BANCA D'ITALIA
EUROSISTEMA

DOCUMENTO PER LA CONSULTAZIONE

Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza

Osservazioni potranno essere formulate entro il 12 novembre 2010, trasmettendole a Banca d'Italia, Servizio Supervisione sui Mercati e sul Sistema dei Pagamenti, Divisione Strumenti e Servizi di Pagamento al Dettaglio, via Milano 60/g – 00184 ROMA. Una copia in formato elettronico dovrà essere contestualmente inviata all'indirizzo di posta elettronica smp201@bancaditalia.it
Nel caso in cui si disponga di casella PEC (Posta Elettronica Certificata) e/o di firma digitale le osservazioni potranno essere inviate esclusivamente all'indirizzo smp@pec.bancaditalia.it ; ove si utilizzi tale modalità il documento contenente le osservazioni dovrà essere inviato come allegato al messaggio.

Settembre 2010

1. Premessa

Tutti i prestatori di servizi di pagamento (PSP) sono sottoposti all'obbligo generale di assicurare per gli strumenti di pagamento offerti alla clientela adeguati profili tecnico-organizzativi di sicurezza al fine di garantire in ogni momento il regolare funzionamento del sistema dei pagamenti nonché la fiducia degli utilizzatori nel ricorso ai servizi compresi nel contesto di applicazione del D.lgs 11/2010 (Decreto). La conformità a tale obbligo generale è dettagliata nella Sezione IV del Provvedimento della Banca d'Italia …… [1]
In tale ambito l'utilizzatore di tali strumenti concorre alle perdite derivanti da utilizzi non autorizzati degli strumenti medesimi di cui all'art. 12 del Decreto.

Le disposizioni del presente documento – da emanarsi ai sensi dell'articolo 12, comma 5, del suddetto Provvedimento - individuano le tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza il ricorso ai quali offre maggiori tutele all'utilizzatore: quest'ultimo non concorre infatti nelle perdite derivanti da utilizzi non autorizzati di tali strumenti più sicuri (v. Sezione IV, paragrafo 2.2, del citato Provvedimento).

2. Identificazione degli strumenti

Si considerano strumenti di più elevata qualità sotto il profilo della sicurezza quelli in grado di garantire presidi di sicurezza "rafforzati" specificamente orientati a:

- ridurre le frodi;
- inibire i furti di identità;
- prevenire i fenomeni di riciclaggio e di finanziamento del terrorismo;
- salvaguardare i dati dell'utilizzatore.

Il presente documento definisce i requisiti tecnico-organizzativi che qualificano i presidi di sicurezza "rafforzati". La conformità a tali requisiti di sicurezza specifici deve essere dimostrata attraverso l'*assessment* di una terza parte indipendente, rispetto al soggetto che opera e gestisce i servizi di pagamento offerti agli utilizzatori.

3. Conformità semplificata

Gli strumenti di pagamento che consentono transazioni di importo contenuto per un totale di 100 euro al giorno sono ritenuti a sicurezza intrinseca. Tale requisito è sufficiente, da solo, a ottenere la qualifica di strumento di più elevata qualità sotto il profilo della sicurezza.

4. Conformità estesa

Gli strumenti di pagamento che consentono transazioni per importi superiori al massimale di 100 euro di cui al paragrafo precedente possono essere qualificati a "maggior sicurezza" quando:

[1] Vedi Sez. IV - § 3 "*Obblighi del prestatore di servizi di pagamento in relazione alla prestazione di servizi e all'emissione di strumenti di pagamento*"

1. la presenza e l'efficacia del processo di gestione e mitigazione dei rischi di natura tecnologica siano dimostrate attraverso un rapporto di valutazione emesso da una terza parte indipendente e qualificata (vedi paragrafo successivo). Il processo in oggetto deve obbligatoriamente includere, nella fase di valutazione dei rischi, la sottrazione delle credenziali di autenticazione dai dispositivi dell'utente (es: smart card, token, PC[2], laptop), dai canali di comunicazione (es: attacchi *man-in-the-middle, man-in-the-browser, man-in-the-application*) e dai dispositivi del PSP (server, data storage, etc..)

