Lezione . 4

Il valore giuridico del documento informatico

Riconoscimento del valore giuridico al documento informatico

Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonchè la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti

Legge 59/97 (cosiddetta Bassanini) art. 15 comma 2

Codice Pubblica Amministrazione digitale (d.lgs. 82/05 art. 20)

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice

1-*bis*. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale

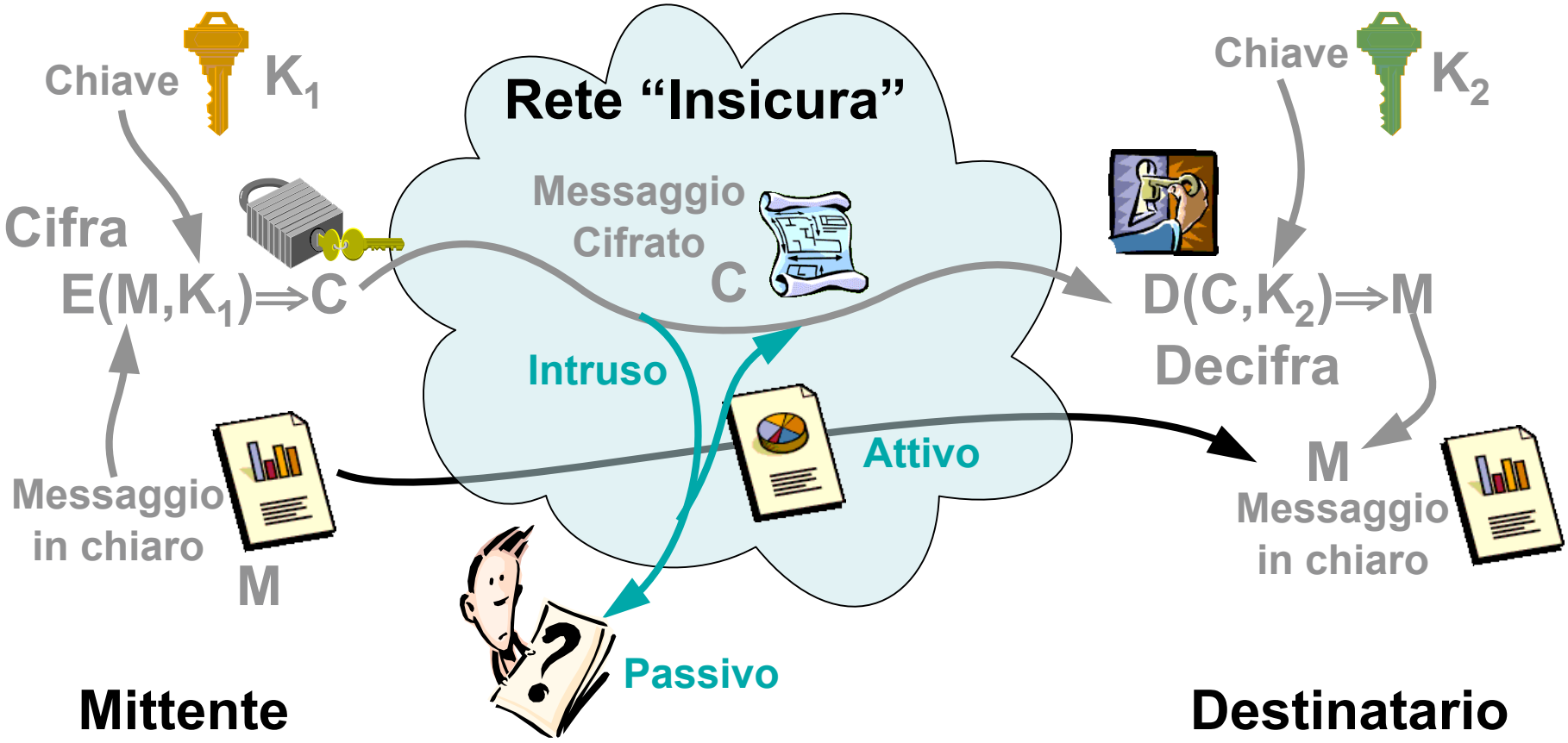
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Identificabilità dell'autore e integrità del documento

Ad oggi tali requisiti vengono garantiti ricorrendo prevalentemente (ma non solo) a tecniche crittografiche.

Crittografia



Crittografia Simmetrica

- I messaggi vengono cifrati e decifrati con la stessa chiave (cioè K1=K2).
- Tutte le parti coinvolte nella transazione devono conoscere la chiave:
  - Serve un canale sicuro per la distribuzione della chiave, ma se c'è un canale sicuro perché non usarlo sempre?
  - Con quale frequenza si deve cambiare la chiave?
  - E' necessario avere un numero di chiavi pari al numero degli interlocutori

