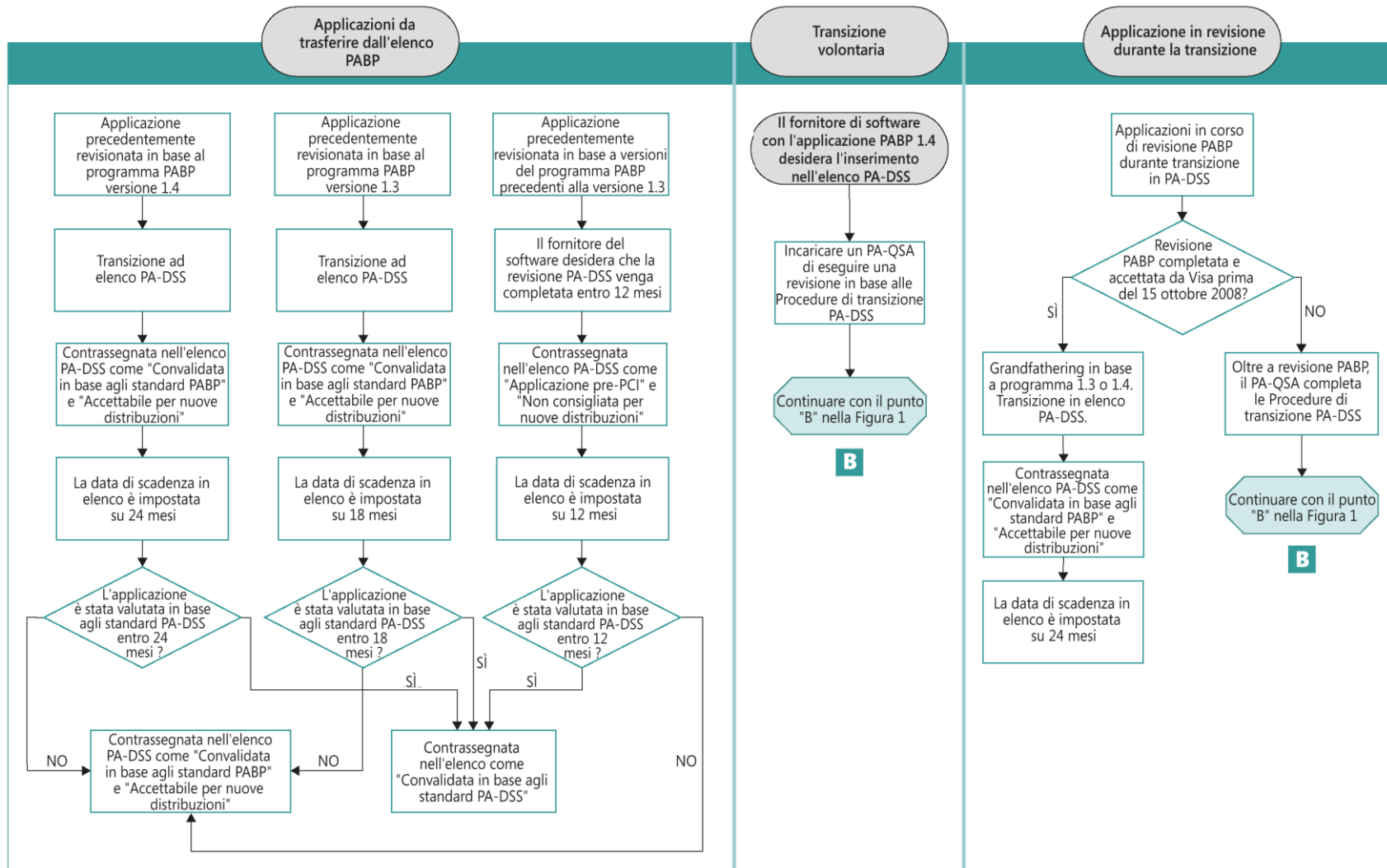


Figura 4: Riconvalida annuale PA-DSS e rinnovo delle applicazioni scadute

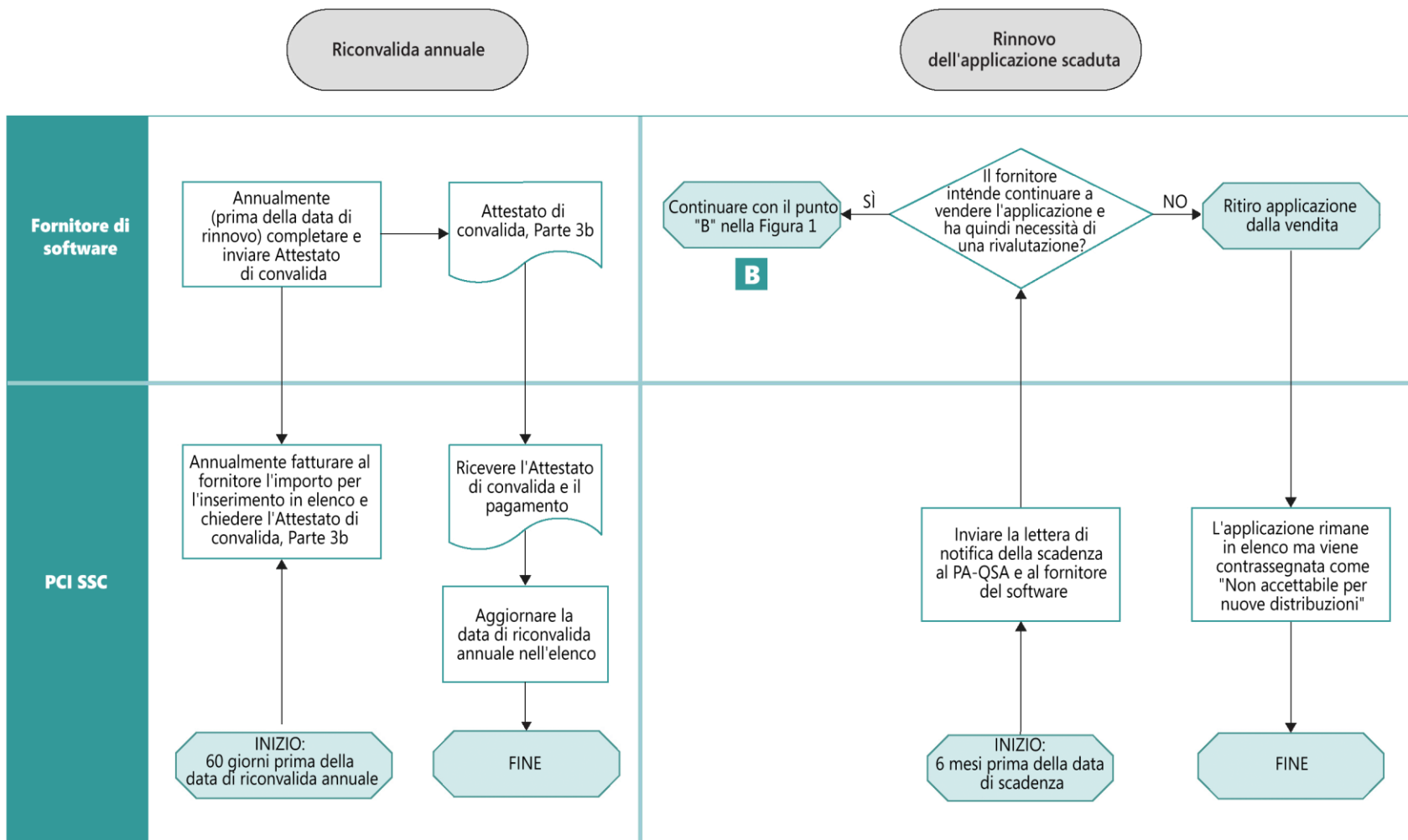
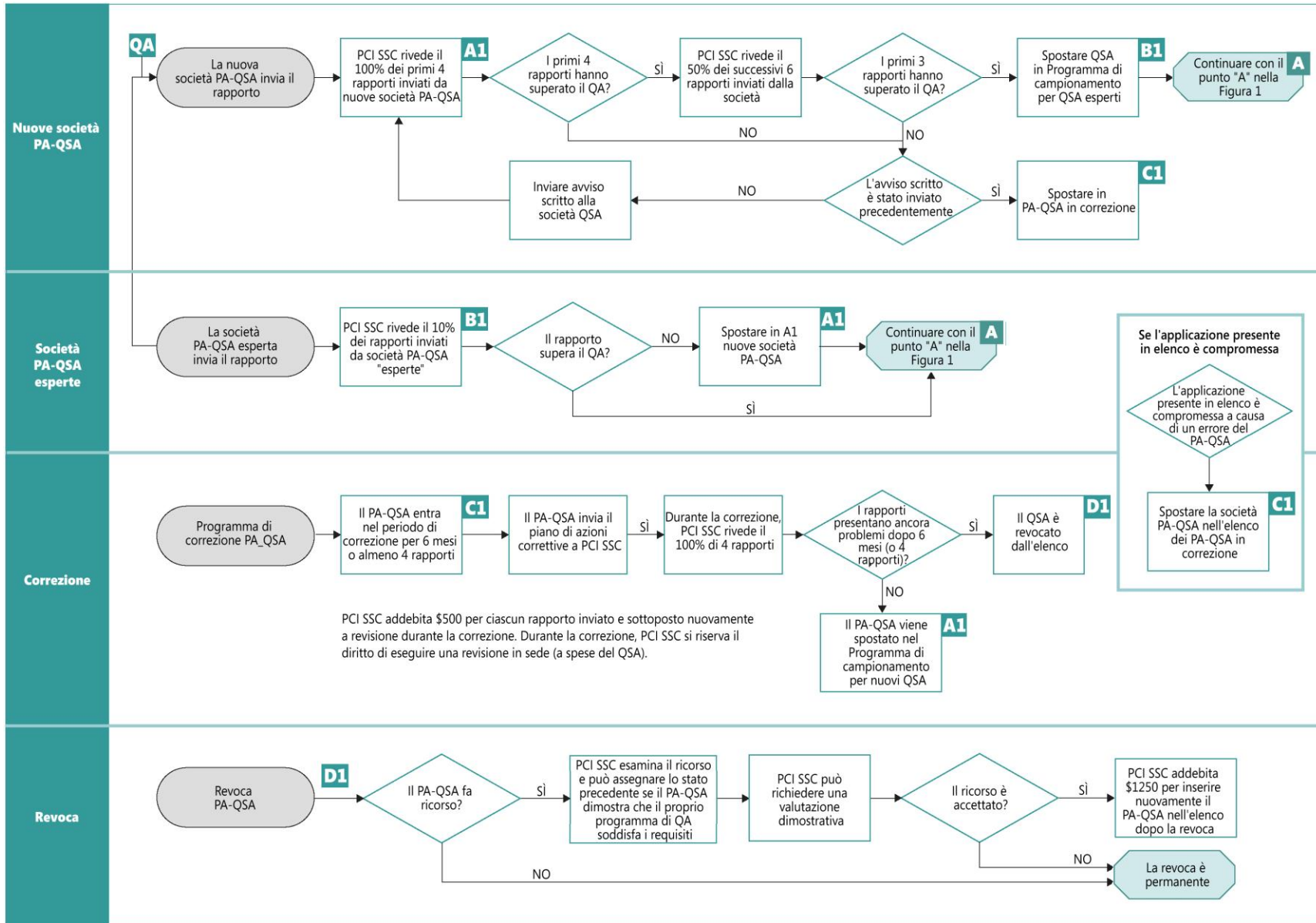


Figura 5: Programmi QA PA-QSA per revisioni dei rapporti



Panoramica del processo di accettazione del rapporto PA-DSS

Il PA-QSA esegue la revisione dell'applicazione di pagamento in base alle *Procedure di audit della sicurezza PA-DSS* e crea un rapporto che viene condiviso con il fornitore. Se tutte le voci del rapporto risultano "presenti", il fornitore firma l'*Accordo di rilascio* e il rapporto viene inviato dal PA-QSA a PCI SSC. Se non tutte le voci del rapporto risultano "presenti", il fornitore deve risolvere i problemi evidenziati. Ad esempio, aggiornare la documentazione per l'utente o il software. Dopo che il PA-QSA ha verificato che tutti i problemi documentati sono stati risolti dal fornitore, quest'ultimo firma l'*Accordo di rilascio* e il rapporto viene inviato dal PA-QSA a PCI SSC.

Tenere presente che le informazioni e tutti i rapporti PA-DSS devono essere inviati a PCI SSC in inglese.

PCI SSC riceve il rapporto e lo sottopone a un controllo di qualità. Se il rapporto soddisfa i requisiti del controllo di qualità come indicato nel documento dei requisiti di convalida QSA e nella documentazione di supporto, PCI SSC invia una Lettera di accettazione PA-DSS al fornitore e aggiunge l'applicazione al proprio elenco entro la fine del mese per le applicazioni finalizzate entro il 10 dello stesso mese. Per problemi di qualità associati al rapporto, PCI SSC comunica tali problemi al PA-QSA. È, quindi, responsabilità del PA-QSA risolvere i problemi con PCI SSC. È possibile che sia sufficiente aggiornare il rapporto in modo che rifletta la documentazione necessaria a supportare le decisioni del PA-QSA. Tuttavia, se sono necessari ulteriori controlli, il PA-QSA deve informare il fornitore di tale esigenza e pianificare tali controlli con il fornitore.

Il flusso del processo per l'accettazione del rapporto è illustrato dettagliatamente nella Figura 1.

