Regole tecniche su firma, identità digitali e banche dati

Stefania Pallottini

Formez 17 maggio 2012

Il Codice dell'Amministrazione digitale: scopi

- Strumento normativo concepito per trasformare le potenzialità dell'innovazione tecnologica in maggiore efficienza, efficacia e soddisfazione dei cittadini e delle imprese.

- Rende possibile il processo di digitalizzazione delle attività amministrative che costituisce il presupposto per una reale modernizzazione degli Enti pubblici.

Il Codice dell'Amministrazione digitale: scopi

- I cittadini e le imprese hanno il diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi PA.

- Nei rapporti tra imprese ed amministrazioni il digitale diventa la regola e il cartaceo l'eccezione

- Deve essere sempre e dovunque disponibile un canale digitale sicuro, certificato e con piena validità giuridica per inoltrare istanze ed effettuare pagamenti per via telematica.
- Non sarà più possibile quindi, per un ente o per un gestore di pubblico servizio, obbligare i cittadini ad andare allo sportello per presentare documenti cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti

Il Codice dell'Amministrazione digitale: articolazione

- Principi generali
- Documento informatico e firme elettroniche pagamenti, libri e scritture
- Formazione, gestione e conservazione dei documenti informatici
- Trasmissione informatica dei documenti
- Dati delle pubbliche amministrazioni e servizi in rete
- Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni
- Sistema pubblico di connettività e rete internazionale della pubblica amministrazione
- Disposizioni transitorie finali e abrogazioni

Il Codice dell'Amministrazione digitale: coordinate

- Emanato con Decreto legislativo del 7 marzo 2005, n. 82, pubblicato sulla Gazzetta ufficiale n. 112 del 16 maggio 2005, a seguito della delega al Governo contenuta all'articolo 10 della legge 29 luglio 2003, n. 229 (Legge di semplificazione 2001).
- Nel 2006, pochi mesi dopo l'entrata in vigore, il Codice è stato oggetto di una serie di correttivi, disposti con il decreto legislativo 4 aprile 2006, n. 159.
- Il Decreto anti-crisi (Decreto legge n. 185/2008, convertito in Legge n. 2/2009) ha modificato i commi 4 e 5 dell'art. 23, prevedendo per la copia firmata digitalmente lo stesso valore dell'originale senza obbligo di autentica da parte di notaio o di altro pubblico ufficiale, salvo i documenti da indicare con decreto del Presidente del Consiglio dei ministri.
- Altre modifiche sono state introdotte dalla legge 18 giugno 2009, n. 69 e dalla legge 3 agosto 2009, n. 102
- Successivamente, importanti modificazioni e integrazioni sono state introdotte dal decreto legislativo 30 dicembre 2010, n. 235. Infatti, sono stati modificati 53 articoli su 92 originari e sono stati introdotti altri 9 articoli.

Il Codice dell'Amministrazione digitale: la riforma

Il Decreto legislativo 30 dicembre 2010, n. 235:

- pieno valore giuridico delle transazioni digitali (valore della stampa su carta di un documento originato in forma digitale e la semplificazione e il rafforzamento dei meccanismi di riconoscimento in linea del soggetto che attiva una transazione digitale);
- standard e regole tecniche per assicurare la sicurezza e l'interoperabilità delle transazioni (i vari strumenti diventano un sistema integrato che consente varietà dei punti di accesso, molteplicità di dispositivi e risposte coordinate);
- scadenze cogenti per la messa a disposizione dei servizi con meccanismi di incentivi e disincentivi per i responsabili dell'eventuale mancato rispetto delle scadenze;
- informazione agli utenti sui servizi disponibili (quale amministrazione presta quali servizi in linea e attraverso quali canali è contattabile, ma anche come l'utente può esprimere il proprio grado di soddisfazione per i servizi erogati);

Il Codice dell'Amministrazione digitale: la riforma

Nuovi scenari e nuove opportunità per i cittadini e le imprese:

- "esigibilità" : il rapporto digitale tra cittadini e Pubblica Amministrazione è un diritto concreto al quale va data attuazione: come tutti i diritti ne vanno precisati i termini le modalità di fruizione e va sanzionato chi non adempie al corrispondente obbligo di metterlo a disposizione
- Approfondimento attraverso i gruppi di lavoro di Digit PA di alcune tematiche fondanti

  Regole tecniche su formazione, tenuta e conservazione deldocumento informatico

  Regole tecniche identità digitali

  Regole tecniche banche dati

  Linee Guida per la continuità operativa e infrastrutture critiche

  Regole tecniche gestione documento informatico e gestione flussi

  Regole tecniche firma digitale

Elementi generali dell'innovazione digitale

- Documenti informatici e loro validità
- Conservazione digitale dei documenti
- Identità digitale e trasmissione digitale dei documenti

Documenti informatici e loro validità

Il Codice assegna al documento informatico **pieno valore probatorio,** riprendendo, non senza alcune ridondanze, i concetti stabiliti dal D.P.R.445/2000:

”*Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni del codice e le regole tecniche di cui all’art. 71”*

→ si elimina l’inciso dopo pubbliche amministrazioni *“che dispongono di idonee risorse tecnologiche”* divenendo obbligo per tutte le PPAA (art. 40 comma 1 d.lgs. 82/2005 modificato da d.lgs. 235/2010).

