Firma digitale e dintorni
di cosa si compone la tecnologia.

Alla base di tutta la tecnologia di cui si tratta c'è la **crittografia** ovvero quell'insieme di tecniche atte a nascondere un messaggio in una forma indecifrabile a coloro che non sono i destinatari del messaggio stesso (il destinatario dovrà disporre di un sistema per 'decrittare' il messaggio).

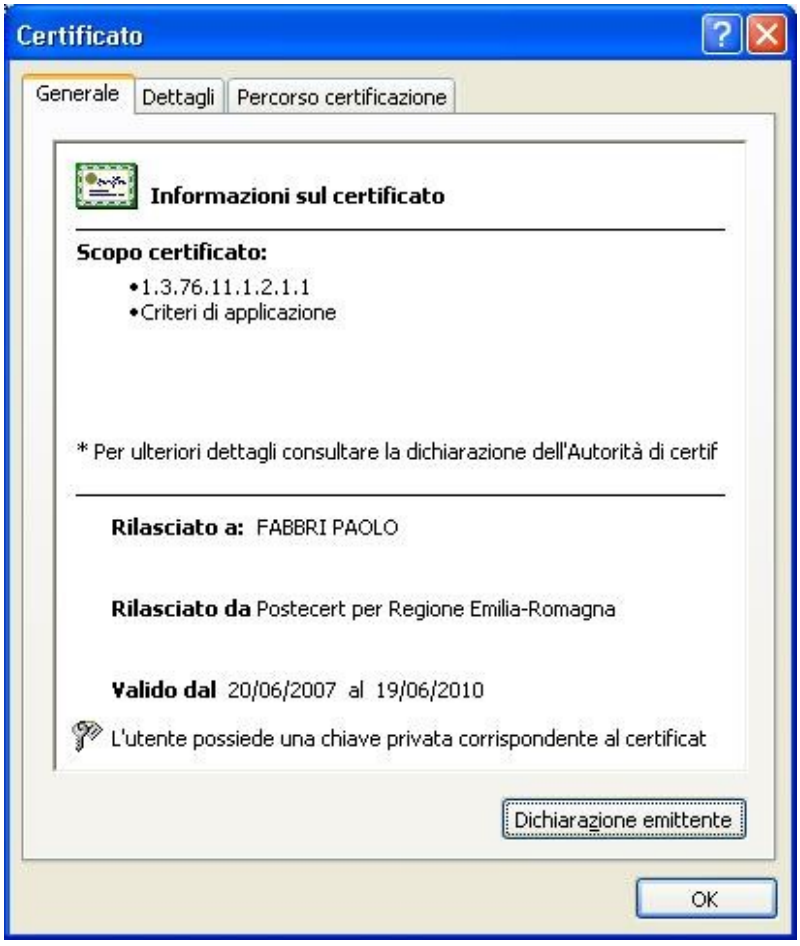
Oggi, la crittografia e altre tecniche correlate consentono l'autenticazione di un soggetto e la firma digitale apposta su un documento elettronico, con validità pari alla firma autografa.

Di seguito gli elementi che compongono la tecnologia.

