

I testi sono stati redatti da:
Domenico Lucà, CSI-Piemonte
Flavio Piovesan, CSI-Piemonte
Ferdinando Ricchiuti, CSP

Hanno collaborato alla organizzazione e redazione della pubblicazione:
Franco Gola, CSI-Piemonte
Sergio Duretti, CSP

Si ringraziano per la revisione finale del testo e i preziosi suggerimenti forniti i Proff. Francesco Bergadano dell'Università di Torino e Anna Vaccarelli dell'Istituto di Informatica e Telematica del CNR di Pisa e Alessandro Sala del CSI-Piemonte.

Si ringraziano i rappresentanti del Consiglio Direttivo dell'Associazione per il contributo fornito nell'ideazione della pubblicazione.

I contenuti della pubblicazione sono soggetti a licenza
Creative Commons Italia, Attribuzione - Non commerciale – Non opere derivate,
il cui contenuto integrale è riportato all'indirizzo
<http://creativecommons.org/licenses/by-nc-nd/2.0/it/deed.it>

**LA GESTIONE
DELL'IDENTITÀ DIGITALE**

Problemi ed opportunità

SOMMARIO

1. Introduzione.....	6
1.1 Cos'è l'identità digitale	6
1.2 La forza di una identità digitale	7
1.3 Identità digitale e anonimato	7
1.4 La relazione con il mondo reale	8
2. Il contesto socio-economico.....	10
2.1 La dimensione economica	10
2.2 La dimensione sociale e culturale	12
3. Il contesto giuridico	15
3.1 La firma elettronica	15
3.1.1 Il valore legale delle firme elettroniche	17
3.1.2 I riferimenti normativi	18
3.1.3 La situazione internazionale.....	18
3.2 Il diritto d'autore - DRM (Digital Rights Management)	19
3.2.1 Il quadro normativo italiano.....	19
3.2.2 Il quadro normativo europeo	20
3.2.2.1 European Union Copyright Directive (EUCD).....	20
3.2.2.2 Intellectual Property Rights Enforcement Directive (IPRED).....	22
4. Il contesto tecnologico.....	23
4.1 La necessità dell'identity management	23
4.2 La terminologia e i concetti di base	24
4.2.1 Meta-directory	24
4.2.2 Provisioning	25
4.2.3 Gestione delegata.....	25
4.2.4 Sistemi federati.....	26
4.3 L'autenticazione e le credenziali	27
4.3.1 Password	27
4.3.1.1 Password usa e getta	28
4.3.2 I sistemi a sfida.....	29
4.3.3 I certificati a chiave pubblica.....	30
4.3.4 Le smart card e i token USB	31
4.3.5 La biometria	32
4.4 L'autorizzazione	33
4.4.1 Il Discretionary Access Control (DAC).....	33
4.4.2 Il Mandatory Access Control (MAC).....	34
4.4.3 Il Role Based Access Control (RBAC).....	34
5. Lo scenario internazionale.....	36
5.1 L'evoluzione del mercato	36
5.1.1 Computer Associates	36
5.1.2 SUN Microsystem	37
5.1.3 Microsoft: da Passport A MIIS 2003.....	37
5.1.4 Oracle.....	37
5.1.5 IBM.....	38
5.1.6 Cisco	38
5.1.7 Critical Path.....	39
5.2 I principali progetti e iniziative	39
5.2.1 Liberty Alliance.....	39

5.2.2	Microsoft .NET Passport	41
5.2.3	PingID Identity Network.....	42
5.2.4	Digital ID World.....	43
5.3	La standardizzazione	43
5.3.1	Open Group.....	43
5.3.2	OASIS.....	44
6.	La situazione italiana.....	45
6.1	I principali progetti e iniziative	45
6.2	La Carta d'Identità Elettronica (CIE)	46
6.3	La Carta Nazionale dei Servizi (CNS)	47
6.4	Le principali iniziative della Pubblica Amministrazione	48
6.5	La firma digitale	52
7.	Riflessioni finali.....	53

Riferimenti e acronimi

Riferimenti	56
Acronimi	56

1. Introduzione

1.1 Cos'è l'identità digitale

In questo capitolo verrà fornita una definizione del concetto di identità digitale. L'obiettivo è quello di mostrare come in realtà non esista una definizione sufficientemente completa di identità digitale. In effetti essa vuole essere una rappresentazione dell'identità reale di una persona quando intrattiene relazioni con altre persone o entità attraverso una rete digitale.

