Firme elettroniche e documento informatico

Corso "Nuove tecnologie e diritto"

Claudia Cevenini
26 maggio 2005

Il concetto di documento

L'ordinamento giuridico italiano non prevede una definizione di 'documento' in generale. Dottrina: "oggetto corporale che reca una serie di segni tracciati direttamente dall'uomo o da apparati predisposti dall'uomo, volti a conferirgli una portata rappresentativa" (Irti, *Sul concetto giuridico di documento*).

Elemento materiale (res signata), elemento immateriale (contenuto).

Documento più comune: documento cartaceo scritto.

Codice civile: atti pubblici (2699-2701), scritture private (2702-2708), riproduzioni meccaniche (2719).

2

Scrittura privata

Art. 2702 c.c. 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.*"

3

La sottoscrizione autografa

Scrittura di pugno del nome e cognome in calce a un documento.

Funzioni:

indicativa (identificazione della persona che sottoscrive),

dichiarativa (assunzione della paternità del documento),

probatoria (prova dell'autenticità del documento).

4

Atto pubblico

Art. 2699. Atto pubblico.

"*L'atto pubblico è il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato.*"

5

Riproduzioni meccaniche

Art. 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 o alle cose medesime.*"

6

Il documento elettronico o informatico

Un documento formato e memorizzato mediante computer, come i documenti cartacei, deve essere:

inalterabile,

conservabile,

accessibile a distanza di tempo,

imputabile a un soggetto determinato,

riconosciuto giuridicamente.

7

Una prima nozione di documento informatico

Legge 23 dicembre 1993, n. 547, art. 3 (criminalità informatica)

Inserimento nel codice penale dell'art. 491 bis (falsità in atti)

"*Se alcune delle falsità previste dal presente capo riguardano un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per* ***documento informatico*** *si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati a elaborarli*".

8

La "dematerializzazione" del supporto

Documento tradizionale: contenitore e contenuto sono inscindibili (es. carta/inchiostro).

Documento su supporto informatico: i *bit* possono essere trasferiti, riprodotti e memorizzati su infiniti supporti diversi.

Qualsiasi strumento informatico impiegato in luogo della sottoscrizione deve quindi essere apposto ai dati che devono essere sottoscritti e non al supporto.

9

Soluzioni

Strumento tecnico **firma elettronica** (se possiede determinate caratteristiche).

Strumento giuridico **riconoscimento della validità e rilevanza giuridica** di firme elettroniche e documenti informatici da parte del legislatore.

10

Crittografia

Dal greco *kryptos*, "nascosto".

Insieme di tecniche per **rendere illeggibili** informazioni a soggetti che non dispongano della 'chiave' di lettura.

Può garantire: riservatezza, origine e non ripudio dei messaggi inviati telematicamente.

E' inoltre la tecnica **alla base della firma digitale**.

Può essere **simmetrica** (a chiave singola) o **asimmetrica** (a doppia chiave).

11

Le chiavi

Stringhe di dati generate mediante elaboratore in base a complessi algoritmi.

Maggiore la lunghezza delle chiavi, più complessa la formula matematica, minore la probabilità di individuare la chiave privata in base alla conoscenza della chiave pubblica, quindi **più sicuro il sistema**.

Una coppia di chiavi = **un solo titolare**.

Tipi di chiavi:
- **di sottoscrizione**
- **di certificazione**
- **di marcatura temporale**

12

Crittografia simmetrica

La **stessa chiave** è utilizzata prima dal mittente per **cifrare** il documento poi dal destinatario per **decifrarlo**.

Occorre un **canale di comunicazione sicuro** per scambiare la chiave.

E' come se si impiegasse la stessa chiave per aprire e chiudere una valigetta.

Sistema non del tutto sicuro e complesso da gestire.

13

Crittografia asimmetrica

Detta anche crittografia 'a doppia chiave' o 'a chiave pubblica'.

Sono impiegate **due chiavi diverse** (una privata e una pubblica), in grado di **funzionare solo congiuntamente**.

Per rendere illeggibile il documento a terzi, il **mittente cifra** il documento con la **chiave pubblica del destinatario**.

Per leggerlo, **il destinatario** lo **decifra** mediante la **propria chiave privata**.

