



Firma Digitale e Non

Clizio Merli



Indice

INDICE	2
PREFAZIONE	3
LA FIRMA.....	4
FIRMA ELETTRONICA	5
FIRMA DEBOLE (SEMPLICE).....	5
FIRMA FORTE (DIGITALE).....	5
<i>Firma Forte Semplice</i>	6
<i>Firma Forte Qualificata</i>	6
<i>Firma Forte Avanzata</i>	6
<i>Firma Forte Avanzata e Autenticata</i>	6
CRITTOGRAFIA, RISERVATEZZA E SPUDORATEZZA.....	7
CRITTOGRAFIA: L'ARTE DELLA RISERVATEZZA.....	7
CRITTOGRAFIA: LE CHIAVI	8
CRACKING: L'ARTE DELLA SPUDORATEZZA	10
CERTIFICATI E CERTIFICATORI	12
I CERTIFICATI E LO SCENARIO DELLA FIRMA DIGITALE.....	12
IL CERTIFICATORE E LE SUE RESPONSABILITÀ.....	14
REQUISITI FORMALI PER IL RILASCIO E LA GESTIONE DEI CERTIFICATI	17
CERTIFICATION AUTHORITY: OPERATIVITÀ.....	18
UN PO' DI TECNOLOGIA: PKI.....	20
ARCHITETTURA GENERALE E COMPONENTI	20
MAPPA DEGLI STANDARD.....	24

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.

Comunque questo libretto 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 2005) 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 rilasciate dalle Camere di Commercio per la firma digitale aziendale delle dichiarazioni dei redditi, e 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, se richiedete a un motore di ricerca di elencarvi le pagine che parlano di firma digitale, otterrete uno sproloquio di siti in cui troverete di tutto e di più, ma soprattutto miriadi di personaggi esoterici (avvocatocchi, aiuti contabili, praticoni, pseudo-esperti, maghi, chiaccheroni e simili ammenicoli) che parlano 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 stanno effettivamente parlando.

Oppure accederete ai siti dei fornitori delle tecnologie sviluppate a corredo della firma digitale: SmartCard, lettori di SmartCard (che in effetti permettono anche di scriverle, ma nessuno lo dice), HSM, software di firma e di verifica, PKI, prodotti aderenti a tutti gli standard del pianeta (che come risultato immediato spesso non riescono nemmeno a essere interoperabili, ovvero compatibili, con sè stessi).

E in mezzo a questo baluginare di sigle, discorsi, articoli, l'unica cosa che forse riuscirete a capire è che in un mondo sempre più rivolto all'open-source una pletera di non ben definiti professionisti e aziende stanno operando in base al più bieco approccio proprietario¹. 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

¹ 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 un 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.

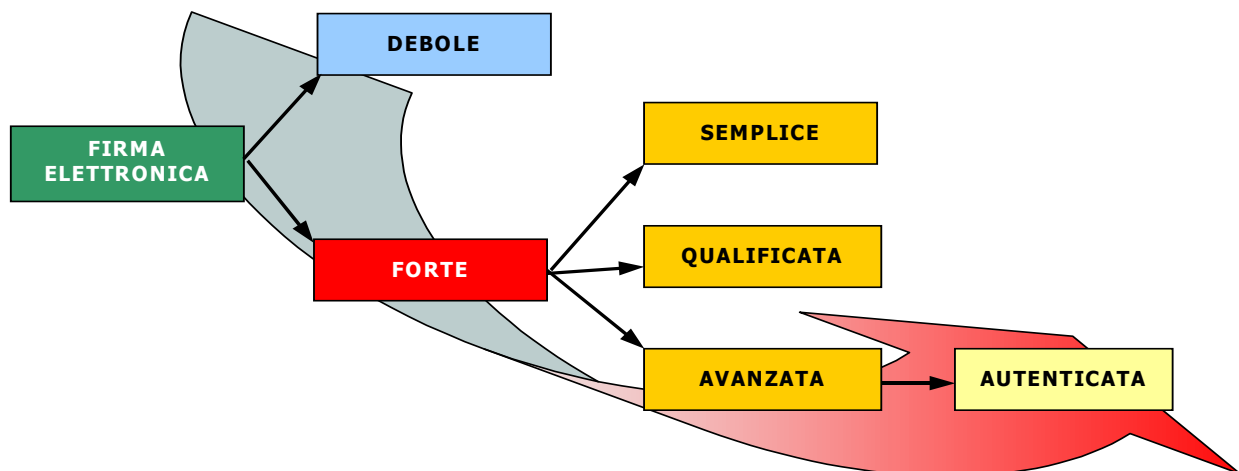
La cosa ha sicuramente un sapore romantico, specialmente per chi ama i libri e la lettura (come ad esempio chi scrive). Ma la stragande maggioranza dei pezzi di carta che firmiamo ha ben poco di romantico: scontrini delle carte di credito, richieste di ferie, documenti bancari, documenti aziendali, e 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.

