Informatica giuridica

Lezione 5
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

Ad oggi la norma di riferimento è il d.lgs. 82/05
Codice dell'amministrazione digitale

Precedenti

In precedenza vi erano stati dei provvedimenti normativi che avevano riconosciuto, in contesti specifici, valore giuridico al documento informatico:

- il d.lgs. 241/90 in materia di procedimento amministrativo e di accesso ai documenti, riporta la seguente definizione di documento amministrativo: *"ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale";*
- il d.l. 357/94 modifica l'art. 2220 del codice civile stabilendo che *"Le scritture e documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti"*
- il d.lgs. 580/93 Riordino delle camere di Commercio, che istituisce il Registro delle Imprese, stabilisce che

"La predisposizione, la tenuta, la conservazione e la gestione, secondo tecniche informatiche, del registro delle imprese ed il funzionamento dell'ufficio sono realizzati in modo da assicurare completezza ed organicità di pubblicità per tutte le imprese soggette ad iscrizione, garantendo la tempestività dell'informazione su tutto il territorio nazionale."

L'obiettivo del legislatore

Creare le condizioni perché il documento informatico abbia le stesse caratteristiche del documento cartaceo:

- Possibilità di verificare la provenienza del documento;
- Possibilità di verificare l'integrità del documento.

Il percorso del legislatore italiano e europeo

- Il legislatore italiano affronta per primo il tema del riconoscimento del valore giuridico del documento elettronico e lo fa riconoscendo tale valore solo al documento sottoscritto con firma digitale(1997)
- Il legislatore europeo interviene sulla materia riconoscendo valori diversi a seconda che si ricorra alla firma semplice o alla firma avanzata (1999). Ciò in considerazione di due aspetti:
  - Non si può vincolare il valore del documento ad una sola soluzione tecnologica, oltrettutto la più rigorosa;
  - Ci possono essere contesti in cui il rigore richiesto dalla firma digitale non è necessario perché i requisiti richiesti possono essere garantiti in altro modo
- Il legislatore italiano recepisce la direttiva comunitaria sposandone l'approccio, anche se con diversi interventi normativi e passaggi spesso confusi

La legge disciplina:

- l'efficacia probatoria
- la forma dei documenti informatici (intesi come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti)

attribuendo loro valore diverso a seconda che:

*siano utilizzati o meno strumenti di firma;

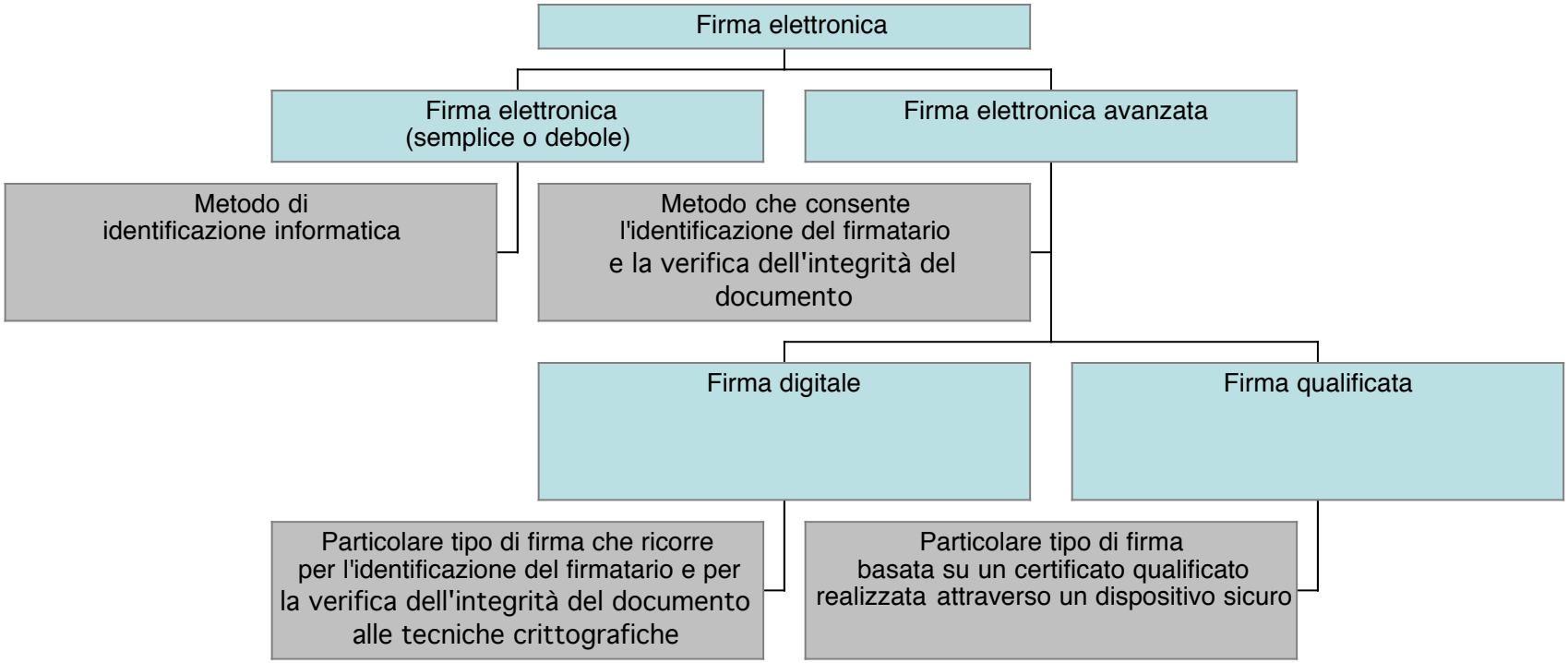
*quale strumento di firma venga utilizzato.

