

(slide riassuntive)

I servizi erogabili con la Carta Nazionale dei Servizi

di Vincenzo Scognamiglio

Vincenzo Scognamiglio - "I servizi
erogabili con la CNS"

1

Certificazione

Un bisogno imprescindibile della CNS
riguarda la presenza di una firma digitale
al proprio interno autenticata dagli enti
certificatori individuati e legittimati dalla



* l'elenco pubblico dei certificatori, previsto dall'articolo 27 comma 3 del DPR 28 dicembre 2000 n.445 e specificato nel DPCM 8 febbraio 1999, viene mantenuto dall'Autorità e reso disponibile per via telematica all'indirizzo <http://www.cnipa.gov.it/>

Vincenzo Scognamiglio - "I servizi
erogabili con la CNS"

2

presupposti organizzativi

la CNS, per essere funzionale, presuppone



individuazione e sviluppo, da parte delle PA interessate, della rete di servizi che intendono veicolare attraverso la carta e che ne giustificano l'esistenza



questo richiede a monte

il riesame accurato dei procedimenti amministrativi interni con impatti a livello normativo e organizzativo

come funziona le opzioni di servizio

la CNS :

- **contiene le informazioni per la firma digitale**
- **può supportare funzioni di pagamento**
- **può contenere applicazioni "speciali" (che vedremo)**
- **deve consentire l'utilizzo del sistema sanitario (pur non contenendo i dati sanitari al proprio interno)**

effetti per le amministrazioni

- **facilitazioni di dialogo con i cittadini**
- **contatto e integrazione delle PA tra di loro e con altri attori pubblici e privati (banche, enti erogatori di servizi di pubblica utilità)**
- **sviluppo di attività di tipo normativo, organizzativo e tecnico volte a semplificare i processi e i meccanismi di funzionamento interni alle PA**

Vincenzo Scognamiglio - "I servizi erogabili con la CNS"

5

La Carta Nazionale dei Servizi



Vincenzo Scognamiglio - "I servizi erogabili con la CNS"

6

I documenti nella PA

- Il supporto base per lo svolgimento delle attività amministrative nelle Pubbliche Amministrazioni è dai tempi più remoti il **DOCUMENTO**
- Negli ultimi anni l'informatica ha cambiato il concetto di documento trascinando quello che prima era solo un supporto cartaceo nel suo mondo digitale

Firma di un documento

- **Firma**: meccanismo che garantisce al supporto fisico:
 - Autenticità
 - integrità
 - riconoscimento
- La natura della firma è strettamente legata al supporto fisico, con il suo cambiamento cambia anche il modo di firmare

Firma nei documenti cartacei

•Per documenti su supporto cartaceo si adotta il meccanismo della **firma autografa** che ha i seguenti pregi:

- universalmente accettata
- Realizzazione semplice e immediata (una penna e via)
- livello di sicurezza sufficiente nei contesti più comuni di utilizzo
- Riconoscimento legale

E nel digitale?

La nascita di nuove tecnologie porta con se la nascita di nuove esigenze.

Per fare il salto di qualità anche i documenti digitali hanno bisogno, per essere riconosciuti e riconoscibili, di un meccanismo di autenticazione.

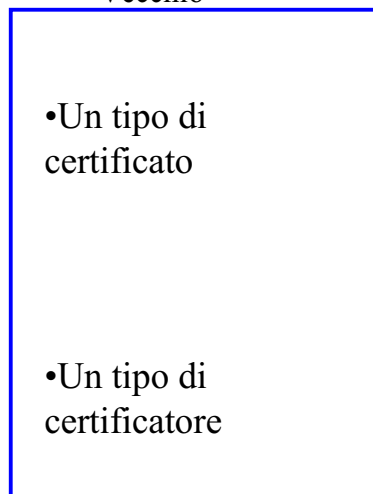
Il percorso che ha portato alla “Firma digitale” non è stato né semplice né veloce

La firma digitale e la CNS

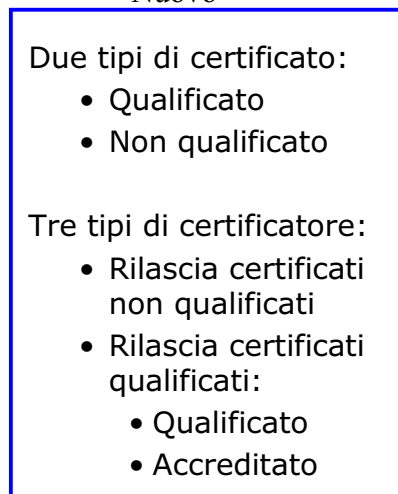
- Come accennato la firma digitale è la colonna portante della CNS in quanto, senza essa, non si può dare alcuno valore alla smart card in questione e nessuna validità ai servizi da essa offerta.

