Il valore giuridico del documento informatico

Lezione n. 5

Il percorso del legislatore italiano e europeo

- 1997 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
- 1999 Il legislatore europeo interviene sulla materia riconoscendo valori diversi a seconda che si ricorra alla firma semplice o alla firma avanzata. 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
- 2002 Il legislatore italiano recepisce la direttiva comunitaria sposandone l'approccio, anche se con diversi interventi normativi e passaggi spesso confusi
- 2005 Viene emanato il Codice dell'amministrazione digitale che costituisce il testo unico in materia
- 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali
- 2013 Regole tecniche in materia di conservazione dei documenti informatici
- 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, validazione temporale dei documenti informatici (dpcm 23.0.14)

Il Regolamento UE Eidas

Entra in vigore a partire dal 1. luglio 2016

Fissa:

- i criteri per il riconoscimento reciproco delle modalità di identificazione elettronica tra pubbliche amministrazioni europee
- ii criteri per il riconoscimento reciproco dei servizi cosiddetti "fiduciari"
  - firma elettronica
  - sigillo elettronico
  - servizi di recapito
  - autenticazione dei siti web

Il Regolamento UE Eidas

Riconoscimento reciproco dei sistemi di identificazione tra pubbliche amministrazioni europee:

- i singoli paesi indicano alla Commissione i sistemi di identificazione utilizzati specificando il livello di garanzia (basso, significativo o elevato). Il regolamento di esecuzione fissa i criteri per assegnare il livello considerando:
  - Registrazione
  - Gestione dei mezzi di identificazione
  - Autenticazione
  - Gestione e organizzazione
- è definito un quadro di interoperabilità in modo che una pa di un paese membro possa procedere all'autenticazione di un cittadino ricorrendo agli strumenti di identificazione stabiliti da un altro paese membro. Il regolamento di esecuzione prevede la costituzione di nodi che consentono lo scambio di informazioni necessarie ai sistemi di identificazione degli Stati di interoperare

Il Regolamento UE Eidas

Il servizio fiduciario è un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

- creazione, verifica e convalida di firme elettroniche, di sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
- creazione, verifica e convalida di certificati di autenticazione di siti web; o
- conservazione di firme, sigilli e certificati elettronici relativi a tali servizi.

Servizi fiduciari

- **Firma elettronica**

Dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare. Il firmatario è una persona fisica.

- **Sigillo elettronico**

Dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di tali dati. Il creatore di sigillo è una persona giuridica.

- **Validazione temporale**

Dati in forma elettronica che collegano altri dati in forma elettronica ad una particolare ora e data così da provare che questi ultimi esistevano in quel momento

Servizi fiduciari

- **Servizio elettronico di recapito certificato**

Servizio che consente la trasmissione di dati tra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, tra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.

- **Certificato di autenticazione di siti web**

Attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato

Tutti i servizi fiduciari possono essere erogati in forma qualificata, se provengono da un prestatore qualificato, iscritto in uno specifico elenco e hanno i requisiti fissati dal Regolamento. I servizi fiduciari qualificati possono ricorrere ad un marchio specifico che li identifica.

Qualche domanda per focalizzare

- Cosa disciplina il Regolamento Eidas?
- Quali sono i servizi fiduciari disciplinati dal Regolamento Eidas?
- Cos’è il sigillo elettronico?

Documento informatico e firme elettroniche

Documento elettronico e informatico

- Reg. Eidas

Documento elettronico:

Qualsiasi contenuto conservato in forma elettronica, in particolare testo, registrazione sonora, visiva o audiovisiva

- CAD

Documento informatico:

Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

Il documento informatico (CAD)

Il documento informatico è formato mediante una delle seguenti principali modalità:

- Redazione tramite l'utilizzo di appositi strumenti software
- Acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico
- Registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione informatica di moduli o formulari resi disponibili all'utente
- Generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi di dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Valore giuridico del documento informatico (CAD)

Il documento informatico da chiunque formato
è valido e rilevante agli effetti di legge

La legge disciplina:

- l'efficacia probatoria
- la forma dei documenti informatici

attribuendo loro valore diverso a seconda che:

*siano utilizzati o meno strumenti di firma;

*quale strumento di firma venga utilizzato.