Modifiche alle applicazioni di pagamento presenti in elenco

I fornitori aggiornano le applicazioni di pagamento già presenti nell'elenco per diversi motivi, ad esempio, l'aggiunta di altre funzionalità o l'aggiornamento dell'applicazione base.

Da un punto di vista dei requisiti PA-DSS, esistono sostanzialmente tre tipi di scenari di modifica:

1. Modifiche minime di un'applicazione di pagamento presente in elenco che non hanno alcun impatto sui requisiti PA-DSS. In tal caso, per la nuova versione da inserire in elenco, il fornitore del software invia la documentazione necessaria sulla modifica al PA-QSA affinché possa eseguire la revisione sulla base di tale modifica; per informazioni specifiche, vedere la sezione *Nessun impatto sui requisiti PA-DSS*.
2. Modifiche di un'applicazione di pagamento presente in elenco che hanno un possibile impatto sui requisiti PA-DSS. In tal caso, per la nuova versione da inserire in elenco, il fornitore del software invia la nuova versione dell'applicazione di pagamento al PA-QSA affinché possa eseguire una revisione completa; per informazioni specifiche, vedere la sezione *Possibile impatto sui requisiti PA-DSS*.
3. Nessuna modifica apportata a un'applicazione di pagamento presente in elenco. In questo caso, viene richiesto solo un attestato annuale; per informazioni specifiche, vedere la sezione *Nessuna modifica apportata all'applicazione di pagamento presente in elenco*.

In casi simili, dove vengono aggiornate applicazioni già presenti nell'elenco e il fornitore desidera che le nuove informazioni sull'applicazione di pagamento vengano riportate nell'elenco, il fornitore deve inviare i dettagli di tali modifiche al PA-QSA, preferibilmente al PA-QSA che originariamente ha valutato l'applicazione di pagamento.

Il PA-QSA, quindi, determina se è necessaria una rivalutazione dell'applicazione. Questa decisione può dipendere dall'impatto delle modifiche apportate sulla sicurezza dell'applicazione. Un'altra considerazione può essere lo scopo o l'ambito delle modifiche apportate. Ad esempio, le modifiche possono avere impatto solo sulla funzionalità aggiuntiva e non sull'applicazione base.

Se un'applicazione di pagamento già presente in elenco è soggetta a continue modifiche che potenzialmente hanno effetto sui requisiti PA-DSS e/o se il fornitore desidera modificare le informazioni nella *Lettera di accettazione PA-DSS* e sul sito Web, il fornitore deve inviare la documentazione delle modifiche appropriata al PA-QSA per determinare se occorre eseguire una valutazione completa. Il PA-QSA, se concorda con il fornitore che le modifiche documentate non hanno impatto sui requisiti PA-DSS, informa il fornitore del software, che a sua volta prepara e firma un modulo di autocertificazione delle modifiche, che il PA-QSA firmerà e invierà a PCI SSC. PCI SSC, quindi, riporta gli aggiornamenti nella *Lettera di accettazione PA-DSS* e sul sito Web. Per ulteriori informazioni, vedere di seguito la sezione *Nessun impatto sui requisiti PA-DSS: Nuova revisione PA-DSS non richiesta*.

Nota:

Se i fornitori delle applicazioni di pagamento possono modularizzare la funzionalità di pagamento, le rivalutazioni a causa di modifiche che non hanno impatto sulla funzionalità di pagamento e sulla sicurezza possono essere ridotte al minimo.

Il flusso del processo per le modifiche delle applicazioni già presenti in elenco è illustrato dettagliatamente nella Figura 2.

Nessun impatto sui requisiti PA-DSS: Nuova revisione PA-DSS non richiesta

Se un'applicazione di pagamento precedentemente elencata viene revisionata, ma tale revisione sembra minima e non ha alcun impatto negativo sulla sicurezza, è possibile inviare la documentazione della modifica ("Analisi della modifica") al PA-QSA per la revisione. È consigliabile che il fornitore utilizzi lo stesso PA-QSA utilizzato per la valutazione originale.

L'Analisi della modifica inviata dal fornitore del software al PA-QSA deve contenere almeno le seguenti informazioni:

- Nome dell'applicazione di pagamento
- Numero della versione dell'applicazione di pagamento
- Nome e numero di versione dell'applicazione di pagamento attualmente presente nell'elenco di PCI SSC
- Descrizione della modifica
- Descrizione del motivo della modifica
- Dettagli dell'eventuale impatto sui dati del titolare di carta e sulle funzioni di pagamento
- Descrizione del funzionamento della modifica
- Descrizione dei test eseguiti dal fornitore per confermare che la modifica non ha un impatto negativo sui requisiti di sicurezza PA-DSS
- Spiegazione del modo e del motivo per il quale non esiste un impatto negativo sui requisiti PA-DSS
- Descrizione di come questa modifica rientra nella metodologia di versioning del fornitore, incluso come questo numero di versione indica che si tratta di una modifica "minima"
- Se applicabile, la descrizione dell'uso di pratiche di programmazione/approcci a moduli e come tale uso impedisce un impatto negativo sui requisiti.

Se il PA-QSA concorda che la modifica come documentata nell'apposita analisi dal fornitore non ha un impatto negativo sulla sicurezza dell'applicazione di pagamento, (i) il PA-QSA informa il fornitore del software, (ii) il fornitore del software prepara e firma un modulo di autocertificazione della modifica e lo invia al PA-QSA, (iii) il PA-QSA firma il modulo e lo inoltra, insieme all'Analisi della modifica, a PCI SSC e (iv) PCI SSC rivede il modulo e la documentazione per eseguire i controlli di qualità necessari.

Se la modifica non ha alcun impatto sui requisiti PA-DSS:

- Una Lettera di accettazione PA-DSS revisionata verrà inviata al fornitore
- L'elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS sul sito Web verrà aggiornato di conseguenza con le nuove informazioni
- La data di scadenza di questa nuova applicazione elencata e il numero di versione saranno uguali a quelli dell'applicazione di pagamento "originaria".

In caso vengano rilevati problemi di qualità nel modulo di autocertificazione della modifica, PCI SSC informa il PA-QSA e tali problemi vengono risolti in base al processo descritto in precedenza.

Possibile impatto sui requisiti PA-DSS: Nuova revisione PA-DSS richiesta

Se le modifiche apportate all'applicazione di pagamento hanno un impatto sui requisiti PA-DSS, deve essere nuovamente valutata la conformità dell'applicazione di pagamento ai requisiti PA-DSS. Il PA-QSA invia, quindi, un nuovo rapporto PA-DSS a PCI SSC per l'accettazione. In questa situazione, il fornitore può inviare prima la documentazione della modifica al PA-QSA, che determinerà se la natura della modifica ha impatto sulla sicurezza dell'applicazione in base ai requisiti PA-DSS correnti.

