Il Codice dell'Amministrazione Digitale

Gianfranco Pontevolpe

Direttore Cisia di Roma - DGSIA

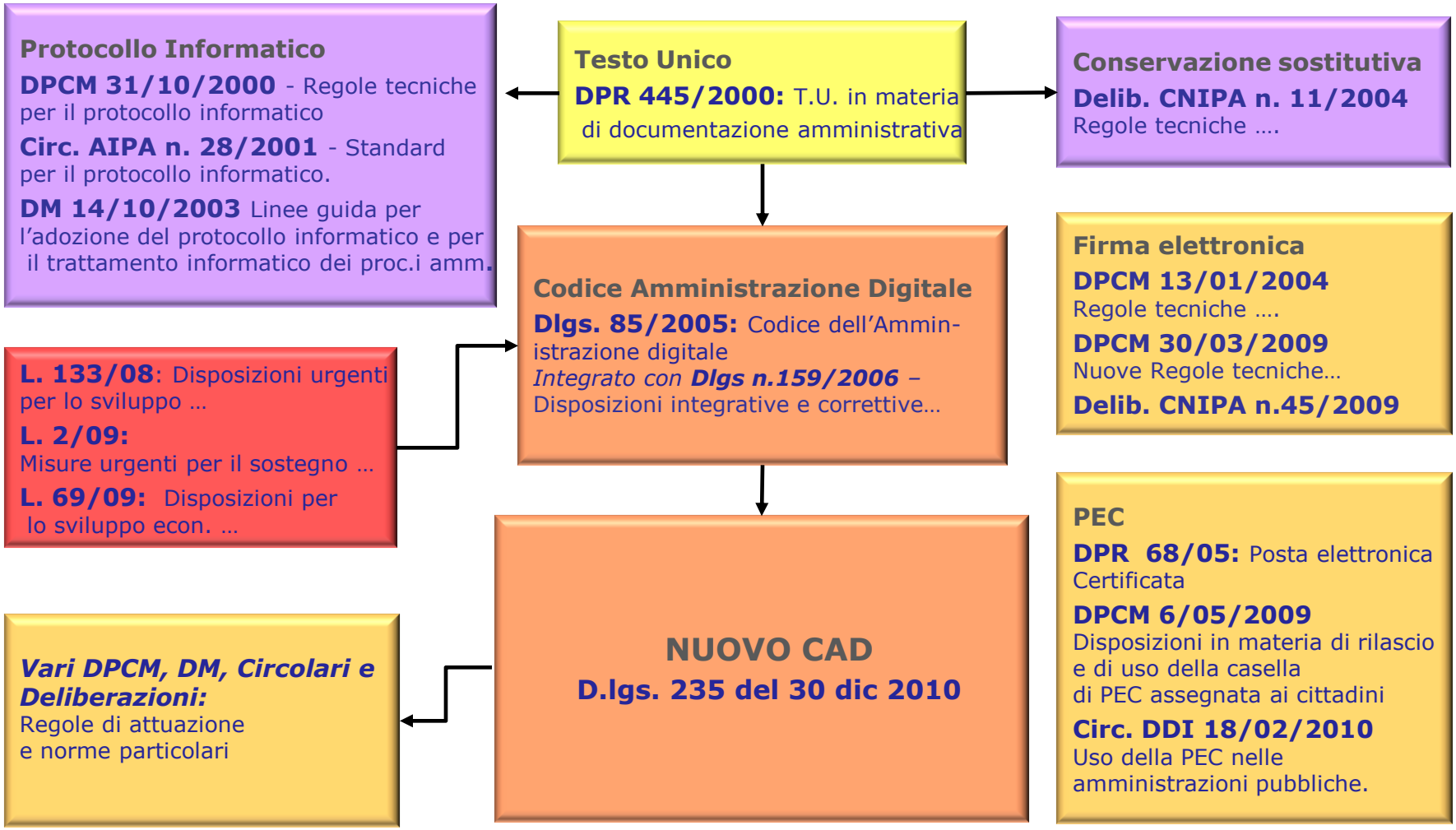
Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- Gli strumenti del CAD nella Giustizia

Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- Gli strumenti del CAD nella Giustizia

Il quadro delle norme tecniche



Atto e documento

- Atto e documento sono il risultato di fasi distinte:
  - quella dell'agire
  - quella della sua memorizzazione e del suo ricordo (o meglio della sua rappresentazione)
- Utilizzo ambiguo dei termini anche nella normativa archivistica
- Necessità di coerenza terminologica sia per il trattamento delle memorie del passato che, soprattutto, per la formazione corretta dei sistemi documentari attivi (record management)

La definizione di documento

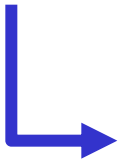
- DOCUMENTO AMMINISTRATIVO ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (DPR 445/2000 art. 1 comma 1 lett a)
- DOCUMENTO INFORMATICO la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (DPR 445/2000 art. 1 comma 1 lett. b e D. Lgs. 82/2005 art. 1 comma 1 lett. p)

Gli elementi del documento

- Nella dottrina un documento deve presentare sempre alcuni elementi:
  - supporto/mezzo di memorizzazione, solitamente inteso come componente **immodificabile**
  - contenuto **stabile**
  - **provenienza certa**, intesa come indicazione certa dell'autore del documento (responsabile per il suo contenuto)

La prima fase della dematerializzazione

- Scomparsa della carta a favore del documento informatico
  - Risparmio nei costi di gestione e stoccaggio
  - Efficienza nel reperimento delle informazioni archiviate



    - Pieno valore dei documenti digitali
    - Procedure per il riversamento delle immagini dei documenti cartacei
    - Conservazione dei documenti digitali

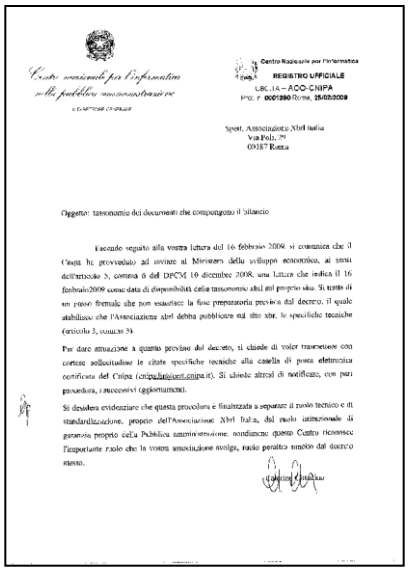
La fase iniziale della diffusione di una nuova tecnologia

FIAT mod. 4 HP - 1899

Fonte: Museo dell'automobile – www.museoauto.it

La fase iniziale del documento informatico

- Il documento informatico è sostanzialmente un documento dattiloscritto
- Le norme sulla gestione documentale sono speculari rispetto a quelle relative al documento tradizionale



Centro nazionale per l'informatica nella pubblica amministrazione

Centro Nazionale per l'Informatica
REGISTRO UFFICIALE
USC.IA – AOO-CNIPA
Prot. n. 0001390/Roma, 16/02/2009

Spett. Associazione Xbrl Italia
via Poli, 29
00187 Roma

Oggetto: tassonomie dei documenti che compongono il bilancio

Facendo seguito alla vostra lettera del 16 febbraio 2009, si comunica che il Cnipa ha provveduto ad inviare al Ministero dello sviluppo economico, ai sensi dell'articolo 3, comma 6 del DPCM 10 dicembre 2008, una Lettera che indica il 16 febbraio2009 come data di disponibilità della tassonomia sul suo proprio sito. Si tratta di un passo formale che non esaurisce la fase preparatoria prevista dal decreto, il quale stabilisce che l'Associazione xbrl debba pubblicare sul sito xbr. le specifiche tecniche (articolo 3, comma 3).

Per dare attuazione a quanto previsto dal decreto, si chiede di voler trasmettere con cortese sollecitudine le citate specifiche tecniche alla casella di posta elettronica certificata del Cnipa (cnipa@cert.cnipa.it). Si chiede altresì di notificare, con pari procedura, i successivi (aggiornamenti.

Si desidera evidenziare che questa procedura è finalizzata a separare il ruolo tecnico e di standardizzazione, proprio dell'Associazione Xbrl Italia, dal ruolo istituzionale di garanzia proprio della Pubblica amministrazione, nonostante questo Centro riconosce l'importante ruolo che la vostra associazione svolge, ruolo peraltro sancito dal decreto stesso.

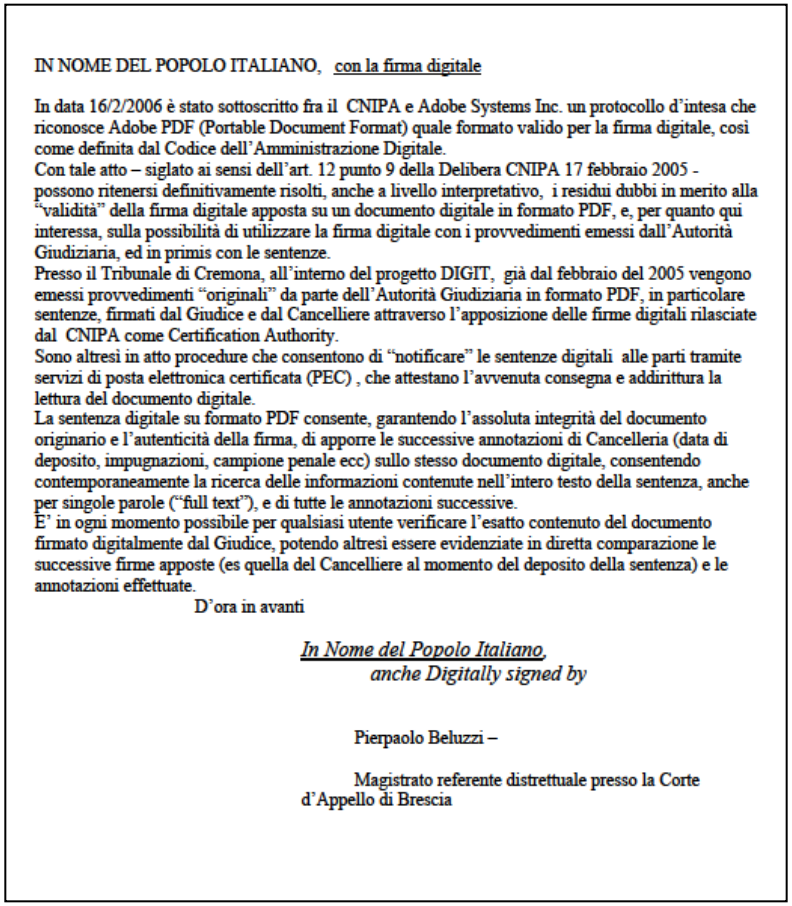
- Maggiore attendibilità dell'originale
- Criticità dei processi di copia

Le diverse forme del documento informatico

- Documento dattiloscritto
- Dati
  - basi dati
  - documenti XML
  - fogli di calcolo
  - moduli elettronici
- Immagini
- Registrazioni informatiche
- Documenti non convenzionali
  - ipertesti
  - documenti multimediali
  - documenti 3D

Il dattiloscritto informatico

- E’ simile al documento tradizionale
- Può essere stampato mantenendo l’aspetto originale
- La sua rappresentazione può essere
  - modificabile (doc, odt …)
  - non modificabile (pdf)



IN NOME DEL POPOLO ITALIANO, con la firma digitale

In data 16/2/2006 è stato sottoscritto fra il CNIPA e Adobe Systems Inc. un protocollo d’intesa che riconosce Adobe PDF (Portable Document Format) quale formato valido per la firma digitale, così come definita dal Codice dell’Amministrazione Digitale.
Con tale atto – siglato ai sensi dell’art. 12 punto 9 della Delibera CNIPA 17 febbraio 2005 - possono ritenersi definitivamente risolti, anche a livello interpretativo, i residui dubbi in merito alla “validità” della firma digitale apposta su un documento digitale in formato PDF, e, per quanto qui interessa, sulla possibilità di utilizzare la firma digitale con i provvedimenti emessi dall’Autorità Giudiziaria, ed in primis con le sentenze.
Presso il Tribunale di Cremona, all’interno del progetto DIGIT, già dal febbraio del 2005 vengono emessi provvedimenti “originali” da parte dell’Autorità Giudiziaria in formato PDF, in particolare sentenze, firmati dal Giudice e dal Cancelliere attraverso l’apposizione delle firme digitali rilasciate dal CNIPA come Certification Authority.
Sono altresì in atto procedure che consentono di “notificare” le sentenze digitali alle parti tramite servizi di posta elettronica certificata (PEC) , che attestano l’avvenuta consegna e addirittura la lettura del documento digitale.
La sentenza digitale su formato PDF consente, garantendo l’assoluta integrità del documento originario e l’autenticità della firma, di apporre le successive annotazioni di Cancelleria (data di deposito, impugnazioni, campione penale ecc) sullo stesso documento digitale, consentendo contemporaneamente la ricerca delle informazioni contenute nell’intero testo della sentenza, anche per singole parole (“full text”), e di tutte le annotazioni successive.
E’ in ogni momento possibile per qualsiasi utente verificare l’esatto contenuto del documento firmato digitalmente dal Giudice, potendo altresì essere evidenziate in diretta comparazione le successive firme apposte (es quella del Cancelliere al momento del deposito della sentenza) e le annotazioni effettuate.

D’ora in avanti

In Nome del Popolo Italiano,
anche Digitally signed by

Pierpaolo Beluzzi –

Magistrato referente distrettuale presso la Corte d’Appello di Brescia

La gestione informatica dei dati

- Record
- File
- Banche dati (data base)
  - Ciascuna banca dati ha uno schema che riporta i nomi dei campi e le relazioni tra questi
  - I dati vengono inseriti e visualizzati in forma di tabelle
  - E' possibile "costruire" tabelle aggregando i dati con qualunque criterio
- File XML

Un esempio di dati: le timbrature

Matricola	Nome	Cognome	Ingr.	Uscita	Ingr.	Uscita
4235	Mario	Rossi	8,05	17,05		
2318	Giulia	Bianchi	8,15	10,00	12,00	18,12
2310	Rosa	Verdi	8,21	18,00		
3023	Franco	Bianchi	8,22	17,00		
3241	Adele	Arancio	8,25	15,00	16,00	19,02
3312	Joe	Campbell	8,30	18,15		
3865	Elena	Rossi	8,32	17,45		

Dati ed etichette

4235MarioRossi08051705

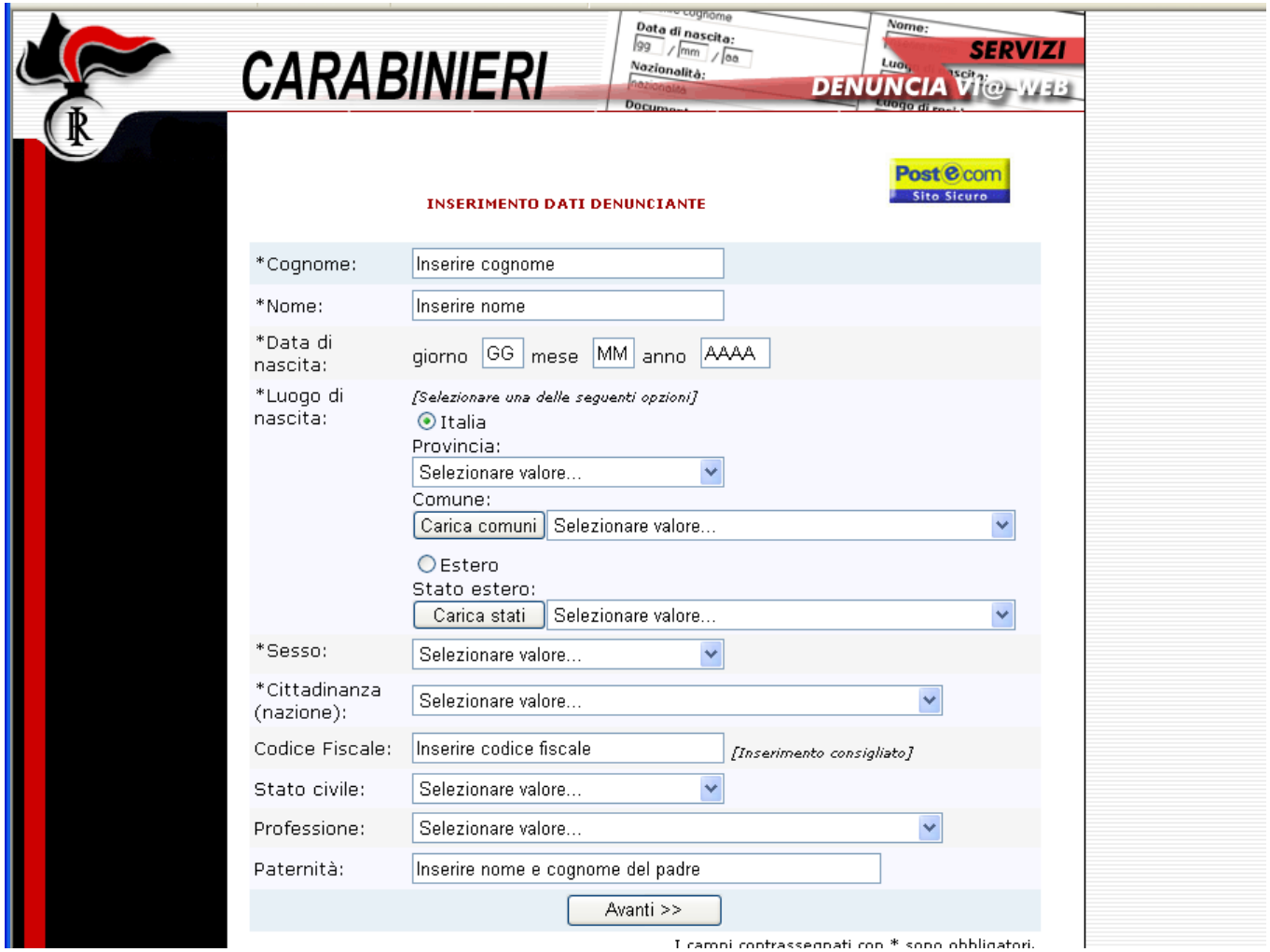
```
<matricola>4235</matricola>
<nome>Mario</nome>
<cognome>Rossi</cognome>
<ingr.>
  <ingr. ore>08</ingr. ore>
  <ingr. minuti>05</ingr. minuti>
</ingr.>
  <uscita>
  <uscita ore>08</uscita ore>
<uscita minuti>05</uscita minuti>
</uscita>
```