Il documento informatico sottoscritto

Secondo il codice dell'amministrazione digitale, il documento informatico può essere sottoscritto con:

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

Tipi di firma



Documento informatico	**Documento informatico con firma elettronica**	**Documento informatico con firma elettronica avanzata**	**Documento informatico con firma digitale**	**Documento informatico con firma elettronica qualificata**
Forma				
Liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, **integrità ed immodificabilità**			Le scritture private di cui all'art. 1350 c.c. (che richiedono la forma scritta) sono sottoscritte a pena di nullità con firma elettronica qualificata o con firma digitale	
Efficacia probatoria				
Liberamente valutabile in giudizio tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, **integrità e immodificabilità**		Efficacia prevista dall'art. 2702 del codice civile che così recita: "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"		

Firma digitale e altre firme

- Fino a febbraio 2013 la soluzione tecnologica che ha avuto specifica disciplina regolamentare è stata quella corrispondente alla firma digitale. Le altre firme, pur identificate dalla norma, non erano disciplinate a livello regolamentare.
- Con il d.p.c.m. 22 febbraio 2013 si sono stabilite le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali
- Ad oggi, quindi, l'ordinamento ha predisposto la disciplina per le firme elettroniche avanzate, per le firme qualificate e per quelle digitali.

Firma qualificata e firma digitale

- Secondo le regole tecniche recentemente approvate la firma qualificata e la firma digitale fanno entrambe ricorso ad un sistema di chiavi crittografiche asimmetriche.
- Differiscono tra loro per i diversi livelli di sicurezza imposti nella creazione dei dispositivi di firma. Nella presente lezione tali aspetti non verranno approfonditi.

Vediamo di comprendere cos'è un sistema crittografico a simmetrico

Crittografia

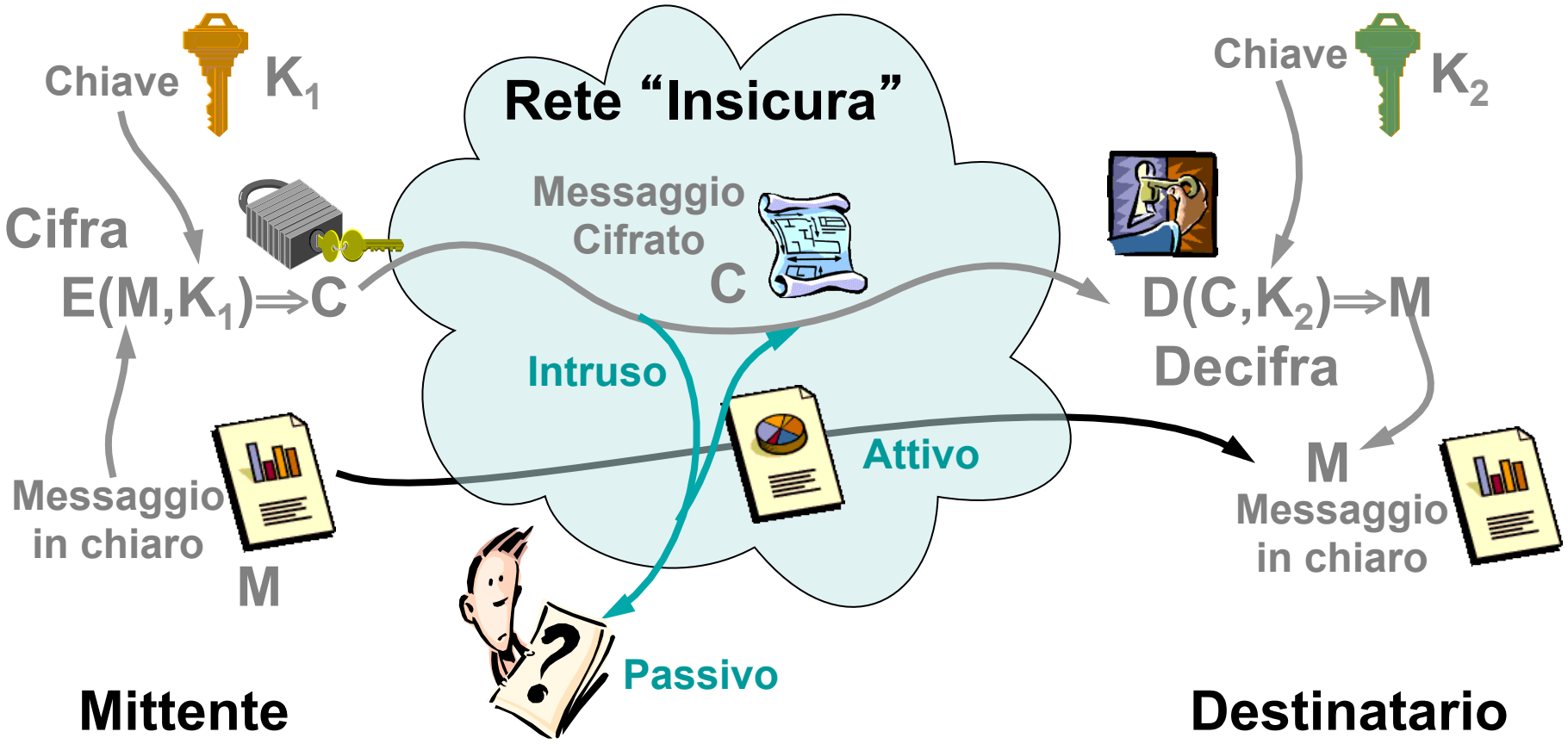
La firma digitale e la firma qualificata utilizzano tecniche di crittografia asimmetrica.