Nessuna modifica all'applicazione di pagamento presente in elenco: Riconvalida annuale richiesta

Annualmente, in base alla data di riconvalida indicata nell'elenco, il fornitore del software deve inviare un Attestato di convalida con la parte 3b completata. L'Attestato di convalida si trova nell'Appendice C PA-DSS.

Il flusso del processo per la riconvalida annuale è illustrato dettagliatamente nella Figura 4.

Rinnovo delle applicazioni scadute

Man mano che un'applicazione si avvicina alla relativa data di scadenza, PCI SSC informa il fornitore del software della prossima scadenza. Le due opzioni disponibili per il fornitore sono:

1. Il fornitore desidera continuare a vendere l'applicazione. In tal caso, deve contattare un PA-QSA per richiedere la rivalutazione dell'applicazione di pagamento.
2. Il fornitore non desidera continuare a vendere l'applicazione. In tal caso, PCI SSC modifica lo stato dell'applicazione di pagamento nell'elenco in "non accettabile per nuove distribuzioni" dopo la data di scadenza.

Tenere presente che se il fornitore sceglie di continuare a vendere l'applicazione, l'applicazione dopo che ha superato di nuovo correttamente il processo di valutazione PA-DSS, viene contrassegnata nell'elenco di PCI SSC come "accettabile per nuove distribuzioni" e viene assegnata una nuova data di scadenza.

Il flusso del processo per il rinnovo delle applicazioni scadute è illustrato dettagliatamente nella Figura 4.

Transizione e grandfathering di applicazioni di pagamento convalidate in base al programma PABP

Grandfathering di applicazioni PABP nell'elenco PABP a partire dal 15 ottobre 2008

PCI SSC sta trasferendo (grandfathering) le applicazioni conformi al programma PABP nell'elenco PCI SSC. Questo approccio "grandfathering" consente alle applicazioni precedentemente valutate e trovate conformi ai requisiti PABP di continuare ad essere distribuite fino a quando applicazioni di pagamento conformi ai requisiti PA-DSS più nuove non saranno disponibili.

Un approccio a fasi è stato applicato alle date di scadenza delle applicazioni PABP, in base alla versione dei requisiti utilizzati per valutare l'applicazione. Per rimanere nell'elenco PCI SSC come applicazioni accettabili per nuove distribuzioni, le applicazioni conformi ai requisiti PABP devono essere valutate in base ai requisiti PA-DSS entro i tempi previsti. Se un'applicazione conforme ai requisiti PABP non viene valutata in base ai requisiti PA-DSS entro i tempi previsti, l'applicazione rimane nell'elenco PCI SSC, ma viene contrassegnata come non accettabile per nuove distribuzioni.

Nota:

L'elenco PCI SSC distingue tra "nuove distribuzioni" e "distribuzioni esistenti". Le applicazioni di pagamento spesso, una volta distribuite, hanno una lunga durata, possibilmente fino a 10-15 anni. PCI SSC è consapevole che la distribuzione di applicazioni di pagamento può essere un processo complesso e costoso e che può non essere pratico per esercenti e acquirenti aggiornare le applicazioni di pagamento ogni anno.

Il seguente diagramma mostra le rispettive date di scadenza e note che verranno incluse nell'*Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS* per le versioni PABP nonché per le revisioni PA-DSS in base agli standard PA-DSS v1.1 correnti.

Versione	Data di scadenza	Elenco PCI SSC prima della scadenza		Elenco PCI SSC dopo la scadenza	
		Note di convalida	Note di distribuzione	Note di convalida	Note di distribuzione
PABP 1,4	24 mesi	Convalidata in base a programma PABP	Accettabile per nuove distribuzioni	Convalidata in base a programma PABP	Non accettabile per nuove distribuzioni
PABP 1.3	18 mesi	Convalidata in base a programma PABP	Accettabile per nuove distribuzioni	Convalidata in base a programma PABP	Non accettabile per nuove distribuzioni
Precedente a PABP 1.3	12 mesi	Applicazione pre-PCI	Non consigliata per nuove distribuzioni	Applicazione pre-PCI	Non accettabile per nuove distribuzioni
PA-DSS 1.1	3 anni dopo la modifica dello standard	Convalidata in base a programma PA-DSS	Accettabile per nuove distribuzioni	Convalidata in base a programma PA-DSS	Non accettabile per nuove distribuzioni

Il flusso del processo di grandfathering e transizione delle applicazioni PABP è illustrato dettagliatamente nella Figura 3.

Applicazioni di pagamento soggette a revisioni PABP durante la transizione

Al momento del rilascio del programma PA-DSS Versione 1.1, ha avuto inizio un periodo di tolleranza di circa 6 mesi durante il quale i PA-QSA apprendono i nuovi standard, ricevono la formazione appropriata e ottengono la qualifica necessaria per eseguire le revisioni in base agli standard PA-DSS. In aggiunta, questo periodo di tolleranza ha consentito ai fornitori di conoscere gli standard PA-DSS e prendere in considerazione i nuovi requisiti PA-DSS durante lo sviluppo di nuove applicazioni di pagamento.

Durante il periodo di tolleranza, le applicazioni di pagamento possono continuare a essere valutate in base agli standard PABP versione 1.4. Il periodo di tolleranza termina il **15 ottobre 2008**¹, i rapporti inviati dopo tale data non verranno accettati per la convalida della conformità ai requisiti PABP.

I rapporti basati sugli standard PABP versione 1.4 inviati dopo il 15 ottobre 2008 devono essere sottoposti alle *Procedure di transizione PA-DSS*. Il PA-QSA può utilizzare i risultati dei rapporti PABP, ma deve inviare a PCI SSC anche una valutazione delta in base alle *Procedure di transizione PA-DSS*.

Il fornitore può scegliere, inoltre, di richiedere la valutazione della propria applicazione di pagamento in base agli standard PA-DSS in qualsiasi momento dopo il rilascio del nuovo standard.

Procedure di transizione PA-DSS

Le Procedure di transizione PA-DSS devono essere utilizzate dai PA-QSA, dove applicabile, per trasferire un'applicazione dall'elenco Visa di applicazioni di pagamento convalidate in base al programma PABP² all'elenco PCI SSC di applicazioni di pagamento convalidate in base al programma PA-DSS³.

Nota: PCI SSC sta trasferendo ("grandfathering") applicazioni di pagamento convalidate in base agli standard PABP versioni 1.3 e 1.4 nell'elenco delle applicazioni convalidate in base al programma PA-DSS per 18 e 24 mesi rispettivamente, prima di sottoporle a una revisione PA-DSS.

Tenere presente i seguenti scenari per l'applicazione di tali procedure di transizione:

Completamento obbligatorio delle procedure di transizione: Se la revisione di un'applicazione di pagamento in base agli standard PABP non viene completata e accettata da Visa prima del 15 ottobre 2008, è **obbligatorio** eseguire le Procedure di transizione per fare in modo che PCI SSC riconosca tale applicazione come convalidata in base agli standard PA-DSS. **Tenere presente che revisioni eseguite esclusivamente in base agli standard PABP NON saranno accettate dopo il 15.10.08.**

Nota:

La stessa società PA-QSA utilizzata per eseguire la revisione PABP deve essere utilizzata per eseguire le procedure di transizione PA-DSS.

