Cosa NON è la firma digitale

- La firma digitale non deve essere confusa, nel modo più assoluto, con la digitalizzazione della firma autografa, ovvero la rappresentazione digitale di un'immagine corrispondente alla firma autografa.

I servizi di sicurezza

In tutti gli scenari di scambio di informazione appare l'esigenza comune di soddisfare uno o più tra i seguenti requisiti di sicurezza:

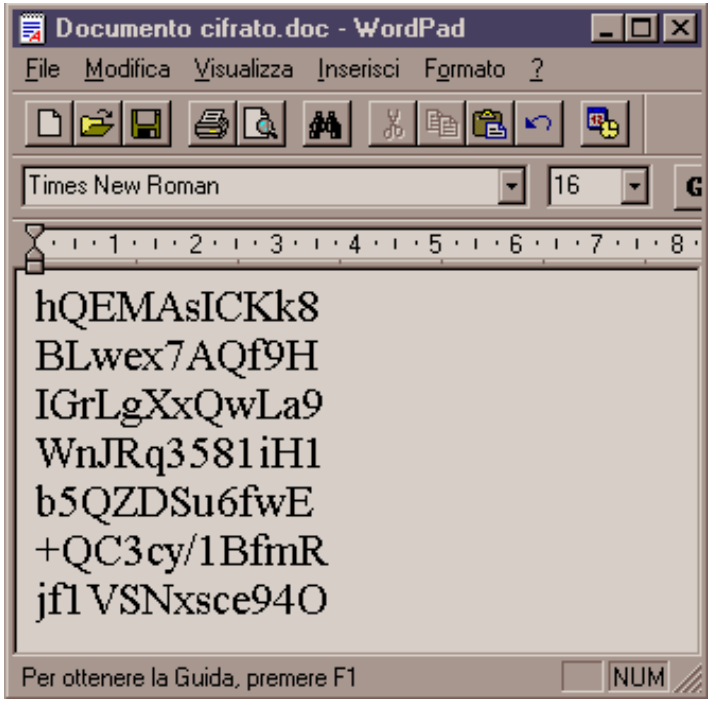
- autenticazione degli interlocutori
- confidenzialita' dei messaggi scambiati
- integrità dei messaggi scambiati
- non-ripudiabilita' dei messaggi scambiati

Autenticazione

- Anche nel mondo elettronico gli interlocutori devono avere a disposizione un mezzo che consenta loro di accertarsi dell'altrui identità, come già avviene nel mondo "fisico".
- In rete non solo le persone, ma anche i server e le applicazioni, devono essere autenticati.

Confidenzialità

- Si vuole un modo per scambiare messaggi che siano intelligibili solo a coloro ai quali sono destinati



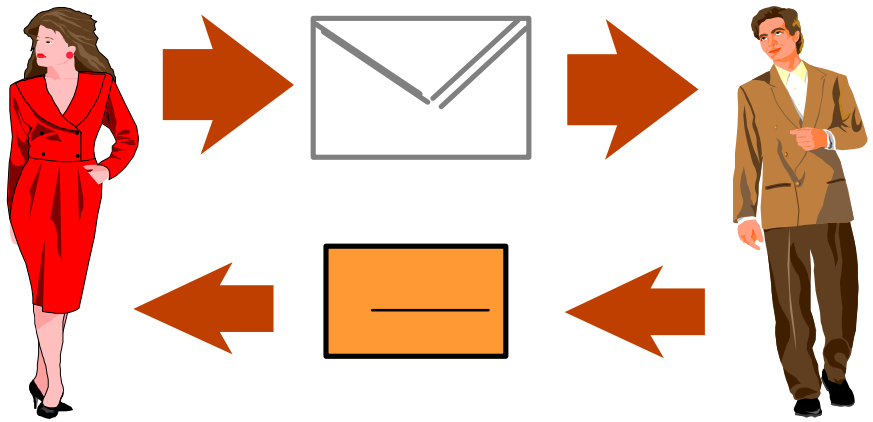
- Attualmente lo scambio riservato di dati viene realizzato mediante sistemi di cifratura
- Soltanto chi possiede la “chiave di lettura” può accedere al contenuto reale del messaggio