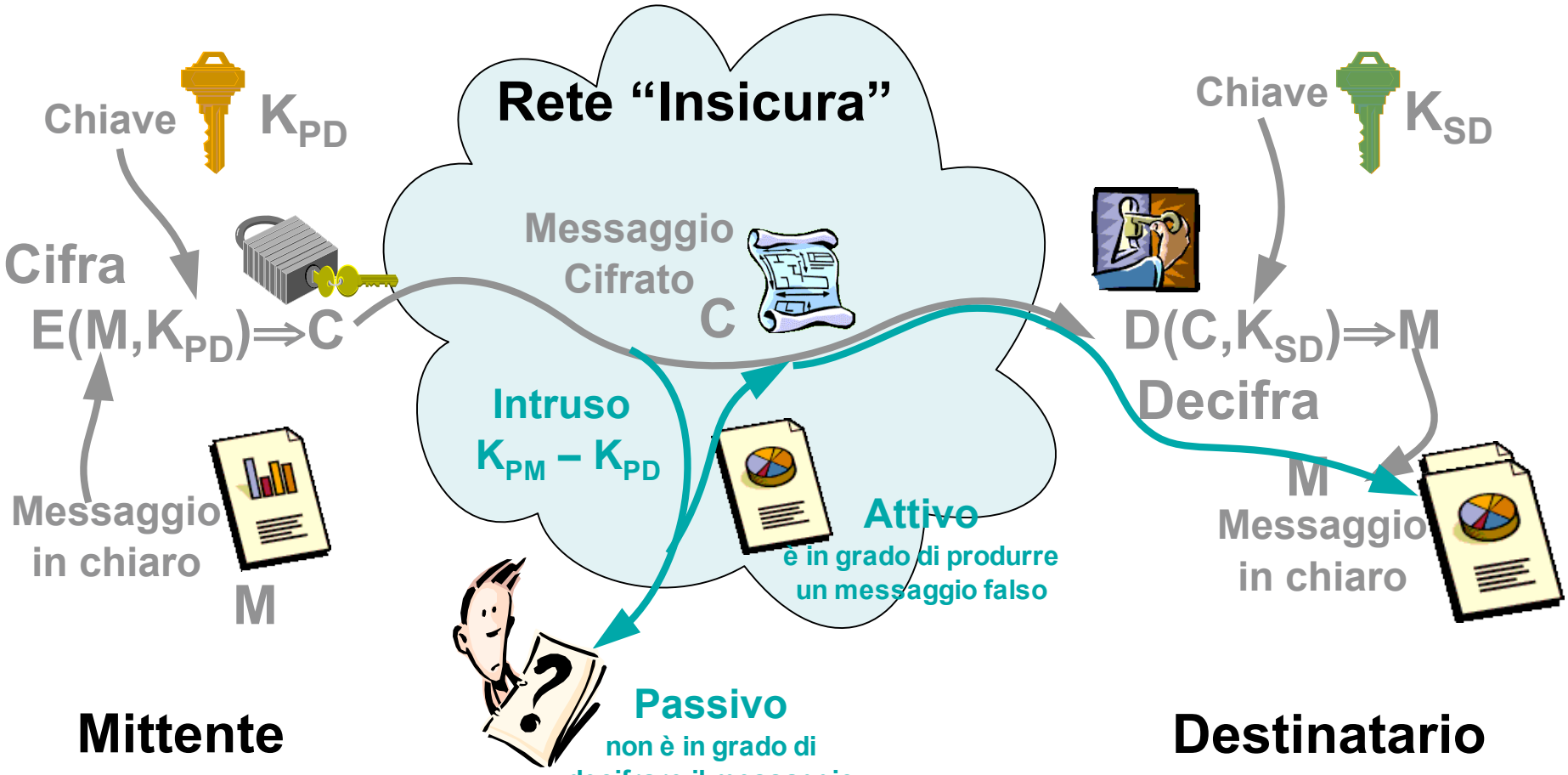
La crittografia: aspetti tecnici

Crittografia Asimmetrica

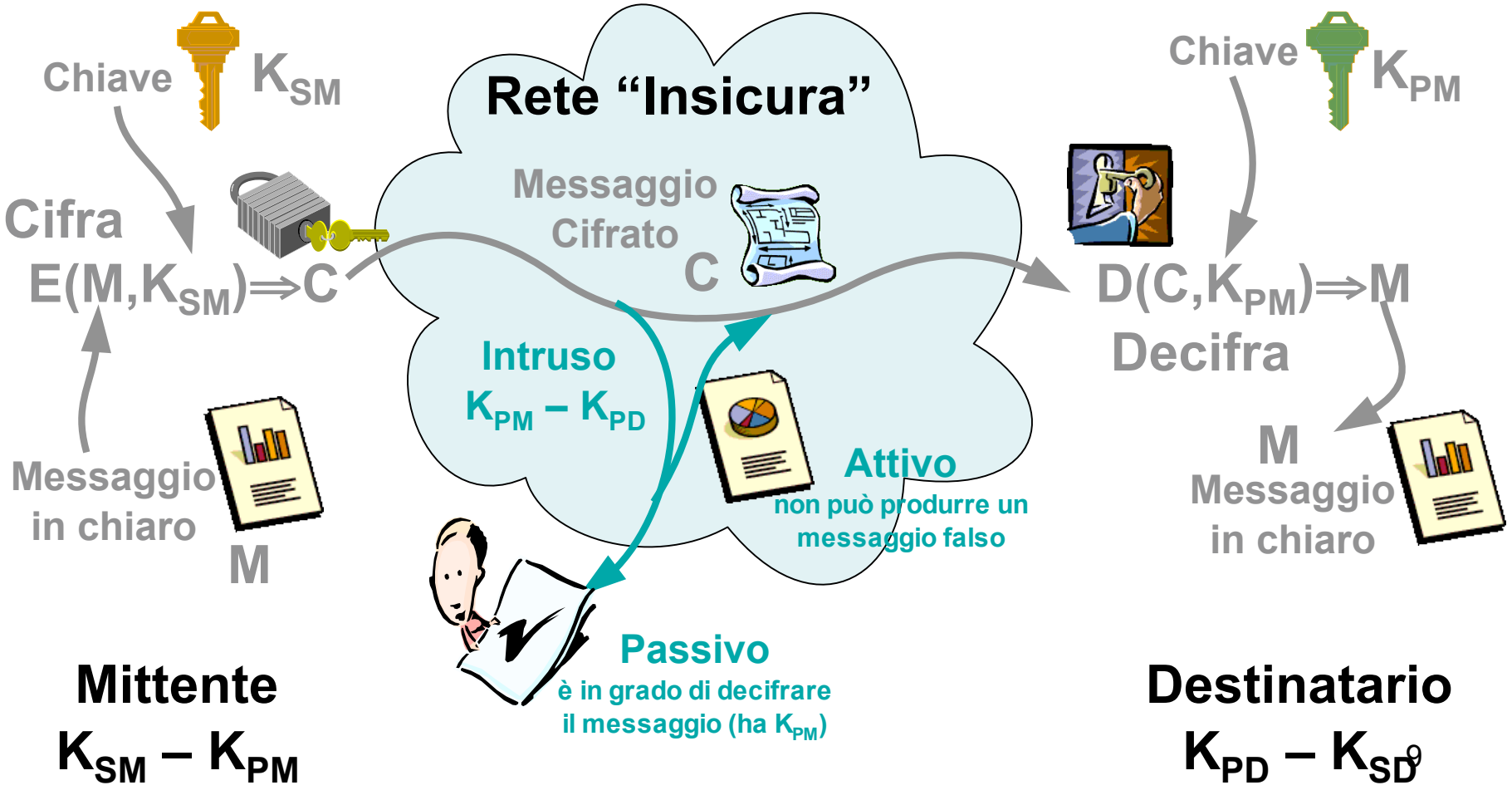
- Ogni partner coinvolto nella transazione ha due chiavi correlate tra di loro, una pubblica (KP) e una segreta (KS)
  - La chiave pubblica è di dominio pubblico, tutti la conoscono e tutti la possono usare!
  - La chiave segreta (o privata) è nota solo al proprietario!
- L'informazione cifrata con una delle due chiavi (KP o KS) può essere decifrata solo usando l'altra chiave (risp. KS o KP)!!