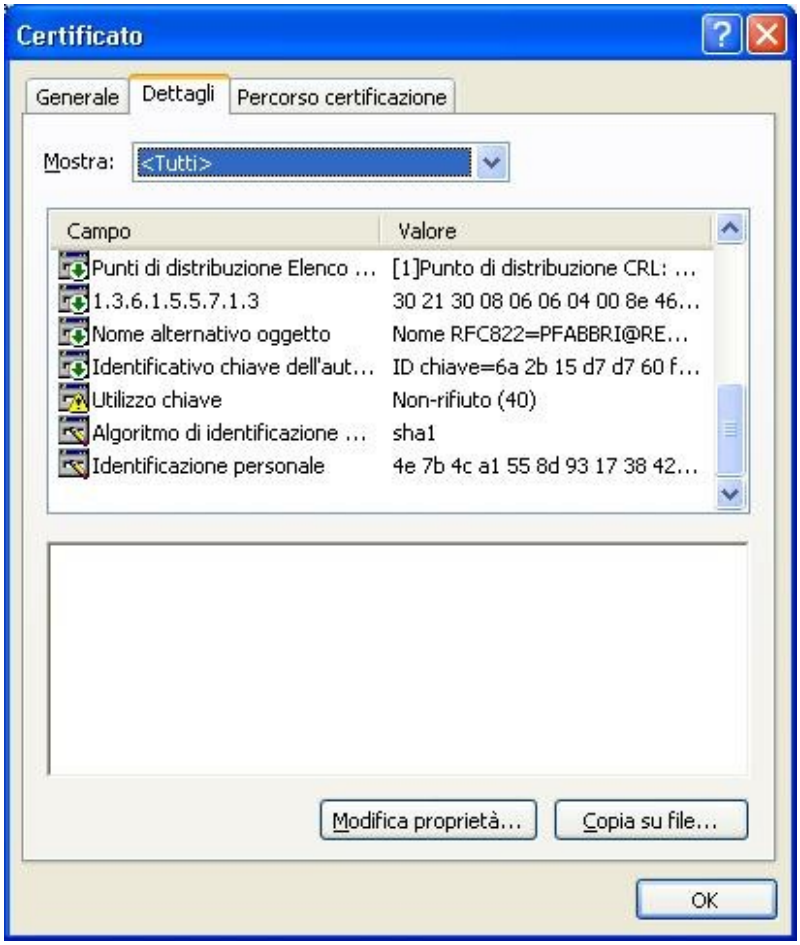
I certificati.

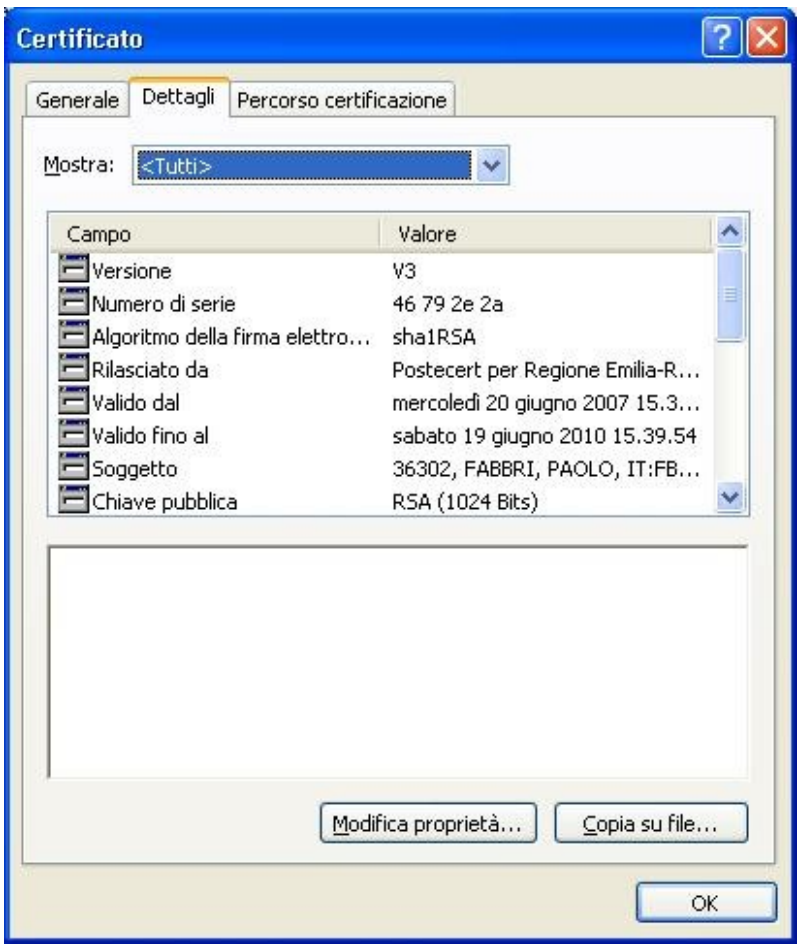
I certificati non sono altro che una raccolta di informazioni, di norma relative ad un soggetto, codificate secondo uno standard internazionale. Nel certificato è riportata anche la chiave di crittografia pubblica del soggetto.