XML

I documenti XML

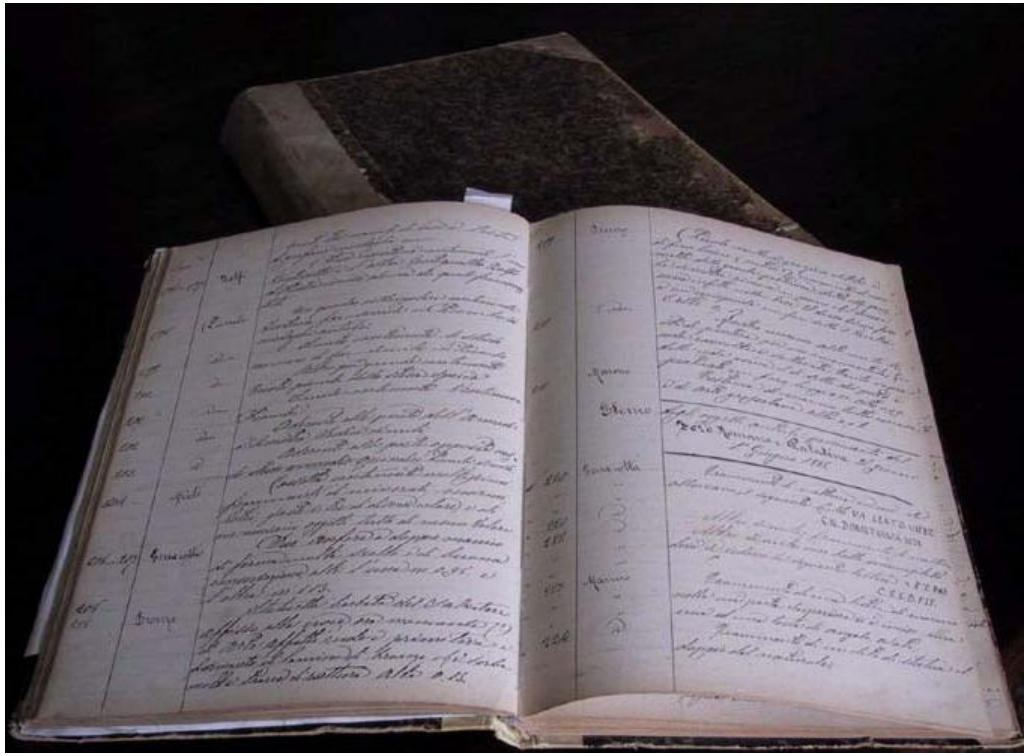
```
<?xml version="1.0" encoding="UTF-8" ?>
- <sincro:PreservationSchema sincro:url="http://www.cnipa.gov.it/sincro/"
sincro:version="1.0" xsi:schemaLocation="http://www.cnipa.gov.it/sincro/ schema.xsd"
xmlns:sincro="http://www.cnipa.gov.it/sincro/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
- <sincro:Objects>
  - <sincro:VdC>
      <sincro:ID sincro:scheme="NumConservazione">0000000012</sincro:ID>
    - <sincro:VdCGroup>
        <sincro:Label>Fatture Attive Servizi</sincro:Label>
        <sincro:ID sincro:scheme="IDDocument">213</sincro:ID>
        <sincro:Description sincro:language="IT">Fatture Attive Servizi come da Sezionale
            IVA n. XXX</sincro:Description>
      </sincro:VdCGroup>
  </sincro:VdC>
 - <sincro:FileGroup>
     <sincro:Label>FileGroup01</sincro:Label>
   - <sincro:File sincro:format="application/pdf" sincro:encoding="binary">
       <sincro:ID sincro:scheme="local">01</sincro:ID>
       <sincro:Path>Amministrazione/fattura0010.pdf</sincro:Path>
```

Maschere e moduli

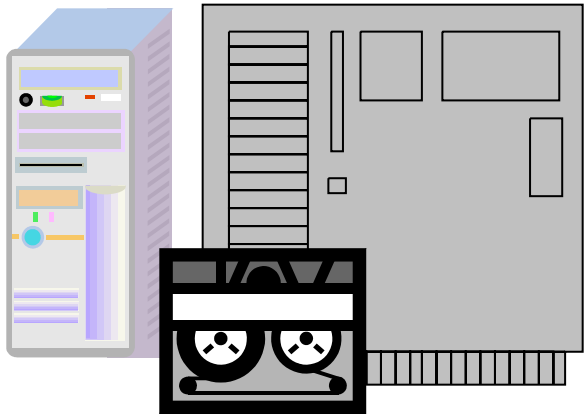


Documento e registrazioni

- Le registrazioni sono spesso riportate in documenti detti registri
  - Registro contabile
  - Registro delle presenze
  - Libro matricola
  - Registro di classe
  - Registro delle notizie di reato
  - …



Le registrazioni informatiche



… le registrazioni informatiche

- Una registrazione informatica è costituita dall'insieme di dati che testimoniano la dinamica di un evento o di una transazione ed il relativo risultato (ad es. il log di una transazione, i dati relativi ad un'operazione contabile, i metadati relativi all'evento …)
- Qualunque evento o transazione in un sistema informativo produce di norma almeno una registrazione, pertanto ad ogni evento è possibile associare
  - La traccia (log) che testimonia la dinamica delle operazioni informatiche
  - L'eventuale evidenza informatica che documenta il risultato dell'evento o della transazione

Un esempio di registrazione opponibile a terzi

Da: Posta Certificata
Data: giovedì 6 maggio 2010 13.53
A: cnipadir@cert.cnipa.it
Oggetto: CONSEGNA: Parere n. 21/2010 - Gara a procedura aperta per l'affidamento dei servizi di sviluppo, manutenzione e gestione del Sistema inf
Allega: daticert.xml (861 byte)
Protezione: Firma digitale e verifica

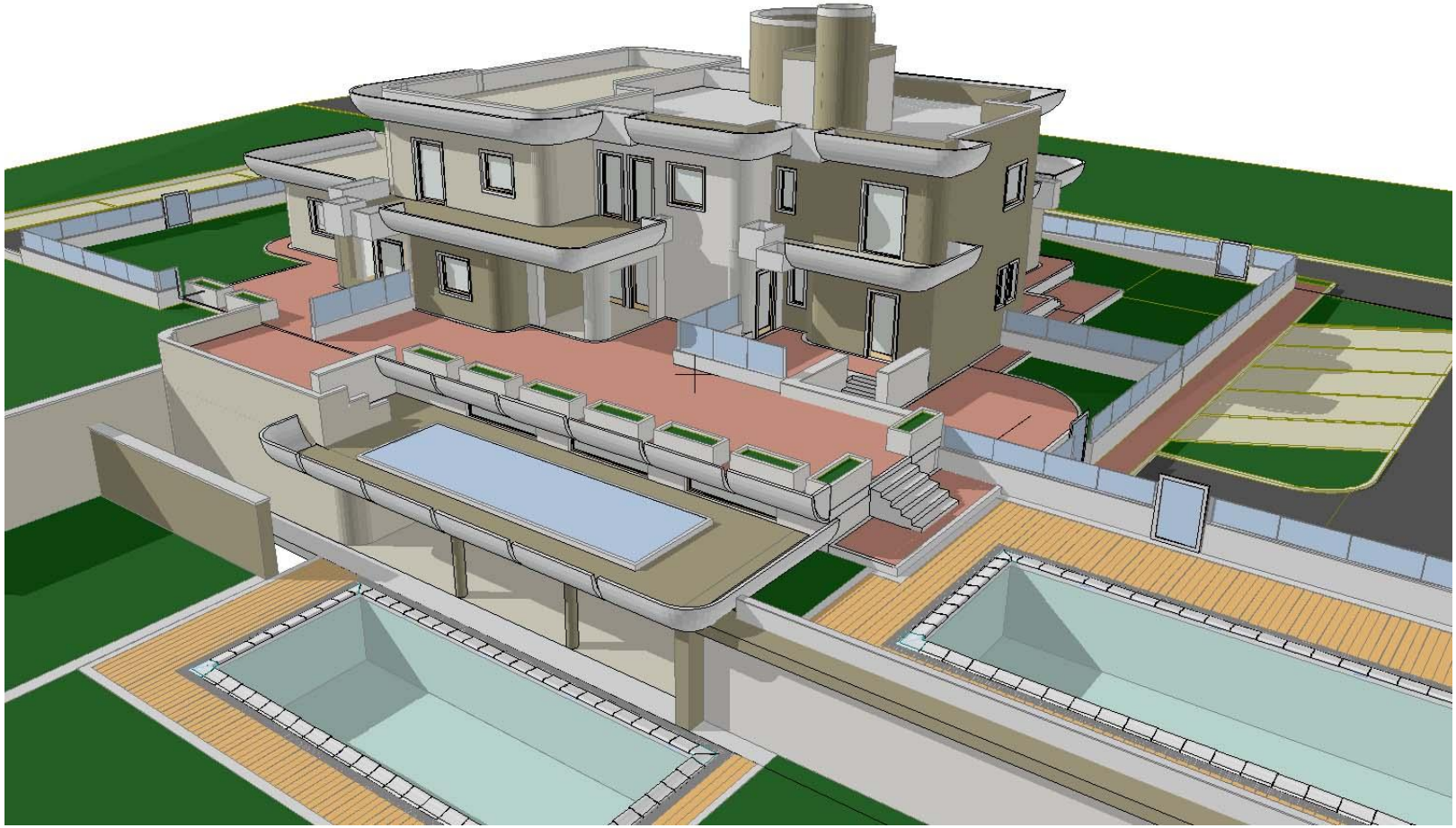
Ricevuta sintetica di Avvenuta Consegna

Il giorno **06/05/2010** alle ore **13:52:55 (+0200)** il messaggio
"**Parere n. 21/2010 - Gara a procedura aperta per l'affidamento dei servizi di sviluppo, manutenzione e gestione del Sistema informativo per l'Amministrazione del personale del Ministero dell'economia e delle finanze.RP/2870**" proveniente da
"**cnipadir@cert.cnipa.it**"
ed indirizzato a:
"adconsip@consippec.tesoro.it"
e' stato consegnato nella casella di destinazione.

Identificativo messaggio: ***0-555C6EDF-540B-4DF6-9655-CD0A9ACC592D@spcoop.postacert.it***

I documenti ipertestuali

I documenti in 3 dimensioni



Documenti tradizionali che oramai sono informatici

- Telegramma (artt. 2705, 2706 c.c.)
- Riproduzioni fotografiche, sonore e cinematografiche (art. 2712 c.c.)
- Fotocopie (art. 2719 c.c.)
- Fax (art. 6, comma2, L. 412/91, art. 28, comma 1 , D.P.R. 445/2000 …)

Decreto legislativo 12 febbraio 1993, n. 39 – art. 3

- Gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite i sistemi informativi automatizzati
- 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 accompagnati dall'indicazione della fonte e del responsabile dell'immissione, riproduzione, trasmissione o emanazione. Se per la validità di tali operazioni e degli atti emessi sia prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile

Differenze fra documento analogico ed informatico

Documento analogico

- **Unitarietà** di registrazione, contenuto e rappresentazione
- Utilizzo **diretto** del supporto di registrazione
- Metodi per assicurare la **conformità** delle copie all'originale
- Associazioni per **contiguità** (fascicoli, serie …)
- **Scarsità** di tracce
- Conservazione condizionata da esigenze di **spazio**

Documento informatico

- **Disaccoppiamento** di registrazione, contenuto e rappresentazione
- Utilizzo **indiretto** del supporto di registrazione
- Metodi per assicurare l'**autenticità** della rappresentazione
- Associazioni per **proprietà** (viste)
- **Ricchezza** di tracce
- Conservazione condizionata da esigenze di **efficienza**

Le diverse tipologie di copia nel mondo digitale

- Il disaccoppiamento di registrazione, contenuto e rappresentazione comporta che si può copiare:
  - la registrazione
    (es. copia del file)
  - il contenuto
    (es. conversione di formato)
  - la rappresentazione
    (es. print screen o
    scansione con scanner)

La terminologia usata dal CAD

- Il disaccoppiamento di registrazione, contenuto e rappresentazione comporta che si può copiare:
  - la registrazione (es. copia del file) — Duplicato
  - il contenuto (es. conversione di formato) — Copia
  - la rappresentazione (es. print screen o scansione con scanner) — Copia per immagine

Il duplicato informatico

duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario

23-bis – Duplicati e Copie informatiche di documenti informatici

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71.

In pratica è un documento, non distinguibile dall'originale, ottenuto mediante funzione di

- ***copia di file***
- ***download/upload***
- **trasmissione via e-mail**

Le copie nel CAD

- **Copia informatica di documento informatico:** il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (ad es. quando si ottiene un nuovo documento cambiando il formato, come nel passaggio da un documento "doc" ad un documento "pdf")
- **Copia per immagine su supporto informatico di documento analogico:** il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto (ad es. quando mediante *scanner* si ottiene un nuovo documento informatico formato dalle immagini di un documento su carta)
- **Copia informatica di documento analogico:** il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto (ad es. quando attraverso uno *scanner* con funzione OCR si ottiene un nuovo documento informatico formato dal testo di un documento su carta)
- **Copia analogica di documento informatico** (ad es. quando si genera un documento su carta con la funzione di stampa a partire da un documento informatico)

Valore delle copie

- Due regimi
  - l'attestazione di conformità da parte di un notaio o altro pubblico ufficiale a ciò autorizzato, nel qual caso le copie hanno in ogni caso la stessa efficacia probatoria degli originali
  - l'impiego della copia senza alcuna attestazione, nel qual caso le copie hanno la stessa efficacia probatoria dell'originale se la conformità non è espressamente disconosciuta
- Il valore delle copie è ora coerente con il valore delle riproduzioni meccaniche (art. 2712 del Codice Civile)
- Fa eccezione la copia informatica di documento analogico (OCR)

Le regole tecniche

- La validità delle copie e dei duplicati è subordinata al rispetto delle regole tecniche (non ancora disponibili)
- Fanno eccezione le copie su supporto analogico di documenti informatici la cui conformità è attestata da un pubblico ufficiale e le copie di atti pubblici, scritture private ecc. spedite o rilasciate dai depositari pubblici autorizzati e dai pubblici ufficiali
- In particolare occorrerà definire la struttura dei dati relativi alla eventuale dichiarazione di conformità e la modalità con cui tali dati dovranno essere “asseverati” alla copia

Il contrassegno elettronico
(timbro digitale)

23-ter – Documenti amministrativi informatici

5. Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico..

