



# **Settore delle carte di pagamento (PCI) Standard di protezione dei dati e Standard di protezione dei dati per le applicazioni di pagamento (PA- DSS)**

---

## **Glossario, abbreviazioni e acronimi**

**Versione 3.0**

Gennaio 2014

Termine	Definizione
<b>AAA</b>	Acronimo di “Authentication, Authorization, Accounting.” Protocollo per l'autenticazione di un utente in base alla sua identità verificabile, per l'autorizzazione di un utente in base ai suoi diritti utente e per la registrazione del consumo di risorse di rete da parte dell'utente.
<b>Accesso amministrativo non da console</b>	Si riferisce all'accesso amministrativo logico a un componente di sistema che si verifica su un'interfaccia di rete anziché tramite una connessione fisica diretta al componente del sistema. L'accesso amministrativo senza console include l'accesso da reti locali/interne e da reti esterne o remote.
<b>Accesso remoto</b>	Accesso alle reti di computer da una postazione remota. Le connessioni di accesso remoto possono provenire sia dall'interno della rete aziendale sia da una postazione remota situata al di fuori della rete aziendale. Un esempio di tecnologia per l'accesso remoto è VPN.
<b>Account predefiniti</b>	Account di accesso predefinito in un sistema, applicazione o dispositivo che permette l'accesso iniziale alla messa in esercizio del sistema. Ulteriori account predefiniti possono essere anche generati dal sistema come parte del processo di installazione.
<b>Acquirente</b>	Definito anche “banca dell'esercente”, “banca acquirente” o “istituzione finanziaria acquirente”. L'entità che inizia e mantiene le relazioni con gli esercenti per l'accettazione delle carte di pagamento.
<b>Addetto alla sicurezza</b>	Responsabile principale delle questioni riguardanti la sicurezza di un'entità.
<b>Adware</b>	Tipo di software dannoso che, una volta installato, impone a un computer di visualizzare o scaricare automaticamente annunci pubblicitari.
<b>AES</b>	Abbreviazione di Advanced Encryption Standard. Cifratura a blocchi utilizzata nella crittografia a chiave simmetrica adottata da NIST nel novembre 2001 come U.S. FIPS PUB 197 (o FIPS 197). Vedere <i>Crittografia avanzata</i> .
<b>Algoritmo di cifratura</b>	Detto anche “algoritmo di crittografia”. Una sequenza di istruzioni matematiche utilizzate per trasformare testo o dati non cifrati in testo o dati cifrati, e viceversa. Vedere <i>Crittografia avanzata</i> .
<b>Ambiente di laboratorio remoto</b>	Un laboratorio che non è mantenuto dal PA-QSA.
<b>Amministratore di database</b>	Definito anche “DBA”. Individuo responsabile della gestione e dell'amministrazione dei database.
<b>Amministratore di rete</b>	Personale responsabile della gestione della rete all'interno di un'entità. Le responsabilità generalmente includono, senza limitazioni, sicurezza di rete, installazioni, aggiornamenti, manutenzione e monitoraggio dell'attività.
<b>Analisi/valutazione del rischio</b>	Processo che identifica le risorse di sistema preziose e le minacce, quantifica l'esposizione alle perdite (vale a dire la perdita potenziale) sulla base delle frequenze stimate e del costo di occorrenza, e facoltativamente consiglia come allocare le risorse come contromisura per ridurre al minimo l'esposizione totale.

Termine	Definizione
<b>ANSI</b>	Acronimo di American National Standards Institute. Organizzazioni private, senza scopo di lucro, che amministrano e coordinano il sistema di valutazione della conformità e della standardizzazione volontarie degli Stati Uniti.
<b>Antivirus</b>	Programma o software in grado di rilevare, rimuovere e proteggere da diverse forme di software dannoso (dette anche “malware”), tra cui virus, worm, cavalli di Troia, spyware, adware e rootkit.
<b>AOC</b>	Acronimo di Attestation of Compliance (attestato di conformità). L'AOC è un metodo attraverso il quale gli esercenti e i provider di servizi attestano i risultati di una valutazione PCI DSS, come documentato nel questionario di autovalutazione o nel rapporto sulla conformità.
<b>AOV</b>	Acronimo di Attestation of Validation (attestato di convalida). L'AOV è un modulo mediante il quale i PA-QSA (Payment Application Qualified Security Assessor, ossia valutatori qualificati delle applicazioni di pagamento) attestano i risultati di una valutazione PA-DSS, come documentato nel ROV (rapporto sulla validazione) di PA-DSS.
<b>Applicazione</b>	Comprende tutti i programmi software, o gruppi di programmi, acquistati e personalizzati, di tipo sia interno che esterno (per esempio sul Web).
<b>Applicazione di pagamento</b>	Nel contesto del programma PA-DSS, un'applicazione software 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. Fare riferimento alla <i>Guida del programma PA-DSS</i> per maggiori dettagli.
<b>Applicazione Web</b>	Un'applicazione a cui si accede di solito mediante un browser Web o attraverso servizi Web. Le applicazioni Web possono essere disponibili via Internet o attraverso una rete interna privata.
<b>Area sensibile</b>	Qualunque centro dati, sala server o area che ospita sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.
<b>ASV</b>	Acronimo di Approved Scanning Vendor (fornitore di scansioni approvato). Società approvata da PCI SSC che conduce servizi di scansione delle vulnerabilità esterni.
<b>Attacchi memory-scraping</b>	Attività malware che esamina ed estrae dati che risiedono in memoria mentre vengono elaborati o che non sono stati adeguatamente cancellati o sovrascritti.
<b>Attacco Rainbow Table</b>	Metodo di attacco dati effettuato utilizzando una tabella pre-calcolata di stringhe hash (digest di messaggio di lunghezza fissa) per identificare l'origine dati originale, di solito per il cracking degli hash delle password o dei dati di titolari di carta.
<b>Audit trail</b>	Vedere <i>Log di audit</i> .

Termine	Definizione
<b>Autenticazione</b>	<p>Processo di verifica dell'identità di un individuo, dispositivo o processo. L'autenticazione di norma avviene utilizzando uno o più fattori di autenticazione come:</p> <ul style="list-style-type: none"> <li>▪ qualcosa che l'utente conosce, come una password o una passphrase;</li> <li>▪ qualcosa in possesso dell'utente, come un dispositivo token o una smart card;</li> <li>▪ qualcosa che l'utente è, come un elemento biometrico.</li> </ul>
<b>Autenticazione a due fattori</b>	<p>Metodo di autenticazione di un utente in cui vengono verificati due o più fattori. Tali fattori comprendono qualcosa in possesso dell'utente (ad esempio un token hardware o software), qualcosa che l'utente conosce (una password, passphrase o PIN) o qualcosa che l'utente usa o svolge (ad esempio le impronte digitali o altre forme di biometrica).</p>
<b>Autorizzazione</b>	<p>Nel contesto del controllo dell'accesso, l'autorizzazione è la concessione dell'accesso o di altri diritti a un utente, programma o processo. L'autorizzazione definisce quello che un individuo o un programma può fare dopo una corretta autenticazione.</p> <p>Nel contesto di una transazione con carta di pagamento, l'autorizzazione avviene quando un esercente riceve l'approvazione per la transazione dopo che l'acquirente convalida la transazione con l'emittente/elaboratore.</p>
<b>Backup</b>	<p>Copia duplicata dei dati creata a fini di archiviazione o per la protezione contro danni o perdite.</p>
<b>BAU</b>	<p>Acronimo di "business as usual". BAU si riferisce alla normale attività quotidiana di un'organizzazione.</p>
<b>Blocco PIN</b>	<p>Un blocco di dati usati per contenere un PIN durante l'elaborazione. Il formato del blocco PIN definisce i suoi contenuti e le modalità di elaborazione per il recupero del PIN. Il blocco PIN è composto da PIN, lunghezza del PIN e può contenere un sottoinsieme del PAN.</p>
<b>Bluetooth</b>	<p>Protocollo wireless che utilizza una tecnologia di comunicazione a corto raggio per facilitare la trasmissione dei dati a breve distanza.</p>
<b>Buffer overflow</b>	<p>Vulnerabilità causata da metodi di codifica insicuri, nella quale un programma supera il limite del buffer e scrive dati nello spazio di memoria adiacente. I buffer overflow sono utilizzati dagli aggressori per ottenere l'accesso non autorizzato ai sistemi o ai dati.</p>
<b>Campionamento</b>	<p>Il processo che prevede la selezione di un campione di un insieme rappresentativo dell'intero gruppo. Il campionamento può essere usato dai valutatori per ridurre le attività di test complessive, una volta che per un'entità sia stata confermata la presenza di processi e controlli operativi e di sicurezza PCI DSS centralizzati, standard. Il campionamento non costituisce un requisito PCI DSS.</p>
<b>Cancellazione sicura</b>	<p>Detta anche "eliminazione sicura", è un metodo per sovrascrivere i dati che risiedono su un disco rigido o su altri supporti digitali, rendendo i dati irrecuperabili.</p>