Integrità

- Si vuole avere garanzia che l'informazione scambiata non sia stata alterata
  - eventuali alterazioni del contenuto originale del messaggio devono essere sempre individuabili (cosa ne sarebbe, altrimenti, dei bonifici bancari…)
- L'obiettivo è impedire la alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali.

Non-ripudiabilità

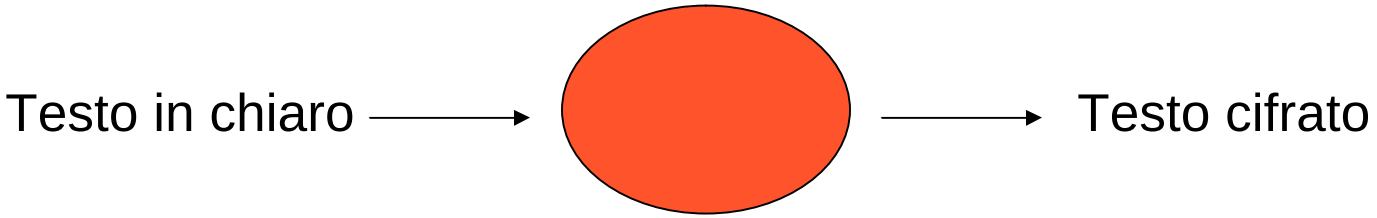
- Assicura che vengano raccolte e mantenute informazioni che provino l'origine e la ricezione di dati



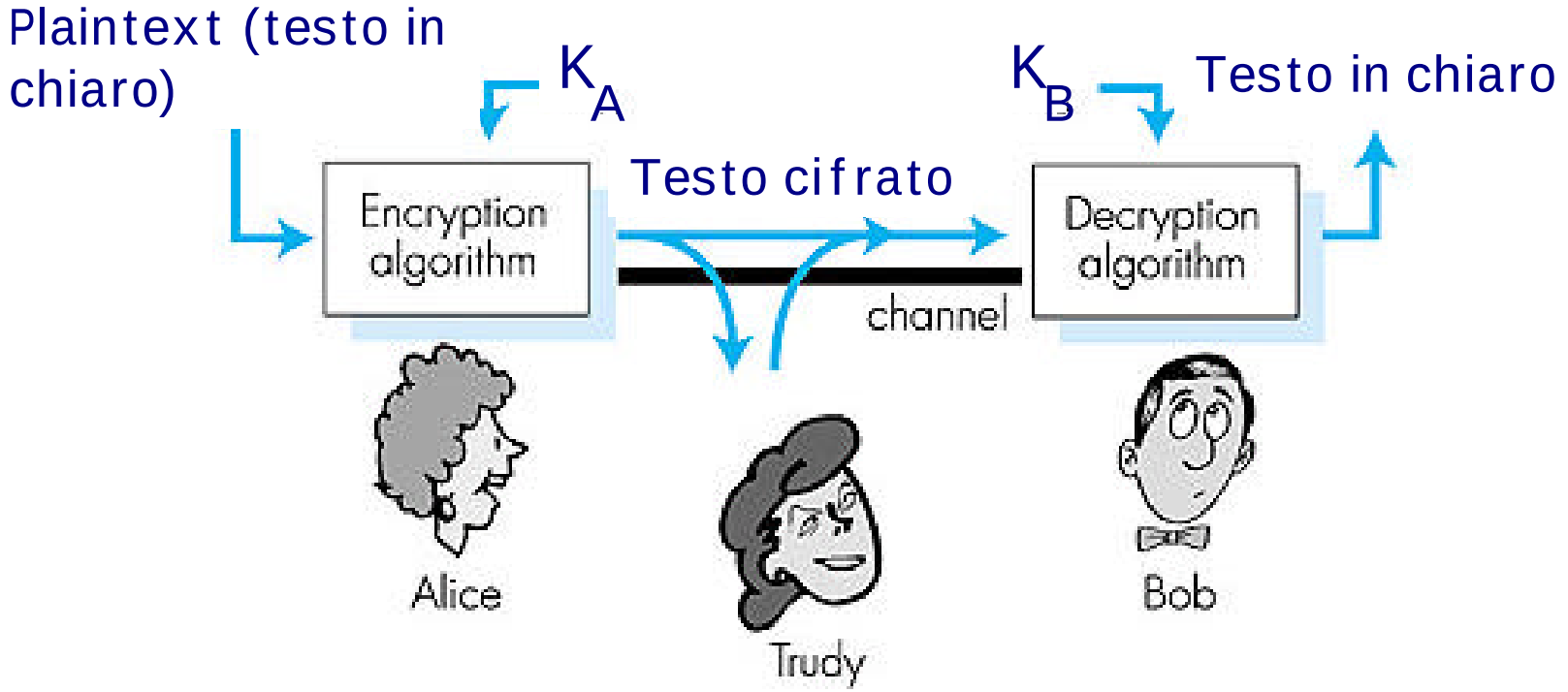
- Protegge il mittente contro la falsa affermazione del ricevente che i dati non sono stati ricevuti
- Protegge il ricevente contro la falsa affermazione del mittente che i dati non sono stati inviati

