Prof. Stefano Pigliapoco

DOCUMENTO INFORMATICO, POSTA ELETTRONICA CERTIFICATA E DEMATERIALIZZAZIONE

s.pigliapoco@unimc.it

La società dell’informazione e della conoscenza

- La digitalizzazione delle comunicazioni, dei documenti, dei processi e dei servizi in genere, è il fenomeno che più di ogni altro caratterizza la società contemporanea
  - Internet conta oggi circa 1 miliardo di utenti
  - Via Internet e rete satellitare transitano ogni giorno non meno di 1 Terabyte di dati digitali
  - Il volume delle e-mail cresce in media del 30-40% ogni anno.

Acquisizione documenti

Stampa/ Produzione documenti

- 115 miliardi di pagine stampate, di cui 19,5 miliardi inutilizzate

Costo: 287 milioni di euro all'anno

Distribuzione documenti

- Ogni documento viene duplicato da 9 a 11 volte => costo: 18 euro per documento

Archiviazione documenti

- 1 documento perduto su 20
- 3% dei documenti archiviati erroneamente
- Costo per recuperare un documento non archiviato correttamente: 120 euro

40%:
Percentuale media del tempo di ogni impiegato speso in attività di gestione documentale

Fonte: Elaborazioni NetConsulting su fonti ISTAT, 2006

Codice dell’amministrazione digitale

- Il codice dell’amministrazione digitale (Co.A.Di.), contenuto nel D. Lgs. 7 marzo 2005, n. 82, entrato in vigore il 1 gennaio 2006 e modificato con D. Lgs. 4 aprile 2006, n. 159, riconosce ai cittadini e alle imprese alcuni diritti fondamentali:
  - [art. 3, c. 1]: il diritto di richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni e con i gestori di pubblici servizi statali. Tale principio si applica alle amministrazioni regionali e locali nei limiti delle risorse tecnologiche e organizzative e nel rispetto dell’autonomia normativa. Le controversie sono devolute alla giurisdizione esclusiva del giudice amministrativo

Codice dell’amministrazione digitale

- [art. 4, c. 2]: ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie della informazione e della comunicazione
- [art. 47]: Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

Piano di e-government 2012

- Il piano di e-government 2012 è un piano da realizzare entro il 2012, composto da 27 obiettivi organizzati in quattro ambiti di intervento prioritari.
  - **Scuola.** Interazione digitale scuola – famiglia; pagella elettronica e registro elettronico; strumenti innovativi per la didattica digitale
  - **Università.** Università digitale (semplificazione e digitalizzazione dell’azione amministrativa; servizi on line agli studenti)

Piano di e-government 2012

- **Salute.** Digitalizzazione del ciclo delle prescrizioni e dei certificati medici; Fascicolo sanitario elettronico
- **Giustizia**. Notificazione telematiche delle comunicazioni e degli atti processuali; certificati giudiziari *on line*
- **Carte dei servizi**. Integrazione tessera sanitaria e carta regionale dei servizi

Piano di e-government 2012

- **Dematerializzazione**. Casella elettronica certificata per i cittadini, le amministrazioni pubbliche, le imprese e i professionisti; fatturazione elettronica verso la pubblica amministrazione; pagamenti *on line* verso la pubblica amministrazione; DURC *on line;* attuazione del codice dell'amministrazione digitale; gestione documentale elettronica
- **Sistema Pubblico di Connettività (SPC).**

Codice dell’amministrazione digitale

- L. 18 giugno 2009, n. 69.
  - Il Governo è delegato a modificare, entro il 2010, il codice dell’amministrazione digitale per prevedere forme sanzionatorie, semplificare la normativa sulla firma digitale, prevedere l’obbligo dell’utilizzo delle reti informatiche nelle comunicazioni tra pubbliche amministrazioni e tra queste e i loro dipendenti.

Fatturazione elettronica verso la PA

- L’art. 1, c. 209-214, della L. n. 244/2007, ha stabilito che l’emissione, la trasmissione, l’archiviazione e la conservazione delle fatture emesse nei rapporti con le Amministrazioni dello Stato e con gli enti pubblici nazionali, deve essere effettuata esclusivamente in forma elettronica.
- Dopo la pubblicazione del regolamento del MEF, atteso ormai da mesi, le Amministrazioni non potranno più accettare né pagare fatture emesse su supporto cartaceo.

Albo on line

- Art. 32, Legge 18 giugno 2009, n. 69
  - A far data dal 1 gennaio 2010, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei propri siti informatici da parte delle amministrazioni e degli enti pubblici obbligati.

Albo on line

- Art. 32, Legge 18 giugno 2009, n. 69
  - Dalla stessa data del 1gennaio 2010, (…), le amministrazioni e gli enti pubblici tenuti a pubblicare sulla stampa quotidiana atti e provvedimenti concernenti procedure ad evidenza pubblica o i propri bilanci, oltre all'adempimento di tale obbligo con le stesse modalità (…), provvedono altresì alla pubblicazione nei siti informatici, secondo modalità stabilite con decreto del Presidente del Consiglio dei Ministri.

Albo on line

- Art. 32, Legge 18 giugno 2009, n. 69
  - Gli adempimenti di cui ai commi 1 e 2 possono essere attuati mediante utilizzo di siti informatici di altre amministrazioni ed enti pubblici obbligati, ovvero di loro associazioni.
  - Al fine di garantire e di facilitare l'accesso alle pubblicazioni di cui ai commi 1 e 2 il CNIPA realizza e gestisce un portale di accesso ai siti di cui al medesimo comma 1.

Albo on line

- Art. 32, Legge 18 giugno 2009, n. 69
  - A decorrere dal 1 gennaio 2011 e, nei casi di cui al comma 2, dal 1 gennaio 2013, le pubblicazioni effettuate in forma cartacea non hanno effetto di pubblicità legale, ferma restando la possibilità per le amministrazioni e gli enti pubblici, in via integrativa, di effettuare la pubblicità sui quotidiani a scopo di maggiore diffusione, nei limiti degli ordinari stanziamenti di bilancio.

Documento informatico

- Senza l’adozione di particolari accorgimenti tecnici e la protezione di un sistema di archiviazione digitale, un documento informatico può essere modificato in qualsiasi momento, anche dopo la sua produzione e senza la volontà esplicita dell’autore.
- Pertanto, ai documenti informatici non sottoscritti digitalmente è riconosciuta la forza giuridica delle riproduzioni meccaniche, che è specificata nell’articolo 2712 del Codice Civile

Firma elettronica e firma digitale

- Nel 1997 lo Stato italiano, con il d.P.R. n. 513, fu il primo in Europa ad introdurre nel proprio ordinamento giuridico la firma digitale, attribuendogli la stessa valenza giuridica della firma autografa.
- Successivamente, l'Unione Europea, con la direttiva n. 1999/93/CE, ha disegnato un quadro comunitario delle firme elettroniche a cui anche l'Italia si è adeguata, emanando il codice dell'amministrazione digitale (d. lgs. n. 82/2005) e il d.P.C.M. 30 marzo 2009, contenente le regole tecniche per la firma digitale

Firma elettronica

- L’art. 1, c. 1, lett. q), del codice dell’amministrazione digitale (CAD), recependo l’art. 2, c. 1, direttiva UE n. 1999/93, definisce firma elettronica “l’insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzati come metodo di identificazione informatica”.
- È generata con un dispositivo che può essere “un software o un hardware usato per applicare i dati per la creazione di una firma (codici o chiavi crittografiche private)”

Firma elettronica

- L'art. 5, c. 2, direttiva n. 1999/93/CE, dichiara che "una firma elettronica non può esser considerata legalmente inefficace o inammissibile come prova in giudizio, unicamente perché è
  - in forma elettronica,
  - o non basata su un certificato qualificato,
  - o non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato,
  - oppure non è creata con un dispositivo per la creazione di una firma sicura

Documento informatico

- L’art. 21, c. 1, d. lgs. n. 82/2005 (CAD), afferma che “il documento informatico cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità”

Firma elettronica avanzata

- L'art. 2, c. 2, direttiva UE n. 1999/93, definisce firma elettronica avanzata "la firma elettronica ottenuta attraverso una procedura informatica che:
  - garantisce la connessione univoca al firmatario
  - è idonea a identificare il firmatario
  - è creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo
  - è collegata ai dati ai quali si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Firma elettronica qualificata

- L’art. 1, c. 1, lett. r), codice dell’amministrazione digitale (CAD), definisce firma elettronica qualificata “la firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro”.
- Le regole tecniche per la generazione, apposizione e verifica delle firma elettroniche qualificate sono contenute nel DPCM 30 marzo 2009, mentre le specifiche tecnologiche sono contenute nella deliberazione CNIPA 21 maggio 2009, n. 45.

