RISORSE PER LA PROTEZIONE DEI PAGAMENTI PER PICCOLI ESERCENTI

Glossario dei termini sulla sicurezza dei pagamenti e delle informazioni

VERSIONE 1.0 | LUGLIO 2016

PCI Security Standards Council®

Introduzione

Questo *Glossario dei termini sulla sicurezza dei pagamenti e delle informazioni* è un supplemento alla *Guida ai pagamenti sicuri*, parte delle Risorse per la protezione dei pagamenti per piccoli esercenti. Il suo scopo è quello di spiegare i termini rilevanti del settore delle carte di pagamento (PCI) della sicurezza delle informazioni in un linguaggio di facile comprensione.

Le definizioni dei termini contrassegnate da un asterisco (*) sono fondate su o derivate dalle definizioni contenute negli *Standard di protezione dei dati (DSS) del settore delle carte di pagamento (PCI)* e negli *Standard di protezione dati dell'applicazione di pagamento (PA-DSS): Il glossario dei termini, delle abbreviazioni e degli acronimi*, Versione 3.2, datato aprile 2016.

Fate riferimento alla *Guida ai pagamenti sicuri* e alle altre Risorse di protezione dei pagamenti per piccoli esercenti ai seguenti:

RISORSA	URL
Guida ai pagamenti sicuri	https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemi di pagamento comuni	https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Domande da chiedere ai vostri fornitori	https://it.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

Nota:
L'ultima versione degli *Standard di protezione dei dati (DSS) del settore delle carte di pagamento (PCI) e degli standard di protezione dati dell'applicazione di pagamento (PA-DSS): Il glossario dei termini, delle abbreviazioni e degli acronimi* viene considerato una fonte autorevole e occorre farvi riferimento per le definizioni correnti e complete degli standard PCI DSS e PA-DSS.

Glossario

TERMINE	DEFINIZIONE
Acquirente *	Consultate *Banca d'affari* ed *Elaboratore pagamenti*.
Software antivirus *	Programma software che rileva, rimuove e protegge da software dannoso (detto anche “malware”), tra cui virus, worm, cavalli di Troia, spyware, adware e rootkit. Denominato anche "software anti-malware".
Applicazione *	Programma software o gruppo di programmi che viene eseguito su un PC, smartphone, tablet, server interno o server Web.
Fornitori di scansioni approvati (ASV) *	Società approvata dal PCI Security Standards Council alla conduzione dei servizi di scansione per identificare i comuni punti deboli nella configurazione del sistema. Consultare anche *ASV*.
ASV *	Acronimo di Approved Scanning Vendor.
Autenticazione *	Processo di verifica dell’identità di un individuo, dispositivo o processo. L’autenticazione di norma avviene utilizzando uno o più fattori di autenticazione come: • qualcosa che l’utente conosce, come una password o una passphrase; • qualcosa in possesso dell'utente, come un dispositivo token o una smart card • qualcosa che l’utente è, come un elemento biometrico
Autorizzazione *	In una transazione della 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.
BIN (Bank Identification Number)	Le prime sei (o più) cifre di un numero di carta di pagamento che identifica l'istituto finanziario che emette la carta di pagamento ai titolari di carta.
Solo se effettivamente necessario	Il principio secondo il quale l'accesso ai sistemi o ai dati viene concesso in base alla necessità professionale dell'utente: solo ciò che è necessario per la funzione professionale di un utente.
Dati delle carte / Dati delle carte dei clienti *	Come minimo, i dati delle carte includono il PAN (Numero di conto primario) e potrebbero includere anche il nome del titolare di carta e la data di scadenza. Il PAN è visibile sulla parte anteriore della carta e codificato nella striscia magnetica della carta e/o nel chip integrato. Noti anche come dati dei titolari di carta. Consultare anche *Dati sensibili di autenticazione* per ulteriori elementi dati che possono far parte di una transazione di pagamento, ma che non devono essere salvati una volta che la transazione viene autorizzata.
Chip	Noto anche come "Chip EMV". Il microprocessore (o "chip") su una carta di pagamento utilizzato durante l'elaborazione delle transazioni in osservanza delle specifiche internazionali per le transazioni EMV.