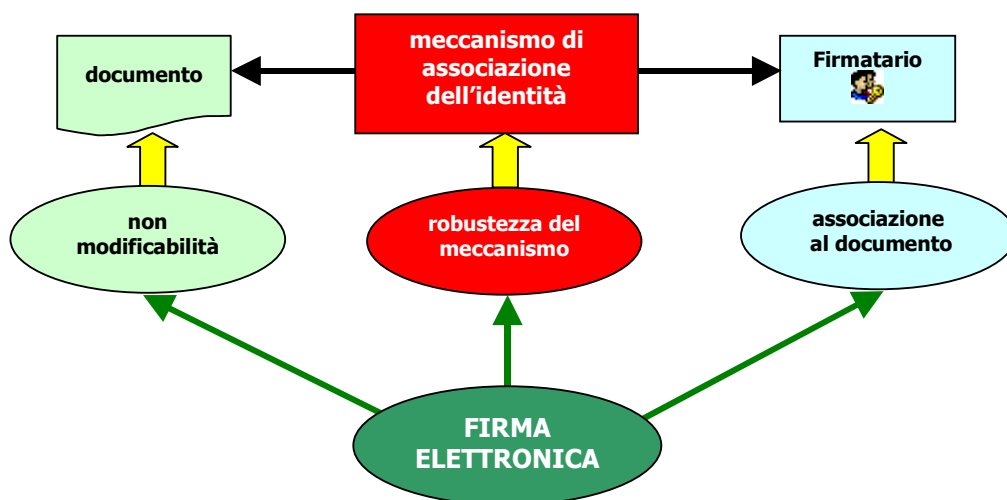


Proviamo ad analizzare il significato dei rettangolini di questa figura.

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 scoperte 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 internazionale².

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 credenziali³ 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 né 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 di 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).

² 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.

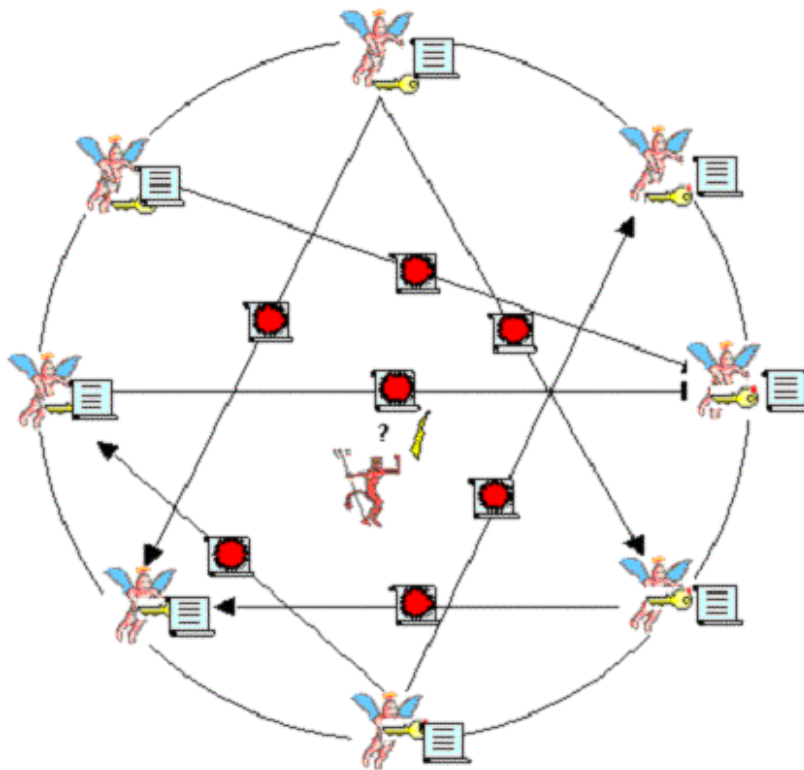
³ Il termine 'credenziali di firma' indica l'insieme delle informazioni di identità e di calcolo necessarie a eseguire il meccanismo di firma digitale (vedi capitolo successivo).