Completamento facoltativo delle procedure di transizione: Per quanto riguarda la *Nota* precedente, se le applicazioni di un fornitore sono idonee per il "grandfathering", ma il fornitore desidera che un'applicazione PABP versione 1.3 o 1.4 venga riconosciuta nell'elenco come applicazione "Convalidata in base agli standard PA-DSS", è necessario utilizzare queste Procedure di transizione. Un PA-QSA esegue le procedure e invia il rapporto in base alla Guida del programma PA-DSS per fare in modo che PCI SSC riconosca le applicazioni PABP versione 1.3 e 1.4 come convalidate.

Per ulteriori informazioni sulle Procedure di transizione PA-DSS, vedere la sezione relativa alle *Procedure di transizione da PABP a PA-DSS* sul sito Web.

¹ Se un'applicazione di pagamento viene valutata in base agli standard PABP versione 1.4 e inviata prima del 15 ottobre 2008 e nel rapporto sono stati evidenziati alcuni problemi di qualità, è prevista un'eccezione. Tale applicazione può continuare il processo di revisione in base agli standard PABP versione 1.4 fino a quando non vengono risolti i problemi di qualità. Eccezioni di questo tipo sono consentite fino al 15 aprile 2009.

² Revisionato in base a standard PABP (Payment Application Best Practices), versioni 1.3 o 1.4

³ Revisionato in base a standard PA-DSS (Payment Application Data Security Standard), versione 1.1

Programma di controllo qualità (QA)

PCI SSC rivede i rapporti inviati dal PA-QSA ai fini del controllo qualità. Come indicato nei *Requisiti di convalida per QSA* e nell'*Accordo PA-QSA*, i PA-QSA devono soddisfare gli standard del controllo qualità definiti da PCI SSC. Le diverse fasi del programma di controllo qualità (QA) sono descritte di seguito.

Il flusso del processo per il programma di controllo qualità è illustrato dettagliatamente nella Figura 5.

Programma di campionamento per nuovi PA-QSA

PCI SSC utilizza un processo di campionamento a fasi per rivedere i rapporti di convalida dei PA-QSA; inizialmente, vengono esaminati più rapporti e man mano che il PA-QSA dimostra di soddisfare gli standard di qualità previsti il numero di rapporti esaminati viene ridotto. Man mano che il PA-QSA continua a soddisfare gli standard di qualità, viene trasferito nel Programma di campionamento per QSA esperti (con tassi di campionamento più bassi). Fin quando il PA-QSA soddisfa gli standard di qualità, sarà soggetto a un campionamento limitato.

Tuttavia, se il PA-QSA non soddisfa gli standard di qualità, vengono intraprese le seguenti azioni:

- Lettera di avviso: inviata al PA-QSA per indicare che è necessario migliorare la qualità.
- Correzione: se gli standard di qualità non sono ancora soddisfatti, il PA-QSA viene messo in fase di correzione e possono essere avviate alcune azioni correttive.
- Revoca: se gli standard di qualità non sono ancora soddisfatti, il PA-QSA viene revocato e rimosso dall'elenco PCI SSC di PA-QSA approvati.

Programma di campionamento per PA-QSA esperti

Una volta che il PA-QSA accede al programma di campionamento per PA-QSA esperti, viene controllato un numero di rapporti limitato. Se gli standard di qualità continuano ad essere soddisfatti, il campionamento rimane limitato. Questo è considerato lo "stato standard" in cui operano i PA-QSA.

Se si verificano problemi di qualità e gli standard non vengono soddisfatti, il PA-QSA ritorna al Programma di campionamento per nuovi PA-QSA.

Correzione

Durante la correzione, i PA-QSA possono comunque eseguire le revisioni, ma PCI SSC sottopone ai controlli di qualità tutti i rapporti da loro inviati. PCI SSC addebiterà \$500 per ciascun rapporto inviato e nuovamente inviato durante la correzione.

Il PA-QSA deve anche inviare un piano di azioni correttive a PCI SSC in cui descrive come intende migliorare la qualità dei propri rapporti. PCI SSC può richiedere, inoltre, un incontro con il PA-QSA per verificarne il programma di controllo qualità utilizzato, a spese del PA-QSA.

Se il PA-QSA soddisfa gli standard di qualità durante la correzione, passa al Programma di campionamento per nuovi PA-QSA. Se il PA-QSA non soddisfa gli standard di qualità durante la correzione, viene revocato.

Tenere presente che se un'applicazione di pagamento inclusa nell'*Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS* di PCI SSC viene compromessa a causa di un errore del PA-QSA, tale PA-QSA viene messo immediatamente in fase di correzione. Il PA-QSA dovrà soddisfare gli standard di qualità per tornare al Programma di campionamento per nuovi PA-QSA.

Revoca

Quando un PA-QSA viene revocato, viene rimosso dall'elenco di PA-QSA approvati di PCI SSC. Una volta revocato, il PA-QSA non può eseguire revisioni delle applicazioni di pagamento. Il PA-QSA può fare ricorso alla revoca, ma deve soddisfare i requisiti come documentato nei Requisiti di convalida per QSA e nei documenti di supporto. PCI SSC si riserva il diritto di richiedere una valutazione dimostrativa.

Per accedere nuovamente al Programma di campionamento per nuovi PA-QSA ed essere inseriti nell'elenco di PA-QSA approvati, è previsto il pagamento di una tariffa pari a \$1.250.

Processi di reporting PA-DSS

PCI SSC basa l'accettazione dei rapporti esclusivamente sui risultati documentati nel rapporto di convalida. Al momento della ricezione del rapporto, viene applicato quanto segue:

- PCI SSC rivede il rapporto (solitamente entro 30 giorni di calendario dalla ricezione) e determina se è accettabile.
- Se non vengono identificati problemi o domande da porre al PA-QSA, PCI SSC fattura al fornitore del software la tariffa prevista per l'inserimento nell'apposito elenco. Una volta ricevuto il pagamento, PCI SSC invia una Lettera di accettazione PA-DSS e pubblica l'applicazione di pagamento e le informazioni del fornitore sul sito Web.
- Se vengono identificati problemi o domande e sottoposti all'attenzione del PA-QSA, il processo sopra descritto viene riavviato una volta ricevuto un rapporto o una risposta completa e accettabile ("Rapporto revisionato") dal PA-QSA. Il processo viene riavviato solo una volta ricevuto un rapporto revisionato accettabile con possibili soluzioni ai problemi precedentemente identificati. PCI SSC solitamente esamina i rapporti revisionati entro 14 giorni di calendario dalla ricezione.
- In caso di ulteriori problemi o domande, il ciclo si ripete fino a quando non si riceve una risposta soddisfacente, in seguito alla quale PCI SSC invia la Lettera di accettazione PA-DSS e pubblica le informazioni sul sito Web. Ulteriori problemi o domande possono essere evidenziati in qualsiasi momento prima dell'invio di una Lettera di accettazione PA-DSS.