Firma digitale

- La firma digitale è “un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l’integrità di un documento informatico o di un insieme di documenti informatici”
- Sotto il profilo tecnico, essa è il risultato di un algoritmo crittografico a chiavi asimmetriche applicato all’impronta digitale del file contenente la rappresentazione del documento

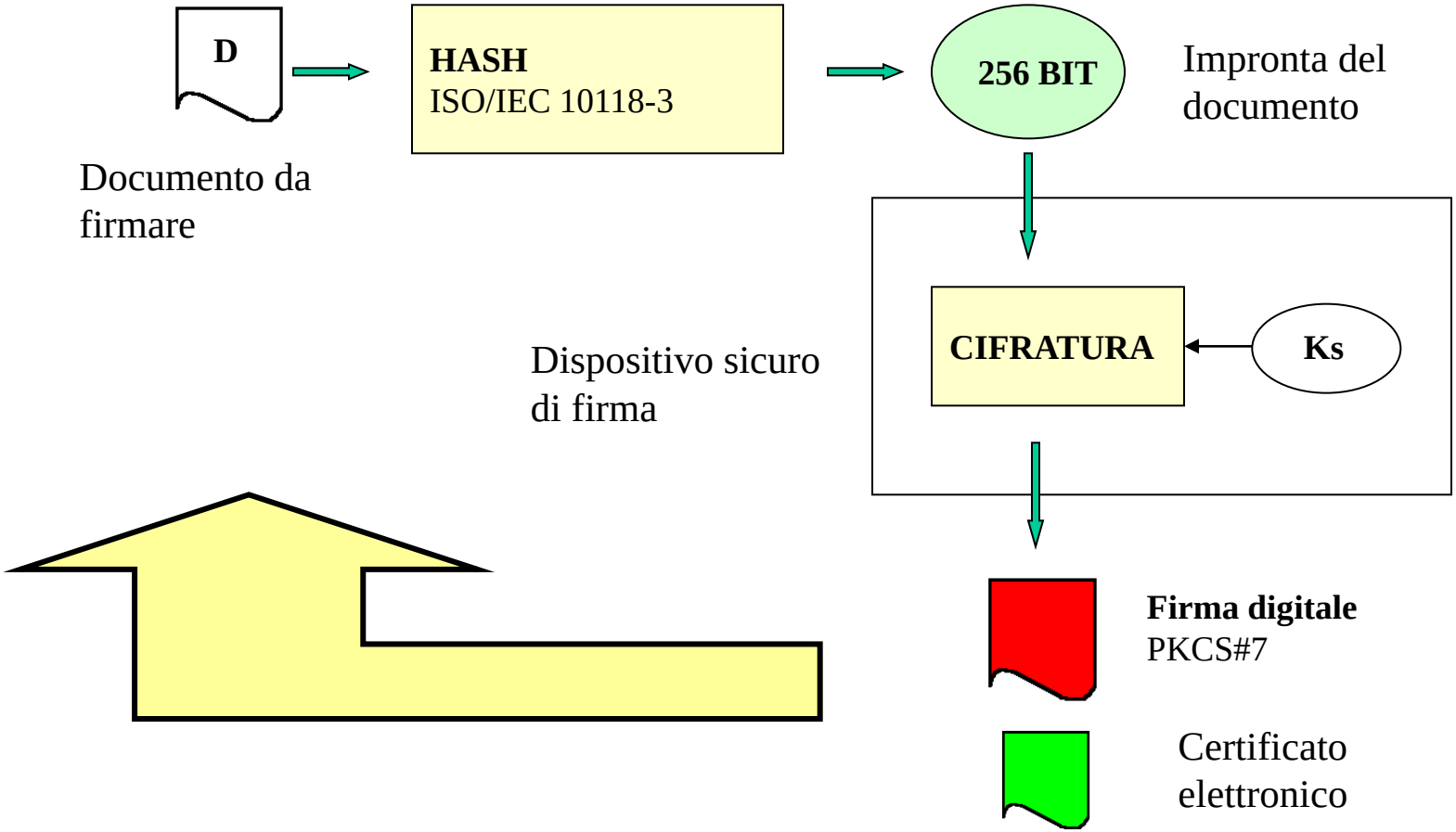
Firma digitale

- Le informazioni contenute in un certificato elettronico qualificato sono (art. 28, d. lgs. n. 82/2005):
  - l'indicazione che il certificato è qualificato
  - i dati anagrafici del titolare, compreso il suo codice fiscale
  - i dati identificativi e qualificativi del certificatore
  - i dati per la verifica della firma
  - il termine iniziale e finale di validità del certificato
  - le qualifiche del titolare e i limiti d'uso (opzionali)
  - la firma elettronica qualificata del certificatore

Firma digitale

- Il periodo di validità dei certificati elettronici qualificati è determinato dal certificatore anche in funzione della robustezza crittografica delle chiavi impiegate.
- I certificati elettronici possono anche essere revocati o sospesi (liste CRL/CSL) su richiesta del titolare, o del certificatore stesso, con le modalità specificate nel manuale operativo del servizio (si veda il DPCM 30/3/2009)
- Il certificatore deve tenere registrazione, anche elettronica, di tutte le informazioni relative ad un certificato qualificato, dal momento della sua emissione per almeno venti anni.