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"		

Le firme elettroniche secondo il Reg. Eidas

Firma elettronica

Dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

Firma elettronica avanzata

Firma elettronica che soddisfa ai seguenti requisiti:

- è connessa univocamente al firmatario
- è idonea a identificare il firmatario
- è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo
- è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati

Firma elettronica qualificata

Firma elettronica avanzata creata da un dispositivo per la creazione della firma elettronica qualificata e basata su un certificato qualificato di firma elettronica

Le firme elettroniche secondo il CAD

Firma elettronica

Insieme di dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici utilizzati come metodo di identificazione

Firma elettronica avanzata

Insieme di dati in forma elettronica allegati oppure connessi ad un documento informatico che consentono l'identificazione del firmatario del documento, e garantiscono la connessione univoca al firmatario creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati siano stati successivamente modificati

Firma elettronica qualificata

un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

Firma digitale

Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica rispettivamente di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

Firma qualificata e firma digitale

- Secondo le regole tecniche 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.

Qualche domanda per focalizzare

- La registrazione informatica delle informazioni acquisite mediante compilazione di un form sul web è un documento informatico?
- Quale firma devo utilizzare perchè il documento informatico faccia prova fino a querela di falso?
- Il documento informatico privo di firma ha efficacia probatoria?

I sistemi crittografici

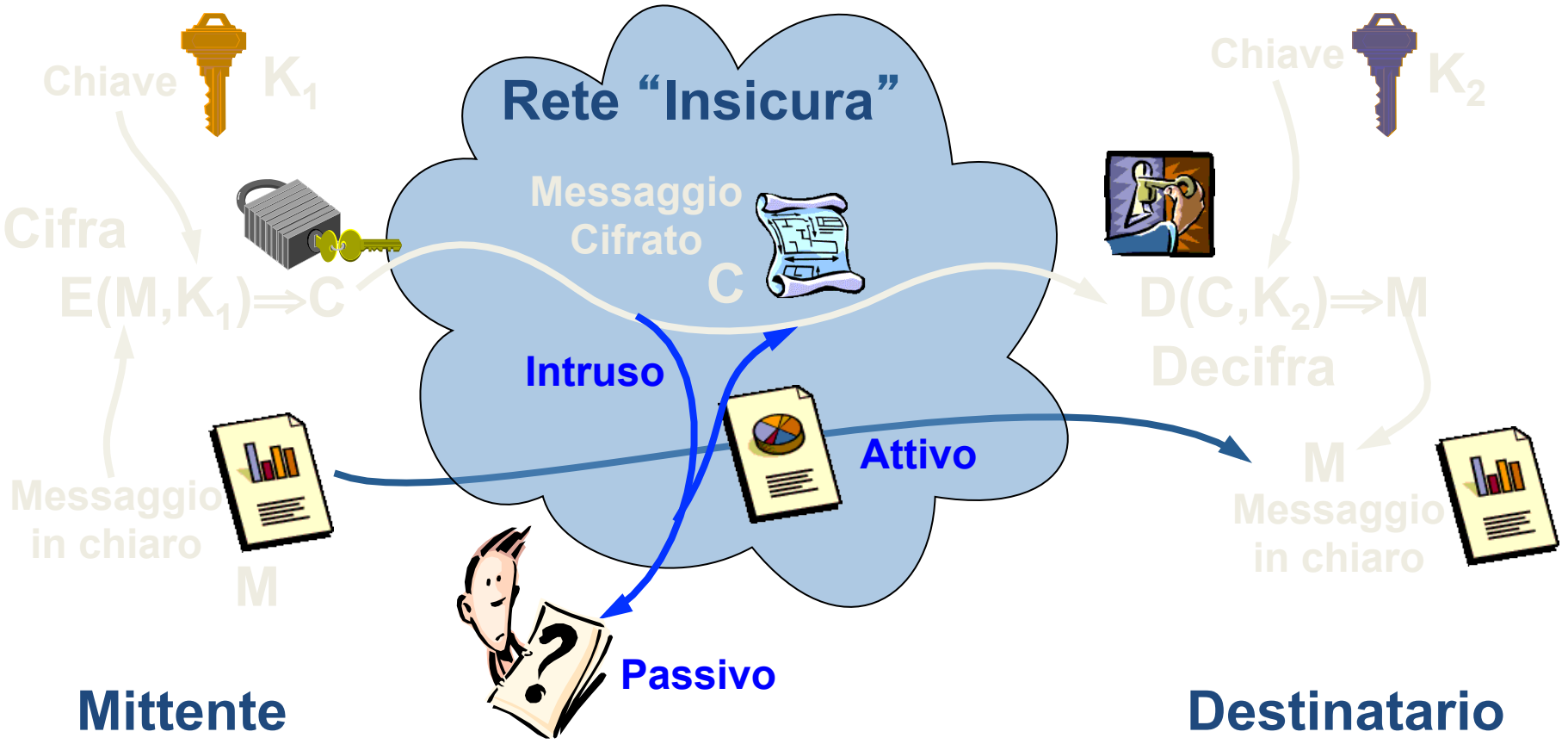
Crittografia

La parola significa “scrittura nascosta”

Si tratta di metodi, inizialmente sviluppati per rendere un messaggio comprensibile solo a persone determinate, e quindi garantirne la riservatezza.