Glossario

TERMINE	DEFINIZIONE
Chip e PIN	Un processo di verifica in cui un consumatore inserisce il proprio PIN in un terminale di pagamento abilitato al chip EMV quando effettua l'acquisto di beni o servizi.
Chip e firma	Un processo di verifica in cui un consumatore utilizza la propria firma con un terminale di pagamento abilitato al chip EMV, al momento dell'acquisto di beni o servizi.
Credenziale	Informazioni utilizzate per l'identificazione e l'autenticazione di un utente perché acceda a un sistema. Ad esempio, le credenziali sono spesso il nome utente e la password. Le credenziali possono includere un'impronta digitale, la scansione della retina o un numero usa e getta generato da un "generatore di token" portatile. La sicurezza è maggiore quando l'accesso richiede più credenziali.
Attacco cibernetico	Qualsiasi tipo di manovra offensiva per intromettersi in un computer o sistema. Gli attacchi cibernetici possono spaziare dall'installazione di spyware su un PC, all'ingresso forzato in un sistema di pagamento per appropriarsi dei dati delle carte di pagamento o al tentativo di danneggiare infrastrutture fondamentali come una rete elettrica.
Violazione dei dati	Una violazione dei dati è un incidente in cui i dati sensibili possono essere potenzialmente visualizzati, rubati o utilizzati da una parte non autorizzata. Le violazioni dei dati interessano dati delle carte di pagamento, informazioni personali sulla salute (PHI), informazioni personalmente identificabili (PII), scambi di segreti o di proprietà intellettuale, ecc.
Password predefinita	Una semplice password fornita con il nuovo software o hardware. Le password predefinite (come "admin" o "password" o "123456") sono facili da indovinare e solitamente sono disponibili mediante la ricerca online. Rappresentano una variabile metasintattica e non offrono una sicurezza effettiva. Devono essere modificate in password difficili una volta installato il nuovo software o hardware.
Registratore di cassa elettronico (RCE)	Un dispositivo che registra e calcola le transazioni e può stampare le ricevute, ma non accetta pagamenti mediante carte di pagamento. Chiamato anche "cassa".
Cifratura	Processo d'uso della crittografia per convertire matematicamente le informazioni in una forma inutilizzabile, eccetto per i possessori di una chiave digitale specifica. L'uso della cifratura protegge le informazioni rendendole inutili ai criminali. Consultare anche *Crittografia*.
Firewall *	Hardware e/o software che protegge le risorse di rete dall'accesso non autorizzato. Un firewall consente o vieta il traffico la comunicazione tra computer o reti con livelli di sicurezza differenti, in base a un set di regole e ad altri criteri.
Investigatore di scienza forense	Gli investigatori di scienza forense (ISF) sono società approvate dall'Ente PCI che aiutano nello stabilire quando e come si è verificata una violazione dei dati delle carte di pagamento. Eseguono delle indagini all'interno del settore finanziario usando metodologie e strumenti investigativi provati. Collaborano inoltre con le forze dell'ordine per assistere gli stakeholder in qualsiasi indagine sul crimine che ne risulta.

