Firma digitale
Profili normativi

Prof. ing. Pierluigi Ridolfi

- **Concetti geneali**
- **Norme italiane**
- **Documento informatico e firma digitale**
- **I Certificatori**
- **Regole tecniche**
- **Ruolo dell'AIPA**
- **Problemi aperti**
- **La Direttiva europea e il suo recepimento**

Referenze bibliografiche

- Per gli aspetti legali:
  - P.Ridolfi "Certificazione e interoperabilità", Alta Frequenza, n.5/2001
  - G.Finocchiaro "Profili giuridici della firma digitale", idem.
- Una raccolta di materiale sulla firma digitale in www.erresoft.it

Concetti generali

- Firma e sottoscrizione
- Documento e documento informatico
- Tipi di documento
- Alcune norme del Codice civile

Firma e sottoscrizione

- **Firma**: impronta di segni alfabetici formanti il nome e il cognome resi mediante autografia.
- **Sottoscrizione**: firma apposta nella fase finale di un documento scritto e manifestazione di volontà di aderire al testo precedente.

  Essa assolve alle seguenti funzioni:
  - identifica l'autore del documento (funzione *indicativa*);
  - consente l'assunzione della paternità del contenuto del documento (funzione *dichiarativa*);
  - fornisce il mezzo per costituire la prova del contenuto del documento (funzione *probatoria*).

Documento

- Un’entità materiale idonea a rappresentare in maniera permanente un fatto, attraverso la percezione di segni incorporati in essa, impressi direttamente dall’uomo o con apparati predisposti dall’uomo.
- Vari tipi di documenti in base all’argomento trattato: privato, storico, giuridico, economico, ecc.
- Documento informatico: naturale estensione del concetto di documento, in cui i bit costituiscono i “segni” e il supporto informatico il mezzo sul quale i segni vengono registrati.

Scrittura privata

- Un documento provvisto di sottoscrizione.
- Una scrittura privata fa piena prova soltanto contro colui che l’ha sottoscritta e non in suo favore ed è subordinata al riconoscimento della sottoscrizione da parte di colui che l’ha apposta.
- Disciplinata dal C.C. art. 2702.

Atto pubblico

- Un documento sottoscritto da un notaio o da altro pubblico ufficiale.
- Un atto pubblico fa piena prova che le dichiarazioni contenute nel documento sono state effettuate in presenza del pubblico ufficiale.
- Per contrastare tale forza probatoria è necessaria la querela di falso.

Scrittura privata autenticata

- Una scrittura privata sottoscritta in presenza di un notaio o altro pubblico ufficiale.
- L'autenticazione attribuisce alla scrittura privata piena priva fino a querela di falso della sola provenienza delle dichiarazioni di chi ha sottoscritto l'atto.
- L'autenticazione non garantisce il contenuto dell'atto.
- Disciplinata dal C.C. art. 2703.

Richiami dal C.C. (1)

- **2702: Efficacia della scrittura privata**

  “La scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni 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”.

Richiami dal C.C. (2)

- **2703: Sottoscrizione autenticata**

  “Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
  L’autenticazione consiste nell’attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve preventivamente accertare la identità della persona che sottoscrive”.

Richiami dal C.C. (3)

- **2712: Riproduzioni meccaniche**

  “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 e alle cose medesime”.

Richiami dal C.C. (4)

- **2214: Libri obbligatori e altre scritture contabili**

  “L’imprenditore che esercita un’attività commerciale deve tenere il libro giornale e il libro degli inventari.
  Deve altresì tenere le altre scritture che siano richieste dalla natura e dalle dimensioni dell’impresa e conservare ordinatamente per ciascun affare gli originali delle lettere, dei telegrammi e delle fatture ricevute, nonché le copie delle lettere, dei telegrammi e delle fatture spedite”.

Norme nazionali sulla Firma digitale

- Legge 59/97, art. 15.
- DPR 513/97: Regolamento in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici.
- ⇒ DPR 445/00 Testo Unico sulla Documentazione Amministrativa.
- DPCM 8/2/99: Regole tecniche per l'attuazione del DPR.
- Circolare AIPA 22/7/99: norme per l'elenco dei Certificatori.
- D.Lgs. 10/02: Recepimento della D.E.

Legge n. 59, 15/3/1997

Art. 15, comma 2.