Le basi della crittografia

- Per **sistema crittografico** si intende un sistema in grado di cifrare e decifrare un messaggio attraverso l'uso di un algoritmo (metodo di calcolo) e di una chiave (una stringa segreta alfanumerica).
- Il messaggio che dovrà essere cifrato viene chiamato **testo in chiaro** (plaintext) mentre il risultato dell'algoritmo crittografico **testo cifrato** (ciphertext).



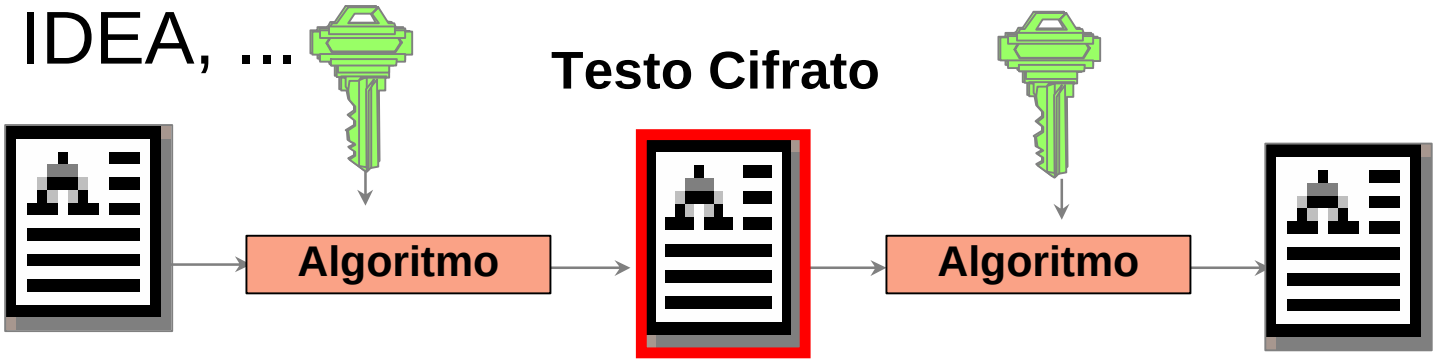
Crittografia: nomenclatura



- Gli algoritmi di crittografia possono essere classificati come
  - **simmetrici**, anche detti ***a chiave segreta*** *(o* ***privata***): usano la stessa chaive per codificare e decodificare
  - **asimmetrici**, anche detti ***a chiave pubblica:*** usano due chiavi distinte: una per codificare e una per decodificare***.***