(Meccanismo semplificato: invio cifrato di una chiave simmetrica di sessione).

14

Il meccanismo di firma digitale 1/2

Si basa sulla tecnica di **crittografia a doppia chiave.**

L'impiego delle chiavi crittografiche per firmare è speculare rispetto a quello per rendere un documento illeggibile.

Il **mittente firma** il documento informatico con la **propria chiave privata** (nota solo a lui).

Il **destinatario legge** il documento con la **chiave pubblica del mittente**.

In questo modo è possibile essere certi della provenienza del documento.

15

Il meccanismo di firma digitale 2/2

Il meccanismo è applicato non all'intero documento ma a una sua "**impronta digitale**" (stringa di dati che ne sintetizza in modo univoco il contenuto).

L'impronta è generata mediante algoritmi, le c.d. "**funzioni di hash**" garantiscono che sia **impossibile** ottenere la **stessa impronta** partendo **da due file di dati diversi**.

Se il **documento** sottoscritto digitalmente è **modificato** anche di un solo *bit* l'algoritmo produrrà due **impronte diverse**.

16

La certificazione

La firma digitale di per sé non è in grado di garantire la reale identità del firmatario: questi potrebbe firmare a nome di un terzo o con un nome inventato.

È necessario l'intervento di soggetti terzi, i c.d. **certificatori,** che verificano e attestano l'**identità** di un soggetto e la sua corrispondenza con la **titolarità della chiave pubblica** di cifratura.

17

La conservazione delle chiavi

-le chiavi private sono conservate in un dispositivo di firma (es. ***smart card***)

-la **chiave privata** e il **dispositivo non** possono essere **duplicati**

-**chiave privata** e **dispositivo** devono essere **conservati con diligenza** per garantire integrità e riservatezza

-**informazioni** di **abilitazione** alla chiave privata vanno conservati in **luogo diverso** dal **dispositivo**

-necessario **richiedere immediatamente** la **revoca** se si è perso il possesso della chiave.

18

Norme essenziali

Legge 15 marzo 1997, n. 59

Direttiva 1999/93/CE del 13 dicembre 1999

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

D.P.C.M. 13 gennaio 2004

Deliberazione CNIPA n. 11/2004

D.Lgs. 7 marzo 2005, n. 82

19

Legge 15 marzo 1997, n. 59

"Gli atti, i dati e i documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici e telematici, sono validi e rilevanti ad ogni effetto di legge".

Validità e rilevanza giuridica degli strumenti informatici e telematici per:

- **formazione di atti, dati e documenti**
- **stipulazione di contratti**
- **archiviazione e trasmissione di documenti**

Stesso principio per la pubblica amministrazione e i privati.

Specifici regolamenti stabiliscono i criteri di applicazione.

20

La Direttiva Europea 1999/93/CE sulle firme elettroniche

Scopi della Direttiva:

Istituisce un **quadro giuridico uniforme per le firme elettroniche e i servizi di certificazione**.

Intende **agevolare l'uso** delle firme elettroniche e contribuire al loro **riconoscimento giuridico**.

Non disciplina la conclusione e la validità dei **contratti**.

Non pregiudica le **norme** nazionali o comunitarie sull'uso dei **documenti**.

21

Principi di base della direttiva

Neutralità nei confronti della **tecnologia** (= non è imposta una tecnologia particolare).

Nessuna autorizzazione preventiva per i servizi di **certificazione**.

Possono essere istituiti **sistemi di accreditamento facoltativo**.

Non può essere **limitata** la prestazione dei **servizi** di certificazione di **altri Stati membri**.

22

La direttiva: regole per il settore pubblico

Gli Stati membri possono stabilire **eventuali requisiti supplementari** per le firme elettroniche nel **settore pubblico**.

I requisiti:

devono essere **obiettivi**, **trasparenti**, **proporzionati** e **non discriminatori**,

non devono ostacolare i servizi transfrontalieri per i cittadini.

23

Firma elettronica e firma elettronica avanzata

Firma elettronica – dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzata come metodo di autenticazione.

Firma elettronica avanzata – firma elettronica connessa in maniera unica al firmatario, idonea ad identificarlo, creata con mezzi su cui questi ha controllo esclusivo; consente l'identificazione di ogni successiva modifica dei dati cui si riferisce.

