



Presentazione



Titolo

**Open Source : scelta vantaggiosa
per la conservazione sostitutiva**

Biografia

- 2002: LAUREA vecchio ordinamento ingegneria telecomunicazioni 110 e lode
- 2003: MASTER in Information e Communication Security
- 2004: Project Manager per Telecom Italia area Top Client & ICT Services 
- 2006: Socio Mensa 

Vantaggi dell'Open Source

- Un modello di creazione non proprietario.
- Un modello di Business
- Una strategia
- Un modo di essere
- Una comunità

Free Software Foundation

- L'obiettivo principale di OS era essere software libero. L'idea è che avrebbe avuto sia un vantaggio sociale, permettendo agli utenti di cooperare, sia un vantaggio etico rispettando la loro libertà.
- Le licenze per la maggior parte dei programmi hanno lo scopo di togliere all'utente la libertà di condividerlo e modificarlo. Al contrario OS è inteso come libertà di condividere e modificare il free software.

Open Source : Un nuovo modello di Business

- Negli ultimi anni ,favorito da internet, si è sviluppato in modo esponenziale un nuovo modo di creare software ed un diverso modello di Business:l'open source
- Il software è prodotto congiuntamente da specialisti diversi, è protetto da strumenti giuridici.
- L'Italia per l'altissimo numero di pubbliche amministrazioni potrebbe avere un impulso straordinario da questo modello.
- L'Open Source ,grazie ai suoi notevoli vantaggi tecnici, economici e competitivi, è diventato il modello di riferimento per lo sviluppo del software

Open Source : I valori dei nuovi mercati

- Trasparenza
- Operazioni in simultanea (real-time)
- Globalità
- Interattività spinta
- Disponibilità gratuita di informazioni
- WIKIPEDIA è una enciclopedia Open Source :
“immagina un mondo in cui ogni singola persona può avere accesso a tutta la conoscenza umana”

Open Source : Stimola l'innovazione

La disponibilità di prodotti OS stimola l'innovazione, in quanto è possibile sottoporre ad aggiornamento singole parti del software applicativo con costi assai ridotti.

Vantaggi per le PA nell'uso dell'OS

- Le PA in un mondo in continua evoluzione hanno bisogno di rivedere i propri processi organizzativi per guadagnare in efficienza e ridurre i costi di funzionamento.
- L'informatica deve contribuire all'innovazione organizzativa, deve essere uno strumento duttile e malleabile. Il software deve poter evolvere e diventare adattabile a nuove esperienze tecniche e organizzative, cioè deve essere liberamente modificabile.
- Per poter modificare il software è necessario avere a disposizione il suo codice.

Vantaggi per le PA nell'uso dell'OS

- Gli applicativi non OS non vengono rilasciati insieme al codice sorgente, ma solo in una forma binario/eseguibile.
- Quando non si trova il software non OS non adatto alla propria organizzazione bisogna creare programmi software di tipo “custom” costosi per sviluppo e manutenzione.
- Il codice OS viene rilasciato completo ai suoi codice sorgenti.

Vantaggi per le PA nell'uso dell'OS

- è possibile cederne una copia a chiunque in completa libertà
- Non occorre sostenere nessun costo di licenza
- È possibile installarlo su quante postazioni si desidera senza oneri aggiuntivi

Vantaggi per le PA nell'uso dell'OS

- Facilmente modificabile per essere adattato alle proprie esigenze, occorre avere competenze tecniche di lato livello, il 42% degli sviluppatori di OS risiede in Europa.
- Nella UE trova spazio sia la cultura della collaborazione sia delle alte competenze per sviluppare OS.

Vantaggi per le PA nell'uso dell'OS

- Il codice sorgente essendo pubblicamente visibile è sottoposto a revisioni continue per scoprire ed eliminare eventuali bug, backdoor, spyware.
- Generalmente il tempo di correzione dei bug è molto basso così come il rilascio dei relativi aggiornamenti.