La crittografia: aspetti tecnici

Riservatezza & Integrità

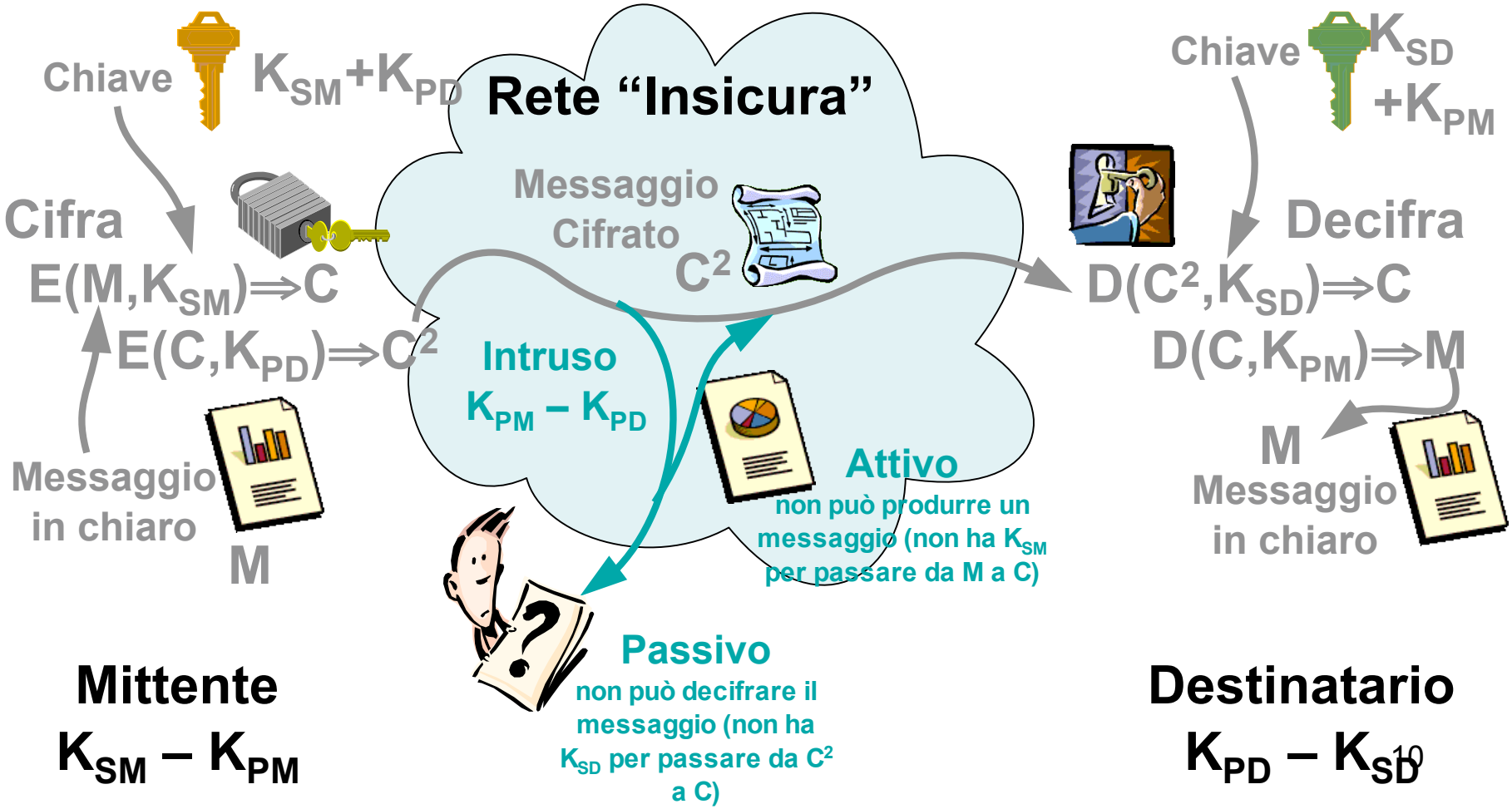


Garanzia di provenienza & Integrità



La crittografia: aspetti tecnici

Riservatezza & Integrità & Provenienza



Identificabilità dell'autore

Le tecniche crittografiche danno garanzia della provenienza del messaggio, ma non consentono da sole di identificare l'autore.

Per fare questo si deve ricorrere ad autorità esterne, le cosiddette autorità di certificazione

Come attribuire il documento ad una persona determinata?

Si istituiscono uno o più registri che alla chiave pubblica associano i dati identificativi della persona.

In questo modo, D non solo sa che il documento è stato firmato da M ma anche che M è il sig. Mario Rossi, nato a… etc:

La scelta del legislatore

- Per dare valore giuridico al documento informatico, il legislatore fa ricorso alle tecnologie crittografiche.

  O meglio, pur riconoscendo la possibilità che gli stessi obbiettivi possano essere raggiunti anche attraverso altre tecnologie, ricorre per attribuire valore di forma scritta ad un documento alla firma digitale, che si fonda su tecnologie crittografiche

Forma e efficacia dei documenti informatici

Documenti informatici	**Forma**	**Efficacia**
