

## Firme elettroniche e documento informatico

---

Corso "Nuove tecnologie e diritto"

Lezione 6 - 1° giugno 2004

Claudia Cevenini

## Problemi fondamentali

Quando si impiegano tecnologie informatiche per formare, trasmettere e memorizzare documenti su supporto non cartaceo è importante garantire:

- **integrità e non modificabilità,**
- certezza dell'**origine,**
- **riservatezza,**
- **validità giuridica.**

2

## Soluzioni

Strumento tecnico → **firma elettronica.**

Dal punto di vista giuridico → **riconoscimento della validità e rilevanza giuridica** di firme elettroniche e documenti informatici da parte del legislatore.

3

## Firma digitale e firme elettroniche

L'ordinamento giuridico italiano disciplina diversi tipi di firme apponibili mediante strumenti informatici.

Il legislatore europeo ha sancito il principio di **neutralità tecnologica** delle firme.

Attualmente il meccanismo maggiormente diffuso e utilizzato è quello della **firma digitale a doppia chiave**, basato sulla c.d. **crittografia a chiave pubblica.**

4

## Crittografia

Dal greco *kryptos*, "nascosto".

Insieme di tecniche per **rendere illeggibili** informazioni a soggetti che non siano il destinatario.

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

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

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

5

## Crittografia simmetrica

La **stessa chiave** è utilizzata prima dal mittente per **crittare** il documento poi dal destinatario per **decrittarlo.**

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.

6

## Crittografia asimmetrica

Sistema 'a doppia chiave' o 'a chiave pubblica'.

Sono impiegate due chiavi diverse: una **privata** (nota solo al titolare), una **pubblica** (nota ai potenziali destinatari).

Il **mittente critta** il documento con la **chiave pubblica del destinatario**;

il **destinatario lo decritta** mediante la **propria chiave privata**.

Meccanismo semplificato: invio crittato di una chiave simmetrica di sessione.

7

## 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**.

8

## La tecnologia di firma digitale 1/2

**Sistema di crittografia a doppia chiave (o a chiave pubblica o asimmetrica)**

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

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

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

9

## La tecnologia 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**.

10

## La certificazione

La firma digitale da sola non può garantire l'identità del firmatario: questi potrebbe firmare a nome di un terzo o con un nome inventato.

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

11

## La procedura di registrazione

- Identificazione certa del titolare (di persona mediante documento)
- Procedura automatica di generazione della coppia di chiavi
- Memorizzazione della chiave privata su *smart card*
- Scelta di una *password* di accesso al meccanismo di firma
- Sottoscrizione di un contratto

12

## La conservazione delle chiavi

- le chiavi private sono conservate in un dispositivo di firma (*smart card*)
- la **chiave privata** e il **dispositivo non** possono essere **duplicati**
- **chiave privata** e **dispositivo** devono essere **conservati con diligenza** (integrità e riservatezza)
- **informazioni** di **abilitazione** alla chiave privata vanno conservati in **luogo diverso dal dispositivo**
- **richiedere immediatamente** la **revoca** se si è perso il possesso della chiave

13

## Documento e sottoscrizione

Nozioni giuridiche di base

14

## Il concetto di documento

La normativa italiana non fornisce una definizione di 'documento' in generale.

Il documento può essere descritto come un **oggetto recante segni**, qualcosa che:

- **rappresenta** un fatto,
- **prova** un fatto.

Alcuni esempi di documenti nel codice civile:

- scrittura privata (art. 2702 c.c.)
- atto pubblico (art. 2699 c.c.)
- riproduzioni meccaniche (art. 2712 c.c.)

15

## 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”.

16

## 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.”

17

## 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.”

18

## La sottoscrizione autografa

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

Funzioni:

**indicativa** (identificare l'autore del documento),

**dichiarativa** (affermare che il documento è formato per conto di chi sottoscrive),

**probatoria** (provare l'identità del firmatario).

19

## Il documento formato mediante elaboratore

La scrittura mediante elaboratore può armonizzarsi con il concetto giuridico di documento se è:

- **inalterabile**,
- **conservabile**,
- **accessibile** a distanza di tempo,
- **imputabile** a un soggetto determinato.

20

## La "dematerializzazione" del supporto

**Documento tradizionale:** inscindibilità tra contenitore e contenuto (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 essere apposto direttamente ai dati e non al supporto.

21

## Il quadro normativo

Le regole che disciplinano la gestione informatizzata dei documenti

22

## 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. Lgs. 23 gennaio 2002, n. 10

D.P.R. 7 aprile 2003, n. 137

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

### Deliberazione CNIPA n. 11/2004

23

## 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.

24

## 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**.

25

## Principi di base della direttiva

**Neutralità** nei confronti della **tecnologia**.

**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**.

26

## 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.

27

## 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.

28

## 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).

29

## 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).

30

### **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.**

31

### **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.**

32

### **D.P.R. 445/2000**

Testo Unico sulla documentazione amministrativa: detta le disposizioni sulla **gestione dei documenti da parte delle Pubbliche Amministrazioni.**

Le norme sui documenti informatici e la firma digitale si applicano anche ai **rapporti tra privati.**

33

### **Firme elettroniche**

- Firma elettronica
- Firma elettronica avanzata
- Firma elettronica qualificata
- Firma digitale

34

### **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”.

35

### **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 sono stati successivamente modificati”.

36

## 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”.

37

## Firma digitale

“Un 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”.