Conservazione Sostitutiva

- Grazie alle regole tecniche del **Cnipa** ai decreti dei **Ministeri dell'Economia e delle Finanze e Lavoro è finalmente possibile smaterializzare tutta la propria documentazione cartacea!**
- Disponibilità di usare toolkit per l'implementazione di una PKI (public key infrastructure) tutto Open Source.
- Rispetto normative CNIPA legate allo sviluppo delle infrastrutture a chiavi pubbliche.

Documento Informatico

- Rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti.
- Sono associate la selezione dell'informazione da rappresentare e la sua forma, che riflettono la volontà e le scelte dell'autore.

- Per "firma elettronica" la legge intende qualunque sistema di autenticazione del documento informatico.
- La "firma elettronica qualificata" è definita come la firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario deve detenere il controllo esclusivo, e la cui titolarità è certificata da un soggetto terzo. Qualunque tecnologia che permetta tale identificazione univoca, rientra nel concetto di "firma elettronica qualificata".
- La "firma digitale", è considerata dalla legge come una particolare specie di "firma elettronica qualificata", basata sulla tecnologia della crittografia a chiavi asimmetriche.

Firma Digitale

- La **firma digitale**, o **firma elettronica qualificata**, **basata sulla tecnologia della crittografia a chiavi asimmetriche**, è un sistema di autenticazione di documenti digitali analogo alla firma autografa su carta. La firma digitale è un sistema di autenticazione forte in quanto si basa sull'uso di un certificato digitale memorizzato su di un dispositivo hardware. I certificati su cui si basa possono essere più di uno

	Firma autografa	Firma digitale
Creazione	manuale	mediante algoritmo di creazione
Apposizione	sul documento: la firma è parte integrante del documento	come allegato: il documento firmato è costituito dalla coppia (documento, firma)
Verifica	confronto con una firma autenticata: metodo insicuro	mediante algoritmo di verifica pubblicamente noto: metodo sicuro
Documento copia	distinguibile	indistinguibile
Validità temporale	illimitata	limitata
Automazione dei processi	non possibile	possibile

La Normativa

- All'articolo 21, il D.Lgs. 82/2005 stabilisce, con un rimando al Codice Civile, che la firma digitale (o altra firma elettronica qualificata) *fa piena prova fino a querela di falso se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta*, equiparando così il documento informatico sottoscritto con firma digitale alla scrittura privata sottoscritta con firma autografa

Algoritmo DSS

- Basato sull'utilizzo della stessa chiave sia per l'operazione di cifratura che quella di decifratura.
La forza della crittografia simmetrica è dunque riposta nella segretezza dell'unica chiave utilizzata dai due interlocutori che la usano, oltre che nella grandezza dello spazio delle chiavi, nella scelta di una buona chiave e nella resistenza dell'algoritmo agli attacchi di crittanalisi.

Algoritmo RSA

- L'algoritmo [RSA](#) non è sicuro da un punto di vista matematico teorico, in quanto esiste la possibilità che tramite la conoscenza della chiave pubblica si possa decriptare un messaggio, ma l'enorme mole di calcoli e l'infinito dispendio in termini di tempo necessari per trovare la soluzione, fa di questo algoritmo un sistema di affidabilità pressoché assoluta.

Funzione Hash

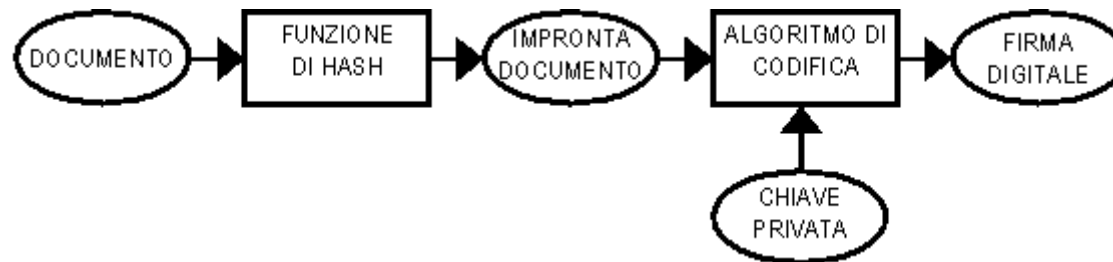
- l'**hash** è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), atta alla trasformazione di un testo di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta *valore di hash*, *checksum crittografico* o *message digest*.