Termine	Definizione
<b>Carattere jolly</b>	Carattere che può essere sostituito da un sottoinsieme di caratteri possibili nello schema di versioni di un'applicazione. Nel contesto di PA-DSS, i caratteri jolly possono opzionalmente essere utilizzati per rappresentare un cambiamento senza impatto sulla sicurezza. Un carattere jolly è l'unico elemento variabile della versione del fornitore e viene utilizzato per indicare solo le modifiche minori senza effetti sulla sicurezza tra ogni versione rappresentata dal carattere jolly.
<b>Card skimmer</b>	Un dispositivo fisico, spesso collegato a un dispositivo di lettura schede legittimo, progettato per catturare e/o conservare illegalmente le informazioni di una carta di pagamento.
<b>Carte di pagamento</b>	Per gli scopi di PCI DSS, qualsiasi carta di pagamento o dispositivo che porta il logo dei membri fondatori di PCI SSC, vale a dire American Express, Discover Financial Services, JCB International, MasterCard Worldwide o Visa, Inc.
<b>Cavallo di Troia</b>	Definito anche "Trojan". Un tipo di software dannoso che, una volta installato, consente a un utente di eseguire una funzione normale mentre il cavallo di Troia esegue funzioni dannosi per il sistema senza che l'utente ne sia a conoscenza.
<b>CDE</b>	Acronimo di "cardholder data environment" (ambiente dei dati di titolari di carta). Le persone, i processi e la tecnologia che memorizzano, elaborano o trasmettono dati dei titolari di carta o dati sensibili di identificazione.
<b>CERT</b>	Acronimo del "Computer Emergency Response Team" della Carnegie Mellon University. Il Programma CERT sviluppa e promuove l'uso di pratiche adeguate per la gestione di sistemi e tecnologie per resistere agli attacchi su sistemi di rete, limitare i danni e assicurare la continuità dei servizi critici.
<b>Chiave di crittografia</b>	Un valore che determina l'output di un algoritmo di cifratura durante la trasformazione di testo normale in testo cifrato. La lunghezza della chiave determina in genere la difficoltà di decifratura del testo cifrato in un determinato messaggio. Vedere <i>Crittografia avanzata</i> .
<b>Cifratura</b>	Processo di conversione delle informazioni in una forma non intellegibile se non per i proprietari di una specifica chiave di crittografia. L'uso della cifratura protegge le informazioni tra il processo di cifratura e quello di decifratura (l'inverso della cifratura) dalla divulgazione non autorizzata. Vedere <i>Crittografia avanzata</i> .
<b>Cifratura a livello di file</b>	Tecnica o tecnologia (software o hardware) per la cifratura dell'intero contenuto di file specifici. In alternativa, vedere <i>Cifratura del disco</i> o <i>Cifratura del database a livello di colonna</i> .
<b>Cifratura del database a livello di colonna</b>	Tecnica o tecnologia (software o hardware) per la cifratura del contenuto di una colonna specifica in un database piuttosto che del contenuto completo dell'intero database. In alternativa, vedere <i>Cifratura del disco</i> o <i>Cifratura a livello di file</i> .

Termine	Definizione
<b>Cifratura del disco</b>	Tecnica o tecnologia (software o hardware) per cifrare tutti i dati memorizzati su un dispositivo (ad esempio, disco rigido, unità flash). In alternativa, per crittografare il contenuto di file o colonne specifici, viene utilizzata la <i>Cifratura a livello di file</i> o la <i>Cifratura del database a livello di colonna</i> .
<b>CIS</b>	Acronimo di Center for Internet Security. Organizzazione senza scopo di lucro con la missione di aiutare le organizzazioni a ridurre il rischio di interruzioni del business e dell'e-commerce derivanti da controlli di sicurezza tecnica inadeguati.
<b>Classificazione dei rischi</b>	Un determinato criterio di misurazione basato sulla valutazione del rischio e sull'analisi del rischio effettuata su una determinata entità.
<b>Codice di servizio</b>	Valore di tre o quattro cifre nella striscia magnetica che segue la data di scadenza della carta di pagamento nei dati di traccia. È utilizzato per diversi scopi, quali la definizione degli attributi di servizio, la distinzione tra scambio internazionale e nazionale, o l'identificazione delle limitazioni all'uso.

Termine	Definizione
<b>Codice o valore di verifica della carta</b>	<p>Anche noto come Codice o valore di validazione della carta oppure Codice di sicurezza della carta.</p> <p>Fa riferimento a: (1) dati della striscia magnetica; (2) caratteristiche di protezione stampate.</p> <p>(1) Gli elementi dei dati sulla striscia magnetica di una carta che utilizzano processi crittografici sicuri per proteggere l'integrità dei dati sulla striscia e rivelare alterazioni e contraffazioni. Definito CAV, CVC, CVV o CSC in base al marchio della carta di pagamento. Nell'elenco seguente sono forniti i termini per ogni marchio di carta:</p> <ul style="list-style-type: none"> <li>▪ <b>CAV</b> - Card Authentication Value, valore di autenticazione della carta (carte di pagamento JCB)</li> <li>▪ <b>CVC</b> - Card Validation Code, codice di validazione della carta (carte di pagamento MasterCard)</li> <li>▪ <b>CVV</b> - Card Verification Value, valore di verifica della carta (carte di pagamento Visa e Discover)</li> <li>▪ <b>CSC</b> - Card Security Code, codice di sicurezza della carta (American Express)</li> </ul> <p>(2) Per le carte di pagamento Discover, JCB, MasterCard e Visa, il secondo tipo di valore o codice di verifica della carta corrisponde al valore di tre cifre più a destra stampato nell'area della firma sul retro della carta. Per le carte di pagamento American Express, il codice è il numero di quattro cifre stampato in rilievo sopra il numero PAN nella parte anteriore delle carte di pagamento. Il codice è associato in modo univoco ad ogni singolo elemento del materiale plastico e associa il PAN al materiale plastico. Nell'elenco seguente sono forniti i termini per ogni marchio di carta:</p> <ul style="list-style-type: none"> <li>▪ <b>CID</b> - Card Identification Number, numero di identificazione della carta (carte di pagamento American Express e Discover)</li> <li>▪ <b>CAV2</b> - Card Authentication Value 2, valore di autenticazione della carta 2 (carte di pagamento JCB)</li> <li>▪ <b>CVC2</b> - Card Validation Code 2, codice di validazione della carta 2 (carte di pagamento MasterCard)</li> <li>▪ <b>CVV2</b> - Card Verification Value 2, valore di verifica della carta 2 (carte di pagamento Visa)</li> </ul>
<b>Codifica sicura</b>	Il processo per la creazione e l'implementazione di applicazioni a prova di manomissione e/o compromissione.
<b>Componenti di rete</b>	Includono, senza limitazioni, firewall, switch, router, punti di accesso wireless, dispositivi di rete e altri dispositivi di sicurezza.
<b>Componenti di sistema</b>	Dispositivi di rete, server, dispositivi di calcolo o applicazioni inclusi o connessi all'ambiente dei dati dei titolari di carta.
<b>Compromissione</b>	Definita anche "compromissione dei dati" o "violazione dei dati". Intrusione in un sistema informatico in cui si sospettano furto/divulgazione, modifica o distruzione non autorizzati dei dati dei titolari di carta.