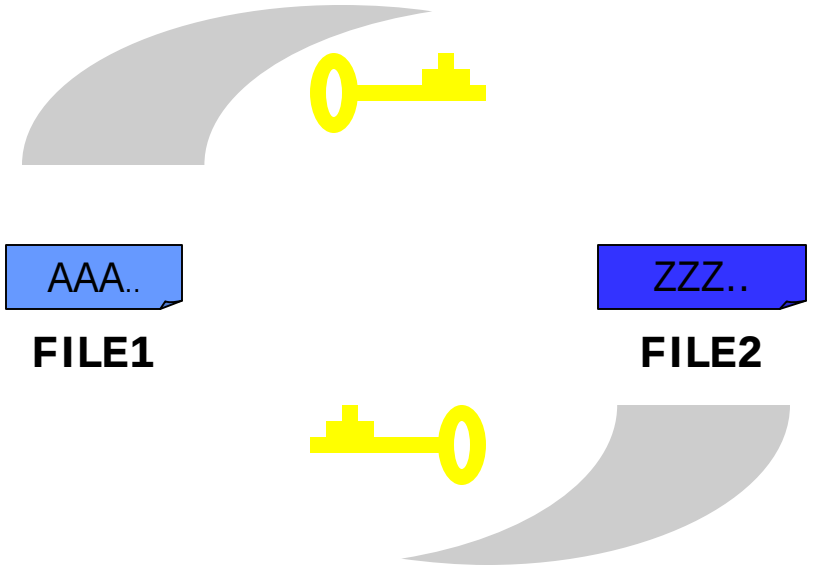
La crittografia simmetrica

- Gli algoritmi a chiave simmetrica usano la stessa chiave per cifrare e decifrare
- Per scambiare informazioni cifrate, mittente e destinatario devono condividere prima la chiave segreta
- Esempi di algoritmi: **DES**, RC2, RC4, RC5, IDEA, ...



Gli algoritmi di crittografia simmetrica

- La stessa chiave serve per cifrare e per decifrare
- Una chiave non può decifrare un file cifrato con un'altra chiave
- La chiave è posseduta dal mittente e dal destinatario



I cifrari simmetrici

- Utilizzano la stessa chiave per cifrare (**encryption**) e decifrare (**decryption**) i messaggi.
- Hanno il problema della trasmissione della chiave tra mittente e destinatario.

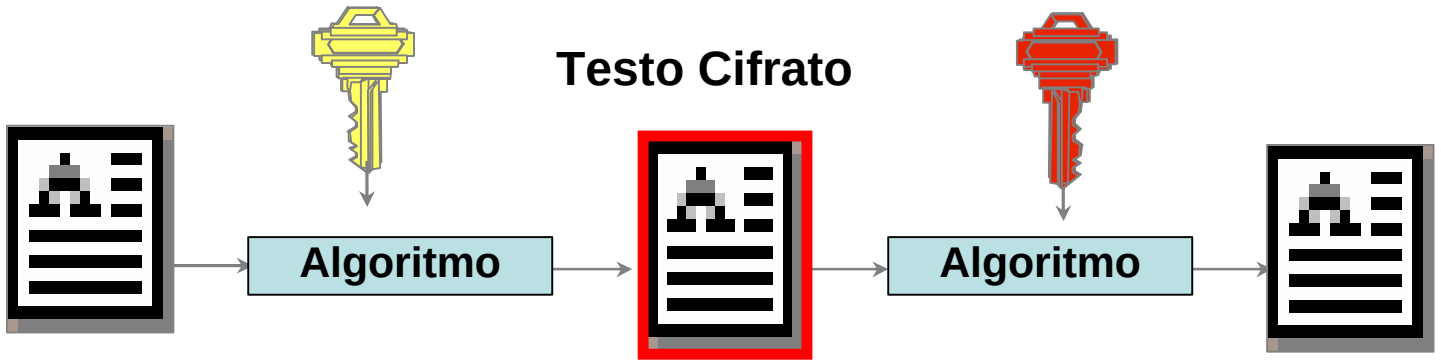
Gli algoritmi di crittografia simmetrica