Il primo tentativo di fornire una definizione completa del concetto di identità digitale è stato fatto da Hal Abelson e Lawrence Lessig del MIT (Massachusetts Institute of Technology) nel white paper "Digital Identity in Cyberspace" [IDCS]:

"L'insieme delle caratteristiche essenziali e uniche di un soggetto sono ciò che è in grado di identificarlo".

Dietro questa semplice definizione si nasconde in realtà una grande complessità che è legata alla definizione di caratteristiche uniche ed essenziali.

La prima categoria di caratteristiche che viene in mente per poter costruire un'identità è quella costituita dai tratti fisici ed immutabili di un determinato soggetto, come il colore degli occhi, le impronte digitali, il sesso e così via. Probabilmente queste sono le caratteristiche che da sempre siamo abituati a concepire come parte dell'identità.

Esistono comunque altre caratteristiche che possono essere utilizzate per individuare una persona. La capacità di guidare una autovettura, di usare un computer o di comprendere una determinata lingua, ad esempio, possono essere considerate parte dell'identità di un soggetto. Anche i gusti culinari, gli hobby e i film preferiti concorrono ad identificare una persona. Esistono persino caratteristiche soggettive che possono concorrere nella determinazione dell'identità. L'affidabilità o la simpatia di una persona sono tipiche caratteristiche che la identificano. Esse sono definibili come caratteristiche soggettive, in quanto sono rappresentate dalla percezione che un altro soggetto ha di una determinata persona.

Un'altra definizione di identità digitale viene da Eric Norlin e Andre Durand di PingID Network Inc. nel loro articolo del dicembre 2002 intitolato "Federated Identity Management" [FIM]:

"L'identità digitale è la rappresentazione virtuale dell'identità reale che può essere usata durante interazioni elettroniche con persone o macchine".

Questa definizione è sicuramente più immediata, tuttavia nel loro articolo anche Norlin e Durand di fatto sottolineano come l'identità digitale sia fatta da diversi componenti: credenziali, attributi e talvolta "reputazione elettronica".

Le credenziali sono gli elementi che permettono la verifica dell'identità (fase di autenticazione), mentre gli attributi sono informazioni aggiuntive legate all'identità e collettivamente noti come "profilo". La reputazione elettronica è un insieme di dati legato a caratteristiche soggettive che una persona si crea interagendo con altri soggetti nel mondo virtuale.

1.2 La forza di un'identità digitale

Abelson e Lessig sottolineano nel loro articolo che due soggetti possono comunque condividere delle caratteristiche. Questo modello riflette la realtà per cui due persone possono avere lo stesso hobby, possono conoscere le stesse lingue e possono avere lo stesso colore degli occhi. In generale deve comunque essere possibile individuare delle caratteristiche che non sono comuni tra due soggetti e che permettono di rendere univoche le loro identità.

Questa osservazione ha due conseguenze immediate:

- l'elenco delle caratteristiche di un'identità può essere lungo a piacere;
- la "forza" di un'identità è proporzionale al numero di caratteristiche distintive che essa contiene.

Ad esempio, quando ci si reca da un tabaccaio per acquistare un pacchetto di sigarette, l' esercente deve conoscere l'identità dell'acquirente al fine di capire se può o meno acquistare quel tipo di prodotto. L' esercente in realtà non necessita di conoscere nome, cognome o residenza dell'acquirente. Tuttavia ha bisogno di sapere se la persona che ha di fronte ha l'età e la disponibilità economica per acquistare il prodotto in questione. In questo caso l'acquirente fornisce un'identità che è costituita dalle caratteristiche necessarie e sufficienti per l'acquisto delle sigarette. Quindi un'identità debole non è detto che sia insufficiente per completare una determinata transazione con un altro soggetto.

1.3 Identità digitale e anonimato

La possibilità di fornire informazioni parziali sulla propria identità è un concetto importante, in quanto evidenzia molto bene come la definizione stessa di identità è fortemente dipendente dal contesto in cui viene utilizzata.

La definizione di Abelson e Lessig permette l'estrapolazione di un interessante concetto legato all'identità digitale: l'unbundling. Con questo termine si intende la possibilità di trattare separatamente le caratteristiche che compongono un'identità digitale. Giocando sul numero di componenti che si forniscono in una transazione elettronica, come è stato già evidenziato, è possibile fornire una maggiore o minore forza all'identità che si presenta. Si configurano due casi estremi:

- anonimato, che si ottiene non fornendo alcuna componente;
- completa identificazione, che si ottiene fornendo tutte le componenti disponibili.

