La Firma Digitale

La sperimentazione nel Comune di Cuneo

Pier Angelo Mariani
Settore Elaborazione Dati
Comune di Cuneo

Perchè questa presentazione

- Il Comune di Cuneo, aderente alla RUPAR, ha ricevuto due kit di Firma Digitale distribuiti dalla Regione Piemonte
- E' intenzione del Comune di Cuneo sperimentare l'uso di questo strumento al fine di
  - ridurre il numero di flussi cartacei
  - diffonderne l'uso

Gli obiettivi della presentazione

Fornire le informazioni necessarie
a comprendere la teoria di base
sui documenti informatici
e sulla firma digitale

Che cos'è un documento informatico

- la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (DPR 445/2000 Art.1)
- in generale una sequenza di caratteri binari e può contenere testo, immagini, sequenze audio e video

Che cos'è non è la Firma Digitale

- Non è l'immagine digitalizzata della firma autografa

Che cosa è la Firma Digitale ?

- E’ il risultato di un processo di calcolo che parte da un documento informatico e da alcuni dati associati alla persona.
- Produce un secondo documento informatico (il documento firmato) che attesta la volontà espressa dalla persona di sottoscrivere il documento originario.
- È *l’equivalente*, per un documento informatico, della firma autografa per un documento cartaceo.

L'inquadramento giuridico

- "Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, [...] sono validi e rilevanti a tutti gli effetti di legge [...]." (L. 59/97, art. 15, comma 2 - Bassanini).
- "L'apposizione e l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo" (D.P.R.445/2000, art.23)

Il problema di fondo : la sicurezza

Come si può dare certezza
sull'identità del firmatario
e sull'integrità di un documento informatico ?

La soluzione : meccanismi di sicurezza

- La tecnologia alla base dei meccanismi di sicurezza è quella che fa uso di processi di calcolo (algoritmi) di:
  - crittografia
  - identificazione univoca (hashing sicuro)
  - servizi di certificazione
- La combinazione delle tecnologie ottiene servizi di livello più alto come:
  - autenticazione
  - integrità

Algoritmi di crittografia

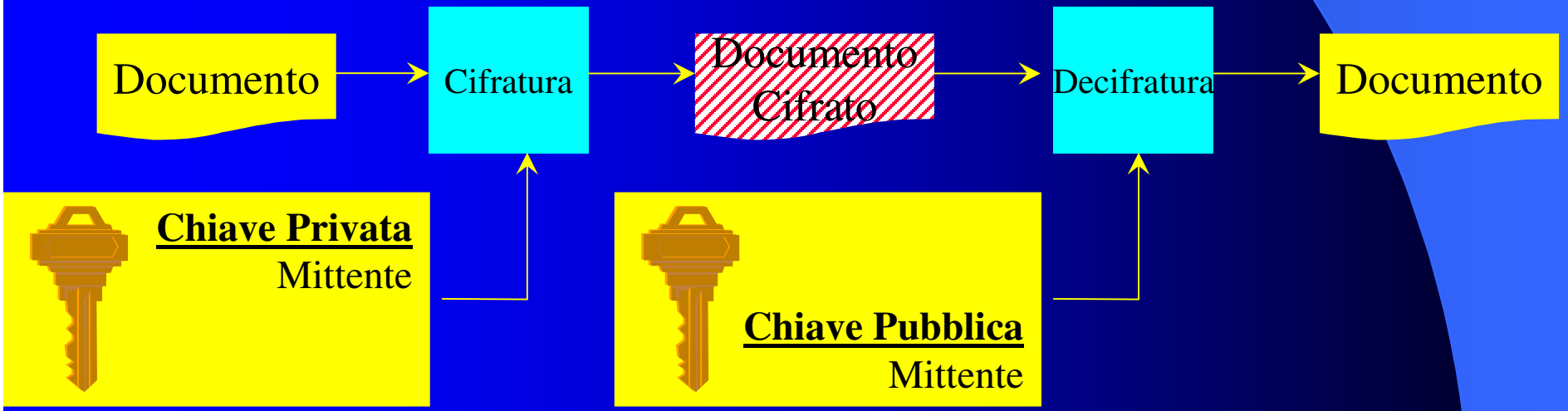
- Sono algoritmi matematici in grado di trasformare (cifrare) reversibilmente un documento informatico, in modo da renderlo non intelligibile.
- Devono soddisfare le seguenti condizioni:
  - la cifratura e la decifratura deve avvenire in funzione di una variabile detta chiave (sequenza di bit)
  - la cifratura e la decifratura sono semplici se si conosce la chiave, praticamente impossibili altrimenti
  - è praticamente impossibile dedurre la chiave confrontando un documento cifrato con quello in chiaro