In pratica le amministrazioni dovranno rendere disponibili applicazioni telematiche con cui i cittadini possano ottenere le eventuali attestazioni o certificazioni in forma elettronica con il contrassegno che ne garantisce l'autenticità, in modo da poter esibire, all'occorrenza, anche la stampa prodotta sulla propria postazione di casa

Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- La giurisprudenza sul CAD
- Gli strumenti del CAD nella Giustizia

La firma tradizionale

- Elemento che identifica l'autore del testo
- Atto con cui si conferma o si accetta il contenuto del documento
- Prova grafica, non riproducibile, che consente di verificare l'autenticità della sottoscrizione

La firma di un documento informatico

- Elemento che identifica l'autore del testo:

  Nome e cognome, codice fiscale, identificativo utente (User Id), PIN, password, dati biometrici
- Atto con cui si conferma o si accetta il contenuto del documento:

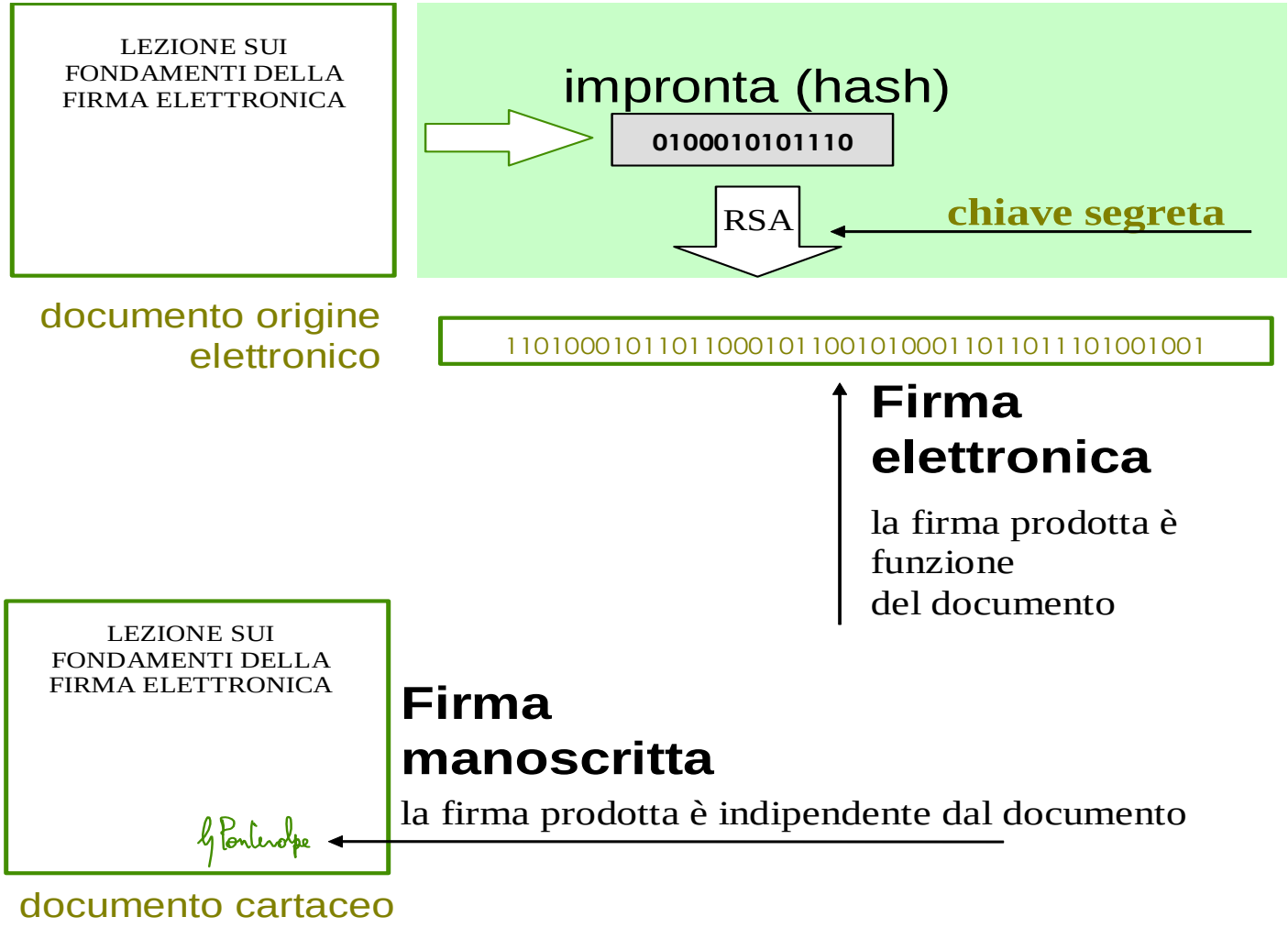
  Click sul pulsante «conferma» o «accetta»
- Prova grafica *non riproducibile* che consente di verificare l'autenticità della sottoscrizione:

  Log (traccia) dell'operazione, registrazione informatica, prova basata su metodi crittografici

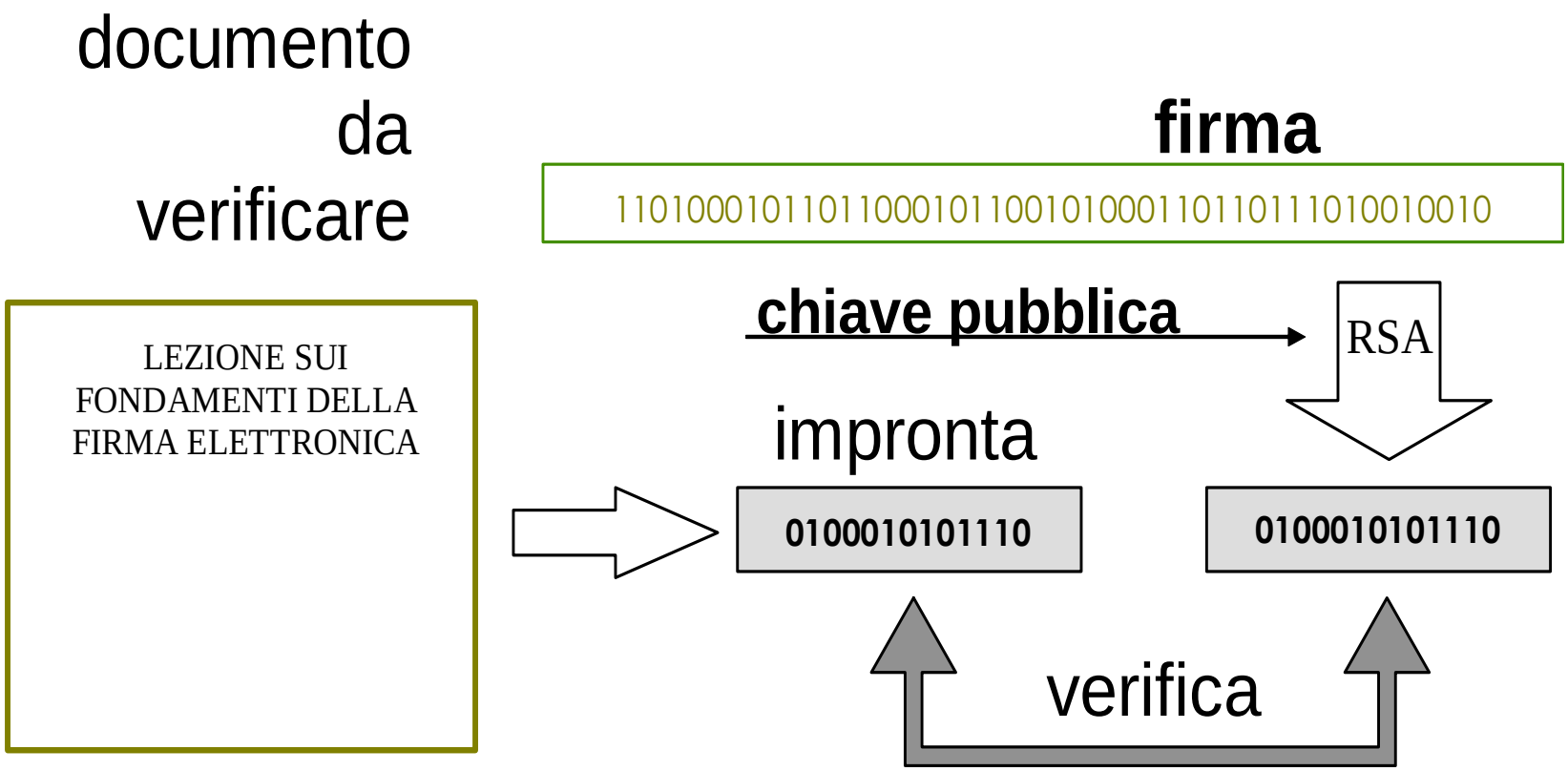
Metodi crittografici per la firma elettronica

- Consistono nel calcolo di particolari funzioni matematiche scelte in modo da assicurare le seguenti proprietà:
  - il risultato dell'operazione è un numero, detto firma elettronica, che può essere ottenuto solo attraverso la conoscenza di un numero segreto (detto chiave segreta)
  - per ogni chiave segreta esiste un numero correlato, detto chiave pubblica, che consente di verificare che l'operazione è stata eseguita con la corrispondente chiave segreta

Firma elettronica e firma manuale



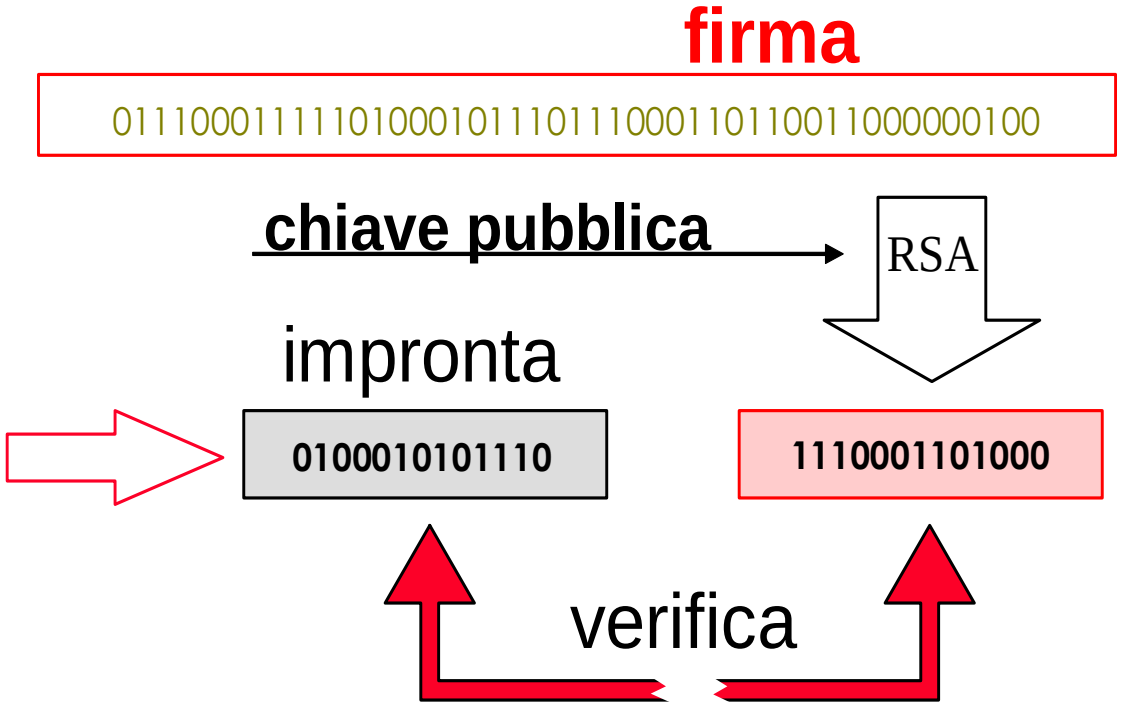
Verifica positiva della firma elettronica



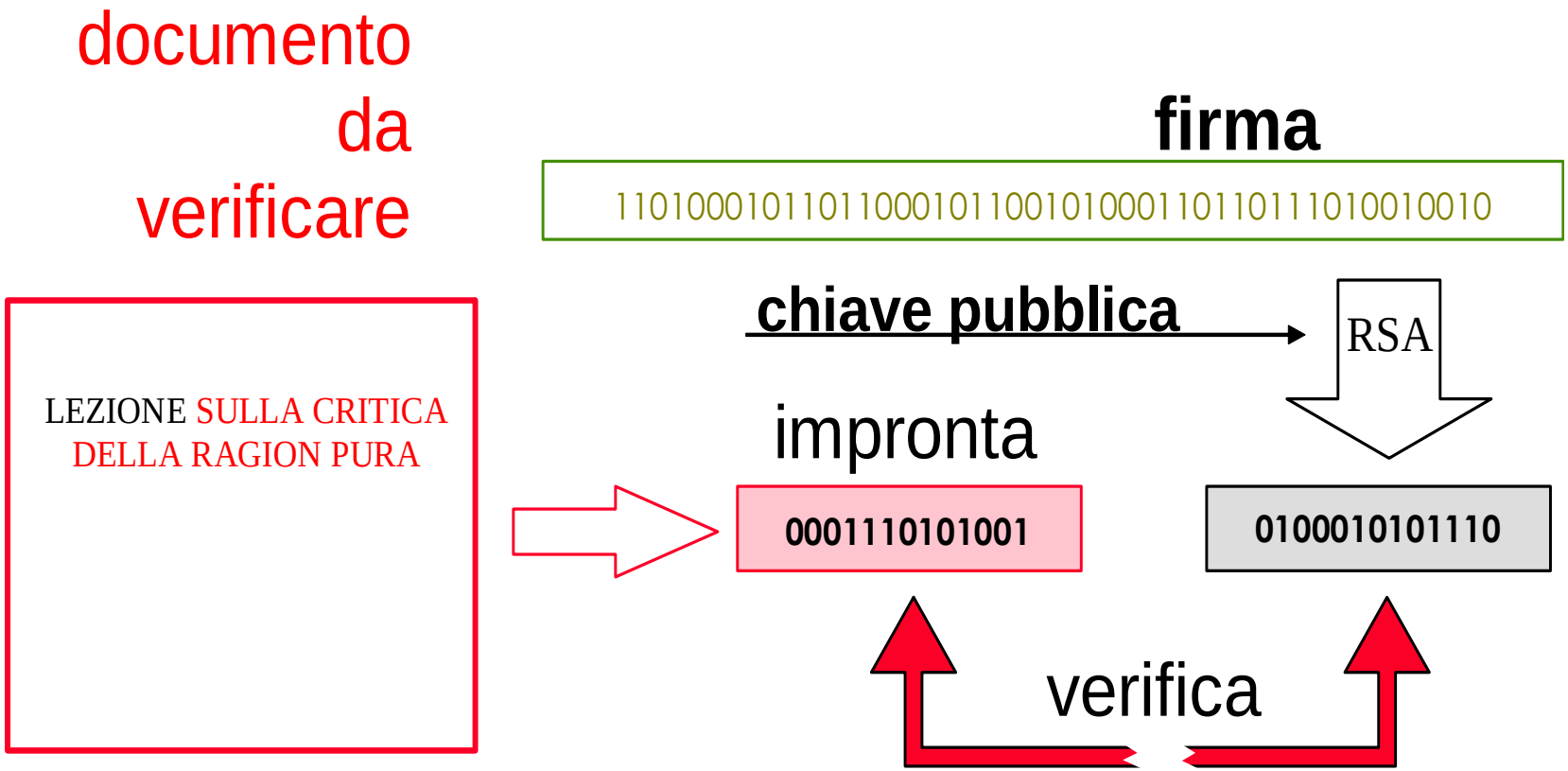
Verifica negativa (1)

documento da verificare

LEZIONE SUI FONDAMENTI DELLA FIRMA ELETTRONICA



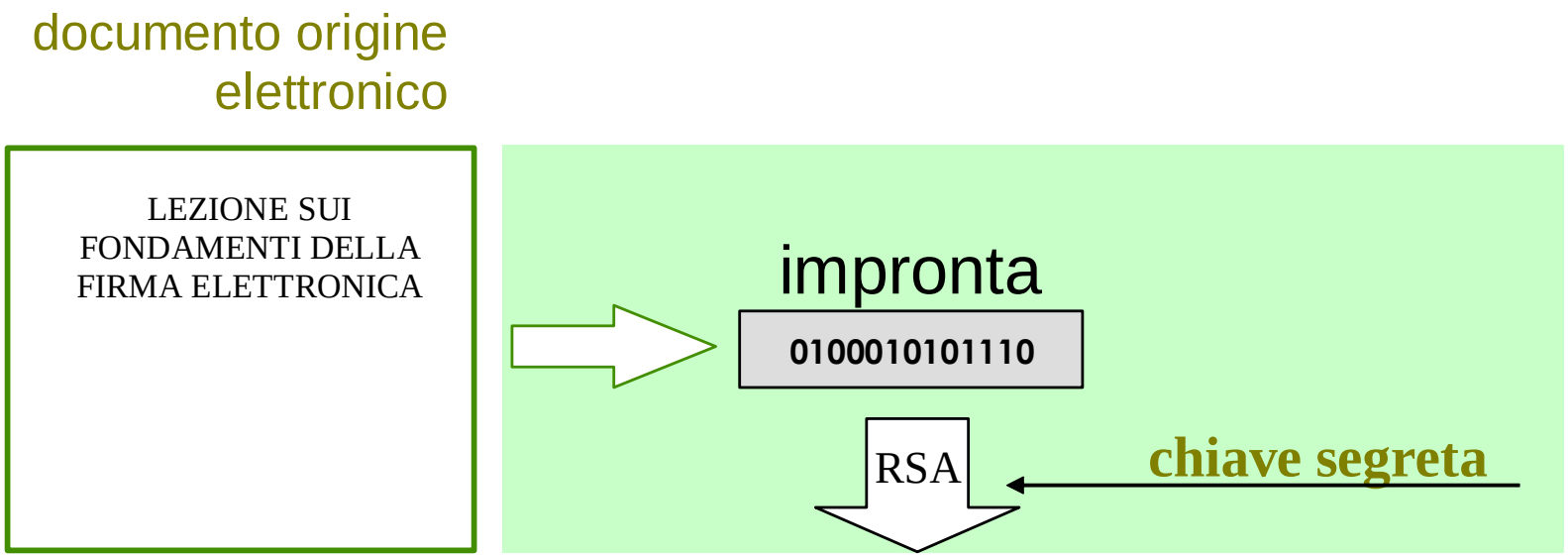
Verifica negativa (2)