- Vantaggi:
  - Efficienza
- Svantaggi:
  - Necessità di prevedere una chiave per ogni coppia di interlocutori (ogni soggetto è costretto a possedere molte chiavi)
  - Problemi di sicurezza in fase di distribuzione della chiave

La crittografia asimmetrica

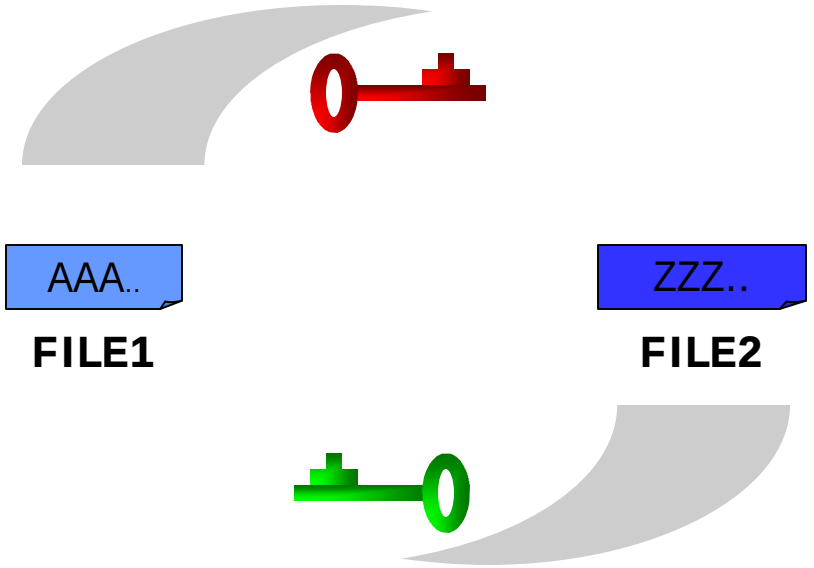
- Usa due chiavi diverse, che possono essere usate entrambe per cifrare e per decifrare, ma…

  i dati cifrati con una possono essere decifrati solo con l'altra
- la conoscenza di una chiave non fornisce informazioni sull'altra
- Esempi di algoritmi: **RSA**, EL GAMAL, ...



Gli algoritmi di crittografia asimmetrica

- Un documento cifrato con una chiave può essere decifrato con l'altra e viceversa
- Ogni chiave può cifrare o decifrare
- La chiave che cifra non può decifrare lo stesso file
- Una chiave è posseduta dal mittente (chiave **privata**) ed è segreta; l'altra chiave (chiave **pubblica**) è accessibile a tutti i destinatari



Le chiavi vengono generate in coppia da uno speciale algoritmo ed è impossibile ottenere una chiave a partire dall'altra.