Termine	Definizione
<b>Console</b>	Schermo e tastiera che permettono l'accesso e il controllo del server, del computer mainframe o di un altro tipo di sistema in un ambiente di rete.
<b>Consumatore</b>	Individuo che acquista beni e/o servizi.
<b>Controlli compensativi</b>	<p>È possibile adottare i controlli compensativi quando un'entità non è in grado di soddisfare un requisito nel modo esplicitamente richiesto, a causa di limitazioni aziendali tecniche o documentate legittime, ma ha posto in essere altri controlli sufficienti a mitigare il rischio associato a tale requisito. I controlli compensativi devono:</p> <ol style="list-style-type: none"> <li>(1) Rispondere allo scopo e alla severità del requisito PCI DSS originale.</li> <li>(2) Fornire un livello di difesa simile a quello del requisito PCI DSS originale.</li> <li>(3) Superare e integrare altri requisiti PCI DSS (non possono essere semplicemente conformi ad altri requisiti PCI DSS).</li> <li>(4) Essere adeguato al rischio ulteriore provocato dalla mancata adesione al requisito PCI DSS.</li> </ol> <p>Vedere "Controlli compensativi" Appendici B e C in <i>Requisiti PCI DSS e Procedure di valutazione della sicurezza</i> per istruzioni sull'utilizzo dei controlli compensativi.</p>
<b>Controllo dell'accesso</b>	Meccanismi che limitano la disponibilità di informazioni o risorse di elaborazione delle informazioni solo alle persone o alle applicazioni autorizzate.
<b>Controllo delle modifiche</b>	Processi e procedure per esaminare, testare e approvare modifiche ai sistemi e al software allo scopo di verificarne l'impatto prima dell'implementazione.
<b>Controllo duale</b>	Processo di utilizzo di due o più entità separate (solitamente persone) che operano insieme per proteggere funzioni o informazioni sensibili. Entrambe le entità sono egualmente responsabili della protezione fisica dei materiali coinvolti nelle transazioni vulnerabili. Nessuna persona singola può accedere o utilizzare i materiali (ad esempio la chiave di crittografia). Per la generazione manuale delle chiavi, il trasporto, il caricamento, la memorizzazione e il recupero, il controllo duale richiede di dividere la conoscenza della chiave tra le entità. Vedere anche <i>Split knowledge</i> .
<b>Credenziali di autenticazione</b>	Combinazione di ID utente o ID account più i fattori di autenticazione utilizzati per autenticare un individuo, dispositivo o processo.
<b>Criterio di protezione</b>	Insieme di leggi, regole e pratiche che stabiliscono il modo in cui un'organizzazione gestisce, protegge e distribuisce informazioni sensibili.
<b>Criterio o politica</b>	Regole a livello dell'organizzazione che stabiliscono l'uso accettabile delle risorse informatiche, le pratiche di sicurezza e lo sviluppo delle procedure operative.



Termine	Definizione
<b>Crittografia</b>	Disciplina della matematica e dell'informatica relativa alla sicurezza delle informazioni, in particolare alla cifratura e all'autenticazione. Nella sicurezza di reti e applicazioni, è uno strumento per il controllo dell'accesso, la riservatezza delle informazioni e l'integrità.
<b>Crittografia avanzata</b>	Crittografia basata su algoritmi testati e accettati, insieme ad adeguate pratiche di gestione delle chiavi e lunghezze delle chiavi (con un'attendibilità minima di 112 bit). La crittografia è un metodo per proteggere i dati e include sia la cifratura (reversibile) sia l'hashing (irreversibile, o "one way"). Al momento della pubblicazione del presente documento, esempi di algoritmi e standard testati e accettati per il livello di crittografia minimo sono AES (128 bit e superiore), TDES (DES triplo), RSA (2048 bit e superiore), ECC (160 bit e superiore) ed ElGamal (2048 bit e superiore). Vedere NIST Special Publication 800-57 Part 1 ( <a href="http://csrc.nist.gov/publications/">http://csrc.nist.gov/publications/</a> ) per maggiori indicazioni sulla forza e sugli algoritmi delle chiavi crittografiche.
<b>Cross-site request forgery (CSRF)</b>	Vulnerabilità causata da metodi di codifica non sicuri, che permette l'esecuzione di azioni indesiderate attraverso una sessione autenticata. Spesso utilizzata in combinazione con XSS e/o SQL injection.
<b>CVSS</b>	Acronimo di Common Vulnerability Scoring System. Standard di settore aperto e non legato a fornitori specifici progettato per descrivere la gravità delle vulnerabilità di sicurezza di un sistema informatico e contribuire a determinare l'urgenza e la priorità di risposta. Fare riferimento alla <i>Guida del programma ASV</i> per ulteriori informazioni.
<b>Database</b>	Formato strutturato per organizzare e mantenere informazioni facili da recuperare. Semplici esempi di database sono tabelle e fogli di calcolo.
<b>Dati dei titolari di carta</b>	I dati dei titolari di carta sono composti, come minimo, dall'intero PAN. I dati dei titolari di carta possono anche comparire nella forma del PAN completo più uno qualsiasi dei seguenti elementi: nome del titolare di carta, data di scadenza e/o codice di servizio. Vedere <i>Dati sensibili di autenticazione</i> per ulteriori elementi di dati che possono essere trasmessi o elaborati (ma non memorizzati) come parte di una transazione di pagamento.
<b>Dati della striscia magnetica</b>	Vedere <i>Dati di traccia</i> .
<b>Dati delle transazioni</b>	Dati relativi alle transazioni con carta di pagamento elettronica.
<b>Dati di account</b>	I dati degli account sono costituiti da dati dei titolari di carta e/o dati sensibili di autenticazione. Vedere <i>Dati dei titolari di carta</i> e <i>Dati sensibili di autenticazione</i> .
<b>Dati di traccia</b>	Definito anche "dati della traccia completa" o "dati della striscia magnetica". Dati codificati nella striscia magnetica o nel chip utilizzati per l'autenticazione e/o l'autorizzazione durante le transazioni di pagamento. Possono corrispondere all'immagine della striscia magnetica su un chip o ai dati sulla traccia 1 e/o sulla traccia 2 della striscia magnetica.

Termine	Definizione
<b>Dati sensibili di autenticazione</b>	Informazioni relative alla sicurezza (comprendenti, senza limitazione, codici/valori di validazione della carta, dati della traccia completa della striscia magnetica o del chip, PIN e blocchi PIN) utilizzate per autenticare i titolari di carte e/o autorizzare le transazioni delle carte di pagamento.
<b>Determinazione dell'ambito</b>	Il processo in base al quale vengono identificati tutti i componenti di sistema, le persone ed i processi da inserire in una valutazione PCI DSS. Il primo passo di una valutazione PCI DSS consiste nello stabilire con precisione l'ambito della revisione.
<b>Diagramma del flusso di dati</b>	Diagramma che mostra il flusso di dati attraverso un'applicazione, un sistema o una rete.
<b>Diagramma di rete</b>	Diagramma che mostra i componenti di sistema e le connessioni all'interno di un ambiente di rete.
<b>Dipendenza</b>	Nel contesto di PA-DSS, una dipendenza è un componente specifico software o hardware (ad esempio un terminale hardware, un database, un sistema operativo, delle API, una libreria di codice ecc.) necessario all'applicazione di pagamento per soddisfare i requisiti PA-DSS.
<b>Dispositivo crittografico protetto</b>	Un insieme di hardware, software e firmware che implementa processi crittografici (compresi algoritmi crittografici e generazione di chiavi) ed è contenuto all'interno di un limite di crittografia definito. Esempi di dispositivi crittografici protetti includono moduli di sicurezza host/hardware (HSM) e dispositivi di punto di interazione (POI) convalidati in base allo standard PCI PTS.
<b>Dispositivo virtuale (VA)</b>	Un VA prende il concetto di un dispositivo preconfigurato per compiere una serie specifica di funzioni ed eseguire questo dispositivo come un carico di lavoro. Spesso, un dispositivo di rete esistente viene virtualizzato per funzionare come dispositivo virtuale come router, switch o firewall
<b>DMZ</b>	Abbreviazione di "demilitarized zone", zona demilitarizzata. Una sottorete fisica o logica che fornisce un livello di protezione aggiuntivo alla rete privata interna di un'organizzazione. La DMZ aggiunge un altro livello di protezione della rete tra Internet e la rete interna di un'organizzazione, in modo che le parti esterne abbiano connessioni dirette solamente ai dispositivi nella zona DMZ anziché all'intera rete interna.
<b>DNS</b>	Acronimo di Domain Name System o Domain Name Server. Sistema che memorizza le informazioni associate ai nomi di dominio in un database distribuito per fornire servizi di risoluzione dei nomi sulle reti, ad esempio Internet.
<b>DSS</b>	Acronimo di Data Security Standard (standard di protezione dei dati). Vedere <i>PA-DSS</i> e <i>PCI DSS</i> .
<b>Dynamic Packet Filtering</b>	Vedere <i>Ispezione stateful</i> .
<b>ECC</b>	Acronimo di Elliptic Curve Cryptography. Metodo per la crittografia a chiave pubblica basato su curve ellittiche su campi finiti. Vedere <i>Crittografia avanzata</i> .