Documento informatico privo di firma	il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità	Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime
Documento con firma elettronica	il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità	Liberamente valutabile dal giudice tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità
Documento con firma elettronica qualificata o con firma digitale	Forma scritta, anche nei casi previsti sotto pena di nullità dall'art. 1350	La scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria

La scelta del legislatore

I tipi di firma introdotti dal legislatore nazionale

- **firma elettronica**

  Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica

- **firma elettronica qualificata**

  La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;

  firma digitale

  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;

Firma Digitale: hash + cifra

Funzioni *hash* (H) generano un riassunto/impronta (*digest*) del messaggio

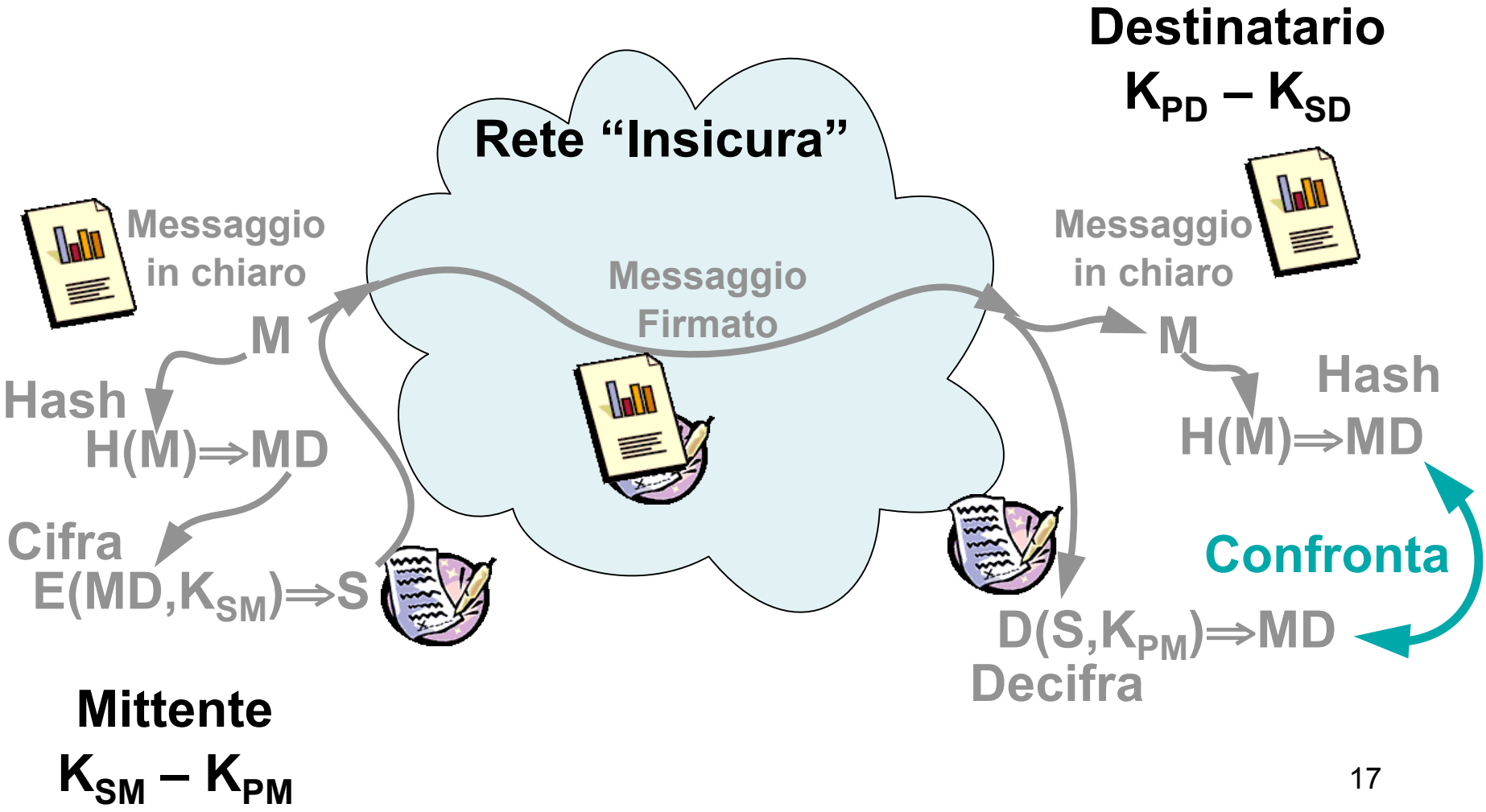
- Dato M è facile calcolare H(M)
- Dato H(M) è praticamente impossibile ricavare M
- Nessuno è in grado di generare due messaggi che abbiano lo stesso *digest* $[M_1 \neq M_2 \Rightarrow H(M_1) \neq H(M_2)]$