2. il processo di gestione e mitigazione dei rischi di natura tecnologica preveda *anche* i presidi di sicurezza specifici di seguito elencati:

   a) **Autenticazione a 2 fattori (2FA)**: le metodologie di autenticazione degli utenti si basano su tre "fattori":

   - qualcosa che l'utente conosce (es: password/PIN);
   - qualcosa che l'utente possiede (es: smart card, token, OTP, SIM cellulare);
   - qualcosa che l'utente è (es: caratteristiche biometriche);

   L'autenticazione dell'utente deve avvenire utilizzando due o più fattori di autenticazione; tali fattori di autenticazione devono essere tra loro indipendenti in maniera che la compromissione dell'uno non comprometta anche l'altro fattore. Nel caso di One-Time-Password di tipo time-based, il tempo di validità della singola password non deve superare i 100 secondi. Nella scheda allegata è riportata una descrizione, a mero titolo indicativo, delle modalità di autenticazione prese in considerazione ai fini del presente documento.

   b) **Autenticazione PSP**: lo strumento di pagamento deve essere in grado di autenticare in maniera sicura il dispositivo di pagamento del PSP con il quale interagisce, al fine di evitare che l''utilizzatore consegni le proprie credenziali e i propri dati a dispositivi malevoli (es: autenticazione POS/ATM verso la carta, autenticazione Web server della banca verso il PC dell'utente).

   c) **Transazioni on-line:** per transazioni il cui importo sia superiore a 500 euro, la transazione deve essere sempre autorizzata on-line attraverso il server centrale del PSP.

   d) **Crittografia end-to-end**: la trasmissione delle credenziali di autenticazione dell'utilizzatore nonché dei suoi dati personali, dal proprio device fino al punto di verifica ad opera del PSP, deve essere effettuata attraverso canali con cifratura end-to-end. Nel caso la tecnologia scelta dal PSP richieda che tali dati siano rimessi in chiaro su dispositivi intermedi, ciò deve avvenire all'interno di dispositivi sicuri (es: tamper-resistant module, HSM).

[2] Ci si riferisce in questo caso alla presenza di Virus, worm, key-logger in grado di catturare le credenziali dell'utente monitorando la sua attività.

e) **Autorizzazione singola transazione**: nel caso lo strumento consenta di effettuare più transazioni dispositive nell'ambito della stessa sessione (es: Internet Banking), ogni transazione deve essere autorizzata singolarmente.

f) **Canale *out-of-band***: lo strumento di pagamento deve mettere a disposizione un canale, differente da quello usuale utilizzato per le transazioni, attraverso cui l'utilizzatore viene informato della transazione avvenuta (es: SMS, e-mail, pagine web riservate, etc.). Tale funzionalità deve essere resa disponibile all'utente e attivata a sua discrezione.

g) **Software download/upgrade**: deve essere impedito lo scarico di aggiornamenti software (per lo strumento di pagamento in possesso dell'utilizzatore) via Internet o, in generale, attraverso reti non sicure, a meno che non siano previsti metodi sicuri[3] per la trasmissione del software dal server del PSP al terminale dell'utente.

h) **Apertura e Gestione Conto di pagamento**: in caso di apertura on-line di uno strumento di pagamento nominativo, il PSP garantisce adeguati controlli per minimizzare il rischio che frodatori possano dare false generalità. Meccanismi di autenticazione affidabili e diversi da quelli utilizzati nelle transazioni dispositive, dovrebbero essere usati per le funzionalità di gestione dello strumento di pagamento (es: riemissione PIN/password, variazione indirizzo e generalità utilizzatore, variazione limiti di spesa, etc..). Il PSP garantisce che non sia possibile ottenere le credenziali di autenticazione dell'utilizzatore (sufficienti ad effettuare una transazione) dalla intercettazione delle comunicazioni periodiche tra PSP e utilizzatore (es: estratti conto via posta, e-mail o SMS).

i) **Monitoraggio transazioni inusuali**: il titolare delle funzionalità di pagamento (il PSP o il circuito a cui aderisce) implementa efficaci meccanismi di sicurezza in grado di rilevare tempestivamente transazioni sospette o attività inusuali potenzialmente riconducibili ad attività illecite di frode o riciclaggio. In particolare, i suddetti meccanismi di monitoraggio devono essere in grado di rilevare situazioni come, ad esempio, le seguenti:

- ripetute transazioni di trasferimento fondi sono eseguite entro un ristretto periodo di tempo[4] verso lo stesso beneficiario e per importi prossimi ai massimali consentiti;
- cambio di indirizzo richiesto dell'utente, a cui fa seguito a stretto giro la richiesta di remissione di PIN/password da consegnare attraverso servizio postale;
- innalzamento dei massimali richiesti dall'utente, a cui fa seguito una improvvisa movimentazione di fondi verso controparti inusuali.