I Sistemi

- Gli algoritmi asimmetrici vengono utilizzati nella firma/verifica dei dati (coppia chiavi , una pubblica e una privata).
- Gli algoritmi simmetrici vengono utilizzati nella cifratura delle informazioni in virtù della elevata velocità di computazione.

Firma Digitale

Schema logico della codifica :

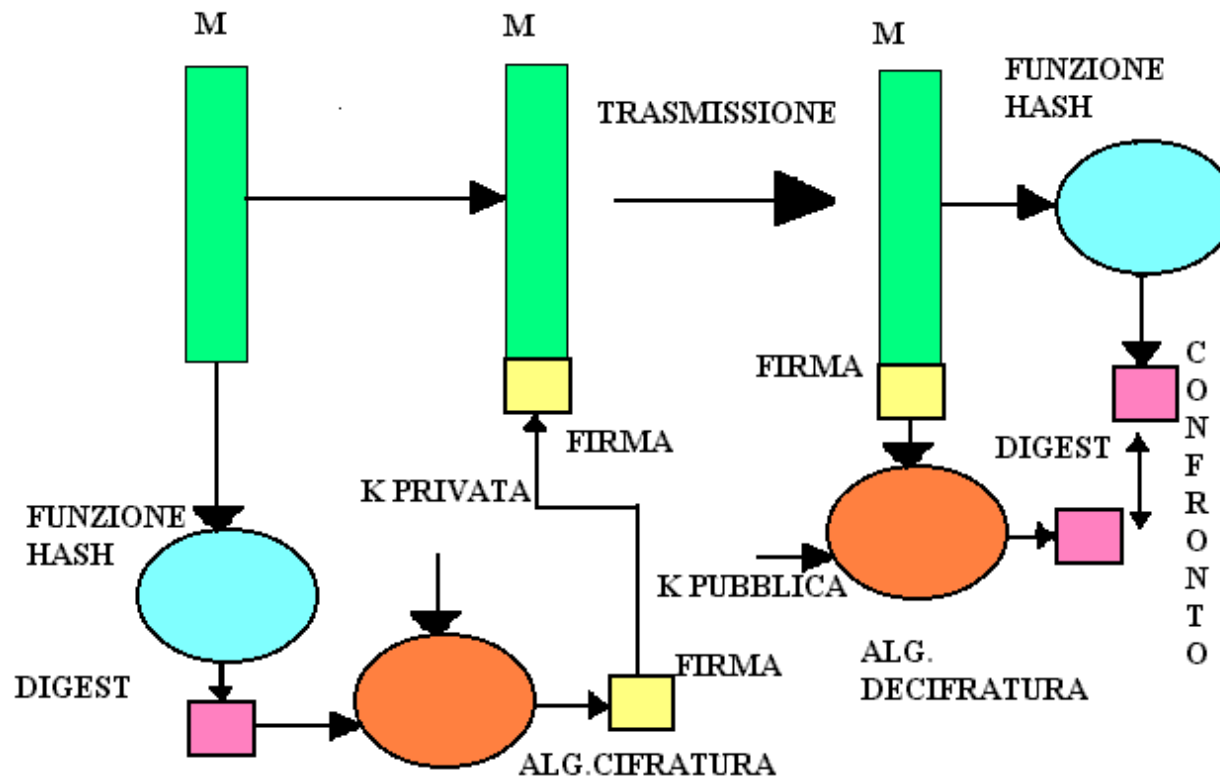