Le immagini che seguono illustrano il contenuto di un certificato digitale:

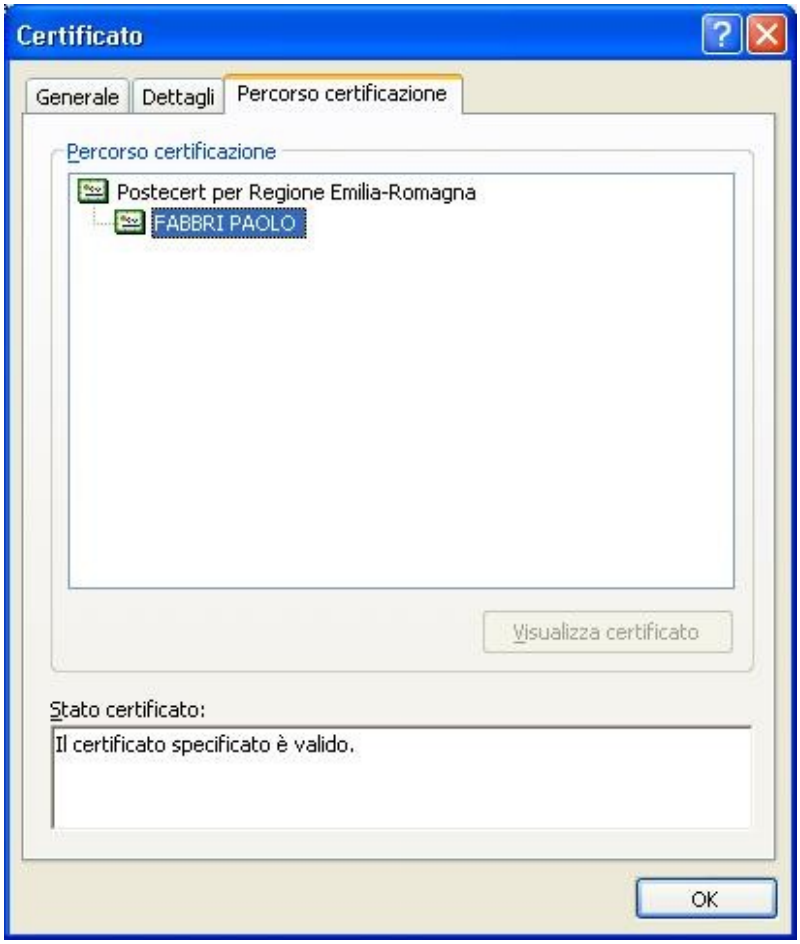


In questa immagine è indicato l'emettitore (Postecert) e il titolare (FABBRI PAOLO).


Certificato
Generale
Dettagli
Percorso certificazione
Mostra:
<Tutti>
Campo
Valore
Punti di distribuzione Elenco ...
[1]Punto di distribuzione CRL: ...
1.3.6.1.5.5.7.1.3
30 21 30 08 06 06 04 00 8e 46...
Nome alternativo oggetto
Nome RFC822=PFABBRI@RE...
Identificativo chiave dell'aut...
ID chiave=6a 2b 15 d7 d7 60 f...
Utilizzo chiave
Non-rifiuto (40)
Algoritmo di identificazione ...
sha1
Identificazione personale
4e 7b 4c a1 55 8d 93 17 38 42...
Modifica proprietà...
Copia su file...
OK


Certificato
Generale
Dettagli
Percorso certificazione
Mostra:
<Tutti>
Campo
Valore
Versione
V3
Numero di serie
46 79 2e 2a
Algoritmo della firma elettro...
sha1RSA
Rilasciato da
Postecert per Regione Emilia-R...
Valido dal
mercoledì 20 giugno 2007 15.3...
Valido fino al
sabato 19 giugno 2010 15.39.54
Soggetto
36302, FABBRI, PAOLO, IT:FB...
Chiave pubblica
RSA (1024 Bits)
Modifica proprietà...
Copia su file...
OK

Queste due immagini mostrano il contenuto del certificato, alcuni sono dati personali (tra cui importante è il codice fiscale) altri elementi specifici dell'utilizzo (si noti “Utilizzo chiave - non rifiuto”) e, importante, la chiave pubblica assegnata al soggetto.