In tali casi il PSP verifica prontamente con l'utilizzatore la genuinità di tali transazioni inusuali.

---

[3] Tali metodi di trasmissione dovrebbero assicurare la autenticazione, riservatezza e integrità del frammento software scaricato via rete.

[4] Ci si riferisce a transazioni di movimento fondi, non direttamente riconducibili a sottostanti acquisiti di beni o servizi, che sono generalmente più appetibili in caso di frode.

5. Assessment indipendente

La conformità ai requisiti di sicurezza specifici deve essere dimostrata attraverso lo svolgimento di un *assessment* sul servizio di pagamento. Per lo svolgimento di tale attività i Vertici Aziendali del PSP devono designare un soggetto terzo indipendente e qualificato (*assessor*). L'assessor[5] deve essere in grado di i) dimostrare il necessario *expertise* nel settore per poter eseguire la valutazione; ii) assicurare la necessaria imparzialità, risultando indipendente dai soggetti che sviluppano o operano i servizi di pagamento.

I rapporti di valutazione devono attestare la conformità ai requisiti di sicurezza specifici di cui ai paragrafi precedenti; in particolare: i) l'esistenza di un efficace processo di risk management; ii) l'adeguatezza dei presidi di sicurezza (tra cui quelli specifici) implementati; iii) il numero e la tipologia delle violazioni di sicurezza perpetrate nel periodo di riferimento della analisi.

Il rapporto di valutazione indipendente deve avere almeno i seguenti contenuti:

- *periodo*: deve essere indicato il periodo di riferimento dell'assessment e quali fasi del progetto ha interessato (progettazione, implementazione, testing, messa in produzione, revisione periodica).
- *contesto*: deve essere descritto il perimetro della valutazione effettuata, indicando quali componenti (sistemi, reti, apparati, dispositivi, strutture organizzative) sono state oggetto della valutazione. Tale perimetro deve obbligatoriamente interessare tutte le componenti tecnologiche e organizzative afferenti il servizio di pagamento in oggetto.
- *metodologia*: deve essere indicato l'approccio seguito nel percorso di valutazione (analisi documentale, interviste, test di laboratorio, ispezioni). Il rapporto deve inoltre prevedere specifici approfondimenti sulle aree a maggior rischio (es: *vulnerability assessment* e *penetration test* per i servizi via Internet, test sulla resistenza alla effrazione per i POS, verifica delle caratteristiche di qualità dei Token). Tali approfondimenti possono essere documentati facendo riferimento anche a rapporti di valutazione o certificazioni emessi da altri laboratori (*assessors*) specializzati su specifiche tematiche.
- *oggetto*: deve essere valutata la presenza di un robusto processo di *Risk Management* supportato dal Vertice Aziendale e da un'adeguata struttura organizzativa. Tale processo deve prevedere presidi di sicurezza adeguati rispetto ai rischi da fronteggiare; tali presidi di sicurezza devono obbligatoriamente includere quelli a valenza specifica sopra elencati.

[5] A titolo esemplificativo, l'*Assessor* potrebbe essere un *external auditor*, una Autorità Finanziaria (Sorveglianza/Vigilanza), un Certificatore accreditato ISO 27001.

- *risultati*: devono essere chiaramente esposti i risultati della valutazione, evidenziando le relative implicazioni sulla sicurezza del servizio di pagamento offerto dal PSP; in tale ambito dovrebbero essere stimati i livelli di rischio residuo;
- *raccomandazioni*: devono essere riportate eventuali raccomandazioni del valutatore sviluppate sulla base dei risultati ottenuti e volte a sanare non conformità o aree con livelli di sicurezza sub-ottimali.

Si sottolinea infine che il rapporto di valutazione deve essere: i) rivisto periodicamente in caso di sostanziali variazioni[6]; iii) rivisto in presenza di significativi aggiornamenti della struttura tecnico-organizzativa del servizio di pagamento.

[6] Sostanziali aggiornamenti del rapporto di valutazione potrebbero verificarsi anche in assenza di variazioni della struttura tecnico-organizzativa del circuito di pagamento, ad esempio, in presenza di nuove vulnerabilità derivanti dalla evoluzione tecnologica, dalla individuazione di nuove forme di attacco rilevate (o teorizzate) dai centri di ricerca, da particolari trend registrati nel settore delle frodi.