Generazione di una firma digitale



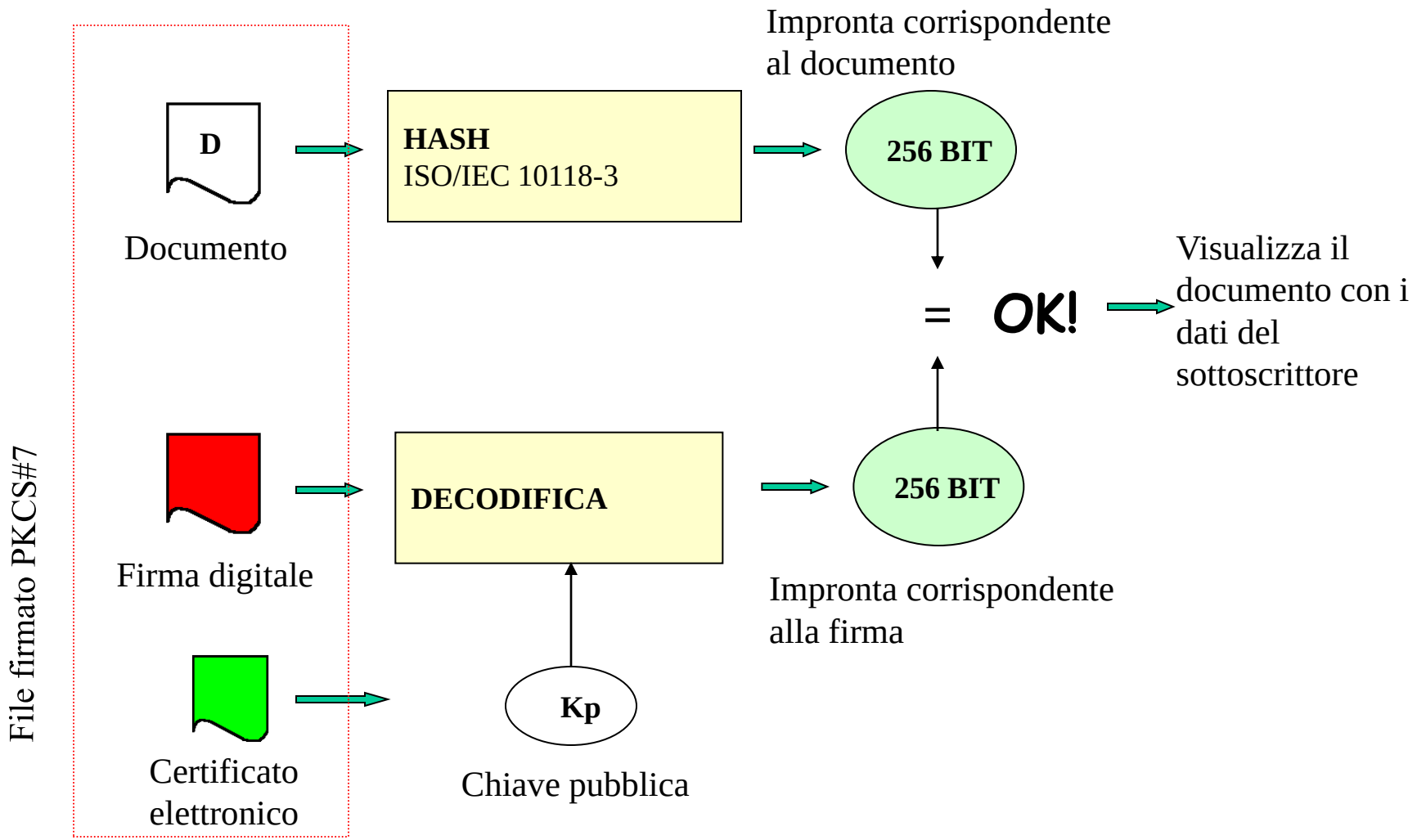
Firma digitale

- Il classico formato di firma digitale è lo standard PKCS#7 che assicura l'indipendenza dalle piattaforme tecnologiche dei vari certificatori
- Recentemente, il 3 marzo 2006, il CNIPA ha stipulato un protocollo d'intesa con la società Adobe Systems Inc. riconoscendo il PDF come un formato valido di firma elettronica
- Con la deliberazione CNIPA 18 maggio 2006, n. 34, sono state emanate le regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in formato XML

Firma digitale

- Sono previsti diversi tipi di firma digitale:
  - Firme multiple: firme digitali apposte da diversi sottoscrittori allo stesso documento
  - Firme parallele: firme apposte da diversi soggetti al medesimo documento informatico utilizzando una sola busta crittografica
  - Controfirma: la firma apposta ad una precedente firma

Verifica di una firma digitale



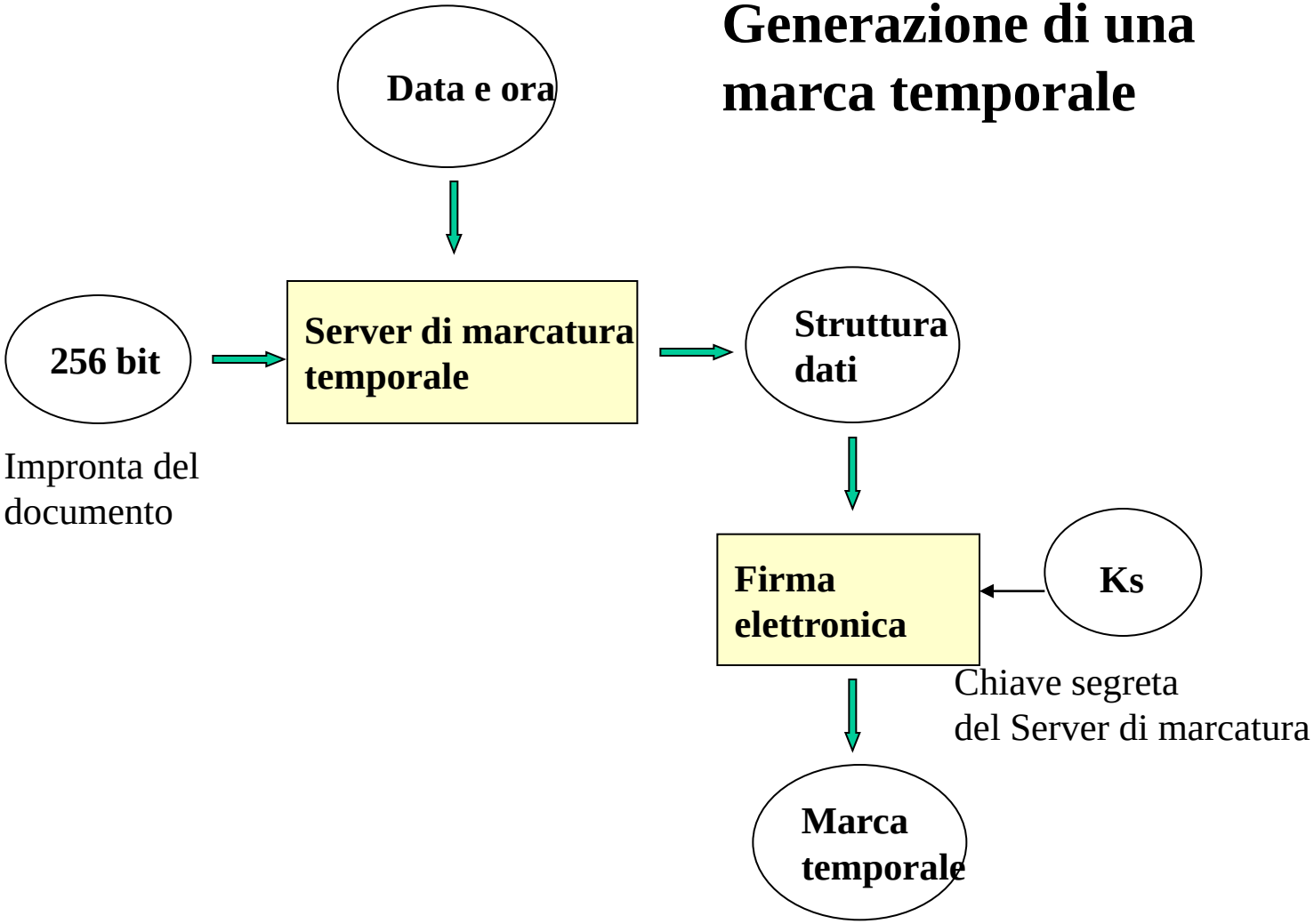
Firma digitale

- Una firma digitale è valida se, al momento della sottoscrizione, il certificato qualificato del firmatario non era scaduto, revocato o sospeso (vedi l'art. 21, c. 3, e l'art. 24, c. 3, d. lgs. n. 82/2005).
- Pertanto, il processo di verifica:
  - comprende la consultazione on line delle liste CRL/CSL del certificatore che ha rilasciato il certificato al firmatario
  - richiede la conoscenza un riferimento temporale che attesti, con certezza giuridica, l'esistenza del documento ad una certa data

Marcatura temporale

- L’art. 1, c. 1, lett. bb), del CAD, definisce il processo di validazione temporale come “il risultato della procedura informatica con cui si attribuisce, ad uno o più documenti informatici, una data e un orario opponibile a terzi”

Generazione di una marca temporale



Marcatura temporale

- Ai sensi dell’art. 49 dello stesso descreto, tutte le marche temporali devono essere conservate per un periodo non inferiore a venti anni, ovvero, su richiesta dell’interessato anche per un periodo maggiore.
- Una marca è valida per l’intero periodo di conservazione.

