La Firma Digitale

Sommaruga Andrea Guido

Collegio dei Geometri e Geometri Laureati
della Provincia di Lodi


3


2


1

Firma Digitale: premessa

Questa NON e' la mia Firma Digitale !

Documenti in formato Digitale

Sono tutte quelle cose che è possibile rappresentare “numericamente” e salvare su supporto informatico. Parliamo quindi di:

- Documenti di testo
- Fogli elettronici
- Disegni
- Immagini
- Filmati / Tracce audio
- Programmi

Formato dei Documenti

- Non esiste “un formato standard” per i documenti in digitale.
- Sono strettamente legati al programma che li genera.
- Un documento digitale “vive” solo se vive il programma che lo ha scritto.
- I programmi sono compatibili con più di un formato.

Formati dei documenti

- Formati Proprietari Chiusi (Doc, Xls, Dwg)
  - Le modifiche al formato sono frequenti per introdurre incompatibilià ed obbligare agli aggiornamenti
- Formati Proprietari Pubblici (Pdf, Ps)
  - Le modifiche al formato NON sono molto frequenti
- Formati Liberi (Open Document)
  - Le modifiche al formato sono rare e decise dalla comunità degli sviluppatori

Contenuti dinamici

Nei documenti digitali è possibile inserire dei contenuti dinamici ad esempio delle informazioni aggiornate on line da internet.

- Con i contenuti dinamici i documenti “cambiano” nel tempo
- Non sono affidabili come contenuto perchè possono cambiare
- Un esempio: “il testo lampeggiante”

Documento Cartaceo: Firma

- La paternità di un documento cartaceo viene attribuita apponendo “firme autografe” e “timbro con la data” su tutte le pagine. (Vedi Atti Notarili)
- L'inalterabilià nel tempo è garantita dalla capacità della carta di mantenere le informazioni scritte
- Se ben conservata può durare anni o secoli

Documento Digitale: Firma

Un documento digitale è un “insieme di bit” che contengono informazione.

- La Firma digitale per un documento informatico consiste nell'aggiunta di ulteriori “bit” al documento
- La Firma digitale viene inserita e verificata solo mediante un programma ed internet
- La Firma digitale certifica paternità, inalterabilià del contenuto e data

Falsificabilità

- La firma autografa è “facilmente falsificabile”

- La firma digitale “non è falsificabile”
- La firma digitale “non è ripudiabile” ed è contenuta in un dispositivo di firma (es. smartcard)
- La smartcard di firma deve essere custodita gelosamente

Firma Digitale: revoche

- Ha una data di scadenza
- Può essere sospesa per un certo periodo
- Può essere revocata definitivamente
- La gestione delle revoche / sospensioni richiede di avere un database centrale (raggiungibile via internet) che consente di verificare le firme
- La “firma digitale” richiede la connessione ad internet

Marca Temporale

Anche per i documenti digitali è previsto un meccanismo analogo al timbro postale, la “Marca Temporale”

- E' una “firma” aggiunta al documento che ne certifica data ed ora
- Richiede la connessione ad internet
- Ha un costo, i kit di firma in genere propongono un certo numero di marche temporali

Dispositivi di firma

Si firma mediante un programma quindi occorre un PC, un programma ed un certificato.

