

L'identità digitale per l'accesso ai servizi ed alle informazioni in rete.

Giovanni Manca
Ufficio Standard e tecnologie d'identificazione



AGENDA

- **Il quadro normativo di riferimento.**
- **I principi base dell'identità digitale.**
- **Le firme digitali in XML.**
- **L'identità federata.**
- **I diritti digitali.**
- **Conclusioni.**



Il quadro normativo di riferimento

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Quadro normativo primario

- **Codice dell'amministrazione digitale (Decreto legislativo 4 aprile 2006, n. 159.**
- **Nel codice possiamo direttamente o indirettamente trovare riferimenti all'identità digitale negli articoli 64, 65 e 66.**
- **Art. 64: Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.**
- **Art. 65: Istanze e dichiarazioni presentate alla pubblica amministrazione per via telematica.**
- **Art. 66: Carta d'identità elettronica e carta nazionale dei servizi.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Regole tecniche

- **Abbiamo regole tecniche per la Carta Nazionale dei Servizi e per la Carta d'Identità Elettronica.**
- **DM 9 dicembre 2004 (CNS).**
- **DM 2 agosto 2005 (CIE) in fase di aggiornamento.**
- **Esistono altri documenti di tipo tecnico connessi ai principali (sistema operativo della smart card, profilo del certificato di autenticazione, ecc.).**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



I principi base dell'identità digitale

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Perché parliamo di identità digitali (1)

- Il numero dei servizi offerti in rete in modo automatizzato esiste da numerosi anni ed è sempre più sviluppato.
- Il servizio in rete può essere anonimo solo in particolari situazioni. Sicuramente non lo è se ci sono delle interrogazioni su dati sensibili ovvero se c'è un pagamento.
- L'identità digitale è importante anche all'interno di una organizzazione.
- Le organizzazioni moderne utilizzano personale "mobile" quindi la gestione corretta delle identità digitali diventa critica anche per gli affari e per la protezione del patrimonio aziendale.
- Le identità digitali vanno gestite correttamente perché sono una parte integrante del business.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Perché parliamo di identità digitali (2)

- Le identità digitali fanno già parte da anni del nostro mondo lavorativo o privato.
- Il bancomat, il telefonino, il computer dell'ufficio, la rete aziendale al quale è connesso, il codice del telefono per particolari abilitazioni alla chiamata, l'abbonamento alla TV satellitare, il codice di accesso ai servizi del fisco o previdenziali, ecc.
- Identità digitale però non è solo uno username e una password.
- E' anche un sistema complesso di gestione di identità, autenticazioni, autorizzazioni, profili, informazioni biometriche.
- L'identità digitale oggi è un'architettura a parte nel mondo sempre più complesso dell'ICT.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Architetture dell'identità digitale (1)

- **Architettura di processo.**

L'architettura di processo è una metodologia che permette di definire il modo mediante il quale la specifica organizzazione affronta le tematiche dell'identità e come le affronterà nel futuro. In tale architettura sono presenti anche elementi relativi alla pianificazione della modifica dei processi organizzativi al fine del miglioramento della loro efficacia.



Architetture dell'identità digitale (2)

- **Architettura dei dati.**

L'architettura dei dati è un modello per l'organizzazione dei dati utilizzati nella struttura (anche in senso lato). Sapere dove sono i dati relativi all'identità, qual è il loro scopo, come vengono utilizzati è indispensabile, oltre che per motivi di efficienza, anche per evitare incidenti di percorso attinenti alle problematiche di privacy.



Architetture dell'identità digitale (3)

- **Architettura tecnologica.**
L'architettura tecnologica costituisce il modo di utilizzo del sistema che utilizza i dati di identità all'interno dei relativi processi.
- **Politiche organizzative.**
Le politiche organizzative devono essere utilizzate a supporto di quelle tecnologiche. La tecnologia non riesce a risolvere tutti i problemi.
- **Schemi di interoperabilità.**
E' indispensabile definire l'insieme di standard che si vogliono utilizzare. Delle buone regole di interoperabilità sono il fondamentale punto di partenza per un sistema di identità digitale che deve svilupparsi.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Le parole dell'identità digitale (1)

- **Soggetto o entità.**
- **Risorsa.**
- **Un soggetto o entità per accedere a un risorsa dichiara una identità.**
- **Le identità sono insiemi di dati su un soggetto e rappresentano attributi, preferenze e tratti.**
- **Sono attributi le informazioni di un soggetto, l'affidabilità commerciale (tipo aste on-line), la sua età, ecc.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Le parole dell'identità digitale (2)

- Sono preferenze il posto preferito in aereo, il gusto della pizza, l'albergo in una città, ecc.
- Sono tratti sono simili agli attributi ma sono del soggetto e non sono acquisiti. In biometria sono fondamentali.
- In generale gli attributi sono sufficienti nel mondo reale.
- Per accedere a una risorsa un soggetto deve usare delle credenziali. Le credenziali trasferiscono "trust" da un soggetto a un altro.
- Le credenziali vengono presentate a un'autorità di sicurezza o a un Policy Enforcement Point che le valida o le rigetta.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Le parole dell'identità digitale (3)