Firma Digitale

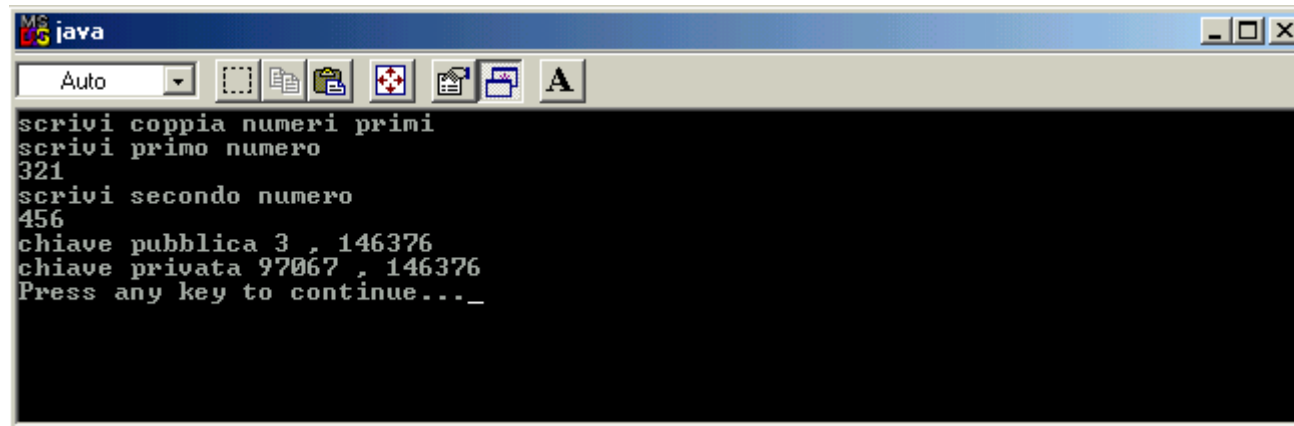
Schema logico della decodifica :



Schema Riassuntivo

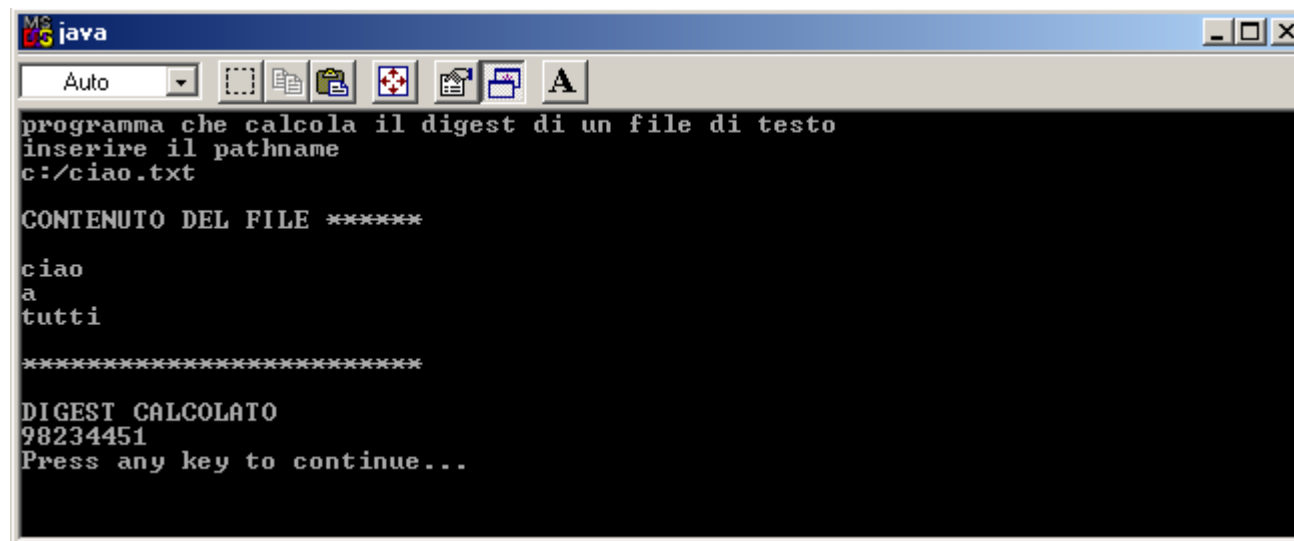


Esempio



```
MS java
Auto
scrivi coppia numeri primi
scrivi primo numero
321
scrivi secondo numero
456
chiave pubblica 3 , 146376
chiave privata 97067 , 146376
Press any key to continue..._
```

