GLI ARCHIVI INFORMATICI: PROBLEMATICHE DI INTEGRITA' NEL TEMPO

23 Novembre 2005

Fondazione Ordine degli Ingegneri di Milano
Corso Venezia

Relatore Ing. Sommaruga Andrea Guido

Firma digitale e CheckSum MD5

sommaa@stcom.com

Che cos'è la firma autografa ?

Un segno sulla carta che è associabile ad una persona.

La firma è personalizzata dal singolo individuo.

sommaa@stcom.com

Che cos'è la firma digitale ?

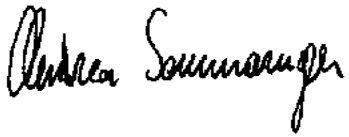
E' un numero !

La firma digitale è inserita da un programma

sommaa@stcom.com

Un esempio ?

La mia firma



La firma digitale di un mio documento

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
Esempio di testo firmato

Con i migliori saluti
andrea sommaruga

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>
iQA/AwUBNo/X8j8XHmMEbbChEQLNHgCfXuXSE/+r8QE5Lbj5qQxK4NcAKkEAoIsFKx
QR/jVDfqNR6sGerHOYP2Ce=t0Hn
-----END PGP SIGNATURE-----
```

sommaa@stcom.com

Che cosa succederà negli anni ?

La mia firma autografa sarà sempre riconoscibile

La mia firma digitale sarà verificata solo se i server delle firme avranno ancora memorizzato i miei dati !

Tra 200 anni ?

sommaa@stcom.com

Segni caratteristici della Firma Digitale

- Valida a tutti gli effetti di Legge
- Molto sicura
- Difficilmente falsificabile
- Non ripudiabile
- Garantisce paternità e contenuto
- Un documento può essere firmato da più persone

- Valida SOLO su documenti elettronici

sommaa@stcom.com

Segni caratteristici della Firma Digitale

Un documento firmato digitalmente nasce in digitale e muore in digitale.

Non è possibile stampare un documento firmato in digitale.
In una copia stampata non è più possibile verificare la firma digitale.

sommaa@stcom.com

Firma Digitale: come si usa

Si deve avere un dispositivo di firma (PC), la firma digitale (Smart Card), un software di firma ed una connessione ad internet.

La firma digitale richiede la connessione internet perché il software di firma appone oltre alla firma una marca temporale.

sommaa@stcom.com

Firma Digitale: come si ottiene

Ci sono degli enti chiamati "certificatori" che rilasciano su richiesta, ed a pagamento, (un tanto all'anno) la firma digitale in genere su "Smart Card".

Dove si ottiene ?

Poste Italiane, Camera Commercio ecc.

sommaa@stcom.com

MD5

E' un algoritmo matematico che consente di determinare il chksum di un file.

Il chksum è un numero univocamente determinato in base al contenuto del file ed è impossibile da falsificare. Una qualsiasi modifica al file altera il chksum.

sommaa@stcom.com

MD5: utilizzo

E' un ottimo sistema per verificare l'integrità dei files archiviati su supporti magnetici.

```
fe8fe79a5f8e66af2ba8516b71a0bab0 *Immagini/arwdown.gif
28f0598db3f482b93a8242d796296bd8 *Immagini/arwleft.gif
29f3f38e683839d90ddf6375de8245eb *Immagini/arwright.gif
7c8150cf1c568166007e745a33e378c6 *Immagini/arwup.gif
7b4700fc1d20fa8816075485c86067ed *Immagini/atwork.gif
33930a3c45b3f364a45e55b6ab2dcd71 *Immagini/BRICKS.JPG
51c27fe4161bbbd9c5bc9d50e7fb4a51 *Immagini/euro.ico
```

sommaa@stcom.com

MD5: come si calcola ?

Su internet ci sono tanti programmi per calcolarlo disponibili per i vari sistemi operativi.

Un semplice programma, rilasciato con licenza GPL, da utilizzarsi con windows, è reperibile al sito

http://www.md5summer.org

sommaa@stcom.com

Archivi in Digitale: La Licenza

Come tutte le cose anche questa presentazione è coperta da licenza d'uso:

Copyright (c) 2005 – Ing. Sommaruga Andrea Guido

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 Copyright (c)

la versione originale in inglese della licenza è disponibile su www.gnu.org/copyleft/fdl.html

sommaa@stcom.com