- Cos'è la crittografia?

La parola significa "scrittura nascosta"

Si tratta di metodi con cui si rende un messaggio comprensibile solo a persone determinate

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

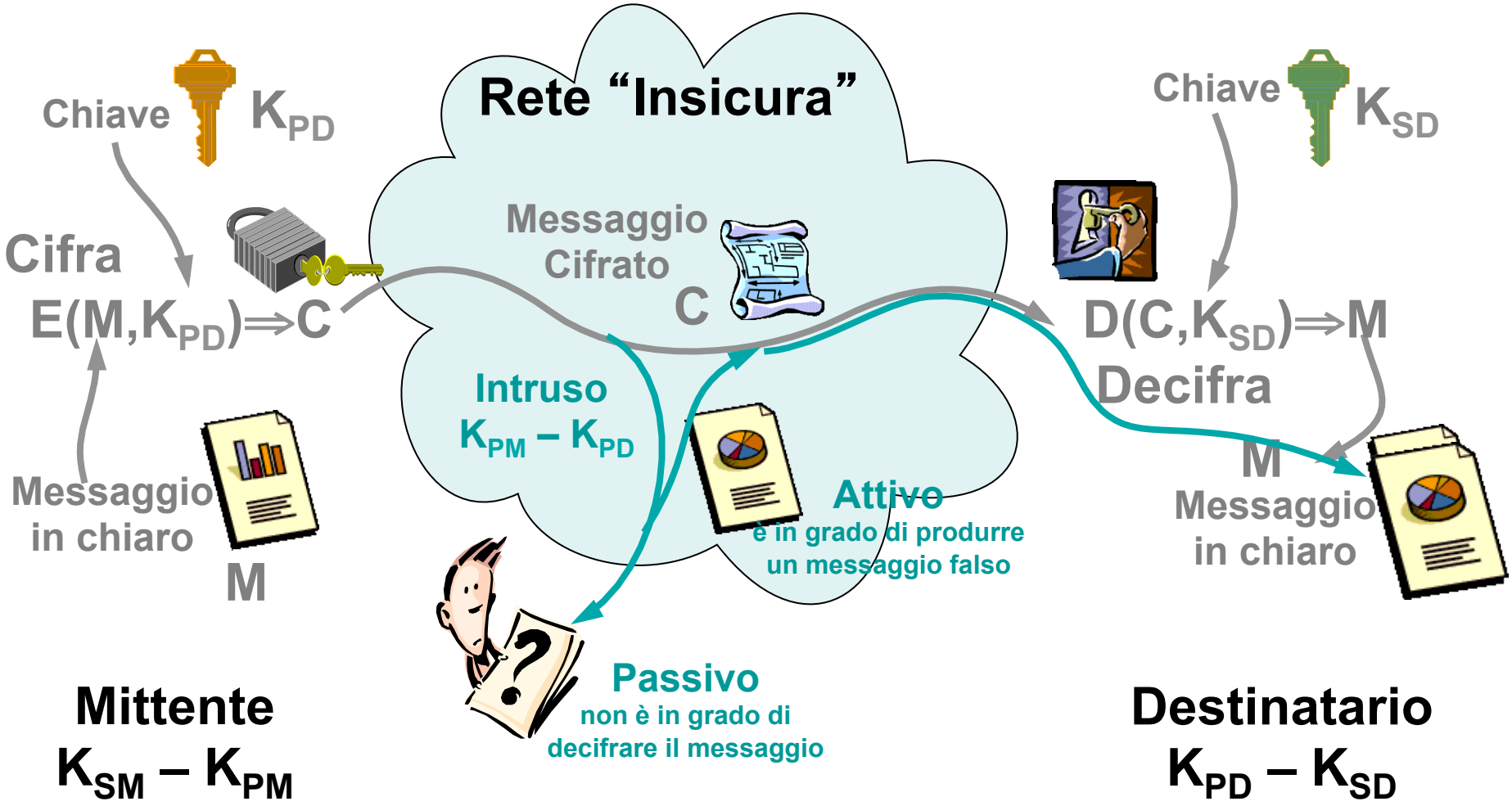
La crittografia: aspetti tecnici

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)!!

