INFORMATION SECURITY

11

La Rivista dell'ICT per la Sicurezza

PRIMO PIANO
Quando le tecnologie si incontrano: le nuove frontiere della videosorveglianza

SPECIALE
Il Rapporto ID Security

SOTTO LA LENTE
Affrontare con successo la sfida delle tre C: Bludis, Kaspersky e i partner ti indicano la strada

SCENARI
Commenti allo schema normativo relativo alla firma elettronica avanzata (FEA)

Edisef s.r.l. ROC n°12983 ISSN 2037 - 2811
Publist mensile registrata presso il Tribunale di Roma il 7/10/2010 n°370 Poste Italiane S.p.A.
Spedizione in abbonamento postale - 70% Roma Aut. n. C /RM/103/2010

Come le mie informazioni personali divennero bit

Uno sguardo ai sistemi di gestione delle identità digitali

Marco Caselli
GCSEC

Nella nostra vita quotidiana siamo abituati a presentare documenti d'identità in banche o uffici pubblici per usufruire di numerosi servizi. Questo semplice gesto permette che i nostri interlocutori siano certi che siamo chi diciamo di essere e, allo stesso tempo, che le informazioni personali che stiamo fornendo siano in qualche modo confermate.

Allo stesso modo, considerando il vasto insieme di servizi già migrati su Internet, stiamo oggi affrontando la sfida di condividere queste informazioni anche nel "virtuale". Di recente l'interesse intorno a quest'argomento è cresciuto notevolmente ed il concetto di un'identità digitale (ID), intesa come una sorta di documento virtuale, sta iniziando a prendere forma.

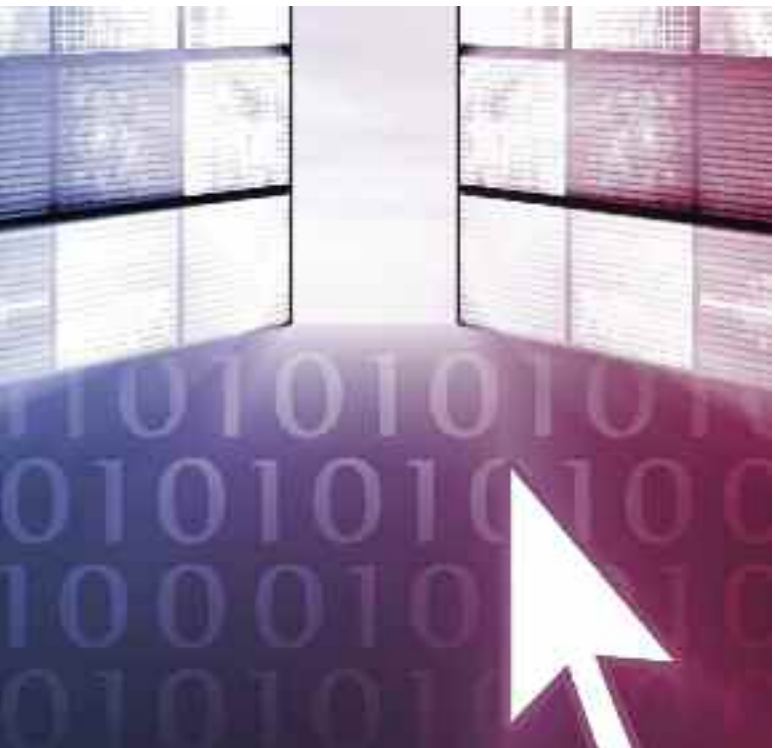
Non esiste ancora una definizione comune ma, nella pratica, possiamo intendere un'identità digitale come l'insieme d'informazioni che l'utente decide di condividere con un sistema IT per accedere a determinati servizi web. Sembra semplice, ma oggigiorno siamo costretti a confrontarci con molteplici ID quasi contemporaneamente. Pensiamo per un secondo a quanti servizi web utilizziamo ogni giorno. Accedere alla propria casella di posta, all'account bancario, ai portali per l'e-commerce ed ai social network sono solo alcune delle operazioni che richiedono ad un utente di loggarsi e fornire le proprie informazioni personali, ogni volta con regole e livelli di sicurezza diversi. Oltretutto, viene spesso richiesto ad una persona di inserire gli stessi dati (nome, cognome, data di nascita, ecc.). Questi pochi elementi già ci conducono ad una considerazione generale: è possibile

gestire questi account coerentemente, in maniera sicura ed evitando il diffondersi di informazioni duplicate?

L'attuale necessità di un sistema di gestione delle identità digitali sta spingendo gli sviluppatori a progettare soluzioni semplici ma sicure con l'obiettivo di riempire questa fetta del mercato IT.