Documento archivistico

Un documento, cioè una informazione fissata su un supporto in forma stabile, prodotto da una persona fisica o giuridica nel corso di un'attività pratica come strumento per portare avanti tale attività (concetto archivistico)

Documento amministrativo

Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (D.PR. 445/2000 art. 1, lettera a)

Documento informatico

"*La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti* "
art. 1, comma 1, lett. p) d.lgs. 82/2005 (e art. 1, comma 1, lett. a) d.p.r. 445/2000) D.PR. 445/2000 art. 1, lettera b) → per rappresentazione informatica si può intendere una sequenza di bit

Il documento analogico viene definizione in negativo rispetto a documento informatico: questo aspetto letterale conferma che il documento "nativo" da cui si parte deve essere il documento informatico

Firma digitale

"In tutti i documenti informatici della pubblica amministrazione la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale" ...(DPR 445/2000 - Art. 25)

Il passaggio dal documento cartaceo a documento informatico cui corrisponde passaggio da firma autografa a firma elettronica

- firma autografa
  - segno apposto manualmente su documento cartaceo e direttamente riconducibile al soggetto,
  - legata al supporto fisico del documento,
  - valutabile in modo diretto,
  - validità temporale illimitata.
- firma elettronica
  - sequenza binaria riconducibile al soggetto solo attraverso procedura informatica,
  - legata in modo indissolubile al contenuto del documento,
  - valutabile solo con mezzi informatici

Firma digitale e autografa

AUTOGRAFA

- Riconducibile al soggetto direttamente
- Legata al documento attraverso il supporto
- Verificabile direttamente usando un campione
- Verifica soggettiva
- Facilmente contraffacibile
- Falso riconoscibile
- Validità illimitata nel tempo

FIRMA DIGITALE

- Riconducibile al soggetto solo attraverso un segreto
- Legata indissolubilmente al contenuto del documento
- Verificabile solo attraverso strumenti informatici
- Verifica oggettiva
- Non contraffacibile (…)
- Falso irriconoscibile
- Validità limitata nel tempo

La firma digitale: definizione

- E' una informazione che viene aggiunta ad una sequenza binaria per garantirne l'integrità e la provenienza certa
- Si può aggiungere a qualunque forma di comunicazione digitale a fini di sicurezza
- Nel caso dei documenti informatici è una sequenza di caratteri che consente di individuare in modo univoco e inequivocabile l'autore del documento. Ha la funzione di un sigillo, nella forma di una serie di informazioni non modificabili che si aggiungono al documento con la funzione di rafforzarne l'autenticità, garantendo integrità e provenienza del documento.
- **4 tipologie** di firme elettroniche → prima della riforma erano 3, si è introdotta un nuovo tipo di firma: la firma elettronica avanzata. La dottrina è critica su questo inserimento, perché seppur sia stato motivato con adeguamento a direttiva europea, non ne coglie pienamente la ratio e complica il sistema.

La firma digitale: tipologie del CAD

Firma elettronica (cosiddetta semplice): insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1 lett. q) CAD)

è quindi uno strumento che consente di associare un insieme di dati elettronici (quali quelli che formano un documento) ad un identificativo unico, costituito appunto dalla firma elettronica. Il suo valore probatorio è liberamente valutabile in giudizio.

Es. identificativo utente e password, PIN ecc.

La firma digitale: tipologie del CAD

Firma elettronica avanzata (c.d. FEA):"*insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati* "(art. 1 lett. q-bis introdotta da d.lgs. 235/2010):

Direttiva europea 93 del 1999; consente l'identificazione e la connessione univoca al firmatario del documento ed è creata con mezzi sui quali il firmatario può conservare un controllo esclusivo. Consente infine di garantire l'integrità del documento sottoscritto: qualunque modifica invalida la firma. Il disconoscimento richiede querela di falso.

FE + connessione univoca con il firmatario, mezzo a controllo esclusivo (non ha certificato qualificato che caratterizza la firma qualificata e la digitale, né dispositivo sicuro della qualificata) ad esempio firma bio metrica

La firma digitale: tipologie del CAD

Firma elettronica qualificata: *"un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 lett. r)"*

è garantita la connessione univoca al firmatario, che ne conserva un controllo esclusivo; la firma è legata al contenuto di un documento, in modo tale da rendere individuabile qualsiasi successiva modifica apportata allo stesso.

FEA + certificato qualificato + SSCD (dispositivo sicuro)

Il disconoscimento richiede querela di falso e soddisfa il requisito della forma scritta ex art.1350 punti da 1 a 12.

La firma digitale: tipologie del CAD

Firma digitale: *"un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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"* (art. 1 lett. s).

FEA + certificato qualificato + crittografia asimmetrica
La nuova firma digitale non richiede l'uso del mezzo sul quale il firmatario può conservare il controllo esclusivo, ad esempio in forma di SSCD.
Vi è una presunzione di titolarità del dispositivo di firma, salvo che il titolare ne dia prova contraria → presunzione legale relativa di utilizzo (si riferisce anche a firma avanzata e qualificata) (art. 21, comma 2)

La firma digitale: tipologie del CAD

In estrema sintesi:

- la firma elettronica avanzata consente di essere sicuri che il documento non è stato modificato ed è riconducibile ad un unico firmatario;

- la firma elettronica qualificata (digitale o meno) consente anche di essere sicuri che il dispositivo di firma è affidabile e che il firmatario è effettivamente colui che dichiara di essere.

- tra la firma qualificata e firma digitale ci sono differenza di carattere tecnico, più che giuridico. Le regole tecniche sulla firma qualificata devono essere ancora menate.

La firma digitale: praticamente

Per avere la firma digitale è necessario:

- recarsi personalmente dall'Autorità di registrazione, ossia il certificatore o *certification authority* (è necessaria la verifica fisica del soggetto), che fornisce al soggetto lo strumento per memorizzare il certificato e per generare le due chiavi
- Ritirare un dispositivo sicuro per la generazione delle firme (costituito da smart card o da token-chiavetta USB),
- Installare un lettore di smart card (nel caso in cui non si utilizzi USB)
- Installare un software in grado di interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso.