Innovazioni (1)

Vecchio



Nuovo



Innovazioni (2)

Vecchio

- Un tipo di firma elettronica



Nuovo

Quattro tipi di firma elettronica:

- semplice
- avanzata
- qualificata
- *digitale*

Tipi di documenti

Le definizioni che seguono sono più burocratiche che informatiche

• Delibera CNIPA (ex AIPA) 42 del 13 dicembre 2001:

- documento analogico: utilizza una grandezza fisica continua (tracce su carta, immagini su film, ...)
- documento digitale: utilizza una grandezza fisica discreta (valori binari)
- documento informatico: documento digitale sottoscritto con firma digitale

Firma digitale

•DPR 445 / 2000:

- firma digitale: il risultato della procedura informatica di validazione basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Gli altri tipi di firma

•Regolamento 137/03:

- FIRMA ELETTRONICA: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
- FIRMA ELETTRONICA AVANZATA: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
- FIRMA ELETTRONICA QUALIFICATA: la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

Certificato (1/2)

- DPR 445 / 2000:

- certificato: il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione e partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche

Certificato (2/2)

- Regolamento 137 / 03:

- certificati elettronici (...) gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi
- certificati qualificati (...) i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva

Certificatore

- Regolamento 137 / 03:
 - CERTIFICATORE ai sensi dell'articolo 2, comma 1, lettera b), del decreto legislativo 23 gennaio 2002, n. 10, il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

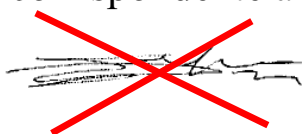
Chiavi

DPR 445 / 2000:

- chiavi asimmetriche: la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici
- chiave privata: l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica
- chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi

Cosa NON è la firma digitale

- La firma digitale non deve essere confusa, nel modo più assoluto, con la digitalizzazione della firma autografa, ovvero la rappresentazione digitale di un'immagine corrispondente alla firma autografa.



Crittografia

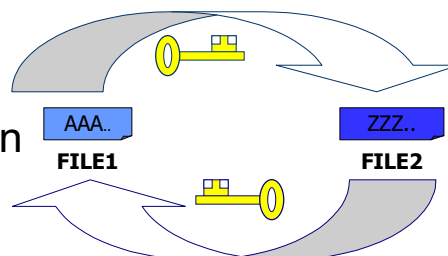
- La crittografia è una tecnica (un procedimento matematico) dalle origini antiche, impiegata storicamente per garantire la riservatezza delle informazioni trasmesse a distanza.
- In ambito informatico, essa può trasformare un file di dati in un insieme di simboli incomprensibili e inutilizzabili per chiunque non possieda lo strumento per decifrarli.

Crittografia

- Esistono due tipi fondamentali di crittografia:
 - a chiave unica (o simmetrica)
 - a doppia chiave (o asimmetrica)

Gli algoritmi di crittografia simmetrica

- La stessa chiave serve per cifrare e per decifrare
- Una chiave non può decifrare un file cifrato con un'altra chiave
- La chiave è posseduta dal mittente e dal destinatario

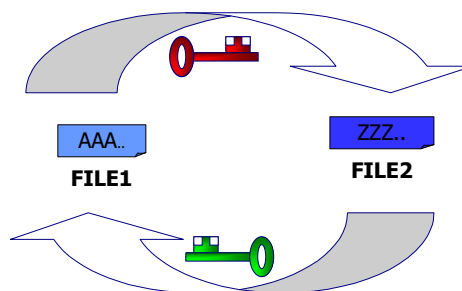


Gli algoritmi di crittografia simmetrica

- Vantaggi:
 - Efficienza
- Svantaggi:
 - Necessità di prevedere una chiave per ogni coppia di interlocutori (ogni soggetto è costretto a possedere molte chiavi)
 - Problemi di sicurezza in fase di distribuzione della chiave

Gli algoritmi di crittografia asimmetrica

- Un documento cifrato con una chiave può essere decifrato con l'altra e viceversa.
- Ogni chiave può cifrare o decifrare.
- La chiave che cifra non può decifrare lo stesso file
- Una chiave è posseduta dal mittente (chiave **privata**) ed è segreta; l'altra chiave (chiave **pubblica**) è accessibile a tutti i destinatari



Le chiavi vengono generate in coppia da uno speciale algoritmo ed è impossibile ottenere una chiave a partire dall'altra.