Da ultimo il percorso di certificazione. Nel caso di certificati rilasciati a persone fisiche da parte di organismi di certificazione (come Postecert) la catena è corta, ma il meccanismo di codifica prevede la possibilità che possano esistere più intermediari tra l'utente finale e l'autorità di certificazione e nel caso qui sarebbe riportata l'intera catena di certificazione.

In Italia le **autorità di certificazione**, le sole abilitate ad emettere certificati digitali, devono essere **riconosciute dal CNIPA.**

Riassumendo i certificati sono contenitori di informazioni personali codificate secondo uno standard internazionale e contengono inoltre la chiave pubblica del soggetto.

L'hardware.

L'hardware è in generale composto da un supporto fisico atto a contenere i certificati e i cosiddetti oggetti di sicurezza.

Questa a fianco è una smart-card ovvero un rettangolino di plastica delle dimensioni di una carta di credito contenente un mircroprocessore specializzato. Perché specializzato? Perché deve proteggere l'accesso alla chiave privata (oggetto di sicurezza) che potrà essere letta solo dopo la digitazione di un PIN segreto di accesso (fornito assieme alla smart-card).

Alla smart-card corrisponde un lettore di smart-card, ovvero lo strumento che consentirà al computer cui si collega l'accesso ai contenuti della smart-card.

Ovviamente il lettore sarà corredato di opportuno software che, una volta installato, consentirà al computer di riconoscere la periferica.

Recentemente Infocamere attraverso la sua controllata Infocert ha prodotto un nuovo strumento che combina software-lettore-smart-card in un unico oggetto:

una chiavetta usb che contiene anche il software di firma, un browser già configurato e tutti gli strumenti software per gestire le operazioni di firma e autenticazione. La comodità dell'oggetto risiede nel fatto che non obbliga a nessuna installazione.

Il software.

Gli standards internazionali si sono limitati alle specifiche dei contenuti dei certificati, pertanto ogni produttore di smart-card produce anche il proprio software per la firma di documenti e i browser web hanno i loro meccanismi proprietari per il riconoscimento dei certificati digitali. L'unico standard è rappresentato dal software che implementa la crittografia di sessione nelle applicazioni che utilizzano il web, per semplificare: tutto ciò che sta dietro l'utilizzo di una url che inizia con https invece che con il semplice http.
Di solito, come nel caso delle applicazioni disponibili sul 'Fai da te dell'agricoltore' , tutta la complessità viene mascherata all'utente finale che con pochi passi si autentica all'applicazione. Tutto ciò che viene prima dell'utilizzo del browser è specifico del tipo di lettore e di smart-card acquistata ed è quindi **a carico dell'acquirente seguire i passi di installazione previsti per il proprio strumento**.

Utilizzo dei certificati

Il plurale non è usato a caso, infatti, di norma, all'interno di una smart-card conforme ai requisiti della Carta Nazionale dei Servizi (stabiliti dal CNIPA) risiedono due certificati, pressoché identici, salvo che per l'utilizzo al quale sono deputati. Un certificato è deputato alle funzioni di autenticazione e di crittografia, mentre l'altro alla firma digitale (quello che ha tra le caratteristiche il “non ripudio”). Quindi con i certificati digitali si può

1) crittografare un file ottenendo una copia dal contenuto incomprensibile e decodificabile solo con l'uso della chiave privata (la cosa infatti ha senso se la codifica la si esegue con la chiave pubblica); lo stesso meccanismo è applicabile alle e-mail da cui la PEC (Posta Elettronica Certificata).
2) autenticarsi ad un sistema, in genere attraverso il protocollo https (SSL3) che prevede lo scambio dei certificati del client (il browser web) e del server (quello che risponde alla url).

3) firmare digitalmente un file. Anche in questo caso si ottiene una copia del file originale alla quale vengono aggiunte alcune informazioni.

Firmare digitalmente un file.