Algoritmi di crittografia a chiave pubblica

- Utilizzano due chiavi distinte, con alcune proprietà fondamentali:
  - un documento cifrato con una chiave può essere decifrato solo con l'altra e viceversa;
  - le chiavi vengono generate in coppia da uno speciale algoritmo ed è di fatto impossibile ottenere una chiave a partire dall'altra;
  - una qualsiasi delle due chiavi viene detta pubblica, e può essere distribuita; l'altra, detta privata, deve essere mantenuta segreta.

Come si ottiene l'autenticità

Il documento viene cifrato con la chiave privata del mittente ed inviato al destinatario il quale lo decodifica con la chiave pubblica del mittente. Se la decodifica ha successo il mittente ha effettivamente firmato il documento.



Come si ottiene l'integrità ?

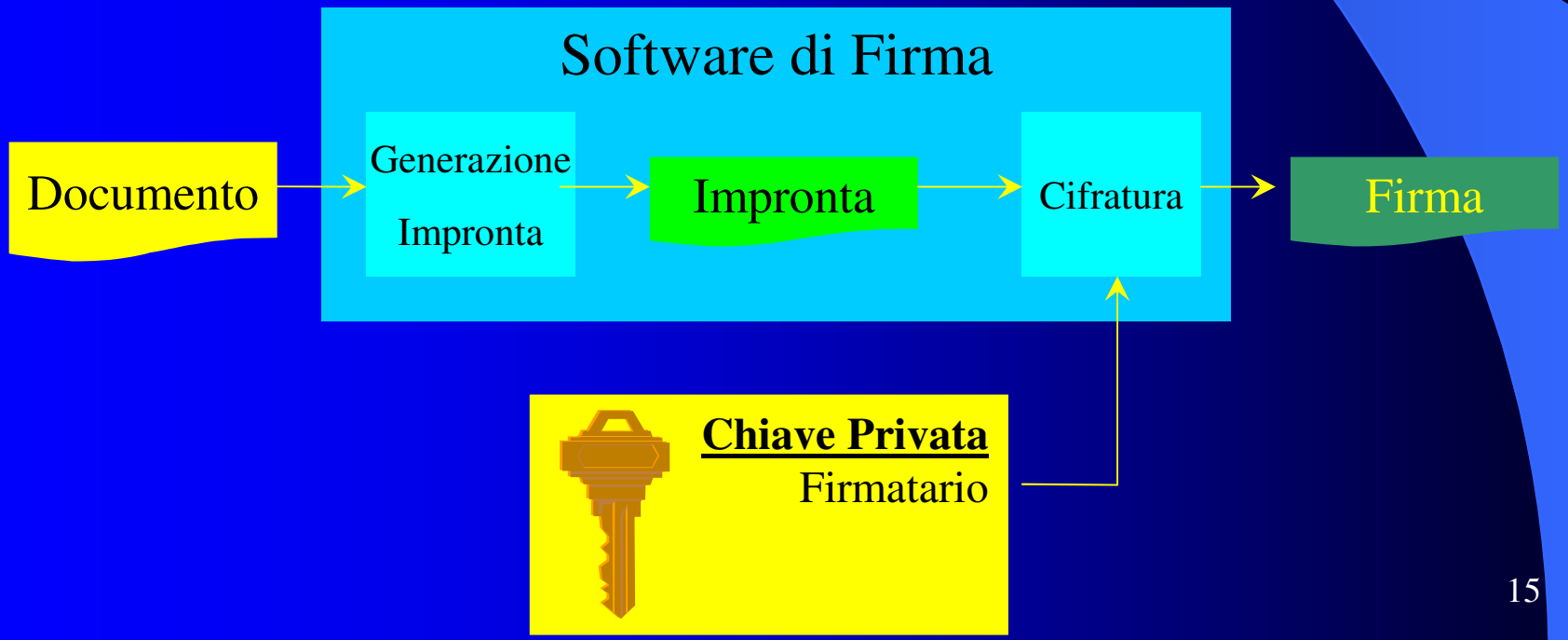
- Il processo di autenticità garantisce indirettamente anche l'integrità del messaggio trasmesso, però...
- Se il documento è grande, la cifratura può essere molto pesante.