Gli algoritmi di crittografia asimmetrica

•Vantaggi:

- Sicurezza (non bisogna distribuire la chiave privata)
- Fruibilità: la stessa coppia di chiavi viene utilizzata da tutti gli utenti

•Svantaggi:

- Complessità algoritmica \Rightarrow elevati tempi di calcolo

Gli algoritmi di hashing sicuro

•Permettono di creare da una sequenza di bit qualsiasi e di qualsiasi lunghezza (tipicamente, un file) una sequenza di bit a lunghezza fissa correlata in modo molto stretto alla sequenza di partenza.

•Questo tipo di compressione garantisce (a meno di probabilità trascurabili) che il file compresso sia univocamente determinato dal file originario; il file compresso che si ottiene viene chiamato **"impronta"** (o "digest") del file.

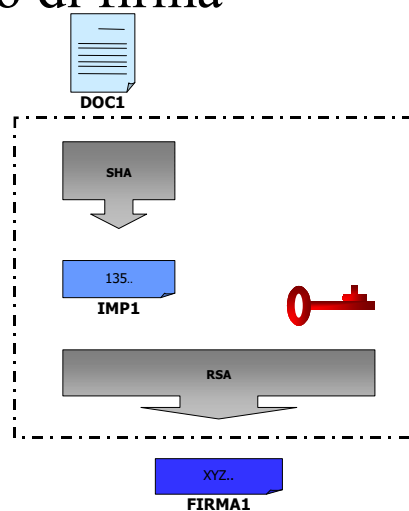
Gli algoritmi utilizzati

- Hashing sicuro: algoritmo **SHA** (Secure Hash Algorithm)
- Crittografia asimmetrica: algoritmo **RSA**, proposto da Rivest, Shamir e Adleman

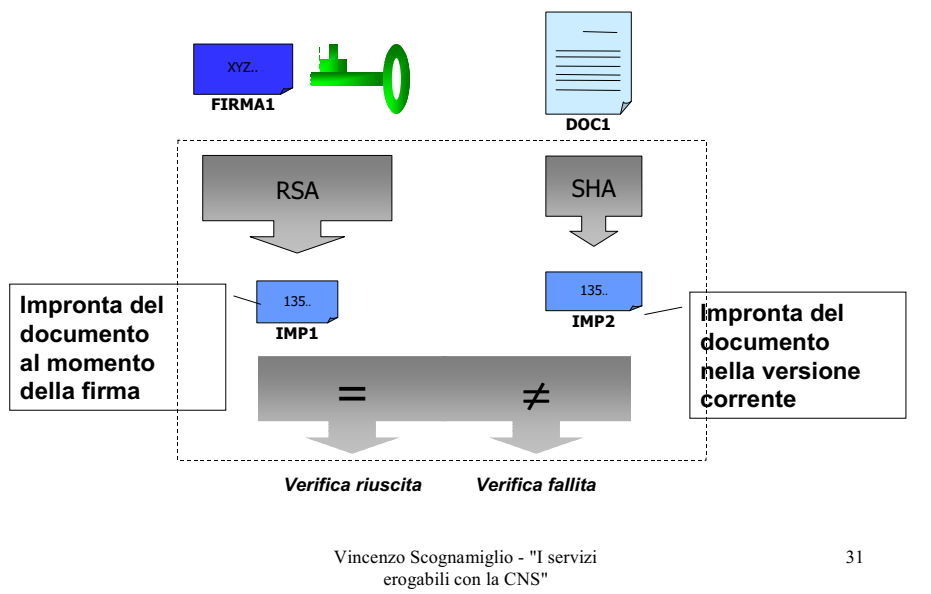
L'algoritmo di firma

- Algoritmo di compressione (SHA)
⇒ impronta univoca

Algoritmo di crittografia (RSA) ⇒ firma



L'algorithmo di verifica



Esito

- Verifica riuscita: la firma è valida
- Verifica fallita: la firma è falsa, oppure la firma è autentica ma è stata apposta su un documento diverso da quello allegato.