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 di 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:

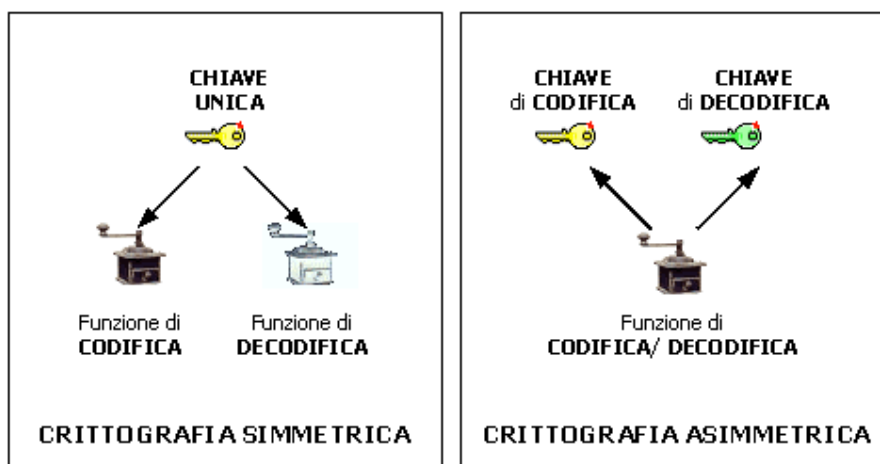
- funzione matematica
- parametro numerico (chiave)

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

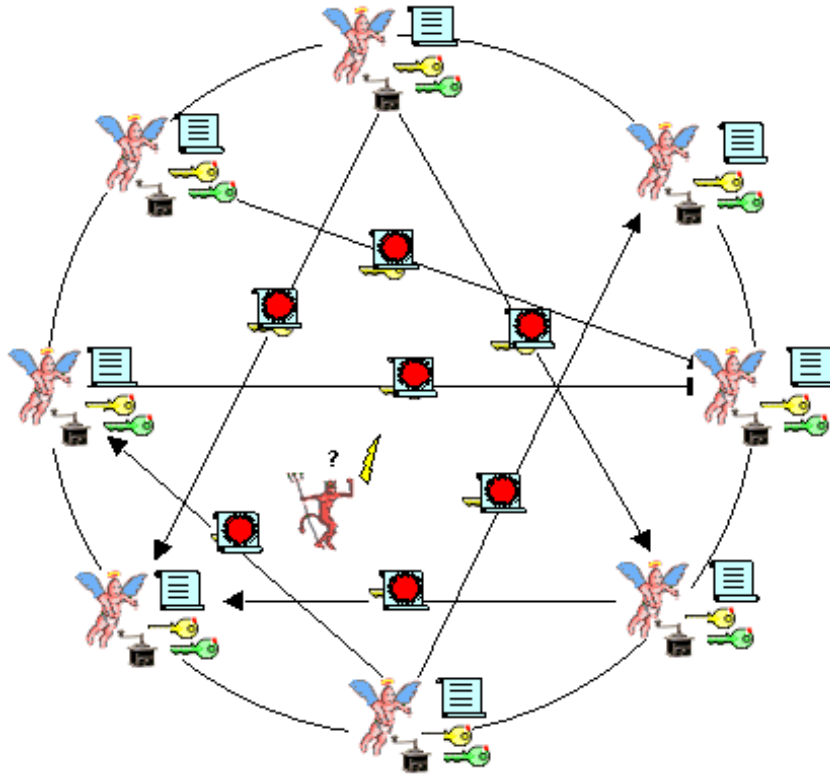
Perché il vero problema è rappresentato dalle chiavi e non dalle funzioni?