Glossario

TERMINE	DEFINIZIONE
Hacker	Una persona o un'organizzazione che prova ad aggirare le misure di sicurezza dei sistemi dei computer per ottenerne il controllo e l'accesso. Solitamente nel tentativo di appropriarsi dei dati delle carte di pagamento.
Provider di hosting *	Offre una varietà di servizi agli esercenti e altri provider di servizi, dove i dati dei clienti sono "ospitati" o si trovano nei server dei provider. I servizi tipici includono uno spazio condiviso per più esercenti su un server, la fornitura di un server dedicato a un solo esercente o app Web, come un sito Web con opzioni "carrello della spesa".
Terminale di pagamento integrato	Un terminale di pagamento e un registratore di cassa in un solo dispositivo, vale a dire che è in grado di ricevere pagamenti, registrare e calcolare transazioni e stampare ricevute.
Rivenditore/Responsabile dell'integrazione	Un rivenditore/responsabile dell'integrazione è una società che implementa, configura e/o supporta i terminali di pagamento, i sistemi di pagamento e/o le applicazioni di pagamento per gli esercenti. Tali società possono anche vendere i dispositivi o le applicazioni di pagamento come parte del loro servizio. Consultare anche *Responsabile dell'integrazione e rivenditore qualificati (QIR)*.
Log *	Un file creato automaticamente quando determinati eventi predefiniti (spesso correlati alla sicurezza) si verificano all'interno di un computer o rete. I dati del log includono data/ora, descrizione dell'evento e informazioni univoche relative all'evento. Questi file sono utili per la risoluzione di problemi tecnici o per un'indagine sulla violazione di dati. Chiamato anche "log di audit" o "audit trail".
Malware *	Software dannoso progettato per infiltrarsi in un computer al fine di appropriarsi di dati o di danneggiare applicazioni o il sistema operativo. Tale software solitamente entra in una rete durante numerose attività approvate dall'azienda, ad esempio mediante email o la navigazione di siti Web. Gli esempi di malware comprendono virus, worm, cavalli di Troia, spyware, adware e rootkit.
Banca d'affari *	Una banca o istituto finanziario che elabora pagamenti con carte di credito o di debito per conto degli esercenti. Chiamata anche "acquirente", "banca acquirente", "elaboratore di carte" o "elaboratore di pagamenti". Consultare anche *Elaboratore di pagamenti*.
Dispositivo mobile	Termine generale per una classe di dispositivi elettronici del consumatore, come smartphone e tablet che sono di piccole dimensioni, portatili e possono connettersi a reti di computer sulla rete wireless.
Accettazione di pagamenti mobili	Utilizzo di un dispositivo mobile per accettare ed elaborare transazioni di pagamento. Il dispositivo mobile viene solitamente associato a un accessorio di lettura carte disponibile a livello commerciale.
Autenticazione a più fattori *	Metodo di autenticazione di un utente quando vengono verificati due o più fattori. Tali fattori comprendono qualcosa in possesso dell'utente (ad esempio una smart card o un token hardware), qualcosa che l'utente conosce (una password, una passphrase o un PIN) o qualcosa che l'utente usa o svolge (ad esempio le impronte digitali o altre forme di biometrica).
Rete *	Due o più computer collegati mediante un mezzo fisico o wireless.

Glossario

TERMINE	DEFINIZIONE
Sistema operativo *	Software di un sistema informatico responsabile della gestione e della coordinazione di tutte le attività e della condivisione delle risorse del computer. Esempi includono Microsoft Windows, Apple OSX, iOS, Android, Linux e UNIX.
P2PE	Acronimo per lo standard Point-to-Point-Encryption dell'Ente PCI. Consultare i dettagli alla pagina *www.pcisecuritystandards.org*.
PA-DSS *	Acronimo di Payment Application Data Security Standard (Standard di protezione dei dati delle applicazioni di pagamento) dell'Ente PCI. Consultare i dettagli alla pagina *www.pcisecuritystandards.org*.
Password *	Una parola, frase o stringa di caratteri utilizzata per l'autenticazione di un utente. Quando combinata con il nome utente, la password ha lo scopo di provare l'identità dell'utente per l'accesso alle risorse del computer.
Patch *	Aggiornamento del software esistente che aggiunge funzionalità o corregge un difetto (o "bug").
Applicazione di pagamento *	Correlata a PA-DSS, un'applicazione software che memorizza, elabora o trasmette dati dei titolari di carta come nell'ambito del processo di autorizzazione o contabilizzazione delle transazioni.
Fornitore dell'applicazione di pagamento	Un'entità che vende, distribuisce o da in licenza un'applicazione di pagamento a responsabili dell'integrazione/rivenditori di POS da integrare ai sistemi di pagamento degli esercenti o direttamente agli esercenti per installazione e utilizzo propri.
Middleware di pagamento	Un termine generico per il software che collega due o più, probabilmente non correlate, applicazioni di pagamento. Ad esempio, potrebbe trasferire dati delle carte magnetiche tra un'applicazione su un terminale di pagamento e altri sistemi di esercenti che inviano dati di carte a un processore.
Elaboratore pagamenti *	Un'entità utilizzata da esercenti per gestire le transazioni delle carte di pagamento per loro conto. Mentre gli elaboratori di pagamenti di solito forniscono servizi di acquisizione, questi non vengono considerati acquirenti (banche d'affari) a meno che non siano così definiti da un marchio di carta di pagamento. Chiamato anche "gateway di pagamento" o "provider di servizi di pagamento" (PSP). Consultare anche *Banca d'affari*.
Sistema di pagamento	Include l'intero processo di accettazione di pagamenti mediante carte di pagamento in un punto vendita (inclusi negozi e vetrine e-commerce) e potrebbe includere un terminale di pagamento, un registratore di cassa elettronico, altri dispositivi o sistemi collegati al terminale di pagamento (ad esempio, Wi-Fi per la connettività o un PC utilizzato per l'inventario), server con componenti e-commerce quali pagine di pagamento e le connessioni a una banca d'affari.
Fornitore di sistemi di pagamento	Un fornitore che vende, fornisce in licenza o distribuisce una soluzione di pagamento completa a un esercente. La soluzione include l'hardware e il software necessari alla gestione dei pagamenti all'interno del negozio e fornisce un metodo di collegamento a un elaboratore pagamenti.
Terminale di pagamento	Dispositivo hardware utilizzato per accettare i pagamenti con carta dei clienti mediante strisciata, dip, inserimento o appoggio. Chiamato anche "terminale POS (point-of-sale)", "macchina delle carte di credito" o "terminale PDQ".

