



# *Firma Digitale e Non*

*Clizio Merli*

**(Versione 3)**



# Indice

<b>INDICE .....</b>	<b>2</b>
<b>PREFAZIONE .....</b>	<b>3</b>
<b>LA FIRMA.....</b>	<b>5</b>
FIRMA ELETTRONICA .....	6
FIRMA DEBOLE (SEMPLICE) .....	6
FIRMA FORTE (DIGITALE).....	6
<i>Firma Forte Semplice</i> .....	7
<i>Firma Forte Qualificata</i> .....	7
<i>Firma Forte Avanzata</i> .....	7
<i>Firma Forte Avanzata e Autenticata</i> .....	7
<b>CRITTOGRAFIA, RISERVATEZZA E SPUDORATEZZA .....</b>	<b>8</b>
CRITTOGRAFIA: L'ARTE DELLA RISERVATEZZA .....	8
CRITTOGRAFIA: LE CHIAVI .....	9
CRACKING: L'ARTE DELLA SPUDORATEZZA .....	11
<b>CERTIFICATI E CERTIFICATORI .....</b>	<b>13</b>
I CERTIFICATI E LO SCENARIO DELLA FIRMA DIGITALE.....	13
UNA SOLA FIRMA? .....	15
IL CERTIFICATORE E LE SUE RESPONSABILITÀ .....	16
REQUISITI FORMALI PER IL RILASCIO E LA GESTIONE DEI CERTIFICATI .....	19
CERTIFICATION AUTHORITY: OPERATIVITÀ.....	20
<b>E LA QUARTA DIMENSIONE? .....</b>	<b>22</b>
MARCA TEMPORALE: LA CERTIFICAZIONE DEL TEMPO .....	23
UNA SORGENTE TEMPORALE GLOBALE E GRATUITA: IL PROTOCOLLO NTP.....	23
TSA, TSQ E TSR .....	24
MARCA TEMPORALE: LO STANDARD RFC 3161.....	25
<b>UN PO' DI COMPLICAZIONI: CADES, PADES, XADES, E MARCHE TEMPORALI.....</b>	<b>28</b>
LE MATRIOSKE, LE FIRME CONGIUNTE .....	28
... E LE CONTROFIRME .....	30
LA UE E L'ADES .....	31
COME ACCOPIARE DOCUMENTI E MARCHE TEMPORALI: M7M E TSD .....	34
<b>UN PO' DI TECNOLOGIA: PKI.....</b>	<b>35</b>
ARCHITETTURA GENERALE E COMPONENTI .....	35
<b>MAPPA DEGLI STANDARD.....</b>	<b>39</b>

## Prefazione

Sono anni che medito di scrivere un libro sulla firma digitale: grazie alla mia pigrizia atavica questo è per ora il modestissimo risultato. Se la mia speranza di una lunga vita si avvererà, forse le generazioni future avranno il privilegio (!?!) di leggere il libro completo. Per ora i poveri lettori devono accontentarsi di queste poche pagine, nella speranza, alla fine di una rapida lettura, di aver avuto finalmente la possibilità di capire meglio cosa significa la firma digitale, e con il rischio di essersi ulteriormente complicate le idee.

La prima versione di questo libretto risale al 2005. Dopo cinque anni di profonda meditazione ho aggiunto il capitolo relativo alla marca temporale (sei pagine), e dopo altri due ho ritoccato qua e là per tentare di chiarire, nel limite del possibile, gli arcani legati alle ultime normative europee e italiane (CADES, PadES, XadES, TSR, TSD e altre chicche).

Comunque questo che state leggendo ha la pretesa di essere un piccolo contributo chiarificatore alla comprensione del mondo che ruota intorno alla firma digitale.

Da anni si parla ormai di questo argomento, e delle mirabilia annesse e connesse. Nella pratica, sino ad ora (anno 2011) gli unici effetti visibili al grosso pubblico, perlomeno in ambito Italiano, sono due: la chiavetta che si chiude nei browser navigando in Internet, segnalando in tal modo che si entra in "siti protetti" (da cosa?); le SmartCard e le chiavette crittografiche USB rilasciate dagli enti certificatori accreditati e utilizzati dalle aziende prevalentemente per lo scambio con l'Agenzia delle Entrate.

Per le aziende non è cambiato molto rispetto alle prime SmartCard rilasciate nei primi anni 2000 dalle Camere di Commercio per la firma digitale aziendale delle dichiarazioni dei redditi, (quelle che erano finite, quasi tutte, nelle casseforti dei commercialisti insieme alle relative password protettive - PIN). Ben poca cosa per una innovazione che avrebbe permesso, almeno potenzialmente, di eliminare gran parte della carta all'interno di organizzazioni, aziende, enti, con risparmi sensibili sia in termini economici che ecologici.

La realtà è più complessa e articolata. Diversi progetti, su scala nazionale e locale, sono in fase avanzata di realizzazione, e stanno preparando un tessuto normativo, tecnologico e organizzativo di tutto rispetto. Ma non siamo ancora arrivati al punto di innesco della reazione a catena che porterà la firma digitale a trovare una applicazione diffusa e capillare. Manca la scintilla che può scatenare la reazione, e le informazioni disponibili sono tante, frammentarie e scoordinate.

Navigando in Internet sino a qualche anno fa i motori di ricerca ritornavano uno sproloquio di siti in cui si trovava di tutto e di più, ma soprattutto miriadi di personaggi esoterici (praticoni, pseudo-esperti, maghi, chiaccheroni, avvoaticchi, aiuti contabili e simili ammenicoli) che parlavano a sproposito di algoritmi di firma, di chiavi pubbliche e segrete, di credenziali di firma, di verifica, e di tante altre cose, senza sapere di cosa stessero effettivamente parlando.

E pure avari di notizie erano i fornitori delle tecnologie sviluppate a corredo della firma digitale: SmartCard, lettori di SmartCard (che in effetti permettevano anche di scriverle, ma nessuno lo diceva), HSM, software di firma e di verifica, PKI, prodotti aderenti a tutti gli standard del pianeta (che come risultato immediato spesso non riuscivano nemmeno a essere interoperabili, ovvero compatibili, con sé stessi).

Oggi la situazione è in parte migliorata (i venditori delle bancherelle Internet sono finiti nelle ultime pagine dei motori di ricerca), ma in quanto a chiarezza ancora poca – il discorso si sta spostando sulle dematerializzazione, la Conservazione Sostitutiva, la PEC, ... – ma la firma digitale continua ad essere una grande sconosciuta, e come tale una cosa che forse è meglio evitare.

In mezzo a questo baluginare di sigle, discorsi, articoli, l'unica cosa che forse si riesce a capire, è che in un mondo sempre più rivolto all'open-source una pletera di non ben definiti professionisti e aziende stanno operando ancora in base al più misero approccio proprietario<sup>1</sup>. Alla faccia della tanto decantata democrazia elettronica, di cui la firma digitale dovrebbe essere una delle punte di diamante!

Pessimismo a parte, la firma digitale rappresenta una sfida formidabile (come dicono i cuginetti di oltre oceano). Credo sia giunto alfine il momento di accettarla ...

*Clizio Merli*

---

<sup>1</sup> Mi è capitato anche di interagire con distributori che dovevano chiedere il permesso alla società costruttrice per rispondere a domande banali, quali le caratteristiche di performance di firma, o la tipologia di interfacce standard supportate dai loro prodotti.

## La firma

La firma è un'assunzione di paternità, di un documento, un'asserzione o un evento.

La nostra vita è stata sempre caratterizzata da una continua apposizione di firme olografe su documenti cartacei, sia da parte nostra che dei nostri partner. Un fatto che da sempre comporta l'accumulo smisurato di "pezzi di carta" raccolti nei nostri archivi personali, negli archivi pubblici, nelle biblioteche e musei, negli archivi aziendali.

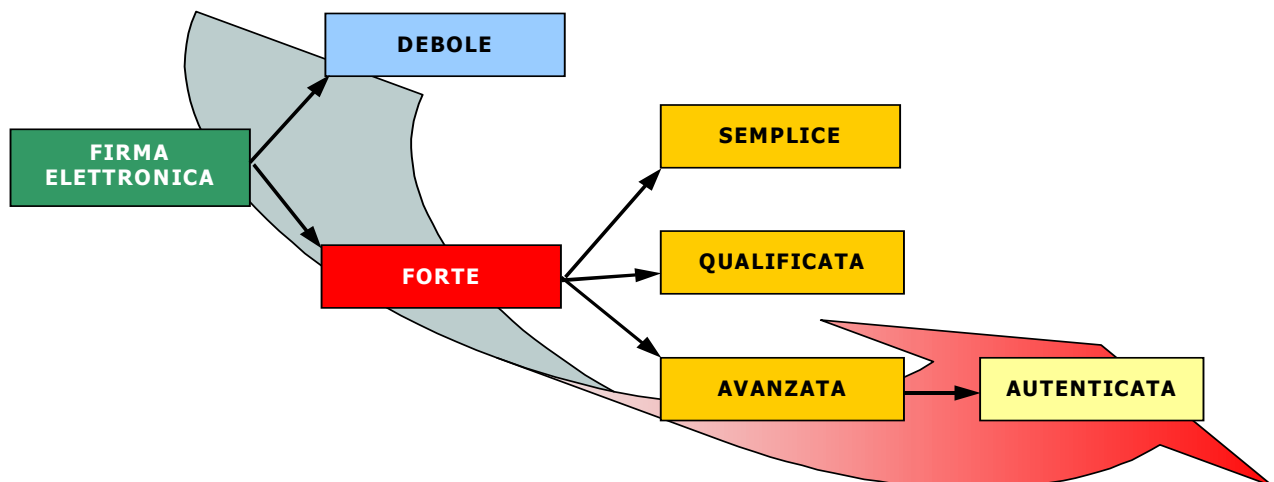
La cosa ha sicuramente un sapore romantico, specialmente per chi ama i libri e la lettura (come ad esempio chi scrive). Ma la stragande maggioranza dei pezzi di carta che firmiamo ha ben poco di romantico: scontrini delle carte di credito, richieste di ferie, documenti bancari, documenti aziendali, e altre amenità di questo tipo, per le quali sprechiamo tonnellate di carta, con buona pace delle foreste amazzoniche e delle altre depauperate zone pluviali del nostro amato pianeta.

Sin dall'avvento dei computer i vari *guru* dell'informatica hanno coltivato un sogno nel cassetto: trasformare i documenti cartacei in documenti elettronici, facili da archiviare, classificare, analizzare, ricercare. Un sogno che si è ulteriormente enfatizzato con l'avvento delle reti e con l'esponenziale aumento della capacità dei supporti di memorizzazione. Un sogno costantemente frustrato dalla impossibilità di apporre una firma sui documenti elettronici. Perché generare documenti elettronici è facile, ma difficile è associarli ai loro autori, garantire la loro effettiva paternità, e la paternità degli atti che da questi documenti derivano.

Con l'avvento delle tecnologie di firma elettronica e digitale questo sogno può uscire dal cassetto.

Affidandosi alla scienza della comunicazione, e alle tecnologie informatiche che ne sono derivate, il concetto di firma di documenti elettronici ha trovato varie forme di implementazione e applicazione, che sono state man mano analizzate e codificate, sia dal punto di vista tecnico che di scambi umani, e quindi legale.

Lo schema seguente illustra la classificazione cui si è arrivati nel corso degli anni, e che trova una sua codificazione nella normativa internazionale, ed europea in particolare.

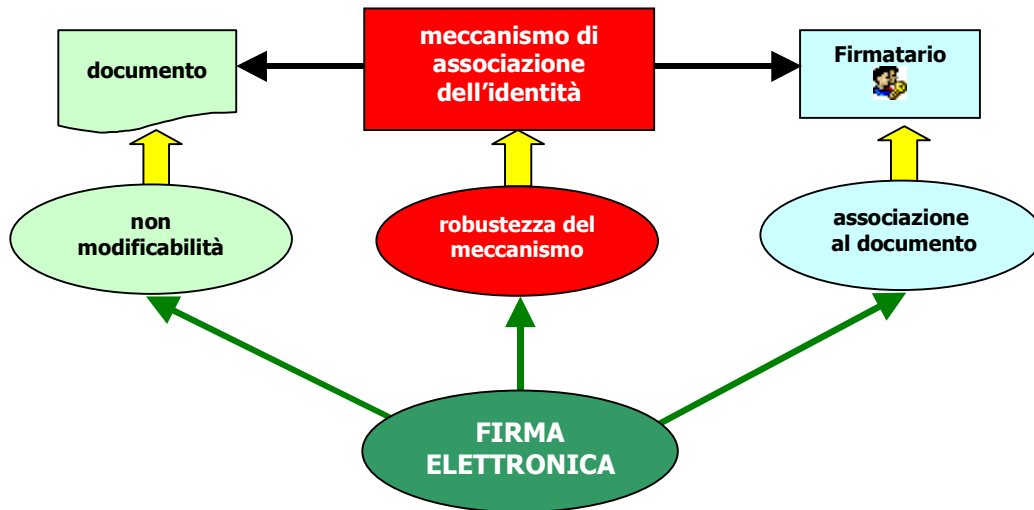


Proviamo ad analizzare il significato dei rettangolini di questa figura.

## Firma elettronica

**L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ed altri dati elettronici, utilizzati come metodo di autenticazione.**

Questa definizione comprende qualunque meccanismo di associazione dell'identità di una persona (firmatario) ad un documento. La successiva classificazione in Firma Debole e Forte dipende dalla robustezza del meccanismo utilizzato, dalla possibilità di associare in modo non violabile l'identità del firmatario ai dati firmati, e dalla possibilità di rendere non modificabili a posteriori i dati firmati.



## Firma Debole (Semplice)

**Qualunque meccanismo informatico orientato ad associare l'identità di una persona a un insieme di dati registrati in formato elettronico (file di log, tecniche di crittografia a chiave semplice, ...).**

Ha un valore probatorio proporzionale alle caratteristiche oggettive intrinseche della qualità e della sicurezza del meccanismo adottato. La firma elettronica è in grado di fornire una prova circa la provenienza del documento ma non circa l'integrità del suo contenuto. Un documento elettronico sottoscritto con firma debole ha un'efficacia probatoria assimilabile a quello di un documento tradizionale munito di semplice sottoscrizione non riconosciuta. Ciò significa che colui contro cui è prodotto il documento può disconoscerlo, e provarne la provenienza e l'integrità del contenuto è a carico di chi intende avvalersene.

## Firma Forte (Digitale)

**Firma elettronica ottenuta in base alla applicazione di un sistema di chiavi asimmetriche (pubblica e segreta), che consente al firmatario di associare prova della propria identità e garantire al tempo stesso l'integrità dei dati firmati.**

I meccanismi di firma forte sino ad ora elaborati e implementati si basano tutti sul principio della crittografia a chiavi asimmetriche, l'unico sinora noto in grado di supportare la prova di identità del firmatario e la non violabilità (ovvero l'integrità) dei dati firmati. In futuro potrebbero essere scoperti e implementati altri meccanismi di eguale o maggiore robustezza.

Inoltre la prova di identità del firmatario richiede ulteriori meccanismi che permettano di associare univocamente le chiavi asimmetriche di firma a una persona specifica. Questi meccanismi non sono, e non possono essere, solo informatici, ma devono coinvolgere la normativa del **Gruppo di Utenza** cui sono rivolti. Quindi per una validità certa su scala nazionale, europea o internazionale, i meccanismi devono essere supportati da norme (leggi) valide su scala nazionale, europea o internazionale<sup>2</sup>.

In base alla robustezza dei meccanismi di firma e dei meccanismi di supporto alla prova di identità del firmatario la Firma Forte viene ulteriormente suddivisa in:

- Firma Forte Semplice
- Firma Forte Qualificata
- Firma Forte Avanzata
- Firma Forte Avanzata e Autenticata

### Firma Forte Semplice

- il meccanismo di apposizione della firma digitale non è sufficientemente sicuro, in quanto il mantenimento delle credenziali<sup>3</sup> di firma digitale può essere violato, **oppure**
- l'identificazione univoca del firmatario è garantita con ragionevole certezza solo nell'ambito di gruppi di utenti limitati (all'interno di organizzazioni, aziende, enti), ma non ha valore pubblico nè legale al di fuori del gruppo in cui viene riconosciuta.