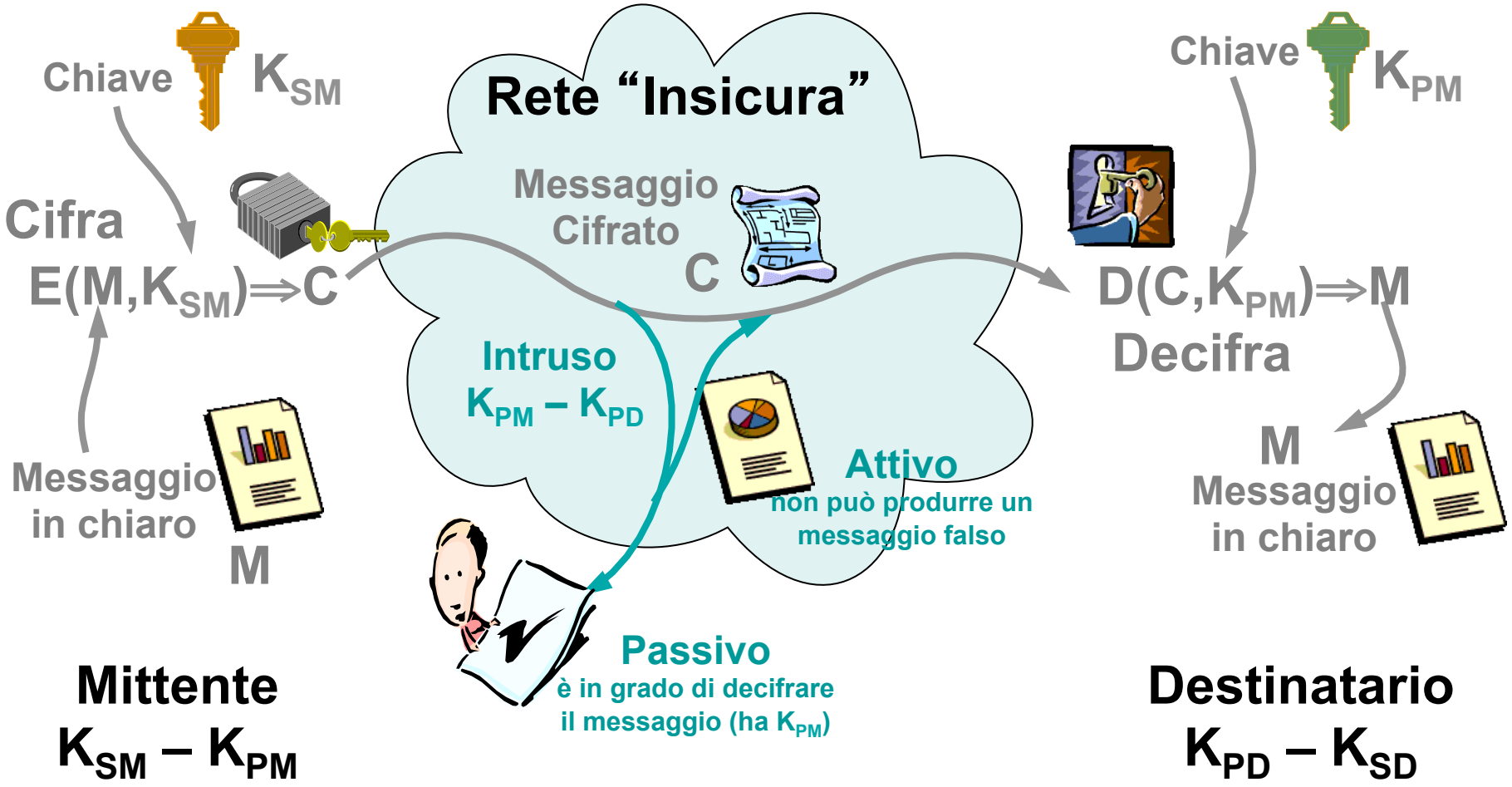
La crittografia: aspetti tecnici

Riservatezza & Integrità

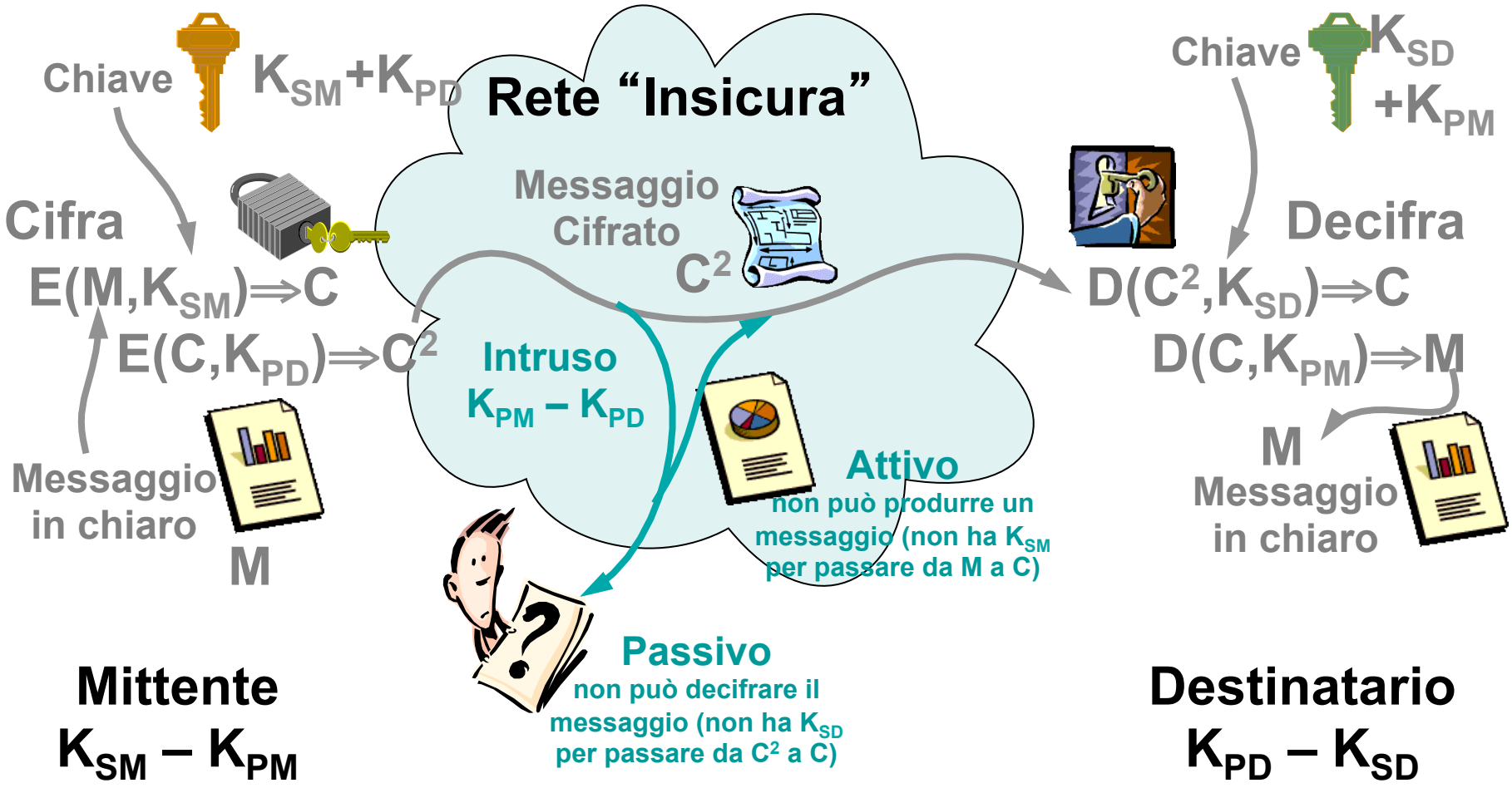


La crittografia: aspetti tecnici

Garanzia di provenienza & Integrità



Riservatezza & Integrità & Provenienza____



Le tecniche di crittografia asimmetrica

- consentono :
  - di assicurare la riservatezza del messaggio (il messaggio viene crittato con la chiave pubblica del destinatario in modo che solo lui possa decrittarlo visto che è l'unico a disporre della corrispondente chiave privata);
  - di identificare la provenienza del messaggio (il mittente critta il messaggio con la propria chiave privata in modo che possa essere decrittato con la corrispondente chiave pubblica. Chi lo riceve, decrittando il messaggio con la chiave pubblica del mittente, sa con certezza che solo quest'ultimo poteva crittarlo con la sua chiave privata)
  - di verificare l'integrità del messaggio (se il messaggio crittato con una delle chiavi viene modificato non può più essere decrittato con l'altra. In questo modo si ha evidenza che il messaggio non è lo stesso dell'originale)

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:

- 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 firma qualificata e la firma digitale

- La firma digitale (e la firma qualificata) utilizza tecniche a crittografia asimmetrica ma non si limita a questo.
- La firma digitale (e la firma qualificata) è infatti costituita dall'hash del documento (impronta) a cui si applica la chiave privata di chi sottoscrive.