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.



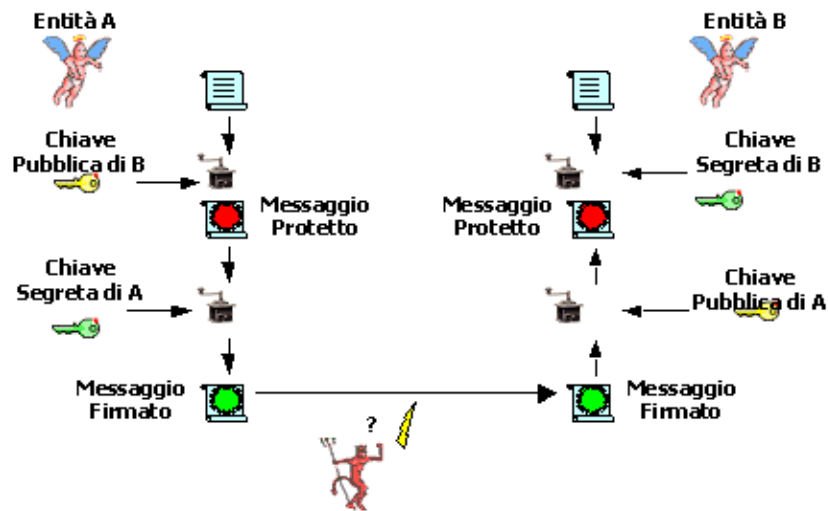
L'uovo di Colombo!

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 ...⁴

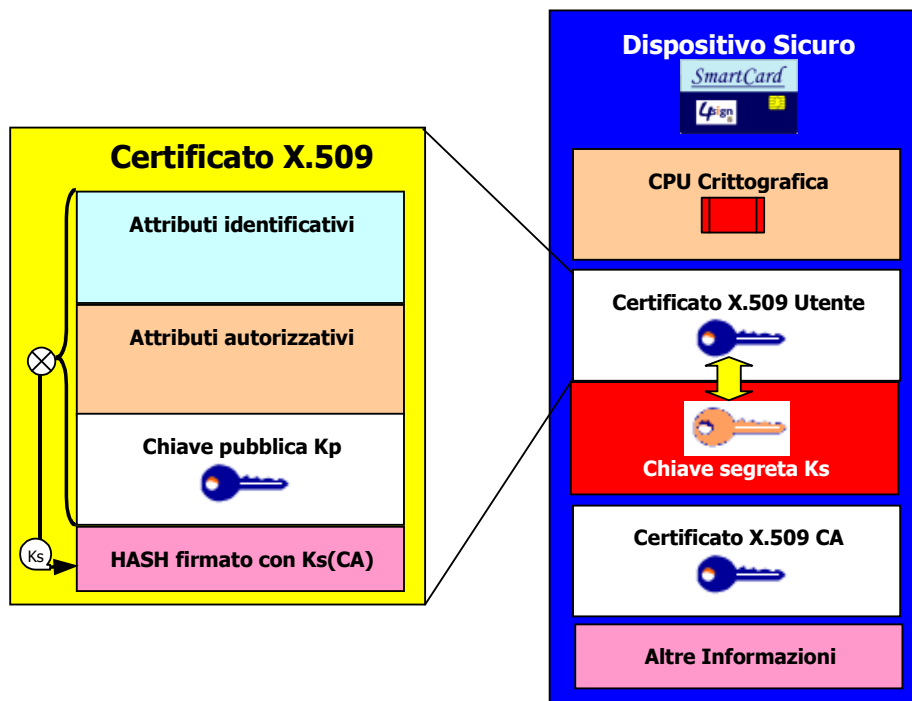
⁴ Almeno per ora!

