CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

La sicurezza nell'accesso ai servizi di e-government.

Giovanni Manca
Ufficio progettuale sicurezza

AGENDA

- **Il quadro normativo di riferimento.**
- **I principi base dell'identità digitale.**
- **L'identità federata.**
- **CIE, CNS o altro ?**
- **Dematerializzazione.**
- **Posta Elettronica Certificata.**
- **Conclusioni.**

Il quadro normativo di riferimento

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.**

Regole tecniche

- **Ci sono specifiche regole tecniche per la Carta Nazionale dei Servizi e per la Carta d'Identità Elettronica.**
- **Decreto interministeriale 9 dicembre 2004 (CNS).**
- **Decreto interministeriale 8 novembre 2007 (CIE).**
- **Esistono altri documenti di tipo tecnico connessi ai principali (sistema operativo della smart card, profilo del certificato di autenticazione, ecc.)**

I principi base dell'identità digitale

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.

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.

Definizione di identità digitale

- **Tra le varie definizioni di identità digitale è opportuno citare il primo tentativo di fornire una definizione completa del concetto. Hal Abelson e Lawrence Lessig del MIT nel white paper "Digital Identity in Cyberspace" dicono:**

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

- **Tale definizione, semplice ed essenziale, nasconde la difficoltà di definire cosa debba essere "essenziale e unico".**

Come identificare ?

- Qualcosa che conosco (password).
- Qualcosa che possiedo (smart card).
- Qualcosa che sono (biometria).
- Combinazioni delle precedenti.
- Un esempio “vero” : accedere ad un sistema tramite una smart card crittografica utilizzando come PIN l’impronta digitale.

Architetture dell'identità digitale

- **Per realizzare "identità digitali":**
  - 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.

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.**

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.**

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 lo 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.**

Qualche altro concetto di base

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).**

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.

Crittografia

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

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.**

I numeri della firma digitale

- **17 certificatori accreditati.**
- **Circa 3.250.000 dispositivi di firma.**
- **Oltre 100.000.000 milioni di documenti sottoscritti all'anno.**
- **Circa 34.000 smart card attive nella PA rilasciate dal CNIPA.**
- **Forte impulso nella sanità elettronica con il progetto Carta Operatore Sanitario (circa 40.000 smart card).**

L’identità federata

Federare l'identità

- **L'evoluzione delle reti "corporate" ha portato a nuove esigenze di gestione dell'identità.**
- **Il problema è nato con la fusione delle aziende.**
- **Due individui (due identità) devono accedere al patrimonio informativo aziendale da due postazioni fisicamente e logicamente distanti tra loro.**
- **L'omogeneizzazione dell'accesso passa per la federazione delle identità.**

Differenti profili di federazione

- **Il paradigma federato costringe a ripensare i ruoli delle organizzazioni nella catena del servizio:**
  - se prima fornitori di servizio e di identità erano la stessa organizzazione, ora appartengono a organizzazioni diverse.
- **I fornitori di servizio ("Service Provider", SP) presidiano l'offerta di funzionalità applicative.**
- **I fornitori di identità ("Identity Provider", IdP) si specializzano nella gestione delle identità digitali.**
- **IdP e SP cooperano sotto diversi "profili".**
- **SPC (Sistema Pubblico di Connettività opera in tal modo).**

CIE, CNS o altro ?

L’identità tramite smart card (1)

- La Carta d’Identità Elettronica (CIE) è uno strumento di identificazione a vista valido anche come documento di viaggio.
- Tramite il microchip è possibile autenticarsi in rete, firmare digitalmente. Nel microchip possono essere installati anche altri servizi di tipo attivo (nel microchip avvengono delle elaborazioni) o passivo (nel microchip sono memorizzati dati).
- Più servizi sono gestiti dalla CIE più complesso è il Suo ciclo di vita.
- Un esempio: se smarrisco la CIE devo revocare la possibilità dell’accesso ai servizi in rete e il servizio di firma digitale. E’ quindi molto utile erogare un servizio di revoca tramite un unico call center.

L’identità tramite smart card (2)

- La Carta Nazionale dei Servizi (CNS) viene utilizzata esclusivamente per l’accesso ai servizi in rete.
- Anch’essa può contenere quanto contiene la CIE visto che le due carte sono progettate coerentemente.
- Per informazioni si sappia che il micro circuito bancario è un’altra cosa.
- Anche il Machine Readable Travel Document (passaporto elettronico) è un’altra cosa.

Dematerializzazione

Le nuove regole tecniche

- **Le regole tecniche della deliberazione Cnipa n. 11/2004 restano in vigore fino all'adozione di quelle previste dall'articolo 71 del Codice dell'Amministrazione Digitale .**

- **La Commissione interministeriale per la dematerializzazione ha predisposto una proposta di decreto.**

- **Attualmente la versione provvisoria di uno schema di decreto è stata inviata al Cnipa dall'Ufficio legislativo del Ministro per il previsto parere.**

Punti qualificanti dello schema - 1

- **Introdotto il concetto di processo di conservazione dei documenti informatici attuato mediante un sistema di conservazione che assicura:**
  - la conservazione, integrata ai documenti, delle informazioni di contesto generate nelle fasi di gestione e di conservazione;
  - la conservazione del software di gestione, consultazione e conservazione, degli strumenti di ricerca, dei piani di classificazione e di conservazione dei documenti, dei manuali di gestione e dei manuali operativi, degli indici e dei repertori formati e utilizzati nei sistemi di gestione dei documenti;
  - l'individuazione delle responsabilità per tutte le fasi di gestione del sistema documentario.

Punti qualificanti dello schema - 2

- **Delineati il processo di riproduzione sostitutiva di documenti analogici e il processo di riproduzione sostitutiva di documenti informatici (scompare il processo di riversamento), ma con una più chiara definizione della funzione del pubblico ufficiale:**
  - per i documenti analogici delle PA è richiesto l'intervento solo del responsabile della conservazione;
  - per i documenti analogici originali non unici dei privati è richiesto l'intervento solo del responsabile della conservazione;
  - per i documenti analogici originali unici dei privati è richiesto l'intervento solo del pubblico ufficiale.

Altri punti rilevanti

- **Vengono distinti i formati di formazione del documento dai formati di conservazione:**
  - la formazione avviene avvalendosi di prodotti informatici di larga diffusione sul mercato, anche “a codice sorgente aperto”;
  - per la conservazione vengono utilizzati formati a standard aperto, compresi tra quelli riconosciuti dagli organismi nazionali e internazionali preposti alla relativa normazione.
- **I supporti per la conservazione devono avere particolari caratteristiche di qualità e durata.**
- **Il CNIPA ha il compito di emettere apposite guide tecniche che approfondiranno gli argomenti con esempi e suggerimenti operativi.**

Posta Elettronica Certificata

I numeri della PEC

- **23 gestori attivi.**
- **Circa 16.300 domini attivi al 30 aprile 2008.**
- **Circa 140.000 caselle all'inizio del 2008.**
- **Scambio di oltre 14 milioni di messaggi con un trend in costante crescita.**

Conclusioni

Il futuro a breve e medio termine

- **L'emissione regolare di CIE definisce il modello "ufficiale" di erogazione del servizio per il front office.**
- **I meccanismi di identità federata regolano lo scambio dei dati nel back office (scambio dati tra amministrazioni) utilizzando l'identity provider della CIE.**
- **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, sociali, ecc.).**
- **Qualche modifica di percorso sta arrivando dal contesto dell'UE (European Citizen Card CEN/TS 15480, SEPA, ecc.).**

Per maggiori informazioni

www.cnipa.gov.it

manca@cnipa.it