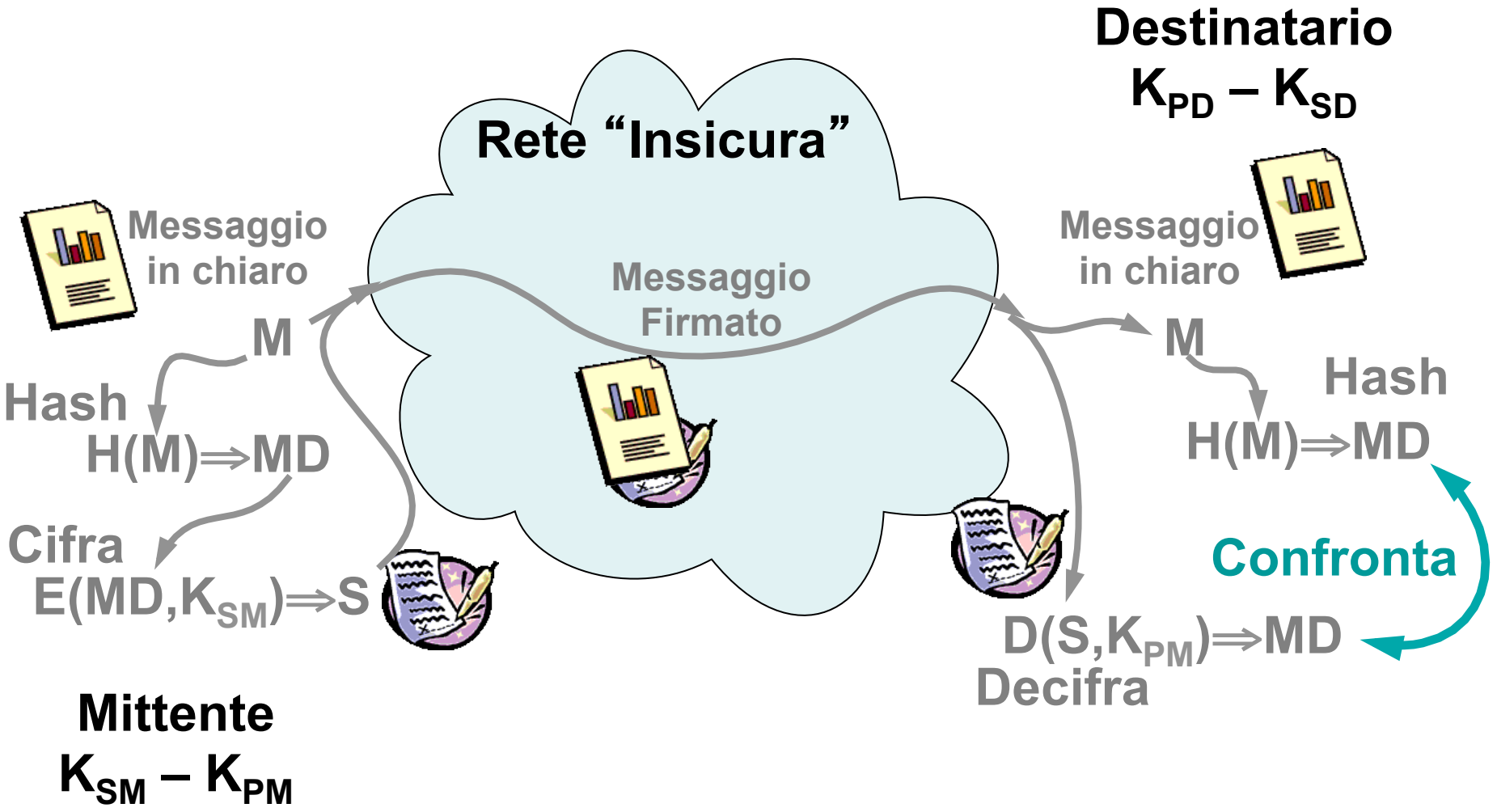
La funzione *hash* (H) genera un riassunto (*digest o impronta*) del messaggio (M), tale per cui:

- 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, in quanto un documento modificato non corrisponderà più all'impronta originaria.

All'impronta del documento si applica la chiave privata di chi sottoscrive. In questo modo si ha garanzia che il documento provenga da chi ha apposto la sua chiave privata, che si può verificare solo con la corrispondente chiave pubblica.

Firma Digitale (e firma qualificata): hash + chiave privata



La firma digitale e la firma qualificata

- Diversamente dalla firma autografa, non si appone in calce al documento ma costituisce un file diverso dal documento (allegato a quest'ultimo) la cui correlazione al documento è garantita dall'impronta digitale.
- Diversamente dalla firma autografa, la firma digitale (e la firma qualificata), essendo costituita dall'impronta del documento, è ogni volta diversa.

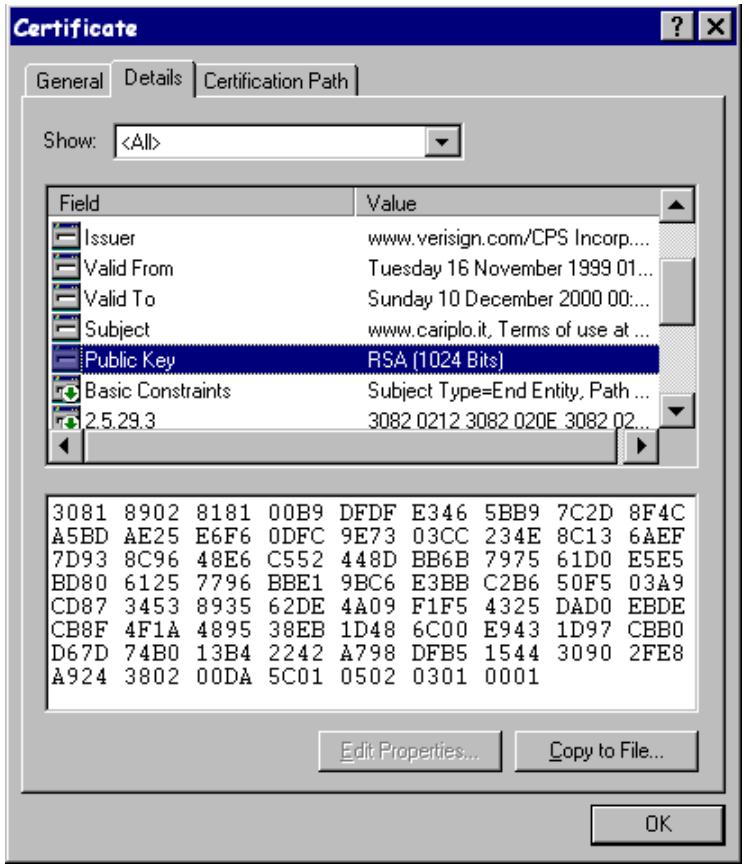
La chiave pubblica, a cui corrisponde la chiave privata utilizzata per la firma digitale (e la firma qualificata), deve essere depositata presso un'autorità di certificazione che:

- identifica il titolare;
- iscrive in un apposito registro il nominativo del titolare e la chiave pubblica utilizzata;
- emette un certificato da cui risulta la corrispondenza tra la chiave pubblica e il titolare

Certificato Digitale

- Autorità di Certificazione
- Periodo di validità
- Nominativo
- Chiave pubblica
- Informazioni aggiuntive
- ... ...