Ma vengono usati anche per verificare l’integrità del messaggio e la sua provenienza, come nel caso della firma qualificata e della firma digitale

Crittografia simmetrica



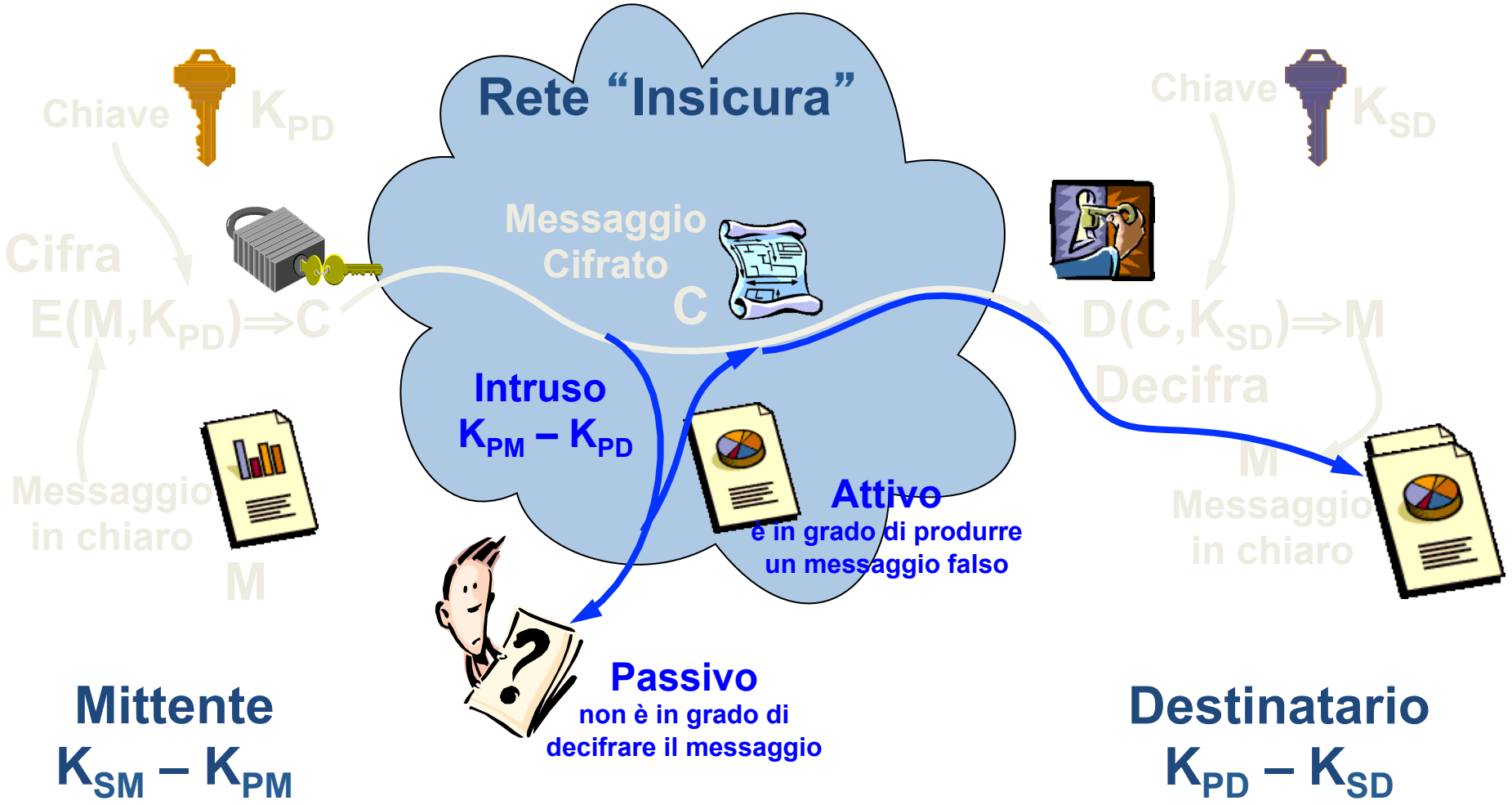