"Gli atti, dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge; i criteri di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare, entro centottanta giorni dalla data di entrata in vigore della presente legge..."

Definizioni (T.U.)

- Documento informatico.
- Firma digitale.
- Dispositivo di firma.
- Certificato.
- Certificatore.

Documento informatico

- Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- Il documento informatico è valido a tutti gli effetti di legge se conforme alle disposizioni del T.U.
- Le regole tecniche per la formazione, la trasmissione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono definite con un DPCM (T.U., art. 8, c. 2)

Firma digitale

Art. 1, comma 1, sub b)

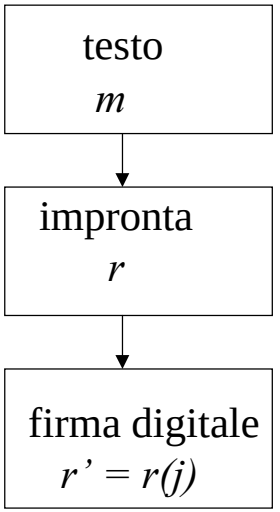
"Il risultato della procedura informatica basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la **provenienza e l'integrità** di un documento informatico …"

Realizzazione della firma digitale

firma digitale

⇓

impronta di
un testo
cifrata con la
chiave privata
del mittente



Forma ed efficacia del documento informatico

- art. 10 T.U.

  “1. Il documento informatico sottoscritto con firma digitale … soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell’art. 2712 C.C.

  3. Il documento informatico, sottoscritto con firma digitale ... ha efficacia di scrittura privata ai sensi dell'articolo 2702 C.C..

  4. Il documento informatico redatto in conformità alle regole tecniche … soddisfa l’obbligo previsto dagli articoli 2214 e seguenti C.C. ...”.

Valore legale della Firma digitale

- art. 23 T.U.

  “6. L’apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l’apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere”.

Firma digitale autenticata

- art. 24 T.U.

  “1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato”.

Contratti informatici

- art. 11 T.U.

  “1. I contratti stipulati con strumenti informatici o per via telematica mediante l’uso della firma digitale secondo le disposizioni del presente T.U. sono validi e rilevanti a tutti gli effetti di legge”.

Definizioni

- **Autenticazione** (CC 2703)

⇒ Attestazione da parte del pubblico ufficiale che la firma è stata apposta in sua presenza; *riguarda la singola firma.*

- **Validazione** (DPR 513/97, art 1, c. 1, sub b)

⇒ Attestazione della provenienza e dell'integrità del documento; *riguarda il singolo documento.*

- **Certificazione** (DPR 513/97, art 1, c. 1, sub h)

⇒ Attribuibilità della chiave pubblica al sottoscrittore e sua identificazione; *riguarda il singolo sottoscrittore.*

Regole tecniche (DPCM)

- Decreto previsto dall'art. 3 del DPR, e confermato dal T.U., relativo a:
  - formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione dei documenti informatici;
  - integrità e riservatezza delle informazioni.
- Pubblicato sulla G.U. del 15/4/99.
- Prossimo a essere rinnovato.

Alcuni punti delle regole tecniche

- Algoritmi per la generazione delle chiavi.
- Algoritmi per la generazione dell'impronta.
- Criteri di sicurezza.
- Requisiti dei Certificatori.

Requisiti dei Certificatori

- S.p.A. con capitale non inferiore a quello necessario all'esercizio dell'attività bancaria (6,3 M).
- Onorabilità dei rappresentanti legali (v. legge bancaria).
- Competenza ed esperienza del personale tecnico.
- Qualità dei processi informatici e dei relativi prodotti.
- Consigliata un'adeguata copertura assicurativa per eventuali danni a terzi.

Profili professionali del personale

a) responsabile della sicurezza;
b) responsabile della generazione e custodia delle chiavi;
c) responsabile della personalizzazione dei dispositivi di firma;
d) responsabile della generazione dei certificati;
e) responsabile della gestione del registro dei certificati;
f) responsabile della registrazione degli utenti;
g) responsabile della sicurezza dei dati;
h) responsabile della crittografia;
i) responsabile dei servizi tecnici;
j) responsabile dell'auditing.

Ruolo dell'AIPA

- Autorità per l'informatica nella pubblica amministrazione.
- Esamina, approva o respinge le domande per esercitare l'attività di Certificatore.
- Tiene l'elenco dei Certificatori.
- È, di fatto, responsabile delle regole tecniche.