Gli algoritmi di crittografia asimmetrica

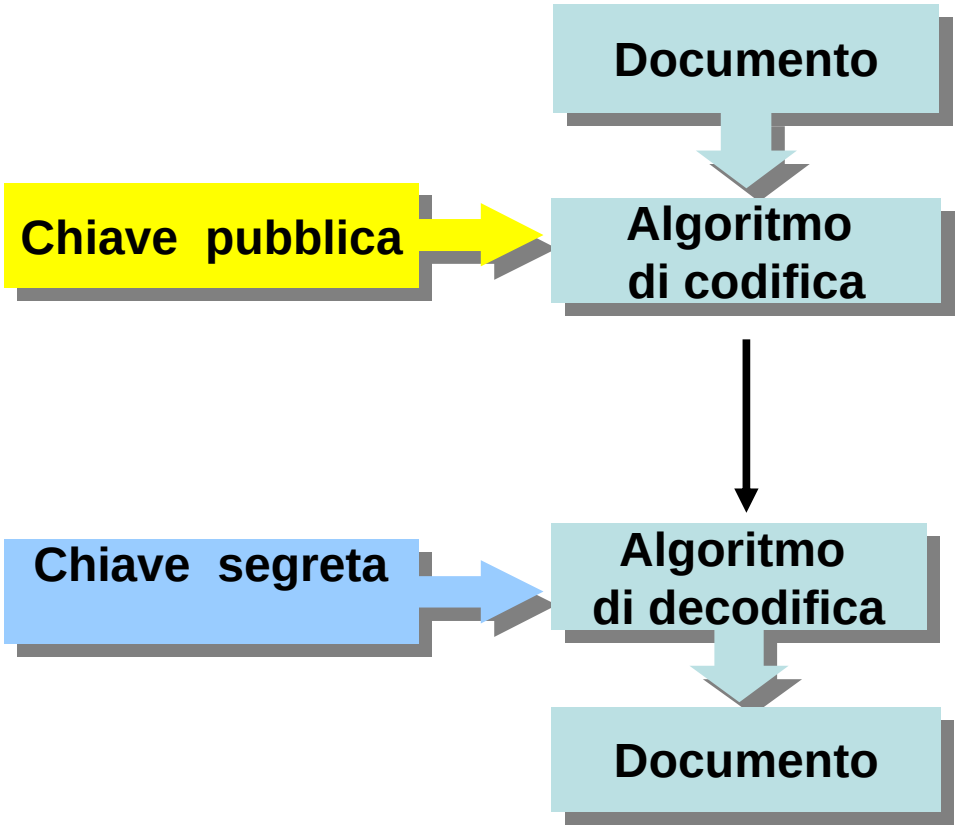
- Vantaggi:
  - Sicurezza (non bisogna distribuire la chiave privata)
  - Fruibilità: la stessa coppia di chiavi viene utilizzata da tutti gli utenti
- Svantaggi:
  - Complessità algoritmica $\Rightarrow$ elevati tempi di calcolo

Principio di Kerckhoffs

- Un principio fondamentale della crittologia moderna afferma che:

  “La sicurezza di un crittosistema non deve dipendere dalla segretezza dell’algoritmo usato, ma solo dalla segretezza della chiave”
- Pubblicato nel 1883 nel libro “La criptographie militarie”
- Basti pensare che ormai quasi tutti gli algoritmi crittografici moderni, utilizzati nelle più disparate tecnologie, vengono rilasciati con i codici sorgenti.