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.

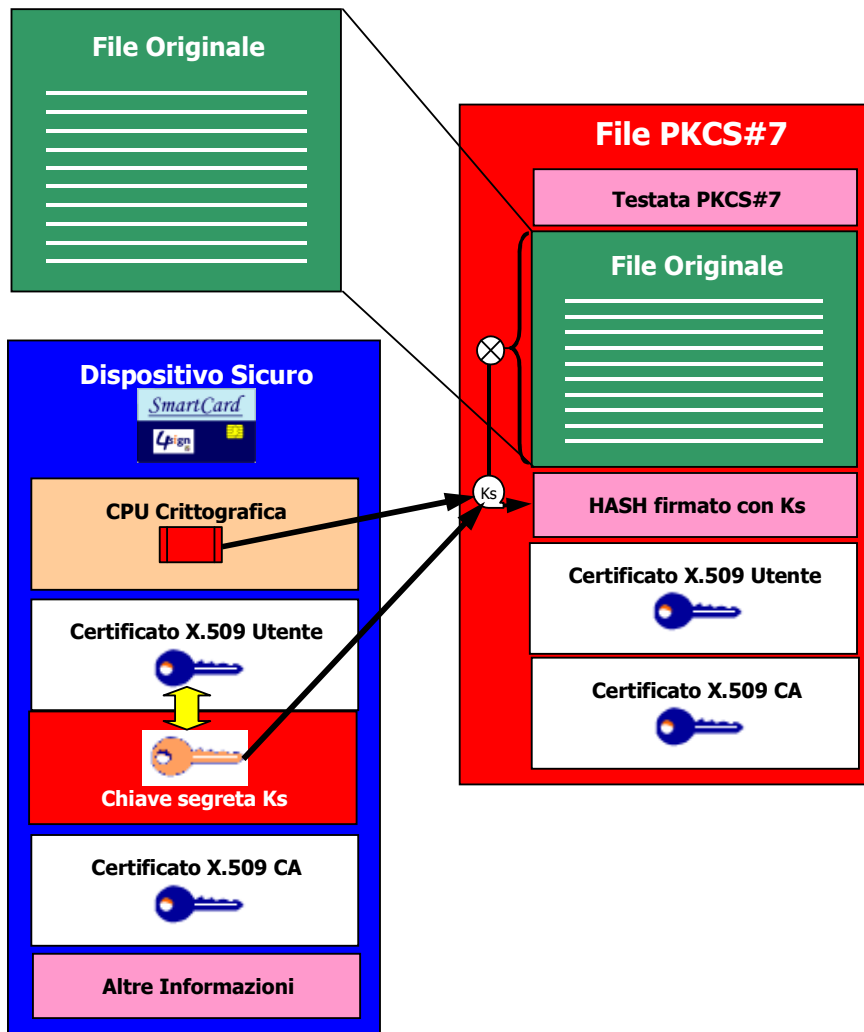
Un certificato di firma digitale è un **contenitore** che permette di **associare una chiave pubblica a un soggetto**: il processo di firma digitale viene invece effettuato con il concorso della chiave segreta associata. Lo scenario complessivo è leggermente più complicato, e vede coinvolti tanto il 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#7⁵: 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.

⁵ 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.



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'HASH⁶ (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.

⁶ 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.

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**"⁷.

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 inter: 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)**

⁷ 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".

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 Authority⁸.

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 policy⁹, 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**.

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**¹⁰ 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"¹¹. 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 conseguenze¹².
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.

⁸ 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.