La funzione di hash garantisce l'integrità del documento

(un documento modificato non corrisponderà più all'hash originario)

La cifra garantisce la provenienza (il documento non può che provenire da chi ha apposto la sua chiave privata, che si può verificare solo con la corrispondente chiave pubblica)

Firma Digitale: hash + cifra



La scelta del legislatore

Le autorità di certificazione

Chi intende utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti previsti dalla legge deve:

- munirsi di un'idonea coppia di chiavi
- rendere pubblica una di esse mediante la procedura di certificazione

La scelta del legislatore

Le autorità di certificazione

La procedura di certificazione coinvolge l'autorità di certificazione.

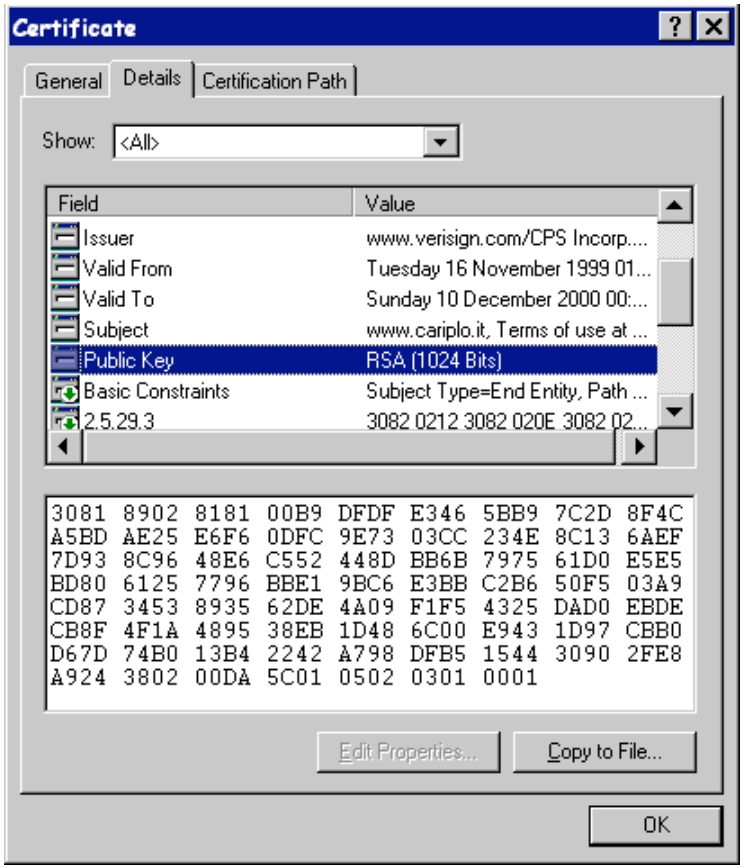
L' autorità deve procedere a:

- identificare la persona che fa la richiesta;
- rilasciare il certificato digitale che associa ad una persona identificata una chiave pubblica;
- pubblicare il certificato in un apposito registro;

La scelta del legislatore

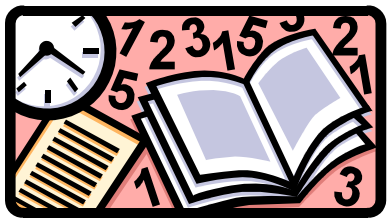
Certificato Digitale

- AC
- Periodo di validità
- Nominativo
- Chiave pubblica
- Informazioni aggiuntive
- ... ...



La scelta del legislatore

La validazione temporale



Per poter opporre a terzi la data e l'ora del documento informatico si ricorre al procedimento di validazione temporale

La scelta del legislatore

La marca temporale

La validazione temporale si ottiene mediante apposizione al documento informatico della marca temporale:

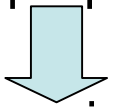
- su richiesta dell'utente il sistema di validazione temporale apporrà la marca temporale al documento;
- la validità della marca temporale potrà essere verificata utilizzando la chiave pubblica del sistema di validazione.