Glossario

TERMINE	DEFINIZIONE
PCI *	Acronimo di Payment Card Industry (Settore delle carte di pagamento).
PCI DSS *	Acronimo di "Standard di protezione dei dati del settore delle carte di pagamento" dell'Ente PCI. Consultare i dettagli alla pagina *www.pcisecuritystandards.org*.
Conforme agli standard PCI DSS	Soddisfa tutti i requisiti applicabili degli standard PCI DSS correnti su base continua, tramite un approccio business-as-usual. La conformità viene valutata e convalidata in un momento specifico; tuttavia, spetta a ciascun esercente seguire costantemente i requisiti, al fine di assicurare una sicurezza solida. Le banche d'affari e/o i marchi di pagamento potrebbero presentare requisiti per convalide annuali formali della conformità agli standard PCI DSS.
PCI DSS convalidati	Forniscono la prova che tutti i requisiti PCI DSS sono stati soddisfatti in un singolo momento. A seconda di specifici requisiti della banca d'affari e/o dei marchi di pagamento, è possibile ottenere la convalida mediante il Questionario di autovalutazione PCI DSS o un rapporto sulla conformità che risulta da una valutazione in loco.
Applicazioni di pagamento convalidate PCI	Applicazione convalidata in base agli Standard di protezione dei dati delle applicazioni di pagamento PCI (PA-DSS) e visualizzata sul sito Web dell'Ente PCI.
Terminale di pagamento approvato dal PCI	Terminale di pagamento approvato in base allo standard PTS (PCI PIN Transaction Security) e visualizzato sul sito Web dell'Ente PCI.
Soluzione di cifratura Point-to-Point elencata elencata dal PCI	Soluzione di cifratura convalidata in base allo standard P2PE (PCI Point-to-Point-Encryption) e visualizzata sul sito Web dell'Ente PCI.
PED *	Acronimo per "PIN entry device". Tastierino con cui il cliente inserisce il proprio PIN. Chiamato anche "tastierino del PIN".
PIN *	Acronimo di "Personal Identification Number". Un numero univoco nota solo all'utente e a un sistema di autenticazione dell'utente. Solitamente i PIN vengono utilizzati nei bancomat per le transazioni di prelievo contante o nelle carte con chip EMV che sostituisce la firma del titolare di carta. I PIN aiutano a stabilire se un titolare di carta sia autorizzato a utilizzare la carta e per impedire l'utilizzo non autorizzato della stessa, nel caso in cui fosse stata rubata.
Primary account number (PAN) *	Numero univoco per carte di credito e di debito che identifica l'account del titolare di carta.
Abuso di privilegio	Uso illecito dei privilegi di accesso a un computer. Gli esempi includono un amministratore di sistema che accede ai dati delle carte di pagamento a fini illeciti o qualcuno che si appropria e utilizza privilegi di accesso elevati di amministratore, sempre a fini illeciti.
PTS *	Acronimo dello standard di PTS (PIN Transaction Security) dell'Ente PCI. PTS è una serie di requisiti di valutazione modulari per terminali POI (point-of -interaction) di accettazione del PIN. Consultare i dettagli alla pagina www.pcisecuritystandards.org.
QIR *	Acronimo di "Qualified Integrator or Reseller". Consultare i dettagli alla pagina *www.pcisecuritystandards.org*.