Algoritmi di identificazione univoca del documento (hashing sicuro)

- Permettono di creare, a partire da un documento D, una sequenza di bit, di lunghezza fissa, detta impronta, che permette di identificare univocamente D.
- Qualunque modifica a D comporta una modifica dell'impronta.
- Utili per effettuare verifiche di integrità: confrontando impronte ottenute dallo stesso documento a distanza di tempo è possibile verificare se il documento ha subito alterazioni

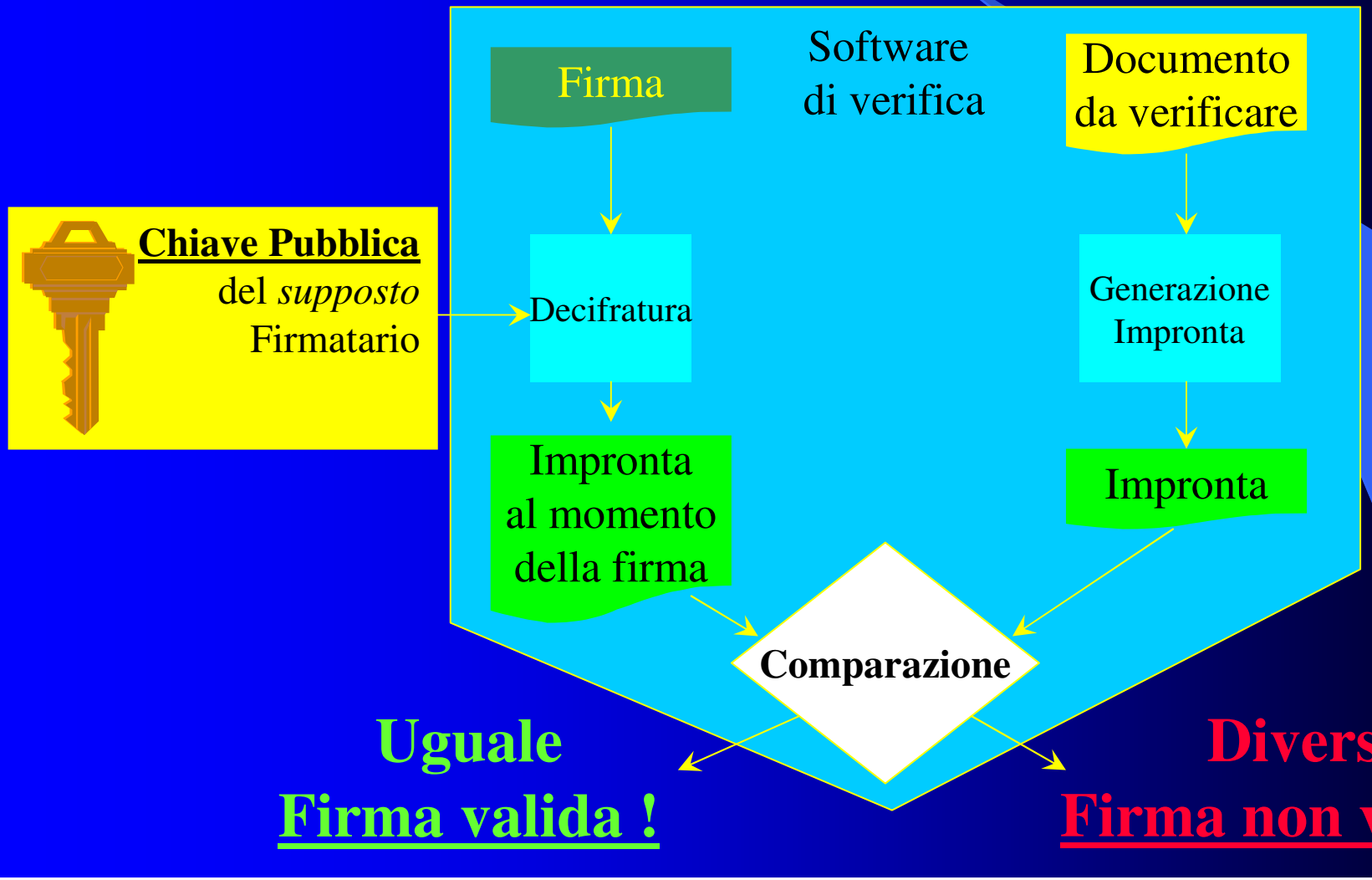
Apposizione di firma digitale

Con un software opportuno, dati un documento e la chiave privata di un firmatario, si genera una sequenza di bit detta firma digitale che prova in modo non ripudiabile la provenienza del documento "firmato" da parte del firmatario.