La scelta del legislatore

le fasi di produzione della marca temporale

l'hash del documento viene inviato dal richiedente al certificatore

il certificatore appone la marca temporale cioè aggiunge la data e l'ora e la cifra con la propria chiave privata



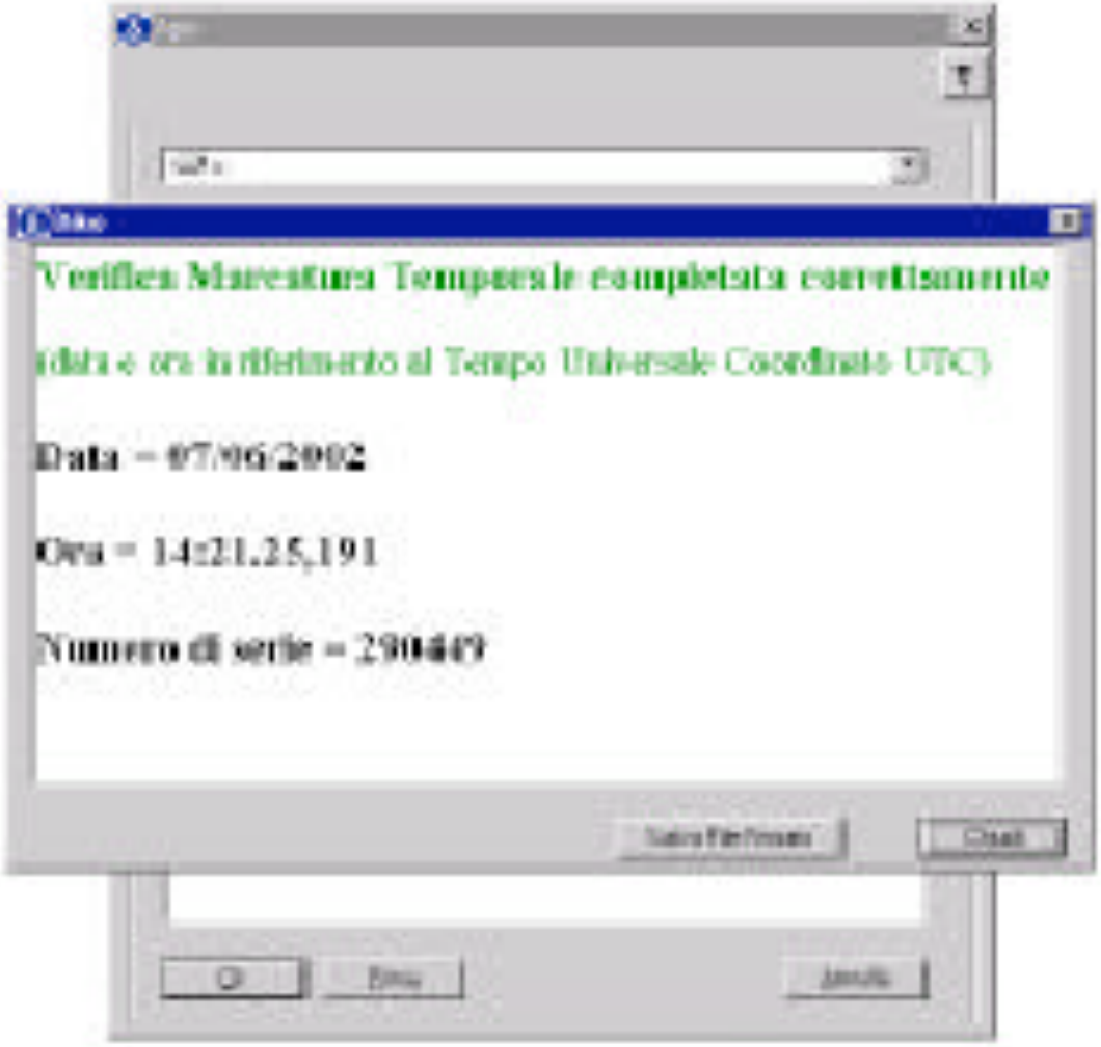
la marca temporale viene inviata al richiedente che la allega al documento