Al soggetto viene attribuito un PIN di protezione. I formati per produrre file firmati digitalmente sono: pkcs#7 (noto come p7m), PDF, XML

La firma digitale nel tempo

- D.p.c.m. 30 marzo 2009 “Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici: *“La firma digitale, ancorchè sia scaduto, revocato o sospeso il relativo certificato qualificato, è valida se alla stessa è associabile un riferimento temporale opponibile ai terzi che collochi la generazione della firma in un momento precedente alla sospensione, scadenza o revoca del certificato.”*
- Artt. 43 ss. validazione temporale con generazione e applicazione di marcatura temporale → rende valido nel tempo il documento. Risultato di una procedura informatica che consente di attribuire ad un documento informatico data e orario certi opponibile a terzi.
- Generalmente i riferimenti temporali usati sono segnatura di protocollo informatico e la PEC; raramente utilizzata marca temporale.

Valore del documento e firma

- **documento informatico semplice, non sottoscritto** (privo di firma elettronica):

  - idoneità a soddisfare il requisito di forma scritta → è liberamente valutabile ex post in giudizio dal giudice*, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità* (art. 20, comma 1 bis).
  - valore probatorio→ è liberamente valutabile ex post in giudizio dal giudice*, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.* D.lgs. 235/2010 ha chiarito esplicitamente il valore probatorio del documento informatico non sottoscritto (art. 20, comma 1 bis).

- **documento informatico cui è apposta una firma elettronica semplice** (non avanzata, qualificata o digitale):

  - non equiparato da codice di per sé a documento sottoscritto con firma autografa e pertanto non soddisfa comunque il requisito legale della forma scritta → quindi si applica art. 20 comma 1 bis.
  - sul piano probatorio ex art. 21, comma 1 documento cui è apposta firma elettronica è liberamente valutabile ex post dal giudice*, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità*.

Valore del documento e firma

Documento informatico sottoscritto con firma digitale ed elettronica qualificata (artt. 21 commi 2 e 2bis, rispettivamente mod. e aggiunto da d.lgs. 235/2010) formato nel rispetto delle regole tecniche ex art. 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento

- equivale a sottoscrizione autografa, soddisfa requisito della forma scritta anche a pena di nullità (ad substantiam) ex art. 1350 c.c..
- efficacia probatoria della scrittura privata ex art. 2702 c.c., fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni di 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.

  Presunzione di titolarità del dispositivo di firma, salvo che il titolare ne dia prova contraria (art. 21, comma 2)→ presunzione legale di utilizzo.

.

Il valore giuridico del documento informatico

Validità

Documenti informatici: validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni di legge.

Documenti informatici delle Pa: costituiscono informazione primaria e originale da cui è possibile estrarre copia.

Efficacia probatoria

Firma elettronica → Prova liberamente apprezzabile

Firma elettronica avanzata o digitale → Prova piena

Forma

La firma elettronica soddisfa il requisito legale della forma scritta

La Direttiva 1999/93/CE distingue diverse tipologie di firma elettronica, delle quali la firma digitale è la più evoluta

tipo di firma	descrizione	requisiti del Certificatore	funzione dei certificati	effetti
ELETTRONICA	Dati elettronici allegati o connessi a documenti informatici per fini di autenticazione	Requisiti di onorabilità degli amministratori ex T.U. sull'attività bancaria e creditizia. L'attività è libera e non necessita di autorizzazione preventiva.	Collegano la firma elettronica al titolare e ne confermano l'identità.	Sul piano probatorio, i documenti con tale firma sono liberamente valutabili in base alle caratteristiche di qualità e sicurezza del sistema di firma utilizzato.
ELETTRONICA AVANZATA	Firma elettronica che garantisce anche l'integrità del documento e creata con mezzi sui quali il firmatario ha un controllo esclusivo			
ELETTRONICA QUALIFICATA	Firma elettronica avanzata, creata con dispositivo "sicuro", con certificato rilasciato da *Certificatore qualificato*	Come sopra, più altri requisiti di affidabilità (organizzativa, tecnica, finanziaria, …). È richiesta una comunicazione di inizio attività al M.I.T.	Contengono i dati previsti dalla normativa, firmati digitalmente dal Certificatore che li ha rilasciati. L'emissione, revoca e sospensione sono oggetto di pubblicazione.	Sul piano probatorio, i documenti con tale firma fanno piena prova di autenticità fino a querela di falso.
DIGITALE	Firma elettronica qualificata con certificato rilasciato da *Certificatore accreditato*	Come sopra, più forma di società di capitali e capitale sociale non inferiore a quello per l'attività bancaria. È richiesto l'accreditamento presso il M.I.T.		

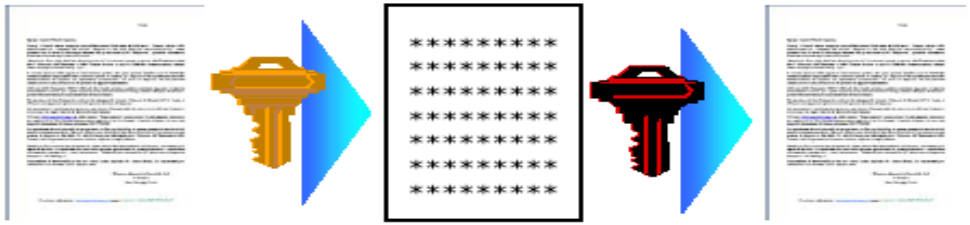
Come funziona la firma digitale

La firma digitale si basa su un sistema di crittografia "evoluto", che utilizza una coppia di chiavi asimmetriche attribuite univocamente a un titolare

La **chiave privata** è a disposizione esclusiva del titolare, custodita all'interno di una "**Smart Card**" (supporto informatico da collegare al PC) e protetta da un codice segreto conosciuto solo da lui

La **chiave pubblica**, anch'essa associata al titolare, è invece contenuta in un "**Certificato Digitale**" (documento informatico) reso accessibile a tutti su Internet da particolari soggetti: i Certificatori Accreditati

Un documento elettronico firmato (cifrato) con la chiave privata può essere verificato (de-cifrato) esclusivamente utilizzando la corrispondente chiave pubblica.