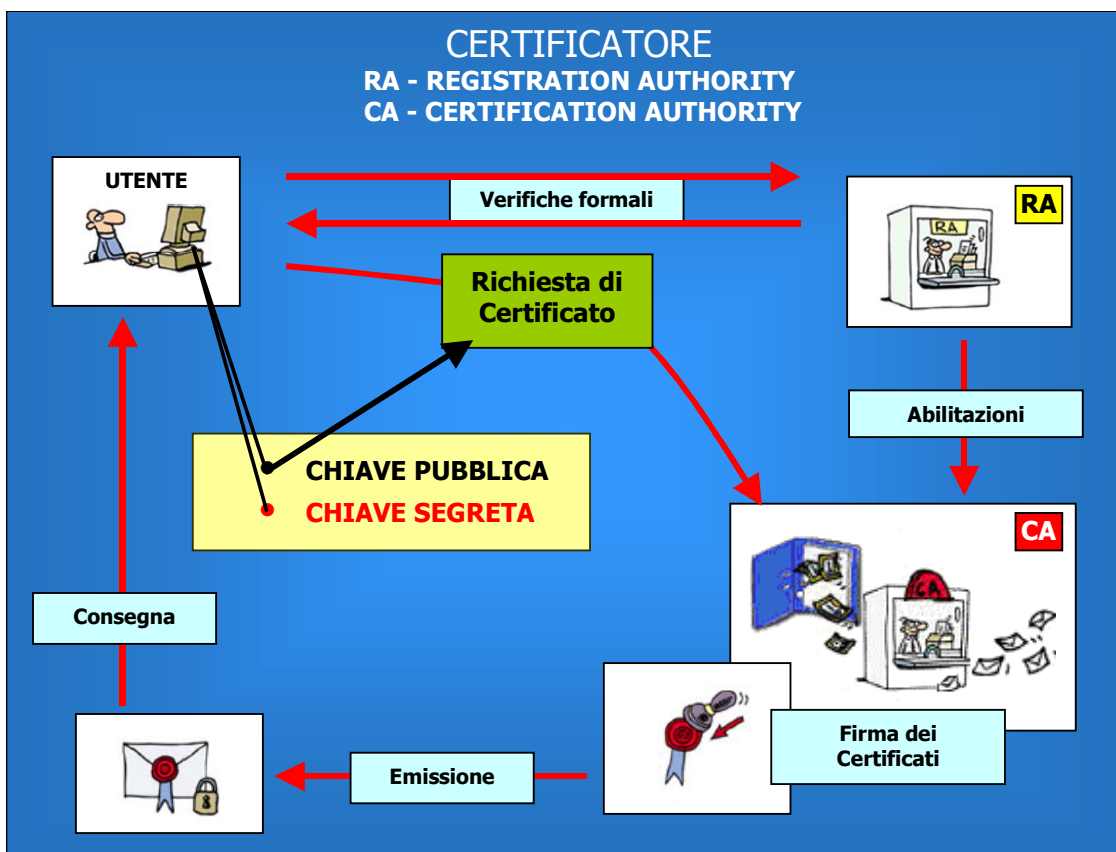
⁹ La traduzione del termine "policy" non è facile: si intende, nella pratica, un insieme di regole che permettono nel loro complesso di coordinare un dato tipo di attività. Onde evitare l'utilizzo di traduzioni estemporanee e poco attinenti, è preferibile mutuare il termine dall'inglese, e utilizzare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

¹⁰ 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.

¹¹ articolo 9 del DPR 513/97

¹² 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".

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.
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 cosumenti.

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 nel sistema del documento informatico "valido e rilevante a tutti gli effetti di legge" all'interno di un Gruppo Chiuso di Utente, e ben si comprendono i motivi che hanno spinto il legislatore italiano 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 ambito¹³.

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

¹³ 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.

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.

E' 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 sulla la 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.

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 Utente. 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.