### Firma Forte Qualificata

- il meccanismo di apposizione della firma digitale è sufficientemente sicuro, in quanto il mantenimento delle credenziali di firma digitale non può essere violato, **e**
- l'identificazione univoca del firmatario è garantita con ragionevole certezza nell'ambito di gruppi di utenti su scala europea, ma non ha valore per gli enti pubblici in quanto l'entità che garantisce l'identificazione si è autocertificata (non ha ottenuto una certificazione da parte di un ente di certificazione pubblica riconosciuto a livello europeo).

### Firma Forte Avanzata

- il meccanismo di apposizione della firma digitale è sufficientemente sicuro, in quanto il mantenimento delle credenziali di firma digitale non può essere violato, **e**
- l'identificazione univoca del firmatario è garantita con ragionevole certezza nell'ambito di gruppi di utenti su scala europea, con valore anche per gli enti pubblici in quanto l'entità che garantisce l'identificazione ha ottenuto una certificazione da parte di un ente di certificazione pubblica riconosciuto a livello europeo.

### Firma Forte Avanzata e Autenticata

- firma forte avanzata la cui **apposizione viene autenticata da un notaio o da altro pubblico ufficiale autorizzato**. L'autenticazione della sottoscrizione consiste nella dichiarazione del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il documento sottoscritto con questo tipo di firma ha la stessa valenza probatoria della scrittura privata autenticata. L'efficacia probatoria è limitata all'elemento intrinseco della sottoscrizione (la provenienza del documento), senza alcuna interferenza sul contenuto della scrittura (la provenienza della dichiarazione).

---

<sup>2</sup> Al momento il massimo grado di validità legale è quella europea (direttiva 1999/93/CE), che a livello nazionale è stata recepita da tutte le norme emanate dall'anno 2000 in poi.

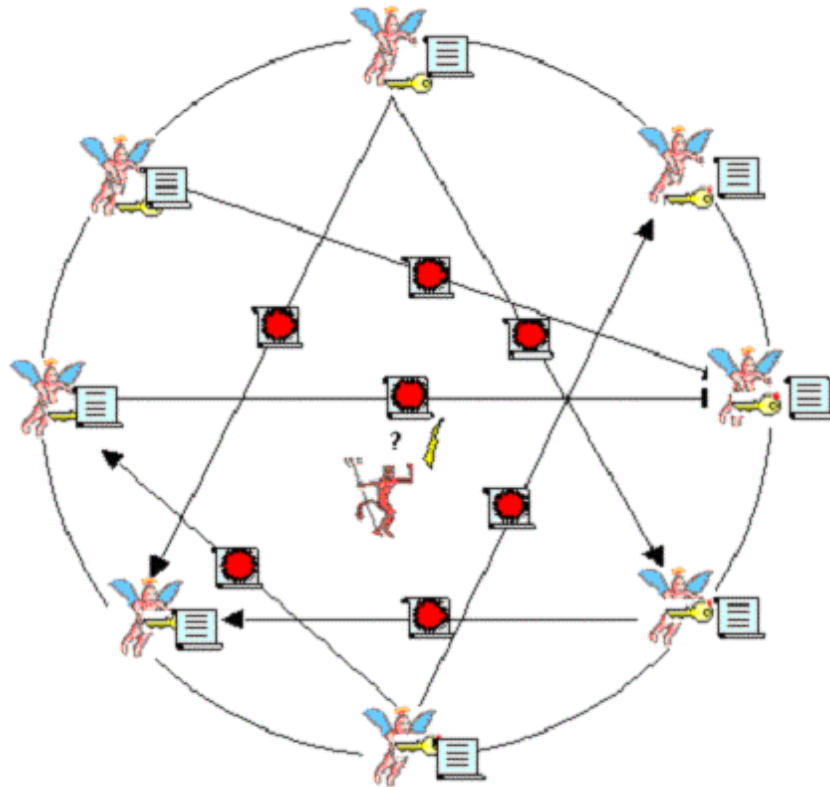
<sup>3</sup> Il termine 'credenziali di firma' indica l'insieme delle informazioni di identità e di calcolo necessarie a eseguire il meccanismo di firma digitale (vedi capitolo successivo).

# Crittografia, Riservatezza e Spudoratezza

## Crittografia: l'arte della riservatezza

Crittografare un documento significa codificarlo in modo tale che risulti illeggibile a chi non conosce il meccanismo di codifica.

Lo scenario tipico è rappresentato da un gruppo di persone (entità) che vogliono comunicare tra di loro in modo riservato, senza che entità terze (aliene) possano capire il significato dei messaggi scambiati all'interno del gruppo.



Tenuto conto che ogni messaggio è una sequenza di caratteri, e che ogni carattere è rappresentabile in un numero compreso tra 0 e 255 (ovvero un byte), un meccanismo di codifica (crittografia) altro non è che una funzione matematica che permette di convertire la sequenza di caratteri che compone un messaggio (ovvero una sequenza di numeri) in una sequenza di caratteri (numeri) modificati. Il risultato è un nuovo messaggio che risulta incomprensibile a chiunque lo legga.

Ovviamente un meccanismo di semplice codifica non serve a nulla senza un meccanismo complementare di decodifica, ovvero una funzione matematica che permette di convertire il messaggio codificato nel messaggio originale.

Cosa distingue il meccanismo di codifica dal meccanismo di decodifica?

Su questo punto i matematici offrono, al momento, due possibili risposte:

1. l'utilizzo di **due funzioni matematiche** differenti, ma complementari, associate a **un solo parametro numerico**, detto **chiave** di codifica/decodifica;
2. l'utilizzo di **una sola funzione matematica** associata a **due parametri numerici** differenti ma complementari, detti rispettivamente **chiave di codifica** e **chiave di decodifica**.

In entrambi i casi i matematici ci offrono una soluzione con componenti di due tipi:

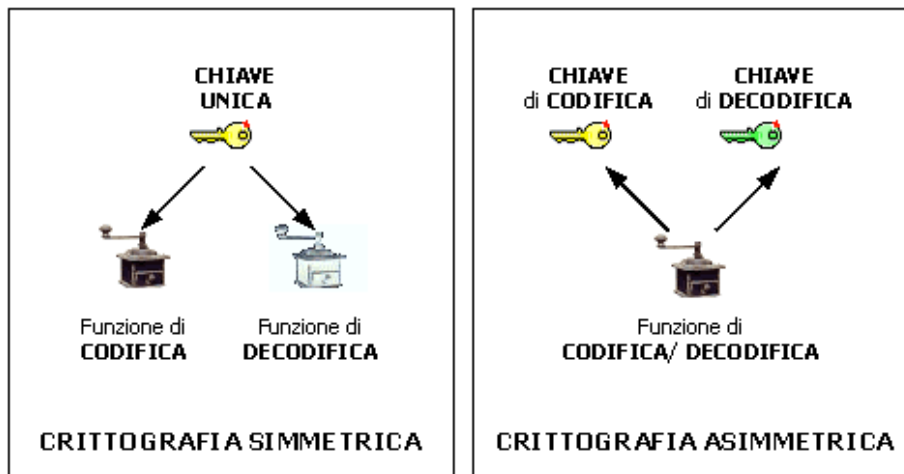
- funzione matematica
- parametro numerico (chiave)

in due possibili combinazioni:

- due funzioni e una chiave
- una funzione e due chiavi.

Poiché il vero problema non sono le funzioni matematiche in gioco, ma le chiavi:

1. nel primo caso si parla di **crittografia simmetrica** (o a chiavi simmetriche – **una sola chiave**),
2. nel secondo caso si parla di **crittografia asimmetrica** (o a chiavi asimmetriche - **due chiavi differenti**).



## Crittografia: le chiavi

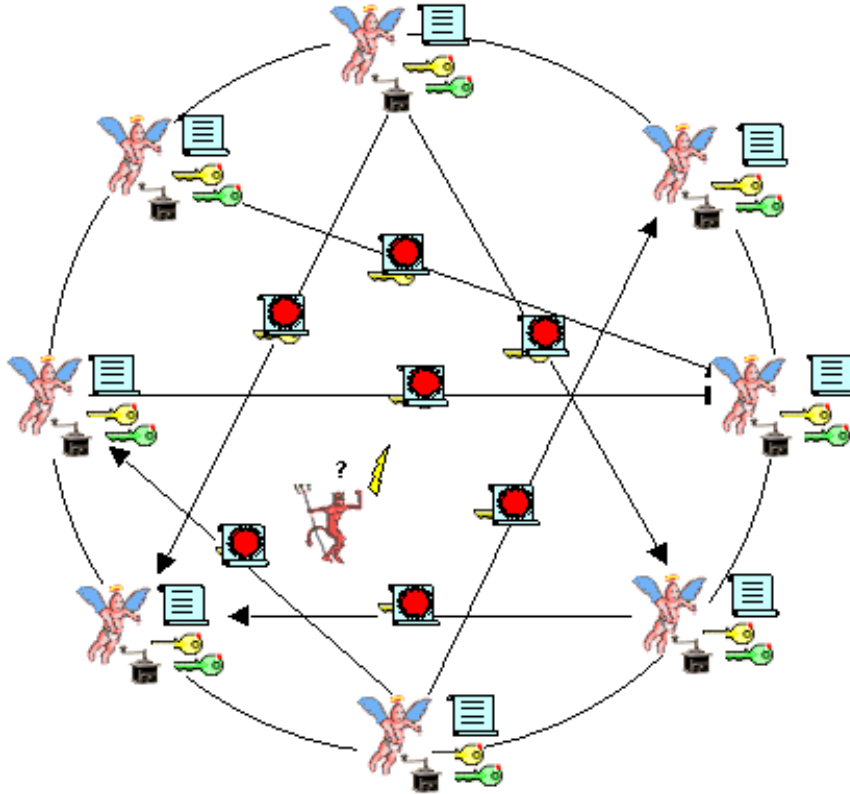
Perché il vero problema è rappresentato dalle chiavi e non dalle funzioni?

La risposta è di tipo economico.

Creare nuove chiavi è un processo poco costoso, che può essere ripetuto più e più volte senza particolari problemi. Per contro sviluppare una funzione di crittografia è un processo costoso, e non è ipotizzabile lo sviluppo di una nuova funzione per ogni messaggio che deve essere trasmesso.

Ora nel primo caso (crittografia simmetrica), sia le chiavi che le funzioni utilizzate devono essere conosciute a tutte le entità del gruppo. Purtroppo quando si trasmettono le chiavi a tutte le entità si corre il rischio che entità terze (aliene) intercettino la chiave, vanificando lo sforzo di rendere sicura e riservata la comunicazione.

Nel secondo caso (crittografia asimmetrica), questo problema non si pone, in quanto ogni entità del gruppo crea due chiavi: una viene comunicata a tutte le altre entità, e una viene mantenuta rigorosamente segreta. La chiave trasmessa a tutti è di fatto pubblica. In virtù di questo fatto la crittografia asimmetrica viene anche detta crittografia a chiavi pubbliche.



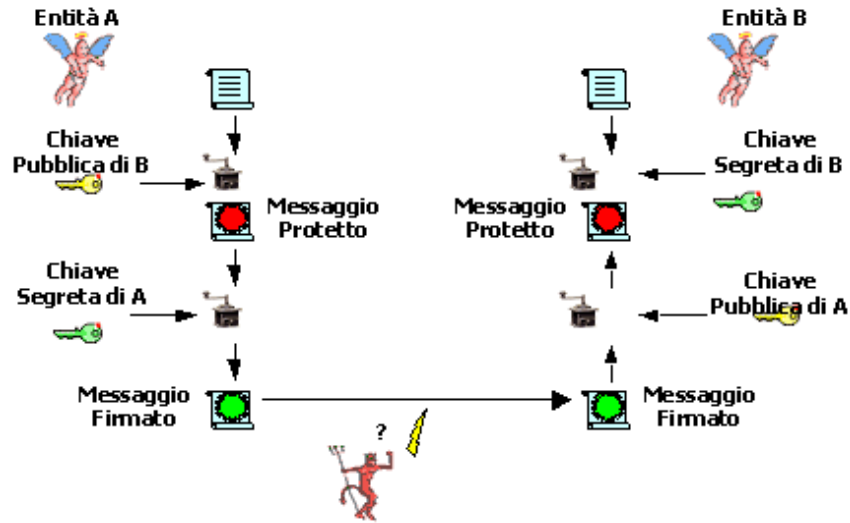
L'uovo di Colombo!

Non proprio.

Quando una entità trasmette a tutte le altre la propria chiave pubblica, deve corredarla di alcune informazioni relative alla propria identità (nominativo). Ora se una entità aliena si maschera da entità del gruppo e trasmette una chiave pubblica falsa dotata di un nominativo vero, le altre entità del gruppo possono essere tratte in inganno, ed essere convinte di parlare con una entità buona invece che con l'aliena.

Tuttavia la crittografia asimmetrica ci offre una possibilità in più rispetto alla crittografia simmetrica. Se al momento di trasmettere un messaggio, dopo aver codificato il messaggio con la chiave pubblica del destinatario (in modo tale che solo lui possa decodificarlo con la propria chiave segreta), codifichiamo ulteriormente il messaggio con la nostra chiave segreta, il destinatario non solo ha la ragionevole certezza che nessun altro ha letto il messaggio durante la trasmissione, ma ha anche la ragionevole certezza che ad inviarlo siamo stati proprio noi, in quanto riesce a decodificarlo con la nostra chiave pubblica (che lui possiede) solo se lo abbiamo codificato noi con la nostra chiave segreta (che solo noi possediamo).

Questo piccolo (!) accorgimento è di fatto una firma, la nostra firma.



## Cracking: l'arte della spudoratezza

Le entità aliene, pur di leggere il contenuto dei messaggi scambiati in modo protetto tra le entità di un gruppo, possono adottare vari stratagemmi matematici, per capire il tipo di crittografia utilizzato, e possibilmente le chiavi utilizzate. Questi stratagemmi sono noti come **meccanismi di cracking**.

La probabilità di successo di un meccanismo di cracking è:

- direttamente proporzionale alla bravura matematica dell'entità aliena
- inversamente proporzionale alla bravura matematica di chi ha studiato la funzione di crittografia (ovvero il crittografo).

Se vogliamo esprimere la cosa matematicamente:

$$P_{\text{cracking}} = k \cdot \frac{B_{\text{alieno}}}{B_{\text{crittografo}}}$$

dove 'k' è una costante.

Per quanto riguarda la crittografia simmetrica bisogna considerare che l'entità aliena può sprotteggere i messaggi codificati catturando le chiavi al momento della loro trasmissione tra le varie entità del gruppo. A questo riguardo bisogna dire che nel corso degli anni sono stati sviluppati e messi a punto vari meccanismi di distribuzione delle chiavi, ma tutti con una dose di rischio non nulla.

Nel caso della crittografia asimmetrica invece il problema della distribuzione delle chiavi non si pone, ma purtroppo i matematici sono come il diavolo: fanno le pentole ma non sempre si ricordano di fare anche i coperchi.

Le funzioni per la crittografia asimmetrica si basano sulla teoria dei numeri primi, e l'unico tentativo di cracking che si può mettere in atto è quello di operare con tecniche di fattorizzazione (che permettono di trovare tutti i numeri primi per cui è divisibile la chiave pubblica).

La fattorizzazione è un processo la cui efficienza diminuisce molto rapidamente al crescere della dimensione della chiave, e poiché sinora nessuno ha messo a punto un algoritmo di fattorizzazione efficiente per grandi numeri il trucco (!) è quello di utilizzare chiavi di grandi dimensioni.

Agli albori della crittografia asimmetrica (inizio degli anni '80) i numeri decimali di cento e più cifre erano praticamente non fattorizzabili con i computer di allora. Cento cifre decimali corrispondono, grosso modo, a 512 bit, per cui inizialmente si utilizzavano chiavi a 512 bit. Con l'aumentare della potenza di calcolo dei computer, e con la diffusione di personal computer sempre più potenti, il fattore di rischio è aumentato, e si è così passati a chiavi da 1024, 2048 e 4096 bit.