La scelta del legislatore

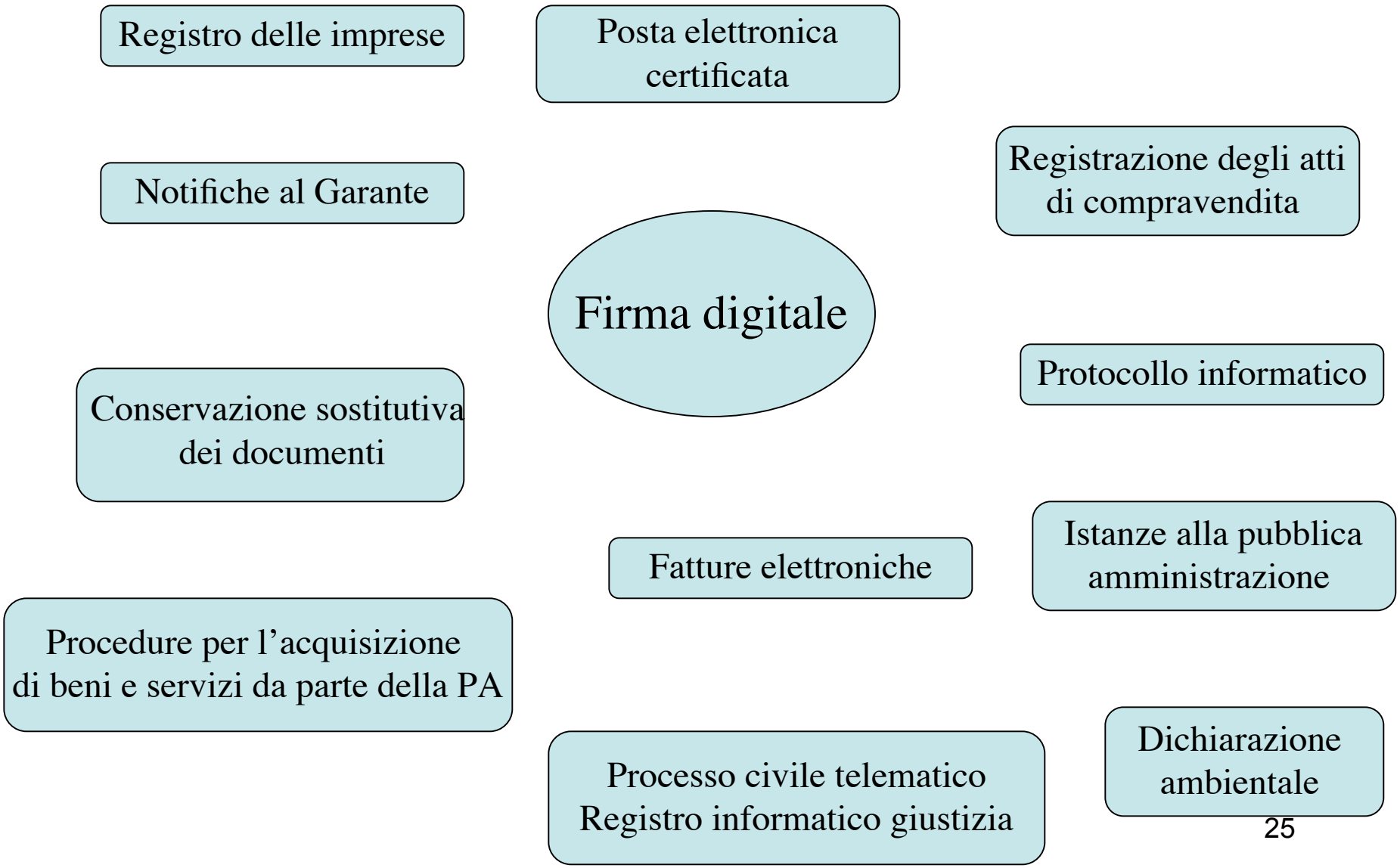
La marca temporale

- data
- ora
- n.serie della marca

.....



Contesti in cui è previsto l'uso della firma digitale



Diritto all’uso delle tecnologie

Articolo 3

I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice.

esempi di applicazione

*la conservazione sostitutiva dei documenti contabili e fiscali ai sensi della delibera CNIPA 11/04 e del DM 23 gennaio 2004

*la fattura elettronica ai sensi del decreto legislativo 52/04

* posta certificata ai sensi del DPR 68/05 e del DM 2.11.05

I principi in materia di conservazione

- Codice civile

(art. 2220)

I libri, i repertori e le scritture (…) di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del codice e secondo le regole tecniche

! Sono conservati anche a fini tributari

- D.lgs. 82/05

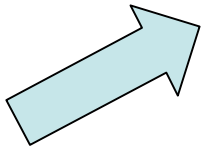
(art. 43)

I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

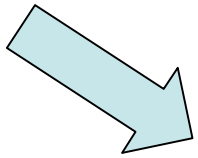
Le regole sono fissate nella delibera Cnipa 11/04 e nel D.M. 23 gennaio 04

La conservazione sostitutiva

conservazione



documenti informatici



documenti analogici

documenti informatici

documenti statici non modificabili

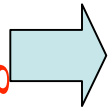
memorizzazione	**conservazione**	**esibizione**
su supporto leggibile nel tempo ordine cronologico senza soluzione di continuità tra i periodi di imposta funzioni di ricerca determinate	firma elettronica qualificata e marca temporale sull'insieme dei documenti o sull'evidenza informatica contenente l'impronta o le impronte dei documenti o dell'insieme di essi del responsabile della conservazione	su supporto cartaceo o informatico nel luogo di conservazione spedito per via telematica

ogni 15 giorni per le fatture almeno annualmente per gli altri documenti

Documenti analogici

- memorizzazione dell'immagine del documento su supporto digitale
- ordine cronologico, senza soluzione di continuità tra i periodi di imposta
- firma elettronica qualificata e marca temporale sull'insieme dei documenti o sull'evidenza informatica contenente l'impronta o le impronte dei documenti o dell'insieme di essi da parte del responsabile della conservazione

documenti originali



- ulteriore apposizione del riferimento temporale e della firma elettronica qualificata del pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine

La riproduzione dei documenti informatici su supporto idoneo

riversamento diretto	**riversamento sostitutivo**
processo che trasferisce uno o più documenti conservati da un supporto ad un altro, non alterando la loro rappresentazione digitale	processo che trasferisce uno o più documenti conservati da un supporto ad un altro, alterando la loro rappresentazione digitale
non sono previste particolari modalità	documenti digitali e analogici conservati: firma digitale e riferimento temporale del responsabile documenti digitali con firma e documenti analogici originali unici: firma digitale e riferimento temporale anche del pubblico ufficiale