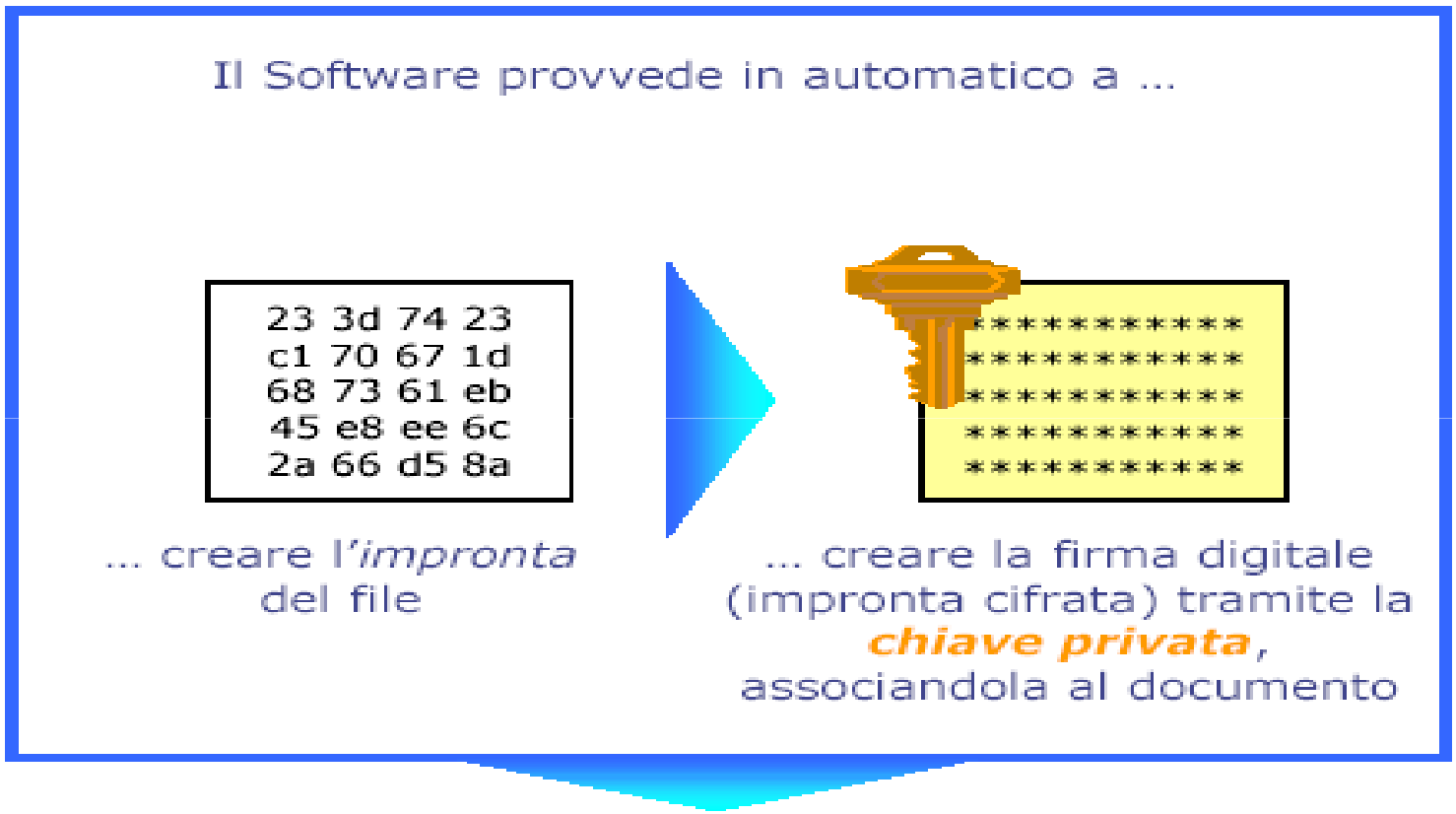


La funzione non è più quella di rendere il testo comprensibile solo al destinatario (la chiave pubblica è accessibile a tutti!) bensì di verificarne la provenienza dal titolare della chiave privata.