Ovviamente non tutte le entità aliene sono così brave matematicamente da cimentarsi in laboriosi tentativi di fattorizzazione. Ma sprotteggere il contenuto dei messaggi trasmessi non è l'unico modo di turbare il processo comunicativo di un gruppo. Anche alterare il normale scambio di messaggi, riuscendo a farsi passare per una entità amica, è un modo efficace di violare il normale scambio di messaggi.

Poiché la crittografia asimmetrica richiede che le chiavi pubbliche siano effettivamente tali, e quindi conosciute a tutti, il problema si sposta sul piano della certificazione, ovvero di meccanismi che permettono di distribuire le chiavi pubbliche associate in modo sicuro al nominativo dell'entità che le ha generate e a cui corrispondono.

Qui, per fortuna, ci vengono in aiuto gli standard di comunicazione, e in particolare gli standard della cosiddetta pila ISO/OSI. In particolare il gruppo di standard denominato X.500, che copre le problematiche dello scambio di messaggi in una rete. Il nono standard di questa serie (X.509) definisce una sorta di **certificato di identità elettronico**, ovvero un file costituito da un certo numero di campi, che permettono di conoscere con ragionevole certezza l'identità di una entità e la relativa chiave pubblica: il tutto certificato da una entità super-partes che svolge una funzione di notaio, ovvero attesta che quanto riportato nel certificato corrisponde a verità, una entità che chiamiamo **Autorità Certificante** (o più comunemente, con il termine inglese **Certification Authority**).

Cosa garantisce che è stata proprio la nostra Certification Authority a rilasciare il certificato di un'altra entità? Il fatto che la Certification Authority ha firmato il certificato con la propria chiave segreta, e ha accluso al certificato il proprio nominativo e la propria chiave pubblica (in parole povere il proprio certificato, ovvero un documento elettronico in cui la Certification Authority attesta di essere proprio lei - un inizio ci dovrà pur essere!).

Ovviamente il certificato della Certification Authority dovrà essere distribuito a tutti (reso pubblico) in modo certo e garantito. Ma chi garantisce tutto ciò? Un'altra autorità? Ma allora non si finisce più.

Come diceva il buon vecchio Shannon la sicurezza assoluta non esiste, a meno di non utilizzare una quantità infinita di informazione ridondante per certificare il tutto. Ma ahimè, noi siamo finiti ...<sup>4</sup>

---

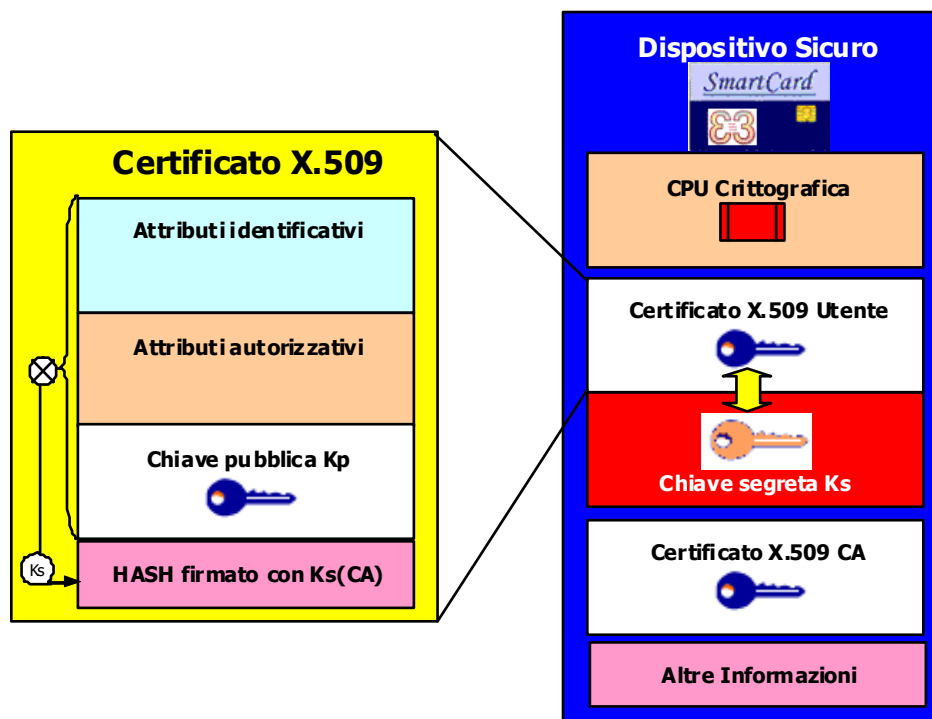
<sup>4</sup> Almeno per ora!

# Certificati e Certificatori

## I Certificati e lo Scenario della Firma Digitale

Quando si parla di certificati di firma digitale si compie spesso l'errore di credere che la firma digitale di un documento elettronico sia effettuata con il solo utilizzo del certificato.

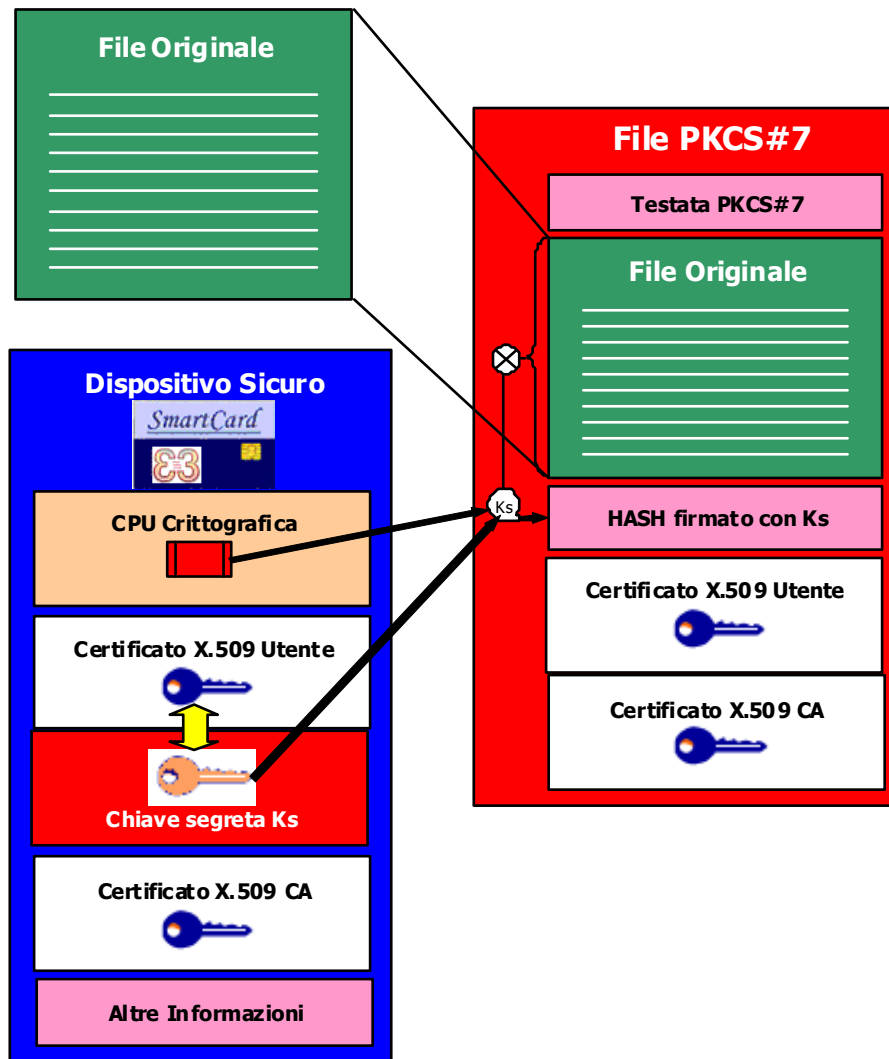
Un certificato di firma digitale è un **contenitore** che permette di **associare una chiave pubblica a un soggetto**: il processo di firma digitale viene invece effettuato con il concorso della chiave segreta associata. Lo scenario complessivo è leggermente più complicato, e vede coinvolti tanto il certificato (con la chiave pubblica in esso contenuta), quanto la chiave segreta: il tutto con il supporto del dispositivo sicuro di firma digitale, come illustrato nella figura seguente.



Il formato dei certificati di firma digitale è definito dallo standard internazionale X.509, con la struttura illustrata in figura. Le chiavi generate (**Kp** e **Ks**) sono numeri interi molto grandi (rappresentabili con almeno 100 cifre decimali, ovvero 512 bit – cifre binarie): allo stato tecnologico attuale si opera con chiavi di almeno 1024 bit per i certificati dei titolari e 2048 bit per i certificati dei certificatori.

Il processo di firma digitale di un documento elettronico (ovvero di un file) è regolato dallo standard PKCS#7<sup>5</sup>, e dalle sue estensioni: obiettivo del processo è la generazione di un file in formato PKCS#7 (detto anche busta PKCS#7) contenente il file originale, la sua impronta (hash) firmata digitalmente con la chiave segreta **Ks**, il certificato del firmatario (con la chiave pubblica **Kp**) e il certificato del certificatore (CA – Certification Authority) che ha emesso il certificato del firmatario. La figura seguente illustra il formato di un file PKCS#7.

<sup>5</sup> Gli standard PKCS (Public Key Cryptographic Standards), numerati da 1 a 15, sono standard de-facto definiti da RSA Inc., che coprono vari aspetti della crittografia a chiavi asimmetriche: lo standard PKCS#7 definisce la struttura dei file firmati digitalmente. Questi standard industriali (de-facto) sono stati acquisiti e fatti propri, nel corso degli anni, dagli standard pubblici (de-iure) che regolano il mondo di Internet: gli RFC (Requests For Comments). In particolare il PKCS#7 è stato fatto proprio dagli standard dall'RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5), e dalle sue successive edizioni (RFC 3369, RFC 3852).



Il processo di firma digitale vede coinvolte due CPU: quella del computer dell'utente, su cui risiede il file da firmare e che connette il dispositivo sicuro di firma, e quella del dispositivo sicuro di firma (SmartCard, HSM). Il processo si articola nei seguenti passi:

1. La CPU del computer costruisce una busta PKCS#7 vuota (comprendente solo la testata: nome del file originale, identificativi degli algoritmi crittografici utilizzati, lunghezza del file da firmare, ...).
2. La CPU del computer appende il file originale alla testata PKCS#7, e contestualmente calcola l'HASH<sup>6</sup> (impronta) mediante un algoritmo di randomizzazione (SHA1, MD5, ...).
3. La CPU crittografica del dispositivo sicuro codifica l'impronta del file con la chiave segreta **Ks** protetta al suo interno.
4. La CPU del computer appende l'impronta firmata in coda al file originale nella busta PKCS#7, seguita dal certificato X.509 dell'utente (firmatario) e dal certificato X.509 del certificatore (CA) che ha emesso il certificato del firmatario.

Il file PKCS#7 che si ottiene alla fine del processo è il corrispondente firmato del file elettronico originale.

<sup>6</sup> Le tecniche di hashing, o randomizzazione, si basano su formule matematiche che permettono di ottenere da una sequenza di bit di dimensioni qualunque (ovvero da un file) una sequenza di bit (HASH) di dimensione fissa (ad esempio 160 bit, 20 byte): caratteristica delle formule di hashing è l'alto grado di variabilità dell'HASH a fronte di minime modifiche (anche di un solo bit) del file originale, garantendo in tal modo la possibilità di evidenziare alterazioni anche minime del file originale con una spesa di calcolo limitata.

Chiunque voglia accedere al file originale a partire dal file firmato deve effettuare il processo detto di **verifica** (o impropriamente in gergo tecnico, di **sfirma!**), che si articola nei seguenti passi:

1. La busta PKCS#7 viene aperta, estraendo gli algoritmi di firma (hashing e crittografia asimmetrica), il nome e la lunghezza del file originale.
2. Viene poi estratto il file originale, e copiato in un file esterno.
3. Viene ricalcolato l'HASH (impronta) del file originale, ottenendo l'impronta in chiaro.
4. L'HASH firmato contenuto nella busta PKCS#7 viene estratto unitamente al certificato X.509 del firmatario e al certificato X.509 del certificatore (CA).
5. L'HASH firmato viene decodificato con la chiave pubblica **Kp** contenuta all'interno del certificato del firmatario: se il risultato è uguale all'HASH ricalcolato al passo 3 il file originale all'interno della busta PKCS#7 è integro.
6. Viene infine verificata l'integrità del certificato del firmatario, con un meccanismo analogo ai passi 1-5 applicato al certificato del firmatario utilizzando la chiave pubblica del certificatore estratta dal suo certificato.
7. Accedendo via rete al sito del certificatore si può verificare infine la bontà del certificato del firmatario, concludendo in tal modo il processo di verifica.

## Una sola firma?

Quando firmiamo un documento cartaceo, possiamo apporre più di una firma, con diversi significati.

Nella maggior parte dei casi si applica una sola firma. Ciò avviene quando scriviamo un documento che mandiamo a qualcuno: lo scriviamo e ce ne assumiamo la paternità (lo firmiamo), e poi se ce ne ricordiamo lo spediamo alla controparte. In tal caso si parla di **firma singola**.

Ma quando stipuliamo un contratto, in cui (per definizione) si hanno due o più contraenti, le parti in gioco che devono fare proprio il documento sono tutti i contraenti. Quindi si hanno più persone che firmano, in modo congiunto: al documento si applicano **firme congiunte**.

Ma quando operiamo in un contesto complesso, come quello di una azienda, si può avere la necessità di dimostrare alla controparte l'effettivo ruolo che svolgiamo all'interno della nostra azienda. In tal caso la nostra firma viene in qualche modo convalidata da una funzione aziendale di ordine superiore: alla nostra firma viene applicata una **controfirma**.

Ad esempio, se chi scrive è un funzionario dell'ufficio acquisti che si rivolge a un fornitore, può essere necessario assicurare alla controparte che lo scrivente è effettivamente autorizzato a formulare certe proposte: la controfirma del direttore generale alla firma del funzionario serve a convalidare il fatto che lo scrivente ricopre effettivamente quella funzione (non quanto ha scritto). Il bello è che anche una controfirma può essere controfirmata (nel nostro esempio la controfirma del direttore generale può essere controfirmata dall'amministratore delegato): e, ipoteticamente, senza soluzione di continuità, creando una vera e propria albero di firme e controfirme sul nostro bel documento.

Poi da sempre ci hanno insegnato che quando scriviamo qualcosa dobbiamo mettere un riferimento temporale (vi ricordate la data sui primi temi che scrivevamo alle elementari?).

Un documento ha una data. Ma anche la singola firma può avere una data (documento del 21 gennaio, firmato in data 23 gennaio ...). Quindi nello scenario di riferimento della firma è necessario prevedere anche i riferimenti temporali, sia del documento che delle singole firme. Ma di questo ne parliamo un po' più avanti, dopo aver disquisito della quarta dimensione.

## Il Certificatore e le sue Responsabilità

Il sistema crittografico su cui si basa la firma digitale non è sufficiente da solo a garantire l'autenticità della firma, ovvero la sua paternità. La firma digitale, infatti, non garantisce l'identificazione personale dell'autore del documento, il quale potrebbe approfittare dell'impersonalità della firma al fine di spacciarsi per un'altra persona o per un individuo inesistente. L'affidabilità del processo di firma digitale è garantito solo dall'intervento di una "terza parte fidata" (trusted third part), generalmente nota come **Certification Authority**, in italiano il "**certificatore**"<sup>7</sup>.

L'elemento più importante, per la certezza dell'identità del mittente e dell'integrità del testo, è l'affidabilità dei certificatori, soggetti che certificano le persone fisiche. Una affidabilità che deve essere garantita nell'ambito dell'insieme di persone che sono interessate a cooperare con le garanzie del certificatore: insieme che viene indicato con il termine di **Gruppo Chiuso di Utenza**. Quando si parla di firma digitale e di certificatori si fa sempre riferimento a un Gruppo Chiuso di Utenza: una organizzazione, una azienda, un ente, una regione, una nazione, una unione di nazioni, il mondo intero: ma sempre un numero finito di persone!