Certificato



Certificato

•Il Certificato include :

- Il nome dell'Autorità di Certificazione
- La data di emissione del certificato
- La data di scadenza del certificato
- Il nominativo del soggetto
- La chiave pubblica del soggetto

Lunghezza e validità ideali delle chiavi



Vincenzo Scognamiglio - "I servizi erogabili con la CNS"

35

Sicurezza delle chiavi

- Una chiave segreta può sempre essere generata da un opportuno programma (maligno)
- La possibilità che una chiave venga generata e applicata al documento corretto è del tutto trascurabile
- La generazione di una chiave per “aprire” illecitamente un documento può richiedere anni

Vincenzo Scognamiglio - "I servizi erogabili con la CNS"

36

Infrastruttura a chiave pubblica

Il termine infrastruttura a chiave pubblica (**PKI**, Public Key Infrastructure) è utilizzato per descrivere l'insieme di software, di attori e di criteri organizzativi che consente di gestire i certificati e le chiavi pubbliche e private

Autorità di Certificazione

L'Autorità di Certificazione (**CA**, Certification Authority) è una terza parte, considerata attendibile da tutti gli attori, che emette e gestisce i certificati



Autorità di Certificazione

Principali attività:

- Riceve le richieste di certificazione
- Genera e sottoscrive i certificati
- Riceve e gestisce richieste di sospensione e revoca
- Mantiene aggiornata la CRL e la CSL (liste di revoca e sospensione)
- Mantiene aggiornata la lista dei certificati emessi
- Garantisce l'unicità dei certificati

Autorità di Registrazione

Principali attività:

- Verifica l'identità del richiedente
- Eventualmente genera la coppia di chiavi per il richiedente
- Genera la richiesta di certificazione e la invia alla CA
- Eventualmente fornisce il dispositivo di firma

Rilascio di un certificato

·Il rilascio di un certificato si concretizza:

- Prenotazione presso una CA
- Riconoscimento fisico del richiedente
- Rilascio del certificato (e del sw di firma)

Revoca e sospensione di un certificato

·Revoca del certificato elettronico:

- l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi

·Sospensione del certificato elettronico:

- l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo

·I certificati revocati e sospesi sono inseriti nell'elenco di revoche di certificati (**CRL**: Certificate Revocation List)

Dispositivi di firma

·La normativa italiana prevede che il processo di firma sia eseguito internamente ad un dispositivo caratterizzato da elevati livelli di sicurezza e di protezione della chiave privata.

·In pratica questo requisito si traduce nell 'uso di speciali smart card certificate ITSEC 4



Vincenzo Scognamiglio - "I servizi erogabili con la CNS"

43

Dispositivi di firma

·Le normali card contengono un chip non duplicabile in grado di memorizzare in modo inalterabile informazioni di interesse per l 'utente e/o necessarie per l'utilizzo di specifiche applicazioni.

·La card dialoga con la stazione di lavoro attraverso un apposito lettore, ed software applicativo pu ò interrogarla per ottenere le informazioni in essa memorizzate.

Vincenzo Scognamiglio - "I servizi erogabili con la CNS"

44

Dispositivi sicuri di firma (smart card)

- Memorizzano in modo inalterabile la chiave privata dell'utente e dispongono di firmware, micro-processore e memoria per eseguire on -board:

Non richiedono il trasferimento della chiave privata dell'utente sulla stazione di lavoro. La chiave viene creata dalla smart-card e rimane sempre stabilmente memorizzata nella sua memoria interna

Firma digitale e sicurezza

La sicurezza nell'utilizzo della firma digitale dipende da diversi aspetti :

- Tecnologici
 - Sistema operativo
 - Software di firma
 - Dispositivi di firma
- Infrastrutturali
 - Autorità di Certificazione
- Organizzativi
 - Modalità di utilizzo degli strumenti a disposizione
 - Attenzione nella conservazione e nell'utilizzo della smart-card

Firma digitale e sicurezza

.Gli aspetti più critici sono sicuramente quelli legati al contesto, all'organizzazione e alle modalità di applicazione della firma digitale, piuttosto che a quelli puramente tecnologici o infrastrutturali

I servizi erogabili

- Ogni Comune che decide di adottare la CNS sceglie quali servizi associarvi in base alle proprie esigenze e alle infrastrutture che ha a disposizione
- Le tipologie di servizio sono svariate ed è necessaria una opportuna preparazione sia da parte di chi rende usufruibile il servizio sia da parte dell'utenza

I servizi erogabili con la CNS

Le caratteristiche che definiscono il circuito di emissione, le modalità di accesso ai servizi e le strutture software degli stessi servizi riportano immediatamente al Web.