24

Dispositivo per la creazione di una firma

Dispositivo per la creazione di una firma – software configurato o hardware usato per applicare i dati di verifica della firma.

Dispositivo per la creazione di una firma sicura – soddisfa ulteriori requisiti (allegato III).

25

Certificato

Certificato – attestato elettronico che collega i dati di verifica della firma ad una persona e ne conferma l'identità.

Certificato qualificato – soddisfa ulteriori requisiti (allegato I).

26

Firme elettroniche avanzate: effetti giuridici

Le **firme elettroniche avanzate** basate su un **certificato qualificato** e generate mediante un **dispositivo per la creazione di una firma sicura** sono:

equiparate alle firme autografe,

ammesse come **prova in giudizio**.

27

Firme elettroniche: effetti giuridici

Alle firme elettroniche **non può essere negata efficacia legale** solo a causa del fatto che sono:

in **forma elettronica**, o

non basate su un **certificato qualificato**, o

non create da un **dispositivo per** la creazione di una **firma sicura**.

28

Il Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82 (pubblicato nel Suppl. Ord. 93/L alla G.U. n. 112 del 16 maggio 2005).

Intende fornire un quadro normativo coerente per l'impiego delle nuove tecnologie nella pubblica amministrazione.

Entrerà in vigore dal 1° gennaio 2006.

Abroga e sostituisce alcune disposizioni del D.P.R. 445/2000 in materia di firme elettroniche e documento informatico.

29

Finalità e ambito di applicazione del Codice

Stato, regioni e autonomie locali devono assicurare la **disponibilità**, **gestione**, **accesso**, **trasmissione**, **conservazione** e **fruibilità** dell'**informazione digitale.**

Il Codice si applica alle **pubbliche amministrazioni**.

Le disposizioni relative a **documenti informatici**, **firme elettroniche**, **pagamenti informatici**, **libri e scritture** si applicano **anche ai privati**.

Disposizioni sull'**accesso** ai **documenti informatici** e **fruibilità** delle **informazioni digitali** si applicano anche ai **gestori di servizi pubblici** e **organismi di diritto pubblico.**

30

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**".

31

Firma elettronica qualificata

"La firma elettronica ottenuta attraverso una procedura informatica che garantisce la **connessione univoca al firmatario** e la sua **univoca autenticazione informatica**, **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**, che sia basata su un **certificato qualificato** e realizzata mediante un **dispositivo sicuro per la creazione della firma**, quale l'apparato strumentale usato per la creazione della firma elettronica".

32

Certificato qualificato 1/2

I certificati qualificati devono contenere almeno le seguenti informazioni:

a) indicazione che si tratta di un certificato qualificato;
b) numero di serie o altro codice identificativo;
c) nome, ragione o denominazione sociale del certificatore e Stato di stabilimento;
d) nome, cognome o pseudonimo e C.F. del titolare;
e) dati per la verifica della firma (chiave pubblica) corrispondenti ai dati per la creazione della firma in possesso del titolare;
f) termine iniziale e finale di validità;
g) firma elettronica qualificata del certificatore.

33

Certificato qualificato 2/2

Su richiesta del titolare il certificato qualificato può contenere ulteriori informazioni:

a) qualifiche specifiche del **titolare** (es. appartenenza ad ordini professionali, poteri di rappresentanza);
b) limiti d'uso del certificato;
c) limiti di valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

34

Firma digitale 1/2

"Un particolare tipo di **firma elettronica qualificata** basata su un sistema di **chiavi crittografiche**, una **pubblica** e una **privata**, correlate tra loro, 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".

35

Firma digitale 2/2

La FD deve riferirsi in modo univoco a **un solo soggetto** e al **documento** (o insieme di documenti) **cui è apposta o associata**.

Integra e sostituisce sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

Per generare la FD deve essere impiegato un **certificato qualificato non scaduto, non revocato o sospeso**.

Dal **certificato qualificato** devono risultare la validità, gli estremi del titolare e del certificatore ed **eventuali limiti d'uso.**

36

Firma digitale autenticata

FD può essere autenticata da un notaio o altro pubblico ufficiale autorizzato.