Esempio



```
MS java
Auto
programma che calcola il digest di un file di testo
inserire il pathname
c:/ciao.txt

CONTENUTO DEL FILE *****

ciao
a
tutti

*****

DIGEST CALCOLATO
98234451
Press any key to continue...
```

```
MS java
Auto
inserisci hostname server> 151.100.9.80
siete connessi al server: 151.100.9.80
FROM SERVER:benvenuto
inserisci nome file
c:/io.txt
ciao
a
tutti
-
FROM SERVER:file ricevuto
digest calcolato in decimale 29395017
premi START e poi digita la FIRMA
59226784
FROM SERVER:messaggio ricevuto originale
FROM SERVER:fine
```

```
MS java
Auto
SERVER on LINE su IP: pentium133a/151.100.9.80
FROM CLIENT:sono il client pentium133a/151.100.9.80
benvenuto
FROM CLIENT:
FROM CLIENT:Ti invio il file
FROM CLIENT:file inviato
FROM CLIENT:Ti invio la firma
FROM CLIENT:59226784

IL FILE RICEVUTO :

ciao
a
tutti
-

AUTENTICITA:
digest calcolato in decimale 29395017
valore della firma 59226784
valore della firma decodificata 29395017
messaggio originale
SERVER on LINE su IP: pentium133a/151.100.9.80
```

Certificato Digitale

Un **certificato digitale** è un documento elettronico che attesta, con una [firma digitale](#), l'associazione tra una [chiave pubblica](#) e l'identità di un soggetto

VERSIONE
NUMERO DI SERIE
IDENTIFIC. ALGORIT.
FORNITORE
PERIODO VALIDITA'
OGGETTO
INFO CHIAVE PUB.
FIRMA

Software utilizzati

- Open SSL : software di crittografia che fornisce le funzionalità di base per la generazione di certificati digitali.
- Java : ottimo linguaggio di programmazione orientato agli oggetti.
- Apache : server web utilizzato come interfaccia ai programmi di supporto sulla CA.
- OpenLDAP : server ldap utilizzato per la pubblicazione dei certificati (CRL)