Elenco Certificatori

- SIA
- SSB
- BNL Multiservizi
- Infocamere
- Finital
- Saritel
- Postecom
- Seceti
- Intesa
- C.T. (Rupa)
- Enel.it
- TrustItalia
- Cedacrinord

Assocertificatori

Problemi aperti

- Interoperabilità
- Certificazione degli attributi
- Validazione temporale
- Alternative al sistema della firma digitale previsto dal T.U.
- Carta d'identità elettronica

Il problema dell'interoperabilità

- **Giuridica**:
  - Valore dei certificati provenienti da altre comunità.
- **Tecnica**:
  - I programmi di gestione per i PC sono diversi per i vari Certificatori.
  - Possibilità per una comunità di "leggere" certificati provenienti da un'altra comunità.
  - Standard in fase di consolidamento.
- **Operativa**:
  - Possibilità per l'utente finale di leggere un certificato proveniente da qualunque altro utente.
  - Accesso alle liste di sospensione/revoca.

Certificazione degli attributi

- **Aspetti tecnici**:
  - attributo inserito nel certificato
  - oppure certificato separato
- **Aspetti normativi:**
  - chi certifica?
  - la certificazione degli attributi è un potere "riservato"
  - differenze sostanziali nelle legislazioni dei vari Paesi

Validazione temporale

T.U., art. 14: Trasmissione del documento

1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato.

2. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente regolamento e alle regole tecniche di cui all'articolo 3, sono opponibili ai terzi.

3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Marca temporale

DPCM, Regole tecniche: art. 1, 52 e segg.

"Marca temporale: un'evidenza informatica che consente la validazione temporale".

"Una evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale che le si applichi".

"La struttura dei dati relativi alla marca temporale è firmata in modo digitale".

"La data e l'ora contenute nella marca temporale sono specificate con riferimento al Tempo Universale Coordinato UTC".

"L'ora assegnata ad una marca temporale deve corrispondere, con una differenza non superiore ad un minuto secondo rispetto all'UTC, al momento della sua generazione".

"La generazione delle marche temporali deve garantire un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo".

Problemi legati alla validazione temporale

- Il sistema è molto complesso: la tecnologia non è consolidata.
- Viene certificato il momento in cui la marca viene apposta sul documento, non quello in cui il documento verrà spedito al mittente.
- Il certificatore di marca temporale potrà avere anche le funzioni di “corriere”? Per ora non è previsto.
- Il procedimento non è paragonabile a quello della raccomandata, tanto meno a quella con avviso di ritorno.

Altre soluzioni di validazione temporale

- Procedure di protocollo informatico.
- Registrazione dei “movimenti” nei file di log dei server $\Rightarrow$ procedure per “bloccare” i file di log.

La materia è in riesame.

Alternative al sistema previsto dal T.U.

- Si può utilizzare qualunque sistema di firma solo se:
  - si rinuncia al valore legale della firma digitale;
  - e/o se si opera su reti dedicate.

Un’alternativa diffusa: il sistema PGP

- Pretty Good Privacy (Philip Zimmerman)
- Tecnologia tipo RSA, molto utilizzata nella posta elettronica.
- Nata per polemica contro restrizioni USA.
- Non ci sono Certificatori.
- Chi attiva una comunicazione manda al destinatario anche la propria chiave pubblica.
- Ogni utente mantiene un “portachiavi” personale.

Carta di identità elettronica

- Prospettiva del massimo interesse.
- Ha la possibilità “teorica” di ospitare anche uno o più dispositivo di firma.
- Vi sono applicazioni sperimentali in corso.
- Problemi di standard e di competenze.

La Direttiva europea

- Pubblicata il 19 gennaio 2000.
- 28 “considerando” e 14 articoli.
- L’impostazione concettuale è diversa da quella italiana.
- L’enfasi non è sulla P.A. ma sul commercio elettronico.
- Criteri di liberalizzazione.

Nuovi concetti

- Firma *elettronica* anziché *digitale*.
- Due tipi di firma.
- Due tipi di certificati.
- Tre tipi di Certificatori.
- Comportamenti uniformi all'interno dell'U.E.