Per i rapporti correlati a modifiche apportate a versioni esistenti di applicazioni presenti nell'elenco, basati sui moduli di autocertificazione della modifica del fornitore, il processo di accettazione del rapporto PA-DSS è lo stesso e PCI SSC invia una Lettera di accettazione PA-DSS revisionata e pubblica le informazioni modificate sul sito Web, se non vengono evidenziati ulteriori problemi o domande come sopra descritto.

La lettera di accettazione e l'elenco sul sito Web di PCI SSC conterranno, almeno, le informazioni di seguito elencate. Tutte le caratteristiche vengono descritte dettagliatamente nell'*Appendice A: Elementi delle applicazioni per l'Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS*.

- Fornitore dell'applicazione di pagamento
- ID dell'applicazione di pagamento
- Numero approvazione
- Note di convalida
- Note di distribuzione
- Autocertificazione per modifica di versione minima, se applicabile
- Data di riconvalida annuale
- Data di scadenza
- Società PA-QSA
- Tipo di applicazione di pagamento
- Mercato di destinazione dell'applicazione di pagamento, se applicabile
- Area o impostazioni specifiche dell'applicazione di pagamento, se applicabile

Nota:

PCI SSC non concede "approvazioni parziali" basate sulla capacità di un'applicazione di pagamento di soddisfare alcuni, ma non tutti i requisiti.

Notifica di una compromissione o violazione della sicurezza

I fornitori devono informare PCI SSC di eventuali violazioni o compromissioni della sicurezza di un'applicazione di pagamento presente nell'elenco, utilizzando le procedure descritte in questa sezione.

Notifica e tempi

Il fornitore, nonostante altri obblighi legali che è tenuto a rispettare, deve immediatamente informare PCI SSC di eventuali violazioni o compromissioni della sicurezza relative a una propria applicazione di pagamento inserita nell'elenco approvato di PCI SSC.

Il fornitore deve anche inviare un feedback immediato sull'impatto (potenziale o effettivo) che la violazione ha avuto, può avere o avrà.

Nota:

La notifica deve essere inviata entro 24 ore dal rilevamento della violazione.

Formato della notifica

Inizialmente, il fornitore deve informare telefonicamente il Coordinatore PA-DSS di PCI SSC della violazione o compromissione della sicurezza; quindi, deve inviare un messaggio e-mail, un fax o una lettera con tutti i dettagli.

Dettagli della notifica

In seguito alla notifica di una violazione o compromissione della sicurezza, il fornitore deve inviare al Coordinatore PA-DSS di PCI SSC tutte le informazioni rilevanti. Tali informazioni sono, senza limitazione:

- Numero dei conti compromessi (se noto)
- Rapporti contenenti dettagli sulla violazione o compromissione della sicurezza
- Rapporti o valutazioni eseguite per rilevare la violazione o compromissione della sicurezza

PCI SSC, come concordato nei termini dell'Accordo di rilascio, può condividere queste e altre informazioni come necessario per supportare o consentire una valutazione della violazione o compromissione della sicurezza al fine di mitigare o prevenire ulteriori violazioni o compromissioni.

Azioni successive a una violazione o compromissione della sicurezza

Nel caso in cui PCI SSC venga a conoscenza di un punto debole o un'effettiva compromissione della sicurezza per un prodotto specifico o un gruppo di prodotti, presente nell'*Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS*, PCI SSC può effettuare le seguenti azioni:

- Informare tutti i marchi di pagamento del punto debole o della compromissione della sicurezza.
- Tentare di ottenere un rapporto forense per valutare esattamente come si è verificata la compromissione.
- Contattare il fornitore per informarlo che il relativo prodotto presenta un problema di sicurezza o è stato compromesso e, dove possibile, condividere le informazioni relative al problema o alla compromissione.
- Supportare gli sforzi del fornitore nel tentativo di mitigare o prevenire ulteriori compromissioni.
- Sostenere gli sforzi del fornitore per 1) correggere eventuali problemi di sicurezza e 2) creare un documento di istruzioni da inviare ai propri clienti per informarli di possibili vulnerabilità indicando le azioni che devono essere intraprese per mitigare o prevenire ulteriori violazioni o compromissioni.
- Collaborare con autorità incaricate dell'applicazione della legge per mitigare o prevenire ulteriori compromissioni.
- Supportare e/o consentire valutazioni del prodotto compromesso internamente o in base ai termini dell'Accordo di rilascio, utilizzando PA-QSA per identificare la causa della compromissione.

Rifiuto di approvazione

PCI SSC si riserva il diritto di rifiutare l'accettazione di un'applicazione di pagamento e rimuovere tale applicazione dall'*Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS*, quando è evidente che l'applicazione non offre protezione adeguata contro le minacce correnti e/o non è conforme ai requisiti PA-DSS. PCI SSC, se considera che l'applicazione di pagamento presenta vulnerabilità o è stata compromessa in termini di sicurezza, informa il fornitore per iscritto della sua intenzione di non approvare l'applicazione.

Termini e condizioni legali

L'approvazione di PCI SSC riguarda solo applicazioni di pagamento/versioni identiche all'applicazione di pagamento revisionata da un PA-QSA. Se una qualsiasi caratteristica dell'applicazione di pagamento è diversa da quella dell'applicazione revisionata dal PA-QSA, anche se conforme alla descrizione di base del prodotto contenuta nella lettera, l'applicazione non deve essere considerata accettata da PCI SSC, né pubblicizzata come applicazione accettata da PCI SSC. Ad esempio, se un'applicazione di pagamento ha lo stesso nome o numero di versione dell'applicazione valutata dal PA-QSA, ma di fatto non è uguale all'applicazione revisionata dal PA-QSA, tale applicazione non deve essere considerata o pubblicizzata come accettata.

Nessun fornitore o terza parte può fare riferimento a un'applicazione di pagamento come "Approvata da PCI" o "Approvata da PCI SSC" né indicare o sottintendere in altro modo che PCI SSC ha, completamente o in parte, approvato tutte le caratteristiche di un fornitore o delle relative applicazioni di pagamento, ad eccezione di quanto indicato nei termini e nelle restrizioni espressamente definite in un accordo scritto con PCI SSC o in una Lettera di accettazione PA-DSS. Tutti gli altri riferimenti all'accettazione di PCI SSC sono rigorosamente e attivamente vietati da PCI SSC.