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

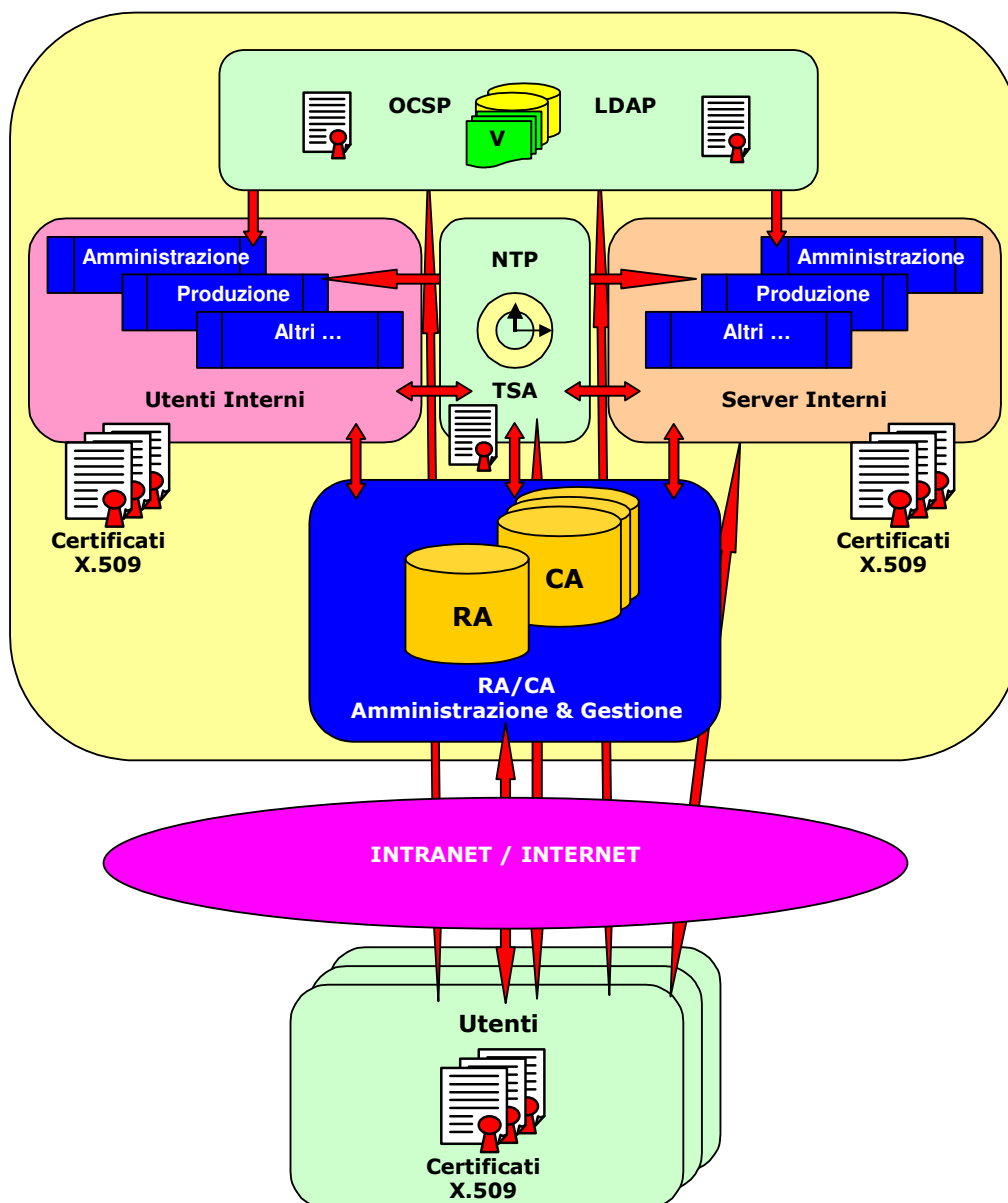
L'implementazione della firma digitale nell'ambito di un Gruppo Chiuso di Utenza viene effettuata, secondo l'architettura di una PKI completa, mediante la realizzazione, l'attivazione e la gestione dei seguenti componenti:

- **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 emittenti.

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

- 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.



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