Termine	Definizione
<b>Emittente</b>	Entità che emette carte di pagamento oppure che esegue, facilita o supporta servizi di emissione inclusi, senza limitazioni, banche emittenti e processori emittenti. Definito anche “banca emittente” o “istituzione finanziaria emittente”.
<b>Entità</b>	Termine utilizzato per indicare la società, l’organizzazione o l’azienda che si sottopone alla revisione PCI DSS.
<b>Esercente</b>	Ai fini del PCI DSS, un esercente è qualsiasi entità che accetta carte di pagamento con il logo di uno dei cinque membri di PCI SSC (American Express, Discover, JCB, MasterCard o Visa) come pagamento per beni e/o servizi. Si noti che un esercente che accetta carte di pagamento per il pagamento di beni e/o servizi può anche essere un provider di servizi, se i servizi venduti comportano la memorizzazione, l’elaborazione o la trasmissione dei dati dei titolari di carta per conto di altri esercenti o fornitori di servizi. Ad esempio, un ISP è un esercente che accetta le carte di pagamento per la fatturazione mensile, ma funge anche da provider di servizi se ospita gli esercenti come clienti.
<b>Evento di sicurezza</b>	Evento che, dal punto di vista di un’organizzazione, presenta potenziali implicazioni per la sicurezza di un sistema o del relativo ambiente. Nel contesto di PCI DSS, gli eventi di sicurezza identificano attività sospette o anomale.
<b>FIPS</b>	Acronimo di Federal Information Processing Standards. Standard riconosciuti pubblicamente dal governo federale degli Stati Uniti, anche per l’uso da parte di agenzie non governative e collaboratori.
<b>Firewall</b>	Tecnologia hardware e/o software che protegge le risorse di rete dall’accesso non autorizzato. Un firewall consente o vieta il traffico informatico tra le reti con livelli di sicurezza differenti in base a un set di regole e altri criteri.
<b>Firewall personale</b>	Prodotto software firewall installato su un singolo computer.
<b>FTP</b>	Acronimo di File Transfer Protocol. Protocollo di rete utilizzato per trasferire i dati da un computer all’altro tramite una rete pubblica come Internet. FTP è ampiamente considerato un protocollo non sicuro, perché le password e il contenuto dei file sono inviati senza protezione e in chiaro. FTP può essere implementato in modo sicuro tramite SSH o altre tecnologie. Vedere <i>S-FTP</i> .
<b>Gestione delle chiavi di crittografia</b>	La serie di processi e meccanismi che supportano la definizione e la manutenzione delle chiavi di crittografia, compresa la sostituzione delle vecchie chiavi con nuove chiavi secondo necessità.
<b>GPRS</b>	Acronimo di General Packet Radio Service. Servizio dati mobile disponibile agli utenti dei telefoni cellulari GSM. Famoso per l’uso efficiente di una larghezza di banda limitata. Particolarmente adatto per l’invio e la ricezione di piccoli pacchetti di dati, quali i messaggi e-mail e l’esplorazione del Web.

Termine	Definizione
<b>GSM</b>	Acronimo di Global System for Mobile Communications. Diffuso standard per reti e telefoni cellulari. L'ampia disponibilità di GSM ha reso particolarmente diffuso il roaming internazionale tra gli operatori di telefonia mobile, consentendo agli abbonati di utilizzare i loro telefoni in molte parti del mondo.
<b>Hashing</b>	<p>Processo che rende illeggibili i dati dei titolari di carta mediante conversione dei dati in un digest di messaggio di lunghezza fissa tramite la <i>Crittografia avanzata</i>. L'hashing è una funzione unidirezionale (matematica) in cui un algoritmo non segreto che considera come input un messaggio di lunghezza arbitraria e produce un output di lunghezza fissa (di solito denominato "codice hash" o "digest di messaggio"). Una funzione hash deve avere le seguenti proprietà:</p> <ul style="list-style-type: none"> <li>(1) È inattuabile computazionalmente determinare l'input originale avendo solo in codice hash.</li> <li>(2) È inattuabile computazionalmente trovare due input che diano il medesimo codice hash.</li> </ul> <p>In ambito PCI DSS, l'hashing deve essere applicato all'intero PAN affinché il codice hash sia considerato reso illeggibile. Si raccomanda che i dati dei titolari di carta codificati mediante hash includano una variabile di immissione per la funzione di hashing allo scopo di ridurre o annullare l'efficacia degli attacchi "rainbow table" precalcolati (vedere <i>Variabile di immissione</i>).</p>
<b>Host</b>	Hardware del computer principale su cui risiede il software del computer.
<b>HSM</b>	Acronimo di Hardware Security Module o Host Security Module. Un dispositivo hardware fisicamente e logicamente protetto che fornisce una serie protetta di servizi di crittografia, utilizzato per funzioni di gestione delle chiavi di crittografia e/o per la decifratura dei dati degli account.
<b>HTTP</b>	Acronimo di HyperText Transfer Protocol. Protocollo Internet aperto per il trasferimento delle informazioni sul World Wide Web.
<b>HTTPS</b>	Acronimo di HyperText Transfer Protocol over Secure Socket Layer. HTTP sicuro che fornisce l'autenticazione e la comunicazione cifrata sul World Wide Web, progettato per la comunicazione di informazioni sensibili quali i dati di accesso basati sul Web.
<b>Hypervisor</b>	Software o firmware responsabile dell'hosting e della gestione delle macchine virtuali. Ai fini del PCI DSS, il componente di sistema hypervisor comprende anche il VMM (Virtual Machine Monitor).
<b>Hypervisor virtuale</b>	Vedere <i>Hypervisor</i> .
<b>ID</b>	Identificatore per un particolare utente o applicazione.

Termine	Definizione
<b>IDS</b>	Acronimo di Intrusion Detection System. Software o hardware utilizzato per identificare e avvertire in caso di anomalie o tentativi di intrusione nella rete o nel sistema. Composto da sensori che generano eventi di protezione, una console per monitorare gli eventi e gli avvisi e per controllare i sensori, un modulo di gestione centrale che registra in un database gli eventi generati dai sensori. Utilizza un sistema di regole per generare avvisi in risposta agli eventi di protezione rilevati. Vedere <i>IPS</i>
<b>IETF</b>	Acronimo di Internet Engineering Task Force. Una grande comunità internazionale aperta di designer di reti, operatori, fornitori e ricercatori interessati all'evoluzione dell'architettura Internet e al corretto funzionamento di Internet. IETF non presenta membri formali ed è aperta a tutti gli individui interessati.
<b>IMAP</b>	Acronimo di Internet Message Access Protocol. Protocollo Internet di livello applicativo che consente a un client e-mail di accedere alla posta elettronica su un server di posta remoto.
<b>Indipendenza organizzativa</b>	Una struttura organizzativa che garantisce che non vi è alcun conflitto di interessi tra la persona o l'ufficio che svolge l'attività e la persona o l'ufficio che valuta l'attività. Ad esempio, gli individui che eseguono le valutazioni sono organizzativamente separati dalla gestione dell'ambiente in corso di valutazione.
<b>Indirizzo IP</b>	Definito anche "indirizzo Internet Protocol". Codice numerico che identifica in modo univoco un particolare computer (host) su Internet.
<b>Indirizzo MAC</b>	Abbreviazione di "indirizzo Media Access Control". Valore di identificazione univoco assegnato dai produttori agli adattatori di rete e alle schede di interfaccia di rete.
<b>Informazioni personalmente identificabili</b>	Informazioni che possono essere utilizzate per identificare o tenere traccia dell'identità di un individuo inclusi, senza limitazioni, nome, indirizzo, numero di previdenza sociale, dati biometrici, data di nascita ecc.
<b>Injection flaw</b>	Vulnerabilità causata da tecniche di codifica non sicure, con conseguente convalida impropria dei dati immessi, che consente agli aggressori di trasmettere codice dannoso attraverso un'applicazione Web al sistema sottostante. Questa classe di vulnerabilità include SQL injection, LDAP injection e XPath injection.
<b>IP</b>	Acronimo di Internet Protocol. Protocollo dello strato di rete contenente informazioni sull'indirizzo e alcune informazioni di controllo che consentono il routing dei pacchetti e il loro invio dall'host di origine all'host di destinazione. IP è il principale protocollo dello strato di rete nella suite di protocolli Internet. Vedere <i>TCP</i> .
<b>IPS</b>	Acronimo di Intrusion Prevention System. Oltre al sistema IDS, IPS si occupa di bloccare i tentativi di intrusione.
<b>IPSEC</b>	Abbreviazione di Internet Protocol Security. Standard per la protezione delle comunicazioni IP nel livello di rete mediante cifratura e/o autenticazione di tutti i pacchetti IP in una sessione di comunicazione.