Glossario

TERMINE	DEFINIZIONE
Qualified Security Assessor (QSA) *	Una società approvata dall'Ente degli standard di sicurezza PCI per convalidare la conformità di un'entità ai requisiti PCI DSS.
Pagamento ricorrente	Un metodo di fatturazione in cui gli esercenti inviano ripetutamente la fattura ai clienti, come nel caso di abbonamenti o sottoscrizioni mensili. Un modo sicuro per effettuare tale operazione per l'acquirente/elaboratore è quello di tokenizzare i dati delle carte. In tal modo assicura la protezione e libera l'esercente da questa responsabilità.
Accesso remoto *	Accesso a una rete di computer da una località esterna a tale rete. Le connessioni di accesso remoto possono provenire sia dall'interno della rete aziendale, sia da una postazione remota. Un esempio di tecnologia per l'accesso remoto è VPN (Virtual Private Network). L'accesso remoto può essere interno (ad esempio l'assistenza IT) o esterno (ad esempio provider di servizi, agenti di terze parti, responsabili di integrazione/rivenditori).
Rivenditori/Responsabili dell'integrazione *	Un'entità che vende e/o integra applicazioni di pagamento ma che non le sviluppa.
Router *	Hardware o software che collega due o più reti di computer interni o esterni per "indirizzare" o guidare i dati attraverso la rete e assicurarsi che vengano trasferiti correttamente tra le stesse. Il router può anche creare più sicurezza consentendo solo il traffico approvato e rifiutando il traffico non approvato.
Lettore di carte sicuro (SCR)	Un dispositivo approvato da PTS che si collega a un telefono mobile o tablet per l'accettazione protetta delle carte di pagamento. I SCR approvati da PTS del PCI proteggono e cifrano i dati delle carte mediante SRED. Consultare anche *SRED*.
Codice di sicurezza *	Un valore a tre o quattro cifre stampato sulla parte anteriore o sul pannello posteriore della firma di una carta di pagamento. Questo codice è associato in maniera esclusiva a una singola carta e viene utilizzato come controllo aggiuntivo per garantire che la carta sia in possesso del titolare di carta legittimo, solitamente durante una transazione in assenza di carta. Chiamato anche codice di sicurezza della carta.
Questionario di autovalutazione (SAQ) *	Strumento di convalida utilizzato per documentare i risultati di autovalutazione relativi alla valutazione PCI DSS di un'entità.
Dati sensibili di autenticazione *	Le informazioni relative alla sicurezza vengono utilizzate per autenticare i titolari di carta e/o autorizzare le transazioni delle carte di pagamento, memorizzate nella striscia magnetica o nel chip.
Provider di servizi *	Un'entità aziendale che fornisce una varietà di servizi agli esercenti. Solitamente, tali entità memorizzano, elaborano o trasmettono i dati delle carte per conto di un'altra entità (quale un esercente) O sono fornitori di servizi gestiti che offrono firewall gestiti, identificazioni di intromissioni, hosting e altri servizi correlati all'IT. Chiamato anche "fornitore".
Skimming	Appropriazione di dati delle carte direttamente dalla carta di pagamento del consumatore o dall'infrastruttura di pagamento presso la sede dell'esercente con un lettore di carte portatile contraffatto o mediante modifiche effettuate sul terminale di pagamento dell'esercente. Il suo scopo è quello di commettere frodi, la minaccia e seria e può colpire qualsiasi ambiente dell'esercente.