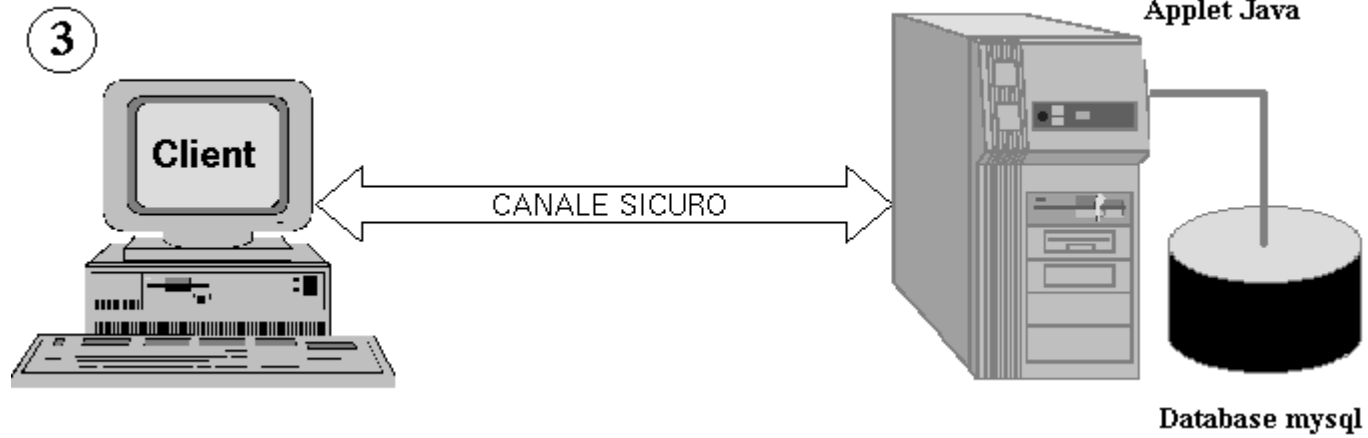
Fase 1



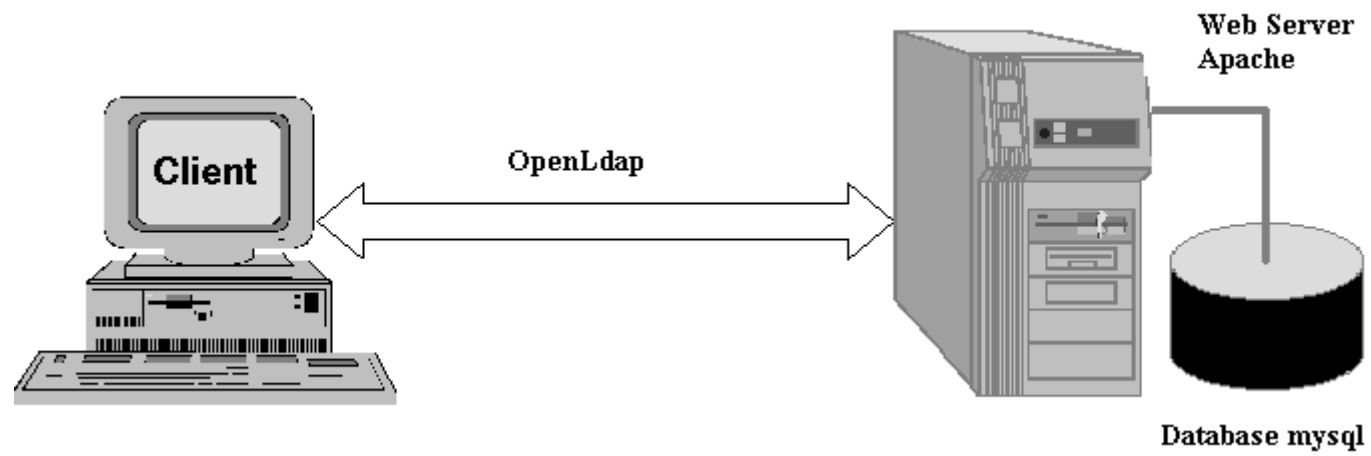
Fase 2



Fase 3



Fase 4



Vigilanza

- Le Certification Authority sono sottoposte ad una rigida regolamentazione e supervisione da parte dello Stato. Il governo italiano è stato il primo a livello europeo, e tra i primi a livello mondiale a darsi una regolamentazione normativa a riguardo, definendo le regole tecniche e logistiche per realizzare una infrastruttura che potesse rilasciare certificati digitali che avessero, ai sensi di legge, la stessa validità di una firma autografa. I certificati devono essere rilasciati da CA iscritte nell'[Elenco Pubblico dei Certificatori](#), diffuso dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA). Tale organismo opera presso la Presidenza del Consiglio per l'attuazione delle politiche del Ministro per le riforme e le innovazioni nella PA, unifica in sé due organismi preesistenti, tra cui l'Autorità per l'Informatica nella Pubblica Amministrazione.

