Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'economia DFE

Segreteria di Stato dell'economia SECO
Comunicazione

Documentazione stampa sulla SuisseID

Data 13 gennaio 2011

Lavori svolti nel 2010 dal gruppo di esperti per la sicurezza

Contesto

Sotto la direzione della Segreteria di Stato dell'economia SECO, i fornitori di servizi di certificazione riconosciuti a norma di legge in Svizzera hanno elaborato, insieme a rappresentanti del settore informatico, lo standard industriale per la prova elettronica dell'identità SuisseID. Questo standard è garante di una firma elettronica giuridicamente vincolante come pure di un'autentificazione sicura. Dal maggio 2010, la SuisseID è ottenibile sotto forma di tesserino elettronico (carta chip) o di chiavetta USB ed è dotata di certificati digitali per l'autenticazione (IAC)[1] e la firma qualificata (QC)[2].

Lavori del gruppo di esperti

Nel settembre 2010, la SECO ha istituito un gruppo di esperti incaricato di avanzare proposte su come ridurre i rischi legati all'uso delle cosiddette «smartcard». Nell'ambito di una perizia è stata esaminata la sicurezza tecnica della SuisseID. A tal riguardo è stato analizzato l'intero ventaglio di prestazioni della SuisseID sotto il profilo del suo potenziale di vulnerabilità (dall'utente all'applicazione server, passando per il certificato, il lettore chip-card e il PC client). Inoltre, nel novembre 2010 la SECO ha svolto un workshop finalizzato a tematizzare vari aspetti legati alla sicurezza della SuisseID. Vi hanno partecipato 35 esperti provenienti dagli ambienti dell'economia, della ricerca, dell'insegnamento e dell'Amministrazione. Nel corso di questi lavori sono state elaborate le avvertenze di sicurezza seguenti.

Avvertenze di sicurezza

Alla luce del fatto che negli ambienti informatici di rete – e quindi anche nelle transazioni online in cui può essere implicato un intermediario o una controparte qualunque – non esiste la sicurezza assoluta, è importante capire che l'affidabilità della SuisseID dipende da numerosi fattori, come ad esempio dallo scopo d'impiego o dall'attrattiva (in termini di lucro)

---

[1] Identification and Authetication Certificate

[2] Qualified Certificate

che un determinato obiettivo d'attacco può esercitare su potenziali hacker. Per evincere un quadro chiaro di quali siano le misure di sicurezza appropriate, occorre considerare, caso per caso, i rischi e gli effetti legati all'impiego della SuisseID. Dato che si tratta per lo più di grandezze dipendenti dall'utilizzo, le avvertenze di sicurezza generali sono da intendersi unicamente come guida, in quanto non possono sostituire un'analisi individuale né una valutazione dei rischi e delle contromisure più indicate.

Le seguenti avvertenze di sicurezza partono dal presupposto che il computer di un utente SuisseID può presentare, in via di principio, falle di sicurezza causate da software nocivi («malware») programmati al fine di comprometterlo e di abusarne.

Avvertenze di carattere generale – La SuisseID dev'essere utilizzata alla stregua di qualsiasi altro sistema di accesso elettronico (p. es. la carta bancaria). Essa va conservata in un luogo sicuro e non va mai lasciata incustodita. Il codice PIN segreto non dev'essere trasmesso a terzi né annotato (tanto meno sulla carta stessa). Se la SuisseID venisse danneggiata o persa, occorre revocarla immediatamente, ossia farla dichiarare invalida. In una tale eventualità, la procedura da seguire è descritta sul sito Internet del relativo fornitore SuisseID nonché nella documentazione consegnata al titolare al momento dell'acquisto.

Avvertenze concernenti il lettore chip-card – In molti Paesi vengono utilizzati, per la firma e l'autenticazione, lettori chip-card nei quali il PIN viene inserito attraverso la tastiera del computer (lettori classe 1). È fuori discussione che questi lettori sono più vulnerabili agli attacchi degli hacker che non i lettori di classe superiore, quali quelli dotati di PIN-Pad e/o di display. Per contro, quelli di classe 1 sono più semplici da utilizzare. Gli utenti con esigenze di sicurezza superiori possono acquistare lettori chip-card più evoluti presso il loro fornitore SuisseID.