Riferimento temporale

- Ai sensi dell'art. 47 del DPCM 30 marzo 2009, in alternativa alla marca temporale, costituiscono validazione temporale:
  - Il riferimento temporale contenuto nella segnatura di protocollo
  - Il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti
  - Il riferimento temporale ottenuto attraverso l'utilizzo del servizio di posta elettronica certificata
  - Il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica (convenzione postale universale)

Firma digitale

- L’art. 3, c. 3, del DPCM 30 marzo 2009 dichiara che il documento informatico sottoscritto con firma digitale (…) non produce gli effetti dell’art. 21, c. 2, del CAD, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati».

Firma digitale

- E’ necessario identificare i formati elettronici da utilizzare per la produzione dei documenti, in quanto essi:
  - devono essere aperti, standard e documentati
  - non devono poter contenere macro istruzioni o, comunque sia, devono essere disponibili gli strumenti capaci di rilevarne la presenza
  - devono essere affidabili, accurati e usabili
  - devono essere indipendenti dalle piattaforme tecnologiche

Firma digitale

- Valore della firma digitale nel tempo (art. 51 del DPCM 30/3/2009)
  - La firma digitale ancorché sia scaduto, revocato, o sospeso il relativo certificato qualificato del sottoscrittore, è valida se alla stessa è associabile un riferimento temporale opponibile a terzi che colloca la generazione della firma in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato.

Documento informatico

- L’art. 21, c. 2 del CAD riconosce al documento informatico sottoscritto con una firma digitale, o con un altro tipo di firma elettronica qualificata l’efficacia prevista dall’art. 2702 del codice civile. L’utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria”.

Documento informatico

- La riproduzione su supporto cartaceo di un documento informatico produce la stampa del contenuto senza, ovviamente, la firma digitale che, essendo una sequenza binaria a cui non corrispondono caratteri dell'alfabeto né simboli grafici, può essere verificata solo su base informatica.
- Per questo motivo, l'art. 23, c. 2-bis, d. lgs. n. 82/2005, dichiara che le copie su supporto cartaceo del documento informatico, anche sottoscritto con firma digitale, sostituiscono ad ogni effetto di legge l'originale da cui sono tratte se la conformità all'originale è attestata da un pubblico ufficiale a ciò autorizzato

Documento informatico

- Il CNIPA ha pubblicato uno studio sul timbro digitale, inteso come “una rappresentazione convenzionale di informazioni contenute nel documento elettronico (tutte o parte di esse), stampabile, riconoscibile con strumenti elettronici e ottenuta utilizzando una codifica grafica definita” (di tipo bidimensionale quale ad esempio il PDF417 o il MAXICODE)

Digitalizzazione dei documenti analogici

- L’art. 22, c. 3, d. lgs. n. 82/2005, dichiara che “le copie su supporto informatico di documenti formati in origine su altro tipo di supporto sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte, se la loro conformità all’originale è assicurata dal funzionario a ciò delegato nell’ambito dell’ordinamento proprio dell’amministrazione di appartenenza, mediante l’utilizzo della firma digitale e nel rispetto delle regole tecniche di cui all’art. 71 del codice dell’amministrazione digitale”

Posta elettronica

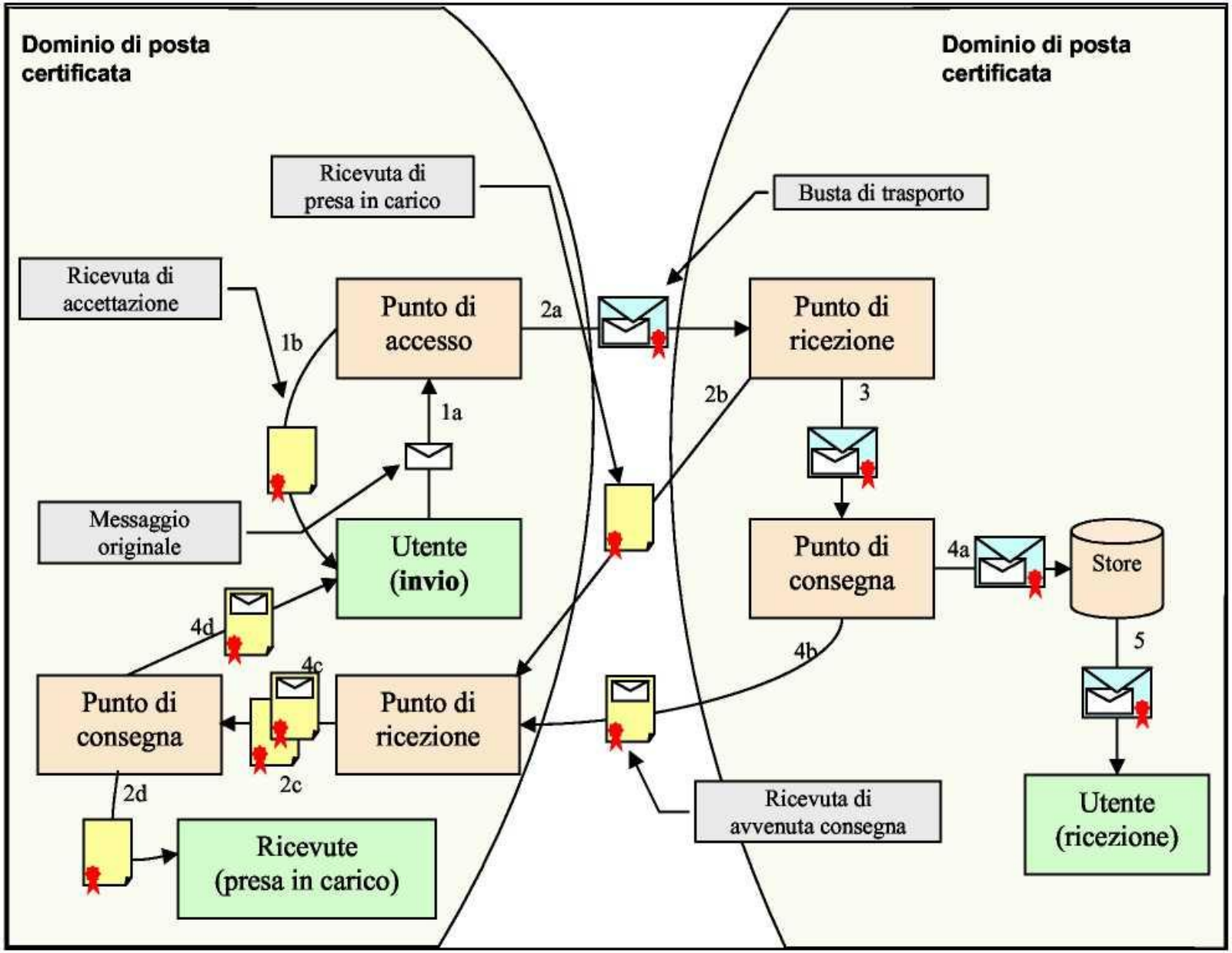
- La posta elettronica “ordinaria” presenta molti vantaggi rispetto a quella cartacea, ma anche alcuni elementi di debolezza:
  - non fornisce certezze giuridiche sulla provenienza, data di spedizione e data di consegna dei messaggi
  - non garantisce l’integrità dei messaggi
  - non garantisce la riservatezza delle comunicazioni
  - non fornisce informazioni sullo stato di avanzamento delle comunicazioni