Classificazione

- Firma elettronica
- Firma elettronica avanzata

- Dispositivo per la creazione di una firma
- Dispositivo per la creazione di una firma sicura
- Dispositivo per la verifica di una firma

- Certificato
- Certificato qualificato

- Certificatore
- Certificatore che risponde a certi requisiti e pertanto può emettere certificati qualificati
- Certificatore accreditato

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”
- Nessun riferimento a specifiche tecnologie.
- Utilizzata come metodo di autenticazione (*recte*: provenienza).

Firma leggera

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”.
- Nessun riferimento a specifiche tecnologie.
- Garantisce provenienza e integrità.

Firma forte

Dispositivo per la creazione di una firma

- Sw o Hw usato per applicare [codici o] chiavi crittografiche private alla creazione di una firma elettronica.

Dispositivo per la creazione di una firma sicura

- Viene garantito, entro limiti ragionevoli di certezza, che:
  - le chiavi possano comparire una volta sola e non possano essere derivate;
  - la firma sia protetta da contraffazioni con l'impiego delle tecnologie attualmente disponibili;
  - i dati da firmare non siano alterati.

Dispositivo per la verifica di una firma

- Sw o Hw usato per applicare [codici o] chiavi crittografiche pubbliche alla verifica di una firma elettronica.

Certificato

- Un attestato elettronico che collega [codici o] chiavi crittografiche pubbliche, utilizzate per verificare una firma, a una persona e ne conferma l’identità.

Certificato qualificato

- Il certificato elettronico è detto “qualificato” se conforme a determinati requisiti fissati dalla Direttiva Europea .

Certificatore

- Una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche.

Certificatore “qualificato”

- Possiede un determinato elenco di requisiti (affidabilità, sicurezza, solidità economica, capacità di identificare le persone alle quali viene rilasciato un certificato qualificato, ecc.).
- Lo Stato esercita una supervisione (a posteriori).

Certificatore “accreditato”

- L’accreditamento è un’operazione facoltativa.
- Vengono stabiliti diritti e obblighi specifici per il Certificatore.
- L’accreditamento richiede un esame preventivo da parte di un organismo preposto alla sorveglianza.

Valore legale della firma

- D.E. art. 5, comma 1:

  "Gli stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura:

  a) posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e

  b) siano ammesse come prove in giudizio".

Confronti con l'attuale sistema italiano

Sostanziale identità tra

> "**firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo per la creazione di una firma sicura**"

e

> "**firma digitale**"

purché il certificatore sia accreditato.

E se è solo "qualificato" ?

La Direttiva europea e le norme italiane

- La Direttiva europea è stata recepita con il D.Lgsl. n.10, 23/01/02 *(G.U. n.39, 15/02/02).*
- L'Aipa viene "sostituita" dal Dipartimento per l'innovazione e le tecnologie.
- Previsto l'aggiornamento delle regole tecniche.
- Innovate le norme sulla modalità di esercizio dell'attività di certificazione e sulla firma.

Modalità per l'esercizio della certificazione

- Certificatori "semplici":
  - *nessuna formalità.*
- Certificatori che rilasciano certificati qualificati:
  - *semplice notifica di inizio attività e successiva azione di controllo*.
- Certificatori accreditati:
  - *preventiva domanda di riconoscimento del possesso di particolari livelli di qualità e sicurezza.*

Confronto versioni vecchia e nuova T.U.

Vecchia versione T.U.	Nuova versione T.U.
Il documento informatico sottoscritto con firma digitale … ha efficacia probatoria ai sensi dell'art. 2712 C.C.	Il documento informatico ha l'efficacia probatoria prevista dall'art. 2712 C.C., riguardo ai fatti ed alle cose rappresentate.
Il documento informatico sottoscritto con firma digitale ….. soddisfa il requisito legale della forma scritta.	Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta.
Il documento informatico, sottoscritto con firma digitale …. , ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.	Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

Inserimento nuova norma

Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto con firma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

Elenco certificatori

- Elenco pubblico solo per quelli accreditati.
- Assorbe quello attuale gestito dall'Aipa.

Problematiche

- Perplessità sulla estensione della "validità" della firma elettronica leggera e dei "poteri" dei Certificatori non accreditati.
- A quali applicazioni sarà riservata la firma forte?
- Quale sarà il campo d'azione degli attuali Certificatori?
- Ci sarà una "invasione" dei Certificatori stranieri?