Termine	Definizione
<b>ISO</b>	Più comunemente nota come International Organization for Standardization. Organizzazione non governativa costituita da una rete di organismi nazionali di normalizzazione.
<b>Ispezione stateful</b>	Detta anche Dynamic Packet Filtering. Funzionalità del firewall che garantisce la protezione avanzata mediante il monitoraggio dello stato delle connessioni di rete. È programmata per riconoscere i pacchetti legittimi di connessioni. Il firewall consente il passaggio dei soli pacchetti che corrispondono a una connessione stabilita; tutti gli altri vengono respinti.
<b>LAN</b>	Acronimo di Local Area Network. Un gruppo di computer e/o altri dispositivi che condividono una linea di comunicazione comune, spesso in un edificio o in un gruppo di edifici.
<b>LDAP</b>	Acronimo di Lightweight Direct Access Protocol. Repository dei dati di autenticazione e autorizzazione utilizzato per le query e per la modifica delle autorizzazioni utente e per concedere l'accesso alle risorse protette.
<b>Log</b>	Vedere <i>Log di audit</i> .
<b>Log di audit</b>	Definito anche “audit trail”. Record cronologico delle attività di sistema. Fornisce una registrazione sufficiente a consentire la ricostruzione, la revisione e l'analisi della sequenza di ambienti e attività che circondano o conducono a un'operazione, procedura o evento in una transazione, dall'inizio al risultato finale.
<b>LPAR</b>	Abbreviazione di “logical partition”, partizione logica. Un sistema di suddivisione, o partizionamento, delle risorse totali di un computer (processori, memoria e spazio di memorizzazione) in unità più piccole, che possono eseguire una copia unica e distinta di sistemi operativi e applicazioni. Il partizionamento logico viene in genere utilizzato per consentire l'uso di sistemi operativi e applicazioni diversi su un singolo dispositivo. Le partizioni possono o meno essere configurate per comunicare tra loro o per condividere alcune risorse sul server, ad esempio le interfacce di rete.
<b>MAC</b>	Nel contesto della crittografia, un acronimo di Message Authentication Code. Una piccola informazione utilizzata per autenticare un messaggio. Vedere <i>Crittografia avanzata</i> .
<b>Macchina virtuale</b>	Un ambiente operativo autonomo che si comporta come un computer separato. È conosciuto anche come “Guest” e la sua esecuzione avviene in aggiunta all'hypervisor.
<b>Mainframe</b>	Computer progettati per gestire enormi volumi di input e output di dati e per aumentare la velocità di elaborazione. I mainframe possono eseguire più sistemi operativi, così che sembrano gestiti da più computer. Molti sistemi legacy dispongono di una struttura mainframe.

Termine	Definizione
<b>Mascheratura</b>	Nell'ambito di PCI DSS, si tratta di un metodo occultamento di un segmento di dati quando viene visualizzato o stampato. La mascheratura è utilizzata quando non esistono requisiti aziendali di visualizzazione dell'intero PAN. La mascheratura si riferisce alla protezione del PAN quando viene visualizzato o stampato. Vedere <i>Troncatura</i> per la protezione del PAN quando viene memorizzato in file, database ecc.
<b>Metodologia di versioning</b>	Processo di assegnazione di schemi di versioni per identificare in modo univoco un determinato stato di un'applicazione o software. Questi schemi seguono un formato versione-numero e un uso versione-numero più un elemento jolly secondo quanto definito dal fornitore del software. I numeri di versione in genere sono assegnati secondo l'ordinamento crescente e corrispondono a una particolare modifica nel software.
<b>Minaccia</b>	Condizione o attività che può potenzialmente causare la perdita, la modifica, l'esposizione, l'inaccessibilità intenzionale o accidentale di informazioni o risorse di elaborazione delle informazioni, o che comunque porta un danno all'organizzazione.
<b>MO/TO</b>	Acronimo di "Mail-Order/Telephone-Order" (ordine via posta o telefono).
<b>Monitoraggio</b>	Utilizzo di sistemi o processi che controllano costantemente il computer o le risorse di rete al fine di avvertire il personale in caso di interruzioni, allarmi o altri eventi predefiniti.
<b>Monitoraggio dell'integrità dei file</b>	Tecnica o tecnologia secondo la quale alcuni file o registri vengono monitorati per rilevarne le modifiche. Se vengono modificati file o registri importanti, vengono inviati avvisi al personale appropriato della sicurezza.
<b>MPLS</b>	Acronimo di Multi Protocol Label Switching. Rete o meccanismo di telecomunicazioni studiato per connettere un gruppo di reti a commutazione di pacchetto.
<b>NAC</b>	Acronimo di Network Access Control o Network Admission Control. Metodo per implementare la sicurezza a livello di rete limitando la disponibilità delle risorse di rete ai dispositivi endpoint in base a una determinata politica di sicurezza.
<b>NAT</b>	Acronimo di Network Address Translation. Detto anche network masquerading o IP masquerading. La modifica di un indirizzo IP utilizzato in una rete in un indirizzo IP diverso all'interno di un'altra rete, per permettere a un'organizzazione di avere indirizzi interni visibili internamente e indirizzi esterni visibili solo esternamente.
<b>NIST</b>	Acronimo di National Institute of Standards and Technology. Agenzia federale non di regolamentazione all'interno della Technology Administration del Ministero del Commercio degli Stati Uniti.
<b>NMAP</b>	Software per scansioni di protezione che connette le reti e identifica le porte aperte nelle risorse di rete.
<b>NTP</b>	Acronimo di Network Time Protocol. Protocollo per la sincronizzazione degli orologi di sistemi informatici, dispositivi di rete e altri componenti di sistema.



Termine	Definizione
<b>Numero di conto</b>	Vedere <i>PAN</i> ( <i>Primary Account Number</i> ).
<b>NVD</b>	Acronimo di National Vulnerability Database. L'archivio del governo degli Stati Uniti contenente i dati sulla gestione delle vulnerabilità basata sugli standard. NVD include i database delle liste di controllo di sicurezza, dei difetti software relativi alla sicurezza, delle configurazioni errate, dei nomi di prodotti e delle metriche di impatto.
<b>OCTAVE®</b>	Acronimo di Operationally Critical Threat, Asset, and Vulnerability Evaluation. Una suite di strumenti, tecniche e metodi per la valutazione strategica e la pianificazione basate sui rischi della sicurezza delle informazioni.
<b>Oggetto a livello di sistema</b>	Ogni elemento di un componente di sistema necessario per il suo funzionamento, inclusi, senza limitazioni, tabelle di database, stored procedure, eseguibili di applicazioni e file di configurazione, file di configurazione di sistema, DLL e librerie statiche e condivise, eseguibili di sistema, driver di dispositivi e file di configurazione dei dispositivi e componenti aggiunti di terzi.
<b>OWASP</b>	Acronimo di Open Web Application Security Project. Un'organizzazione senza scopo di lucro mirata a migliorare la sicurezza del software applicativo. OWASP si occupa di un elenco delle vulnerabilità più importanti delle applicazioni Web. Vedere <a href="http://www.owasp.org">http://www.owasp.org</a> .
<b>Pad</b>	In crittografia, one-time pad è un algoritmo di cifratura che combina il testo con una chiave casuale, o pad, lunga quanto il testo in chiaro e utilizzata una sola volta. Inoltre, se la chiave è realmente casuale, mai riutilizzata e tenuta segreta, one-time pad è inviolabile.
<b>PA-DSS</b>	Acronimo di Payment Application Data Security Standard.
<b>PAN</b>	Acronimo di Primary Account Number e definito anche "numero di conto". Numero univoco della carta di pagamento (tipicamente per le carte di credito o debito) che identifica l'emittente e il conto del titolare della carta.
<b>PA-QSA</b>	Acronimo di Payment Application Qualified Security Assessor. I PA-QSA sono qualificati da PCI SSC per la valutazione delle applicazioni di pagamento rispetto ai requisiti di PA-DSS. Fare riferimento alla <i>Guida del programma PA-DSS</i> ed ai <i>requisiti di qualifica di PA-QSA</i> per i dettagli sui requisiti relativi alle società ed ai dipendenti PA-QSA.
<b>Password predefinita</b>	Password di amministrazione del sistema, utente o degli account di servizio predefinita in un sistema, applicazione o dispositivo; generalmente è associata all'account predefinito. Gli account e le password predefiniti sono pubblicati e conosciuti, pertanto possono essere facilmente indovinati.
<b>Password/passphrase</b>	Una stringa di caratteri per l'autenticazione dell'utente.
<b>PAT</b>	Acronimo di Port Address Translation e definito anche "traduzione della porta per l'indirizzo di rete". Un tipo di NAT che converte anche i numeri di porta.