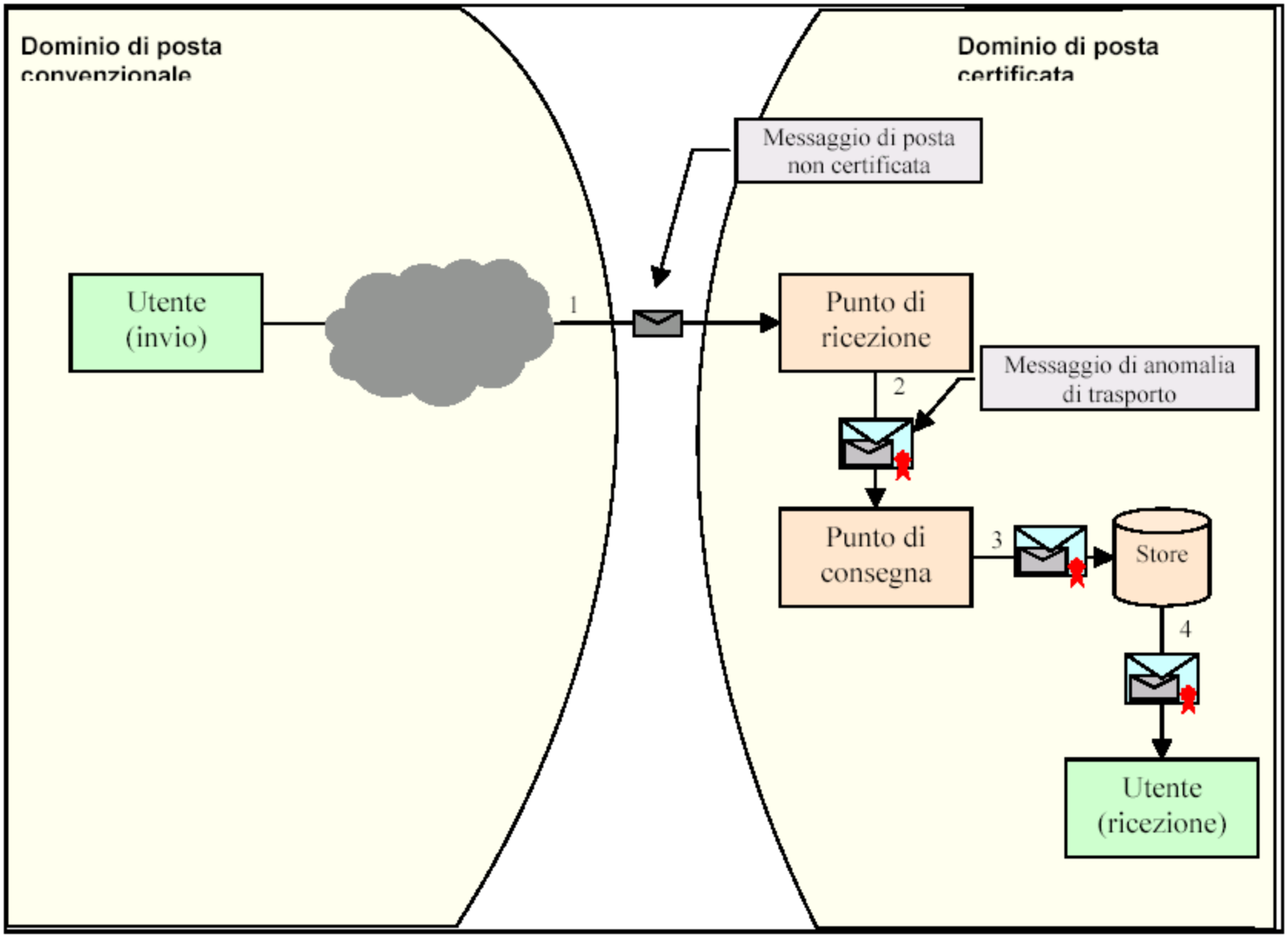
Posta elettronica certificata

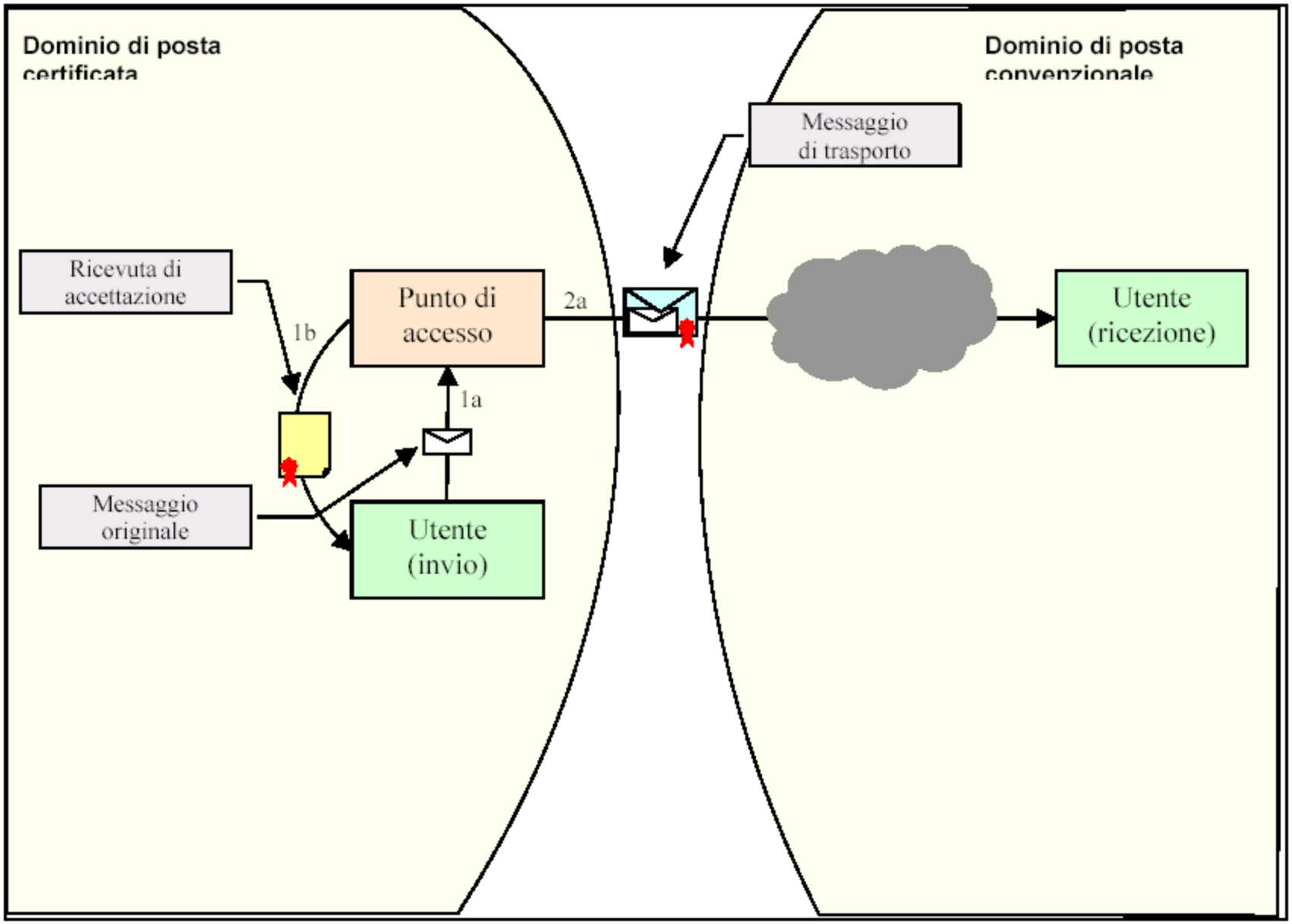
- Le disposizioni per l'utilizzo della posta elettronica certificata (PEC) sono contenute nel d.P.R. 11 febbraio 2005, n. 68, mentre le regole tecniche sono state emanate con D.M. 2 novembre 2005
- Altre disposizioni inerenti alla PEC sono riportate nel codice dell'amministrazione digitale (d. lgs. n. 82/2005) e nella legge 28 gennaio 2009, n. 2, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale

Posta elettronica certificata

- I privati e le pubbliche amministrazioni che intendono svolgere questa attività devono presentare al CNIPA una domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata e dimostrare di possedere i requisiti richiesti.
- Le caselle di PEC rilasciate a privati da pubbliche amministrazioni producono gli effetti giuridici riconosciuti a questo mezzo di trasmissione solo per le comunicazioni che nascono nell'ambito dei rapporti tra le amministrazioni medesime e i titolari delle caselle


Dominio di posta certificata
Dominio di posta certificata
Ricevuta di presa in carico
Busta di trasporto
Ricevuta di accettazione
Punto di accesso
2a
Punto di ricezione
1b
1a
2b
3
Messaggio originale
Utente (invio)
Punto di consegna
4a
Store
4d
4c
4b
5
Punto di consegna
Punto di ricezione
2c
2d
Ricevuta di avvenuta consegna
Utente (ricezione)
Ricevute (presa in carico)


Dominio di posta convenzionale
Dominio di posta certificata
Messaggio di posta non certificata
Utente (invio)
1
Punto di ricezione
Messaggio di anomalia di trasporto
2
Punto di consegna
3
Store
4
Utente (ricezione)


Dominio di posta certificata
Dominio di posta convenzionale
Messaggio di trasporto
Ricevuta di accettazione
Punto di accesso
2a
1b
1a
Utente (ricezione)
Messaggio originale
Utente (invio)

Posta elettronica certificata

- Qualora, per un motivo qualsiasi, un messaggio non risulti consegnabile al destinatario, il gestore del servizio di PEC del mittente è tenuto a comunicargli l'esito negativo della trasmissione entro 24 ore dall'invio
- I gestori dei servizi di PEC devono tenere traccia delle operazioni effettuate per la trasmissione dei messaggi in un apposito registro informatico denominato *log dei messaggi*. Tale registro deve essere conservato per almeno 30 mesi

Posta elettronica certificata

- [Art. 45, d. lgs. n. 82/2005] – I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale

Posta elettronica certificata

- [Art. 47, c. 1, d. lgs. n. 82/2005] - Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta verificata la provenienza

Posta elettronica certificata

- [Art. 47, c. 2, d. lgs. n. 82/2005] – Ai fini della verifica della provenienza, le comunicazioni sono valide se:
  - sono sottoscritte con firma digitale
  - sono dotate di protocollo informatico (è il caso dei documenti provenienti da pubbliche amministrazioni)
  - sono trasmesse con sistemi di posta elettronica certificata
  - è comunque possibile accertarne altrimenti la provenienza secondo quanto previsto dalla normativa vigente

Posta elettronica certificata

- [Art. 48, d. lgs. n. 82/2005] – La trasmissione di un documento per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.
- La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi.

Posta elettronica certificata

- Poiché la ricevuta di avvenuta consegna attesta che un messaggio è stato depositato nella casella elettronica del destinatario, ma non che questi l'abbia letto, è necessario che il destinatario dichiari la sua casella di PEC, impegnandosi a scaricare sistematicamente la posta ivi depositata.

Posta elettronica certificata

- [Art. 16, c. 6, L. n. 2/2009] – Le imprese costituite in forma societaria sono tenute ad indicare il loro indirizzo di PEC nella domanda di iscrizione al registro delle imprese. Quelle già costituite lo devono dichiarare alla CCIAA entro 3 anni dall'entrata in vigore della presente legge

Posta elettronica certificata

- [Art. 16, c. 7, L. n. 2/2009] – I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di PEC entro 1 anno dall’entrata in vigore della presente legge

Posta elettronica certificata

- [Art. 16, c. 8, L. n. 2/2009] – Le amministrazioni pubbliche di cui all'art. 1, c. 2, del d. lgs. n. 165/2001 istituiscono una casella certificata per ciascun registro di protocollo e ne danno comunicazione al CNIPA che provvede a pubblicarle in un elenco consultabile per via telematica (si veda anche il d.P.C.M. 31 ottobre 2000, contenente le regole tecniche per il protocollo informatico, e la circolare AIPA n. 28/2001, recante standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni)

Posta elettronica certificata

- Oltre che sull’indice nazionale gestito da DigitPA, ai sensi dell’art. 54, c. 2-ter, del codice dell’amministrazione digitale, le amministrazioni pubbliche che già dispongono di propri siti sono tenute a pubblicare nella pagina iniziale: a) un indirizzo di posta certificata cui il cittadino possa rivolgersi per qualsiasi richiesta; b) l’elenco completo delle caselle di posta elettronica istituzionale attivate, specificando se si tratta di caselle di PEC conformi al DPR n. 68/2005.

Posta elettronica certificata

- [Art. 16, c. 9, L. n. 2/2009] – Le comunicazioni tra i soggetti di cui ai commi 6, 7, 8 del presente articolo, che abbiano provveduto agli adempimenti ivi previsti, possono essere inviate attraverso la PEC senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo.

Posta elettronica certificata

- [Art. 16 bis, c. 6, L. n. 2/2009] – Ogni amministrazione pubblica utilizza unicamente la posta elettronica certificata, con effetto equivalente, ove necessario, alla notificazione per mezzo della posta, per le comunicazioni aventi come destinatari dipendenti della stessa o di altra amministrazione pubblica.

Servizio CEC-PAC

- Il DPCM 6 maggio 2009, emanato ai sensi dell'art. 16-bis, c. 7, del D.L. n. 185/2008, convertito con L. n. 2/2009, disegna un servizio finalizzato al rilascio di caselle di posta certificata ai cittadini, che prevede per essi la possibilità di ottenere gratuitamente un indirizzo di PEC, richiedendolo direttamente, o tramite l'affidatario del servizio, al Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri

Servizio CEC-PAC

- Una volta assegnata, la casella di CEC-PAC diventa per il titolare un indirizzo valido, ad ogni effetto giuridico, ai fini dei rapporti con le pubbliche amministrazioni, e la volontà da questi espressa all'atto della richiesta rappresenta l'esplicita accettazione dell'invio, tramite essa, da parte delle pubbliche amministrazioni, di tutti i provvedimenti e gli atti che lo riguardano.

Servizio CEC-PAC

- Il gestore del servizio CEC-PAC deve garantire:
  - il rilascio delle caselle di posta elettronica per ogni cittadino maggiorenne che ne faccia richiesta, destinate esclusivamente alle comunicazioni tra PA e cittadino;
  - la possibilità di attivare la funzionalità aggiuntiva della ricevuta di presa visione da parte dell'utente;
  - il servizio di notifica dell'avvenuta ricezione di un messaggio sulla casella CEC-PAC tramite canali di comunicazione tradizionali

Servizio CEC-PAC

- la formazione del fascicolo elettronico personale del cittadino con i documenti ricevuti e trasmessi alle pubbliche amministrazioni;
- la messa a disposizione dei cittadini di un indirizzario delle pubbliche amministrazioni provviste di PEC.
- In aggiunta al servizio base di notifica tramite *e*-mail è prevista per il cittadino, a pagamento, la possibilità di ricevere le stesse segnalazioni anche via SMS, IVR e posta cartacea.