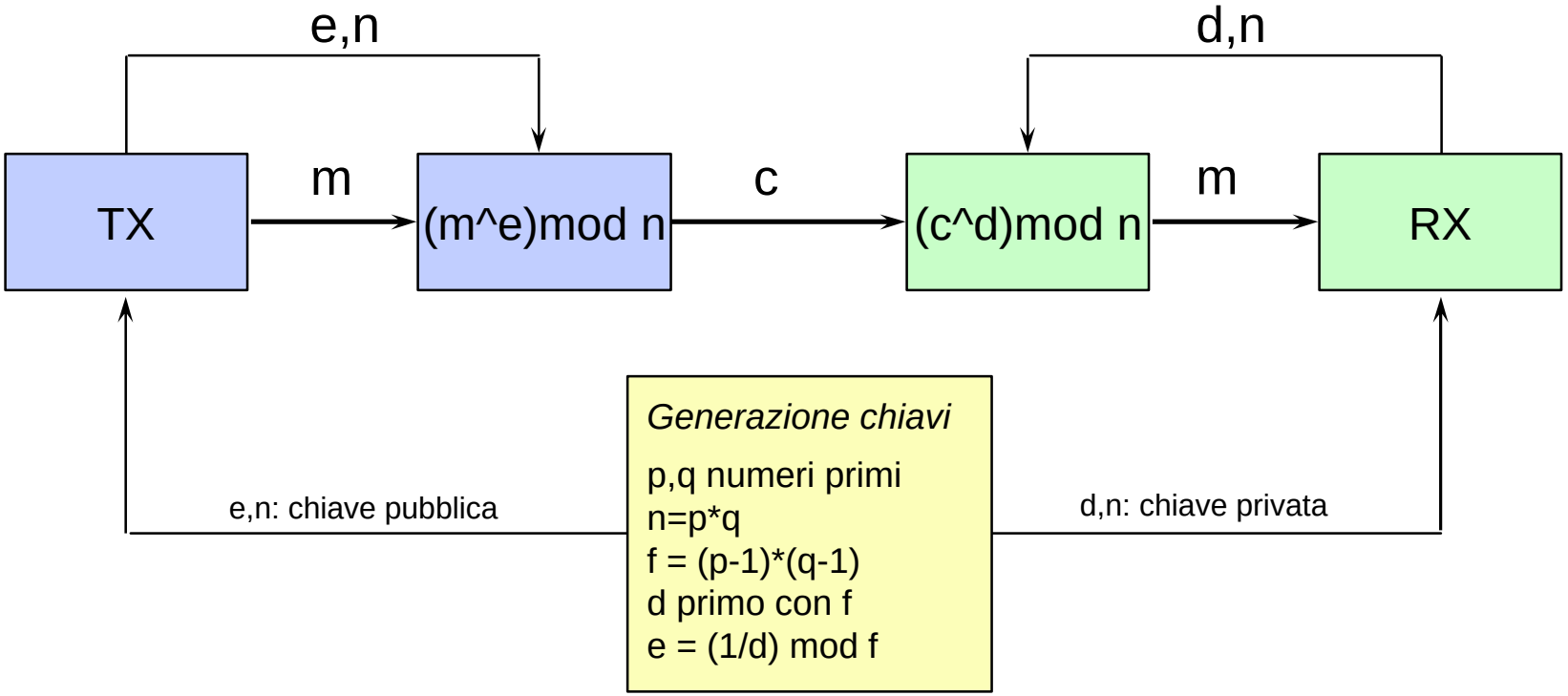
Algoritmi asimmetrici: codifica e decodifica



Conoscere la chiave pubblica non deve permettere di conoscere la chiave segreta

RSA: Rivest, Shamir, Adleman

Algoritmo che sfrutta l'esponenziazione modulare e la complessità computazionale della fattorizzazione



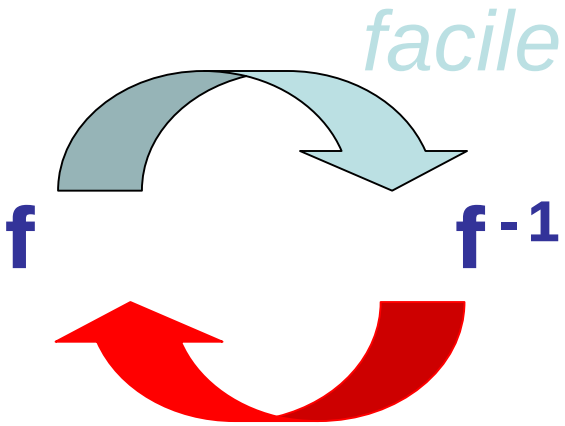
La robustazza di RSA si basa sulla difficoltà di scomporre in fattori primi n, qualora n sia generato dal prodotto di due grani numeri primi.

f(n)=(p-1)*(q-1) è la funzione di Eulero (numero di interi inferiore a n e primi con esso) Con RSA la cifratura è a blocchi m.
La lunghezza in binario di m deve essere minore di n.