E' indispensabile che i certificatori siano soggetti assolutamente scrupolosi e fidati e, in qualche modo, a loro volta certificati nell'ambito del loro Gruppo Chiuso di Utenza, al fine di evitare che dalla massima sicurezza consentita dalla crittografia a chiavi asimmetriche, si passi alla massima insicurezza che deriva dalla malafede, o più semplicemente dalla negligenza, aggravate dall'impossibilità di "distinguere i bit veri dai quelli falsi".

**Il certificatore** è colui che "**presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime**" (art. 1 del D.P.R. 445/2000).

Sul piano teorico e organizzativo bisogna poi operare una **separazione dei ruoli** nell'ambito del certificatore, tra:

- **RA (Registration Authority)** e
- **CA (Certification Authority)**

La prima (RA) ha la responsabilità di identificare in modo affidabile i soggetti che richiedono la certificazione (notarizzazione), mentre la seconda (CA) ha il compito, oltre che di rilasciare i certificati di firma, di gestire un archivio delle chiavi pubbliche e dei relativi certificati di firma emessi, consultabile da parte dei soggetti che operano con certificati emessi dalla Certification Authority<sup>8</sup>.

Sul piano tecnico e delle normative quando si parla di certificatori si parla di **PKI (Public Key Infrastructure)**, comprendendo in questo termine "**il personale, le policy<sup>9</sup>, le procedure, i componenti e le funzioni che permettono di collegare i nominativi identificativi degli utenti alle chiavi pubbliche e ai relativi certificati, così da permettere agli utenti l'utilizzo dei certificati e delle chiavi segrete associate per effettuare operazioni sicure sulle informazioni**".

Si deve tener presente che il risultato non è un sistema informatico di sicurezza, bensì **un sistema di fiducia basato sulla sicurezza informatica**.

---

<sup>7</sup> Sul piano legale è inesatto tradurre *Certification Authority* con "autorità di certificazione", perché nel nostro ordinamento la qualifica di "autorità" è attribuita solo a particolari soggetti pubblici. E' più corretto tradurre con "enti di certificazione" o, ancora più esattamente, "società di certificazione", dal momento che la legge prescrive la forma di società per azioni a quelli che definisce "soggetti certificatori" o semplicemente "certificatori".

<sup>8</sup> Questo sdoppiamento è stato rifiutato dal legislatore italiano, che ha voluto unificare in un unico soggetto (il certificatore) tutte le responsabilità derivanti dall'esercizio della certificazione, con l'evidente vantaggio di offrire al consumatore-utente una maggiore tutela, sia in sede contrattuale, sia, e soprattutto, in sede di contenzioso.

<sup>9</sup> La traduzione del termine "policy" non è facile: si intende, nella pratica, un insieme di regole che permettono nel loro complesso di coordinare un dato tipo di attività. Onde evitare l'utilizzo di traduzioni estemporanee e poco attinenti, è preferibile mutuare il termine dall'inglese, e utilizzare direttamente la parola "policy".

**L'attività di certificazione** ad opera di soggetti stabiliti nel territorio dello stato italiano o di altro stato europeo è libera, purchè coloro che la svolgono possiedano i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione direzione e controllo presso istituti di credito.

Sono considerati **certificatori qualificati**<sup>10</sup> ai sensi della normativa nazionale (art.27 D.P.R.445/2000) i certificatori che:

1. sono in grado di dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere l'attività di certificazione;
2. impiegano personale dotato di competenze specifiche;
3. utilizzano tecniche consolidate e sistemi affidabili, sicuri e in grado di garantire la riservatezza nella generazione delle chiavi.

Il processo di certificazione si svolge in un certo numero di passi, in cui il richiedente e il certificatore svolgono ruoli certi e complementari:

1. Il primo compito di un certificatore è "identificare con certezza la persona che fa richiesta della certificazione"<sup>11</sup>. Senza dubbio è la fase più critica della procedura di certificazione, perché se un soggetto riesce a farsi passare per un altro tutti i successivi passaggi sono viziati dall'inganno iniziale e possono derivarne spiacevoli conseguenze<sup>12</sup>.
2. Una volta esaurita la fase di identificazione, il richiedente genera la propria coppia di chiavi crittografiche asimmetriche (pubblica e segreta) e trasmette al certificatore una copia della propria chiave pubblica unitamente a una richiesta di certificazione (un documento elettronico contenente le informazioni identificative del richiedente associate alla chiave pubblica), adottando le necessarie modalità e politiche di sicurezza dettate dal certificatore stesso.
3. A questo punto il certificatore provvede alla generazione e firma del certificato, ovvero di un documento elettronico che contiene informazioni identificative del richiedente associate alla sua chiave pubblica, il tutto firmato digitalmente dal certificatore con la propria chiave segreta.
4. Il certificatore inserisce il certificato del richiedente in un pubblico registro consultabile per via telematica.
5. Infine il certificatore trasmette il certificato firmato al richiedente, che provvederà a conservarlo sul dispositivo di firma.

Affinchè il certificatore possa svolgere la propria attività deve essere a sua volta certificato, ovvero identificato, registrato, e dotato di un proprio certificato di firma digitale, con associata la sua chiave segreta. Un processo che vede il Gruppo Chiuso di Utenza riconoscere formalmente il certificatore, mediante un atto pubblico all'interno del gruppo, e che termina con una fase di **autocertificazione del certificatore**:

1. Il certificatore genera la propria coppia di chiavi crittografiche asimmetriche (pubblica e segreta) e compila una richiesta di autocertificazione (un documento elettronico contenente le informazioni identificative del certificatore associate alla chiave pubblica), adottando le necessarie modalità e politiche di sicurezza dettate dal Gruppo Chiuso di Utenza.
2. A questo punto il certificatore provvede alla generazione e firma del proprio certificato, ovvero di un documento elettronico che contiene le sue informazioni identificative associate alla chiave pubblica, il tutto firmato digitalmente dal certificatore stesso con la propria chiave segreta.
3. Il certificatore inserisce il proprio certificato in un pubblico registro consultabile per via telematica.

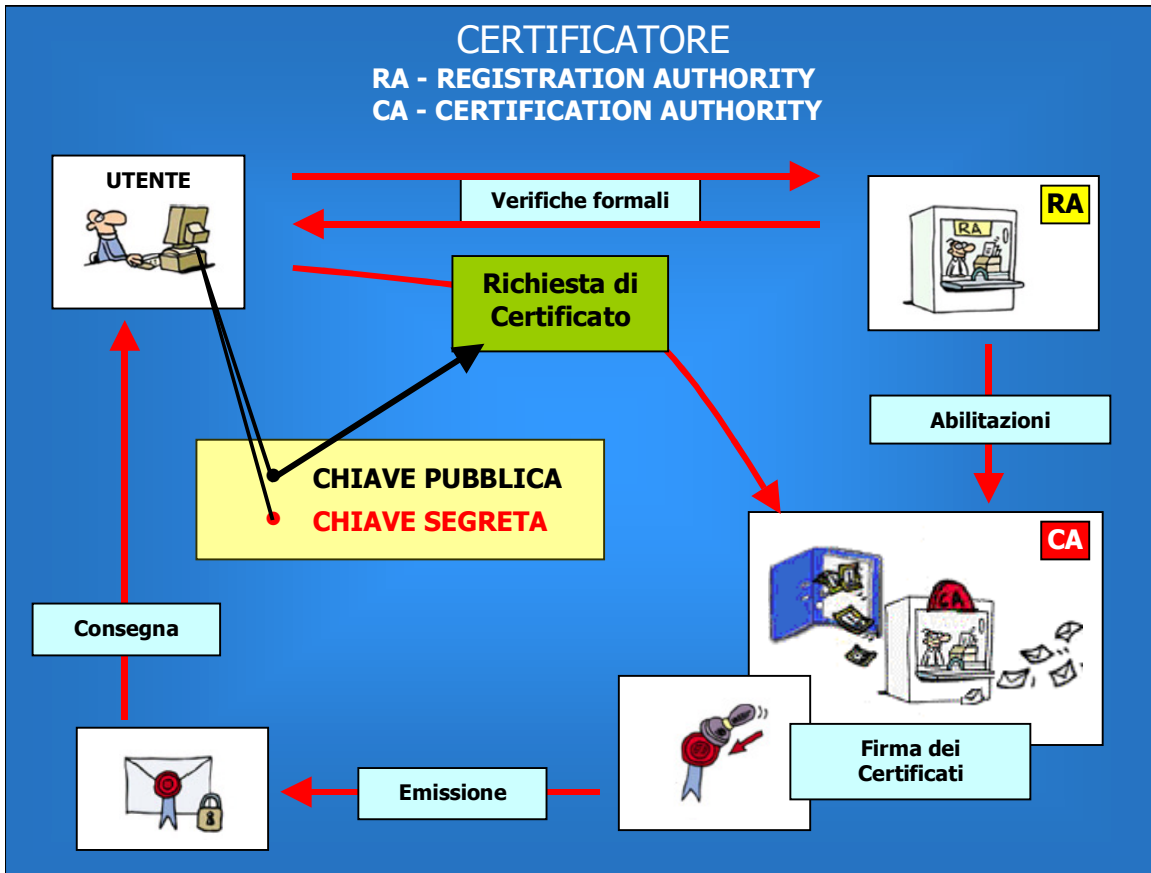
---

<sup>10</sup> Tali soggetti, i soli che possono rilasciare certificati qualificati (cioè certificati conformi ai requisiti previsti dall'allegato I della direttiva europea 1999/93-CE), debbono fare precedere l'inizio della loro attività di certificazione da una dichiarazione di inizio di attività al dipartimento dell'innovazione e delle tecnologie presso la Presidenza del consiglio dei Ministri. Il dipartimento può procedere a verifiche periodiche e, ove riscontri l'assenza dei requisiti prescritti, può emettere un divieto di prosecuzione dell'attività, salvo che il certificatore non regolarizzi la sua posizione nel termine prefissatogli dall'amministrazione stessa.

<sup>11</sup> articolo 9 del DPR 513/97

<sup>12</sup> E' da sottolineare l'importanza dell'espressione "identificare con certezza", mutuata dalla legislazione notarile, per la quale l'identificazione non può avvenire con la mera esibizione di un documento, ma rappresenta la somma di una serie di attività finalizzate a questo scopo, con evidente aggravio di responsabilità per colui che "identifica".

4. Infine il certificatore inserisce il proprio certificato firmato sul dispositivo di firma su cui sono state generate le chiavi e su cui viene conservata in modo sicuro la chiave segreta del certificatore, utilizzata per firmare i certificati dei soggetti richiedenti.



In un certificato di firma digitale possono essere inserite indicazioni sull'attività professionale o sulle cariche del titolare, o sui suoi eventuali poteri di rappresentanza. In questo modo con la verifica della firma digitale si può avere anche la certezza che il firmatario sia legittimato alla firma di determinati documenti.

Un certificato, e la chiave segreta associata, **non "vive" all'infinito**. Esso ha una data di nascita e una data di scadenza, dopo la quale perde di validità. Ma un certificato può perdere di valore anche prima della propria scadenza: essere **revocato** in seguito al verificarsi di qualche "incidente" (ad esempio, la perdita di segretezza della chiave segreta), o **sospeso temporaneamente** (ad esempio su richiesta dello stesso utente certificato). Comunque il certificatore deve rendere pubblica la revoca o la sospensione in tempi molto stretti, perchè un ritardo può trarre in inganno chi riceve un documento elettronico firmato, e verifica come valida una firma digitale che invece non lo è (ad esempio in seguito alla perdita, da parte del titolare, del potere di rappresentanza).

"Tempi molto stretti" non significa settimane o giorni, ma minuti o addirittura secondi: è il contesto operativo a suggerire la migliore politica da adottare. La tempestività di segnalazione della revoca o sospensione è particolarmente importante: basti pensare alle conseguenze che può avere una serie di ordini di pagamento sottoscritti dall'amministratore di una società dopo che gli è stato revocato il mandato. Sino a quando la revoca del mandato (e quindi del certificato che lo documenta) non viene resa pubblica, quell'ordine è valido per chiunque compia la verifica della firma.

## Requisiti Formali per il Rilascio e la Gestione dei Certificati

A questo punto dovrebbe essere chiara la criticità del ruolo del certificatore nello scenario di creazione di un documento informatico "valido e rilevante a tutti gli effetti di legge" all'interno di un Gruppo Chiuso di Utenti, e ben si comprendono i motivi che hanno spinto il legislatore (italiano ed europeo) a prevedere per i certificatori pubblici norme restrittive, tanto da disegnare un sistema molto più rigido delle prassi di certificazione in uso in ambiti meno critici (ad esempio su Internet).

L'art.8 del D.P.R.513/1997 stabilisce, tra l'altro, che l'attività di certificazione possa essere svolta da soggetti privati che abbiano gli stessi requisiti richiesti per l'esercizio dell'attività bancaria e che siano iscritti in un apposito elenco, tenuto dall'Autorità per l'informatica nella pubblica amministrazione; analoghi requisiti (tranne quelli di tipo soggettivo) sono richiesti per le Amministrazioni pubbliche che intendono svolgere l'attività di certificazione nel proprio ambito<sup>13</sup>.

Il certificatore privato deve avere la "forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria". Questo significa che solo società di grandi dimensioni, come le banche e i maggiori operatori di telecomunicazioni possono realizzare strutture con i requisiti richiesti per l'emissione di certificati che consentono di firmare documenti informatici "validi e rilevanti a tutti gli effetti di legge".

In effetti, l'esperienza Internet dimostra che l'attività di certificazione può essere svolta con successo da strutture di dimensioni ben più piccole di quelle rese obbligatorie dalla nostra normativa. È invece discutibile che l'affidabilità dei singoli certificatori possa essere ottenuta con il sistema del *web-trust*, cioè della fiducia e della certificazione reciproca: "io ti certifico perché un mio amico ti conosce" e così via. In molti casi basta inviare per fax la fotocopia di un documento per essere abilitati al rilascio di un certificato: quanto ci vuole per inviare un documento contraffatto?

Evidentemente il livello di sicurezza tipico della rete non è idoneo alla sottoscrizione di documenti validi e rilevanti a tutti gli effetti di legge.

Con la firma digitale certificata secondo la normativa italiana si possono sottoscrivere atti anche per importi rilevanti; nella pubblica amministrazione si può gestire l'intero flusso documentale, si possono emanare atti di qualunque tipo e, soprattutto, si semplificano enormemente i rapporti tra gli uffici e i cittadini, compresi i flussi di denaro.

Per la normativa italiana non ci sono limiti qualitativi o quantitativi alle transazioni che possono essere compiute con la firma digitale: si potranno comperare o vendere società, ottenere prestiti per miliardi, certificare bilanci di società di dimensioni sovranazionali. E tutto ciò anche tra soggetti che non si conoscono e che non hanno avuto precedenti rapporti, o che non fanno parte di "sistemi chiusi", come quello delle transazioni tra istituzioni finanziarie, che da tempo avvengono per via telematica.

È evidente che questo scenario globale può funzionare solo con un livello molto elevato di affidabilità dei certificati e delle chiavi digitali, poiché sul certificato è fondata la sicurezza del documento informatico.

Si giustifica così il rigore delle norme relative alla registrazione dei certificatori, compresa la dimensione economica delle società: non si deve dimenticare che il certificatore può essere chiamato a risarcire i danni causati da vizi dei certificati, o più semplicemente da un ritardo nella pubblicazione della sospensione o della revoca di una coppia di chiavi.

---

<sup>13</sup> Si deve sottolineare che le pubbliche amministrazioni hanno i medesimi obblighi dei privati (tranne la forma societaria, ovviamente) per quanto concerne organizzazione oggettiva e sicurezza, ma solo se intendono produrre certificati con valenza esterna: possono invece adottare regole più "leggere" per la sottoscrizione di documenti interni e non destinati all'esterno.

Con le norme sui requisiti e sui compiti dei certificatori il legislatore italiano ha voluto costruire un edificio di certezza e di affidabilità del documento informatico, in quanto la sua diffusione in ambito pubblico e la sua adozione da parte dei privati sono in buona parte legate al clima di fiducia che si creerà sull'uso del nuovo sistema.