- Le credenziali possono utilizzare username e password, certificati digitali di tipo X.509, un PIN e una smart card, informazioni biometriche.
- Dopo l'autenticazione delle credenziali mediante le politiche di sicurezza un Policy Decision Point (o più PDP) individua i diritti e i permessi associati ad una risorsa per una data identità.
- I diritti sono servizi o risorse ai quali una identità può accedere.
- I permessi sono le azioni che il soggetto può effettuare sulla risorsa.
- Un tipico permesso è il limite di prelievo giornaliero del bancomat.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Altri concetti di base

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Ciclo di vita (1)

- Provisioning (creazione dei record di identità e popolazione degli stessi).
- Propagazione (in situazioni di sistemi complessi soprattutto eterogenei).
- Uso →→→ Manutenzione (mi sono dimenticato la password, devo accedere ad un nuovo disco di rete, ecc.) →→→ Propagazione.
- Uso →→→ Rimozione (mi sono dimesso).

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Integrità, confidenzialità e non ripudio

- **L'integrità assicura che un messaggio o una transazione non siano modificabili.**
- **La confidenzialità assicura che solo le persone o i processi autorizzati possono accedere ai contenuti di un messaggio o in genere a delle informazioni.**
- **Il non ripudio da evidenza dell'esistenza di un messaggio o di una azione che non può essere contestata.**
- **Per queste attività si utilizzano la crittografia simmetrica e asimmetrica.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Crittografia

- **Crittografia a chiave segreta o simmetrica.**
- **Crittografica asimmetrica.**
- **RSA.**
- **Curve ellittiche.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Firme elettroniche e digitali

- Le firme elettroniche assicurano l'integrità.
- Il meccanismo della terza parte fidata (il certificatore) introduce anche il concetto di non ripudio.
- La nostra legislazione parla di firma elettronica qualificata che poi viene realizzata tramite un sistema di crittografia asimmetrica e diventa firma digitale.
- E' ovviamente solo una questione di definizioni normative derivanti in maniera significativa dalla direttiva UE 1999/93/CE.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Le firme in linguaggio XML

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



XML e identità digitale

- **L'XML è presente con particolari tassonomie e semantiche nei sistemi di identità digitale.**
- **Lo standard SAML (Security Assertion Markup Language) è l'esempio più attuale.**
- **Si pensi alle SOA (Service Oriented Architectures).**
- **Si pensi ai sistemi di interoperabilità basati sui web services.**
- **La firma digitale in linguaggio XML assume un ruolo rilevante.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Le basi tecniche

- **eXtendend Markup Language. Insieme di regole per strutturare in formato testo i dati oggetto di elaborazione.**
- **Vengono utilizzate le regole stabilite nella specifica RFC 3275 (XML - Signature Syntax and Processing).**
- **Per alcune operazioni viene referenziato anche la specifica ETSI TS 101 903 nota come XADES.**
- **I principi generali della busta crittografica non cambiano. Ovviamente passiamo dalla elaborazione di formati binari (ASN.1, BER, DER) a quella di testo. Questo in generale è più oneroso in termini di carico sui sistemi.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



I vantaggi dell'XML

- In ogni caso l'XML offre indubbi vantaggi nello scambio dei dati sulle reti di comunicazione a tecnologia Internet.
- Offre la possibilità di gestire sottoscrizioni su particolari strutture di dati.
- In alcuni ambienti operativi, come quello sanitario e finanziario, l'utilizzo dell'XML come linguaggio per i dati di lavoro richiede la definizione di uno standard per l'autenticazione e la sottoscrizione digitale.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Gli scenari di utilizzo

- Busta di e-government nel Sistema Pubblico di Connettività.
- HL7-CDA2 nella documentazione sanitaria.
- Corporate Banking (Gruppo CBI dell'ABI).
- Strutture dati per la gestione documentale.
- Particolari formati utilizzati in applicazioni proprietarie.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'interoperabilità nella firma XML

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'interoperabilità in XMLDSIG (1)

- **Come al solito non è sufficiente aderire agli standard.**
- **Gli standard tra l'altro sono in continua evoluzione.**
- **L'XML ha grandi caratteristiche di flessibilità che però non è ovvio armonizzare con le rigide esigenze della firma elettronica/digitale.**
- **La deliberazione CNIPA n.34 del 2006 stabilisce le "Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML".**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'interoperabilità in XMLDSIG (2)

- Sono ammesse le tipologie di firma Enveloped, Enveloping e Detached.
- Nella enveloped signature è necessario assicurare che tutte le firme successive alla prima vengano applicate sugli stessi dati sui quali è stata calcolata la prima firma, il che non accade in modo automatico.
- Vengono fornite precise indicazioni su trasformazioni, Xpath, XSLT.
- La frase "Il foglio di stile utilizzato deve essere incluso nel file firmato" va intesa come "si deve garantire l'integrità del foglio di stile".