Verifica di firma digitale

Con un software opportuno, dati un documento firmato e la chiave pubblica del firmatario, si verifica l'autenticità di una firma digitale



Definizione elementare e caratteristiche della Firma Digitale

- Impronta di un documento informatico codificata con la chiave privata del firmatario.
- La firma digitale dipende dal documento informatico e dal firmatario.
- Documenti uguali, firmatari diversi = firme diverse.
- Documenti diversi, uguale firmatario = firme diverse

Chi fornisce le garanzie ?

- Chi assegna ad un soggetto la coppia di chiavi ?
- Come si fa a mantenere segreta la chiave privata ?
- Chi rende nota a tutti la chiave pubblica ?

Una terza parte fidata:

L'Autorità di Certificazione

Compiti dell'Autorità di Certificazione

- Registrare i titolari, previ opportuni controlli.
- Assegnare ai titolari la coppia di chiavi, utilizzando un dispositivo sicuro per la chiave privata.
- Garantire la corrispondenza il titolare e la chiave pubblica.
- Impedire l'esistenza di due chiavi pubbliche identiche.
- Rendere disponibile la chiave pubblica in un certificato.
- Pubblicare gli elenchi di certificati validi, sospesi o revocati garantendone la consultazione via Internet.

I Servizi di certificazione

- L'autorità di certificazione fornisce un certificato digitale, ovvero un documento informatico che garantisce l'effettiva corrispondenza tra la persona fisica e la sua chiave pubblica.

- Il certificato per ragioni di sicurezza, ha una validità temporale di due anni.

- Il certificato può essere sospeso o revocato.

Requisiti per svolgere l'attività di Autorità di Certificazione

- I requisiti sono gli stessi necessari per svolgere una attività bancaria.
- L'Autorità di Certificazione deve essere iscritta all'albo tenuto dall'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA).

Ruolo dell'AIPA

- Esamina, approva o respinge le domande per esercitare l'attività di Certificatore.
- Tiene l'elenco dei Certificatori .
- E' di fatto responsabile delle regole tecniche.

Che cosa serve per firmare i documenti

- Smart Card

- Lettore di Smart Card, connesso a un Personal Computer

- Software di firma e di verifica

Il Certificato

- L'Autorità di Certificazione emette un certificato per ogni chiave pubblica.

- Il certificato contiene:
  - l'identificativo dell'Autorità di Certificazione;
  - un numero progressivo;
  - l'identificativo del titolare;
  - la chiave pubblica del titolare;
  - eventuali "qualifiche" del titolare;
  - il periodo di validità.

- E' firmato digitalmente dall'Autorità di Certificazione.