Crittografia Simmetrica

- 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

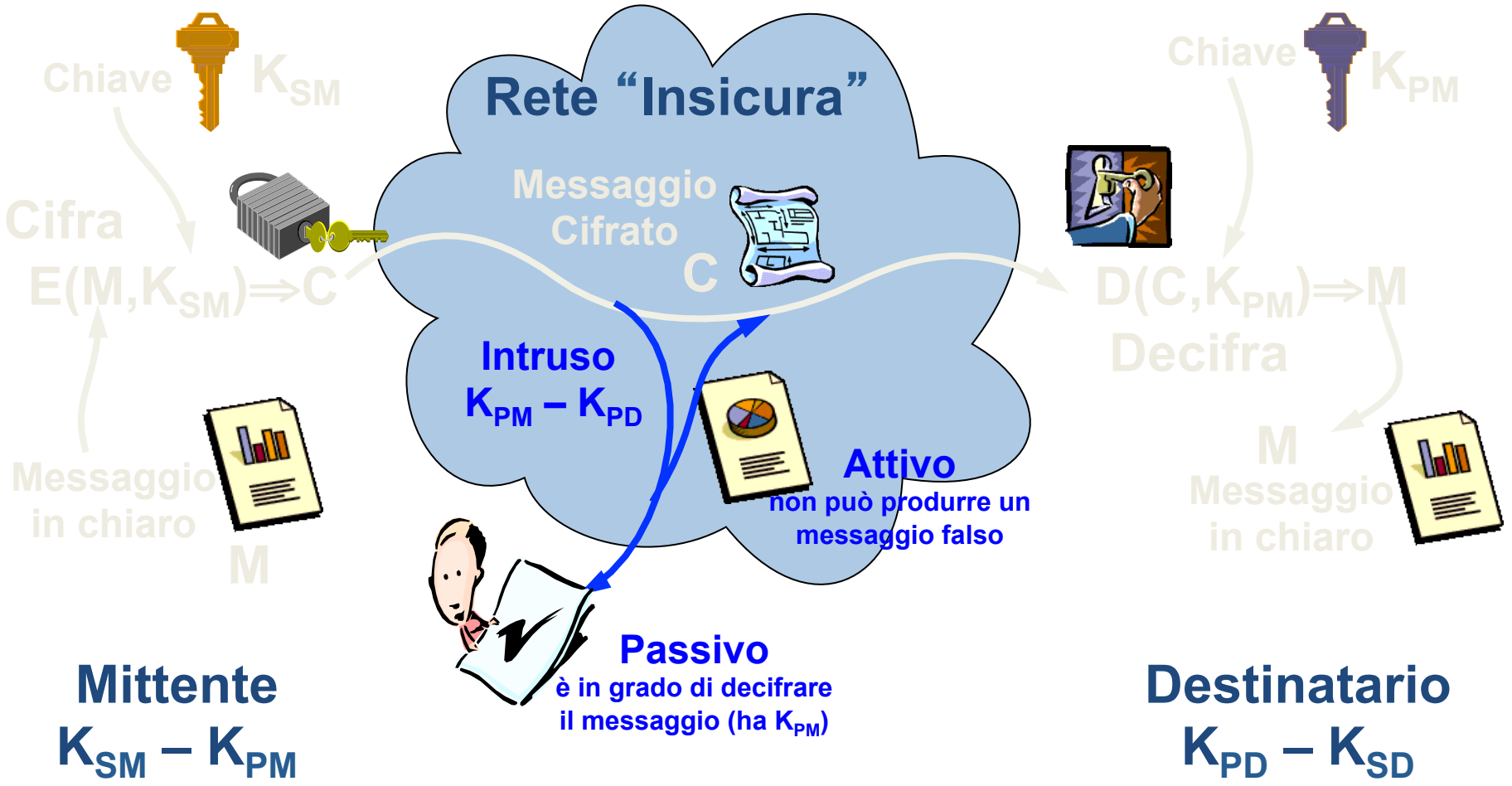
Crittografia Asimmetrica

- 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)