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'interoperabilità in XMLDSIG (3)

- Vengono stabilite anche regole tecniche tratte dallo standard europeo in materia ETSI TS 101 903 (XadES).
- Da questo documento, in particolare viene tratta la standardizzazione del legame tra documento firmato e marca temporale (XadES-T).
- Ma bisogna fare anche i conti con la normativa primaria della firma digitale ovvero sul principio (CAD art. 35, comma 2, secondo capoverso) "*I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità...*".
- Ma questo è compatibile con le esigenze applicative nei vari contesti operativi ?.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'interoperabilità in XMLDSIG (4)

- **Bisogna definire la normalizzazione della presentazione.**
- **Il rapporto con i dati firmato deve essere completo ovvero bisogna evitare di firmare solo parte dei dati soggetti a "non ripudio".**
- **In alcuni contesti si fa riferimento a documenti esterni, come ad esempio le immagini.**
- **Il mercato sta collaborando a definire una serie di possibili soluzioni.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'interoperabilità in XMLDSIG (5)

- **Le opportunità al momento identificate (ma non definite) sono:**
 - Tipologia di firma enveloped per una facilità di visualizzazione con i browser internet.
 - L'applicazione di firma può dover avere una conoscenza diretta del contenuto applicativo.
 - Alcuni spunti tratti da XFDL possono aiutare a circoscrivere e risolvere il problema.
 - Per quanto possibile bisognerebbe evitare una normativa "nazionale" sui fogli di stile.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Uno schema di firma XML

- **<tomcat-users>**

```
<role rolename="tomcat"></role>
<role rolename="test"></role>
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"></ds:CanonicalizationMethod>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
<ds:Reference URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
<dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">/descendant::ds:Signature</dsig-xpath:XPath>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>f/Rcq6wu9gORMioxAxaof7pZux8=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
bEGGalaT6geHfM.....
</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIGYDCBUigAw.....
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</tomcat-users>
```

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



L'identità federata

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Standard di identità (1)

- **Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML), eXtensible Access Control Markup Language (XACML).**
- **SAML maturo e ampiamente utilizzato.**
- **SPML potrebbe prendere il posto del SAML.**
- **XACML immaturo e ancora in fase di consolidamento.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Standard di identità (2)

- **Da tempo esistono sistemi per la distribuzione delle credenziali. Uno famoso è Kerberos.**
- **Lo standard SAML viene utilizzato per la rappresentazione di credenziali in linguaggio XML.**
- **L'utilizzo del SAML comporta anche l'utilizzo di una particolare architettura dove vengono utilizzate asserzioni d'autenticazione, d'attributo e d'autorizzazione.**
- **Queste asserzioni sono fondamentali nei moderni sistemi di identità federata.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



I diritti digitali

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Tecniche per i diritti digitali (1)

- La gestione dei diritti digitali ha anche delle rilevanze sociali.
- Copyleft e Copyright.
- Il servizio iTunes di Apple ha introdotto un esempio reale di realizzazione di un sistema DRM.
- Il formato con il quale il file viene scaricato è ACC. I file ACC sono racchiusi in un involucro digitale che usa un sistema DRM denominato Fairplay.
- L'acquisto di diritti standard permette all'utente di ascoltare brani all'infinito su un massimo di tre computer e di masterizzare CD contenenti i brani acquistati.

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Tecniche per i diritti digitali (2)

- **Quando una cosa serve al mercato subito nascono standard e azioni commerciali.**
- **XrML è un linguaggio basato sull'XML per la gestione dei diritti digitali.**
- **Le prospettive di XrML sono molto positive e siamo già alla versione 2.0 e oltre.**
- **Rimane il fatto che il DRM è molto un fatto sociale/commerciale dove gli aspetti tecnici passano rapidamente in secondo piano.**

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Conclusioni

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Il futuro a breve e medio termine

- L'emissione a regime di CIE definirà il modello "ufficiale" di erogazione del servizio per il front office.
- I meccanismi di identità federata regoleranno lo scambio dei dati prevalentemente nel back office.
- Nel medio periodo si dovrà valutare l'opportunità della presenza e il conseguente ruolo di una carta di accesso ai servizi non contemplati nella CIE (Servizi EMV, sanitari, ecc.).
- Qualche modifica di percorso potrebbe arrivare dal contesto dell'UE (European Citizen Card, SEPA, etc.).

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca



Per maggiori informazioni
www.cnipa.gov.it
manca@cnipa.it

Roma - 14/06/2007

L'identità digitale per l'accesso ai servizi, G. Manca