Il certificato ha una durata (2/3 anni). Trascorso tale periodo il certificato scade



Dispositivi sicuri

Su smart card e chiave usb risiedono, protetti da codici di accesso: chiave privata e certificato digitale

Smart card

Chiave USB

La smart card e la chiave USB non sono la firma digitale ma i supporti su cui risiedono gli strumenti di firma

Valore della firma digitale (e firma qualificata) nel tempo

- La coppia di chiavi e il relativo certificato hanno una durata di validità (ad oggi due/tre anni). Trascorsi gli anni di validità, il titolare modifica la propria coppia di chiavi.
- Si pone quindi un problema: trascorsi gli anni di validità come verificare la firma?
- E' possibile verificarla al sussistere di tre condizioni:
  - L'apposizione della marca temporale al documento firmato durante il periodo di validità del certificato;
  - La tenuta nel tempo presso le autorità di certificazione dei certificati (ad oggi per venti anni) in modo da poter individuare, nota la data attraverso la marca temporale, il certificato che il sottoscrivente utilizzava in quel periodo;
  - La conservazione nel tempo (per un periodo non inferiore a venti anni) delle marche temporali prodotte dal sistema di validazione.

La marca temporale

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

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 validazione 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 marca temporale

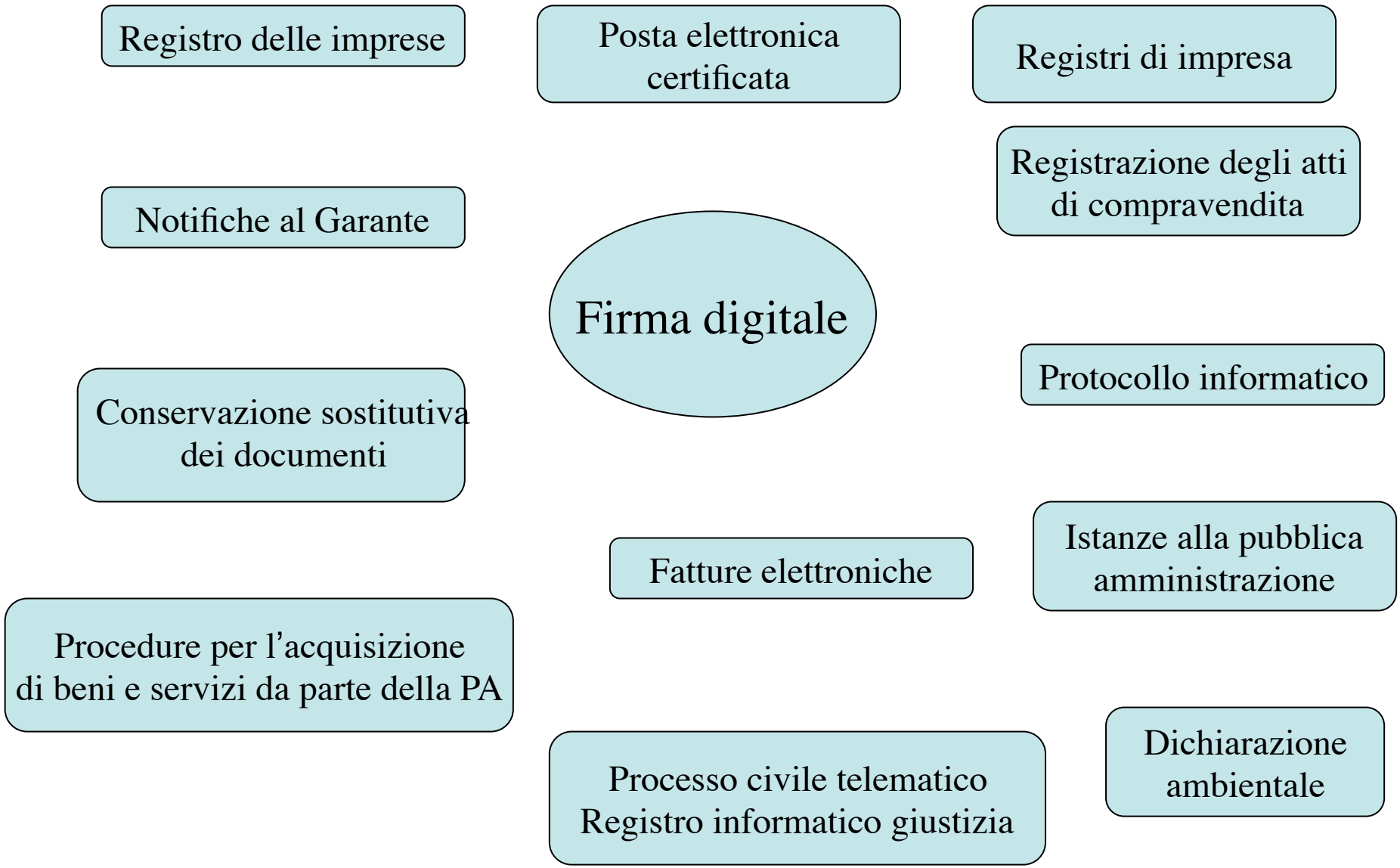
- data
- ora
- n.serie

  della marca

  .....