Compiti

- Descriviamo ora a grandi linee i compiti di una CA standard. Il procedimento illustrato è una linea guida che può variare caso per caso:
- identificazione certa di chi richiede la certificazione della chiave pubblica;
- rilascio e pubblicazione del certificato (firmato con la propria chiave privata);
- manutenzione del registro delle chiavi pubbliche;
- revoca o sospensione dei certificati in caso di istanza dell'interessato o in caso di abusi, falsificazioni, ecc e nel contempo aggiornamento della lista pubblica dei certificati sospesi o revocati (certificate revocation list);
- risposta (per via telematica) alle domande di trasmissione dei certificati.
- si occupa periodicamente di pubblicare due liste sul Certificate Server:
- [Certificate Revocation List](#) (CRL)
- [Certificate Suspension List](#) (CSL)

Come ottenere il certificato utente.

- I certificati utente generati da una CA hanno le seguenti caratteristiche:
- Un qualsiasi utente che abbia accesso alla chiave pubblica della CA può ricostruire la chiave pubblica dell'utente cui il certificato si riferisce.
- Nessun altra parte, ad eccezione della CA, può modificare il certificato senza essere scoperta.
- Dato che i certificati non sono falsificabili, possono essere messi in una directory senza adottare particolari precauzioni per la loro protezione.

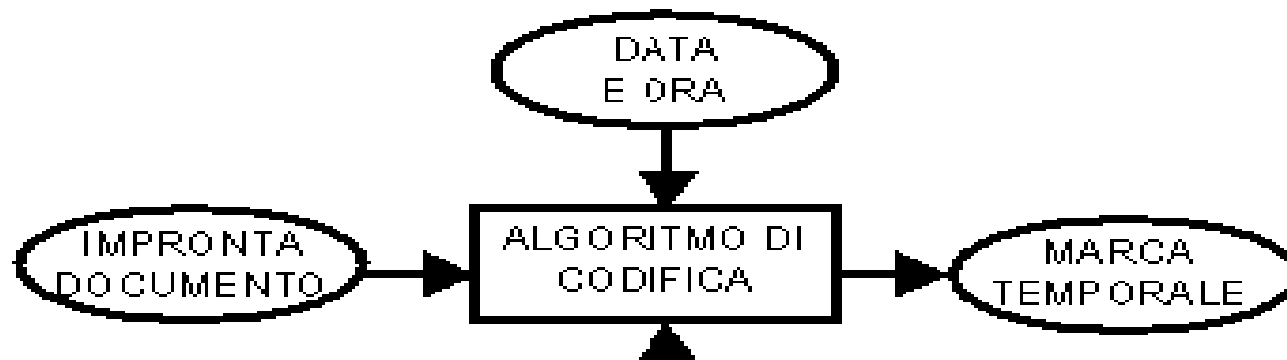
Procedura

- 1 L'utente richiede alla CA la registrazione fornendo la documentazione richiesta da questa per accertare la sua identità.
- 2 Verificata la validità della richiesta, CA attribuisce all'utente un identificatore di cui essa garantisce l'univocità.
- 3 La CA inserisce l'utente con l'identificatore attribuitogli nei cataloghi di utenti registrati che essa gestisce.
- 4 La CA fornisce attraverso un canale sicuro la chiave crittografica che l'utente dovrà utilizzare per le richieste di certificazione delle chiavi e per accedere ai registri dell'autorità.

Marcatura Temporale

- Per **referimento temporale** si intende quella informazione, associata ai documenti oggetto della **conservazione sostitutiva**, che attesta la corretta conclusione di tale processo. In seguito, con l'apposizione della firma digitale tale riferimento viene "bloccato" al contenuto dei documenti a cui si riferisce.

Marcatura Temporale



Marcatura Temporale

- L'impronta del documento viene inviata al servizio di marcatura temporale, l'impronta costituisce un riferimento certo al testo originale ma non ne consente la ricostruzione, pertanto la marcatura può essere effettuata senza compromettere la confidenzialità del testo.
- Il servizio di marcatura aggiunge all'impronta ricevuta la data e l'ora, ottenendo una "impronta Marcata".
- L'impronta marcata viene cifrata con la chiave segreta del servizio, ottenendo la marca temporale da cui è possibile recuperare, mediante la chiave pubblica del servizio, l'impronta del documento e la data e l'ora della sua generazione.
- La marca temporale viene inviata al richiedente il quale la allega al documento.