Se gli utenti non si fideranno della firma digitale il suo impiego sarà evitato o rallentato il più a lungo possibile, con conseguenze negative per la modernizzazione della pubblica amministrazione e lo sviluppo stesso della società dell'informazione.

## Certification Authority: operatività

Un'Autorità di Certificazione (Certification Authority - CA) è un'entità che riceve un insieme di informazioni, le verifica e le garantisce rispetto a una terza parte (ovvero gli utenti del Gruppo Chiuso di Utenza di cui è certificatore).

La CA deve realizzare le seguenti funzioni principali:

1. accettare le richieste di certificazione
2. verificare l'identità delle persone o delle organizzazioni che richiedono la certificazione
3. emettere i certificati
4. revocare i certificati
5. fornire informazioni sui certificati che ha emesso.

Le prime due funzioni sono dette di registrazione, mentre le altre rispettivamente di emissione e gestione dei certificati. I certificati emessi da una CA forniscono alle entità certificate un mezzo per provare la propria identità in un contesto di transazione elettronica. I certificati sono basati su un sistema di crittografia a chiave pubblica.

Un certificato emesso da una CA e firmato con la chiave segreta della CA tipicamente contiene:

- la chiave pubblica del titolare certificato;
- il nome del titolare: se il titolare è una persona fisica il suo nome e cognome, data di nascita, eccetera - se invece è un server il nome è il suo indirizzo di rete (indirizzo simbolico DNS o indirizzo IP);
- la data di scadenza del certificato;
- il nome della CA che ha emesso il certificato;
- la firma digitale della CA che ha emesso il certificato (ovvero l'HASH delle informazioni precedenti codificato con la chiave segreta della CA).

Le informazioni inserite nel certificato sono estratte da un documento elettronico presentato alla CA dall'aspirante titolare: la Richiesta di Certificazione (Certification Request). I campi inseriti nella richiesta di certificazione e le procedure utilizzate per verificarli sono parte della "policy" specifica della CA.

Se le procedure definite dalla policy della CA sono state eseguite correttamente, la CA emette un documento elettronico in formato X.509, ovvero il certificato del titolare richiedente, contenente la chiave pubblica associata.

Chiunque può verificare la policy ed il certificato della CA, che la CA deve rendere pubblici all'interno del proprio Gruppo Chiuso di Utenza. La CA deve mantenere un Registro Pubblico dei Certificati emessi, una Lista dei Certificati Revocati (**Certification Revocation List - CRL**), e una Lista dei Certificati Sospesi (**Certification Suspension List - CSL**), che devono essere disponibili come stabilito dalla policy.

Solitamente una CA può emettere tre tipi di certificati:

- **Personali**, rilasciati a persone fisiche: contengono informazioni quali nome, cognome, indirizzo, casella email, eccetera: possono essere utilizzati per garantire la provenienza di una email, per inviare un numero di carta di credito, per firmare documenti elettronici, e così via.
- **Server**, rilasciati ai titolari di server che operano in rete (www, ftp, TSA, ...). Questi certificati sono emessi per garantire l'identità del server stesso, e sono particolarmente utili per implementare siti di commercio elettronico in cui i clienti vogliono essere certi di operare con particolari server, o per i server TSA (di marcatura temporale, TSA – Time Stamp Authority).
- **Software**, per garantire l'autenticità della provenienza del software, specialmente se questo viene distribuito in Rete.

## E la quarta dimensione?

Dire che una persona ha firmato un documento, assumendone la paternità, non sempre è sufficiente. Spesso è importante definire con la maggior certezza possibile **il momento in cui tale assunzione è stata fatta**.

Se si parla di una poesia, o di un brano musicale, la cosa non è poi così determinante<sup>14</sup>. Ma quando si ha a che fare con documenti che comportano il passaggio di proprietà di un bene, o la cessione di valori, stabilire con esattezza il momento da cui il cambio o la cessione ha effetto è molto importante, in quanto **la firma non è un atto fine a se stesso, ma un anello di una catena di eventi distribuita nel tempo**.

Nel campo della firma olografa l'apposizione della nostra firma è accompagnata quasi sempre dalla contestuale apposizione di una data, e in alcuni casi anche dell'ora. Quando firmiamo un assegno dobbiamo mettere la data (onde evitare strani giochini con la valuta e il calcolo degli interessi), e quando l'agente assicurativo ci consegna la polizza auto firmata, compila l'ora da cui la polizza ha effetto.

Nel campo della firma digitale il problema si pone in modo analogo, ma la sua soluzione è leggermente più complicata. Un parallelo è, a questo punto, doveroso.

- Se firmiamo un documento cartaceo, e scriviamo nello stesso documento un riferimento temporale (la data, ed eventualmente l'ora), inseriamo nel documento una **informazione che ha la stessa fisicità delle altre informazioni**<sup>15</sup> (quali il titolo, il testo del documento, la firma, ...).
- Quando si trattano documenti in formato elettronico, **il corpo del documento viene racchiuso in una busta**, ovvero l'insieme di una testata (in cui sono registrate le informazioni identificative del documento) e una coda (in cui sono registrate le informazioni accessorie)<sup>16</sup>. Questa formalizzazione è necessaria in quanto i documenti elettronici non sono trattati direttamente da esseri senzienti (come nel cartaceo), ma con il supporto di programmi di elaborazione che operano in base a schemi rigidi.

Ciò significa che a un documento firmato digitalmente dobbiamo aggiungere le informazioni relative alla data e ora di firma. Queste sono già incluse nel formato PKCS#7, ma sono quelle definite dall'orologio del computer su cui è stato creato il file firmato, e quindi **non opponibili a terzi se non sulla base della buona fede del firmatario**.

Per dare maggior enfasi e garanzia è possibile calcolare una **marca temporale del file firmato**, ovvero una **evidenza firmata digitalmente da una entità esterna accreditata**, che afferma in modo **inequivocabile che il file firmato era tale a un certo tempo**.

È un pò come firmare un documento davanti a un notaio, che sotto alla nostra firma appone una data, un'ora e la propria firma. Il notaio è l'entità esterna accreditata, la cui valenza è accettata anche in sede legale. Nel caso della firma digitale i notai coinvolti nel processo sono due:

1. il **certificatore** che ha rilasciato il certificato al firmatario, e che attesta la validità del certificato, della chiave segreta associata, ed entro certi limiti l'identità del firmatario,
2. il **marcatore temporale**, che attesta la certezza di esistenza del file firmato in un certo momento temporale.

---

<sup>14</sup> ... ovviamente gli storici della letteratura o della musica non sono molto d'accordo al riguardo ...

<sup>15</sup> Con fisicità si intende lo stesso pezzo di carta, fisicamente distinto da altri pezzi di carta (quali ad esempio una busta).

<sup>16</sup> Si veda ad esempio il formato dei file PKCS#7 illustrato nei paragrafi precedenti.

## Marca Temporale: La certificazione del tempo

Stabilire con certezza il momento in cui un dato evento ha avuto luogo è una necessità sempre presente nella nostra vita, professionale e non.

Come stabiliamo "il momento" di un evento?

La risposta è semplice: con la **memoria**.

Ma non solo. La risposta completa è: **con la memoria e con la sua affidabilità**.

Quando ricordiamo un evento ricordiamo (salvo gli smemoranda 🙄) anche il momento in cui si è verificato, e se ci fidiamo della nostra memoria tanto ci basta.

Ma quando il momento in cui si è verificato un dato evento interessa non solo noi, ma anche altre persone, dobbiamo darne in qualche modo una evidenza comune. Se chiacchieriamo con un amico basta la nostra memoria e quanto riportiamo verbalmente (l'affidabilità è un componente di base dell'amicizia!).

Se invece l'evento si riferisce a un contesto non strettamente amichevole, e quindi soggetto in qualche forma a essere manipolato (quando ad esempio vendiamo l'automobile usata, o compriamo casa), abbiamo la necessità di identificare in modo univoco e possibilmente non contestabile il momento in cui l'evento si è verificato.

E qui la forma scritta diventa indispensabile

**verba volant, scripta manent** 🙄 ...

ma scrivere su un pezzo di carta una data e/o un'ora non basta: ci vuole una assunzione di paternità di quanto afferma lo scritto, ovvero **una firma**.

In una scrittura privata si riporta data (e ora), e si appongono le firme degli interessati. E salvo prova contraria ciò è sufficiente a garantire quella che i legali chiamano "opponibilità a terzi".

In una scrittura redatta da un notaio è la firma del notaio a garantire la veridicità di quanto affermato dallo scritto, data (e ora) compresa (un informatico direbbe, a questo punto, che il notaio è affidabile "per default").

Quando dal mondo reale ci spostiamo al mondo elettronico dei documenti informatici abbiamo bisogno di qualcosa che ci dia le stesse garanzie temporali dell'orologio e del calendario del notaio. E qui ci viene in aiuto il meraviglioso mondo degli orologi atomici, e del loro utilizzo in Internet per garantire un allineamento globale degli orologi e della misura del tempo.

## Una sorgente temporale globale e gratuita: il protocollo NTP

Sin dal momento della sua nascita la **suite TCP/IP** (sembra il nome di una collezione di mobili d'epoca!) ha previsto nei suoi protocolli l'NTP (Network Time Protocol – Protocollo del Tempo di Rete), identificato dal magico numerello del codice servizio 123 (sì, proprio un, due, tre, e non è un caso).

Nello schema NTP una miriade di computer possono connettersi tra di loro per scambiarsi informazioni relative alla propria visione del tempo. Alcuni di questi computer fungono da **server**, altri (la maggior parte) da **client**. I server erogano informazioni attendibili sul tempo (in pratica, quando richiesti, dicono che ora è secondo loro), mentre i client allineano i propri orologi interni (i system clock) sulla base delle indicazioni ricevute dai server.

I server si distinguono in base alla affidabilità delle loro sorgenti di riferimento temporale. Quei computer che possono avvalersi di dispositivi hardware (orologi atomici, connessioni via radio a orologi atomici ufficiali, ...) sono di classe **stratum-1**, mentre i server che non dispongono di dispositivi hardware e mantengono il loro system-clock aggiornato in base ad indicazioni che pervengono loro da server stratum-1, sono di classe **stratum-2**: e così di seguito si hanno server **stratum-3** (che ridistribuiscono il tempo di server stratum-2), server **stratum-4** (che ridistribuiscono il tempo di server stratum-3), sino ai server di affidabilità più bassa, gli **stratum-16**.

Gli elenchi ufficiali dei server pubblici stratum-1 e stratum-2 sono pubblicati sul sito ufficiale NTP (<http://www.ntp.org/>), e in particolare all'indirizzo <http://support.ntp.org/bin/view/Servers/WebHome>. Qualunque server o client che installiamo in casa nostra può richiedere il supporto della rete NTP (l'insieme distribuito dei server NTP stratum-1 e stratum-2), e aggiornare con costanza e sicurezza il proprio system-clock al prezzo di qualche pacchetto UDP scambiato ogni tanto sulla rete Internet:

un aggiornamento ogni dieci minuti al costo di qualche decina di byte – una spesa folle 🤔!!!

## TSA, TSQ e TSR

Ma, ma, ma ...

... tutto ciò non è sufficiente. Chi ci assicura che il documento firmato in formato PKCS#7 riporti effettivamente una data-ora ricavata da un server NTP ufficiale?

Nessuno!

E allora ecco venirci in aiuto la nostra beneamata firma digitale. Se a indicare la data-ora del nostro file firmato è una entità terza accreditata (in gergo tecnico una **TSA – Time Stamp Authority**), che a lato della data-ora del documento mette la sua riverita firma digitale opponibile a terzi, allora siamo salvi. Evviva.

Ma se il file che stiamo firmando è, ad esempio, di 100 Mbyte cosa facciamo? Lo spediamo via rete alla TSA? E scarichiamo da questa il file marcato temporalmente da 100 Mbyte? Una cosuccia un pò dispendiosa.

E ancora una volta dobbiamo richiedere l'aiuto degli amici matematici e del loro miracoloso hash (o impronta, ricordate?). E così procediamo in pochi semplici passi:

- calcolo l'hash del file firmato (20 byte),
- lo includo in una richiesta di marca temporale (**TSQ – Time Stamp Query** – un piccolo file di meno di 1 Kbyte),
- invio la TSQ alla TSA,
- la TSA trasforma la TSQ in una marca temporale firmata e opponibile a terzi (**TSR - Time Stamp Response** – altro piccolo file di circa 4 Kbyte contenente il mio hash e la data-ora certificata, il tutto firmato dalla TSA),
- la TSA mi ritorna la TSR ...

sino ad associare a fianco del mio documento firmato (il file PKCS#7, con estensione .p7m) la sua marca temporale (il file TSR, con estensione .tsr). La coppia di file **.p7m + .tsr** mi permette finalmente di avere un documento elettronico, firmato digitalmente, marcato temporalmente, e opponibile a terzi.

Più difficile a dirsi che a farsi. Alla faccia di chi ci vuol male.

Una piccola nota: le TSA accreditate (dal CNIPA ovviamente) non lavorano gratis, e le marche temporali se le fanno pagare. In media circa 30 centesimi di euro a marca. Da utilizzare *cum juicio* direbbe il Manzoni.

## Marca temporale: lo standard RFC 3161

Tutto il ragionamento dei paragrafi precedenti è riassunto formalmente nello standard Internet RFC-3161 (Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - TSP).

Questo standard definisce il contesto

“Un servizio di marcatura temporale supporta l’asserto probatorio che uno specifico dato esiste prima di un dato momento temporale.”

“I servizi di non ripudio (ISO/IEC 10181-5: Security Frameworks in Open Systems. Non-Repudiation Framework. April 1997) richiedono l’abilità di stabilire l’esistenza di uno specifico dato prima di un dato momento temporale.”

gli attori

“La TSA è un TTP (Trusted Third Party – terza parte affidabile) in grado di creare marche temporali al fine di indicare che uno specifico dato esiste prima di un dato momento temporale.”

il come

“La TSA DEVE:

1. utilizzare una sorgente temporale affidabile;
2. includere un valore temporale affidabile in ogni marca temporale;
3. includere un nuovo numero intero univoco in ogni nuova marca temporale generata;
4. produrre una marca temporale ogni qualvolta riceve una richiesta valida da una entità richiedente, quando possibile;
5. includere in ogni marca temporale un identificatore che indichi univocamente la policy di sicurezza adottata al momento di creazione della marca;
6. marcare temporalmente solo la rappresentazione hash del dato (ovvero una impronta numerica associata con una funzione hash a una via, resistente alle collisioni e univocamente identificata da un OID – Object Identifier);
7. esaminare l’OID della funzione hash a una via resistente alle collisioni, e verificare che la lunghezza dell’hash sia consistente con l’algoritmo di hash.
8. non esaminare in alcun modo l’impronta che viene marcata temporalmente (ad esclusione della verifica della lunghezza, come sopra specificato);
9. non includere alcuna identificazione della entità richiedente nella marca temporale;
10. firmare ogni marca temporale utilizzando una chiave generata esclusivamente a questo scopo, con l’indicazione esplicita della finalità della chiave riportata nel certificato corrispondente;
11. includere nella marca temporale solo le estensioni supportate dalla TSA se richieste esplicitamente dalla entità richiedente – se non possibile la TSA DEVE rispondere con un messaggio di errore.”

il cosa

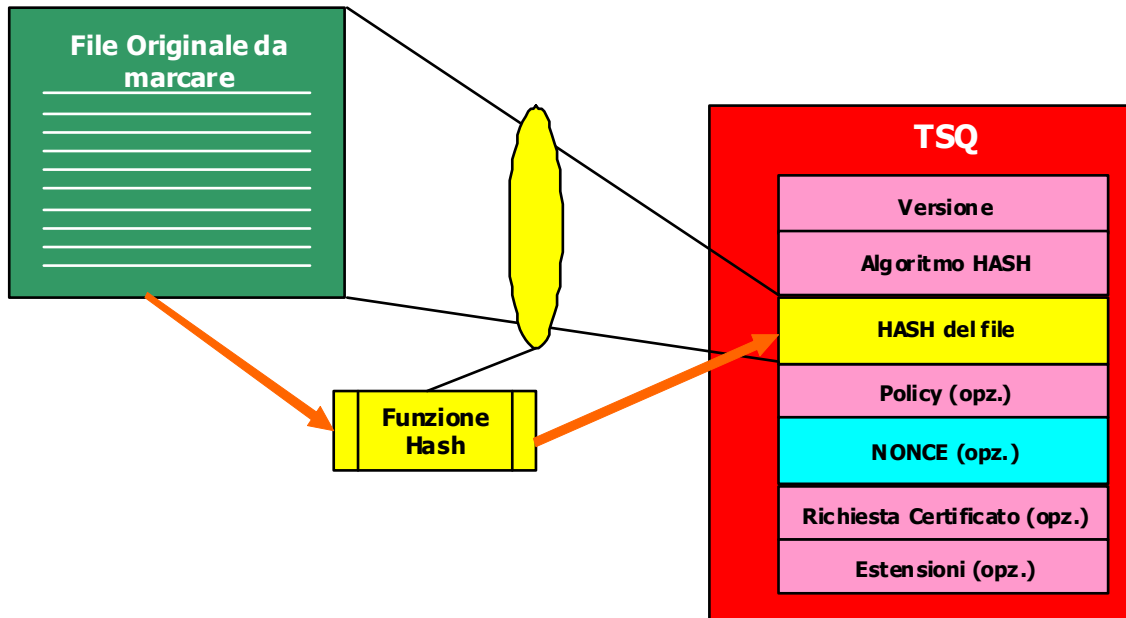
“TSQ – la richiesta di marca temporale”

“TSR – la risposta di marca temporale”.