Cosa fa il software di firma

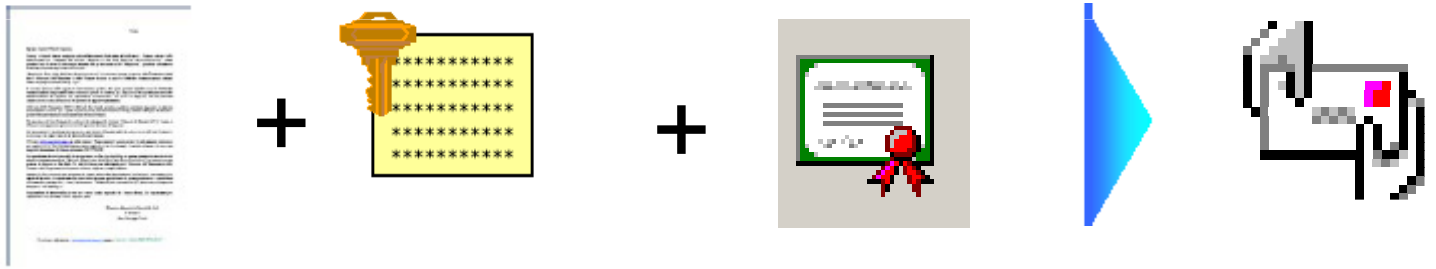
- Procedura di firma (totalmente automatizzabile):
  - calcola l'impronta del documento
  - esegue la cifratura dell'impronta del documento utilizzando la chiave privata
  - allega il certificato rilasciato dall'Autorità di certificazione
  - allega il documento in chiaro
  - spedisce il tutto in una busta (.P7m) al destinatario.

Cosa fa il software di firma



L'IMPRONTA è una sorta di "riassunto" del documento: più breve, ma costruita in modo da risultare diversa anche a seguito di variazioni in uno solo dei caratteri digitati.

Cosa fa il software di firma



Documento + Impronta cifrata + Certificato → Busta .P7m

Firma digitale

- **Verifica dell'autenticità e dell'integrità del messaggio arrivato:**
  - apre la busta
  - calcola l'impronta del documento in chiaro allegato
  - decifra, con la chiave pubblica, l'impronta del documento
  - confronta le due impronte. Se l'esito del risultato è positivo, il documento non è stato manomesso ed è perfettamente corrispondente a quello che il mittente ha firmato.
  - accede ai servizi dell'Autorità di certificazione che ha rilasciato il certificato per verificare che non ci siano atti di revoca o di sospensione nei confronti dello stesso e per verificarne l'identità.

Cosa fa il software in apertura di un file firmato

In automatico, il Software …

23 3d 74 23
c1 70 67 1d
68 73 61 eb
45 e8 ee 6c
2a 66 d5 8a

… crea l'*impronta del file ricevuto* …

****
****
****
****
****

23 3d 74 23
c1 70 67 1d
68 73 61 eb
45 e8 ee 6c
2a 66 d5 8a

… decifra la firma digitale tramite la ***chiave pubblica*** …

… e ottiene così l'*impronta del file originario* …

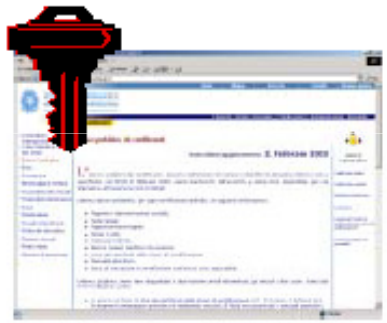
Il Software verifica *l'integrità* del documento…

23 3d 74 23
c1
68
4
2a

23 3d 74 23
c1 70 67 1d
68 73 61 eb
45 e8 ee 6c
2a 66 d5 8a

… confrontando le due impronte: se quella del *file ricevuto* è identica a quella del *file originario*, il documento è integro

Il Software verifica *l'autenticità* della firma e la *validità* del certificato:



attraverso gli elenchi messi on-line dai Certificatori accreditati, il Software risale all'**identità** del titolare della firma e verifica che il certificato sia **valido** (cioè non sia stato sospeso/revocato)

Identità digitale: in cosa consiste

- L'identità digitale, ovvero l'identificazione univoca di un soggetto per via telematica, è un prerequisito per dispiegare efficacemente il processo di erogazione on-line di molti servizi pubblici e per consentire una piena comunicazione in via telematica fra cittadino e amministrazioni.
- Per effettuare transazioni in rete (pagamenti, acquisti, richiesta di servizi, accesso a dati riservati) con è necessario avere la certezza, ottenibile attraverso particolari requisiti tecnologici di sicurezza, che ad un utenza digitale (cioè, ad esempio, ad un nomeutente e ad una password) sia associato univocamente un soggetto fisico o giuridico.

Identità digitali: quali servizi

- **servizio ad accesso libero**

  servizio diretto alla generalità degli utenti: dati e documenti possono essere resi disponibili a tutti gli utenti senza restrizioni particolari per mezzo ad esempio di sito web.

- **servizio ad accesso limitato**

  servizio con destinatari determinati: PA dovrà accertare l'identità del soggetto prima di erogazione del servizio.

↓

nei servizi ad accesso limitato necessità di strumenti di identificazione informatica

Identità digitali: identificazione informatica

Si parla di strumenti di identificazione informatica e non più di autenticazione informatica a seguito delle modifiche apportate da d.lgs. 235/2010.

- **autenticazione del documento informatico** → la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione (lett. b modificata da d.lgs. 235/2010).
- **identificazione informatica** → la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso (lett. u-ter aggiunta da d.lgs. 235/2010).

Identità informatica: le carte

Sono strumenti per l'accesso ai servizi erogati on line da PA per i quali sia necessaria l'identificazione informatica (art. 64 d.lgs. 82/2005 mod. da d.lgs. 235/2010)

- **carta d'identità elettronica (CIE)**: art. 1 lett. c) Codice modificato da d.lgs. 235/2010): col documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare.
- **carta nazionale dei servizi (CNS)**: art. 1 lett. d) codice): il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

Le carte elettroniche sono personali (intestate ad una determinata persona fisica) e consistono in smart card dotate di microchip.

Strumenti diversi da CIE e CNS →le PPAA possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla CIE e dalla CNS, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. L'accesso con CIE e CNS è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni (art. 64, comma 2 modificato da d.lgs. 235/2010).