Firmatario ICDTS200605PR02
Ente Certificatore InfoCert Time Stamping Authority 4
Marca Temporale del 19.05.2006 15:08:09.283 GMT
S/N Marca 9073186 (0x8A7222)
Marca Temporale Valida

Contesti in cui è previsto l'uso della firma digitale o della firma qualificata



Firma elettronica avanzata

- La realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva.

Firma elettronica avanzata

Le soluzioni di firma elettronica avanzata garantiscono:

a) l'identificazione del firmatario del documento;

b) la connessione univoca della firma al firmatario;

c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;

d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;

e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

f) l'individuazione del soggetto che utilizza il sistema nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali;

g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;

h) la connessione univoca della firma al documento sottoscritto.

Limiti all’uso della firma elettronica avanzata

La firma elettronica avanzata realizzata in conformità con le disposizioni delle regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che decide di ricorrere a tale soluzione nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali.

Il sottoscrittore è quindi un soggetto terzo che per motivi istituzionali, societari o commerciali intrattiene rapporti con colui che ricorre a tale soluzione.

Esempio di firma elettronica avanzata

Un esempio di firma elettronica avanzata è la firma grafometrica cioè la sottoscrizione autografa apposta su tablet con una particolare pen drive

Tuttavia, non tutte le firme grafometriche sono firme elettroniche avanzate, ma solo quelle che rispondono alle condizioni previste dalle regole tecniche.

Così, ad esempio, la firma apposta su un tablet nel caso di consegna di un pacco da parte del corriere non è una firma elettronica avanzata mentre lo è quella per l'effettuazione di un bonifico in banca.

La differenza sta nel fatto che nel primo caso, generalmente, il corriere non identifica con documento di riconoscimento il firmatario, non conserva copia del documento, non gli richiede di aderire alle condizioni del servizio, non effettua una conservazione dei documenti conforme alla normativa specifica vigente in materia di conservazione. Nel secondo caso, la banca, generalmente, effettua le operazioni sopra elencate, e molte altre, che soddisfano i requisiti di sicurezza, non solo tecnologica, ma anche organizzativa, previsti dal processo di firma elettronica avanzata.

La posta elettronica certificata

Valore legale e aspetti tecnici

La posta elettronica certificata

Art. 48 d.lgs. 82/05

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.

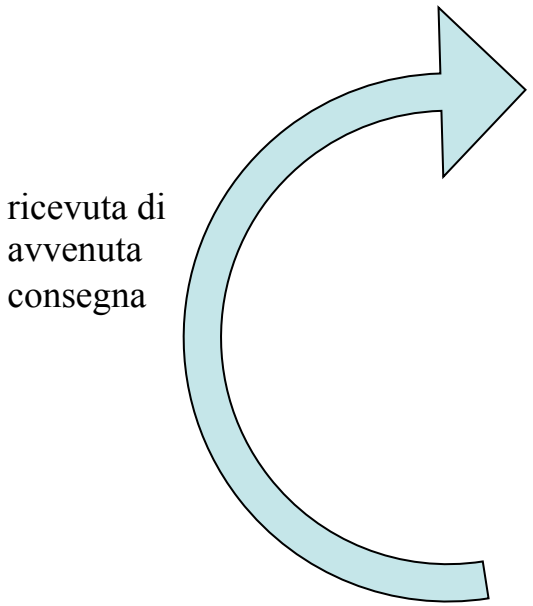
Cos’è la PEC?

- E’ il servizio di posta elettronica che fornisce la ricevuta di invio e di consegna, producendo gli stessi effetti della raccomandata con ricevuta di ritorno

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
3. Mittente e destinatario debbono possedere un indirizzo di pec

Le modalità



- Mittente

Messaggio

ricevuta di
accettazione

- Gestore di pec del mittente

Busta con il
messaggio

ricevuta di
presa in consegna

- Gestore di pec del destinatario

Busta con il
messaggio

- Destinatario

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

Due aspetti importanti

1) Se il destinatario non possiede la pec ma un indirizzo di posta elettronica, l'invio mediante un indirizzo di pec produce l'effetto della raccomandata semplice (il mittente dispone della ricevuta di accettazione)
2) Pur non essendo un obbligo di legge, i servizi di pec generalmente prevedono che la ricevuta di consegna comprenda anche copia completa del messaggio. Diversamente dalla raccomandata con ricevuta di ritorno, usando la pec si ha prova non solo che un documento è stato consegnato ma anche di quale documento sia stato consegnato.

Bibliografia

Dieci lezioni per capire e attuare l'e-government
(a cura di Luca De Pietro)
Marsilio Editore, 2011
Capitolo 3
Firma digitale, posta elettronica certificata e dematerializzazione
(Daniela Redolfi)