38

## Disciplina della firma digitale

- ✓ FD deve essere riferita a **un solo soggetto** e al documento cui è apposta o associata.
- ✓ Deve essere generata con una chiave privata la cui corrispondente **chiave pubblica** sia **valida**.
- ✓ Può essere impiegata in luogo di **sigilli, punzoni, timbri, contrassegni e marchi**.
- ✓ Deve consentire di **verificare la validità del certificato** e gli **elementi identificativi del titolare e del certificatore**.

39

## 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**).

40

## Il documento informatico

Definizione: “la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”.

Forma ed efficacia. Si distingue tra:

- Documento non sottoscritto
- Documento sottoscritto con firma elettronica
- Documento sottoscritto con firma digitale

41

## D.I. senza firma

Ha l'**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.

42

## 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.).

43

## D.I. con firma digitale

D.I. sottoscritto 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.

**NON** ha questa **validità** se contiene **macroistruzioni** o **codice eseguibile** tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati rappresentati.

44

## Copie informatiche

**Duplicati, copie ed estratti di documenti informatici** su qualsiasi supporto sono validi se conformi al T.U. (art. 20 T.U.).

**Copie informatiche di originali cartacei** hanno la stessa validità degli originali se la loro conformità è attestata da un pubblico ufficiale.

**Copie informatiche di documenti rilasciati dai pubblici ufficiali** sono valide ex artt. 2714 e 2715 c.c. se firmate digitalmente da chi li spedisce o rilascia.

45

## Trasmissione del D.I. 1/2

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

Occorre dimostrare l'avvenuta trasmissione del documento per provare che questo sia giuridicamente pervenuto al destinatario.

46

## Trasmissione del D.I. 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**.

47

## 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**.

48

## La validità nel tempo del documento informatico

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

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

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

49

## Rilevanza della marcatura temporale

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

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

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

50

## La certificazione

Funzione basilare: garantire la **corrispondenza** tra gli **strumenti di firma** e la loro **titolarità**, garantendo l'**identificazione** del soggetto legittimato a firmare.

51

## Accesso al mercato

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.

52

## Accreditamento

- ✓ **Riconoscimento di requisiti di livello più elevato**
- ✓ Funziona su base **volontaria**
- ✓ Richiesta al Dipartimento
- ✓ Necessari **requisiti tecnici, di solidità finanziaria e di onorabilità**
- ✓ Iscrizione in **elenco pubblico**

53

## Obblighi del titolare e del certificatore

Il titolare e il certificatore devono adottare tutte le **misure organizzative e tecniche** idonee a **evitare danno ad altri**.

54

## Obblighi 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

55

## Obblighi 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.

56

## Responsabilità dei certificatori 1/2

I certificatori che rilasciano certificati qualificati o che garantiscono al pubblico l'affidabilità dei loro certificati sono **responsabili dei danni** causati a terzi per:

- **esattezza e completezza** delle **informazioni** contenute nel certificato;
- **garanzia che il firmatario detenesse i dati** per creare la firma corrispondenti ai dati per la verifica al **momento di emissione** del certificato;
- **garanzia che i dati di creazione e verifica** di firma siano **complementari** (se sono stati generati dal certificatore).

57

## Responsabilità dei certificatori 2/2

I certificatori sono responsabili per danni se non hanno regolarmente provveduto a **registrare la revoca** o la **sospensione** dei certificati.

Possono **liberarsi** da responsabilità dimostrando di avere **agito senza colpa**.

Non sono responsabili per danni derivanti dall'**impiego** di un certificato **oltre i limiti d'uso o di valore** eventualmente indicati.

58

## Cessazione dell'attività

Il certificatore qualificato o accreditato per cessare l'attività deve **avisare 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**.

59

## 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).

60

## Archiviazione e conservazione dei documenti

61

## Conservazione dei documenti

- I **documenti di cui è imposta la conservazione** possono essere sostituiti - sia dalla Pubblica Amministrazione, sia dai privati - con la loro **riproduzione su supporto fotografico, ottico o altro mezzo idoneo a garantire la conformità agli originali** (D.P.R. 445/2000, art. 6, c. 1).
- Gli **obblighi di conservazione** sono **soddisfatti** su supporto ottico se conformi alle **regole tecniche AIPA** (D.P.R. 445/2000, art. 6, c. 2).

62

## Deliberazione CNIPA n. 11/2004

“Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali”.

[Nota: La deliberazione CNIPA 11/2004 sostituisce integralmente e abroga la deliberazione AIPA n. 42/2001]

63

## Obblighi di conservazione sostitutiva

Gli obblighi di conservazione sostitutiva dei documenti previsti dalla legislazione vigente - sia per le P.A., sia per i privati - sono soddisfatti a tutti gli effetti di legge se conformi a quanto previsto dalla Deliberazione CNIPA n. 11/2004.