Il pubblico ufficiale **verifica l'identità** del firmatario e la **validità della chiave pubblica** e attesta che la **firma** è stata **apposta in sua presenza**.

Verifica inoltre che il **contenuto** del documento corrisponda alla **volontà della parte** e **non sia contrario all'ordinamento giuridico**.

La FD autenticata si considera giuridicamente riconosciuta ai sensi dell'art. 2703 c.c. (**non potrà essere disconosciuta dal suo autore**).

37

Documento informatico

"La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Soddisfa il requisito legale della **forma scritta** se sottoscritto con **firma elettronica qualificata** o con firma **digitale** nel rispetto delle **regole tecniche**, che garantiscano **identificabilità** dell'**autore** e **integrità** del **documento**.

38

Valore probatorio del D.I.

DI con firma elettronica: **liberamente valutabile** in giudizio, tenuto conto delle caratteristiche oggettive di qualità e sicurezza.

DI con firma digitale (o altra firma elettronica qualificata): efficacia dell'art. **2702 c.c.** (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."

Utilizzo del dispositivo di firma si presume riconducibile al titolare salvo prova contraria.

39

Libri e scritture

I **libri**, i **repertori** e le **scritture** (inclusi quelli previsti dalla legge sull'ordinamento del notariato e gli archivi notarili) di cui è **obbligatoria la tenuta** possono essere **formati** e **conservati** su **supporti informatici** in **conformità al Codice e** alle **regole tecniche**.

40

D.I. nel D.P.R. 445/00 (1/3)

[norma in vigore fino a dicembre 2005]

D.I. senza firma: efficacia probatoria dell'art. 2712 c.c. (**riproduzioni meccaniche**).

Fa **piena prova** dei fatti e delle cose in esso rappresentate, a condizione che **il soggetto contro il quale è prodotto non ne disconosca la conformità** alle cose e ai fatti stessi.

41

D.I. nel D.P.R. 445/00 (2/3)

D.I. con firma elettronica: soddisfa il requisito legale della **forma scritta**.

Dal punto di vista probatorio è **liberamente valutabile** dal giudice in base alle sue caratteristiche di qualità e sicurezza.

Soddisfa gli obblighi previsti in materia di **scritture contabili** (artt. 2214 ss. c.c.).

42

D.I. nel D.P.R. 445/00 (3/3)

D.I. con firma digitale (o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata con un dispositivo per la creazione di firma sicura):

fa **piena prova fino a querela di falso** della provenienza da parte del firmatario.

43

Copie di atti e documenti informatici 1/2

Il Codice modifica l'art. **2712** del **codice civile**, aggiungendo il concetto di riproduzioni '**informatiche**'.

"Le riproduzioni fotografiche, **informatiche** 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."

44

Copie di atti e documenti informatici 2/2

Copie informatiche di originali cartacei non unici sostituiscono a ogni effetto di legge gli originali se la loro conformità è attestata dal responsabile della conservazione con propria firma digitale.

Copie informatiche di originali cartacei unici sostituiscono a ogni effetto di legge gli originali se la conformità è autenticata da notaio o altro pubblico ufficiale autorizzato con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche.

45

La validità nel tempo del documento informatico

Il documento cartaceo, una volta formato, non richiede ulteriori interventi per mantenere la sua validità e rilevanza giuridica.

La **conservazione** del documento informatico sottoscritto necessita della **marcatura temporale**.

Ciò permette la **continuità nel tempo degli effetti giuridici** del documento informatico, anche oltre il limite della validità della chiave di sottoscrizione.

46

Rilevanza della marcatura temporale

Attribuisce **data ed ora certa** al documento informatico.

Prova **l'anteriorità della sottoscrizione** rispetto alla revoca o sospensione del certificato.

Permette di **estendere l'efficacia** del documento informatico.

47

Valore giuridico della trasmissione dei documenti informatici

I **documenti informatici trasmessi** a una **Pubblica Amministrazione** mediante **qualsiasi mezzo telematico o informatico** (incluso il fax, idoneo ad accertarne la fonte di provenienza) soddisfano il requisito della **forma scritta** e **non è necessario** far seguire alla trasmissione telematica l'**invio** del **documento originale**.