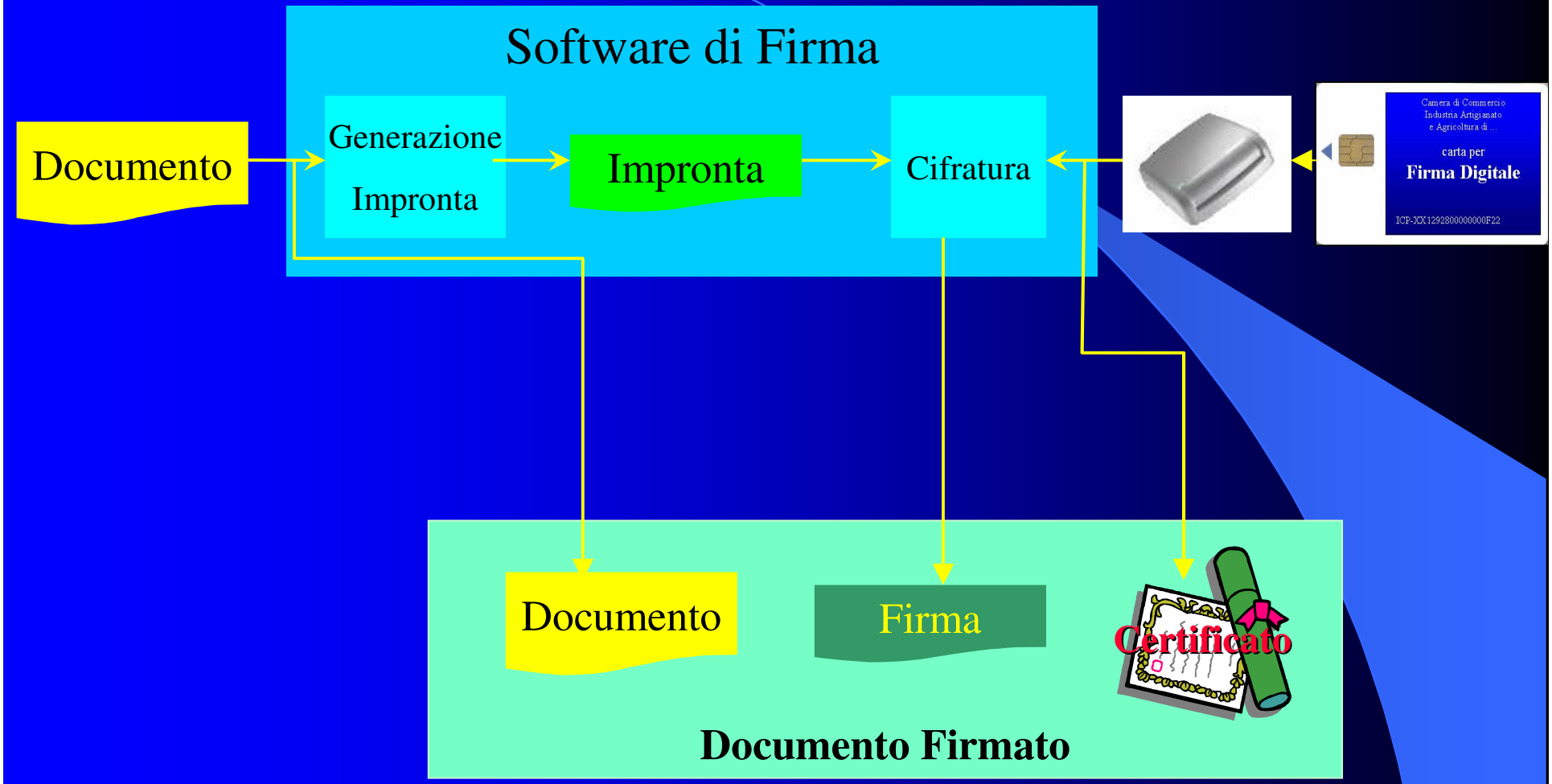
- Risiede sulla Smart Card in possesso del titolare.

- Viene allegato al documento da firmare.