OpenID è stato probabilmente il primo tentativo concreto di risolvere la situazione. Questa infrastruttura, progettata nel 2005, propone un sistema per l'autenticazione decentralizzata degli utenti. L'idea chiave è lasciare che l'utente scelga liberamente un provider OpenID per salvare le informazioni personali e che, quest'ultimo, assegni a lui/lei un identificatore specifico (ad esempio uno URL) con cui accedere ad esse. Attraverso questo identificatore l'utente potrà utilizzare qualsiasi web service OpenID-compliant lasciando che sia il provider ad occuparsi dell'autenticazione e della condivisione delle informazioni e facendo dunque a meno di molteplici username e password. La soluzione è ampiamente diffusa su Internet ma a volte gli utenti hanno contestato l'utilizzo di un identificatore così poco user-friendly. Collegare la nostra identità ad uno URL generico può, in effetti, sembrare strano e soluzioni più recenti stanno cercando di eliminare tale ambiguità.

Questo è il caso di BrowserID. La soluzione proposta da Mozilla usa, infatti, indirizzi email invece di generici identificatori e, paragonata ad OpenID, pone maggiore attenzione alle questioni di privacy. Nel protocollo di comunicazione di OpenID descritto in precedenza i repository di ID ed i web service condividono direttamente le informazioni dell'utente. Ciò significa che, i primi conoscono tutto ciò che l'utente fa con le sue informazioni. Dato che questo è un chiaro problema dal punto di vista della privacy BrowserID cambia radicalmente il modo in cui tali informazioni vengono scambiate assegnando maggior importanza alla figura dell'utente. Il processo di autenticazione di BrowserID consiste nel condividere un certificato digitale firmato in cui il provider d'identità asserisca che quelle informazioni appartengano davvero all'utente. Questo certificato è gestito dal browser dell'utente stesso e viene fornito a qualsiasi web service BrowserID-compliant per effettuare il login. Nessun'altra comunicazione è richiesta ed, in questo modo, gli utenti sono sicuri di essere i soli a poter tenere traccia dei servizi utilizzati. L'idea potrebbe essere di successo ma l'implementazione dell'infrastruttura è ancora in fase embrionale.



OneID cerca di fare un ulteriore passo in avanti proponendo uno schema che consenta agli utenti di essere gli unici a conoscere l'intero set di informazioni contenute nel repository. Il concetto alla base di OneID è semplice ma innovativo: è possibile crittare le informazioni prima di mandarle ai provider di ID e decrittare i dati localmente qualora ve ne fosse bisogno. Come nel caso di BrowserID siamo sempre in controllo dei flussi di comunicazione, ma nessuno eccetto il web service dovrà sapere nulla di noi. Un'altra importante caratteristica di OneID riguarda il collegamento dell'identità digitale non più ad un identificatore ma a dei device. PC, cellulari, tablet diventano dunque le chiavi di accesso per le nostre informazioni digitali. Quando faremo un login al nostro repository di ID l'infrastruttura riconoscerà il nostro device e manderà automaticamente ad esso i dati relativi. Da una prospettiva legata unicamente alla privacy il sistema può essere senz'altro conveniente ma OneID dipende sempre dalla disponibilità dei device e ciò a volte potrebbe non essere pratico.

È importante notare come nessuna delle precedenti sia "la" soluzione. Ognuna di esse propone un modo sicuro per gestire le informazioni concentrandosi su processi di autenticazione e data-sharing differenti. Come già accennato, gli utenti vogliono essere gli unici a poter leggere le informazioni personali ma forse i web service vogliono maggiori garanzie sui dati che ricevono. Questa garanzia può nascere dal parlare direttamente con i repository d'identità che, a loro volta, hanno tutto l'interesse nel monitorare ciò che gli utenti fanno. Non c'è ancora alcuna risposta concreta, ma le cose si muovono velocemente. Oggi ci poniamo il problema di scrivere il nostro numero di telefono su Internet ma, con ogni probabilità, un domani considereremo i sistemi di gestione delle identità digitali sicuri abbastanza da consegnare loro i nostri più reconditi segreti.

Una, nessuna, centomila identità digitali

La sicurezza dell'identità digitale richiede un'analisi approfondita e multidisciplinare che deve produrre risultati importanti sia per chi possiede delle identità digitali (e che quindi vuole garanzie sulla riservatezza dei dati che costituiscono la propria identità digitale e sul loro corretto utilizzo), sia per chi le identità digitali le gestisce (al fine di fornire servizi che gestiscano correttamente le informazioni relative ai proprietari delle identità digitali).