In cosa consiste apporre la firma digitale? Consiste in:

- un processo che si applica ad un file, ovvero ad una sequenza di bit;
- a fine processo viene prodotto un secondo file il cui nome è identico a quello dell'originale più il suffisso ".p7m": questo è il file firmato;
- il file firmato contiene:
    - il file originale;
    - il contenuto del certificato digitale di firma (comprensivo della chiave pubblica del firmatario);
    - una impronta che per il file dato è univoca, ovvero se il contenuto del file cambia anche di un solo bit l'impronta cambia; l'impronta è crittografata con la chiave privata del firmatario.

Chiunque disponga del file firmato può tramite opportuno software:

- verificare l'identità del firmatario estraendo il certificato digitale e verificando la validità della firma;
- con la chiave pubblica presente sul certificato può decrittare l'impronta e controllare che il contenuto originale non sia stato alterato

Riassumendo

Per dotarsi di un certificato digitale conforme alle specifiche della Carta Nazionale dei Servizi è sufficiente recarsi da un certificatore autorizzato (dal CNIPA), ad esempio le Camere di Commercio (attraverso Infocert) o alle Poste (un qualunque ufficio postale).

Dal certificatore autorizzato si può acquistare la sola smart-card che è il supporto contenente i certificati digitali di autenticazione e di firma (attenzione! Per essere aderente alla CNS ci devono essere entrambe) oppure il kit completo che comprende la smart-card e il lettore (che serve a collegarla al computer). Il costo complessivo è di poche decine di Euro; le Camere di Commercio forniscono gratuitamente la prima smart-card.

Per il lettore di smart-card va seguita una procedura di installazione che consente al computer di riconoscere il dispositivo. In alternativa ci si può dotare di una Business Key presso Infocert e risparmiarsi tutta l'installazione, in quanto la chiavetta è immediatamente operativa sul PC sul quale viene collegata.

Il software delle applicazioni disponibili sul sito ermesagricoltura utilizzerà solo il certificato di autenticazione estraendone il Codice Fiscale del soggetto. Non utilizza quindi la firma digitale perché (art.64 del D.Lgs 82/2005) per le pubbliche amministrazioni è sufficiente identificare in questo modo il soggetto che presenta la denuncia. Il codice fiscale viene ricercato negli archivi del SIAR (anagrafe aziende agricole), se trovato l'utente è autenticato e può procedere nella compilazione.

La smart-card di cui ci si dota sarà valida anche per numerosi altri adempimenti (ad esempio di tipo fiscale); in altre parole un piccolo investimento verso un futuro senza più code agli sportelli.

In pratica.

Per accedere via Internet alle applicazioni del portale ermes agricoltura sezione **Sportello dell'agricoltore** "Fai da te dell'Agricoltore" è necessario disporre di due certificati:

4) uno di autorizzazione (per essere riconosciuti con certezza ed accedere alle applicazioni)
5) uno di firma digitale (per firmare digitalmente i documenti prodotti)

I certificati sono rilasciati esclusivamente a persone fisiche.
I certificati sono rilasciati esclusivamente da certificatori autorizzati.

Sul sito del CNIPA esiste un elenco ufficiale dei certificatori autorizzati attivi:

Due dei certificatori più conosciuti sono:

- **Infocamere** attraverso la società Infocert S.p.A**.**
- **Poste Italiane** attraverso la società Postecom S.p.A**.**

I certificati possono essere residenti su una smart cart (tipo bancomat o carta di credito); per utilizzare la smart card è necessario disporre di un dispositivo hardware, il lettore (ne esistono con interfaccia seriale o USB), collegato al PC ed è necessario installare il relativo "driver".
In alternativa sono disponibili dispositivi USB che non necessitano di installazioni né hardware né software e per questo motivo sono di solito più costosi delle equivalenti versioni smart cart + lettore.
I diversi certificatori li chiamano in modo diverso (per **Infocert S.p.A.** è **Business Key,** per **Postecom S.p.A.** è **PosteKey …)**

Sui siti dei certificatori sono disponibili tutte le informazioni commerciali per l'acquisto e tecniche per l'installazione e l'utilizzo. A titolo di esempio si veda:

Infocert S.p.A.	
Smart card + lettore	per il rilascio per l'installazione con particolare attenzione al punto 3 su come importare i certificati nel proprio browser.
Business Key	
Postecom S.p.A.	
Smart card + lettore	Per l'acquisto per l'installazione
Postekey	