L'accettazione, quando concessa da PCI SSC, ha lo scopo di assicurare la presenza di determinate caratteristiche di sicurezza e operative importanti per il raggiungimento degli obiettivi di PCI SSC, ma non include in alcuna circostanza alcuna approvazione ufficiale o garanzia di funzionalità, qualità o prestazioni di un determinato prodotto o servizio. PCI SSC non garantisce alcun prodotto o servizio fornito da terze parti. PCI SSC con l'accettazione non fornisce o sottintende alcuna garanzia del prodotto incluse, senza limitazione, garanzie implicite di commerciabilità, idoneità all'uso o non violazione, che sono espressamente negate da PCI SSC. Tutti i diritti e le soluzioni relative a prodotti e servizi, che hanno ricevuto l'accettazione, verranno forniti dalla parte che fornisce tali prodotti o servizi e non da PCI SSC o dai marchi di pagamento.

Se non diversamente concordato per iscritto da PCI SSC, tutte le proprietà e i servizi contemplati in questo documento che PCI SSC fornisce a terze parti vengono forniti "come sono", "con tutti i difetti", senza alcuna garanzia.

Appendice A: Elementi per la Lettera di accettazione e per l'*Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS*

Fornitore dell'applicazione di pagamento

Questa voce contiene il nome del **Fornitore dell'applicazione di pagamento** per l'applicazione convalidata.

ID dell'applicazione di pagamento

L'**ID dell'applicazione di pagamento** è utilizzato da PCI SSC per fornire informazioni rilevanti che rappresentano un'applicazione di pagamento convalidata ed è costituito da:

- Nome applicazione di pagamento
- Versione applicazione di pagamento

Per accertarsi che venga utilizzata un'applicazione di pagamento convalidata, viene consigliato a clienti o relativi agenti di acquistare e distribuire solo applicazioni di pagamento con informazioni che corrispondono esattamente alle informazioni fornite nell'ID dell'applicazione di pagamento. Esempio di un **ID dell'applicazione di pagamento** (due componenti):

Componente	Descrizione
Nome applicazione	Acme Payment 600
Versione applicazione di pagamento	PCI 4.53

Versione applicazione di pagamento

La **Versione dell'applicazione di pagamento** rappresenta la versione specifica dell'applicazione sottoposta alla valutazione PA-DSS. I campi che costituiscono la Versione dell'applicazione di pagamento possono essere una combinazione di caratteri alfanumerici fissi e variabili.

Nota:

In PA-DSS, vedere la sezione Istruzioni e contenuto del rapporto di convalida per dettagli sul contenuto da includere nel rapporto di convalida PA-DSS per i metodi di versioning del fornitore.

È fortemente consigliato ai clienti di acquistare e distribuire solo le applicazioni di pagamento con versione esattamente corrispondente (caratteri alfanumerici) alla Versione dell'applicazione di pagamento inclusa nell'Elenco delle applicazioni di pagamento convalidate in base al programma PA-DSS o nella Lettera di accettazione PA-DSS di PCI SSC.

Numero approvazione

PCI SSC assegna il **Numero approvazione** al momento dell'accettazione; questo numero rimane invariato fin quando l'applicazione rimane nell'elenco.

Note di convalida

Le **Note di convalida** vengono utilizzate da PCI SSC per indicare se la revisione è stata eseguita in base al programma PABP di Visa o al programma PA-DSS di PCI SSC e per annotare la versione di standard PABP o PA-DSS applicabile. Per alcuni esempi, vedere la tabella sotto le Note di distribuzione.

Note di distribuzione

Le **Note di distribuzione** vengono utilizzate da PCI SSC per indicare se un'applicazione di pagamento può essere distribuita, in base alla data di scadenza, di seguito riportata. Per ulteriori dettagli, fare riferimento alla tabella completa a pagina 22.

Elenco PCI SSC prima della scadenza		Elenco PCI SSC dopo la scadenza	
Note di convalida	Note di distribuzione	Note di convalida	Note di distribuzione
Convalidata in base a programma PABP	Accettabile per nuove distribuzioni	Convalidata in base a programma PABP	Non accettabile per nuove distribuzioni
Applicazione pre-PCI	Non consigliata per nuove distribuzioni	Applicazione pre-PCI	Non accettabile per nuove distribuzioni
Convalidata in base a programma PA-DSS	Accettabile per nuove distribuzioni	Convalidata in base a programma PA-DSS	Non accettabile per nuove distribuzioni

Autocertificazione per modifica di versione minima, se applicabile

L'**Autocertificazione per modifica di versione minima** viene utilizzata, dove applicabile, per indicare le versioni delle applicazioni che vengono sottoposte al processo per modifiche minime descritto nella sezione *Nessun impatto sui requisiti PA-DSS* di questo documento.

Data di riconvalida annuale

La **Data di riconvalida annuale** viene utilizzata da PCI SSC per indicare quando il fornitore del software deve presentare l'Attestato di convalida. La riconvalida annuale fa parte dell'Attestato di convalida, che si trova nell'Appendice C PA-DSS, parte 3b.

Data di scadenza

La **Data di scadenza** per applicazioni di pagamento convalidate in base al programma PA-DSS è la data entro la quale un fornitore deve ricevere l'applicazione rivalutata in base ai requisiti PA-DSS correnti per mantenere l'accettazione. La data di scadenza è correlata alle Note di distribuzione, sopra descritte.

PCI SSC si impegna ad aggiornare i requisiti PA-DSS ogni 24 mesi, insieme agli aggiornamenti dei requisiti PCI DSS. L'accettazione per applicazioni di pagamento convalidate in base al programma PA-DSS scade tre anni dopo la data effettiva di un successivo aggiornamento dei requisiti PA-DSS. L'obiettivo è una durata minima di tre anni per l'approvazione, salvo gravi minacce che possono richiedere modifiche immediate.

Nota:

Qualsiasi valutazione PA-DSS effettuata in base alla versione 1.1 avrà la stessa data di scadenza delle revisioni effettuate in base alla versione 1.2 degli standard PA-DSS, in conformità al normale processo di scadenza.

Ad esempio: Gli standard PA-DSS versione 1.1 e versione 1.2 avranno la stessa data di scadenza. Con la versione successiva degli standard PA-DSS (successiva alla versione 1.2) prevista per ottobre 2010, le revisioni in base agli standard PA-DSS versioni 1.1 e 1.2 scadranno a ottobre 2013.

Attualmente non esiste una data di fine per le applicazioni di pagamento convalidate in base al programma PA-DSS presenti nell'elenco approvato al momento della distribuzione. Le applicazioni distribuite con approvazioni scadute possono essere comunque utilizzate. La scadenza è associata a nuovi acquisti/distribuzioni, non ad applicazioni già distribuite.

Società PA-QSA

Questa voce contiene il nome della **Società PA-QSA (Payment Application Qualified Security Assessor)** che ha eseguito la convalida dell'applicazione di pagamento in quanto conforme agli standard PA-DSS.