L’importanza della chiave pubblica

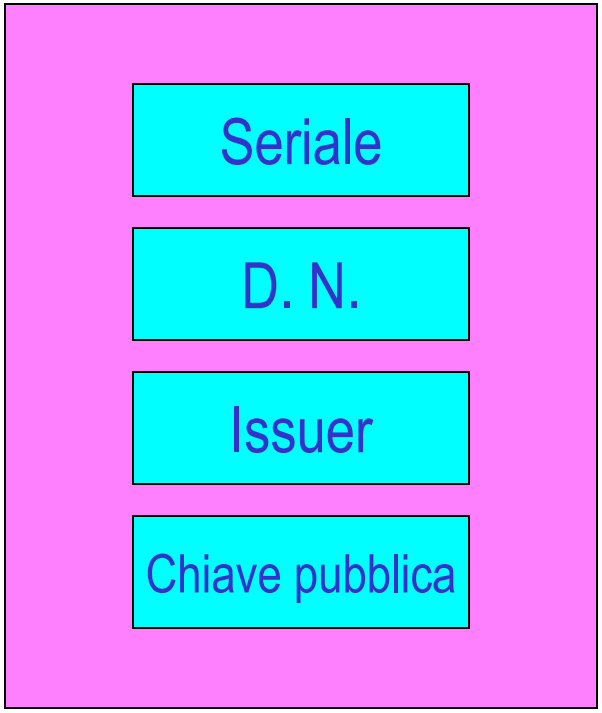
- Ciascuna chiave pubblica deve essere associabile univocamente ad una determinata entità (persona, sistema, nodo di rete, ecc.)
- Deve essere possibile attribuire con certezza una determinata chiave pubblica all’entità che ha utilizzato la corrispondente chiave segreta

La certificazione della chiave pubblica



Il certificato di chiave pubblica

Come ottengo la chiave pubblica di Tizio?



- E’ nel Certificato Digitale
- X509.V3 standard de facto

Le categorie principali di firma

- Identificazione informatica
  (PIN/password, biometria)

  I dati che comprovano la firma sono custoditi da un soggetto terzo

  Common law

- Crittografia
  (chiavi asimmetriche, PKI)

  I dati che comprovano la firma sono pubblici

  Civil law

La terminologia della Direttiva europea

- Identificazione informatica
  (PIN/password, biometria)

I dati che comprovano la firma sono custoditi da un soggetto terzo

Firma elettronica

- Crittografia
  (chiavi asimmetriche, PKI)

I dati che comprovano la firma sono pubblici

Firma elettronica avanzata

Opzioni della firma elettronica avanzata:

- Dispositivo sicuro per la creazione della firma
- Certificatore qualificato (garante dell'identità del firmatario)

Definizione di firma elettronica nella direttiva europea

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

La firma elettronica avanzata

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

Identificazione (autenticazione) informatica e firma digitale in Italia

- Con l'identificazione informatica si verifica l'utenza utilizzata per l'accesso a servizi informatici
  - È un processo on line
  - Ha obiettivi di sicurezza
  - Non è necessariamente connessa alla propria identità (possono esserci utenze anonime o collettive)
- Col la firma digitale si dimostra la paternità o la condivisione di un determinato documento
  - È un processo fuori linea
  - Ha obiettivi legali o amministrativi
  - È fortemente connessa alla propria identità

La firma digitale

- Prodotta con metodi crittografici che assicurano che solo un soggetto possa generare la firma, ma tutti la possano verificare
- Per la verifica della firma è necessario disporre del certificato che contiene la chiave crittografica di verifica (chiave pubblica)
- Il certificato attesta l'identità del soggetto cui è stata assegnata la chiave
- Le norme italiane assegnano al certificato ulteriori funzioni (sospensione o revoca della firma, limiti d'uso, ruolo, ecc.)

Le firme ibride

- Coniugano la semplicità della firma basata su identificazione informatica con la garanzia di integrità del documento propria della firma con crittografia asimmetrica
- Il firmatario invia "l'ordine di firma" ad un sistema remoto che genera la firma con una chiave attribuita solo a lui
- Il valore probatorio è quello della firma con crittografia asimmetrica (digitale/qualificata)
- Si distinguono in
  - Firma automatica
  - Firma remota

Firme apposte con procedura automatica

- Articolo 35, comma 3 del CAD: “L’apposizione di firme con procedura automatica è valida se l’attivazione della procedura medesima è chiaramente riconducibile alla volontà del titolare e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente”
- La firma viene generata da un server dotato di dispositivo sicuro di firma (smart card o HSM)
- Per soddisfare il comma 3 è necessario che l’utente utilizzi un sistema di autenticazione robusto

La firma biometrica

- Si basa sulla misura delle caratteristiche biometriche di un individuo (ad esempio la posizione degli elementi caratterizzanti un'impronta digitale)
- La c.d. "firma grafometrica" sulla dinamica dell'atto di sottoscrizione tradizionale
- La biometria può essere utilizzata come metodo di identificazione
- Per ottenere le caratteristiche proprie della firma digitale, occorre combinare le tecniche biometriche con la crittografia

Qualifiche e limiti d'uso

- Il certificato può contenere informazioni aggiuntive che possono essere utili nei rapporti professionali o nei negozi
- Tali informazioni sono enumerate nell'art. 28, comma 3, Cad che prevede che il certificato qualificato possa contenere
  a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
  b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'art. 30, comma 3.
  c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili

Revoche e sospensioni

- La revoca comporta l'iscrizione in una "lista nera" (chiamata anche lista di revoca o CRL *Certificate Revocation List*) del codice del certificato di chiave pubblica relativo alle chiavi che si intende bloccare
- La revoca produce effetti definitivi, la sospensione invece può essere annullata
- L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione (art. 21, comma 3, D.Lgs. 82/2005)

La validazione temporale

- E’ il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi (art. 1, comma 1, lett. bb, D.Lgs. 82/2005)
- Le regole tecniche correnti (DPCM 30 marzo 2009, art. 37) individuano cinque metodi idonei per la validazione temporale
  - l’attestazione della data ed ora operata da un certificatore accreditato nel giornale di controllo (*log*) oppure in un documento specifico che prende il nome di **marca temporale**;
  - la **registrazione di protocollo** effettuata da una pubblica amministrazione mediante il cosiddetto protocollo informatico;
  - l’indicazione della data ed ora di **conservazione** di un documento informatico ad opera di un pubblico ufficiale o di una pubblica amministrazione;
  - la registrazione di data ed ora effettuata dal fornitore del servizio di **posta elettronica certificata**;
  - l’attestazione di data ed ora ottenuta con il servizio di **marcatura postale elettronica** (EPCM - *Electronic Postal Code Mark*) offerto dai gestori del servizio postale universale (in Italia da Poste italiane).

La verifica della firma

- I prodotti di verifica della firma controllano
  - che la verifica crittografica della firma sia andata a buon fine, condizione che assicura che il documento non è stato modificato dopo la sua sottoscrizione
  - che il certificato del sottoscrittore sia firmato correttamente da un Certificatore incluso nell'Elenco pubblico tenuto dall'Agenzia per l'Italia Digitale, condizione che assicura l'attendibilità dell'identità del sottoscrittore
  - che il certificato del sottoscrittore non sia scaduto
  - che il certificato del sottoscrittore non sia stato sospeso o revocato
  - che il formato del documento firmato sia aderente agli standard europei (Pades o Cades), obbligatori per le firme emesse dal 1 luglio 2011

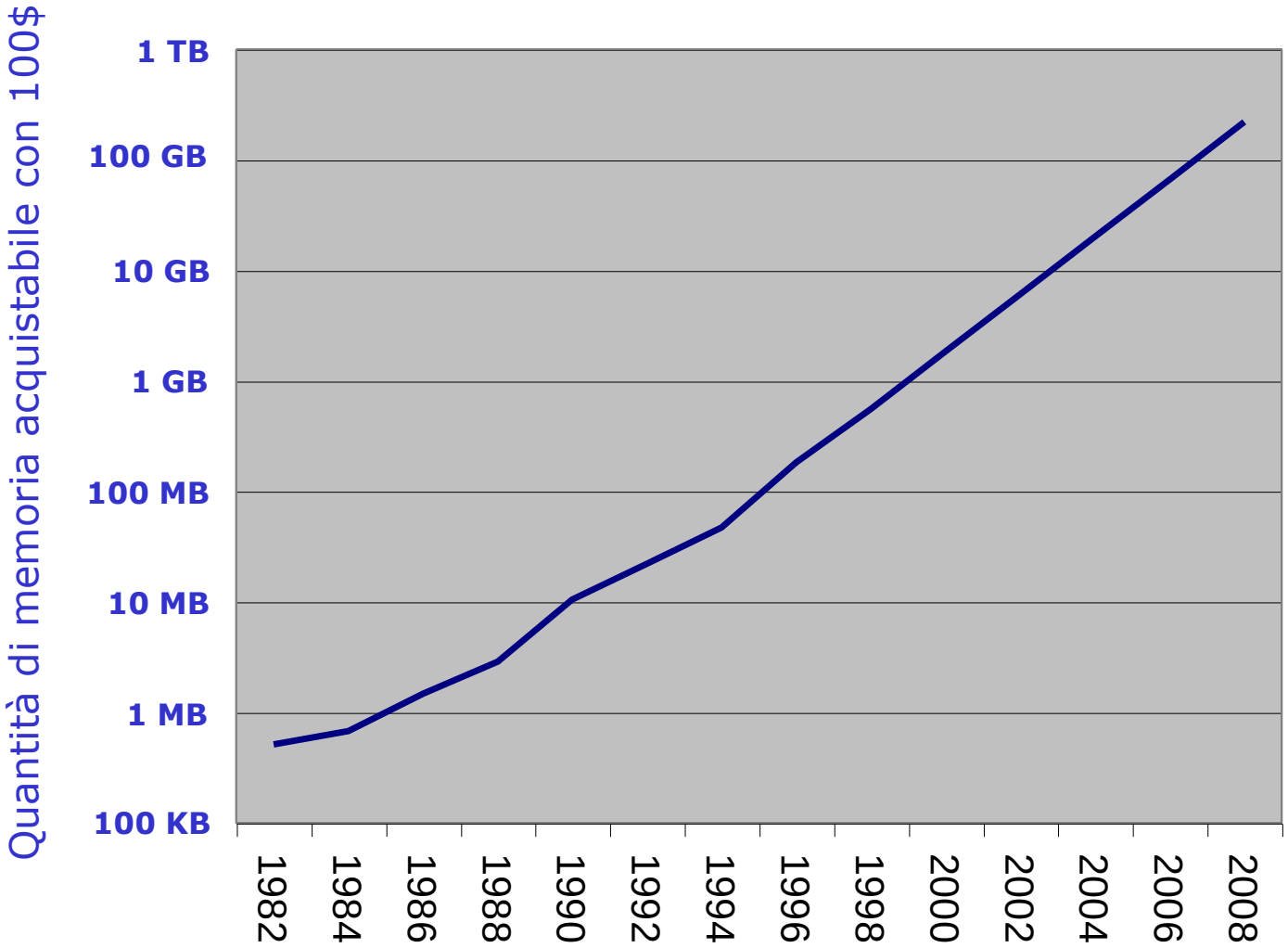
La verifica della firma al trascorrere del tempo

Tempo trascorso	Risultato verifica alla data		Note
	corrente	di firma	
Durante il periodo di validità del certificato di firma	**OK**	**OK**	
Dopo la scadenza del certificato	**Certificato non valido**	**OK**	**Alcuni prodotti determinano automaticamente la data di firma in presenza di marca temporale**
20 anni dopo l'emissione del certificato	**Certificato non valido**	**le liste di revoca non necessariamente sono disponibili**	**Le liste di revoca potrebbero essere comunque disponibili, anche per accordi con il certificatore**

Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- Gli strumenti del CAD nella Giustizia

La conservazione: il (non ancora) problema dello spazio su disco



La conservazione: i problemi della custodia e salvaguardia

- Mutevolezza delle tecnologie e dei formati
- Non provata affidabilità dei supporti di memorizzazione
- Immaterialità dei contenuti

ma

- Facilità di duplicazione (originali e copie sono indistinguibili)
- Protezioni crittografiche

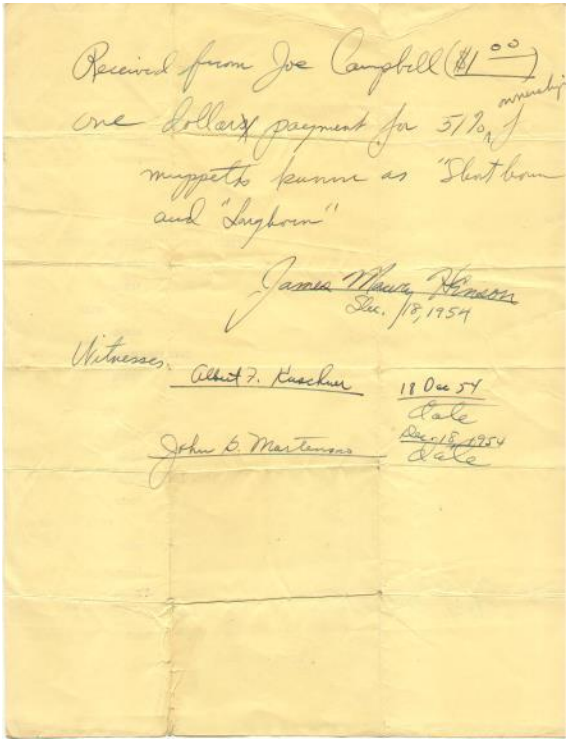
Criteri per la fruibilità nel tempo

- 3 possibili approcci
  - Mantenere software ed hardware originale
  - Scegliere regole (formati) **stabili**
  - Prodotti in grado di applicare le regole originali, anche se superate

- La fruibilità è favorita da
  1. **Semplicità**
  2. **Diffusione**
  3. Conoscibilità
  4. Standard