Maria Luisa Papagni
Almaviva/GCSEC

Quello dell'identità digitale è un tema molto attuale, che apre diversi scenari suscitando l'interesse di esperti del settore ma anche di semplici utenti. Infatti, in seguito ai moltissimi casi di furto di identità e di frode che hanno colpito tutto il mondo digitale (vedi il caso della Sony PSP nel 2011), è maturata la consapevolezza che il tema è tra i più delicati e gli utenti hanno cominciato a realizzare che la sicurezza delle loro identità digitali è estremamente importante.

La sicurezza dell'identità digitale richiede un'analisi approfondita e multidisciplinare che deve produrre risultati importanti sia per chi possiede delle identità digitali (e che quindi vuole garanzie sulla riservatezza dei dati che costituiscono la propria identità digitale e sul loro corretto utilizzo), sia per chi le identità digitali le gestisce (al fine di fornire servizi che gestiscano correttamente le informazioni relative ai proprietari delle identità digitali).

Innanzitutto è importante fare chiarezza su alcuni concetti che possono fin dall'inizio originare confusione. La definizione stessa di identità digitale non è ancora comunemente riconosciuta. Una prima definizione è stata fornita da HalAbelsone Lowrence Lessig del MIT nel whitepaper "*Digital Idenity in Cyber Space*": "L' insieme delle caratteristiche essenziali ed uniche di un soggetto che permettono di identificarlo". Già questa semplice definizione nasconde concetti molto complessi legati all'identificazione di quegli aspetti che possono essere considerati come

unici ed essenziali.

Si parla di identità digitale quando si accede ad una qualsiasi piattaforma social, quando si utilizzano servizi e-banking, quando si acquistano dei prodotti on-line o si accede a qualsiasi altro servizio dove, per autenticarsi, sono richieste almeno due classi di informazioni:

- identità (chi sei)
- alcuni attributi di questa identità.

E' ormai possibile affermare con discreta certezza che la maggioranza dei cittadini dei paesi industrializzati possiede almeno un'identità digitale: profilo di Facebook, e-passaport, PayPal, numero di conti bancari o account di Amazon, sono tutti esempi di identità digitali.

Il fatto che una singola persona possa essere il proprietario di diverse identità digitali aggiunge un ulteriore livello di complessità. Il concetto di molteplici identità digitali è chiarito nel documento "Managing multiple electronic identities" dell'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione (ENISA) della Commissione Europea: ad ogni entità fisica può essere associata una serie di diverse identità, non necessariamente con la stesse credenziali, e non necessariamente gestite dallo stesso provider. Una persona può scegliere di interagire con un'altra persona come individuo, attraverso uno pseudonimo, in quanto dipendente di una società e così via, a seconda dei casi. Una metafora esprime chiaramente il concetto: un soggetto che possiede più identità digitali può essere confrontato ad una persona con molte carte di credito diverse, una per ogni identità.

Inoltre, ENISA fa una classificazione delle identità digitali secondo due fattori:

- Livello di affidabilità, determinato sulla base dell'indagine che è stata eseguita sul proprietario di un'identità digitale e delle credenziali associate da parte di un'autorità di registrazione. Questo valore è compreso tra "basso" (nessun controllo) a "molto alto" (controllo *de visu*);
- Livello di robustezza dell'autenticazione, che rappresenta la qualità dell'associazione tra un'entità e la relativa identità. Diverse tecnologie vengono utilizzate per effettuare l'autenticazione, come password, token, chip o dispositivi biometrici.

Comunque l'obiettivo di ENISA non è solo quello di identificare e descrivere i diversi tipi di identità digitali e le tecniche generali per la loro gestione. Il progetto fa parte della politica promossa dalla Commissione Europea sul "digital inclusion", che significa diffondere le nuove tecnologie tra le popolazioni di ogni Paese, in modo che le persone possano beneficiarne. In questo paper, ENISA vuole promuovere la digitalizzazione delle identità al fine di consentire sia agli utenti che ai fornitori di beneficiare di servizi on-line sicuri, affidabili e di semplice utilizzo. La crescita del commercio elettronico e dell'e-business e l'attuazione delle procedure amministrative online nel mercato unico sono i temi chiave che hanno portato anche alla creazione dell'Agenda Digitale per l'Europa.

L'Agenda Digitale Europea è stato lanciata il 19 maggio 2010 dalla Commissione Europea e costituisce la strategia per diffondere l'ICT e per sfruttare i vantaggi di un mercato unico digitale per famiglie ed imprese. Questo programma è uno dei "progetti faro" d'Europa 2020.

La sezione 2.1.2 dell'Agenda Digitale Europea fa esplicito riferimento alle identità digitali: "Le tecnologie relative all'identità elettronica e i servizi di autenticazione sono indispensabili per le transazioni su internet, sia nel settore privato che in quello pubblico. [...] Le possibilità saranno numerose, perciò il settore, sostenuto da iniziative a livello di politiche, in particolare per quanto riguarda i servizi di "e-Government" (pubblica amministrazione online), deve assicurare l'interoperabilità sulla base di standard e piattaforme di sviluppo aperte".