(art. 2 Del. CNIPA n. 11/2004)

64

## La conservazione dei documenti su supporto non cartaceo

Il documento cartaceo, una volta formato, non richiede ulteriori interventi per mantenere nel tempo la propria validità. La **conservazione dei documenti su supporto non cartaceo** deve rendere possibile la **continuità nel tempo** della loro **validità** e **rilevanza giuridica**.

65

## Concetti di base

La Del. CNIPA n. 11/2004 fornisce numerose **definizioni**, in particolare quelle di:

- documento,
- documento analogico,
- documento analogico originale,
- documento informatico,
- documento archiviato,
- documento conservato.

66

## Documento

"**Rappresentazione** informatica o in formato analogico di **atti, fatti e dati** intelligibili **direttamente o attraverso** un processo di **elaborazione elettronica**".

67

## Documento analogico

"Documento formato utilizzando una **grandezza fisica** che assume **valori continui**, come le tracce su carta (es.: documenti cartacei), come le immagini su film (es.: pellicole mediche, *microfiche*, *microfilm*), come le magnetizzazioni su nastro (es.: cassette e nastri magnetici audio e video). Si distingue in **documento originale** e  **copia**".

68

## Documento analogico originale

"**Documento analogico** che può essere **unico** oppure **non unico** se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi".

69

## Documento informatico

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

70

## Documento archiviato

"**Documento informatico**, anche sottoscritto, sottoposto al **processo di archiviazione elettronica**".

71

## Documento conservato

"**Documento** sottoposto al **processo di conservazione sostitutiva**".

72

## Conservazione e archiviazione

La **conservazione sostitutiva** rende un **documento** non deteriorabile e quindi **disponibile nel tempo**, garantendone l'**integrità** ed **autenticità**. Deve essere svolta con le modalità della **Del. CNIPA n. 11/2004**.

L'**archiviazione elettronica** è la **memorizzazione** su un supporto idoneo di **documenti digitali**, **identificati univocamente** con un codice di riferimento. E' propedeutica alla conservazione, **non è obbligatoria** e **non** sono stabilite **particolari modalità operative** per la sua effettuazione.

73

## Supporti di memorizzazione

Può essere utilizzato **qualsiasi supporto** di memorizzazione digitale che consenta la registrazione con **tecnologia laser** (es. cd rom e DVD).

E' consentito l'uso di **qualsiasi supporto di memorizzazione (anche non ottico)** se **non ostano altre motivazioni** e se ciò avviene in **conformità alle regole tecniche**.

(art. 8 Del. 11/2004)

74

## Conservazione sostitutiva (I)

### Documenti informatici:

- memorizzazione su supporto ottico,
- apposizione del riferimento temporale,
- apposizione della firma digitale del responsabile della conservazione.

(art. 3 Del. 11/2004)

75

## Conservazione sostitutiva (II)

### Documenti analogici:

- memorizzazione immagine direttamente su supporto ottico,
- apposizione del riferimento temporale,
- apposizione della firma digitale del responsabile della conservazione.

(art. 4 Del. 11/2004)

Per i documenti analogici originali unici occorre anche la firma digitale di un pubblico ufficiale.

76

## Riversamento diretto

Processo che **trasferisce** uno o più **documenti** conservati **da un supporto** ottico di memorizzazione **ad un altro**, **non alterando** la loro **rappresentazione informatica**. Per tale processo non sono previste particolari modalità.

77

## Riversamento sostitutivo

Processo che **trasferisce** uno o più **documenti conservati da un supporto** ottico di memorizzazione **ad un altro**, **modificando** la loro **rappresentazione informatica**.

78

## Procedura di riversamento sostitutivo

- **Memorizzazione** su supporto ottico
- Apposizione del **riferimento temporale**
- Apposizione della **firma digitale** del responsabile della conservazione

Per i **documenti informatici sottoscritti** e per i **documenti analogici originali unici** occorre anche l'apposizione del riferimento temporale e della firma digitale da parte di un **pubblico ufficiale**.

79

## Responsabile della conservazione

- Definisce caratteristiche e requisiti del sistema di conservazione
- Archivia e rende disponibile una serie di informazioni (es. descrizione del contenuto dei documenti, gli estremi identificativi propri e delle persone delegate, indicazione delle copie di sicurezza)
- Mantiene e rende accessibile un archivio del software dei programmi nelle diverse versioni
- Verifica la corretta funzionalità del sistema e dei programmi
- Adotta le misure necessarie di sicurezza fisica e logica del sistema e delle copie
- Richiede la presenza di un pubblico ufficiale se previsto
- Definisce e documenta le procedure di sicurezza per il riferimento temporale
- Verifica periodicamente (almeno ogni 5 anni) l'effettiva leggibilità dei documenti

80

## Distruzione del documento analogico

I **documenti analogici** di cui è **obbligatoria** la **conservazione** possono essere **distrutti** solo **dopo** il completamento della procedura di **conservazione sostitutiva**.

Sono fatti salvi i poteri di controllo del Ministero per i Beni culturali sugli archivi delle Pubbliche Amministrazioni.

81