Il cosa è illustrato nelle figure alle pagine seguenti.

Nella richiesta TSQ sono inclusi:

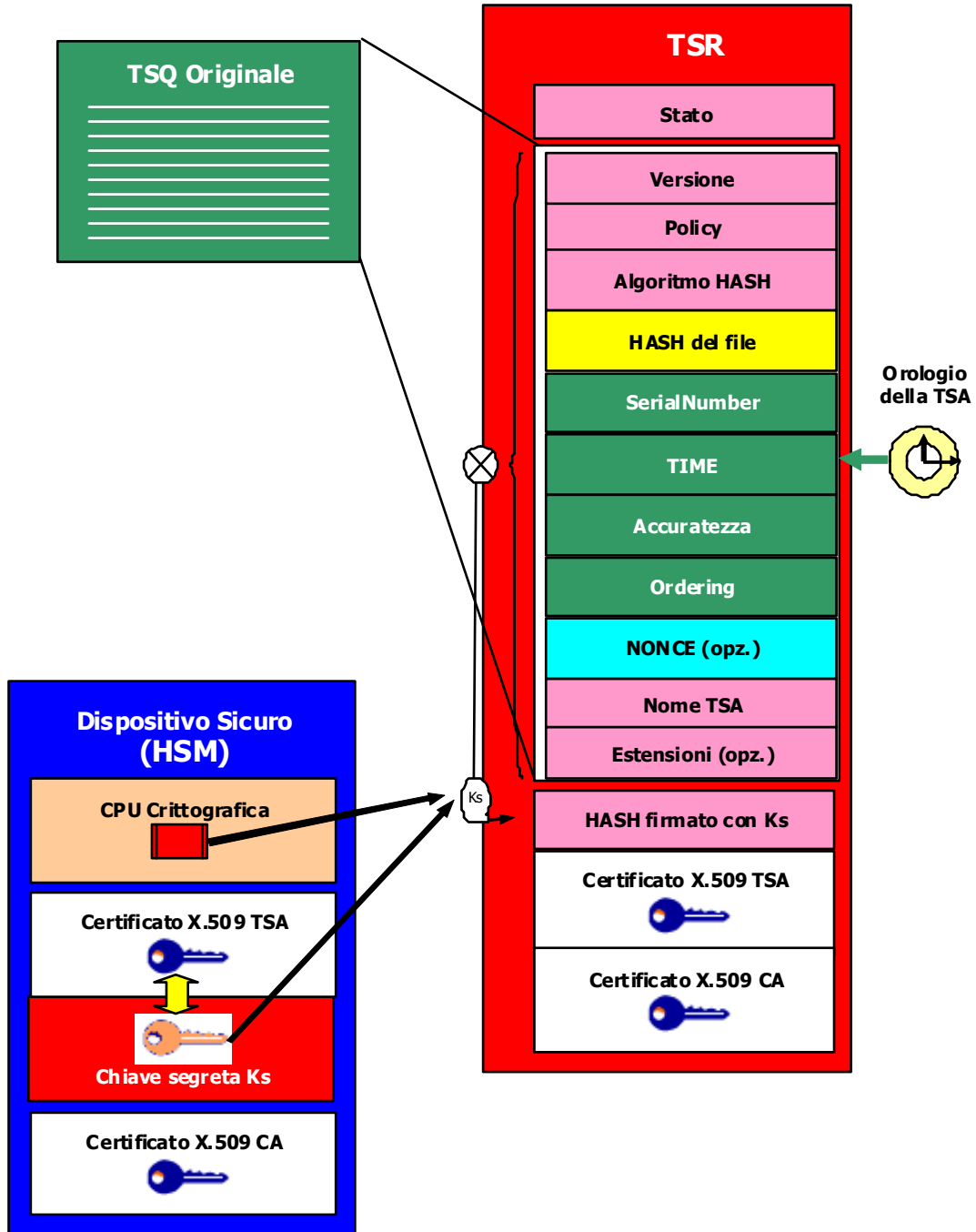
- la versione della marca richiesta (attualmente v1)
- l'algoritmo di hash
- l'hash del file (o più generalmente del dato) da marcare
- l'OID della policy di sicurezza richiesta alla TSA (opzionale)
- il NONCE, un numero random di 64 bit generato dall'entità richiedente, e quanto più univoco possibile per il richiedente (opzionale)
- il flag di richiesta di presenza del certificato di firma della TSA nella risposta (opzionale)
- eventuali estensioni (opzionale).



Nella risposta TSR (la nostra marca temporale) sono inclusi:

- lo stato della operazione di marcatura
- i campi della TSQ completati da:
  - numero di serie univoco della marca temporale (SerialNumber)
  - la MARCA TEMPORALE (TIME)
  - l'accuratezza della marca (al minuto, al secondo, al millisecondo, ...)
  - flag di ordinamento delle marche rilasciate (Ordering)
  - nome della TSA
- l'hash dei campi TSQ completati dalla TSA (vedi sopra) crittografato con la chiave segreta  $K_s$  della TSA da parte del dispositivo sicuro di firma (HSM – Hardware Security Module)
- il certificato X.509 di firma della TSA (contenente la chiave pubblica  $K_p$  associata alla chiave segreta  $K_s$  di firma)
- il certificato X.509 della CA che ha emesso il certificato X.509 di firma della TSA.

Nel caso di errore la TSR non contiene la marca temporale firmata, ma solo i dati identificativi della condizione di errore (Stato).



## Un po' di complicazioni: CADES, PAdES, XAdES, e marche temporali

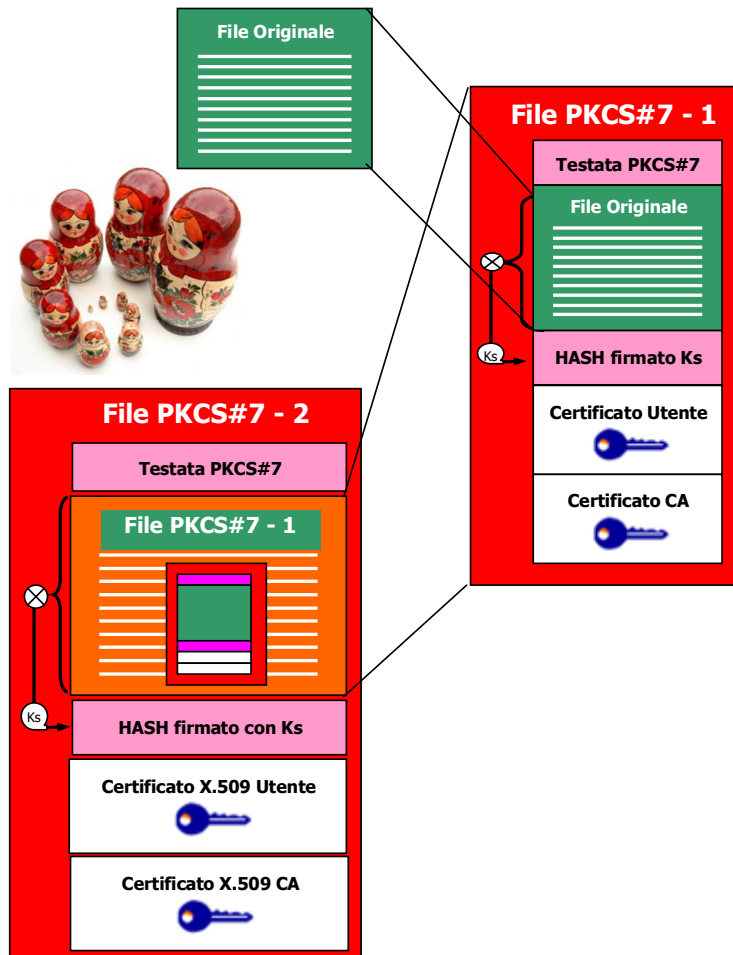
Fin qui tutto bene, e forse anche abbastanza chiaro.

Ma chi si è avventurato nel corso degli anni nella lettura delle varie leggi e regolamenti che venivano man mano sfornati dai nostri solerti legislatori, si sarà sicuramente accorto di un percorso evolutivo delle norme, e degli scenari che venivano man mano delineati.

### Le Matrioske, le Firme congiunte ...

Dalla semplice idea di "un documento, una firma", si è affrontato in primis il problema delle firme congiunte in un modo un po' spartano. Ci si è inventati il concetto di "**firma matrioska**", rifacendosi al concetto delle bamboline russe (qualcuno avrebbe preferito le scatole cinesi, ma tant'è ...).

In pratica, poichè sul piano elettronico un documento firmato è in realtà assimilabile a una busta (come si è detto parlando del PKCS#7) che contiene al suo interno sia il documento, sia la firma, se si vogliono fare firme congiunte è sufficiente rifirmare il file già firmato, creando una nuova busta che al suo interno contiene la seconda firma e la prima busta, che a sua volta contiene al suo interno la prima firma e il documento originale.

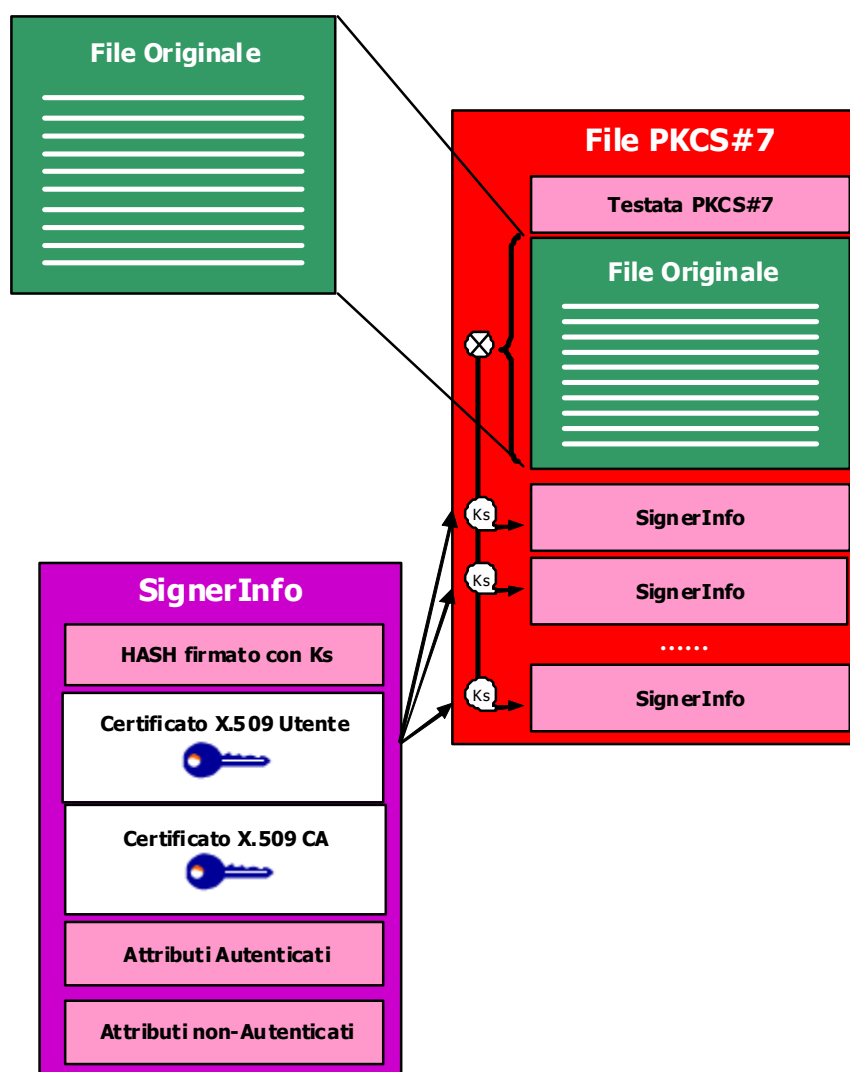


E il gioco può essere ripetuto tante volte quante si vuole (esattamente come con le matrioske). Per accedere al documento e contestualmente verificare le varie firme è necessario aprire man mano le varie buste, verificando di volta in volta le varie firme<sup>17</sup>.

Ma in realtà lo standard PKCS#7 prevede sin dall'inizio la soluzione. Una busta PKCS#7 può contenere al suo interno più firme: ogni firma viene registrata in una apposita struttura denominata **SignerInfo** (informazioni del firmatario). Ogni SignerInfo comprende una serie di elementi (**attributi**) che possono essere **'autenticati'** (ovvero firmati) e **'non-autenticati'** (non firmati). Quindi per avere due o più firme congiunte è sufficiente registrare due o più SignerInfo nella busta PKCS#7.

Un documento firmato inizialmente da un solo firmatario (PKCS#7 con una sola SignerInfo), può essere riaperto, e rifirmato, riscrivendo il nuovo file PKCS#7 con due SignerInfo. E così via<sup>18</sup>.

E così viene raggiunto, in modo elegante, il problema delle firme congiunte.



<sup>17</sup> Sul piano informatico una gestione a 'matrioska' crea un po' di complicazioni. Se si firma inizialmente un documento registrato in un file con estensione '.doc', si ottiene un file con doppia estensione: '.doc.p7m'. Firmando ulteriormente questo file in modalità matrioska, si hanno tre estensioni: '.doc.p7m.p7m'. E così via. Proviamo ad immaginare cosa succederebbe con ventidue firmatari che appongono firme congiunte in modalità matrioska!!!

<sup>18</sup> In tal modo, rifacendoci all'esempio della nota precedente, il file firmato rimane sempre con solo due estensioni ('.doc.p7m'), ma al suo interno il numero delle SignerInfo aumenta progressivamente.