Servizio CEC-PAC

- Per rendere efficace l'utilizzo della casella di PEC da parte dei cittadini, l'art. 4 del DPCM 6 maggio 2009 ha imposto alle pubbliche amministrazioni di rendere disponibile sul loro sito istituzionale, per ciascun procedimento, ogni tipo di informazione idonea a consentire l'inoltro di istanze da parte dei cittadini titolari di PEC, inclusi i tempi previsti per l'espletamento della procedura.

Evoluzione della PEC

- Da più parti sono state sollevate perplessità sull’incompatibilità del servizio di posta elettronica certificata con gli analoghi sistemi internazionali.
- Per questo motivo, le recenti disposizioni sulla posta certificata aprono le porte ad un servizio di posta elettronica alternativo alla PEC, comunque capace di certificare la data e l’ora dell'invio e della ricezione delle comunicazioni, nonché l’integrità del contenuto delle stesse, garantendo l’interoperabilità con analoghi sistemi internazionali

Evoluzione della PEC

- A conferma della volontà di correggere e migliorare l'attuale servizio di PEC, l'art. 35, della Legge 18 giugno 2009, n. 69, impegna il Governo ad adottare, entro sei mesi dalla data di entrata in vigore della legge, un regolamento recante modifiche al DPR 11 febbraio 2005, n. 68, anche al fine di garantire l'interoperabilità del sistema di posta elettronica certificata con analoghi sistemi internazionali.

Direttive del DDI sulla PEC

- Il Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica, recentemente, ha emesso due Circolari, la n. 1 e la n. 2 del 2010, per egolamentare l'uso della PEC nelle Amministrazioni Pubbliche, dichiarando anche che "La mancata disponibilità di almeno una casella di PEC per ciascun registro di protocollo e la prosecuzione delle tradizionali forme di comunicazione configurano l'inosservanza di disposizioni di legge e una fattispecie di improprio uso di denaro pubblico".

Canali di comunicazione via Web

- Un canale di comunicazione via Web presuppone:
  - l’autenticazione degli utenti
  - la sicurezza e riservatezza delle comunicazioni
  - la disponibilità di modulistica elettronica
  - la possibilità di effettuare pagamenti on line

Autenticazione on line

- Le procedure e le regole tecniche per l’emissione della carta d’identità elettronica e del documento d’identità elettronico sono contenute nel DPCM 22 ottobre 1999, n. 437, e nel Decreto Ministeriale 8 novembre 2007.
- Il periodo di validità di una CIE, inizialmente di 5 anni, è stato recentemente ampliato a 10 anni

Autenticazione on line

- Le procedure e le regole tecniche per l’emissione della carta nazionale dei servizi, invece, sono definite nel DPR 2 marzo 2004, n. 117, oltre che nel decreto interministeriale 9 dicembre 2004 e nell’art. 66 del Codice dell’amministrazione digitale
- Per carta nazionale dei servizi (CNS) s’intende il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni

Autenticazione on line

- L’art. 2, c. 1, del DPR 2 marzo 2004, n. 117, recante il regolamento per la diffusione della carta nazionale dei servizi, specifica che «la carta nazionale dei servizi, in attesa della carta d’identità elettronica, è emessa dalle pubbliche amministrazioni interessate al fine di anticipare le funzioni di accesso ai servizi in rete delle pubbliche amministrazioni».
- A differenza della CIE, la CNS ha la validità temporale determinata dall’amministrazione emittente e comunque non superiore a 6 anni

Autenticazione on line

- [art. 64, c. 1 e 2, d. lgs. n. 82/2005] – la CIE e la CNS costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.
- Le pubbliche amministrazioni possono utilizzare anche strumenti diversi, ma in ogni caso devono consentire l'accesso ai loro servizi tramite la CIE e la CNS

Carta nazionale dei servizi (CNS)

- [art. 64, c. 3, d. lgs. n. 82/2005] – A decorrere dal 31 dicembre 2010 non sarà più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni con strumenti diversi dalla carta d'identità elettronica (CIE) e dalla carta nazionale dei servizi (CNS).
- Tale termine è stato prorogato al 31 dicembre 2010 dall’art. 1, c. 5, L. 26 febbraio 2010, n. 25

Istanze presentate per via telematica

- L’art. 65, c. 1, d. lgs. 82/2005, stabilisce che le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica sono valide se:
  - sono sottoscritte con firma digitale, il cui certificato è rilasciato da un certificatore accreditato
  - ovvero quando l’autore è identificato dal sistema informatico con l’uso della CIE o della CNS, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente

Istanze presentate per via telematica

- ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'art. 64, c. 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente e fermo restando il disposto dell'art. 64, c. 3 (termine fissato al 31 dicembre 2010)
- ovvero quando l'autore è identificato dal sistema informatico attraverso le credenziali di accesso relative all'utenza personale di posta elettronica certificata di cui all'art. 16-bis della L. n. 2/2009

Istanze presentate per via telematica

- Il comma 2 dello stesso articolo riconosce che le istanze e le dichiarazioni inviate o compilate su sito con queste modalità sono equivalenti alle dichiarazioni e alle istanze sottoscritte con firma autografa apposta in presenza al dipendente addetto al procedimento.
- Resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui sia necessaria la sottoscrizione mediante firma digitale

Modulistica elettronica

- [art. 57 del Co.A.Di.]: Le pubbliche amministrazioni provvedono a definire e a rendere disponibili anche per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.

Sistemi di pagamento elettronici

- I sistemi di pagamento elettronici sono indispensabili per la corresponsione degli oneri dovuti all’atto della presentazione di determinate istanze (ad esempio, per il pagamento dell’imposta di bollo o per la fruizione di particolari servizi).
- L’art. 5 del codice dell’amministrazione digitale impone alle pubbliche amministrazioni centrali l’attivazione di sistemi di pagamento elettronici

Bollo virtuale

- L’articolo 7 del decreto del Ministero delle Finanze 23 gennaio 2004 specifica le modalità di assolvimento dell’imposta di bollo sui documenti informatici.
- Il Ministero delle Finanze – Agenzia delle entrate – autorizza la riscossione dell’imposta di bollo da parte delle Amministrazioni procedenti, le quali dovranno successivamente provvedere al versamento degli oneri incassati

Procedimenti amministrativi *on line*

- La possibilità e l’opportunità di sostituire i documenti cartacei con i documenti informatici devono essere valutate in relazione ai procedimenti amministrativi a cui si riferiscono.
- E quindi occorre ridisegnare i procedimenti, agevolando l’uso delle tecnologie informatiche

Procedimenti amministrativi *on line*

- Nella modellazione dei procedimenti amministrativi, per ognuno di essi, al minimo, occorre specificare:
  - la denominazione e l’unità organizzativa di competenza
  - il nominativo del responsabile
  - il tempo di svolgimento
  - la normativa di riferimento ed altri eventuali vincoli
  - la sequenza delle fasi e dei sub-procedimenti
  - i documenti ricevuti o prodotti nell’ambito di ciascuna fase o sub-procedimento

Procedimenti amministrativi *on line*

- Se si analizza la produzione documentaria nell'ambito dei procedimenti amministrativi, per ogni documento rilevato si possono fissare i requisiti per:
  - la firma elettronica, il tempo di conservazione, i metadati e l'indice di classificazione, l'accessibilità e la riservatezza
  - si può preordinare la formazione del fascicolo
  - si può predisporre la modulistica elettronica

