

E Privacy 2003

Firenze, Palazzo Vecchio 14 giugno 2003

firma digitale

“ tra sicurezza per l'utente ed esigenza della Rete”

Presidente Centro Studi di Informatica Giuridica
www.csig.it presidente@csig.it

Cos'è un documento informatico?

- D.P.R. 28 dicembre 2000, n. 445

TESTO UNICO DELLE DISPOSIZIONI
LEGISLATIVE E REGOLAMENTARI IN
MATERIA DI DOCUMENTAZIONE
AMMINISTRATIVA

- Art. 1, lett. b)

Ai fini del presente testo unico si intende per:
DOCUMENTO INFORMATICO

la rappresentazione informatica di atti, fatti o dati
giuridicamente rilevanti

Il documento informatico

- In sé considerato, il documento informatico come sopra definito prescinde dal requisito di una firma digitale o elettronica.

Infatti:

art. 23, comma 1, T.U.

A ciascun documento informatico, o a un gruppo di documenti informatici, nonchè al duplicato o copia di essi, **può** essere apposta, o associata con separata evidenza informatica, una firma digitale.

firma elettronica o firma digitale

E' una informazione formata da un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, il fine è di ottenere un metodo di autenticazione informatica che viene aggiunta ad un documento informatico al fine di garantirne integrità (messaggio non manipolato) e provenienza (che il mittente sia effettivamente quello dichiarato).

E' il risultato di una operazione matematica applicata al documento informatico

Il documento informatico con firma digitale

Art. 23, comma 2, T.U.

L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo

Art. 10, comma 3, T.U.

Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del Codice civile

Efficacia della scrittura privata

- Art. 2702 c.c.

La scrittura privata fa piena prova, fino a querela di falso, della provenienza della dichiarazione da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

Equivalenza con la forma scritta

- Art. 10, comma 1, T.U.

Il documento informatico sottoscritto con firma digitale (...) soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile.

Riproduzioni meccaniche

- Art. 2712 c.c.

Le riproduzioni fotografiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

FIRMA ELETTRONICA

- **Art. 10 DPR n. 445/2000**
- **DLgs. 23 febbraio 2002, n. 10**
- **DPR 31 gennaio 2003 (Reg.coordinamento firme elettroniche a norma dell'art.13 Dlgs. n. 10/2002).**

Documento Informatico art. 2712 c.c.

(= fotocopia)

Cass.1145/2001

Documento Informatico firma elettronica

(= forma scritta)

Documento Informatico firma elettronica qualificata

(= scrittura privata riconosciuta) piena prova

✓ Firma elettronica



L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica

✓ Firma elettronica qualificata



Firma digitale
Firma elettronica avanzata



basata su certificato qualificato & **generata** mediante dispositivo di creazione firma sicura

- riservatezza della transazioni
- integrità del contenuto delle transazioni
- autenticità della provenienza dei messaggi
- non ripudiabilità del documento

firma elettronica e firma digitale

- La firma *elettronica* ha valore di autenticazione
- La firma *digitale* o avanzata soddisfa particolari requisiti di sicurezza (integrità, autenticità e non ripudio) ed ha valore legale come la firma autografa

FIRMA ELETTRONICA AVANZATA

la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

FIRMA ELETTRONICA QUALIFICATA

la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma

FIRMA DIGITALE

particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

- ***Riservatezza***: certezza che la comunicazione inviata non sia intercettabile e violabile da alcuno
- ***Integrità dei dati***: la certezza che in nessun punto la comunicazione sia stata modificata
- ***Autenticazione***: certezza del mittente
- ***Non ripudio***: impossibilità del mittente di negare di aver trasmesso e del ricevente di avere ricevuto

L'Ente Certificatore: definizione

- identifica la persona che richiede il certificato
- rende certa l'identità del soggetto fisico che ha generato una firma
- rilascia, pubblica, revoca e sospende i certificati di sottoscrizione
- assicura la corrispondenza tra il titolare e la sua chiave pubblica
- impedisce di fatto il disconoscimento della firma

Requisiti e controllo

Certezza di chi e con quali procedure (*policy*) provvede alla generazione e gestione delle chiavi e abilita all'uso della firma (*Certification Authority, CA*)

Gerarchia di certificazione, cioè come usare la firma data dalla CA verso il mondo (problema di interoperabilità delle CA)

Confronto tra le firme

FIRMA AUTOGRAFA

Riconducibile al soggetto direttamente

Legata al documento attraverso il supporto fisico

Verifica diretta e soggettiva (attraverso il campione)

Facilmente falsificabile, ma il falso è riconoscibile

Deve essere autenticata per impedire il ripudio

FIRMA DIGITALE

Riconducibile al soggetto solo attraverso una procedura informatica

Legata indissolubilmente al contenuto del documento

Verifica indiretta e oggettiva (tramite una terza parte fidata)

Non falsificabile senza conoscere la chiave privata, ma falso irriconoscibile

Ripudio solo tramite querela di falso

La firma: possibili applicazioni

- protocollo informatico nella P.A.
- E-government
- processo telematico
- rilancio dell'e-commerce
- E-democracy
- digitalizzazione delle informazioni
- E-procurement
- trasmissione dei bilanci presso le CCIAA

C:\>

“ In the Beginning Was the Command Line”