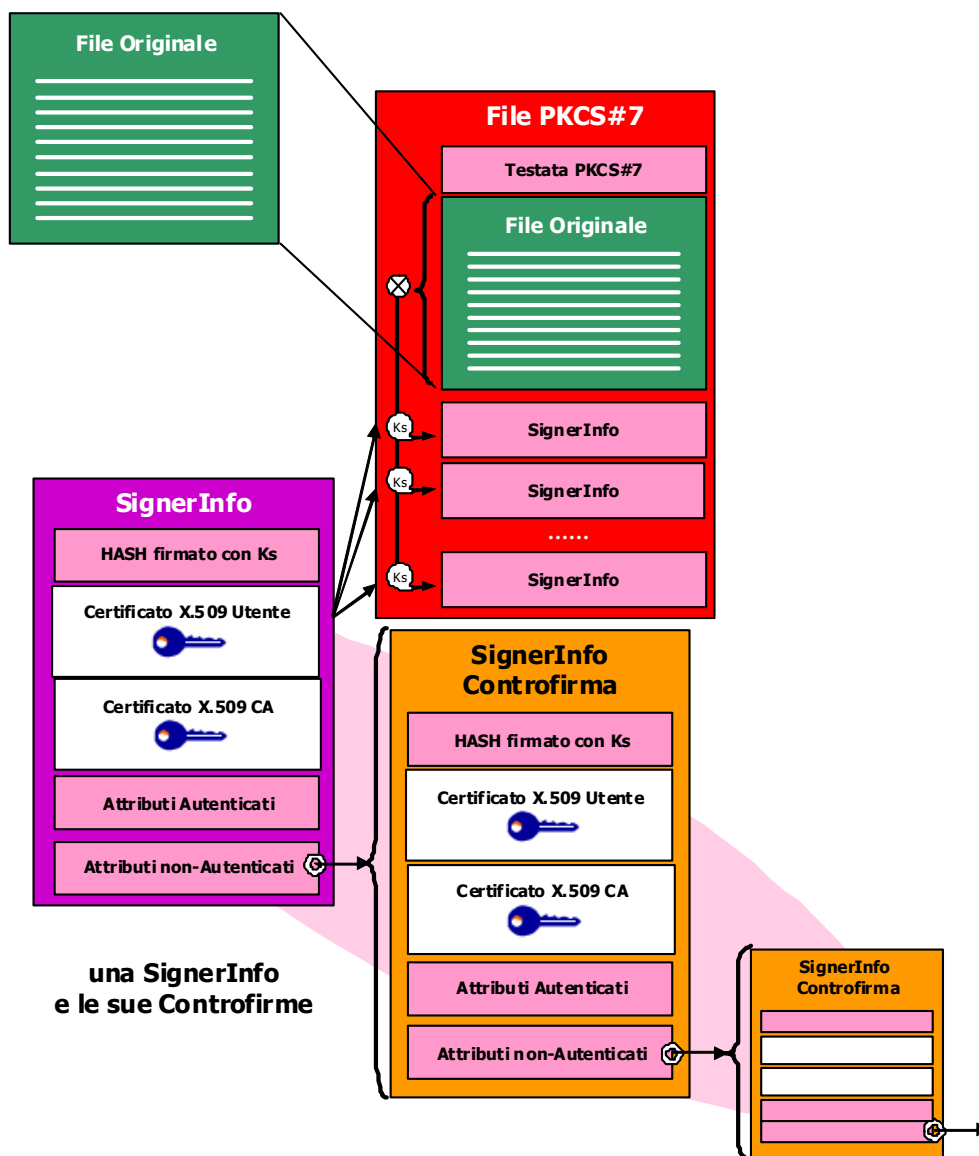
## ... e le Controfirme

Ma e le controfirme?

Beh, ragionando in modo logico viene da pensare che essendo la controfirma una 'firma di una firma', deve essere registrata nella SignerInfo della firma firmata (che giochino di parole !) come attributo (non-autenticato, in quando viene inserita dopo la firma originale). E in effetti, gli standard RFC a supporto del PKCS#7 definiscono sin dall'inizio la possibilità di inserire controfirme di una firma come attributi non-autenticati, codificati in base allo standard PKCS#9.

Quindi se voglio controfirmare una firma, apro la sua SignerInfo e inserisco tra i suoi attributi non-autenticati la SignerInfo della controfirma. E controfirmando una controfirma opero in modo analogo, ottenendo un insieme di SignerInfo nidificate).

Un po' complesso, ma tutto sommato logico e relativamente semplice.



## La UE e l'AdES

Poi entra in gioco l'Unione Europea, che ha definito un proprio insieme di standard che estendono il 'corpus' degli RFC.

L'ETSI (European Telecommunications Standards Institute) è un ente europeo che produce gli standard applicabili a livello globale per le tecnologie dell'informazione e delle comunicazioni (ICT), per reti fisse, mobili, radio, convergenti, broadcast e relative tecnologie internet.

Il 28 novembre 2008 la Commissione europea ha adottato un 'Piano d'azione sulle firme elettroniche (eSignatures) e sulla identificazione elettronica (eIdentification)' per facilitare la fornitura di servizi pubblici transfrontalieri nel mercato unico' (COM-2008 798). Il 22 dicembre 2009 la Commissione Europea ha emanato un mandato di normalizzazione in materia di firme elettroniche (M/460) per la definizione di un quadro di normazione razionalizzata<sup>19</sup>. La normativa italiana si ispira ovviamente a questi standard.

In particolare ci interessano gli standard ETSI relativi alla cosiddetta **famiglia AdES** (CAAdES, XAdES, e PAdES). No, non si tratta della versione europea della famiglia Adams!

**AdES** sta per '**Advanced Electronic Signature**', e conseguentemente:

**CAAdES** sta per '**Cryptographic Message Syntax Advanced Electronic Signature**',  
**XAdES** sta per '**XML<sup>20</sup> Advanced Electronic Signature**,  
**PAdES** sta per '**PDF<sup>21</sup> Advanced Electronic Signature**'.

Un approccio, quello ETSI, un po' più razionale e coordinato di quello codificato dagli RFC in base a una logica del tipo 'quando mi serve uno standard me lo faccio'. Ma proprio perchè più razionale e coordinato (e soprattutto volto alla normalizzazione dei paesi europei) più complesso da capire e interpretare.

Sul piano pratico una SignerInfo AdES, rispetto a una firma PKCS#7 'classica', si differenzia per la presenza di un ulteriore attributo autenticato (e quindi firmato): l'**ESS signing-certificate-v2**<sup>22</sup>.

Un documento firmato CAAdES è quindi un file di tipo '.p7m', le cui SignerInfo comprendono tutte l'attributo autenticato (firmato) ESS signing-certificate-v2.

A ulteriore chiarimento, i documenti firmati XAdES riportano la firma secondo uno schema di imbustamento differente rispetto a quello PKCS#7, ma sostanzialmente equivalente (di norma un normale utente finale accede a documenti XML, e quindi XAdES, non in modo diretto, ma con la mediazione di servizi di rete via WEB).

Analogamente i documenti firmati PAdES riportano la firma secondo uno schema di imbustamento definito da Adobe, e quindi presente solo nei programmi che trattano file di tipo PDF (ad esempio Adobe Writer, o jSignPDF).

Rimane infine un ultimo punto toccato dagli standard ETSI e RFC, quello delle **marche temporali**.

<sup>19</sup> Chi vuole documentarsi in modo dettagliato può accedere al sito dell'ETSI (<http://www.etsi.org/>) e ricercare gli standard emessi (<http://www.etsi.org/WebSite/Standards/Standard.aspx>).

<sup>20</sup> XML (eXtended Markup Language) è un formato largamente utilizzato per la creazione e la gestione di documenti scambiati elettronicamente: ad esempio la fattura elettronica SEPA (Single Euro Payments Area - Area Unica dei Pagamenti in Euro) è un documento XML per la registrazione e scambio di fatture elettroniche con valenza comunitaria.

<sup>21</sup> PDF (Portable Document Format) è un formato di file basato su un linguaggio di descrizione di pagina sviluppato da Adobe Systems nel 1993 per rappresentare documenti in modo indipendente dall'hardware e dal software utilizzati per generarli o per visualizzarli. Viene largamente utilizzato per la trasmissione di documenti in formato elettronico - ad esempio le fatture.

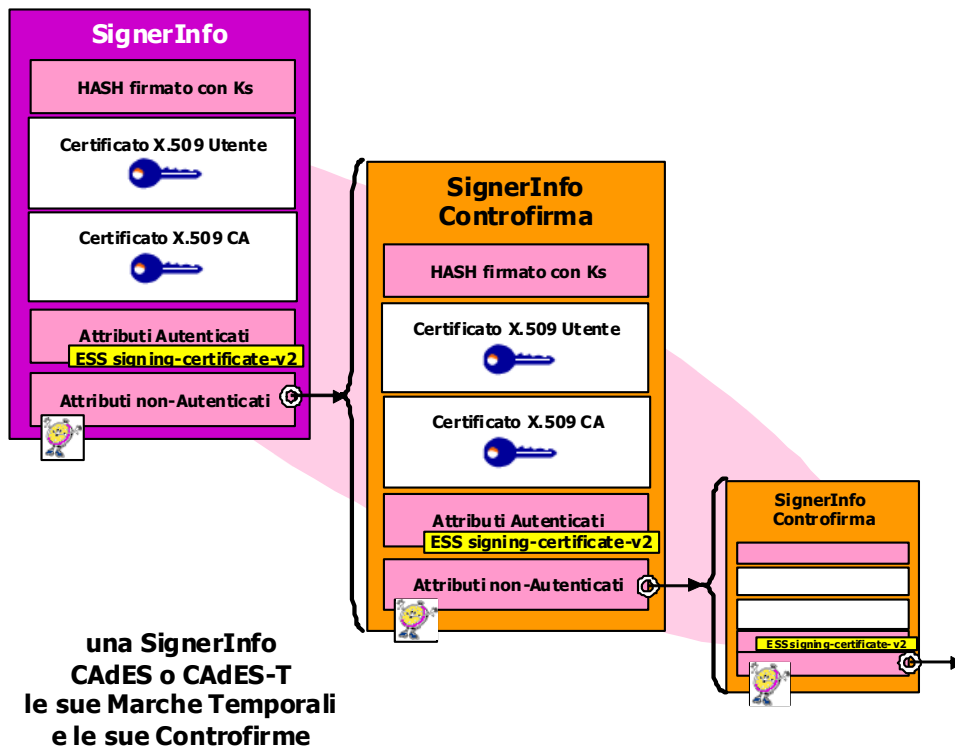
<sup>22</sup> L'attributo 'ESS signing-certificate-v2' (ESS - Extended Security Services) è definito nell'RFC 5032 e successivo 5035 (ESS Update: Adding CertID Algorithm Agility), e permette l'utilizzo di qualsiasi algoritmo di hashing. L'attributo è stato progettato per evitare attacchi basati sulla sostituzione e riemissione, e per limitare il numero di certificati da utilizzare per verificare una firma, in quanto contiene gli elementi identificativi dei certificati di firma e delle rispettive policy.

Lo standard ETSI TS 101 733 V1.7.3 (Technical Specification Electronic Signatures and Infrastructures - ESI; CMS Advanced Electronic Signatures - CADES) definisce il modo in cui una marca temporale viene associata a una firma (a essere marcata temporalmente è la firma, non il documento nel suo complesso).

La cosa è tutto sommato abbastanza semplice.

Una volta generata la firma digitale di una SignerInfo (ovvero l'impronta – hash – codificata con la chiave segreta **Ks** del dispositivo di firma, la SmartCard o l'eToken), viene calcolato un hash della SignerInfo, imbustato in una richiesta di marca temporale (TSQ – ricordate il capitolo precedente?), e inviato a una TSA, che marca temporalmente, firma digitalmente, e ritorna un TSR: questo TSR (marca temporale della firma) viene registrato come attributo non-autenticato (non firmato) nella SignerInfo.

Quindi mi trovo ad avere SignerInfo che sono marcate temporalmente, a comprovare il fatto che quella firma è stata apposta in un dato momento (nei limiti di accettabilità e affidabilità della TSA – Time Stamp Authority – che ha creato la marca temporale firmata).



Abbiamo così concluso il nostro viaggio nel magico mondo della firma digitale.

Putroppo (per chi legge) non è ancora finita.

Rimane il problema dell'accoppiamento delle marche temporali apposte a documenti (file) generici, non necessariamente firmati, che smarchiamo nel prossimo e ultimo paragrafo.

Per completezza di informazione, gli standard ETSI che interessano la firma digitale sono elencati di seguito. Se ne ho dimenticato qualcuno, mi scuso in anticipo. (A proposito: nella tabella la sigla ESI significa Electronic Signatures and Infrastructures).

ETSI TR 102 030 V1.1.1 (2002-03)	Provision of harmonized Trust Service Provider status information
ETSI TR 102 040 V1.3.1 (2005-03)	ESI: International Harmonization of Policy Requirements for CAs issuing Certificates
ETSI TR 102 041 V1.1.1 (2002-02)	Signature Policies Report
ETSI TR 102 044 V1.1.1 (2002-12)	ESI: Requirements for role and attribute certificates
ETSI TR 102 045 V1.1.1 (2003-03)	ESI: Signature policy for extended business model
ETSI TR 102 046 V1.2.1 (2004-06)	ESI: Maintenance report
ETSI TR 102 047 V1.2.1 (2005-03)	International Harmonization of Electronic Signature Formats
ETSI TR 102 153 V1.1.1 (2003-02)	ESI: Pre-study on certificate profiles
ETSI TR 102 272 V1.1.1 (2003-12)	ESI: ASN.1 format for signature policies
ETSI TR 102 317 V1.1.1 (2004-06)	ESI: Process and tools for maintenance of ETSI deliverables
ETSI TR 102 437 V1.1.1 (2006-10)	ESI: Guidance on TS 101 456 (Policy Requirements for certification authorities)
ETSI TR 102 438 V1.1.1 (2006-03)	ESI: Application of Electronic Signature Standards in Europe
ETSI TR 102 458 V1.1.1 (2006-04)	ESI: Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)
ETSI TR 102 572 V1.1.1 (2007-07)	Best Practices for handling electronic signatures and signed data for digital accounting
ETSI TR 102 605 V1.1.1 (2007-09)	ESI: Registered E-Mail
ETSI TS 101 456 V1.4.3 (2007-05)	ESI: Policy requirements for certification authorities issuing qualified certificates
ETSI TS 101 862 V1.3.2 (2004-06)	Qualified Certificate profile
ETSI TS 101 733 V1.8.1 (2009-11)	ESI: CMS Advanced Electronic Signatures (CAAdES)
ETSI TS 101 861 V1.3.1 (2006-01)	Time stamping profile
ETSI TS 101 862 V1.3.3 (2006-01)	Qualified Certificate profile
ETSI TS 101 903 V1.4.1 (2009-06)	XML Advanced Electronic Signatures (XAdES)
ETSI TS 102 023 V1.2.2 (2008-10)	ESI: Policy requirements for time-stamping authorities
ETSI TS 102 280 V1.1.1 (2004-03)	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
ETSI TS 102 573 V1.1.1 (2007-07)	ESI: Policy requirements for trust service providers signing and/or storing data for digital accounting
ETSI TS 102 734 V1.1.1 (2007-02)	ESI: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAAdES)
ETSI TS 102 904 V1.1.1 (2007-02)	ESI: Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)
ETSI TS 102 042 V2.1.2 (2010-04)	ESI: Policy requirements for certification authorities issuing public key certificates
ETSI TS 102 231 V3.1.2 (2009-12)	ESI: Provision of harmonized Trust-service status information
ETSI TS 102 176-1 V2.0.0 (2007-11)	ESI: Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
ETSI TS 102 176-2 V1.2.1 (2005-07)	ESI: Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices
ETSI TS 102 640-1 V2.1.1 (2010-01)	ESI: Registered Electronic Mail (REM); Part 1: Architecture
ETSI TS 102 640-2 V2.1.1 (2010-01)	ESI: Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM
ETSI TS 102 640-3 V2.1.1 (2010-01)	ESI: Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains
ETSI TS 102 640-4 V2.1.1 (2010-01)	ESI: Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles
ETSI TS 102 640-5 V2.1.1 (2010-01)	ESI: Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles
ETSI TS 102 778-1 V1.1.1 (2009-07)	ESI: PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES
ETSI TS 102 778-2 V1.2.1 (2009-07)	ESI: PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1
ETSI TS 102 778-3 V1.1.2 (2009-12)	ESI: PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
ETSI TS 102 778-4 V1.1.2 (2009-12)	ESI: PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile
ETSI TS 102 778-5 V1.1.2 (2009-12)	ESI: PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures

## Come accoppiare documenti e marche temporali: M7M e TSD

Con lo standard CADES-T abbiamo trovato il modo di associare alle singole firme la loro marca temporale (ove necessario). Questo per le firme.

E per i documenti marcati temporalmente nel loro complesso?

Nel capitolo precedente relativo alle marche temporali e allo standard RFC 3161, si era detto che da un qualunque file è possibile ottenere, con il supporto di una TSA, la sua marca temporale (file di tipo `.tsr`).