Glossario

TERMINE	DEFINIZIONE
Dispositivo di skimming	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. Chiamato anche "card skimmer".
Piccolo esercente	Un'azienda che solitamente ha una sola sede o forse alcune sedi, con budget IT limitato o assente e solitamente senza personale.
SRED	Un acronimo per la lettura e lo scambio dei dati protetti. Una serie di requisiti PTS PCI progettati per proteggere e cifrare i dati della carte nei terminali di pagamento. Una soluzione P2PE elencata dall'Ente PCI deve utilizzare un terminale di pagamento approvato dal PTS ed elencato con SRED abilitato e la cifratura eseguita attivamente dei dati delle carte.
Terminale autonomo	Un terminale di pagamento che non fa affidamento sulla connessione a un altro dispositivo all'interno dell'ambiente dell'esercente e non esegue altre funzioni. Il solo requisito per il suo funzionamento è una connessione all'elaboratore tramite una connessione Internet o linea telefonica. Se il terminale richiede la connessione a un registratore di cassa elettronico computerizzato o se ha più funzioni (come un dispositivo mobile), non è un terminale autonomo.
Autenticazione solida	Utilizzata per verificare l'identità di un utente o dispositivo al fine di garantire la sicurezza del sistema che protegge. Il termine autenticazione solida viene spesso utilizzato come sinonimo di autenticazione a più fattori (MFA).
Cassa	Consultare *Registratore di cassa elettronico.*
Tokenizzazione	Un processo mediante il quale il numero di conto primario (PAN) viene sostituito con un valore surrogato chiamato token. I token possono essere utilizzati al posto del PAN originale per eseguire funzioni quando la carta non è presente, come nel caso di assegni annullati, rimborsi o fatturazione ricorrente. I token forniscono una maggiore sicurezza se rubati in quanto non sono utilizzabili e pertanto non sono di alcuna utilità ai criminali.
Dati non cifrati	Tutti i dati leggibili senza decifrazione. Chiamato anche dati del "testo non formattato" e "testo non cifrato".
Fornitore	Un'entità aziendale che fornisce a un esercente un prodotto o servizio necessario all'esecuzione dei propri affari. Laddove vengono offerti servizi, il fornitore potrebbe essere considerato un provider di servizi e potrebbe richiedere l'accesso a sedi fisiche o a computer all'interno dell'ambiente dell'esercente, condizione che potrebbe avere un impatto sulla sicurezza dei dati delle carte di pagamento. Consultate anche *Provider di servizi.*
Terminale di pagamento virtuale *	L'accesso basato sul browser a un acquirente, a un elaboratore o al sito Web del provider di servizi di terze parti al fine di autorizzare le transazioni delle carte di pagamento. A differenza dei terminali fisici, i terminali di pagamento virtuali non leggono i dati direttamente da una carta di pagamento. L'esercente inserisce manualmente i dati delle carte di pagamento mediante il browser Web con connessione protetta. 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.

Glossario

VPN (Virtual Private Network) *	La VPN è composta da circuiti virtuali all'interno di una rete più grande, ad esempio Internet, invece di collegamenti diretti mediante fili fisici. Gli end point del "tunnel" della VPN attraverso la rete più grande, realizzato per creare una connessione privata e sicura.
Virus	Malware che replica le copie di se stesso in un altro software o file di dati su un computer "infetto". Al momento della replica, il virus potrebbe eseguire un'operazione dannosa, come l'eliminazione di tutti i dati sul computer. Un virus potrebbe essere silente ed eseguire successivamente un'operazione dannosa o mai innescarla. Un virus che replica se stesso mediante il re-invio di se stesso come allegato a un'email o come parte di un messaggio di rete viene chiamato "worm".
Vulnerabilità *	Punti deboli in un sistema che consentono a un utente non autorizzato di sfruttare quel sistema e violarne l'integrità.
Scansione della vulnerabilità	Uno strumento software che rileva e classifica i potenziali punti deboli (vulnerabilità) su un computer o su una rete. Una scansione potrebbe essere eseguita dal reparto IT di un'organizzazione o da un provider di servizi di sicurezza (come ad esempio un fornitore di scansione approvato). Consultare anche *Fornitore di scansione approvato (ASV)*.
Wi-Fi *	Rete wireless che connette i computer senza un collegamento fisico mediante fili.
Terminale di pagamento wireless	Terminale di pagamento che si connette a Internet utilizzando una qualsiasi delle varie tecnologie wireless.