- Smart Card
- Smart Card in formato SIM
- Dispositivi dedicati

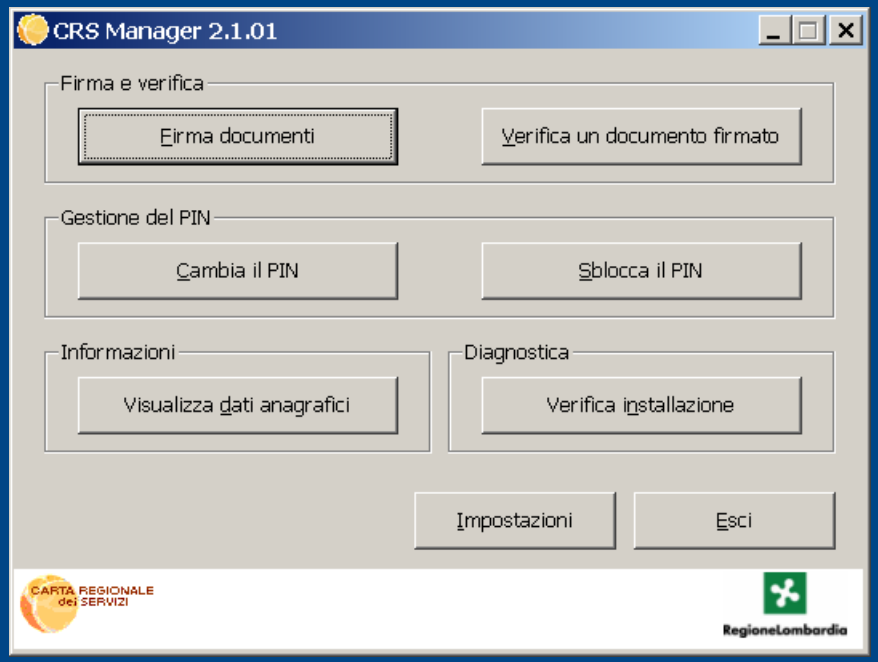
Carta Regionale dei Servizi

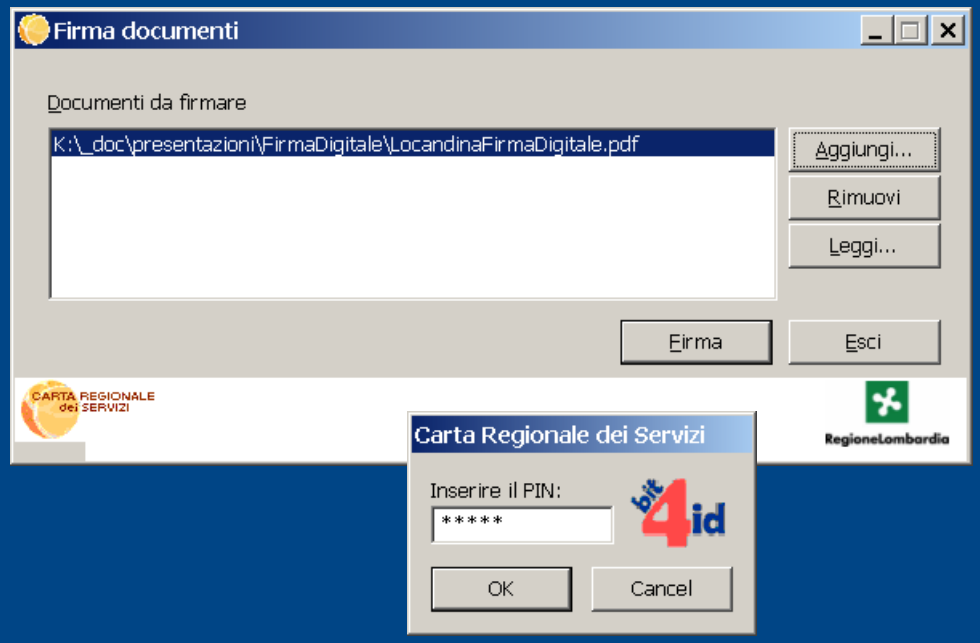
La carta regionale dei servizi contiene un certificato di firma

- E' riconosciuta dagli enti della Regione Lombardia
- Non ha validità Nazionale come firma perchè l'ente emittente (Regione Lombardia) non è una “Cetification autority” riconosciuta