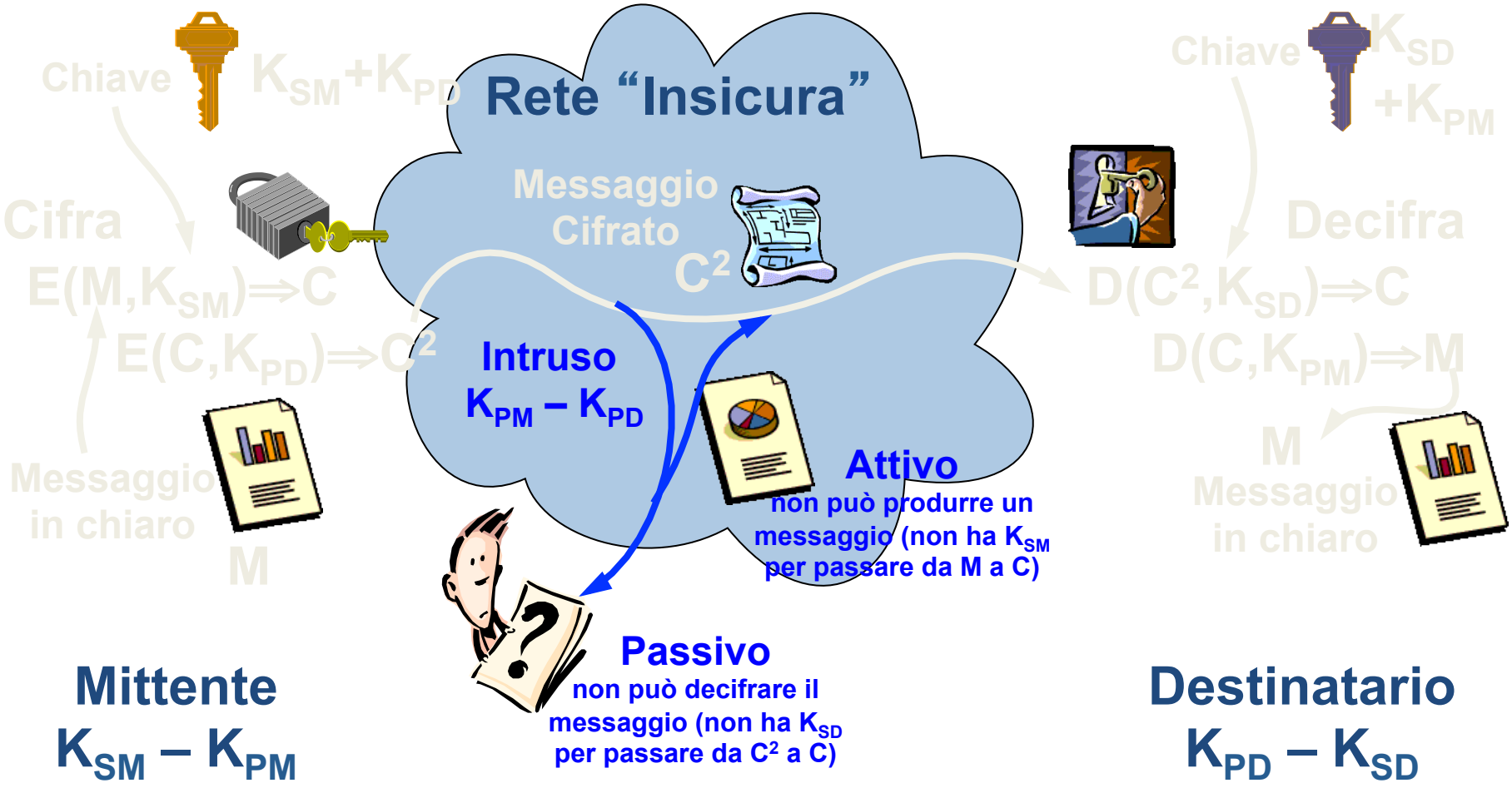
Riservatezza & Integrità



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)

Qualche domanda per focalizzare

- Un sistema a crittografia simmetrica quante chiavi utilizza?
- In un sistema a crittografia asimmetrica se voglio garantire la riservatezza del documento quale chiave applico?
- In un sistema a crittografia asimmetrica se voglio garantire la provenienza del documento quale chiave applico?