Smart card

- Le smart cards sono in continua evoluzione ed il costo tende a diminuire.
- Permettono di trasportare in sicurezza le chiavi segrete e di poterle utilizzare in differenti postazioni.
- Molti produttori forniscono software proprietari per la gestione delle carte e dei certificati con molti problemi di interoperabilità.
- Molti progetti Open Source iniziano ad avere strutture consolidate e soluzioni avanzate (PKCS#11)

LA CONSERVAZIONE DIGITALE E' UN PROCESSO COMPLESSO

- Per conservare i documenti digitali non è sufficiente mantenerne il contenuto poiché contenuto e struttura sono ormai del tutto separati e il contesto dell'informazione è vitale alla sua comprensione
- Il paradosso riguarda la ***duplicità contraddittoria*** delle richieste degli utenti:
 - il mantenimento della *forma originaria*, dell'integrità e dell'affidabilità
 - ma anche la garanzia di un *accesso dinamico e interattivo* che inevitabilmente introduce cambiamenti nei documenti, nella loro struttura e nelle relative informazioni descrittive.

I NODI DA SCIOGLIERE

- Il ritardo nel riconoscimento della centralità del problema è grave in tutti gli ambienti
- Il legislatore nazionale ha emanato disposizioni che mancano di coerenza interna e comunque non affrontano il problema nella sua reale dimensione tecnica e organizzativa
- E' indispensabile definire presto **linee d'azione** e **infrastrutture** commisurate alle dimensioni e ai mezzi delle diverse istituzioni di conservazione e delle diverse della produzione documentaria

- La conservazione digitale lungi dal caratterizzarsi come un processo ad esclusivo carattere tecnico dimostra sempre più la sua natura politica:
 - La misura e l'attenzione con cui una comunità saprà e vorrà investire nella conservazione delle memorie (digitali) del presente costituiranno un segno rilevante di civiltà o un'altra significativa prova di inconsapevolezza e ignoranza di cui faremo mostra nei decenni (e, ancor prima, nei mesi e negli anni) che abbiamo di fronte.

Punti di forza

- Accessibilità al codice: l'accesso al codice stesso favorisce una possibile verifica da parte dell'utilizzatore
- Indipendenza della piattaforma: il software, essendo principalmente scritto in linguaggi largamente diffusi disponibili per qualsiasi SO, risulta facilmente portabile.
- Standard: l'utilizzo degli standard lascia la porta aperta ad un alta integrazione con altri sistemi.

Problematiche

- Organizzazione interna: nelle PA ci sono forti limiti nell'utilizzo delle nuove tecnologie basate sul trattamento dei documenti in formato elettronico
- Politiche interne: uno dei maggiori problemi nel proporre servizi di certificazione è l'individuazione delle procedure e responsabili di servizio.
- Inadeguatezza leggi: le leggi attuali spesso risultano essere non adeguate (es. decreto su firme massive)
- Integrazione : l'integrazione e lo sviluppo delle applicazioni richiede tempo ed investimenti

Scopi futuri

- Firme massive: in progetto la possibilità di firmare una grande quantità di documenti con un sistema di firma tipo HSM (Hardware Security Module).

Il dubbio è l'ammissibilità del processo tecnico-giuridico (decreto appena approvato molto complesso e poco chiaro per gli addetti ai lavori)

DPCM_Autocertificazione_HSM_12102007

- È stato pubblicato in Gazzetta Ufficiale il decreto in oggetto, si sancisce che:
“... 1. Per un periodo di ventiquattro mesi decorrente dall’entrata in vigore del presente decreto, i certificatori di firma elettronica attestano, mediante autodichiarazione, la rispondenza dei propri prodotti e dispositivi relativi alle firme elettroniche da apporre con procedure automatiche ai requisiti di sicurezza previsti dalla vigente normativa. ...”

contatti

- Mail : fabrizio.lappa@telecomitalia.it
- Tel : 3316025115