La posta elettronica certificata

Art. 48

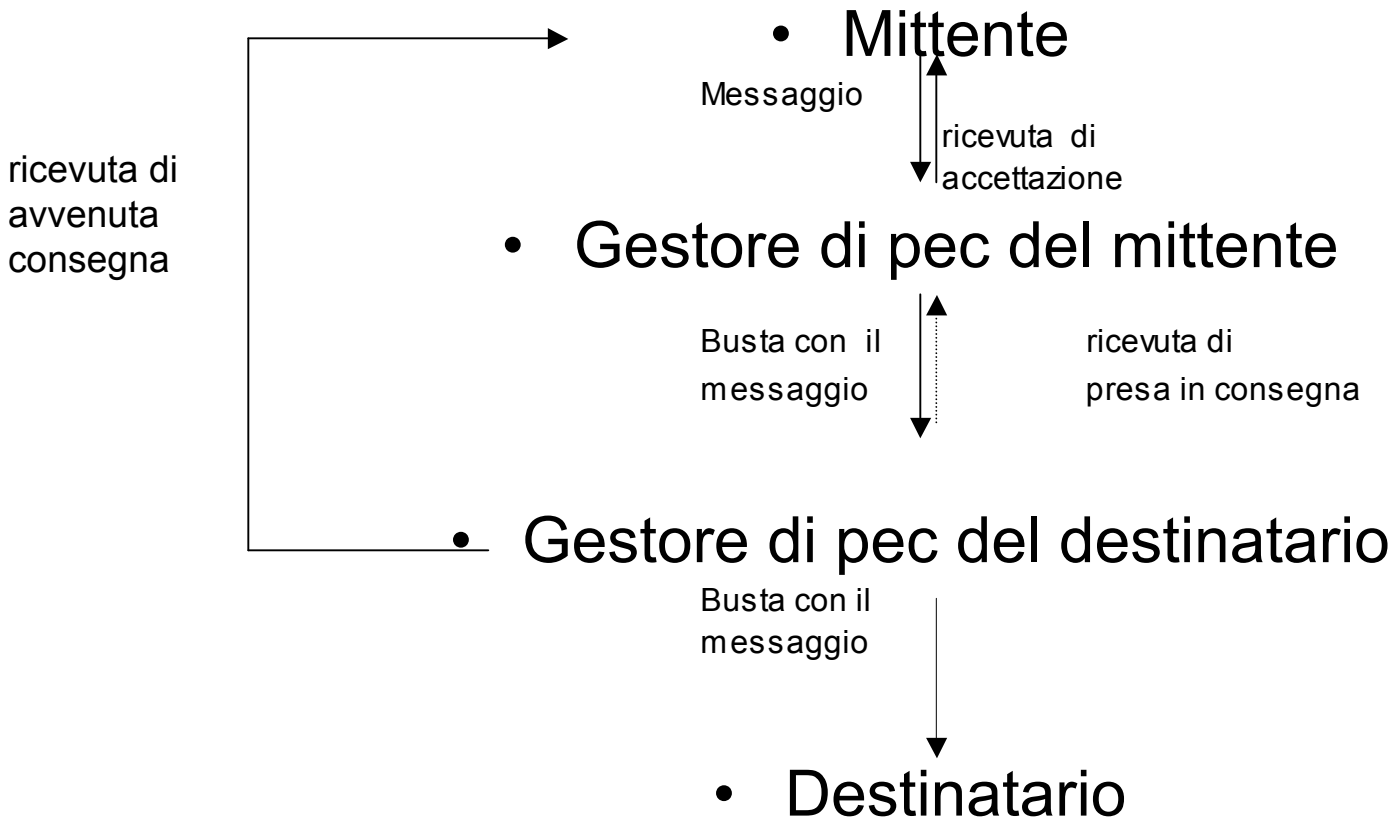
1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del dpr 68/05.
2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al dpr 68/05 ed alle relative regole tecniche.

Le condizioni

1. Utilizzo di un indirizzo valido
    1. Indirizzo valido è quello dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni
    2. Indirizzo valido è quello dichiarato ai fini di ogni singolo rapporto intrattenuto tra privati e tra questi e le pubbliche amministrazioni
2. Valersi di uno dei gestori inclusi nell'elenco pubblico

- Non è sufficiente l'indicazione dell'indirizzo di pec nella corrispondenza
- Le imprese possono dichiarare l'esplicita volontà di accettare l'invio di pec con iscrizione sul RI
- Le modalità della dichiarazione sono stabilite dalle regole tecniche

Le modalità



Se il Gestore del mittente e quello del destinatario corrispondono il Gestore del mittente provvede all'invio diretto al destinatario

Le ricevute

- Ricevuta di accettazione
  - Prova l'avvenuta spedizione del messaggio
  - Contiene il riferimento temporale
  - E' firmata con firma digitale del Gestore
- Ricevuta di avvenuta consegna
  - Prova l'avvenuta consegna nella casella postale del destinatario
  - Contiene il riferimento temporale
  - E' firmata con firma digitale del Gestore
  - Può contenere anche la copia completa del messaggio di pec consegnato

La fattura elettronica

- Il d.lgs. 52/04 consente la produzione e la conservazione delle fatture su supporto informatico.

La fattura elettronica

Condizioni:

1. Accordo con il destinatario

   È possibile trasmettere la fattura elettronica solo con il consenso del destinatario

2. Attestazione della data

   Si ricorre al riferimento temporale

3. Autenticità dell'origine
4. Integrità del contenuto

   } firma digitale

5. Non deve contenere macroistruzioni o codice eseguibile