Avvertenze concernenti la firma elettronica – Le firme elettroniche che la SuisseID consente di effettuare sono già in uso in numerosi Paesi. Una volta sottoscritto, un documento elettronico è al sicuro da alterazioni nascoste e da falsificazioni di firma. Una firma elettronica dovrebbe essere effettuata unicamente se l'apposito software è fornito da un'impresa affidabile e se risulta chiaro al firmatario quali sono i termini che sta per accettare. Inoltre, il software di firma deve mostrare tutti i contenuti, senza reprimere alcunché. In particolare, esso non deve accettare contenuti dinamici. La sicurezza del software di firma dipende dalla sicurezza del computer su cui viene installato e reso operativo. Se vi è il sospetto che il computer sia stato compromesso, la SuisseID non deve più essere impiegata, né come strumento di firma né per l'autenticazione (login).

Avvertenze sul formato dei dati per la firma - In via di principio ogni documento elettronico può essere firmato mediante la SuisseID in modo giuridicamente vincolante. A tal proposito la legge sulla firma elettronica non prevede alcuna limitazione. Oltre ad essere un formato diffuso e idoneo, il PDF/A è l'unico ad essere accettato dalle autorità per l'immissione elettronica. Vi sono numerosi strumenti per apporre e valutare la firma su documenti PDF. Dato che l'affidabilità di tali strumenti dipende anch'essa da quella del computer, in questo caso vale lo stesso discorso di cui sopra: se vi è il sospetto che il computer sia stato compromesso, la SuisseID non deve più essere impiegata, né come strumento di firma né per l'autenticazione (login).

Avvertenze concernenti la protezione da virus – La SuisseID non può essere danneggiata da software nocivi, ma l'ambiente informatico in cui viene impiegata sì. Rientra nella responsabilità dell'utente applicare le dovute misure precauzionali a tutela del suo computer. Tra queste figurano, in particolare, l'utilizzo di programmi antivirus e anti-spyware nonché l'esecuzione a scadenza regolare di update di sicurezza per il sistema operativo, i software e i dati. Queste misure garantiscono una protezione di base capace di vanificare la maggior parte degli attacchi usuali.

Avvertenze concernenti l'accesso a siti Internet - Il principio di funzionamento del login mediante SuisseID è giudicato molto sicuro e rappresenta un notevole passo in avanti rispetto al login mediante nome-utente e password. Un possibile pericolo, tuttavia, potrebbe derivare dal sito Internet a cui si accede. La SuisseID dovrebbe essere impiegata unicamente su siti affidabili. Non esiste al momento alcun marchio di qualità per i siti che supportano la SuisseID (il logo «SuisseID LOGIN» è unicamente un elemento di creazione di identità). I siti Internet con certificati server complessi – riconoscibili in molti browser dal colore verde dell'URL – sono reputati seri e affidabili, in particolare perché l'identità dei responsabili è nota e confermata. Anche qui, tuttavia, vale la regola di cui sopra: se vi è il sospetto che il computer sia stato compromesso, la SuisseID non deve più essere impiegata, né come strumento di firma né per l'autenticazione (login).

Prospettive

Anche in futuro la SECO intende proseguire il dialogo con gli esperti in materia di sicurezza. Essa si impegnerà attivamente a favore di una riduzione dei rischi connessi all'impiego delle tecnologie informatiche, motivo per cui ha fatto della sicurezza una priorità assoluta a cui subordinare le sue attività di economia elettronica.

Inoltre, all'interno dell'Associazione SuisseID è stato istituito un gruppo di lavoro addetto alla sicurezza. I risultati della perizia 2010 saranno utilizzati in tale sede e, quest'anno, il suddetto gruppo orienterà il suo operato in base ad essi.

Per ulteriori informazioni sulla SuisseID rimandiamo al sito: www.suisseid.ch.