Firma digitale e firma qualificata

firma qualificata e firma digitale

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

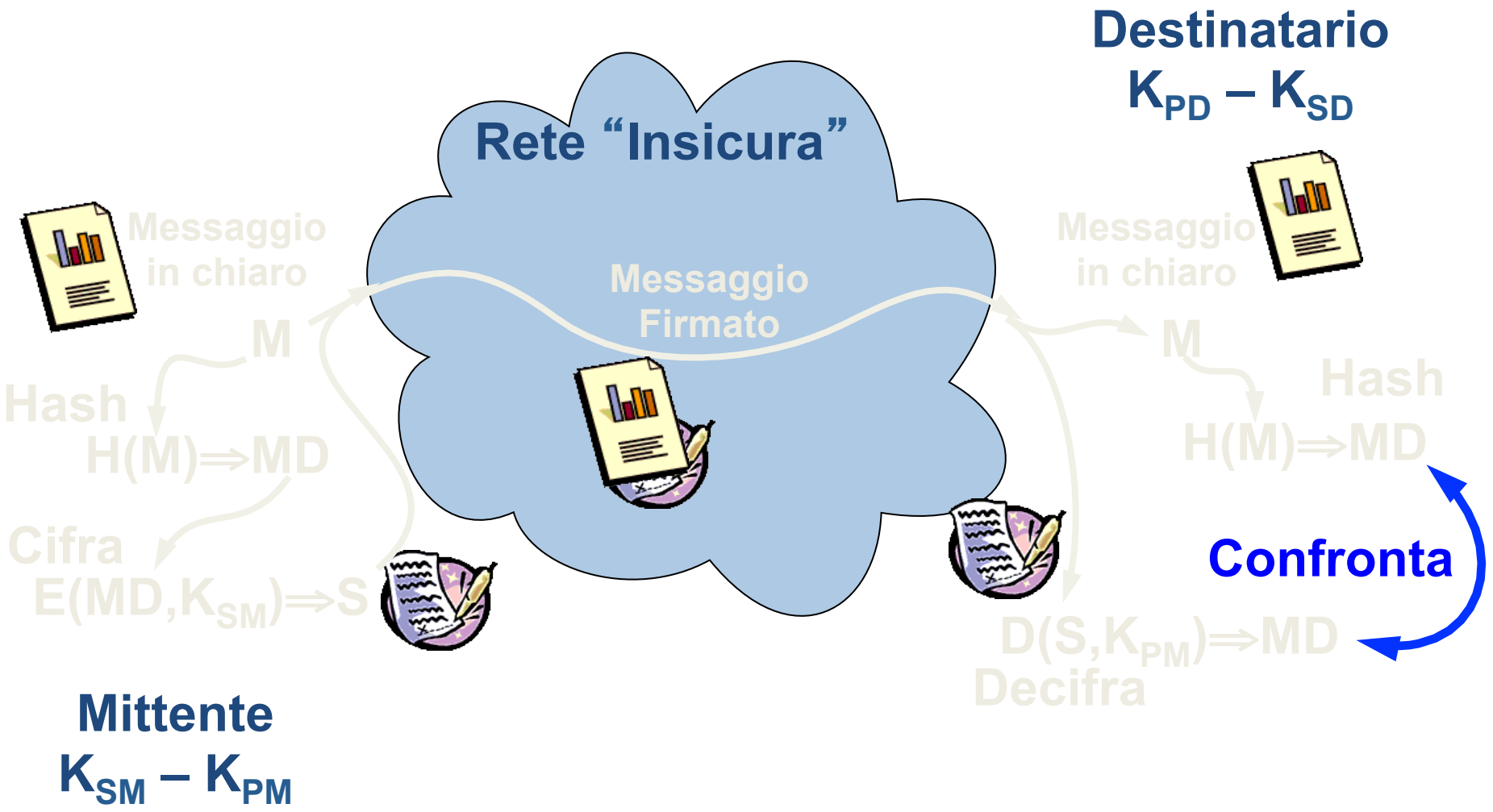
La funzione *hash* (H) genera un riassunto (*digest o impronta*) del messaggio (M), tale per cui:

- 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

Firma Digitale e firma qualificata: impronta + chiave privata



La firma digitale e la firma qualificata

Diversamente dalla firma autografa, la firma digitale (e la firma qualificata), essendo costituita dall’impronta del documento, è ogni volta diversa.

