



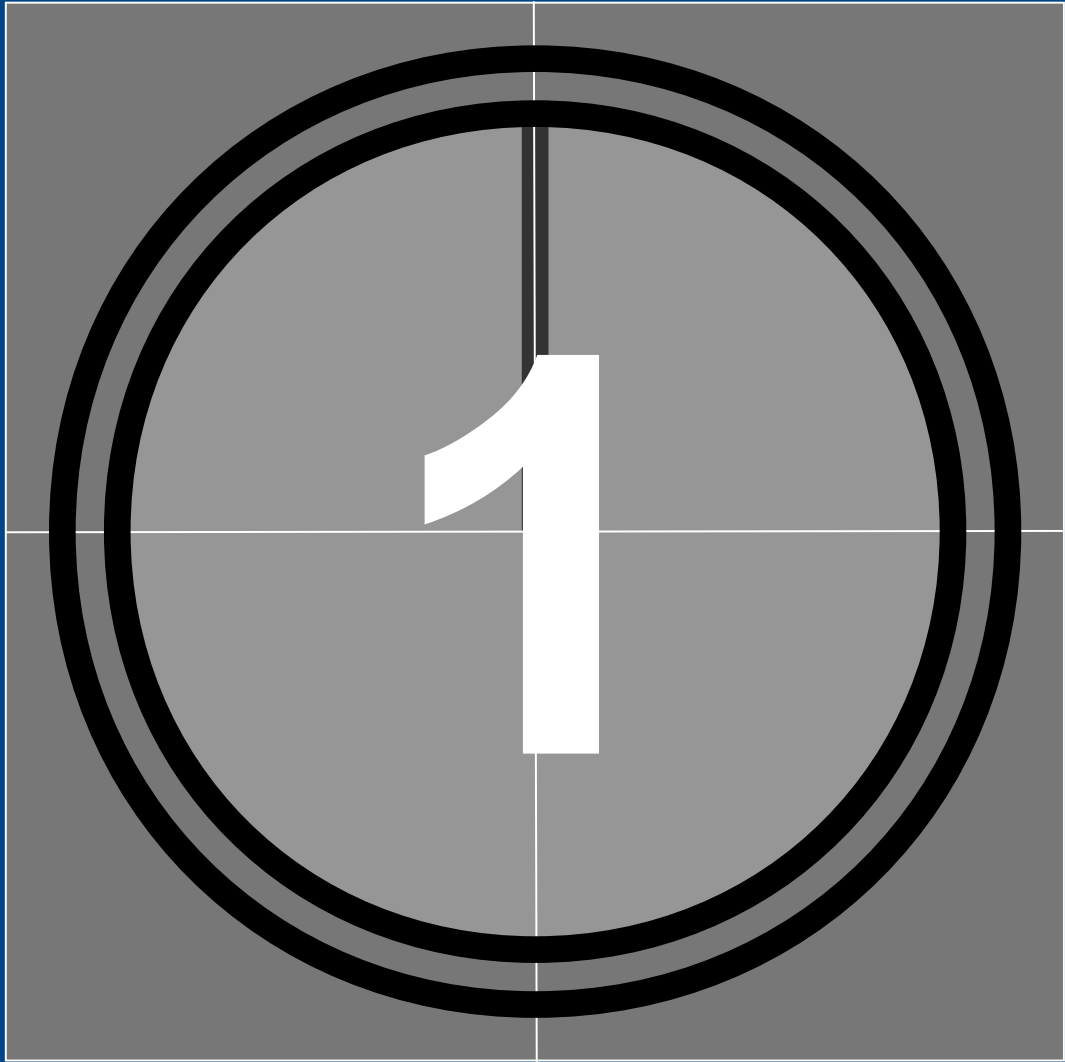
La Firma Digitale

Sommaruga Andrea Guido

Collegio dei Geometri e Geometri Laureati
della Provincia di Lodi

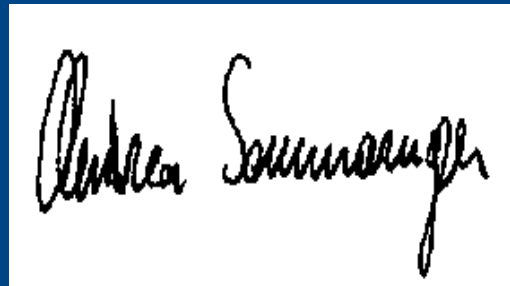






Firma Digitale: premessa

Questa NON e' la mia Firma Digitale !

A white rectangular box containing a handwritten signature in black ink. The signature is written in a cursive style and reads "Andrea Sommeruga".

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 incompatibilità 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'inalterabilità 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, inalterabilità 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