Le singole componenti possono inoltre offrire un legame più o meno forte nei confronti della reale identità di una entità. I due casi estremi per questo tipo di caratteristica sono:

- anonimato, inteso questa volta come nessun legame rispetto all'identità reale;
- completa associazione, che si ottiene fornendo componenti che hanno un legame forte con la reale identità di un determinato soggetto.

Queste considerazioni portano immediatamente alla constatazione che è possibile identificarsi nel mondo digitale in maniera completa pur mantenendo un completo anonimato. Questa naturalmente sembra una possibilità allettante in quanto permette di separare la nostra vita reale da quella che si trascorre nel mondo digitale di Internet.

Tuttavia occorre anche notare che ci sono particolari transazioni digitali che riguardano anche aspetti reali. È il caso ad esempio della firma digitale. Se un documento elettronico firmato digitalmente deve avere una valenza giuridica, si hanno due mondi che devono essere integrati: il mondo virtuale dei documenti digitali e quello legislativo reale. In tal caso non è possibile usare un'identità digitale non associabile alla persona fisica o giuridica che essa rappresenta nel mondo reale.

Naturalmente esistono invece tante situazioni in cui è possibile usare un'identità dissociata completamente da quella reale. È il caso ad esempio delle chat, vere e proprie stanze virtuali dove lo scopo è unicamente la condivisione di informazioni senza nessun interesse nella conoscenza diretta dei propri interlocutori.

1.4 La relazione con il mondo reale

Un altro importante concetto legato all'identità digitale è che spesso la forza di identificazione o di collegamento verso l'identità reale è una caratteristica oggettiva. Per comprendere a fondo il significato di questa affermazione, basti pensare alla posta elettronica.

Qualunque esperto di sicurezza informatica sa bene che la posta elettronica, nel suo utilizzo di base, non offre alcuna certezza circa l'identità del mittente. Tuttavia, la maggior parte delle persone confida completamente nell'attendibilità del mittente. In pratica la percezione che tutti hanno è che l'indirizzo di posta elettronica sia di fatto una componente forte dell'identità digitale di un soggetto.

Questo è uno dei problemi che ha portato allo sviluppo della metodologia di attacco denominata "social engineering". Si tratta in realtà di un fenomeno concettualmente simile alla truffa, ovvero la capacità di raggirare le persone al fine di ottenere informazioni o privilegi che normalmente non possono essere concessi.

Uno dei maggiori cultori della tecnica di social engineering è il noto hacker Kevin Mitnick, conosciuto come "il condor". Mitnick è anche autore di un libro intitolato "The Art of Deception: Controlling the Human Element of Security" [TAD]. Questo libro spiega i diversi modi con cui è possibile conquistarsi la fiducia di una persona e abusarne per ottenere da questa ogni genere di informazione.

L'identità percepita da un messaggio di posta elettronica è così forte che molte persone possono essere raggirate inviando messaggi in cui si falsifica il mittente, sostituendolo con una persona di cui l'ignaro raggirato si fida. D'altra parte è pur vero che in moltissimi casi, quando si legge un messaggio di posta, si fa una operazione di autenticazione implicita. Nello specifico, quando si legge il testo di un messaggio in molti casi è abbastanza facile capire quando chi ci scrive non può essere l'apparente mittente. Questo è il risultato di un processo non digitale e legato ad una conoscenza che si ha del mittente nel mondo reale.

Una cosa ancora più interessante accade quando si ricevono messaggi di posta elettronica che contengono una firma digitale. In questa situazione, la tecnologia ci fornisce un meccanismo obiettivo che garantisce l'autenticità. Tuttavia se per una semplice questione di configurazione (cosa che capita assai frequentemente) il programma di posta non riconosce come valida la firma digitale, l'utente medio considera non affidabile il mittente o comunque ha un senso di insicurezza nell'apertura del messaggio di posta.

Questi esempi mostrano come il ruolo della percezione degli utenti nell'utilizzo di certe componenti dell'identità digitale sia alla fine importante per determinarne la forza, soprattutto in un contesto in cui vi è molta interazione con il mondo reale. La posta elettronica è un servizio digitale, ma il suo compito è quello di mettere in comunicazione le persone. In contesti più digitali, dove ad esempio l'interazione avviene con un sistema, la forza dell'identità digitale presentata è una questione completamente obiettiva e legata sostanzialmente alle tecnologie impiegate.