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:

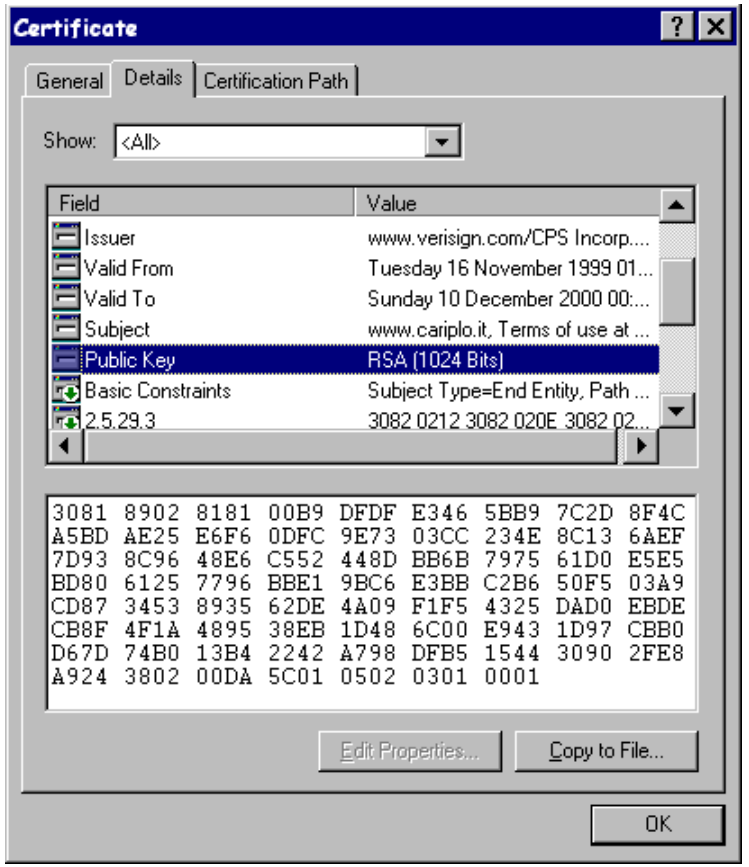
La chiave pubblica, a cui corrisponde la chiave privata utilizzata per la firma digitale (e la firma qualificata), deve essere depositata presso un'autorità di certificazione che:

- 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

La verifica delle firme

La firma è verificata mediante uno specifico software o mediante dei servizi via web messi a disposizione da autorità di certificazione.

Ad esempio:

- https://www.firma.infocert.it/utenti/verifica.php.
- https://postecert.poste.it/verificatore/service?type=0

Qualche domanda per focalizzare

- In cosa consiste la firma digitale?
- Quali sono i compiti delle autorità di certificazione?
- Cos’è il certificato digitale?

Copie e duplicati

Copia per immagine su supporto informatico di documento analogico

- La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia
- la copia per immagine di uno o più documenti analogici può essere sottoscritta con firma digitale o firma elettronica qualificata da chi effettua la copia
- Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche hanno la **stessa efficacia probatoria degli originali** da cui sono tratte.
  - **se la loro conformità all'originale non è espressamente disconosciuta**
  - **se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi**

Copia su supporto informatico di documenti amministrativi analogici

- **L'attestazione di conformità della copia informatica** di un documento amministrativo analogico, formato dalla pubblica amministrazione, ovvero da essa detenuto, **può essere inserita nel documento informatico contenente la copia informatica**. Il documento informatico così formato è **sottoscritto con firma digitale o firma elettronica qualificata del funzionario delegato**.
- L'attestazione di conformità anche nel caso di uno o più documenti amministrativi informatici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la

Duplicati

- Il duplicato informatico di un documento informatico è prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la **stessa sequenza di bit del documento informatico di origine**.
- I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento

Copie ed estratti informatici di documenti informatici

- La copia e gli estratti informatici di un documento informatico sono prodotti attraverso **l'utilizzo di uno dei formati idonei** di cui all'allegato 2 al presente decreto, mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia
- La copia o l'estratto di uno o più documenti informatici, ha la stessa **efficacia probatoria**

Copie analogiche di documenti informatici

- Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno **la stessa efficacia probatoria dell'originale** da cui sono tratte se la loro **conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato**.
- Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta

Copie analogiche di documenti amministrativi informatici, i Glifi

- Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.
- Risponde ai requisiti il cosiddetto **Glifo**, cioè il contrassegno basato su codici grafici bidimensionali generato elettronicamente, costituito da una sequenza di bit, codificata mediante una tecnica grafica e idonea a rappresentare un documento amministrativo informatico o un suo estratto o una sua copia o un suo duplicato o i suoi dati identificativi.
- Il contrassegno è disciplinato dalla circolare Agid n. 62/2013 “Linee guida per il contrassegno generato elettronicamente”

Qualche domanda per focalizzare

- A quali condizioni la copia scannerizzata di un documento cartaceo ha la stessa efficacia probatoria dell'originale?
- Che differenza c'è tra copia informatica e duplicato informatico?
- Cos'è un glifo?