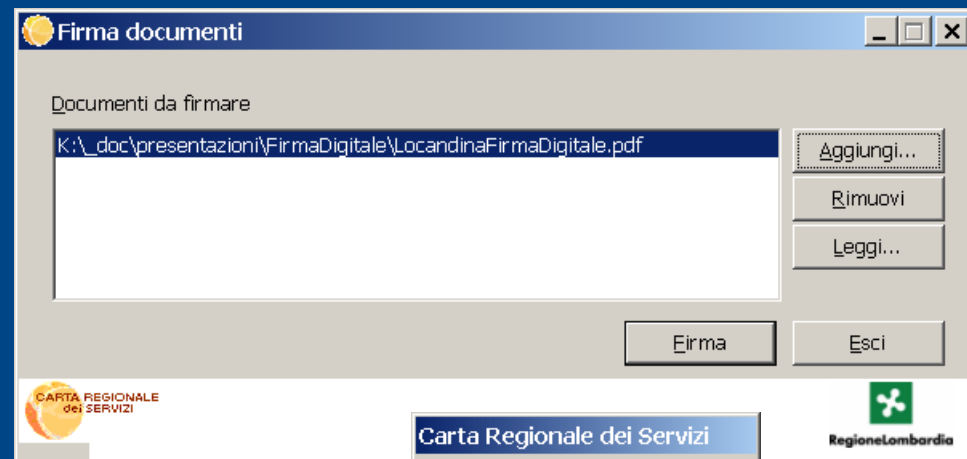
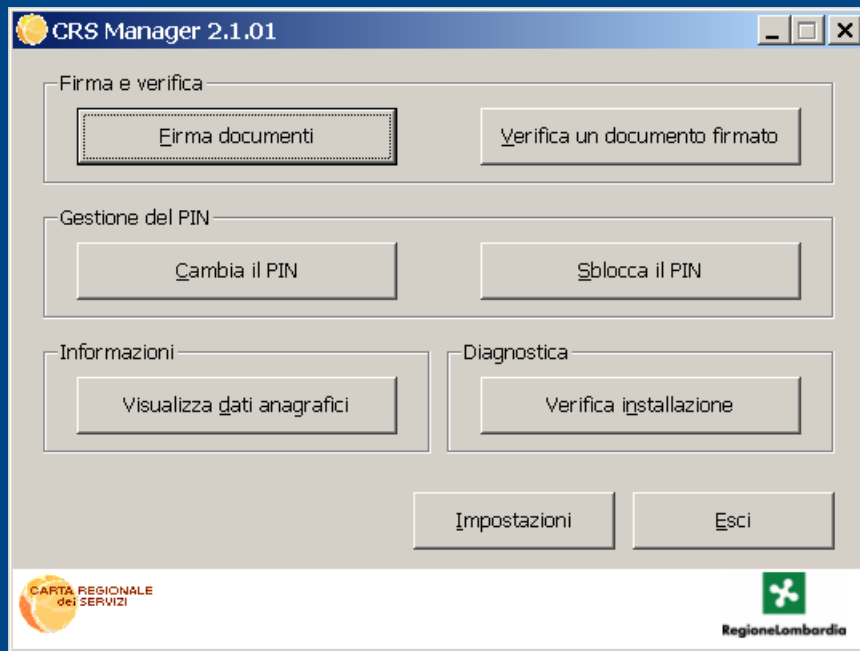
Carta Regionale dei Servizi

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 "Certification authority" riconosciuta

CRS manager

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



Verifica Firma

The screenshot shows the 'Verifica firma' application window. The title bar reads 'Verifica firma'. The menu bar includes 'File', 'Strumenti', and 'Aiuto'. The main interface is divided into several sections:

- File:** A text box contains the path 'K:_doc\presentazioni\FirmaDigitale\LocandinaFirmaDigitale.pdf.p7m' with an 'Sfoggia...' button to its right.
- Documento originale:** A text box contains 'LocandinaFirmaDigitale.pdf' with 'Leggi' and 'Salva...' buttons to its right.
- Certificati utilizzati nella firma:** A scrollable list box contains a single entry: 'SMMNRG59S24F205H/6030602453652004.3kQgfcfOeT0d79FeL:'. Below the list is a 'Mostra certificato' button.
- Attributi della firma:** A section containing:
 - 'Data e ora:' with a text box containing '17/04/2010 19:59:10'.
 - 'Tipo di:' with a text box containing 'Firma elettronica (attestazione)'.
 - A scrollable text box containing an information icon and the text 'Il certificato è valido.'.
- Attività:** A scrollable list box containing three items:
 - An information icon followed by 'Analisi del file in corso...'.
 - An information icon followed by 'Il documento è firmato correttamente e integro.'.
 - An information icon followed by 'Analisi del file completata con successo.'.

At the bottom of the window, a blue progress bar shows 'Analisi del file completata. 100%'. To the right of the progress bar is an 'Esci' button. The bottom-left corner features the logo for 'CARTA REGIONALE dei SERVIZI' and the bottom-right corner features the logo for 'Regione Lombardia'.

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:

The screenshot shows the 'Opzioni' (Options) dialog box in Thunderbird, with the 'Avanzate' (Advanced) tab selected. The 'Certificati' (Certificates) sub-tab is active, showing the 'Dispositivi di sicurezza' (Security Devices) section. A 'Gestione dispositivi' (Device Management) dialog is open, allowing the user to add a new PKCS#11 module. The 'Carica dispositivo PKCS#11' dialog prompts for the module name and file path. The file path is set to 'C:\WINDOWS\system32\bit4p11.dll'. The 'Gestione dispositivi' dialog shows a table of installed security modules.

Moduli e dispositivi di sicurezza	Dettagli	Valore
<input checked="" type="checkbox"/> NSS Internal PKCS #11 Module Servizi crittografici generici Disp. di sicurezza software	Modulo	Nuovo modulo PKCS#11
<input checked="" type="checkbox"/> Modulo radice predefinito Builtin Object Token	Percorso	C:\WINDOWS\system32\bit4p11.dll
<input checked="" type="checkbox"/> Nuovo modulo PKCS#11 CNS		

Copyleft 2010 Ing. Sommaruga Andrea Guido

<http://sommaruga.stnet.net>

- è garantito il permesso di copiare, distribuire e/o modificare questo documento seguendo i termini della Licenza per Documentazione Libera GNU, Versione 1.2, oppure ogni versione successiva pubblicata dalla Free Software Foundation;
- senza Sezioni Non Modificabili
- senza Testi Copertina
- senza Testi di Retro Copertina
- Mantenendo intatte le indicazioni di Copyleft
- la versione originale in inglese della licenza è disponibile su www.gnu.org/copyleft/fdl.html