48

Trasmissione del documento informatico

Il documento informatico inviato telematicamente si intende:

- **spedito dal mittente** se **inviato al proprio gestore**;
- **consegnato al destinatario** se **reso disponibile all'indirizzo elettronico** da questi **dichiarato**, nella **casella di posta elettronica** del destinatario messa a disposizione dal gestore.

49

Trasmissione del documento informatico nel D.P.R. 445/00 (1/2)

[norma in vigore fino a dicembre 2005]

Il D.I. inviato telematicamente si considera "**inviato e pervenuto**" al destinatario quando è stato **trasmesso** al suo indirizzo elettronico.

50

Trasmissione del documento informatico nel D.P.R. 445/00 (2/2)

Data e ora di formazione, trasmissione o ricezione di un D.I. conforme al Testo Unico e alle regole tecniche sono **opponibili ai terzi**.

Se sono impiegate **modalità** che **assicurino l'avvenuta consegna** del D.I. la trasmissione equivale alla **notificazione a mezzo posta**.

51

Tutela della segretezza

Per i D.I. inviati telematicamente è prevista una **tutela di segretezza** analoga a quella della corrispondenza cartacea.

Gli **addetti alla trasmissione** non hanno il diritto di prendere cognizione del contenuto dei D.I., di effettuare copie o cedere informazioni a terzi.

I **dati** sono di **proprietà del mittente finché** non pervengono al **destinatario**.

52

Codice: trasmissione mediante posta elettronica certificata

L'invio telematico di **comunicazioni** che richiedono una **ricevuta di invio** e **di consegna** avviene mediante **pec**.

La **trasmissione** del **documento informatico** per via telematica mediante **pec** equivale, nei casi consentiti dalla legge, alla **notificazione a mezzo posta**.

Data e ora di **trasmissione** e **ricezione** di un **documento informatico** mediante **pec** sono **opponibili ai terzi** se conformi alla normativa vigente, incluse le regole tecniche.

53

Accesso al mercato dei certificatori

Attività dei certificatori:

è libera,

***non** richiede **autorizzazione preventiva**.*

Dipartimento per l'innovazione e le tecnologie:

ha funzioni di vigilanza e controllo,

può avvalersi dell'AIPA e di altre strutture pubbliche.

54

Accreditamento dei certificatori

Riconoscimento di requisiti di **livello più elevato.**

Funziona su base **volontaria.**

Richiesta al Dipartimento per l'Innovazione e le Tecnologie.

Necessari **requisiti tecnici, di solidità finanziaria e di onorabilità.**

Iscrizione in **elenco pubblico.**

55

Compiti dei certificatori 1/2

1) identificare con certezza il richiedente
2) rilasciare e rendere pubblico il certificato
3) indicare ulteriori requisiti nel certificato qualificato
4) rispettare le regole tecniche
5) fornire informazioni sulla procedura
6) rispettare misure minime sicurezza per il trattamento dei dati personali
7) non accettare in deposito dal titolare i dati per generare firme

56

Compiti dei certificatori 2/2

8) pubblicare tempestivamente revoca e sospensione del certificato
9) gestire in modo ottimale i servizi di elencazione, revoca e sospensione
10) determinare con certezza data e ora di rilascio, revoca e sospensione dei certificati
11) conservare per 10 anni tutte le informazioni sui certificati qualificati emessi
12) non copiare o conservare le chiavi private di firma degli utenti
13) fornire informazioni su supporto durevole
14) gestire il registro dei certificati.

57

Responsabilità dei certificatori 1/2

I certificatori che rilasciano un certificato qualificato o che garantiscono al pubblico l'affidabilità del certificato, **se non provano** di avere agito **senza colpa o dolo,** sono **responsabili** dei danni arrecati a chi ha fatto ragionevole affidamento su:

a) esattezza e completezza delle informazioni necessarie per verificare la firma;

b) garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica;

c) garanzia che i dati per la creazione e per la verifica della firma funzionino in modo complementare (se entrambi generati dal certificatore);

d) adempimento degli obblighi di legge (art. 32 Codice).

58

Responsabilità dei certificatori 2/2

I certificatori che rilasciano un certificato qualificato o che garantiscono al pubblico l'affidabilità del certificato sono **responsabili** dei **danni** derivanti da **mancata o non tempestiva registrazione** della **revoca** o della **sospensione** del **certificato**, **a meno che** non provino di avere agito **senza colpa**.