Termine	Definizione
<b>Patch</b>	Aggiornamento del software esistente per aggiungere funzionalità o correggere un difetto.
<b>PCI</b>	Acronimo di Payment Card Industry.
<b>PCI DSS</b>	Acronimo di Payment Card Industry Data Security Standard
<b>PDA</b>	Acronimo di Personal Data Assistant o Personal Digital Assistant. Dispositivi palmari con funzionalità di telefono cellulare, client e-mail o browser Web.
<b>PED</b>	PIN Entry Device (dispositivo di immissione PIN)
<b>Periodo di crittografia</b>	Periodo durante il quale una determinata chiave di crittografia può essere usata per uno scopo specifico in base, ad esempio, ad un periodo di tempo definito e/o alla quantità di testo di cifratura che è stato prodotto e secondo le linee guida e le migliori pratiche del settore (ad esempio, <i>NIST Special Publication 800-57</i> ).
<b>Personale</b>	Dipendenti a tempo pieno e part-time, dipendenti con contratto a tempo determinato, collaboratori o consulenti che svolgono le proprie prestazioni presso la sede dell'entità o che hanno in altro modo accesso all'ambiente dei dati dei titolari di carta.
<b>PIN</b>	Acronimo di Personal Identification Number. Password numerica segreta nota solo all'utente e a un sistema di autenticazione dell'utente. L'utente ottiene l'accesso solamente se il PIN specificato corrisponde a quello nel sistema. I PIN vengono in genere utilizzate agli sportelli Bancomat per le transazioni di anticipo contante. Un altro tipo di PIN è utilizzato nelle carte con chip EMV, dove il PIN sostituisce la firma del titolare della carta.
<b>POI</b>	Acronimo di Punto di interazione, il punto iniziale in cui sono letti i dati da una carta. Prodotto elettronico per l'accettazione della transazione, il POI è composto da hardware e software ed è ospitato nell'apparecchiatura di accettazione per consentire al titolare di carta di eseguire una transazione con carta. Il POI può sotto sorveglianza o meno. Le transazioni POI sono in genere transazioni di pagamento basate su carta con striscia magnetica e/o circuito integrato (chip).
<b>POP3</b>	Acronimo di Post Office Protocol v3. Protocollo di livello applicazione utilizzato dai client di e-mail per recuperare la posta elettronica da un server remoto tramite una connessione TCP/IP.
<b>Porta</b>	Punti di connessione logici (virtuali) associati a un determinato protocollo di comunicazione per facilitare le comunicazioni tra reti.
<b>POS</b>	Acronimo di Point of Sale. Hardware e/o software utilizzato per elaborare le transazioni delle carte di pagamento nelle sedi degli esercenti.
<b>Privilegio più basso</b>	Dotato dell'accesso e/o dei privilegi minimi necessari per eseguire i ruoli e le responsabilità previsti dalla mansione.
<b>Procedura</b>	Descrizione narrativa di un criterio. La procedura è la "guida pratica" a un criterio e ne descrive l'implementazione.

Termine	Definizione
<b>Prodotti standard</b>	Descrizione di prodotti in stock, non personalizzati o progettati per un cliente o utente specifico e facilmente disponibili per l'uso.
<b>Protocolli di sicurezza</b>	Protocolli di comunicazione di rete progettati per rendere sicura la trasmissione dei dati. Esempi di protocolli di sicurezza comprendono, senza limitazioni, SSL/TLS, IPSEC, SSH, HTTPS ecc.
<b>Protocollo</b>	Metodo di comunicazione concordato utilizzato nelle reti. Specifica che descrive regole e procedure che i prodotti per computer devono seguire per svolgere attività su una rete.
<b>Protocollo/servizio/porta non sicuri</b>	Un protocollo, un servizio o una porta che presenta problemi di protezione a causa della mancanza di controlli sulla riservatezza e/o sull'integrità. Questi problemi di protezione comprendono servizi, protocolli o porte che trasmettono dati o credenziali di autenticazione (ad es. password/passphrase in chiaro su Internet) o che consentono facilmente lo sfruttamento sia per impostazione predefinita sia in caso di errata configurazione. Esempi di servizi, protocolli o porte non sicuri includono, senza limitazioni, FTP, Telnet, POP3, IMAP e SNMP v1 e v2.
<b>Provider di hosting</b>	Offre diversi servizi agli esercenti e ad altri provider di servizi. I servizi sono di tipo semplice o complesso, dallo spazio condiviso su un server a un'intera gamma di "carrelli per gli acquisti", dalle applicazioni di pagamento alle connessioni a gateway ed elaboratori di pagamenti, fino all'hosting dedicato a un solo cliente per server. Un provider di hosting può anche essere un provider di hosting condiviso, che ospita più entità su un singolo server.
<b>Provider di servizi</b>	Entità commerciale che non rappresenta un marchio di pagamento ma è direttamente coinvolta nell'elaborazione, nella memorizzazione o nella trasmissione dei dati dei titolari di carta per conto di un'altra entità. Sono comprese anche le società che forniscono servizi che controllano o possono influire sulla sicurezza dei dati dei titolari di carta. Gli esempi comprendono provider di servizi gestiti che mettono a disposizione firewall gestiti, IDS e altri servizi, così come provider di hosting e altre entità. Se un'entità fornisce un servizio che coinvolge <i>solo</i> la fornitura dell'accesso pubblico alla rete (ad esempio una società di telecomunicazioni che fornisce solo il collegamento di comunicazione), l'entità non sarebbe considerata un provider di servizi per tale servizio (anche se potrebbe essere considerata un provider di servizi per altri servizi).
<b>PTS</b>	Acronimo di PIN Transaction Security, PTS è un serie di requisiti di valutazione modulare gestito da PCI Security Standards Council, per terminali POI di accettazione del PIN. Fare riferimento a <a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a> .
<b>Punto di accesso wireless</b>	Definito anche AP. Dispositivo che consente ai dispositivi di comunicazione wireless di connettersi a una rete wireless. Di solito connesso a una rete cablata, può inoltrare i dati tra i dispositivi wireless e cablati della rete.
<b>PVV</b>	Acronimo di PIN Verification Value. Valore discrezionale codificato nella striscia magnetica della carta di pagamento.

Termine	Definizione
<b>QIR</b>	Acronimo di Qualified Integrator or Reseller. Per ulteriori informazioni, fare riferimento alla <i>Guida del programma QIR</i> sul sito Web PCI SSC.
<b>QSA</b>	Acronimo di Qualified Security Assessor. I QSA sono qualificati da PCI SSC per condurre valutazioni PCI DSS in loco. Fare riferimento ai <i>Requisiti di qualifica di QSA</i> per i dettagli sui requisiti per le aziende e i dipendenti QSA.
<b>Query parametrizzate</b>	Un modo di strutturare query SQL per limitare l'escape e quindi impedire attacchi injection.
<b>RADIUS</b>	Abbreviazione di Remote Authentication Dial-In User Service. Sistema di autenticazione e accounting. Verifica se le informazioni, quali nome utente e password, passate al server RADIUS sono corrette, quindi autorizza l'accesso al sistema. Questo metodo di autenticazione può essere usato con un token, una smart card ecc. per fornire l'autenticazione a due fattori.
<b>Re-keying</b>	Processo di modifica delle chiavi di crittografia. Il re-keying periodico limita la quantità di dati crittografati da una singola chiave.
<b>Rete</b>	Due o più computer collegati mediante un mezzo fisico o wireless.
<b>Rete attendibile</b>	Rete di un'organizzazione che può essere controllata o gestita dall'organizzazione stessa.
<b>Rete non attendibile</b>	Una rete esterna alle reti che appartengono a un'organizzazione e che l'organizzazione non è in grado di controllare o gestire.
<b>Rete privata</b>	Rete stabilita da un'organizzazione che utilizza uno spazio degli indirizzi IP privato. Le reti private sono comunemente pensate come reti locali. L'accesso alla rete privata da parte delle reti pubbliche deve essere opportunamente protetto mediante l'uso di firewall e router.
<b>Rete pubblica</b>	Rete stabilita e gestita da un provider di telecomunicazioni, allo scopo specifico di fornire servizi di trasmissione dati al pubblico. I dati sulle reti pubbliche possono essere intercettati, modificati e/o deviati durante il transito. Esempi di reti pubbliche nell'ambito di PCI DSS comprendono, senza limitazioni, Internet e le tecnologie wireless e mobile.
<b>Reti wireless</b>	Reti che connettono i computer senza un collegamento fisico mediante fili.
<b>RFC 1918</b>	Lo standard identificato da Internet Engineering Task Force (IETF) che definisce l'uso e gli intervalli di indirizzi adeguati per le reti private (non instradabili su Internet).
<b>Rivenditori/Responsabili dell'integrazione</b>	Un'entità che vende e/o integra applicazioni di pagamento ma che non le sviluppa.
<b>ROC</b>	Acronimo di Report on Compliance (rapporto sulla conformità). Relazione che documenta i risultati dettagliati della valutazione PCI DSS di un'entità.
<b>Rootkit</b>	Tipo di software dannoso che, una volta installato senza autorizzazione, è in grado di celare la sua presenza e di ottenere il controllo amministrativo di un sistema informatico.