La fruibilità in caso di degrado della registrazione

- Con il passare del tempo i materiali su cui sono presenti le registrazioni tendono a rovinarsi (macchie, scoloriture, ecc.)
- Nelle forme documentarie tradizionali è possibile comunque recuperare (almeno in parte) i contenuti
- Anche nei documenti elettronici sono possibili recuperi, con un'efficacia che dipende dal formato utilizzato
- In presenza di crittografia o compressione le possibilità di recupero sono minime


Received from Joe Campbell ($1.00) one dollar payment for 5?% of royalty on puppetto known as "Short horn and "Long horn"

James Maury Henson
Dec. 18, 1954

Witnesses: Albert F. Kuschner 18 Dec 54 Date

John E. Martenson Dec 18 1954 Date

Deliberazione CNIPA n. 11/2004

- Snellisce il processo di conservazione degli originali informatici
- Consente la conservazione sostitutiva dei documenti analogici
- Stabilisce la distinzione tra documento analogico unico e non unico
- Consente l'utilizzo di qualsiasi supporto di memorizzazione
- Introduce la figura del Responsabile della conservazione

Conservazione digitale

- Documenti digitali:
  - La conservazione dei documenti informatici, termina con l'apposizione sull'insieme dei documenti del riferimento temporale e della firma digitale da parte del responsabile della conservazione
- Documenti analogici (conservazione sostitutiva):
  - Le immagini digitali dei documenti analogici devono essere memorizzate direttamente sui supporti
  - La conservazione delle immagini digitali dei documenti analogici avviene con la stessa procedura dei documenti digitali
  - Per i documenti analogici unici è necessaria l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale che attesti la conformità dell'operazione

L’interoperabilità dei prodotti di conservazione

- Le attuali norme sulla conservazione (CAD, Deliberazione CNIPA n. 11/2004) non forniscono indicazioni sulla struttura delle informazioni necessarie per la conservazione
- Il problema è stato affrontato dal progetto SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali) che ha avuto come obiettivo
  - la definizione di uno standard nazionale riguardante la struttura dell’insieme dei dati a supporto del processo di conservazione
  - la descrizione della struttura tramite il formalismo XML schema
- Il progetto ha dato origine allo standard UNI 11386:2010

Lo standard UNI 11386

- L'unità di conservazione è il Volume di Conservazione (VdC)
- Il VdC è composto da:
  - uno o più *file* ai quali si applica il processo di conservazione
  - l'Indice di Conservazione (IdC)
- L'IDC contiene un insieme di informazioni, strutturate secondo in uno Schema XML, tra cui
  - Il riferimento temporale
  - La firma digitale del soggetto che ha eseguito il processo di conservazione

Il profilo del responsabile della conservazione

- Una nuova figura professionale definita in base a:
  - Requisiti
  - Attività principali
  - Responsabilità principali
  - Capacità
  - Competenze
  - Un apposito tavolo tecnico interministeriale ha il compito di definirlo e di proporre un percorso formativo ed una adeguata collocazione nel pubblico impiego

Il profilo del responsabile della conservazione: responsabilità principali

- Garantisce la leggibilità dei documenti conservati nel tempo
- Ove previsto, appone sull'insieme dei documenti riferimento temporale e la firma digitale
- Nelle pubbliche amministrazioni svolge il ruolo di pubblico ufficiale
- Può delegare in tutto o in parte le proprie attività ad altri soggetti interni alla struttura
- Può affidare in tutto o in parte il processo di conservazione a soggetti terzi

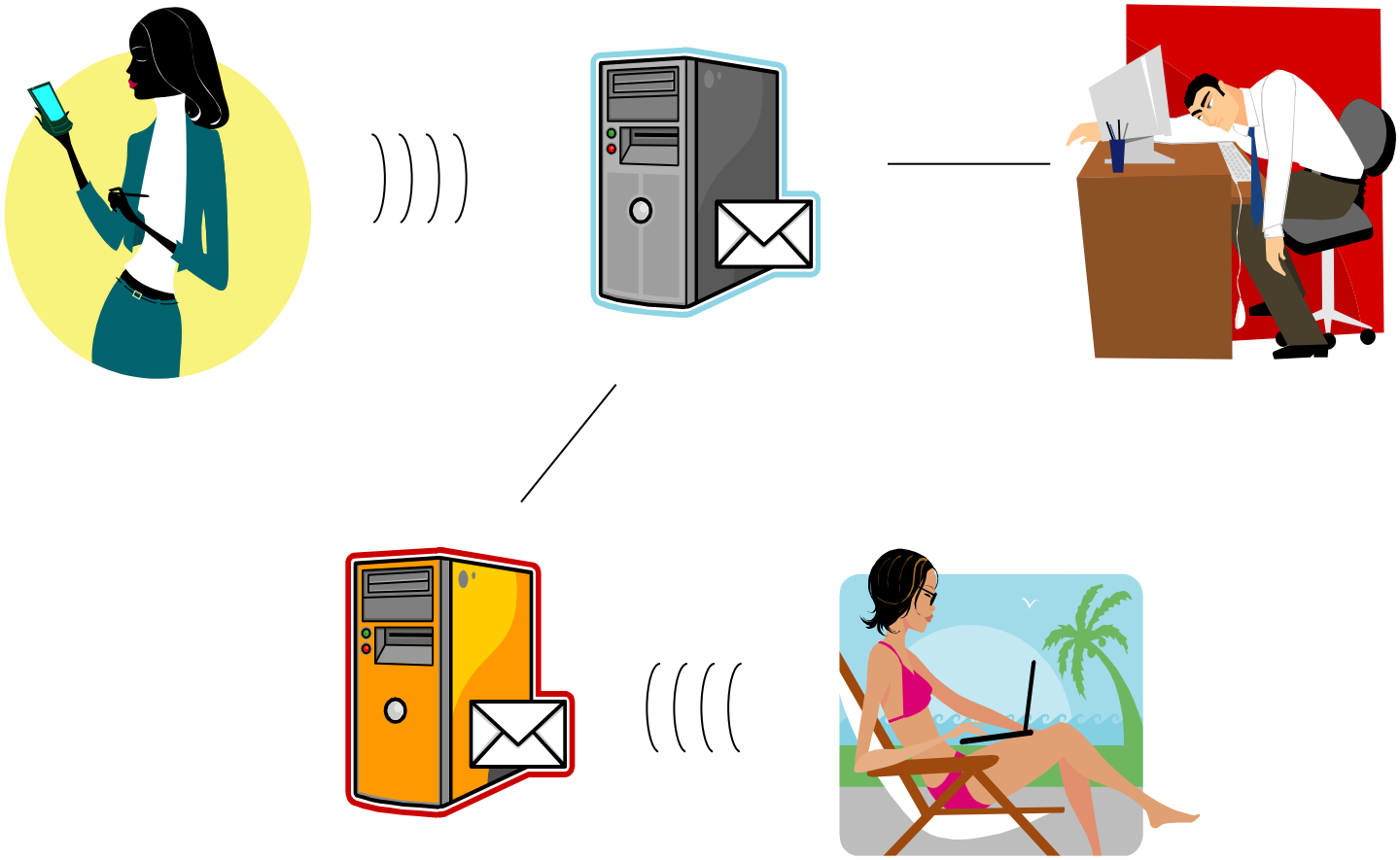
Il sistema di conservazione (art. 44 CAD)

- Il sistema di conservazione dei documenti informatici garantisce :
  - L'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento
  - L'integrità del documento
  - La leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari
  - Il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto

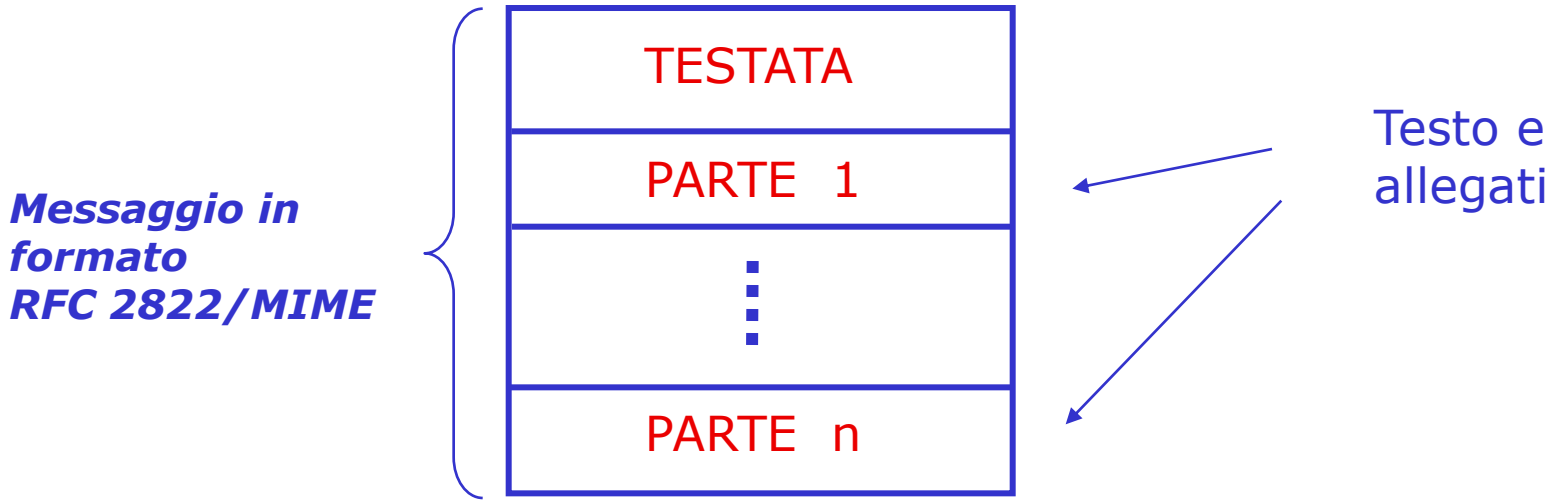
Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- Gli strumenti del CAD nella Giustizia

La posta elettronica



Il messaggio di e-mail



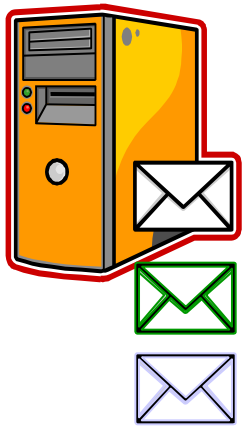
- Il formato MIME consente di spedire file in una grande varietà di formati
- Ciascuna parte può essere visualizzata contestualmente all'apertura del messaggio o come allegato
- Nella maggior parte dei messaggi di posta il corpo del messaggio corrisponde ad un file in formato html

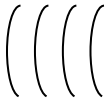
La posta elettronica certificata

Vengono automaticamente prodotte due tipologie di ricevute:

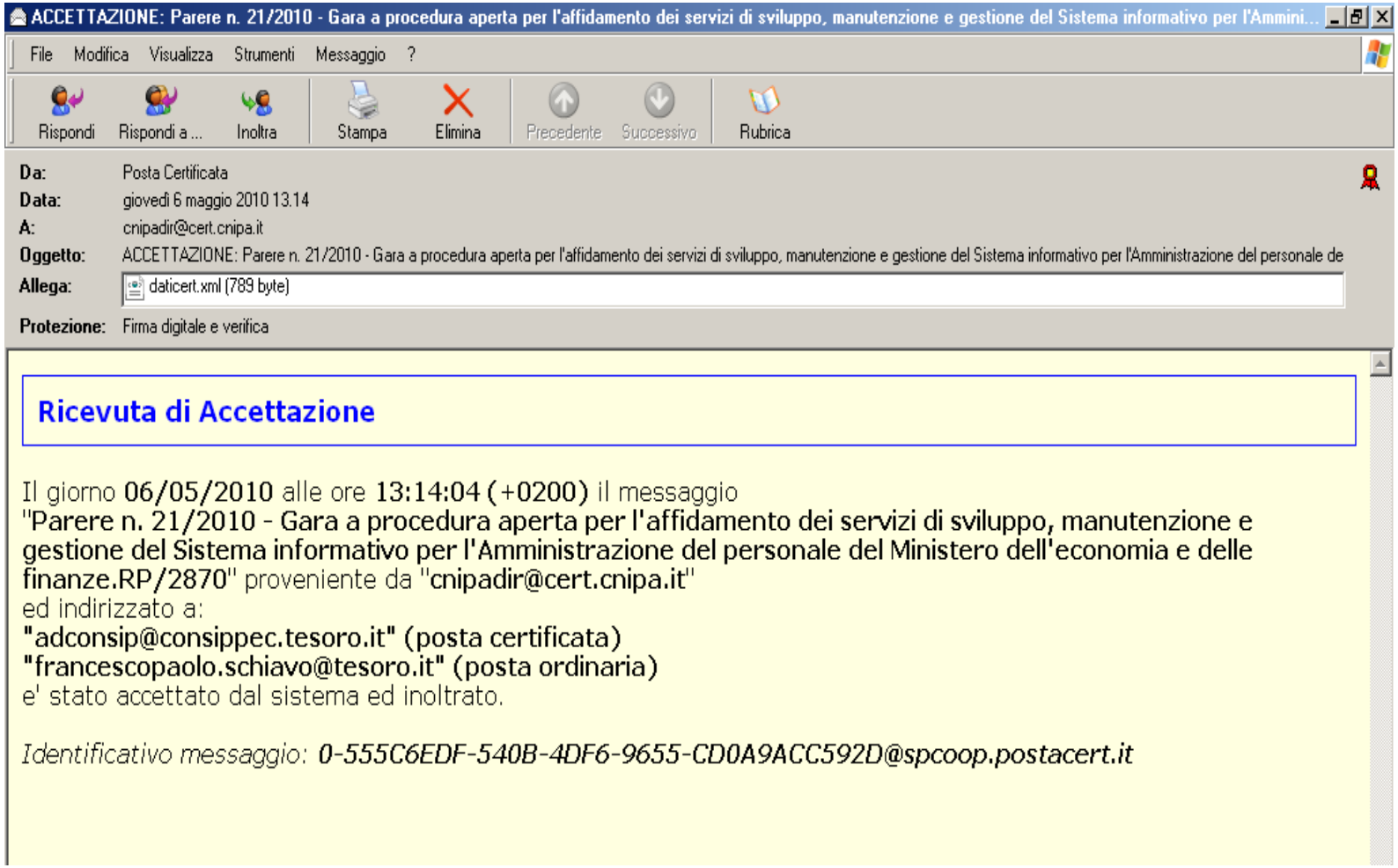
- accettazione
- avvenuta consegna

Le ricevute sono firmate elettronicamente

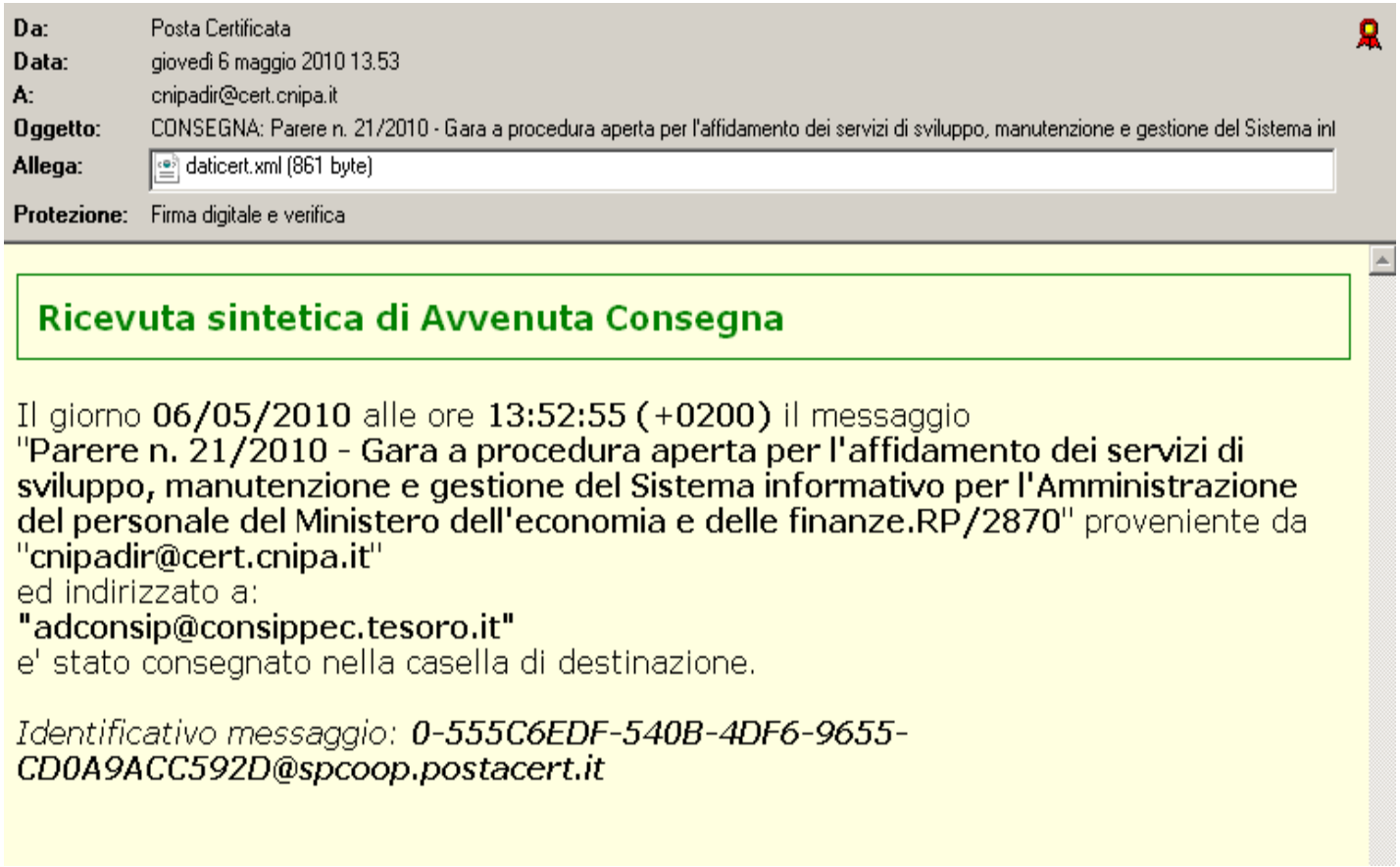




La ricevuta di accettazione



La ricevuta di avvenuta consegna



Da: Posta Certificata
Data: giovedì 6 maggio 2010 13.53
A: cnipadir@cert.cnipa.it
Oggetto: CONSEGNA: Parere n. 21/2010 - Gara a procedura aperta per l'affidamento dei servizi di sviluppo, manutenzione e gestione del Sistema inf
Allega: daticert.xml (861 byte)
Protezione: Firma digitale e verifica

