Titolo della proposta

I-AM – Identity Authentication Model

1 Nomi dei proponenti

Andrea Caccia (a.caccia@kworks.it), Vito Umberto Vavalli (v.u.vavalli@kworks.it)

2 Pillar di riferimento

La proposta si inserisce direttamente nell'ambito del Pillar 1 (Mercato Unico Digitale) trattandosi di una tecnologia di gestione delle identità a supporto di un modello di autenticazione innovativo.
Leggiamo infatti al §2.1.2 "Semplificare le transazioni online e transfrontaliere" della Comunicazione della Commissione Europea sull'Agenda Digitale [1] "*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. La modalità di autenticazione più diffusa oggi, ossia l'uso di password, può essere sufficiente per molte applicazioni, ma si rendono progressivamente necessarie soluzioni più sicure*".
In questo ambito è prevista la "Azione fondamentale 3: nel 2011 proporre una 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**."
La proposta oggetto di questo documento riguarda un modello di autenticazione più forte dell'uso di password, pur mantenendone la versatilità, e che si pone l'obiettivo di rimediare al proliferare di password che l'utilizzatore finale dei servizi on line si trova a dover gestire.
Si basa, ove possibile, su standard aperti Europei ed internazionali (cfr Libro Bianco sulla standardizzazione ICT della Commissione Europea [2]) che possono contribuire all'attività di standardizzazione tecnica che scaturiranno dalla revisione della direttiva sulla firma elettronica già menzionata e che rientrano nel Pillar 2 (Interoperabilità e standard).
Infine la proposta rientra nel Pillar 3 (Fiducia e sicurezza) ponendosi l'obiettivo di rafforzare la sicurezza nell'accesso ai servizi on line nel rispetto della normativa sulla privacy.

3 Individuazione e analisi di bisogni e requisiti

Il modello di autenticazione proposto si pone l'obiettivo di soddisfare il bisogno sempre più diffuso di accedere ai servizi on line rispettando i requisiti di usabilità, sicurezza e privacy.
L'utilizzatore di servizi on-line si trova a dover gestire decine di credenziali, ognuna con regole di produzione e tempi di scadenza propri. La situazione, all'aumentare dei servizi offerti è destinata a peggiorare.
Il modello I-AM si pone l'obiettivo da un lato di eliminare le cause di antipatici disservizi (servizi bloccati, mancati accessi, ...) e dall'altro di superare i comportamenti poco sicuri (userid e password scritte o salvate su file, spesso banali e ripetute, ...) derivanti da un complesso di soluzioni che singolarmente dovrebbero proteggere l'identità dell'utilizzatore ma che nella pratica tendono ad abbassare la sicurezza complessiva.
Il modello proposto adotta un meccanismo di autenticazione basato su password usa e getta (One time Password – OTP) basato su applicazioni residenti su smartphone incrementando così la sicurezza della singola transazione. L'uso di un unico strumento elimina i problemi causati dalla gestione di numerose credenziali e la corrispondenza persona-identità minimizza i rischi derivanti da impersonificazione e furto di identità.
Il modello prevede inoltre che i propri dati siano gestiti da un circuito di fornitori di servizi di trust che rispetta un insieme di regole condivise e verificabili, in linea con l'attuale rete di trust europea basata sulle "Trust List" già implementate da tutti gli Stati Membri europei nell'ambito della direttiva sulla firma

elettronica e consente all'utilizzatore di decidere quale delle proprie informazioni personali siano rese disponibili al fornitore di servizi on-line. In ogni caso, l'identificazione certa, anche se in forma anonima verso il fornitore di servizi, renderebbe possibile un maggiore controllo dell'accesso ad internet da parte dei minori ed un forte deterrente ad abusi che vengono coperti dalla difficoltà da parte delle autorità ad identificare gli autori degli stessi.
I-AM/OTP capovolge il modello secondo il quale è il fornitore di servizi a imporre all'utente il meccanismo di autenticazione basandolo su specifiche credenziali e consente di sostituire ad esse un unico strumento di identificazione per tutti i canali e le piattaforme di utilizzo.