Fattori di autenticazione

Nella presente scheda sono descritte le principali metodologie utilizzate, secondo le tecnologie allo stato disponibili, nell'implementazione dei fattori di autenticazione.

- *Qualcosa che la persona conosce*: si tratta in elementi informativi condivisi (***shared secrets***) in via esclusiva tra l'utilizzatore e l'entità di autenticazione (in genere il PSP). Password e PIN rappresentano gli esempi più conosciuti, ma altri tipi di segreti condivisi possono essere consentiti dalle moderne tecnologie, quali: i) domande che richiedono la conoscenza dell'utente (importo rata mensile del mutuo); ii) immagini prescelte dall'utente in un gruppo di immagini preselezionate. Tipicamente durante la fase di attivazione del servizio, all'utilizzatore è richiesta la selezione dei codici PIN/Password, la formulazione delle domande con le relative risposte, nonché la selezione delle immagini da riconoscere. Successivamente il PSP mette a disposizione dell'utente le funzionalità per cambiare tali impostazioni su evento o comunque obbligatoriamente entro un certo periodo di tempo prefissato
- *Qualcosa che la persona possiede:* Un primo esempio di fattore di questo tipo è costituito dalla **Smart-card**, vale a dire una carta di pagamento munita di un microprocessore con capacità elaborativa, memoria e funzioni crittografiche. In genere il microchip contiene al suo interno codici che identificano in maniera univoca la card al sistema; la autenticazione della card avviene inserendola in un lettore abilitato, in grado di scambiare con essa i messaggi del protocollo di autenticazione. Se la smart card è riconosciuta (primo fattore di autenticazione), all'utilizzatore è poi richiesto l'inserimento del proprio PIN (secondo fattore) per completare l'autenticazione. In questo ambito sono disponibili protocolli più avanzati che effettuano la autenticazione mediante codici dinamici (diversi da sessione a sessione[7]. Un'altra famiglia di dispositivi adatti a realizzare il fattore di autenticazione in oggetto, sono i cosiddetti TOKEN. I **Token** sono in generale dei dispositivi fisici utilizzati in uno schema di autenticazione a più fattori. Si distingue in genere tra:
    - **USB Token device**: sono dispositivi di piccolo formato collegabili alla porta USB del computer, che contengono al loro interno credenziali di autenticazione, quali certificati digitali di una infrastruttura PKI. Presentano una struttura tamper-resistant e sono difficili da duplicare, per cui si prestano a immagazzinare credenziali di autenticazione. Questo dispositivo viene impiegato in genere insieme a una password/PIN (secondo fattore) in maniera simile a quanto avviene per le smart-card.
    - **Password-Generating Token**: sono dispositivi in grado di generare one-time-password (OTP) e di mostrarle su un piccolo display. Il Token assicura che la stessa OTP non possa essere usata due volte

[7] Un esempio in tal senso è costituito dal protocollodi autenticazione dinamica (DDA) prevista dallo standard EMV, basato su algoritmi di cifratura Asimmetrica (PKI).

consecutivamente, in quanto una nuova OTP è generata dopo poche decine di secondi. Le OTP hanno natura random e non sono predicibili (il valore della OTP nell'istante Tn, non dà indicazioni sul valore della OTP all'istante Tn+1). Generalmente nella fase di autenticazione l'utilizzatore deve inserire il valore OTP prelevato dal Token (primo fattore) insieme a una password impostata in precedenza (secondo fattore).

Appartengono a questa tipologia anche le cosidette non-hardware-OTP, quali le **matrici con codici OTP** forniti all'utente (all'utente è richiesto il valore presente a riga n, colonna m) e le cosiddette **scratch-card.**

- *Qualcosa che la persona è*: le **tecnologie biometriche** indentificano e autenticano la identità di una persona viva sulla base delle caratteristiche fisiche e fisiologiche della stessa. Esempi di tecniche biometriche sono: riconoscimento impronte, della faccia, della voce, geometria della mano, scansione della retina dell'occhio. Nella fase di set-up del sistema, campioni delle grandezze fisiche/fisiologiche sono registrati e ricondotti a un *template* di risconoscimento (fase di *enrollment*); nelle fasi di autenticazione, il valore biometrico rilevato sulla persona viene confrontato con il template memorizzato dal sistema in fase di enrollment. Come negli altri casi, le tecnologie biometriche sono in genere combinate con password o Token, per realizzare sistemi di autenticazione a più fattori.