Ricevuta sintetica di Avvenuta Consegna

Il giorno **06/05/2010** alle ore **13:52:55 (+0200)** il messaggio
"**Parere n. 21/2010 - Gara a procedura aperta per l'affidamento dei servizi di sviluppo, manutenzione e gestione del Sistema informativo per l'Amministrazione del personale del Ministero dell'economia e delle finanze.RP/2870**" proveniente da
"**cnipadir@cert.cnipa.it**"
ed indirizzato a:
"**adconsip@consippec.tesoro.it**"
e' stato consegnato nella casella di destinazione.

Identificativo messaggio: ***0-555C6EDF-540B-4DF6-9655-CD0A9ACC592D@spcoop.postacert.it***

L’allegato xml alla ricevuta

```
<?xml version="1.0" encoding="utf-8" ?>
<postacert tipo="avvenuta-consegna" errore="nessuno">
  <intestazione>
    <mittente>cnipadir@cert.cnipa.it</mittente>
    <destinatari tipo="certificato">adconsip@consippec.tesoro.it</destinatari>
    <destinatari tipo="esterno">francescopaolo.schiavo@tesoro.it</destinatari>
    <risposte>cnipadir@cert.cnipa.it</risposte>
     <oggetto>Parere n. 21/2010 - Gara a procedura aperta per l'affidamento dei servizi di sviluppo,
     manutenzione e gestione del Sistema informativo per l'Amministrazione del personale del Ministero
     dell'economia e delle finanze.RP/2870</oggetto>
  </intestazione>
  <dati>
    <gestore-emittente>EDS Italia S.p.A.</gestore-emittente>
    <data zona="+0200">
       <giorno>06/05/2010</giorno>
       <ora>13:52:55</ora>
       </data>
    <identificativo>0-555C6EDF-540B-4DF6-9655-
     CD0A9ACC592D@spcoop.postacert.it</identificativo>
    <msgid><27153453.1273144446975.JavaMail.oracle@pdpas202.speed.it></msgid>
    <ricevuta tipo="sintetica" />
    <consegna>adconsip@consippec.tesoro.it</consegna>
  </dati>
</postacert>
```

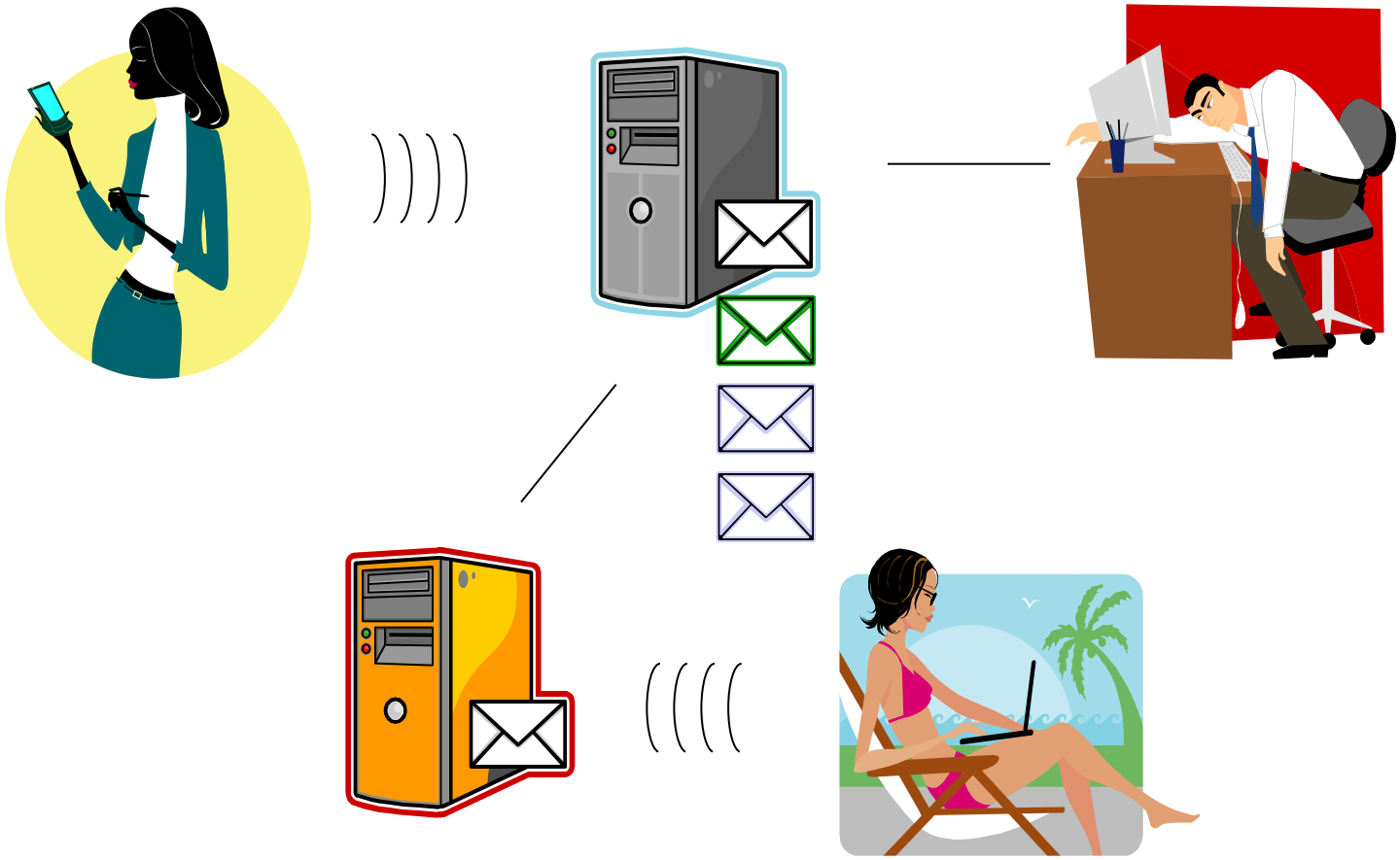
Tipologie di ricevute di avvenuta consegna

- Completa
  - riporta gli estremi del messaggio, il testo e gli allegati
- Breve
  - riporta gli estremi del messaggio e il testo
- Sintetica
  - riporta gli estremi del messaggio

I gestori PEC sono tenuti a mantenere per 30 mesi un registro dei messaggi (log) che riporta data e ora, mittente, destinatari e oggetto

Ogni messaggio è contraddistinto da un identificativo univoco che compare nella ricevuta e nel log

La PEC tra più soggetti



Il Progetto CEC-PAC

- Con il servizio di comunicazione elettronica certificata tra pubblica amministrazione e cittadino (denominato CEC-PAC) la PA fornisce al cittadino che la richiede una casella di posta elettronica certificata (PEC) e una serie di servizi accessori
- LA CEC-PAC garantisce un canale di comunicazione esclusivo tra PA e cittadini. Non sono previste e consentite comunicazioni al di fuori di tale canale chiuso ad es. tra cittadini e cittadini

… il Progetto CEC-PAC

- Ogni cittadino dotato di CEC-PAC potrà dialogare con PA da casa, o con qualsiasi dispositivo in grado di connettersi a internet, in modalità sicura e certificata.
- La comunicazione elettronica certificata tra PA e cittadino (CEC-PAC) è uno strumento di dialogo privilegiato tra cittadino e PA che:
  - fornisce tutte le garanzie di una posta elettronica certificata(PEC)
  - permette di dare a un messaggio di posta elettronica lo stesso valore di una raccomandata con ricevuta di ritorno tradizionale
  - garantisce provenienza e destinazione dei messaggi e i messaggi hanno validità legale

Confronto tra le comunicazioni "certificate"

	Raccomandata A.R.	PEC	CEC/PAC
Certezza mittente	NO - chiunque può spedire una raccomandata a nome di un altro	NO - chiunque può spedire una e-mail a nome di un altro	SI – l'utente viene identificato all'atto dell'assegnazione
Integrità del contenuto	SI - nella misura in cui si confida che il gestore non apra dolosamente la busta	SI - garantita da sistemi crittografici	SI - garantita da sistemi crittografici
Riservatezza del contenuto	SI - nella misura in cui si confida che il gestore non apra dolosamente la busta	SI - nella misura in cui si confida che il gestore non acceda dolosamente al server	SI - nella misura in cui si confida che il gestore non acceda dolosamente al server
Certezza della ricezione	Del soggetto che firma la ricevuta (non sempre coincidente con il destinatario)	Nella mailbox del destinatario	Nella mailbox del destinatario
Sottoscrizione contenuto	Firma tradizionale (può essere disconosciuta)	Firma digitale (non può essere disconosciuta)	Firma digitale, non necessaria per le istanze
Ripudiabilità del contenuto	SI - salvo invio senza busta	NO con servizio aggiuntivo a pagamento	NO con servizio aggiuntivo a pagamento
Gestore	Poste italiane	Gestori accreditati	Postecom

Campi di utilizzo

	Raccomandata A.R.	PEC	CEC/PAC
Cittadini	Cittadini non informatizzati	Comunicazioni di cui è opportuno avere una prova opponibile a terzi (es. transazioni finanziarie, applicazioni di e-commerce, ecc.)	Comunicazioni con la PA nell'ambito di procedimenti amministrativi. Può essere integrata con programmi che facilitano la redazione di istanze, opposizioni amministrative, ricorsi, denunce, ecc. Fornisce un riscontro immediato e consente di rimediare in tempo utile ad eventuali errori o vizi di forma.
Professionisti e imprese	Non consentita per comunicazioni con PA	Comunicazioni, integrate con i processi di business, di cui è opportuno avere una prova opponibile a terzi	Non consentita
Comunicazioni tra amministrazioni	La finanziaria 2008 ha imposto una riduzione del 50% Il CAD ne proibisce l'uso	Comunicazioni con la PA nell'ambito di procedimenti amministrativi. Può essere utilizzata per lo scambio di informazioni strutturate ed integrata con funzioni di cooperazione applicativa	Comunicazioni con la PA nell'ambito di procedimenti amministrativi. Può essere utilizzata per lo scambio di informazioni strutturate ed integrata con funzioni di cooperazione applicativa

L’indice delle Pubbliche Amministrazioni - IPA

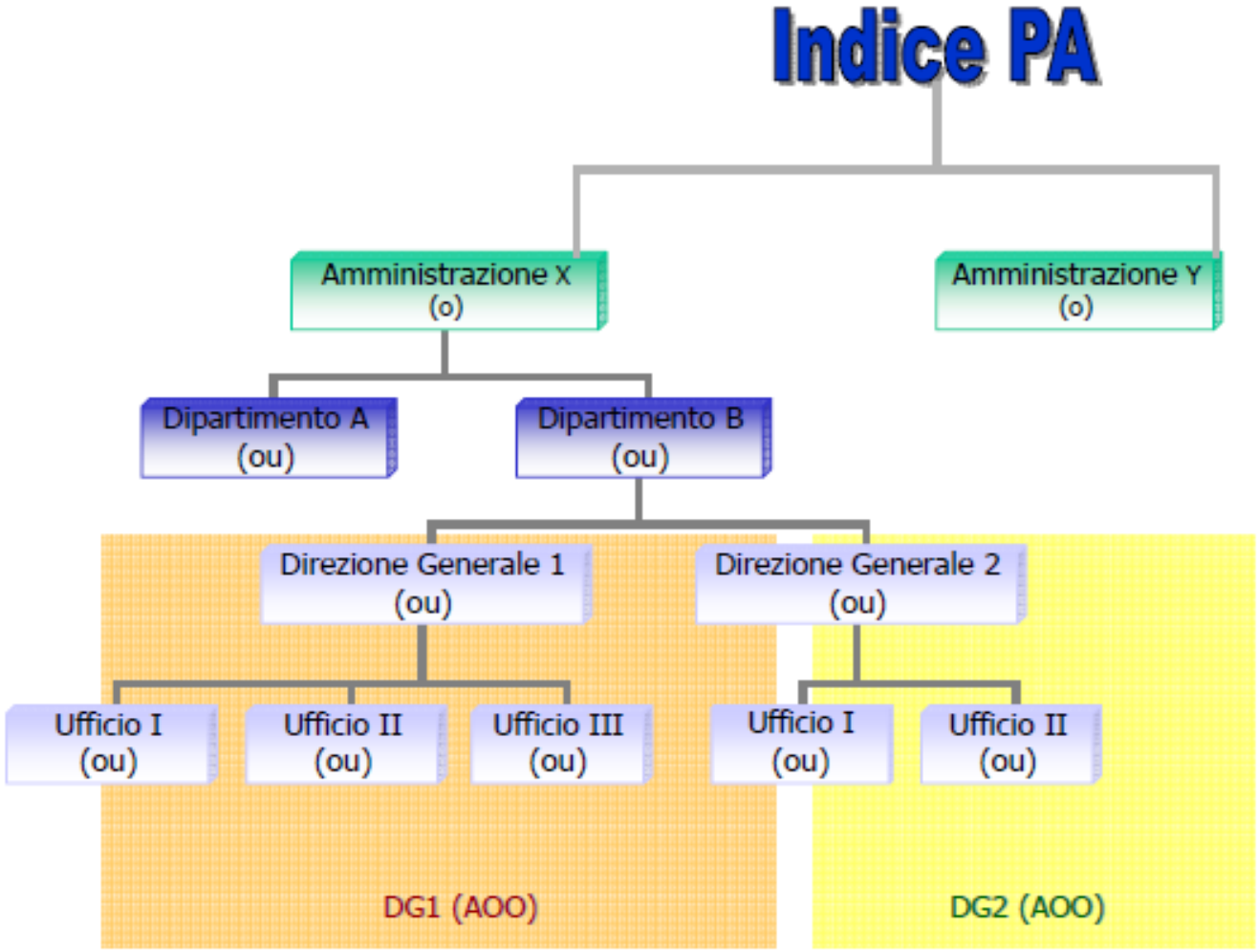
- Il sito dell'Indice della P.A. (IPA) rende agevole la ricerca di informazioni sulle PA e le avvicina sempre più al cittadino

- Attraverso l‘IPA ogni amministrazione espone la struttura dei propri uffici e l'elenco dei servizi offerti, con le informazioni per il loro utilizzo e gli indirizzi di posta elettronica da impiegare per comunicazioni e per lo scambio di documenti e informazioni, anche ufficiali e a valore legale

L’indice delle Pubbliche Amministrazioni - IPA

- Infrastruttura di directory pubblica per la PA
- Per ciascuna amministrazione accreditata le informazioni pubblicate:
  - elenco delle AOO con gli indirizzi delle relative caselle istituzionali (posta certificata)
  - elenco delle unità organizzative utenti di ciascuna AOO (protocollo informatico)
  - descrizione della struttura organizzativa in termini di Unità e di servizi erogati

IPA – La struttura



Art. 48 del CAD
Posta elettronica certificata.