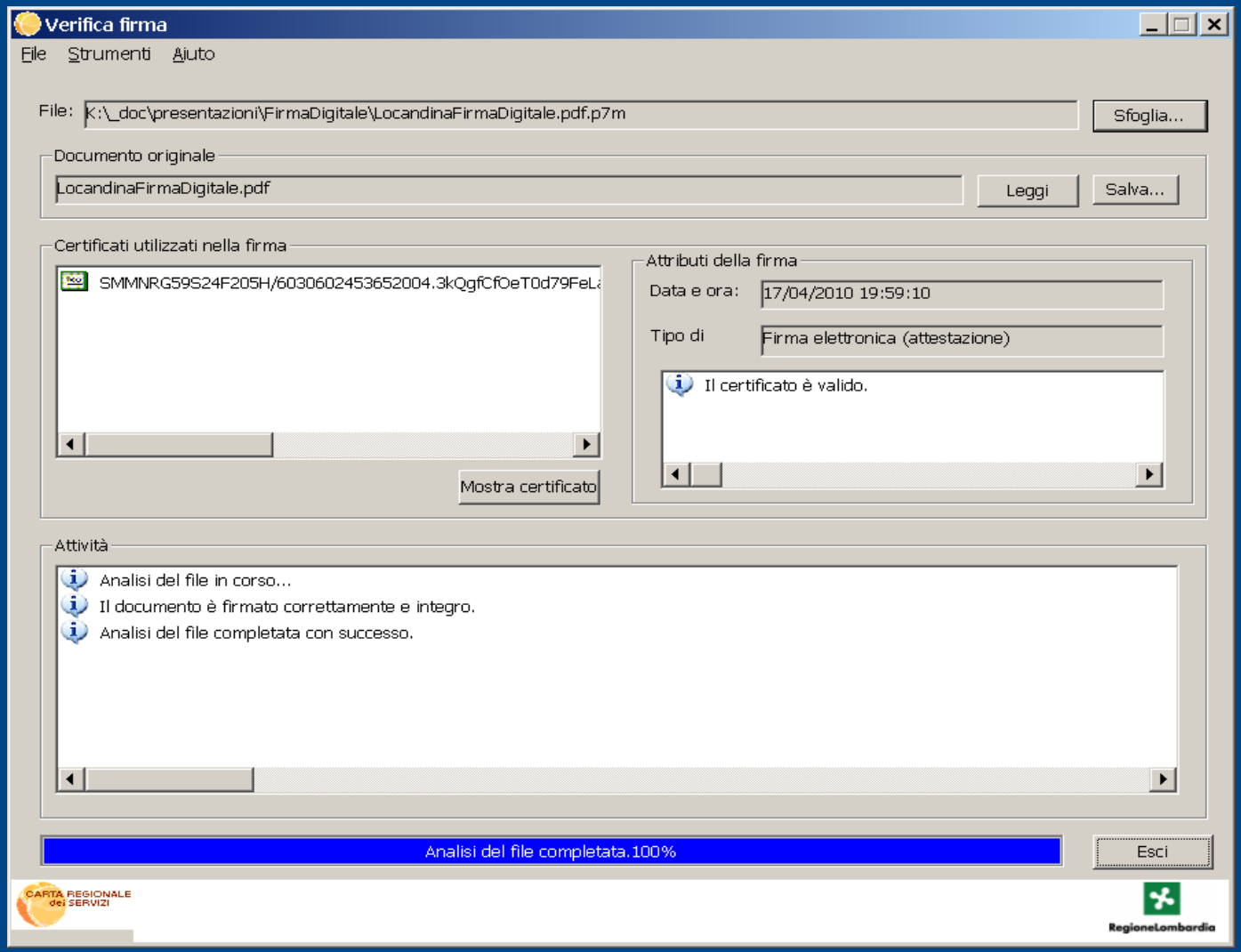
CRS manager

- Con il PIN e la CRS si può firmare un documento o verificare le firme





Verifica Firma

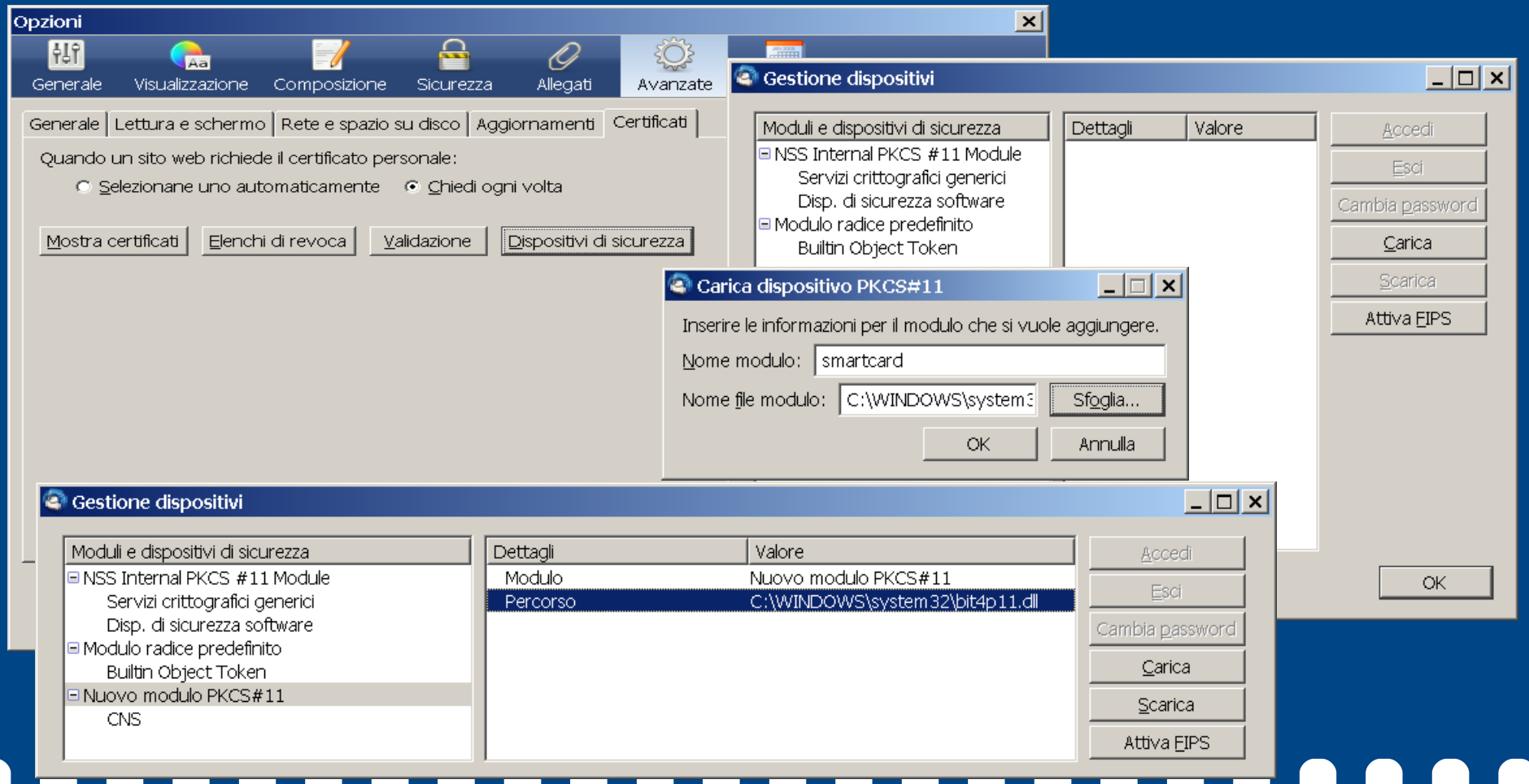


File con estensione p7m

- Un documento firmato contiene il documento originale e le informazioni di firma
- Viene salvato con estensione p7m
- Il software di verifica firma consente di estrarre il documento originale
- Il “documento originale” non viene toccato durante le operazioni di firma

Thunderbird e Firma Digitale

Dal menu Strumenti alla voce Opzioni:



Copyleft 2010 Ing. Sommaruga Andrea Guido

http://sommaruga.stnet.net