Identità informatica: le carte

Strumenti per l'accesso ai servizi erogati on line da PA per i quali sia necessaria l'identificazione informatica (art. 64 d.lgs. 82/2005 mod. da d.lgs. 235/2010)

- **carta d'identità elettronica (CIE)**: art. 1 lett. c) Codice modificato da d.lgs. 235/2010): ol documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare.
- **carta nazionale dei servizi (CNS)**: art. 1 lett. d) codice): il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

Le carte elettroniche sono personali (intestate ad una determinata persona fisica) e consistono in smart card dotate di microchip.

strumenti diversi da CIE e CNS →le PPAA possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla CIE e dalla CNS, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. L'accesso con CIE e CNS è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni (art. 64, comma 2 modificato da d.lgs. 235/2010).

Identità informatica: le carte

- **Carta d'identità elettronica (CIE)** : art. 66 caratteristiche e modalità per il rilascio definite con d.p.c.m.
  - contenuto obbligatorio → dati identificativi della persona e codice fiscale.
  - contenuto facoltativo → l'indicazione del gruppo sanguigno; le opzioni di carattere sanitario previste dalla legge; le procedure informatiche e le informazioni che possono o debbono essere conosciute, occorrenti per la firma elettronica etc.

- **Carta nazionale dei servizi (CNS)** : art. 66 caratteristiche e modalità per il rilascio, diffusione e uso sono definite con uno o più regolamenti, ex art. 17, comma 2, l. 400/1988 nel rispetto dei seguenti princìpi:

a) all'emissione provvedono, su richiesta del soggetto interessato, le PPAA che intendono rilasciarla;

b) l'onere economico è a carico delle singole amministrazioni che le emettono;

c) eventuali indicazioni di carattere individuale connesse all'erogazione dei servizi al cittadino, sono possibili nei limiti di cui al d.lgs. 196/2003;

d) le PPAA che erogano servizi in rete devono consentirne l'accesso ai titolari della CNS indipendentemente dall'ente di emissione responsabile del suo rilascio;

e) può essere utilizzata anche per i pagamenti informatici tra soggetti

Identità informatica: le carte

- **utilizzazione CIE e CNS** (art. 66 commi 5 e 7):

  - possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e PPAA, secondo le modalità stabilite con le regole tecniche ex art. 71, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.

  - nel rispetto della disciplina generale fissata dai decreti della norma e delle disposizioni in materia di privacy, le PA nell'ambito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.

Identità digitale: gli strumenti

Le ultime modifiche al CAD definiscono con chiarezza quali sono gli strumenti e le modalità di identificazione attraverso i quali poter usufruire di servizi on line e presentare istanze e dichiarazioni a una Pubblica Amministrazione:

- la firma digitale;
- la Carta d'Identità Elettronica (CIE) , ovvero il documento di identità rilasciato ai cittadini dai Comuni, provvisto di banda magnetica e microchip, e la Carta Nazionale dei Servizi (CNS), strumento di accesso ai servizi on-line rilasciata a discrezione delle singole Amministrazioni;
- la casella di posta elettronica certificata (PEC), in cui le credenziali di accesso sono rilasciate previa identificazione, anche telematica, del titolare della casella;
- altri strumenti che consentono l'individuazione del soggetto che richiede il servizio, compreso l'invio per via telematica delle istanze e la copia fotostatica del documento di identità.

Identità digitale: la PEC

Il campo di utilizzo della PEC viene reso ancora più esteso per i cittadini e le imprese e vincolante per le Amministrazioni.

L'invio di documenti tramite PEC è equivalente alla notificazione per mezzo della posta tradizionale "salvo che la legge disponga diversamente": quindi l'invio di documenti ed istanze alla PA tramite posta elettronica certificata va sempre bene, a meno che non sia esplicitamente proibito.

Il cittadino non deve più domandarsi: "La posso usare?" ma è l'amministrazione che deve chiaramente indicare i casi in cui non sia possibile usarla

Identità digitale: la PEC

Le amministrazioni:

- devono utilizzare la PEC per tutte le comunicazioni che necessitano di una ricevuta di invio e di una di consegna –raccomandata A/R – verso cittadini che hanno preventivamente comunicato il proprio di indirizzo di PEC;
- devono pubblicare i propri indirizzi di posta elettronica certificata nell'Indice delle PA , che costituisce la rubrica degli indirizzi delle amministrazioni, accessibile e consultabile da tutti all'indirizzo www.indicepa.gov.it;
- interventi di natura tecnico-organizzativa volti a permettere l'utilizzo delle stesse caselle nell'ambito di procedimenti amministrativi, associandole alle opportune strutture organizzative, uffici di protocollo innanzitutto.

I cittadini:

- accettano automaticamente l'invio di atti e provvedimenti che li riguardano da parte delle PA una volta dichiarato il proprio indirizzo PEC;
- possono trovare gli indirizzi di PEC dei diversi enti all'indirizzo: www.indicepa.gov.it.

Le imprese:

- la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni tra imprese e Pubbliche Amministrazioni avviene esclusivamente utilizzando modalità telematiche, in coerenza con l'obbligo, per tutti i

Comunicazione tra PA

- ✓ **La trasmissione dei documenti tra pubbliche amministrazioni**: art. 47 (mod. da d.lgs. 235/2010): le comunicazioni di documenti tra PPAA avvengono **mediante l'utilizzo della posta elettronica o in cooperazione applicativa**; esse sono valide ai fini del procedimento amministrativo **una volta che ne sia verificata la provenienza**.

↓

ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata ;

b) ovvero sono dotate di segnatura di protocollo di cui all'art. 55 d.p.r. 445/2000;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'art. 71;

d) ovvero trasmesse attraverso sistemi di PEC di cui al d.p.r. 68/2005.