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA
2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1

Le norme sulla PEC

- DECRETO DEL PRESIDENTE DELLA REPUBBLICA DPR 11 febbraio 2005, n. 68, “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.” (G.U. 28 aprile 2005, n. 97)
- DECRETO MINISTERIALE/REGOLE TECNICHE - Decreto Ministeriale 2 novembre 2005, “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata” (G.U. del 14 novembre 2005, n. 265)
- CIRCOLARE CNIPA (ACCREDITAMENTO) - Circolare CNIPA CR/49 24 novembre 2005, “Modalità per la presentazione delle domande di iscrizione all’elenco pubblico dei gestori di posta elettronica certificata” (G.U. 5 dicembre 2005, n. 283)
- CIRCOLARE CNIPA (VIGILANZA) - Circolare CNIPA CR/51 7 dicembre 2006, “Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell’elenco dei gestori di posta elettronica certificata (PEC) di cui all’articolo 14 del DPR 68/2005.

Contenuti del DPR

- Soggetti del servizio [art. 2]
- Garanzia per l'interoperabilità tra gestori [art. 5]
- Sicurezza della trasmissione [art. 11]
- Gestione dei virus [art. 12]
- Livelli minimi di servizio [art. 13]
- Requisiti relativi ai gestori [art. 14]
- Assegnazione al CNIPA delle funzioni di vigilanza e controllo sulle attività dei gestori [art. 14]
- Disposizioni per le pubbliche amministrazioni [art. 16]

Contenuti del DM

- Certificati di firma e di accesso all'indice dei gestori rilasciati dal CNIPA [art. 7/18]
- Criteri per la conservazione dei log dei messaggi [art. 10]
- Livelli di servizio: disponibilità del 99,8% riferita ad un quadrimestre [art. 12]
- Modalità di gestione dell'avviso di mancata consegna [art.13]
- Elenco pubblico dei gestori [art. 18]
- Certificazione ISO 9001:2000 [art. 20]
- Definizione dei requisiti organizzativi dei gestori [art.21/22/23]
- Allegato recante "Regole tecniche"

Obblighi per professionisti e imprese

- Le imprese devono comunicare alla camera di commercio di competenza il proprio indirizzo di posta elettronica certificata?
  Il decreto legge n. 185 del 29 novembre 2008, pubblicata sulla GU n. 280 del 29 novembre 2008, S.O. n. 263 convertito nella legge n. 2/2009, prevede che le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese.
  Le imprese già costituite in forma societaria alla medesima data di entrata in vigore del succitato decreto, hanno l'obbligo di comunicare al registro delle imprese l'indirizzo di posta elettronica certificata entro tre anni (29/11/2011) dalla data di entrata in vigore del succitato decreto.
- I professionisti devono comunicare ai rispettivi ordini di appartenenza il proprio indirizzo di posta elettronica certificata?
  Il decreto legge n. 185 del 29 novembre 2008, pubblicata sulla GU n. 280 del 29 novembre 2008, S.O. n. 263 convertito nella legge n. 2/2009 prevede che i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata entro un anno (29/11/2009) dalla data di entrata in vigore del succitato decreto.

Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- Gli strumenti del CAD nella Giustizia

Il protocollo informatico

Linee generali:

- L'adozione del protocollo informatico comporta la "totale automazione delle fasi di produzione, gestione, diffusione e utilizzazione dei propri dati, documenti, procedimenti e atti", art. 51, comma 2, dPR 445/00.
- Data di riferimento (art.50 comma 3) 1° gennaio 2004
- Il sistema di protocollo informatico non è la riproduzione informatizzata del registro cartaceo, ma un insieme integrato e coordinato di azioni relative alla produzione, gestione e conservazione dei documenti cartacei e informatici di un ente pubblico.

Il “nucleo minimo” del sistema di gestione informatica dei documenti

- registrazione di protocollo;
  - data e numero progressivo annuale automatico e non modificabile,
  - mittente/destinatario registrati non modificabili;
  - oggetto, non modificabile;
  - impronta;
  - altri elementi.
- segnatura di protocollo;
  - risponde a una funzione di certezza giuridica;
  - consente di individuare ciascun documento in modo inequivocabile;
  - apposizione o associazione all’originale in forma permanente e non modificabile delle informazioni riguardanti il documento, di cui obbligatorie: amministrazione, data e numero di protocollo.
- classificazione/fascicolazione.
  - si effettua nei confronti di tutti i documenti correnti, protocollati e non, a prescindere dal loro stato di trasmissione, (spediti, ricevuti o interni), e dal supporto utilizzato, secondo un piano coerente che definisca la posizione di ciascun documento all’interno dell’archivio in formazione.

Classificazione

- La classificazione è un'attività fondamentale per la gestione dei documenti in una pubblica amministrazione e la sua obbligatorietà è riaffermata dal Dpr n.445/2000 artt. 50 e 56.
- Lo strumento di cui avvalersi per organizzare e classificare i documenti è il titolario.
- Tutte le attività svolte da una PA viene rappresentata con un documento
- L'Archivio è il luogo in cui si conservano tutti i documenti prodotti nelle attività istituzionale di una organizzazione
- i documenti archiviati hanno valore probatorio e con essi anche tutti i collegamenti tra di essi attraverso l'attività di classificazione e la creazione di fascicoli.

Fascicolazione

- Assegnazione di un documento a una definitiva unità archivistica generalmente indicata con il termine fascicolo.

- La definizione dell'unità archivistica di riferimento, cioè il fascicolo, deve avvenire al momento della formazione del documento o dell'acquisizione ufficiale di oggetti documentari nel sistema archivistico di un soggetto.

Il sistema di gestione dei flussi documentali

Prevede:

- gestione automatizzate dei procedimenti amministrativi
- progressiva reingegnerizzazione dei processi amministrativi

Consente:

- rapida acquisizione delle informazioni relative a: fascicolo, procedimento, responsabile, gestione fasi procedimento, informazioni singolo procedimento, informazioni statistiche, ecc.

Informazioni strutturate previste

- parte comune a tutte le amministrazioni
  - Informazioni minime obbligatorie
    - codice dell'Amministrazione;
    - codice dell'area organizzativa omogenea;
    - data di protocollo;
    - progressivo di protocollo
    - l'oggetto;
  - Informazioni opzionali
    - indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento
    - indice di classificazione;
    - identificazione degli allegati;
    - informazioni sul procedimento e sul trattamento.
- parti specifiche definite dalle amministrazioni
  - Informazioni specifiche su particolari procedimenti
    - esempio: scheda preliminare su richieste di parere al DIgitPA

Il responsabile del protocollo

- ART 61 DPR 445/2000
  - dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione ad hoc
- ART 4 DPCM 31/10/2000
  - predisporre lo schema del manuale di gestione del protocollo che deve essere adottato dalle pubbliche amministrazioni (il Cnipa ha predisposto lo schema di riferimento)
  - proporre i tempi, le modalità e le misure organizzative e tecniche per l'adeguamento
  - predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il responsabile dei sistemi informativi automatizzati e con il responsabile della sicurezza dei dati personali.

Il manuale di gestione

(art. 3, comma c del DPCM 31 ottobre 2000)

- Ambito di applicazione e definizioni
- Tipologie documentarie (trasmissione e trattamento)
- Descrizione dei flussi documentari (acquisizione, assegnazione, spedizione, circolazione)
- Modalità di registrazione e segnatura
- Organizzazione dell'archivio corrente (classificazione/fascicolazione, formazione serie, relazione flussi amministrativi) e di deposito
- Regole di selezione, trasferimento, versamento, conservazione
- Sicurezza (accesso, privacy, protocollo emergenza)
- Funzioni di interoperabilità
- Utilizzo, comunicazione
- Aggiornamento

… il manuale di gestione

- Riconoscimento della piena autonomia delle amministrazioni nella definizione dei propri criteri organizzativi e regolamentari che però non esclude la necessità di una struttura comune degli strumenti regolamentari che includono

… il manuale di gestione

- Descrive il sistema di gestione e di conservazione dei documenti
- Fornisce le istruzioni per il corretto funzionamento del Servizio
- È reso pubblico dalle amministrazioni secondo le modalità previste dai singoli ordinamenti

… il manuale di gestione

- Indicazione delle unità organizzative responsabili delle attività di registrazione, di organizzazione e tenuta dei documenti all'interno
- Utilizzazione degli strumenti informatici per lo scambio dei documenti all'interno e all'esterno dell'area organizzativa omogenea
- Criteri e modalità per il rilascio delle abilitazioni di accesso interno ed esterno
- Descrizione del flusso di lavorazione dei documenti ricevuti, spediti, interni
- Regole di smistamento e di assegnazione dei documenti ricevuti

… il manuale di gestione

- Regole di registrazione per documenti pervenuti secondo particolari modalità di trasmissione
  - Documenti informatici non attraverso posta elettronica
  - Fax
  - raccomandata assicurata
- Elenco dei documenti soggetti a registrazione particolare e relative modalità di trattamento
- Pianificazione e modalità per l'eliminazione dei protocolli particolari
- Utilizzo del registro di emergenza

… il manuale di gestione

- Descrizione del sistema di classificazione con l'indicazione delle modalità di aggiornamento
- Integrazione dello schema di classificazione con le informazioni relative ai tempi, ai criteri ed alle regole di selezione e conservazione anche con riferimento all'uso di supporti sostitutivi
- Descrizione funzionale ed operativa del protocollo informatico
- Modalità di produzione e conservazione delle registrazioni di protocollo informatico
- Soluzioni tecnologiche per garantire
  - la non modificabilità
  - La contemporaneità dell'operazione di segnatura
  - Registrazioni delle informazioni annullate o modificate

Canali di trasmissione

- In generale, la posta elettronica è da considerarsi il canale privilegiato per lo scambio di documenti con l'esterno
- Si ricorda che per le amministrazioni pubbliche è obbligatorio accettare i documenti trasmessi via posta elettronica (sia certificata che semplice)
- E' altresì opportuno accettare documenti registrati su memorie portatili di tipo CD o DVD e trasmessi mediante posta ordinaria (i *floppy disk* possono essere considerati obsoleti e pertanto rifiutati)
- Una ulteriore possibilità è fornita dalle funzioni di "caricamento" dei documenti (*upload*) dei siti web: tale modalità deve essere utilizzata quando il documento è parte di un processo che viene svolto attraverso un'applicazione di tipo web

PEC e posta semplice

- Nei casi di richieste inviate via PEC l'Amministrazione è tenuta a prendere in considerazione le medesime alla stessa stregua di quanto avviene per le richieste inviate con lettera convenzionale, attivando un procedimento amministrativo quando previsto dall'ordinamento
- Nei casi di mail semplice l'Amministrazione può decidere discrezionalmente quale seguito dare al messaggio:
  - nessuno se il messaggio è considerato irrilevante o spam
  - una risposta informale (ad esempio per rinviare ad un ufficio competente)
  - l'avvio di un procedimento (in tal caso il destinatario del messaggio avrà cura di inoltrarlo al protocollo perché possa confluire nel sistema di gestione documentale)

Controllo delle sottoscrizioni

- È consigliabile effettuare all'atto dell'inserimento nell'archivio il controllo delle sottoscrizioni e delle validazioni temporali, ciò consente di verificare sia l'autenticità che l'integrità del documento nella forma in cui esso è stato ricevuto. Gli effetti di tale controllo, grazie al principio di ininterrotta custodia, mantengono la loro validità per tutta la vita del documento
- E' consigliabile verificare anche eventuali qualifiche e vincoli d'uso della sottoscrizione
- In corrispondenza al controllo della sottoscrizione è opportuno generare i metadati che ne attestano l'esito ed i dettagli

Modalità di rifiuto

- Nel caso il documento non superi i controlli elencati, è necessario decidere se accettare o meno il documento
- La decisione dovrebbe essere presa dal responsabile del protocollo, di concerto con il responsabile dell'archivio informatico che dovrà valutare se il documento sia gestibile, pur non superando i controlli elencati
- In caso di rifiuto dovrebbe essere fornita al mittente un'adeguata informativa che riporti le motivazioni della mancata accettazione
- Il documento contenente le motivazioni dovrebbe essere trasmesso con lo stesso canale utilizzato dal mittente

Sistema Pubblico di connettività

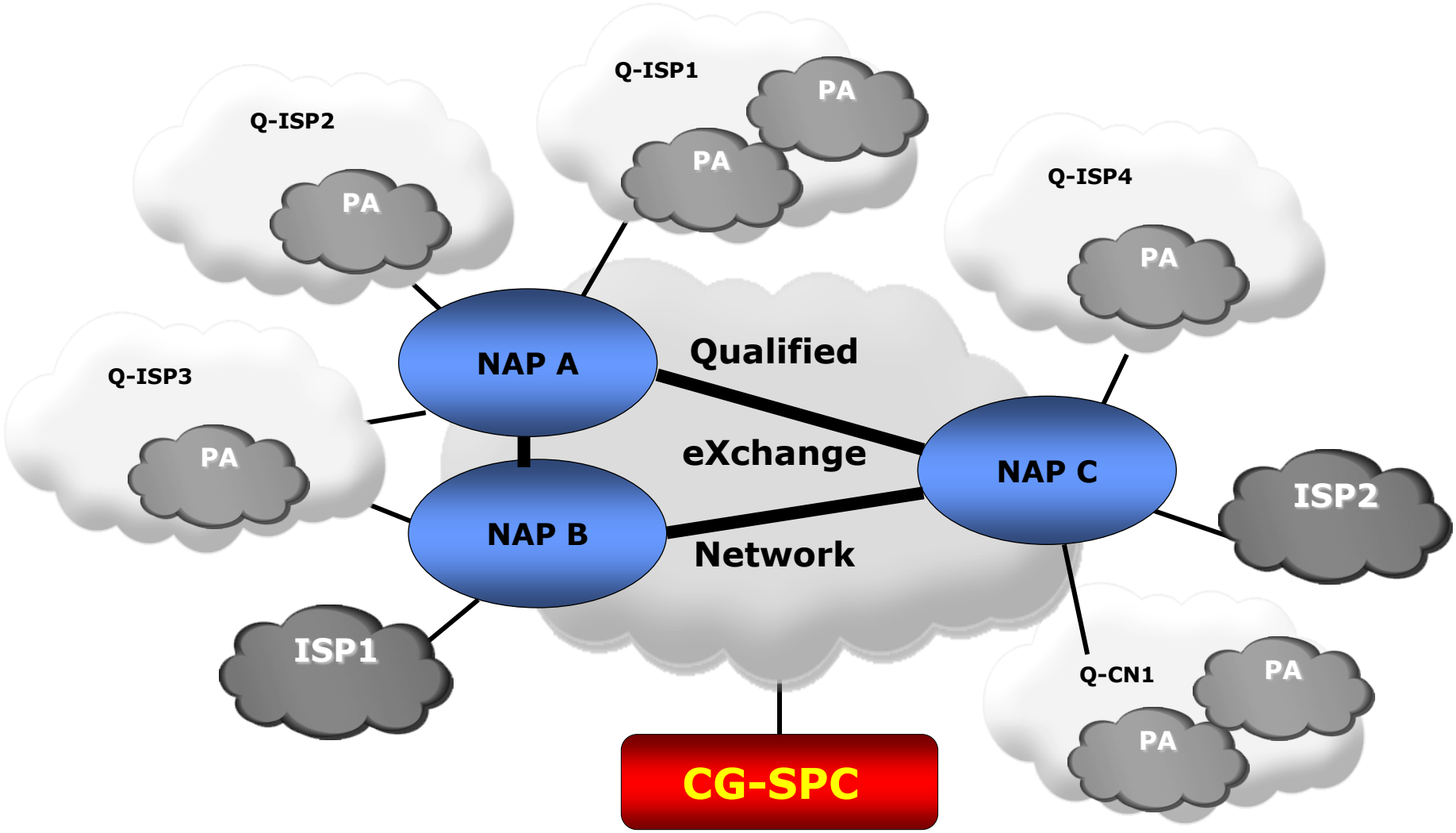
- Il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, con le seguenti finalità:
  - fornire un insieme di servizi di connettività sicura condivisi dalle pubbliche amministrazioni interconnesse
  - garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet, nonché con le reti di altri enti
  - fornire un'infrastruttura sicura di scambio e servizi di connettività e cooperazione alle pubbliche amministrazioni che ne facciano richiesta
  - realizzare un modello di fornitura di servizi multifornitore
  - salvaguardare la sicurezza dei dati e la riservatezza delle informazioni **(CAD, artt.73 e 77)**