L'Agenda Digitale Europea mira a combattere la mancanza di fiducia da parte dei cittadini europei, che tendono a diffidare da attività on-line, a meno che non sentano di poter operare ad alti livelli di sicurezza

Relativamente al tema dell'identità digitale, l'Agenda Digitale si focalizza su:

- Tecnologie relative alle identità elettroniche ed ai servizi di autenticazione;
- Crimini informatici, compresi furti di identità e frodi;
- Proposta di revisione della direttiva sulla firma elettronica, al fine di istituire un quadro normativo per il riconoscimento e l'interoperabilità transfrontalieri di sistemi di autenticazione elettronica sicuri.

L'Agenda Digitale Europea mira a combattere la mancanza di fiducia da parte dei cittadini europei, che tendono a diffidare da attività on-line, a meno che non sentano di poter operare ad alti livelli di sicurezza. L'Agenda Digitale esprime la necessità di sviluppare meccanismi per rispondere alle nuove forme di criminalità informatica. La sicurezza dell'identità digitale è parte integrante di questo progetto.

Uno dei paesi che più velocemente sta attuando i principi dell'Agenda Digitale Europea è l'Estonia. Infatti, proprio in Estonia, si è registrato un uso diffuso della carta di identità elettronica (quasi tutti gli abitanti la posseggono). La carta d'identità elettronica viene utilizzato in Estonia per molti servizi on-line come le transazioni bancarie, l'acquisto di biglietti e persino il voto elettronico.

L'Estonia è infatti uno dei pochi paesi al mondo dove si può votare on-line. Dal 2005 i cittadini estoni hanno avuto la possibilità di usufruire di questo servizio e alle ultime elezioni europee una buona percentuale della popolazione ha preferito questa modalità, aumentando anche notevolmente il tasso di partecipazione.

Dall'altra parte dell'oceano Atlantico, anche il governo americano sta lavorando sul tema dell'identità digitale al fine di mitigare i rischi connessi alla sicurezza e alla privacy. Il progetto più importante, coordinato dal Dipartimento della Difesa (DoD), si chiama "The National Strategy for Trusted Identities in Cyberspace" (NSTIC). L'obiettivo è quello di permettere alle persone di certificare in modo sicuro la loro identità, attraverso la minima divulgazione dei propri dati sensibili, quando effettuano operazioni (come ad esempio e-banking) e, al tempo stesso, mantenere l'anonimato quando, ad esempio, scrivono nei blog.

La strategia promuove un ecosistema delle identità, "un ambiente on-line in cui individui, organizzazioni, servizi e dispositivi possono fidarsi l'uno dell'altro, perché fonti autorevoli stabiliscono e autenticano la loro identità digitali".

NSTIC ha quattro principi guida che specificano quali sono le caratteristiche essenziali delle soluzioni che supportano le identità nel Cyberspace:

- Sicurezza e resilienza – le soluzioni che supportano le identità dovrebbero essere sicure, (garantendo riservatezza, integrità e disponibilità), e resilienti (in grado di recuperare e di adattarsi al cambiamento drastico e repentino).
- Interoperabilità – l'interoperabilità supporta la portabilità dell'identità, consentendo agli individui di beneficiare dell'uso delle loro credenziali sicure in vari fornitori di servizi.
- Riservatezza e volontarietà – Le soluzioni dovrebbero non solo migliorare la sicurezza, ma porre anche una particolare attenzione ai dati personali. Inoltre questo principio esprime un altro concetto semplice: la partecipazione all'ecosistema delle identità sarà del tutto volontaria. Le organizzazioni non sono costrette ad adottare soluzioni di identità specifiche, né gli individui sono costretti a ottenere credenziali sicure. L'impegno nelle transazioni on-line dovrebbe essere volontario da parte di entrambi.
- Convenienza e facilità d'uso - le soluzioni devono essere semplici, intuitive, facili da usare; dovrebbero promuovere l'efficienza operativa e ridurre al minimo i costi di implementazione, aumentando così il potenziale ritorno sull'investimento.

NSTIC è una strategia ambiziosa, ma essenziale! Ogni paese dovrebbe muoversi in questa direzione perché, citando Barak Obama: "Questo mondo, il cyberspace, è un mondo da cui noi dipendiamo ogni singolo giorno ... ci ha reso più interconnessi di quanto lo siamo mai stati in un qualsiasi altro momento della storia umana ". Pertanto, oggi più che mai, vi è la necessità di disporre di identità digitali sicure.