I certificatori non sono responsabili dell'uso di un certificato che ecceda eventuali limiti d'uso o di valore, **se riconoscibili** da parte dei terzi e **chiaramente evidenziati** nel processo di **verifica.**

59

Cessazione dell'attività

Il certificatore qualificato o accreditato per cessare l'attività deve **avvisare il Dipartimento** per l'Innovazione e le Tecnologie con almeno **60 giorni di anticipo** e informare tempestivamente i **titolari** dei certificati.

I **certificati non scaduti** al momento della cessazione saranno **revocati**.

Il certificatore potrà **indicare** un **certificatore sostitutivo**.

60

Obblighi del titolare e del certificatore

Il titolare deve adottare **tutte** le **misure organizzative** e **tecniche idonee** ad **evitare danno ad altri** e **custodire** e **utilizzare** il **dispositivo di firma** con la diligenza del **buon padre di famiglia.**

Il certificatore deve adottare **tutte** le **misure organizzative** e **tecniche idonee** ad **evitare danno ad altri, compreso** il **titolare** del **certificato.**

Il certificatore è **responsabile** dell'**identificazione** del **soggetto** che richiede il **certificato qualificato** di firma, **anche se l'attività** è **delegata** a soggetti **terzi**.

61

Atti amministrativi 1/2

D.Lgs. 12 febbraio 1993, n. 39. "**Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche**".

Art. 3, c. 1: "gli **atti amministrativi** adottati da tutte le pubbliche amministrazioni sono di norma predisposti **mediante sistemi informativi automatizzati**".

62

Atti amministrativi 2/2

Art. 3, c. 2: "nell'ambito delle pubbliche amministrazioni l'immissione, la riproduzione su qualunque supporto e la trasmissione di dati, informazioni e documenti mediante **sistemi informatici o telematici**, nonché l'emanazione di atti amministrativi attraverso i medesimi sistemi, devono essere accompagnate dall'**indicazione della fonte e del responsabile** dell'immissione, riproduzione o emanazione. Se per la validità di tali operazioni e degli atti emessi sia prevista l'emanazione di **firma autografa**, la stessa è sostituita dall'**indicazione a stampa**, sul documento prodotto dal sistema automatizzato, **del nominativo** del soggetto responsabile".

63

Le regole tecniche

D.P.C.M. 13 gennaio 2004.

"Regole tecniche per la **formazione**, la **trasmissione**, la **conservazione**, la **duplicazione**, la **riproduzione** e la **validazione**, anche temporale, dei **documenti informatici**".

(Gazz. Uff. 27 aprile 2004, n. 98).

64

Macroistruzioni e codice eseguibile

Il documento informatico sottoscritto con firma digitale **NON** produce gli **effetti giuridici** previsti dal Testo Unico se contiene **macroistruzioni** o **codici eseguibili** in grado di **modificare** gli atti, i fatti o i dati rappresentati nel documento stesso.

(art. 3, c. 3 reg. tecn.)

65

Tipi di chiavi

Chiavi di sottoscrizione (per la generazione e verifica delle firme apposte o associate ai documenti informatici).

Chiavi di certificazione (per la generazione e verifica delle firme apposte o associate ai certificati qualificati, alle liste di revoca e sospensione, o per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale).

Chiavi di marcatura temporale (per la generazione e verifica delle marche temporali).

(art. 4, c. 4 reg. tecn.)

66

Conservazione delle chiavi

E' **vietato duplicare** la **chiave privata** e i **dispositivi** che la contengono.

Il **titolare** di una coppia di chiavi deve:

conservare la **chiave privata** e il **dispositivo** che la contiene con la **massima diligenza**, per garantirne **integrità** e **riservatezza**;

conservare le **informazioni di abilitazione** all'uso della chiave privata **separatamente** dal **dispositivo** che contiene la chiave;

richiedere immediatamente la **revoca** dei **certificati qualificati** se il dispositivo risulta difettoso o se ne ha perduto il possesso.

(art. 7 reg. tecn.)

67

Periodo di validità dei certificati

Il **certificatore** determina il **periodo** di **validità dei certificati qualificati**.