↓

d.lgs. 235/2010 introduce possibilità di cooperazione applicativa (prevista accanto all'utilizzo della posta elettronica).

Comunicazioni tra PA

- ✓ **Le comunicazioni di documenti tra pubbliche amministrazioni e propri dipendenti** (art. 47, comma 3) avvengono mediante posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di privacy e previa informativa agli interessati sul grado di riservatezza degli strumenti utilizzati.

- ✓ **La trasmissione di documenti che necessitano di una ricevuta di invio e di una ricevuta di consegna** (art. 48, comma 1) avviene mediante PEC ai sensi del d.p.r. 68/2005 o mediante altre soluzioni tecnologiche individuate con d.p.c.m., sentito DigitPA.

  In tal caso la trasmissione, salvo che la legge disponga diversamente, corrisponde alla notificazione per mezzo della posta; data e ora di trasmissione e ricezione così trasmessi sono opponibili ai terzi in caso di PEC se conformi a disposizioni del d.p.r. 68/2005 (su PEC) e alle relative regole tecniche ovvero in caso di altre soluzioni tecnologiche se conformi al d.p.c.m. che le prevederà.

.

Comunicazioni tra PA e cittadini e imprese

Le istanze e le dichiarazioni possono essere presentate alla PA attraverso molteplici canali e sono valide

1) se sottoscritte mediante **firma digitale o la firma elettronica qualificata**
2) ovvero, quando l'autore è identificato dal sistema informatico con **l'uso della CIE o CNS** nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente.
3) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti ex art. 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione → **strumenti diversi da CIE e CNS** → strumenti diversi dalla CIE e dalla CNS, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio.

   ↓

   D.lgs. 235/2010 opera **apertura a pluralità degli strumenti** che abilitano all'accesso ai servizi, cui conferisce pari dignità; prima si prevedeva quale modalità "ad esaurimento" ossia dopo il 31/12/2010 strumento non più valido, ora invece la soluzione non ha più limite temporale e diventa permanente. Es. identificativo utente + chiave di accesso.

4) ovvero se trasmesse dall'autore mediante la propria **casella di posta elettronica certificata** purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare,

Comunicazioni tra PA e cittadini e imprese

Il D.lgs. 235/2010 pone requisiti in più rispetto a versione precedente (prevedeva soltanto "*quando l'autore è identificato dal sistema informatico attraverso le credenziali di accesso relative all'utenza personale di PEC*").

Esigenza di associare casella PEC al rispettivo titolare in modo sia possibile attribuire paternità a messaggi inoltrati.

Dal combinato disposto di artt. 6, 48 e 65 PEC assolve al tempo stesso al ruolo di canale di comunicazione e strumento di identificazione.

Comunicazioni telematiche

Comunicazioni telematiche:

- **c.d. decreto Semplificazioni** → decreto legge 9 febbraio 2012, n. 5 (Disposizioni urgenti in materia di semplificazione e di sviluppo) convertito con modificazioni dalla legge 4 aprile 2012, n. 35.

- art. 6 → **comunicazione di dati per via telematica**: prevede che una serie di comunicazioni e trasmissioni tra enti pubblici (dettagliate dalla norma, es. relativamente all'elettorato attivo e tenuta e revisione liste elettorali) siano effettuate esclusivamente in modalità telematica in conformità alle disposizioni di cui al decreto legislativo 82/2005. Modalità e termini per l'attuazione saranno disciplinati con uno o più decreti ministeriali.
- art. 8 → **semplificazioni per la partecipazione a concorsi e prove selettive**: le domande e i relativi allegati per la partecipazione a selezioni e concorsi per l'assunzione nelle pubbliche amministrazioni centrali banditi a decorrere dal 30 giugno 2012 sono inviate esclusivamente per via telematica secondo le modalità di cui all'art. 65 del d.lgs. 82/2005. Sono nulle le clausole dei bandi in contrasto con la presente disposizione. PPAA provvedono a quanto previsto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri a carico della finanza pubblica. Regioni adeguano i propri ordinamenti a quanto previsto.

La PEC: come funziona

Il funzionamento del servizio PEC (d.p.r. 68/2005):

- autenticazione del mittente (password) per accedere a servizio
- mittente invia messaggio di PEC al proprio gestore di PEC
- gestore di PEC del mittente trasmette al destinatario direttamente o lo trasferisce al gestore di PEC di cui si avvale il destinatario
- gestore del destinatario provvede alla consegna nella casella di PEC del destinatario
- il gestore di PEC del mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di PEC oppure, se non risulta consegnabile, comunica al mittente, entro le 24 ore successive all'invio, la mancata consegna tramite un avviso
- quando la trasmissione del messaggio di PEC avviene tramite più gestori il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio
- gestore di PEC utilizzato dal destinatario fornisce al mittente, all'indirizzo elettronico del mittente, la ricevuta di avvenuta consegna
- durante le fasi di trasmissione del messaggio di PEC, i gestori mantengono traccia delle operazioni svolte su un apposito *log* dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di PEC per 30 mesi, tracce informatiche dei *log* dei messaggi sono opponibili ai terzi.

La PEC: i soggetti

I soggetti del servizio di PEC (artt. 1 e 2 d.p.r. 68/2005)

- utente di posta elettronica certificata → la persona fisica, la persona giuridica, la PA e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di PEC.