Termine	Definizione
<b>Router</b>	Hardware o software che connette due o più reti. Svolge le funzioni di ordinamento e interpretazione osservando gli indirizzi e passando le informazioni alle destinazioni appropriate. I router software sono a volte definite gateway.
<b>ROV</b>	Acronimo di Report on Validation (rapporto di convalida). Report contenente i risultati dettagliati di una valutazione PA-DSS per gli scopi del programma PA-DSS.
<b>RSA</b>	Algoritmo per la cifratura a chiave pubblica descritto nel 1977 da Ron Rivest, Adi Shamir e Len Adleman del Massachusetts Institute of Technology (MIT); le lettere RSA sono le iniziali dei loro cognomi.
<b>SANS</b>	Acronimo di SysAdmin, Audit, Networking and Security. Un istituto che fornisce formazione per la sicurezza informatica e certificazione professionale. Vedere <a href="http://www.sans.org">www.sans.org</a> .
<b>SAQ</b>	Acronimo di Self-Assessment Questionnaire (questionario di autovalutazione). Tool di reportistica utilizzato per documentare i risultati di autovalutazione relativi alla valutazione PCI DSS di un'entità.
<b>Scansione della protezione di rete</b>	Processo mediante il quale i sistemi di un'entità vengono controllati in remoto alla ricerca di vulnerabilità, per mezzo di strumenti automatici o manuali. Scansioni di protezione che includono l'analisi di sistemi interni ed esterni e la creazione di rapporti sui servizi esposti alla rete. Le scansioni possono identificare le vulnerabilità in sistemi operativi, servizi e dispositivi che possono essere utilizzate da utenti non autorizzati.
<b>Schema</b>	Descrizione formale della struttura di un database, compresa l'organizzazione di elementi di dati.
<b>Scienza forense</b>	Definita anche "scienza forense per l'informatica". Per quanto riguarda la sicurezza delle informazioni, l'applicazione di strumenti di indagine e tecniche di analisi per raccogliere prove dalle risorse informatiche al fine di determinare la causa delle compromissioni dei dati.
<b>SDLC</b>	Acronimo di System Development Life Cycle o Software Development Lifecycle. Fasi dello sviluppo di un software o di un sistema informatico che comprendono pianificazione, analisi, progettazione, test e implementazione.
<b>Segmentazione di rete</b>	Definita anche "segmentazione" o "isolamento". La segmentazione di rete isola i componenti di sistema che memorizzano, elaborano o trasmettono dati dei titolari di carta dai sistemi che non lo fanno. Un'adeguata segmentazione di rete può ridurre l'ambito dell'ambiente dei dati dei titolari di carta e quindi ridurre l'ambito della valutazione PCI DSS. Vedere la sezione Segmentazione di rete in <i>Requisiti PCI DSS e procedure di valutazione della sicurezza</i> per istruzioni sull'uso della segmentazione di rete. La segmentazione di rete non costituisce un requisito PCI DSS.
<b>Separazione dei compiti</b>	Pratica di divisione dei passaggi di una funzione tra individui diversi, in modo da evitare che una singola persona possa sabotare il processo.

Termine	Definizione
<b>Server</b>	Computer che fornisce un servizio ad altri computer, ad esempio l'elaborazione delle comunicazioni, la memorizzazione dei file o l'accesso a un servizio di stampa. I server comprendono, senza limitazioni, Web, database, applicazioni, autenticazione, DNS, posta, proxy e NTP.
<b>Server proxy</b>	Server che funge da intermediario tra una rete interna e Internet. Ad esempio, una funzione di un server proxy è terminare o negoziare connessioni tra collegamenti interni ed esterni, in modo che ciascuno di essi comunichi solo con il server proxy.
<b>Server Web</b>	Computer che contiene un programma che accetta richieste HTTP dai client Web e serve le risposte HTTP (in genere pagine Web).
<b>Servizi di emissione</b>	Esempi di servizi di emissione includono, senza limitazioni, autorizzazione e personalizzazione della carta.
<b>S-FTP</b>	Acronimo di Secure-FTP. S-FTP ha la possibilità di crittografare le informazioni di autenticazione e i file di dati in transito. Vedere <i>FTP</i> .
<b>SHA-1/SHA-2</b>	Acronimo di Secure Hash Algorithm. Un insieme di funzioni di hash crittografico correlate che comprende SHA-1 e SHA-2. Vedere <i>Crittografia avanzata</i> .
<b>Sicurezza delle informazioni</b>	Protezione delle informazioni per garantire la riservatezza, l'integrità e la disponibilità.
<b>Sistema informatico</b>	Insieme discreto di risorse dati strutturate, organizzato per la raccolta, l'elaborazione, la manutenzione, l'uso, la condivisione, la distribuzione o lo smaltimento delle informazioni.
<b>Sistema operativo</b>	Software di un sistema informatico responsabile della gestione e della coordinazione di tutte le attività e della condivisione delle risorse del computer. Alcuni esempi di sistemi operativi sono Microsoft Windows, Mac OS, Linux e Unix.
<b>Smagnetizzazione</b>	Definita anche "smagnetizzazione del disco". Processo o tecnica per smagnetizzare il disco in modo tale che tutti i dati memorizzati sul disco siano permanentemente distrutti.
<b>Smart card</b>	Detta anche "carta con chip" o "carta IC (carta a circuito integrato)". Un tipo di carta di pagamento in cui sono incorporati circuiti integrati. I circuiti, detti anche "chip", contengono i dati della carta di pagamento, compresi, senza limitazioni, i dati equivalenti a quelli della striscia magnetica.
<b>Sniffing di rete</b>	Definito anche come "packet sniffing" o "sniffing". Tecnica che controlla passivamente o raccoglie le comunicazioni di rete, decodifica i protocolli ed esamina i contenuti alla ricerca di informazioni di interesse.
<b>SNMP</b>	Acronimo di Simple Network Management Protocol. Supporta il monitoraggio dei dispositivi di rete per qualsiasi condizione che richiede attenzione a livello amministrativo.

Termine	Definizione
<b>Software dannoso/malware</b>	Software o firmware progettato per infiltrarsi in un sistema informatico o danneggiarlo a insaputa o senza il consenso del proprietario, con l'intento di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o del sistema operativo del proprietario. Il software di questo tipo in genere penetra nella rete durante molte attività aziendali approvate, sfruttando così le vulnerabilità del sistema. Gli esempi comprendono virus, worm, cavalli di Troia, spyware, adware e rootkit.
<b>Split knowledge</b>	Metodo tramite cui due o più entità dispongono separatamente di componenti chiave che singolarmente non trasmettono alcuna conoscenza sulla chiave crittografica risultante.
<b>Spoofing dell'indirizzo IP</b>	Tecnica di attacco utilizzata per ottenere l'accesso non autorizzato a reti o computer. L'utente non autorizzato invia messaggi ingannevoli a un computer con un indirizzo IP che indica che il messaggio proviene da un host attendibile.
<b>Spyware</b>	Tipo di software dannoso che, una volta installato, intercetta o assume il controllo parziale del computer senza il consenso dell'utente.
<b>SQL</b>	Acronimo di Structured Query Language. Linguaggio informatico utilizzato per creare, modificare e recuperare i dati dai sistemi di gestione dei database relazionali.
<b>SQL injection</b>	Forma di attacco su siti Web guidati da database. Un utente non autorizzato esegue comandi SQL non autorizzati sfruttando il codice non sicuro su un sistema connesso a Internet. Gli attacchi SQL injection sono utilizzati per sottrarre informazioni da un database in cui i dati normalmente non sarebbero disponibili e/o per ottenere l'accesso ai computer host di un'organizzazione tramite il computer che ospita il database.
<b>SSH</b>	Abbreviazione di Secure Shell. Suite di protocolli che fornisce la cifratura dei servizi di rete, quali accesso remoto o trasferimento di file remoto.
<b>SSL</b>	Acronimo di Secure Sockets Layer. Standard di settore che cifra il canale tra un browser Web e il server Web per garantire la riservatezza e l'affidabilità dei dati trasmessi su questo canale. Vedere <i>TLS</i> .
<b>Supporto elettronico rimovibile</b>	Supporto che memorizza dati digitalizzati e che può essere facilmente rimosso e/o trasportato da un sistema informatico a un altro. Esempi di supporti elettronici rimovibili comprendono CD-ROM, DVD-ROM, unità flash USB e unità disco rigido rimovibili.
<b>Switch o router virtuale</b>	Uno switch o router virtuale è un'entità logica con funzionalità di switching e routing di dati a livello di infrastruttura di rete. Uno switch virtuale costituisce una parte integrante di una piattaforma server virtualizzata come un plug-in, modulo o driver hypervisor.
<b>SysAdmin</b>	Abbreviazione di "system administrator", amministratore di sistema. Individuo con privilegi elevati, responsabile della gestione di un sistema o di una rete di computer.