Il certificatore custodisce le **informazioni** relative ai **certificati qualificati** per un periodo di almeno **10 anni dalla** data di **scadenza o revoca** del **certificato**.

(art. 15 reg. tecn.)

68

Revoca e sospensione del certificato qualificato

Se la **chiave privata** o il **dispositivo** sono **compromessi**, il certificatore è tenuto a **revocare** o **sospendere** il certificato.

E' necessario specificare **data e ora di pubblicazione** nella **lista di revoca/sospensione**.

Revoca può avvenire:

su iniziativa del **certificatore**,

su richiesta del **titolare**,

su richiesta del **terzo interessato** da cui derivano i poteri di rappresentanza del titolare.

(artt. 16-24 reg. tecn.)

69

Accesso ai certificati

Le **liste dei certificati revocati e sospesi** devono essere rese **pubbliche.**

I **certificati qualificati** possono essere resi **accessibili al pubblico su richiesta del titolare**, o **comunicati a terzi** nei **casi consentiti dal titolare** (**sempre** nel **rispetto** del **D.Lgs. 30 giugno 2003, n. 196**).

Le **liste** possono essere **utilizzate solo** per le finalità di **applicazione** delle **norme** sulla verifica e validità della **firma digitale**.

(art. 29 reg. tecn.)

70

Riferimenti temporali opponibili a terzi

I **riferimenti temporali** realizzati in conformità alle **regole tecniche** sono **opponibili ai terzi**.

Le **pubbliche amministrazioni** possono usare come sistemi di validazione temporale:

il **riferimento temporale** contenuto nella segnatura di **protocollo**;

il riferimento temporale ottenuto attraverso la procedura di **conservazione dei documenti**;

il riferimento temporale ottenuto attraverso l'utilizzo di **posta certificata**.

(art. 39 reg. tecn.)

71

Regole per la validazione temporale

La validazione temporale di un documento informatico avviene mediante la **generazione e l'applicazione** di una **marca temporale.**

Le marche temporali sono **generate** da un **sistema elettronico sicuro**, che deve:

mantenere la data e l'ora secondo le regole tecniche;

generare la struttura di dati secondo le regole tecniche;

sottoscrivere digitalmente la struttura di dati.

(art. 44 reg. tecn.)

72

Informazioni nella marca temporale

Le **marche temporali** devono contenere **almeno** le seguenti **informazioni**:

identificativo dell'emittente;

numero di serie;

algoritmo di sottoscrizione della m.t.;

identificativo del certificato relativo alla chiave di verifica della m.t.;

data e ora di generazione della m.t.;

identificatore dell'algoritmo di *hash* utilizzato per generare l'impronta del documento informatico sottoposto a validazione temporale;

valore dell'impronta del documento informatico.

(art. 45 reg. tecn.)

73

Chiavi di marcatura temporale

Ogni **coppia di chiavi** di marcatura temporale deve essere univocamente **associata a un sistema di validazione temporale.**

Per motivi di sicurezza occorre **limitare** il **numero** di **marche temporali generate con la stessa coppia** di chiavi = le chiavi di m.t. devono essere **sostituite**, e deve essere emesso un **nuovo certificato**, dopo non più di un mese di utilizzazione, a prescindere dal loro periodo di validità.

(art. 46 reg. tecn.)

74

Registrazione delle marche

Tutte le marche temporali generate da un sistema di validazione devono essere conservate in un **apposito archivio digitale non modificabile** per un periodo **non inferiore a 5 anni** (o per un periodo più lungo su richiesta dell'interessato).

La marca temporale è valida per l'intero periodo di conservazione.

(art. 50 reg. tecn.)

75

Estensione della validità del documento informatico

Se gli **effetti** di un **documento informatico** si protraggono nel tempo **oltre** il limite di **validità** della chiave di **sottoscrizione**, tale **validità** può essere **estesa** mediante l'associazione di una **marca temporale**.

(art. 52 reg. tecn.)

76

Lunghezza delle chiavi

In attesa della pubblicazione degli algoritmi per la generazione e verifica della firma digitale previsti dalle regole tecniche, i **certificatori accreditati** devono utilizzare l'algoritmo RSA con **lunghezza delle chiavi non inferiore a 1024 bit**.

(art. 53 reg. tecn.)

77