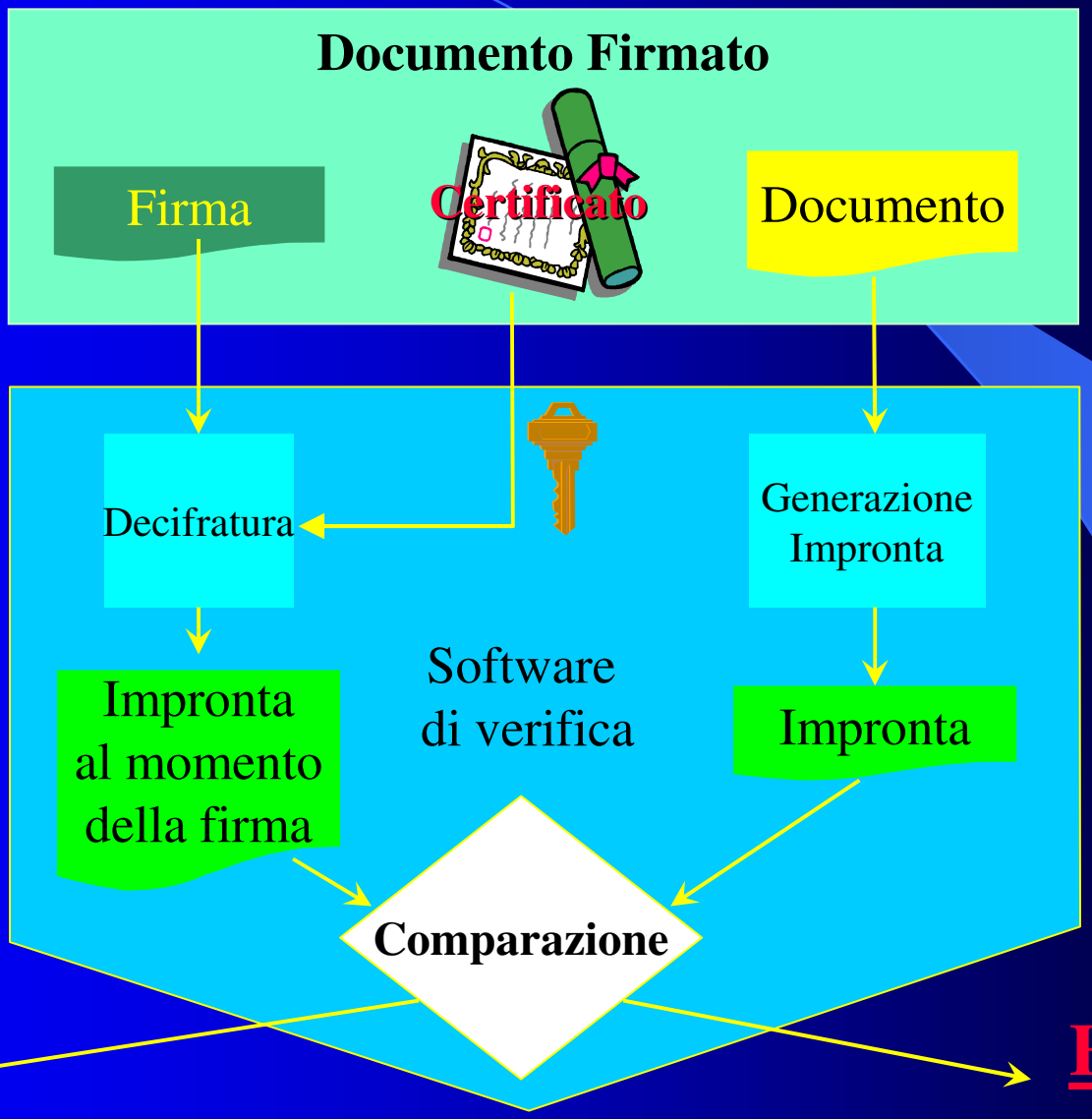
Esempio del contenuto di un Certificato Digitale (sommario)

Campi del Certificato		Valori dei campi
Numero di serie del Certificato		136036 (0x00021364)
Certificatore	Common Name	InfoCamere Firma Digitale
	Unità Organizzativa	Certification Service Provider
	Organizzazione	InfoCamere SCpA
	Stato	IT
Validità	valido dal	Feb 14, 02 11:03:37 GMT
	valido sino al	Feb 14, 04 11:03:37 GMT
Soggetto	Common Name	MARIANI/PIER ANGELO/MRNPNG63S15A182X/2002147501130
	Unità Organizzativa	RA=CSI PIEMONTE
	Organizzazione	CSI PIEMONTE
	Stato	IT
Utilizzo Chiave		Non Ripudio

Il processo di firma



Verifica di firma digitale



Uguale
Firma valida !

Diverso
Firma non valida !

Verifica del certificato

- Il software accede anche alla lista dei certificati mantenuta dal Certificatore.
- Se il certificato è valido, la verifica ha pieno successo.
- Altrimenti il responsabile del procedimento deve stabilire la validità.
- Si rende necessario conoscere la data in cui è stata apposta la firma digitale.

Le prossime attività

- Adozione del Manuale di Gestione del Protocollo (05/2002)
- Sperimentazione operativa della firma presso il S.E.D. e la Segreteria Generale (05-12/2002) :
  - Identificazione dei flussi
  - Formazione dei destinatari/mittenti
- Analisi dei risultati e dei problemi (01/2003)
- Raffronto con altri sperimentatori (05-12/2002)
- Introduzione della firma digitale nei settori comunali che lo richiederanno (2003) :
  - Identificazione ed analisi dei flussi
  - Pianificazione, definita dalla Giunta
  - Articolazione organizzativa per l'emissione delle firme

Fonti

- Presentazione RUPAR (http://www.ruparpiemonte.it/firmadig/index.htm)
- Sito Aipa: (http://www.aipa.it)
- FAQ Firma Digitale dal sito AIPA Protocollo (http://protocollo.aipa.it)
- Presentazione della Commissione Informatica del Collegio dei Ragionieri e Periti Commerciali di Torino
- Centro Tecnico della Presidenza del Consiglio (http://www.ct.rupa.it)