SPC multifornitore

Il Sistema multifornitore comprende:

- Servizi di trasporto
- Servizi di supporto (indirizzamento, gestione indirizzi pubblici ,domain name service)
- VoIP
- Interoperabilità di base : posta elettronica, trasporto di protocolli proprietari e web hosting/housing/mirroring
- Manutenzione ed assistenza
- Servizi di sicurezza

Infrastruttura di comunicazione multifornitore



Servizi di hosting e gestione

Hosting

- Realizzazione di siti web
- Servizi di redazione per siti web
- Adattamento delle applicazioni in modalità web
- Hosting di siti web

Gestione

- lan
- postazioni di lavoro
- server
- applicazioni

Supporto

- Help desk
- Risorse professionali
- Formazione

Servizi di interoperabilità evoluti e cooperazione applicativa

Messaggistica	▪ Posta elettronica (esclusiva, certificata) ▪ Archiving ▪ Unified messaging
Cooperazione applicativa	▪ Porta di dominio ▪ Integrazione applicativa ▪ Composizione e coordinamento di servizi
Sicurezza applicativa	▪ Identity & Access management ▪ Firewall applicativo
Supporto	▪ Risorse professionali, help desk, formazione

Infrastruttura nazionale per la cooperazione applicativa

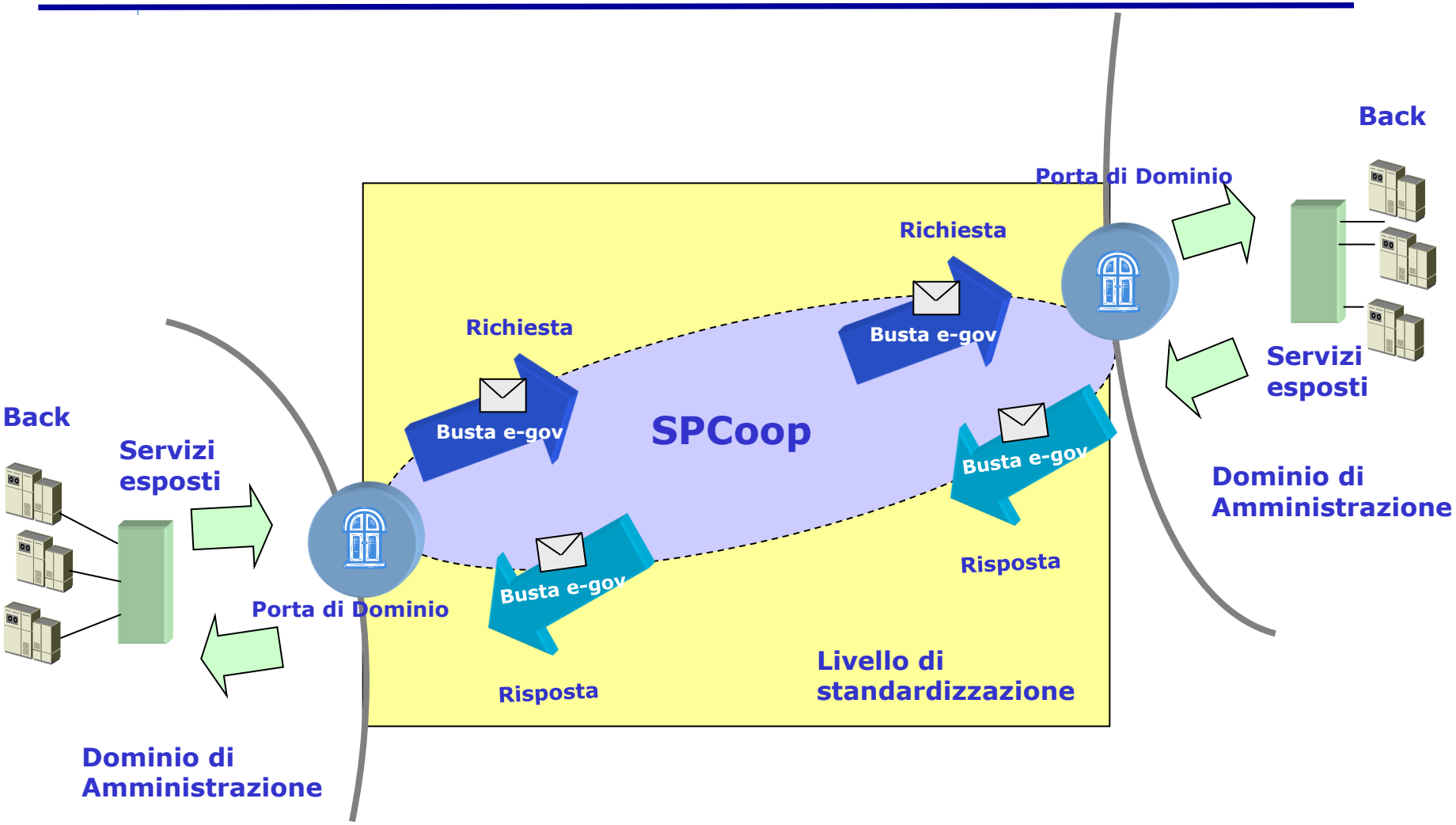
Servizi di infrastruttura (SICA)

- Registro di servizi (**comprende Indice PA**)
- Catalogo di schemi/ontologie
- Gestione delle identità federate
- Indice dei soggetti (**comprende Rubrica PA**)
- Servizi di certificazione (rilascio e gestione dei certificati SpCoop)
- Servizi di monitoraggio, gestione e sicurezza interna

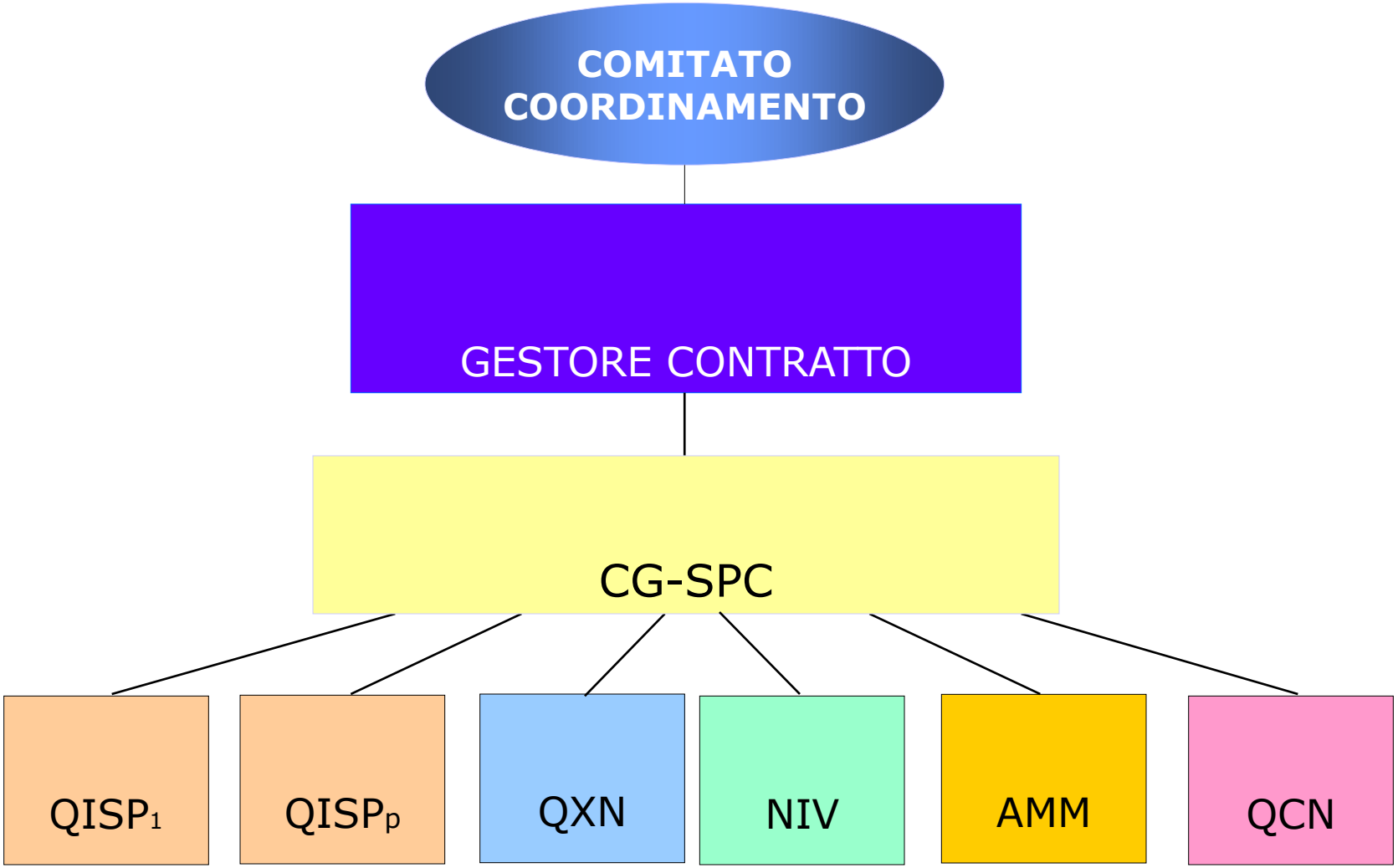
Qualificazione

- Porta di dominio campione
- Qualificazione SICA secondari

La cooperazione



La gestione di SPC



Il modello italiano per la gestione dell'identità

- Un sistema istituzionale affidabile per l'identificazione in rete

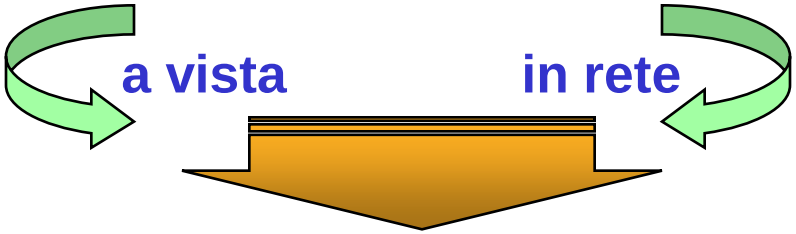
  Carta d'Identità elettronica (CIE) e
  Carta Nazionale dei Servizi (CNS)

- Un insieme di regole per la cooperazione applicativa

  Sistema Pubblico di Connettività (SPC)

CIE - la scelta architetturale

tipologie di identificazione



scelta progettuale

microprocessore

consente il riconoscimento in rete e la fruizione dei servizi

banda ottica a lettura laser - worm

consente la non contraffazione del documento per il riconoscimento *a vista* del titolare

tutte le informazioni contenute nei supporti elettronici sono certificate da un bollo elettronico emesso dal M.I. e dal Comune all'atto dell'emissione della carta

La Carta d'Identità Elettronica (CIE)

- La CIE è una carta ibrida composta da due differenti tecnologie: un circuito elettronico e una banda ottica
- Sulla parte anteriore della carta, nella parte superiore ci sono la foto e i dati personali del titolare. Nella parte inferiore, la cosiddetta ICAO MRZ (International Civil Aviation Organization - Machine Readable Zone) che consente la lettura automatica degli stessi dati, codificati su tre righe e stampati in OCRB (secondo le disposizioni ICAO)
- Sul retro della carta, oltre ad altri dati personali, sono installati il circuito elettronico, la banda ottica e un ologramma di sicurezza
- Il circuito elettronico ha una capacità di almeno 32k ed è conforme agli standard ISO della famiglia 7816

La Carta Nazionale dei Servizi (CNS)

- "il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni"
- "la carta nazionale dei servizi, in attesa della carta d'identità elettronica, è emessa dalle pubbliche amministrazioni interessate al fine di anticiparne le funzioni di accesso ai servizi in rete delle pubbliche amministrazioni"
- "l'onere economico di produzione e rilascio delle carte nazionali dei servizi è a carico delle singole amministrazioni che le emettono"

La Carta Nazionale dei Servizi

- La CNS, contrariamente alla Carta d'Identità Elettronica (CIE), non è un documento per l'identificazione "a vista"

- E' uno strumento di autenticazione in rete: consente l'accesso ai servizi resi disponibili per via telematica dalle PP.AA.

… la Carta Nazionale dei Servizi

- La CNS può contenere le informazioni necessarie per apporre firme digitali
- La CNS può contenere quindi quanto necessario per accedere ai servizi in rete (autenticazione) e sottoscrivere istanze, dichiarazioni, documenti (firma digitale)

L’integrazione della CIE/CNS con la Firma Digitale

- Carta Identità Elettronica e Carta Nazionale Servizi
  - Strumenti di identificazione e di autenticazione in rete
- Firma Digitale
  - Consente di sottoscrivere una dichiarazione, atto, istanza, o qualunque atto o fatto rappresentato in una evidenza informatica

… il quadro normativo di riferimento

- La CNS non identifica a vista
- La CNS deve contenere un certificato di autenticazione rilasciato da un certificatore accreditato
- I dati identificativi della CNS sono verificati tramite il sistema informativo del Centro Nazionale per i Servizi Demografici del Ministero dell'Interno.

… il quadro normativo di riferimento

- "La carta può contenere eventuali informazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione di servizi al cittadino, cui si può accedere tramite la carta…"
- La CNS ha una validità temporale non superiore ai sei anni.
- "Tutte le pubbliche amministrazioni che erogano servizi in rete devono consentire l'accesso ai servizi medesimi da parte dei titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio".
- Attraverso opportuni protocolli d'intesa tra le PA, le banche e le poste, è possibile utilizzare la CNS per funzioni di pagamento tra privati e PA.

Altre carte istituzionali

- Dal Codice dell'Amministrazione Digitale
  - "Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni" (art. 66, comma 8)

Interoperabilità delle smart card

- Basata sul protocollo d'intesa 13 maggio 2003 tra il Ministero dell'Interno, il Ministro per l'Innovazione e le tecnologie e 11 produttori di sistemi operativi per smart card
- Le specifiche tecniche risultanti dal protocollo d'intesa sono disponibili sul sito dell'Agenzia per l'Italia digitale
- Sullo stesso sito Internet sono disponibili le altre specifiche tecniche concordate con i sottoscrittori del protocollo d'intesa
- I sistemi operativi sostanzialmente hanno gli stessi comandi (APDU)

Sommario

- Il documento informatico
- La sottoscrizione del documento informatico
- La conservazione dei documenti informatici
- La PEC
- Altri strumenti regolamentati nel CAD
- Gli strumenti del CAD nella Giustizia

Documento informatico

Nel civile:

- Dattiloscritto informatico – Ms Office, PCT, Consolle del magistrato o MagOffice
- Copia di immagine mediante scanner – PCT, Sicid
- Documento XML – PCT, Sicid
- Registrazione informatica PCT, Sicid

Nel penale:

- Dattiloscritto informatico – Ms Office
- Copia di immagine mediante scanner – Digit, Tiap, Sidip, Aurora
- Registrazione informatica – Rege, SICP

PEC

- L’uso della PEC è obbligatorio per tutte le comunicazioni nell’ambito del processo civile e penale (biglietti di cancelleria e notifiche), unica eccezione sono le notifiche nei confronti di cittadini che potrebbero non disporre di una casella di PEC
- Oggi si è in una fase di transizione in cui l’uso della PEC è ancora limitato
- Nel civile la comunicazione non può avvenire in formato libero, ma deve seguire precisi standard
- Alcuni prodotti (punto d’accesso, Sicid) si fanno carica di costruire opportunamente il messaggio e di gestire la comunicazione via PEC

Firma digitale

Nel civile:

- Depositi telematici - PCT

Nel penale:

- Notifiche telematiche – SNT

Per la firma vengono usate

- Carte firma
- Carte mod. AT elettronico - CMG

Per maggiori informazioni

gianfranco.pontevolpe@giustizia.it