4 Considerazioni e osservazioni

I-AM garantisce la rigorosa associazione tra la persona e la sua credenziale digitale sfruttando una credenziale frutto dell'identificazione operata da una Pubblica Amministrazione Europea.
Il progetto STORK (https://www.eid-stork.eu) sta istituito una piattaforma per l'interoperabilità dei dispositivi di identità elettronici in Europa. In Italia, ad esempio, è possibile utilizzare una Carta d'Identità Elettronica o una Carta Nazionale dei Servizi per la quale è stato rilasciato il PIN o un dispositivo di firma digitale. Essendo l'autenticazione basata su smartphone, è ipotizzabile anche l'utilizzo di SIM telefoniche, previa definizione delle necessarie procedure di produzione ed accesso alle SIM da parte dei terminali telefonici.
I-AM è un' iniziativa OPEN, che contempla la pubblicazione del codice sviluppato dai soggetti partecipanti al progetto e l'uso gratuito di detto codice.
In aggiunta ai tradizionali canoni dell'Open Source, I-AM aggiunge un livello di interoperabilità ulteriore quale condizione imprescindibile per l'uso gratuito del software: gli utilizzatori intermedi e finali dovranno operare come "Open Community" a salvaguardia dei valori condivisi alla base dell'operare in rete mediante credenziali di identità digitale. Specificamente, ogni attore, consapevole del fatto che la modalità sicura e veloce offerta dal modello I-AM per l'esercizio del diritto di riconoscere l'identità è un valore fondativo della comunità a cui si partecipa e che la condivisione della Rete richiede la mutua collaborazione e il rispetto di regole costitutive dei commons, adotta le norme tecniche e di comportamento definite in piena libertà come parte integrante dell'iniziativa.
In particolare:

- l'Organizzazione che fornisce i servizi si assume le responsabilità caratteristiche del proprio ruolo davanti all'intera comunità, garantendo il principi di tracciabilità e trasparenza, necessari a preservare la sicurezza di ogni credenziale creata e del suo utilizzo all'interno del circuito;
- l'utilizzatore adotta le regole di comportamento atte a presidiare la creazione e l'uso delle credenziali e, quando sceglie di utilizzarle, accetta le clausole contrattuali che ne disciplinano il valore di elemento contrattualmente rilevante entro la comunità degli operatori che hanno espresso formalmente l'accettazione del'OTP generato dalla routine I-AM quale credenziale.

5 Risultato che si intende ottenere

Il risultato che si vuole ottenere è l'ottenimento di benefici per tutti gli attori coinvolti:

- Gli utilizzatori finali, che possono avere un miglioramento della user experience nell'uso dei servizi on line anche in mobilità, non dovendo gestire decine di credenziali e ottenendo un servizio più sicuro;
- I fornitori di servizio, che possono accedere ad una tecnologia di autenticazione più efficiente ed economica, che risolve anche il problema dell'identificazione, fonte delle maggiori criticità e costi;
- I fornitori di servizi di trust, con la possibilità di ampliare la propria offerta

6 Descrizione proposta di iniziativa regolamentare e/o legislativa

La proposta si inserisce nell'attuale framework delle firme elettroniche definito dalla direttiva 1999/93/CE, che è necessario integrare per tener conto dei sistemi di autenticazione elettronica, attività peraltro già prevista nell'ambito delle azioni della Commissione Europea relative all'Agenda Digitale.
È inoltre necessario integrare gli attuali standard sulla firma elettronica per tener conto delle specifiche esigenze dell'autenticazione informatica. Si tratta soprattutto di portare a livello di standard europei

specifiche in gran parte già esistenti a livello internazionale; questa attività può sicuramente essere svolta dagli enti di standardizzazione europea nell'ambito degli usuali mandati comunitari.
Non si rilevano comunque ostacoli significativi alla realizzazione della proposta nell'ambito della normativa esistente. In Italia, ad esempio, il Codice dell'Amministrazione Digitale come modificato dal D. Lgs. 235/2010 già entrato in vigore fornisce già gli strumenti necessari per garantire la base legale necessaria, grazie agli strumenti di accertamento, accreditamento e vigilanza previsti da parte di OCSI e DigitPA.

7 Riferimenti

[1] Comunicazione della Commissione Europea COM(2010) 245 del 26.8.2010 "Un'agenda digitale europea"
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:IT:PDF

[2] Comunicazione della Commissione Europea COM(2009) 324 del 3.7.2009 "Libro bianco - Ammodernamento della normalizzazione delle tecnologie dell'informazione e della comunicazione nell'UE – Prospettive"
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0324:FIN:IT:PDF