Infatti le basi tecnologie alla base della CNS come di qualsiasi altra smart card con servizi multipli sono simili (se non le stesse) di Internet e del World Wide Web.

CNS

- Ad esempio, la CNS prevede la possibilità di essere usata per il pagamento di imposte tramite una opportuna abilitazione tramite una banca, questo è a tutti gli effetti un sistema di pagamento/riscossione on line.
- Sono riportabili a servizi web anche le richieste di documenti on line, di autocertificazioni, etc.

Servizi distribuiti

- Impostazione Client - Server
- Database distribuiti
- Informazione in broadcast (mailing)
- Distribuzione dei client su territorio
- Accesso alla carta tramite Internet
- Proiezione su scala nazionale
- Difficoltà di interoperabilità a causa della frammentazione delle scelte dei comuni

I servizi nel web

- Aste on line
- Sportello Bancomat elettronico
- Gestione bolletta del telefono
- Mailing list

- Utilizzo di queste funzioni nella CNS

CNS: I servizi

- Tessera sanitaria
- Richiesta certificato anagrafe
- Esempi pratici e loro implementazione

Sistemi distribuiti

Per sistemi distribuiti si intendono dei sistemi la cui capacità computazionale non risiede in una unica entità fisica.

I sistemi distribuiti possono essere di due tipi:

- Hardware
- Software

Sistemi distribuiti

Il fatto che esistano due tipi di sistemi distribuiti non vuol dire che siano mutuamente esclusivi, anzi, molto spesso la presenza di uno implica l'altro.

Sistemi distribuiti

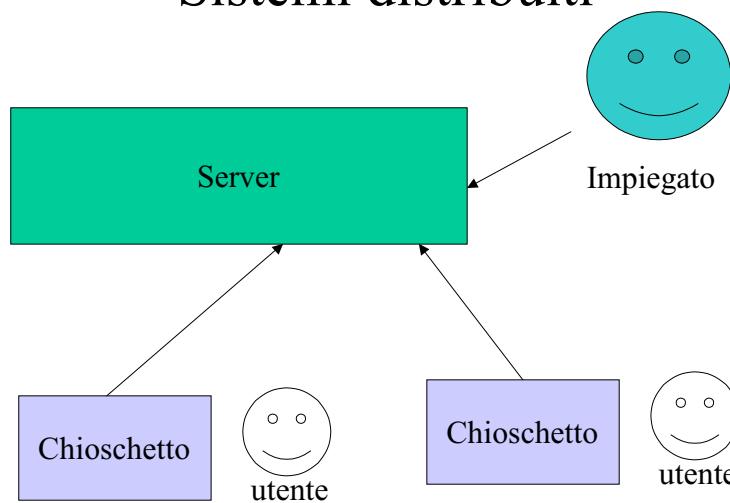
- Il World Wide Web è un sistema distribuito hardware (architettura client-server)
- I programmi di condivisione Mp3 sono sia software che hardware
- Il circuito di utilizzo della CNS è di base hardware ma può essere implementato anche come software

Sistemi distribuiti

Se si accede a un sito web si sta sfruttando in parte l'elaborazione di un computer remoto (server) e in parte quello del computer locale (client).

Nel sistema CNS saranno previsti dei "chioschetti" e vari server.

Sistemi distribuiti



Sistemi distribuiti

- A seconda delle scelte della PA i chioschetti delle CNS potranno avere diversi gradi di “autosufficienza”, la richiesta minima è che siano capaci di garantire la **SICUREZZA** delle transazioni

Sistemi distribuiti

- Infatti, il problema principale di qualsiasi forma di comunicazione sicura risiede nel canale, ovvero nel mezzo di trasmissione delle informazioni
- Una intercettazione del canale deve essere resa difficile e, nel caso avvenga, l'informazione deve essere protetta in maniera alternativa (crittografia).

Sistemi distribuiti

- Nel caso dei servizi erogabili dalla CNS la sicurezza è ancora più importante, questo è il motivo principale per cui un sistema così vecchio (smart-card) trova applicazione solo ora che la sicurezza digitale ha raggiunto obiettivi soddisfacenti

Servizi distribuiti

- La CNS deve offrire, su una struttura distribuita, anche dei servizi distribuiti.
- Tramite lo stesso “chioschetto” devono essere accessibili i servizi di più Enti Pubblici e Privati (Comune, Ospedale, Banca etc)
- L’interoperabilità hw e sw è quindi indispensabile