Soggetti:

- mittente → l'utente che si avvale del servizio di PEC per la trasmissione di documenti prodotti mediante strumenti informatici;
- destinatario → l'utente che si avvale del servizio di PEC per la ricezione di documenti prodotti mediante strumenti informatici;
- gestore del servizio → il soggetto, pubblico o privato, che eroga il servizio di PEC e che gestisce domini di PEC. Definizione di gestore di PEC di cui ad art. u-bis CAD (aggiunta da d.lgs. 235/2010): il soggetto che presta servizi di trasmissione dei documenti informatici mediante PEC.

La PEC: validità

- Il documento informatico trasmesso per via telematica si intende: spedito dal mittente se inviato al proprio gestore e consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore (art. 45, comma 2 d.lgs. 82/2005): indipendentemente quindi dalla sua effettiva lettura;
- La trasmissione del documento informatico per via telematica, effettuata mediante PEC, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta (art. 48, comma 2 d.lgs. 82/2005).
- La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante PEC sono opponibili ai terzi se conformi alle disposizioni di cui al d.p.r. 68/2005 ed alle relative regole tecniche (art. 48, comma 3 d.lgs. 82/2005).
- La PEC consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge (art. 4 d.p.r. 68/2005).

La PEC: ruolo centrale

Il passaggio all'esclusività dell'utilizzo di tecnologie, nei rapporti fra PA ed imprese, è centrale

Per tutti, l'utilizzo della PEC è ampliato: le PA utilizzano la PEC per le comunicazioni con tutti i soggetti che hanno preventivamente dichiarato il proprio indirizzo. La dichiarazione dell'indirizzo vincola solo colui che lo dichiara e rappresenta espressa accettazione dell'invio, tramite PEC, da parte delle PA degli atti e dei provvedimenti che lo riguardano.

Fruibilità dei servizi in rete e strumenti di accesso

- Centralità della corretta gestione del patrimonio informativo pubblico: le amministrazioni devono condividere, nel rispetto della privacy dei cittadini, i dati di cui sono titolari: un'informazione data una volta ad un'amministrazione o di proprietà dell'amministrazione stessa non deve più essere richiesta al cittadino, ma deve essere messa a disposizione delle altre PA interessate.
- Le "basi di dati di interesse nazionale" costituiscono un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che deve garantire l'allineamento delle informazioni e l'accesso alle medesime da parte delle PA

  Innovativa rispetto al passato l'indicazione di quali sono le basi di dati di interesse nazionale, e precisamente:

a) repertorio nazionale dei dati territoriali;

b) indice nazionale delle anagrafi;

c) banca dati nazionale dei contratti pubblici;

d) casellario giudiziale;

e) registro delle imprese;

f) archivi automatizzati in materia di immigrazione e di asilo.

Disponibilità e fruibilità dei dati pubblici, open data e sicurezza

- Dato delle pubbliche amministrazioni → art. 1, lett. m) d.lgs. 82/2005: il dato formato, o comunque trattato da una pubblica amministrazione
- Dato pubblico → art. 1, lett. n) d.lgs. 82/2005: il dato conoscibile da chiunque.

Principi

- Disponibilità → art. 1, lett. o) d.lgs. 82/2005: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge
- Fruibilità dei dati pubblici → art. 1, lett. t) d.lgs. 82/2005: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione.

Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato (art. 58, comma 1 d.lgs. 82/2005).

Disponibilità e fruibilità dei dati pubblici, open data e sicurezza

- I dati delle PPAA sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre PPAA e dai privati.
- Interoperabilità fra PPAA ed erogazione servizi on line → centralità e valorizzazione di informazione digitale (società dell'informazione)→ passaggio dal documento al dato (così E. Belisario).

Limiti alla conoscibilità dei dati:

- quelli previsti dalle leggi e dai regolamenti (es. esclusioni ad accesso)
- le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico (d.lgs. 36/2006 di recepimento dir. 2003/98/CE) (art. 50 d.lgs. 82/2005)

Fruibilità dei servizi in rete e strumenti di accesso

- I dati delle Pubbliche Amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione.

- L'informazione pubblica deve essere valorizzata attraverso progetti di elaborazione e diffusione dei dati, che possono essere finanziati dalle amministrazioni ricorrendo a strumenti di finanza di progetto.

- Oltre ad aggiornare tempestivamente i dati dei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi, le amministrazioni devono consentire l'accesso gratuito alle banche dati accessibili per via telematica di cui sono titolari. Tale accesso deve essere disciplinato mediante apposite convenzioni da stipulare con le amministrazioni interessate.

- Anche i dati pubblicati sui siti pubblici devono essere fruiti gratuitamente e devono inoltre essere resi disponibili secondo un formato aperto.

Fruibilità dei servizi in rete e strumenti di accesso

- Fra i dati gestiti dalla Pubblica Amministrazione, il Codice assegna una particolare rilevanza al tema dei dati territoriali. Per dato territoriale si intende qualunque informazione geograficamente localizzata.

- La conoscenza del dato territoriale, nei suoi vari aspetti, è determinante sia come strumento per lo sviluppo di nuovi servizi sia come supporto alle decisioni in molteplici campi: politiche di sicurezza, di protezione civile, agricoltura, pianificazione territoriale, trasporti, ambiente, catasto, governo del territorio, gestione delle infrastrutture, sviluppo economico, reti tecnologiche, ecc., con ricadute significative anche sul terreno della fiscalità

- In Italia sono molte le materie "concorrenti" spesso distribuite tra più soggetti: numerosi Enti o Amministrazioni raccolgono, producono o gestiscono dati territoriali in funzione delle proprie competenze istituzionali. L'informazione territoriale è quindi caratterizzata da un consistente patrimonio di dati e, contestualmente, da una significativa frammentazione non strutturata e da molteplici sovrapposizioni