Validazione temporale

Valore della firma digitale e firma qualificata nel tempo

Le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Valore della firma digitale e firma qualificata nel tempo

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: fasi di produzione

l’hash del documento viene inviato dal richiedente al sistema di validazione temporale

il sistema di validazione 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 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

Validazione temporale

CAD

Validazione temporale

Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi

Reg. Eidas

Validazione temporale

Dati in forma

Altre modalità di validazione temporale

Oltre 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 in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata
- il riferimento temporale ottenuto attraverso

Qualche domanda per focalizzare

- Una volta scaduto il certificato di firma, la firma che era stata apposta al documento informatico è ancora valida?
- In cosa consiste la marca temporale?
- Oltre alla marca temporale esistono altri modi per validare temporalmente un documento?

Firma elettronica avanzata

Firma elettronica avanzata

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

Perché le soluzioni adottate possano essere qualificate come soluzioni di firma elettronica avanzata è necessario che esse rispettino i seguenti requisiti

Firma elettronica avanzata

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)

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.

Le condizioni di utilizzo debbono essere previamente accettate per iscritto dal sottoscrittore

Firma grafometrica

Soluzione che prevede la memorizzazione dei dati comportamentali (dati biometrici) del sottoscrittore legati all'apposizione materiale della firma autografa. Sono acquisiti parametri quali la pressione esercitata, l'accelerazione, il grado di inclinazione della penna etc.

Soluzioni che prevedono la mera acquisizione dell'immagine della firma autografa non sono firme grafometriche. L'efficacia giuridica di questi tipi è quella prevista dagli articoli 2712 (Riproduzioni meccaniche) e 2719 (Copie fotografiche di scritture) del codice civile. Hanno quindi efficacia pari all'originale a meno che non siano disconosciute.

La firma grafometrica è una firma elettronica avanzata?

La soluzione deve essere valutata considerando i requisiti previsti dalle Regole tecniche per la qualifica di firma elettronica avanzata.

Sicuramente la firma grafometrica risponde al requisito del controllo esclusivo del firmatario del sistema di generazione della firma.

Gli altri requisiti debbono essere valutati considerando la soluzione proposta.

Sono presenti sul mercato soluzioni di firma grafometrica che possono qualificarsi come firma elettronica avanzata.

Soluzioni di firma elettronica avanzata

L'invio tramite posta elettronica certificata effettuato richiedendo la ricevuta completa sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata.

L'utilizzo della Carta d'Identità Elettronica, della Carta Nazionale dei Servizi, del documento d'identità dei pubblici dipendenti (Mod. ATe), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata per i servizi erogati in rete dalle pubbliche amministrazioni e per le istanze e le dichiarazioni presentate alla pa per via telematica

Qualche domanda per focalizzare

- La realizzazione di soluzioni di firma elettronica avanzata è soggetta ad autorizzazione?
- Quali sono i limiti all'uso della firma elettronica avanzata?
- La firma grafometrica è una firma elettronica avanzata?

La posta elettronica certificata

La posta elettronica certificata

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.

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.

Funzionamento

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

Condizioni

- Valersi di uno dei gestori inclusi nell’elenco pubblico
- Mittente e destinatario debbono possedere un indirizzo di pec

- 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)
- 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.

Ini-pec

Al fine di favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico.

2. L'Indice nazionale di cui al comma 1 è realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali.

3. L'accesso all'INI-PEC è consentito alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini tramite sito web e senza necessità di autenticazione. L'indice è realizzato in formato aperto, secondo la definizione di cui all'articolo 68, comma 3.

Comunicazioni

- **tra PA e imprese/professionisti**

Le comunicazioni possono essere inviate attraverso la posta elettronica certificata senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo

- **tra PA**

Le comunicazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

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

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

b) ovvero sono dotate di segnatura di protocollo

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche. E' in ogni caso esclusa la comunicazione a mezzo fax

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata

Qualche domanda per focalizzare

- Chi sottoscrive digitalmente la ricevuta di consegna?
- La ricevuta contiene il contenuto del messaggio o il documento allegato?
- La pubblica amministrazione per trasmettere una comunicazione ad un’impresa tramite pec ha bisogno della sua autorizzazione?