Gestione informatica dei documenti

- La transizione dai documenti cartacei ai documenti informatici implica l'attivazione di sistemi per la protocollazione, classificazione e archiviazione degli atti digitali oltre a quelli cartacei.
- Le disposizioni per la gestione informatica dei documenti sono contenute nelle seguenti norme:
  - DPR n. 445/2000
  - DPCM 31 ottobre 2000
  - Circolare AIPA n. 28/2001

Registrazione di protocollo

- Ai sensi dell’art. 53, c. 5, del DPR 28 dicembre 2000, n. 445, la registrazione di protocollo è «un’operazione obbligatoria per i documenti ricevuti o spediti da una pubblica amministrazione e per tutti i documenti informatici»
- Con l’entrata in funzione del sistema di gestione informatica dei documenti devono essere eliminati tutti i sistemi di registrazione dei documenti alternativi al protocollo informatico (art. 3, comma 1, lettera d), DPCM 31 ottobre 2000)

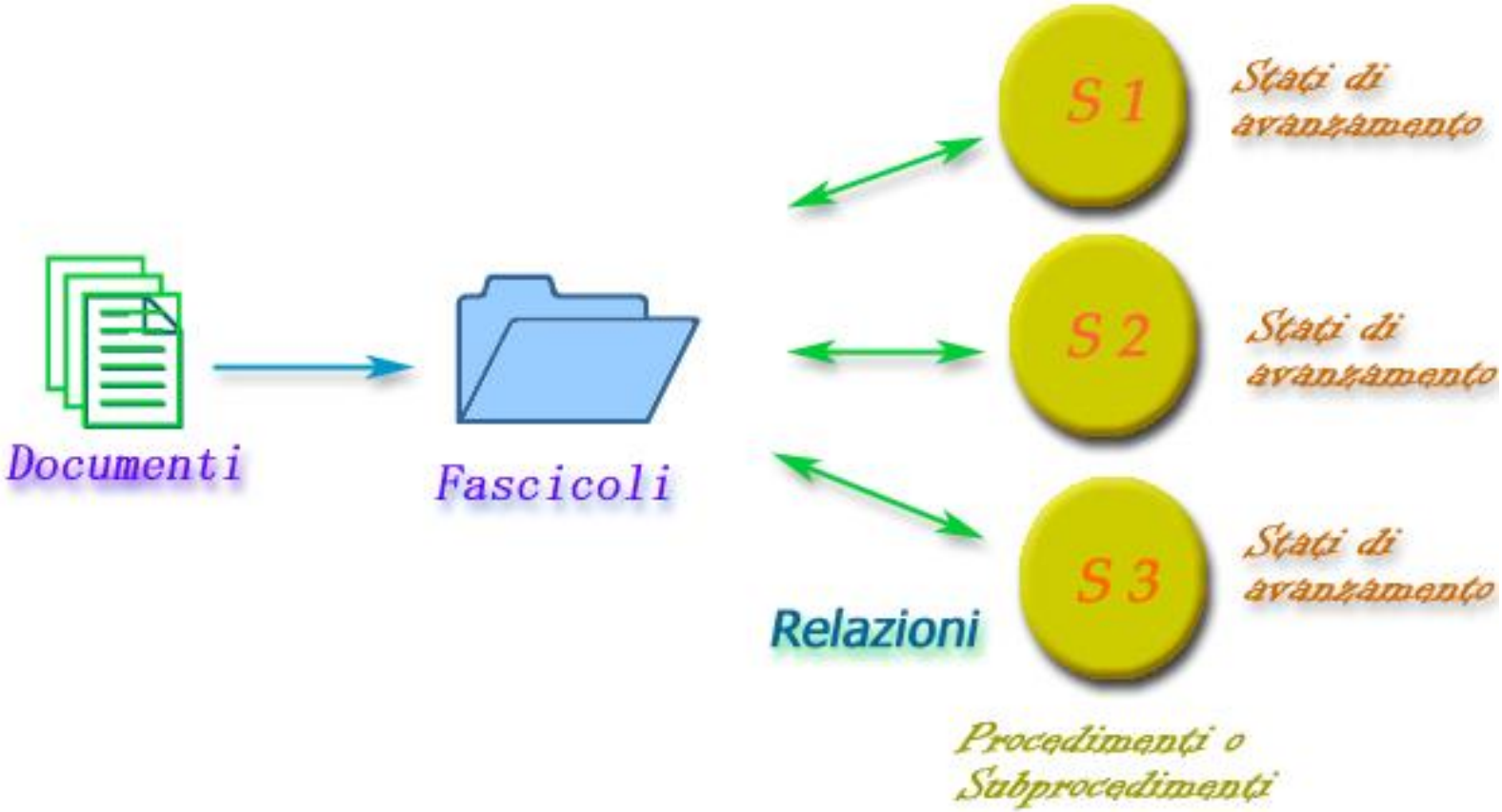
Classificazione e fascicolazione

- Le operazioni di classificazione e fascicolazione dei documenti determinano il momento costitutivo dell’archivio in quanto permettono di disporre le “carte” secondo un ordine logico che rispecchia lo sviluppo e l’evoluzione dell’attività dell’ente

Fascicolo informatico

- Un documento informatico, non avendo la fisicità della carta, può essere riunito ai suoi precedenti e susseguenti, formando una unità archivistica equivalente al fascicolo cartaceo, solo attraverso un sistema che permetta l'esecuzione sistematica delle operazioni di registrazione di protocollo, classificazione e fascicolazione
- Nel caso dei documenti informatici tale sistema rappresenta il *mezzo* con cui si formano le unità archivistiche e il *luogo* dove esse vengono archiviate insieme ai documenti che le compongono.

Gestione integrata dei documenti e dei procedimenti amministrativi



Conservazione digitale

- I fattori che incidono negativamente sulla conservazione digitale sono riconducibili:
  - all’obsolescenza delle firme elettroniche
  - all’obsolescenza dei supporti
  - all’obsolescenza dei formati
  - all’obsolescenza dei sistemi e delle tecnologie in genere

Conservazione digitale

- Il legislatore italiano si è orientato sul metodo della migrazione, emanando la Deliberazione CNIPA 19 febbraio 2004, n. 11, recante le regole tecniche per la riproduzione e conservazione dei documenti su supporto ottico
- Per l'archiviazione ottica dei documenti sono utilizzabili qualsiasi tipo di supporto di memorizzazione digitale che consenta la registrazione mediante la tecnologia laser (Worm, CD-R, magneto-ottici, DVD). Tuttavia, è consentito l'impiego di supporti anche non ottici purché siano idonei a garantire la conformità dei documenti agli originali

Conservazione digitale

- I documenti analogici si possono presentare in stato di originale o di copia; gli originali a loro volta possono essere *unici* o *non unici*. Questi ultimi sono rappresentati dai documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
- Solo per i documenti analogici originali unici è richiesta l’apposizione del riferimento temporale e della firma digitale, oltre che del responsabile della conservazione, anche da parte di un pubblico ufficiale per attestare la conformità al documento d’origine.

Conservazione digitale

- La distruzione dei documenti analogici è consentita dopo il completamento della procedura di conservazione digitale, salvo i «poteri di controllo del Ministero per i Beni e le Attività Culturali sugli archivi delle amministrazioni pubbliche e sugli archivi dei privati dichiarati di notevole interesse storico».

Conservazione digitale

- Il complesso delle attività da svolgere, i requisiti giuridici da soddisfare e le competenze professionali necessarie per la corretta conservazione della memoria digitale non sono alla portata della maggior parte delle amministrazioni pubbliche di piccola e media dimensione
- Per questo motivo è opportuna la costituzione di ***centri di conservazione digitale***, ovvero di strutture dedicate alla conservazione della memoria digitale di più soggetti produttori e dotate di tecnologie avanzate e personale archivistico e informatico altamente qualificato