Il file originale e la relativa marca temporale possono:

- essere mantenuti separatamente (ad esempio un file `.doc` e il file `.tsr`): ma bisogna ricordarsi che i due file sono correlati, altrimenti la marca temporale da sola non serve a nulla;
- essere accoppiati in un unico file secondo una regola pratica introdotta a suo tempo nel panorama italiano da InfoCamere, e largamente condivisa: viene creato un file di tipo **S/MIME**<sup>23</sup>, con estensione `.m7m`, che comprende sia il file originale, ad esempio `.doc`, che la marca temporale `.tsr`;
- essere accoppiati in un unico file secondo lo standard **RFC 5544** (Syntax for Binding Documents with Time- Stamps ): in tal caso viene creato un file con estensione `.tsd`, che comprende sia il file originale, ad esempio `.doc`, che la marca temporale `.tsr`.

E con questo abbiamo terminato.

Rimangono ovviamente tutte le novità che ci riserva il futuro. Purtroppo tra le tante mie doti (e vi assicuro, non sono poche!) mi manca la sfera di cristallo, e mi trovo pertanto costretto a smettere di tediarvi.

Alla prossima.

---

<sup>23</sup> S/MIME: acronimo di Secure/Multipurpose Internet Mail Extensions, è un formato sviluppato dalla RSA Data Security Inc. basato sullo standard PKCS#7 lo standard X.509v3.

## Un po' di tecnologia: PKI

Una **PKI (Public Key Infrastructure)** è l'insieme delle risorse tecnologiche, organizzative e amministrative utilizzate e adottate da un certificatore per svolgere le proprie funzioni di **Registration Authority e di Certification Authority**. In particolare con PKI si intende una suite di componenti software e hardware orientata a gestire il ciclo completo di firma digitale basata sui certificati X.509, in termini di:

1. gestione di una **Registration Authority centrale**, eventualmente interoperante con una Struttura Anagrafica centrale di licenze e utenti;
2. gestione di una o più **Certification Authority centrali**, interoperanti con la Registration Authority ed eventualmente con la Struttura Anagrafica;
3. gestione delle **attività di richiesta, acquisizione e gestione** locale dei **certificati X.509 degli utenti** operanti all'interno di una licenza;
4. gestione delle **attività di firma dei documenti e di verifica dei documenti firmati**, con l'utilizzo di certificati X.509.

Da un punto di vista tecnico lo scenario di firma digitale può essere realizzato utilizzando certificati e chiavi segrete mantenuti su supporti ottici o magnetici (e comunque manipolabili direttamente dall'utente), oppure su dispositivi protetti quali SmartCard o HSM (Hardware Security Module). Quando i certificati e le relative chiavi segrete sono mantenuti su supporti ottici o magnetici si parla comunemente di **firma digitale debole** (dove la CPU che opera crittograficamente nel processo di firma è la stessa CPU del computer su cui sono gestiti i documenti), mentre quando i certificati e le relative chiavi segrete sono mantenuti su dispositivi protetti si parla di **firma digitale forte** (dove la CPU che opera crittograficamente nel processo di firma è una CPU dedicata operante all'interno del dispositivo protetto).

## Architettura Generale e Componenti

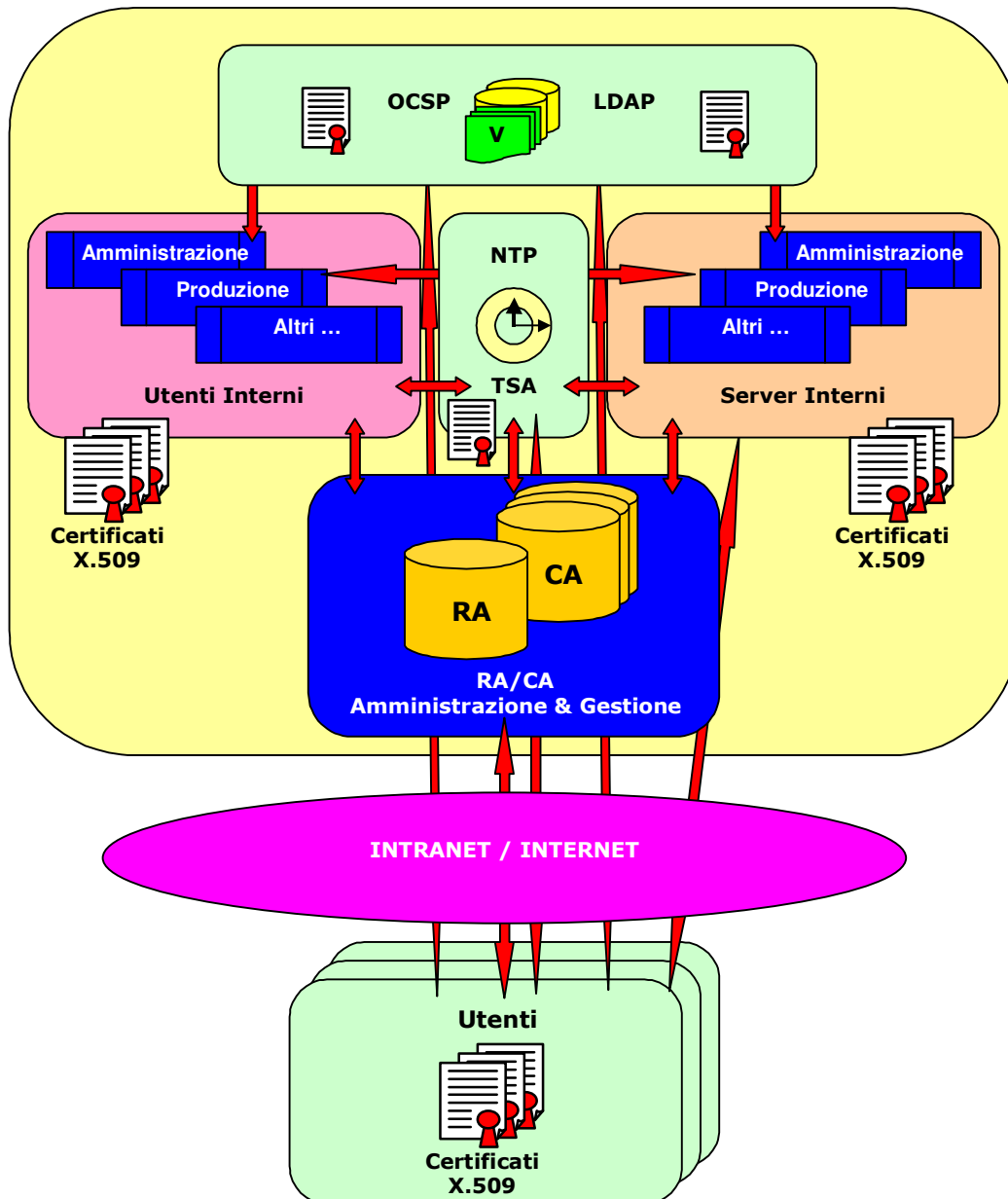
L'implementazione della firma digitale nell'ambito di un Gruppo Chiuso di Utenza viene effettuata, secondo l'architettura di una PKI completa, mediante la realizzazione, l'attivazione e la gestione dei seguenti componenti:

- **Database Centrale di Registration e Certification Authority (RA/CA-DB)**  
Database SQL nel quale sono mantenute e gestite tutte le informazioni necessarie alla registrazione notarile degli utenti (RA), le CA collegate al gruppo chiuso di utenza, le richieste ricevute dagli utenti, i certificati emessi, le liste di revoca delle CA.
- **Database del Giornale di Controllo delle Certification Authority (CAJG-DB)**  
Database SQL nel quale sono registrati gli eventi significativi della vita di ogni CA (le richieste ricevute dagli utenti, i certificati emessi, le liste di revoca delle CA).
- **Database del Giornale di Controllo della Time Stamp Authority (TSAJG-DB)**  
Database SQL nel quale sono registrati tutti gli eventi significativi della vita della TSA (marche temporali rilasciate).
- **Web di Amministrazione di RA/CA**  
Sito Web per l'amministrazione del database di Registration e Certification Authority: accesso consentito solo a utenti che operano all'interno della rete del Gruppo Chiuso di Utenza.

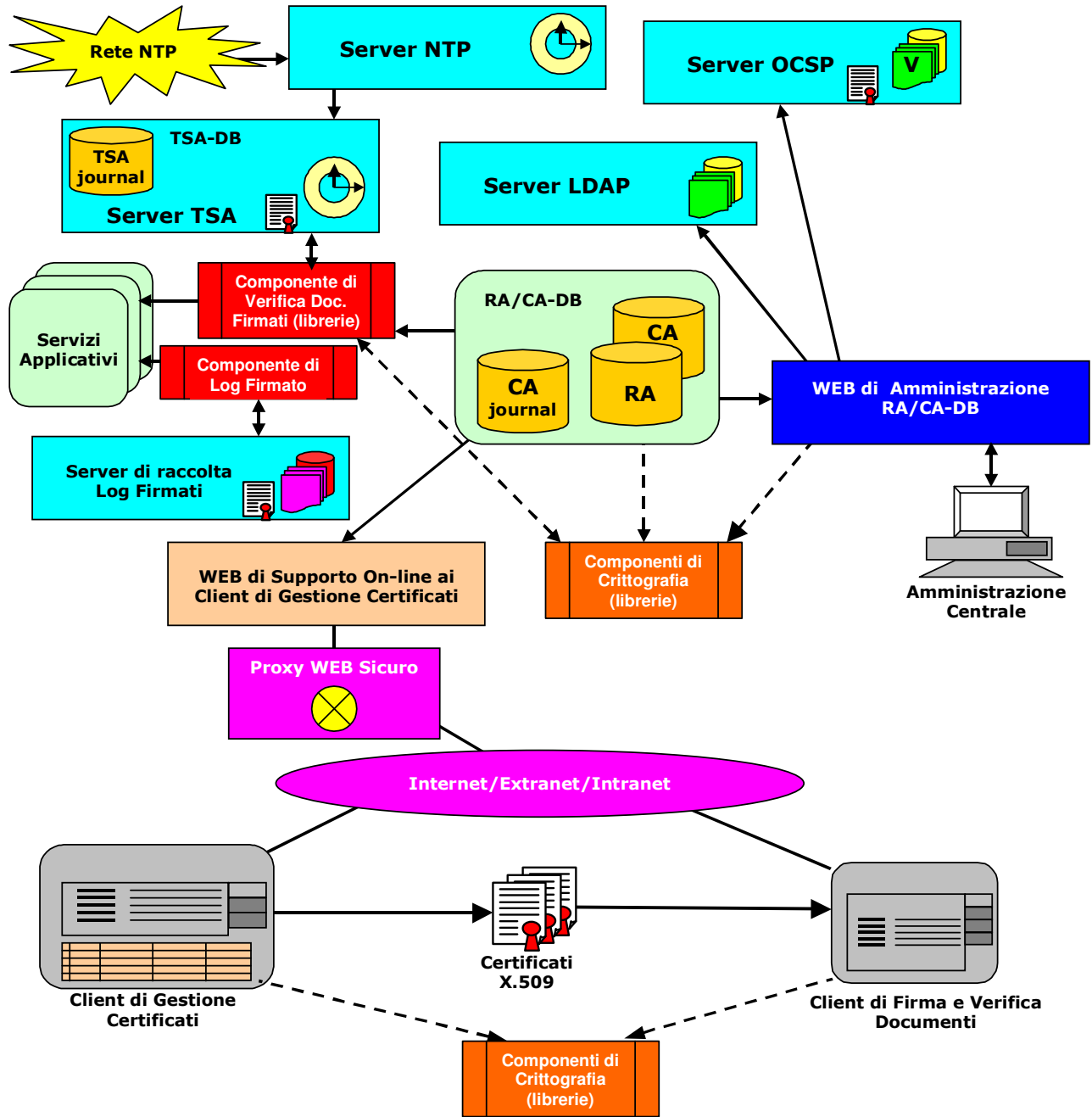
- **Server NTP (Network Time Protocol)**  
Di tipo stratum-1 o stratum-2 per l'erogazione di data/ora certa alla rete del Gruppo Chiuso di Utenza: questo server deve essere interconnesso con server pubblici (Internet) di tipo stratum-1 e stratum-2, per garantire il miglior allineamento della propria data/ora alla data/ora di Internet, anche a fronte della non disponibilità di uno o più server esterni.
- **Server TSA (Time Stamp Authority)**  
Sito Web con funzionalità TSA per il rilascio di marche temporali certificate: opera con un certificato di TSA rilasciato da una CA interna, a ciò dedicata. È aperto agli utenti del Gruppo Chiuso di Utenza che devono effettuare le operazioni di firma dei documenti con marcatura temporale.
- **Server OCSP (Online Certificate Status Protocol)**  
Server di rete per la verifica di validità dei certificati utente. Viene attivato con i dati di una CRL/CSL, e alimentato con la cadenza propria delle CRL/CSL di una CA: è aperto al Gruppo Chiuso di Utenza per la verifica di validità certificati.
- **Server LDAP (Lightweight Directory Access Protocol)**  
Database di rete per la pubblicazione dei certificati emessi, delle CRL (Certificate Revocation List) e delle CSL (Certificate Suspension List) delle CA. Viene alimentato costantemente con i certificati emessi dalle singole CA e con le relative CRL/CSL: è aperto al pubblico (Gruppo Chiuso di Utenza) per la verifica dei certificati e delle CRL/CSL.
- **Client di Gestione dei Certificati Utente**  
Applicativo Client di Gestione dei Certificati utente: richiesta e scarico dei certificati, gestione locale dei certificati sulle workstation degli utenti.
- **Supporto on-line ai Client di Gestione dei Certificati Utente**  
Sito Web dedicato e protetto dagli accessi esterni, su cui opera un insieme di CGI per la gestione on-line dei Client di Gestione dei Certificati. Le CGI accedono al database RA/CA-DB per il login degli utenti, il supporto alla preparazione delle richieste, l'acquisizione delle richieste di certificazione, il rilascio dei certificati emessi.
- **Client di Firma Digitale dei Documenti**  
Applicativo Client di Firma Digitale, in grado di richiedere marche temporali certificate al server TSA, per la firma digitale dei documenti utente, la produzione di documenti firmati con data certa, la verifica di documenti firmati con accesso alle liste di revoca delle CA emittenti.
- **Componenti di Crittografia**  
Librerie statiche e dinamiche che implementano le API necessarie alla gestione crittografica dei certificati, delle richieste, delle liste di revoca, eccetera. Organizzate in due gruppi specializzati, uno per i programmi server e uno per i programmi client.
- **Componenti di Verifica dei Documenti Firmati**  
Libreria utilizzabile sia sui server applicativi centrali che dal programma applicativo Client di Firma Digitale per effettuare la verifica di firma dei documenti, della data certa e delle liste di revoca della CA emittente.

La figura seguente illustra l'architettura generale della PKI, evidenziando, all'interno del Gruppo Chiuso di Utenza:

- l'**infrastruttura centrale** di Amministrazione e Gestione della RA e delle CA;
- il **sottosistema di gestione temporale** e delle marche temporali NTP-TSA;
- il **sottosistema di pubblicazione e verifica di certificati e CRL/CSL** (LDAP e OCSP);
- l'**insieme dei server interni della PKI** che possono effettuare la firma automatica di documenti, azioni, messaggi per conto degli operatori del sistema;
- l'**insieme degli utenti interni** alla organizzazione centrale, che utilizzano il sistema di firma digitale per la richiesta di certificati di navigazione e di firma e per la firma di documenti;
- l'**insieme degli utenti esterni**, che utilizzano il sistema di firma digitale per la richiesta di certificati di navigazione e di firma e per la firma di documenti.



La figura seguente illustra invece l'architettura della PKI in termini dei componenti funzionali.



# Mappa degli Standard

Il mondo della firma digitale è definito e regolato da un insieme di standard. La cosa dovrebbe semplificare le cose, ma la complessità del problema e il numero di attori coinvolti ha in effetti complicato ulteriormente il quadro della situazione, lasciandoci alle prese con una miriade di sigle, codici, comitati ed enti.

È un pò come guardare un batuffolo di cotone da varie angolazioni, cercando di distinguere e interpretare la trama delle singole fibre.

## Standard per la Firma Digitale