Termine	Definizione
<b>TACACS</b>	Acronimo di Terminal Access Controller Access Control System. Il protocollo di autenticazione remota utilizzato comunemente nelle reti che comunicano tra un server di accesso remoto e un server di autenticazione per determinare i diritti di accesso dell'utente alla rete. Questo metodo di autenticazione può essere usato con un token, una smart card ecc. per fornire l'autenticazione a due fattori.
<b>TCP</b>	Acronimo di Transmission Control Protocol. Uno dei protocolli del livello di trasporto di base della suite Internet Protocol (IP), e il linguaggio o protocollo di comunicazione di base di Internet. Vedere <i>IP</i> .
<b>TDES</b>	Acronimo di Triple Data Encryption Standard; definito anche 3DES o Triple DES. Cifratura a blocchi formata dalla applicazione per tre volte della cifratura DES. Vedere <i>Crittografia avanzata</i> .
<b>Tecnologie mobili</b>	Comunicazioni mobili attraverso reti di telefonia senza fili, inclusi, senza limitazione, GSM (Global System for Mobile), CDMA (Code Division Multiple Access) e GPRS (General Packet Radio Service).
<b>TELNET</b>	Abbreviazione di Telephone Network Protocol. Utilizzato in genere per fornire sessioni di accesso ai dispositivi di una rete dalla riga di comando orientata all'utente. Le credenziali dell'utente vengono trasmesse in chiaro.
<b>Terminale di pagamento virtuale</b>	Un terminale di pagamento virtuale è un accesso basato su browser Web al sito Web 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 Web connesso in modo sicuro. A differenza dei terminali fisici, i terminali di pagamento virtuali non leggono i dati direttamente da una carta di pagamento. Dal momento che le transazioni della carta di pagamento sono inserite manualmente, i terminali di pagamento virtuali sono in genere usati al posto dei terminali fisici in ambienti di esercenti con un volumi limitati di transazioni.
<b>Test di penetrazione</b>	I test di penetrazione tentano di individuare i modi con cui sfruttare le vulnerabilità allo scopo di eludere o vanificare le caratteristiche di sicurezza dei componenti di sistema. I test di penetrazione includono test a livello di rete e applicazione nonché altri controlli e processi relativi a reti e applicazioni e vengono eseguiti sia dall'esterno dell'ambiente (test esterno) che dall'interno dell'ambiente.
<b>Titolare di carta</b>	Cliente consumatore e non per cui viene emessa una carta di pagamento o qualsiasi individuo autorizzato a utilizzare la carta di pagamento.
<b>TLS</b>	Acronimo di Transport Layer Security. Progettato per garantire la segretezza e l'integrità dei dati tra due applicazioni di comunicazione. TLS è il successore di SSL.
<b>Token</b>	Nel contesto del controllo dell'accesso e di autenticazione, un token è un valore fornito da hardware o software che funziona con un server di autenticazione o VPN per eseguire l'autenticazione dinamica o a due fattori. Vedere <i>RADIUS</i> , <i>TACACS</i> e <i>VPN</i> .



Termine	Definizione
<b>Token indicizzato</b>	Un token crittografico che sostituisce il numero PAN in base a un dato indice per un valore imprevedibile.
<b>Troncatura</b>	Metodo per rendere illeggibile l'intero PAN rimuovendo in modo permanente una parte dei dati PAN. La troncatura si riferisce alla protezione del PAN quando viene <u>memorizzato</u> in file, database, ecc. Vedere <i>Mascheratura</i> per la protezione del PAN quando viene <u>visualizzato</u> su schermi, ricevute cartacee, ecc.
<b>URL</b>	Acronimo di Uniform Resource Locator. Una stringa di testo formattato utilizzata dai browser Web, dai client di posta elettronica e da altro software per identificare una risorsa di rete su Internet.
<b>Uso di filtri in ingresso</b>	Metodo di filtraggio del traffico in entrata in modo tale che l'accesso alla rete sia consentito solo al traffico espressamente autorizzato.
<b>Uso di filtri in uscita</b>	Metodo di filtraggio del traffico in uscita in modo che solo al traffico espressamente autorizzato sia consentito lasciare la rete.
<b>Utente con privilegi</b>	Qualsiasi account utente con privilegi di accesso superiori a quelli di base. In genere, questi account hanno privilegi elevati o aumentati, con più diritti rispetto a un account utente standard. Tuttavia, l'estensione dei privilegi tra i diversi account privilegiati può variare notevolmente a seconda dell'organizzazione, della mansione o del ruolo e della tecnologia in uso.
<b>Utenti non consumatori</b>	Individui, ad esclusione dei titolari di carte, che accedono ai componenti di sistema, compresi senza limitazioni dipendenti, amministratori e terze parti.
<b>Variabile di immissione</b>	Stringa di dati casuali che viene concatenata con i dati di origine prima dell'applicazione di una funzione hash unidirezionale. Le variabili di immissione possono contribuire a ridurre l'efficacia degli attacchi rainbow table. Vedere anche <i>Hashing e Rainbow Table</i> .
<b>Virtual Machine Monitor (VMM)</b>	Il VMM è incluso nell'hypervisor ed è il software che implementa l'astrazione hardware della macchina virtuale. Gestisce l'elaboratore di pagamenti, la memoria ed altre risorse del sistema per assegnare ciò che serve ad ogni sistema operativo ospite.
<b>Virtualizzazione</b>	La virtualizzazione si riferisce all'astrazione logica di risorse informatiche dalle limitazioni fisiche. Un'astrazione comune riguarda le macchine virtuali (VM) che, prelevando i contenuti di una macchina fisica, ne consentono il funzionamento su un hardware fisico diverso e/o insieme ad altre macchine virtuali sul medesimo hardware fisico. Oltre che con le VM, è possibile eseguire la virtualizzazione su molte altre risorse informatiche comprese applicazioni, desktop, reti e memorizzazione.
<b>VLAN</b>	Abbreviazione di "virtual LAN" o "virtual local area network", rete locale virtuale. Rete locale logica che si estende oltre una singola rete locale fisica tradizionale.



Termine	Definizione
<b>VPN</b>	<p>Acronimo di Virtual Private Network. Una rete di computer in cui alcune connessioni sono circuiti virtuali all'interno di una rete più grande, ad esempio Internet, invece di collegamenti diretti mediante fili fisici. I punti finali della rete virtuale sono in tunneling nella rete più grande, quando è il caso. Se un'applicazione comune è costituita da comunicazioni attraverso la Internet pubblica, una VPN può o meno disporre di caratteristiche di sicurezza avanzata quali l'autenticazione o la cifratura del contenuto.</p> <p>Una VPN può essere usata con un token, smart card, ecc., per fornire l'autenticazione a due fattori.</p>
<b>Vulnerabilità</b>	Punti deboli in un sistema che consentono a un utente non autorizzato di sfruttare quel sistema e violarne l'integrità.
<b>WAN</b>	Acronimo di Wide Area Network. Rete di computer che copre un'area estesa, spesso l'intero sistema informatico di una società o di una zona.
<b>WEP</b>	Acronimo di Wired Equivalent Privacy. Algoritmo debole utilizzato per cifrare le reti wireless. Sono stati identificati diversi punti deboli da parte degli esperti del settore, che consentono di violare una connessione WEP con software disponibile entro pochi minuti. Vedere <i>WPA</i> .
<b>WLAN</b>	Acronimo di Wireless Local Area Network. Rete locale che collega due o più computer o dispositivi senza l'uso di fili.
<b>WPA/WPA2</b>	Acronimo di WiFi Protected Access. Protocollo di protezione creato per proteggere le reti wireless. WPA è il successore del WEP. È disponibile anche WPA2, la generazione successiva di WPA.
<b>XSS (Cross-Site Scripting)</b>	Vulnerabilità causata da tecniche di codifica non sicure, con conseguente convalida impropria dei dati immessi. Spesso utilizzata in combinazione con CSRF e/o SQL injection.