Tipo di applicazione di pagamento

Il **Tipo di applicazione di pagamento** può essere uno dei seguenti:

- Punto vendita (POS)
- Middleware
- Distributore di carburante automatico
- Carrello
- Contabilizzazione
- Carta non presente
- Gateway
- Altro

Mercato di destinazione

Il **Mercato di destinazione** indica un mercato per l'applicazione di pagamento, se applicabile. Ad esempio:

- Rivenditore al dettaglio
- Chioschi di parcheggi
- Distributori di gas/benzina
- e-Commerce

Nota:

Indica se l'applicazione di pagamento è progettata per un determinato mercato e non per scopi di marketing del fornitore di software.

Area o impostazioni specifiche dell'applicazione di pagamento, se applicabile

L'area o le impostazioni specifiche per l'applicazione di pagamento indicano le applicazioni di pagamento sviluppate per specifiche aree e impostazioni e che possono essere utilizzate solo in tali aree o con tali impostazioni.

Appendice B: Identificazione di build di applicazioni di pagamento certificate

Nota: *Per considerazioni future.*

Sebbene build di applicazioni di pagamento certificate non siano un requisito in questo momento, si consiglia ai fornitori di software e ai PA-QSA di sviluppare insieme metodi per certificare e firmare in modo digitale build di applicazioni di pagamento. PCI SSC si riserva il diritto di richiedere build di applicazioni certificate in futuro.

Di seguito un metodo di esempio:

I fornitori identificano chiaramente una build certificata per il rilascio. Idealmente, una build certificata da un PA-QSA come conforme agli standard PA-DSS deve essere firmata in modo digitale dal fornitore del software e dal QSA quando inviata per la consegna. La consegna deve essere identificata in modo univoco almeno da nome, versione, numero di build, data e ora e deve essere verificabile con un digest MD5 e una corrispondente intestazione di build. Questa condizione supporta ulteriormente i requisiti PA-DSS 7.2 per la consegna mediante "canali affidabili". Inoltre, aiuta a supportare un marchio di pagamento relativamente ai programmi PA-DSS e ad aumentare la consapevolezza e la fiducia dei clienti.

Appendice C: Autocertificazione per modifica di versione minima

Istruzioni per l'invio

Il Fornitore dell'applicazione di pagamento e il PA-QSA devono completare questo documento come dichiarazione dello stato di modifica dell'applicazione di pagamento rispetto agli standard PA-DSS. Il Fornitore dell'applicazione di pagamento deve completare tutte le sezioni applicabili e inviare l'analisi della modifica e l'autocertificazione al PA-QSA.

Dopo aver esaminato la documentazione fornita, il PA-QSA deve completare le sezioni applicabili e inviare questo documento insieme alle copie di tutta la documentazione richiesta a PCI SSC utilizzando le istruzioni per la cifratura e l'invio dei rapporti di PCI SSC.

Parte 1. Informazioni sul fornitore dell'applicazione di pagamento

Nome società:			
Nome contatto:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP: <input type="text"/>
URL:			

Parte 1a. Informazioni sull'applicazione di pagamento

Nome e numero di versione dell'applicazione di pagamento "originaria" attualmente presente nell'elenco PCI SSC:

Nome applicazione esistente: Numero versione esistente:

Numero approvazione PCI SSC:

Nuovo nome applicazione di pagamento e numero di versione, se applicabile:

Nuovo nome applicazione: Nuovo numero di versione:

Descrizione della modifica, se applicabile:

Funzionalità dell'applicazione di pagamento (selezionare tutte le risposte appropriate):

- | | | |
|--|--|---|
| <input type="checkbox"/> Punto vendita (POS) | <input type="checkbox"/> Carrello | <input type="checkbox"/> Carta non presente |
| <input type="checkbox"/> Middleware | <input type="checkbox"/> Contabilizzazione | <input type="checkbox"/> Gateway |
| <input type="checkbox"/> Distributore di carburante automatico | <input type="checkbox"/> Altro (specificare): <input type="text"/> | |

Mercato di destinazione per applicazione:

Parte 2. Informazioni su società PA-QSA

Nome società:				
Nome contatto PA-QSA principale:		Mansione:		
Telefono:		E-mail:		
Indirizzo ufficio:		Città:		
Stato/Provincia:		Paese:		CAP:
URL:				

Parte 3. Conferma dello stato di modifica

Parte 3a. Attestato del fornitore dell'applicazione di pagamento

In base all'analisi della modifica interna e all'apposita documentazione, (*PA Vendor Name*) valuta lo stato dell'applicazione (applicazioni) e la versione (versioni) identificate nella Parte 1a di questo documento a partire da (*date*) (selezionare campi applicabili):

<input type="checkbox"/>	Sono state apportate <i>solo modifiche minime</i> all'applicazione di pagamento "originaria" sopra indicata per creare la Nuova applicazione, senza alcun impatto sui requisiti PA-DSS
<input type="checkbox"/>	Tutte le modifiche sono state accuratamente registrate nel documento di analisi delle modifiche del fornitore inviato al PA-QSA come indicato nella Parte 2
<input type="checkbox"/>	Tutte le informazioni contenute nell'autocertificazione rappresentano i risultati dell'analisi delle modifiche negli aspetti fondamentali
<input type="checkbox"/>	Nessuna prova di memorizzazione dei dati della striscia magnetica (traccia) ⁴ , CAV2, CVC2, CID, o CVV2 ⁵ o di dati PIN ⁶ successiva all'autorizzazione della transazione è stata trovata su ALCUN file o funzionalità generata dall'applicazione

Parte 3b. Attestato del PA-QSA

In base alla documentazione dell'analisi delle modifiche interna del Fornitore dell'applicazione di pagamento indicato nella Parte 1, (*PA-QSA Name*) dichiara il seguente stato dell'applicazione (applicazioni) e versione (versioni) identificate nella Parte 1a di questo documento a partire da (*date*) (selezionare campi applicabili):

<input type="checkbox"/>	In base alla nostra revisione della documentazione di analisi delle modifiche, concordiamo che la documentazione supporta quanto dichiarato dal fornitore, ossia che sono state apportate <i>solo modifiche minime</i> all'applicazione sopra indicata, senza alcun impatto sui requisiti PA-DSS.
--------------------------	--

⁴ Dati della striscia magnetica (traccia): 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. I soli elementi dei dati di traccia che possono essere conservati sono il numero cliente, la data di scadenza e il nome.

⁵ 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.

⁶ Dati PIN: 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 3c. Accettazione PA-QSA e fornitore dell'applicazione

<i>Firma PA-QSA principale</i> ↑	<i>Data</i> ↑
<i>Nome PA-QSA principale</i> ↑	<i>Mansione</i> ↑
<i>Firma del funzionario esecutivo fornitore applicazione</i> ↑	<i>Data</i> ↑
<i>Nome funzionario esecutivo fornitore applicazione</i> ↑	<i>Mansione</i> ↑
<i>Società rappresentata da fornitore applicazione</i> ↑	