RSA: Sicurezza

Funzione one way:

- facile da calcolare
- difficile da invertire



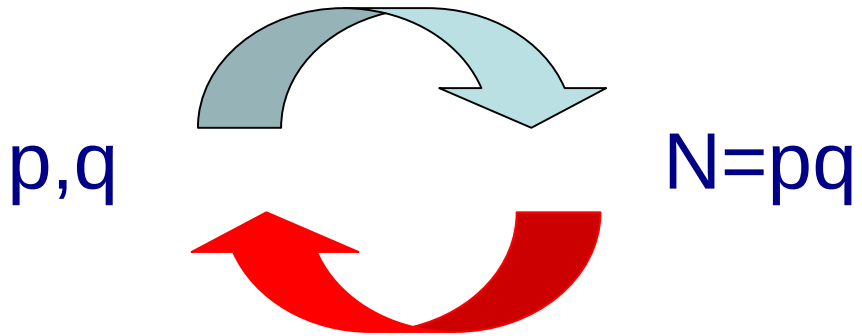
Facile: Esiste Algoritmo veloce

Difficile: Non esiste (o si crede che non esista) un algoritmo veloce

RSA: Sicurezza

Moltiplicare e fattorizzare:

facile



difficile

Funzione one way:

Facile da calcolare

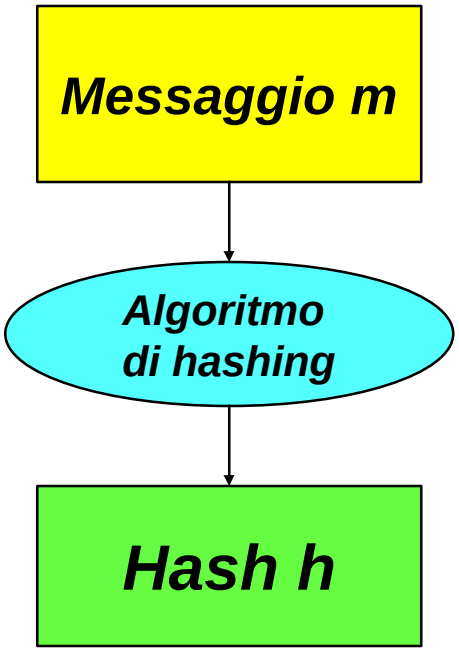
Difficile da invertire

Moltiplicazione facile ⟶ codifica veloce

Fattorizzazione difficile ⟶ decodifica molto lunga
(se non si conosce la chiave)

Hash

- Campo di lunghezza fissa ottenibile *rapidamente*



- Corrispondenza non biunivoca (ovvero dal documento si ottiene l'hash ma NON viceversa. **MA** l'alterazione di un solo bit del messaggio iniziale *invalida* l'hash r (viene evidenziata la discrepanza).
- Lunghezza attuale = 160 bit (2^{160} combinazioni)= $(2^{10})^{16}$

($2^{10} = 1024$)

Gli algoritmi di hashing sicuro

•Permettono di creare da una sequenza di bit qualsiasi e di qualsiasi lunghezza (tipicamente, un file) una sequenza di bit a lunghezza fissa correlata in modo molto stretto alla sequenza di partenza.

•Questo tipo di compressione garantisce (a meno di probabilità trascurabili) che il file compresso sia univocamente determinato dal file originario; il file compresso che si ottiene viene chiamato “**impronta**” (o “digest”) del file.

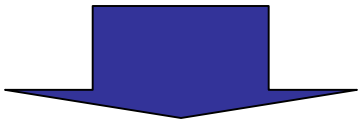
Gli algoritmi utilizzati

- Hashing sicuro: algoritmo **SHA** (Secure Hash Algorithm)

- Crittografia asimmetrica: algoritmo **RSA**, proposto da Rivest, Shamir e Adleman

Gli algoritmi di crittografia asimmetrica: complessità

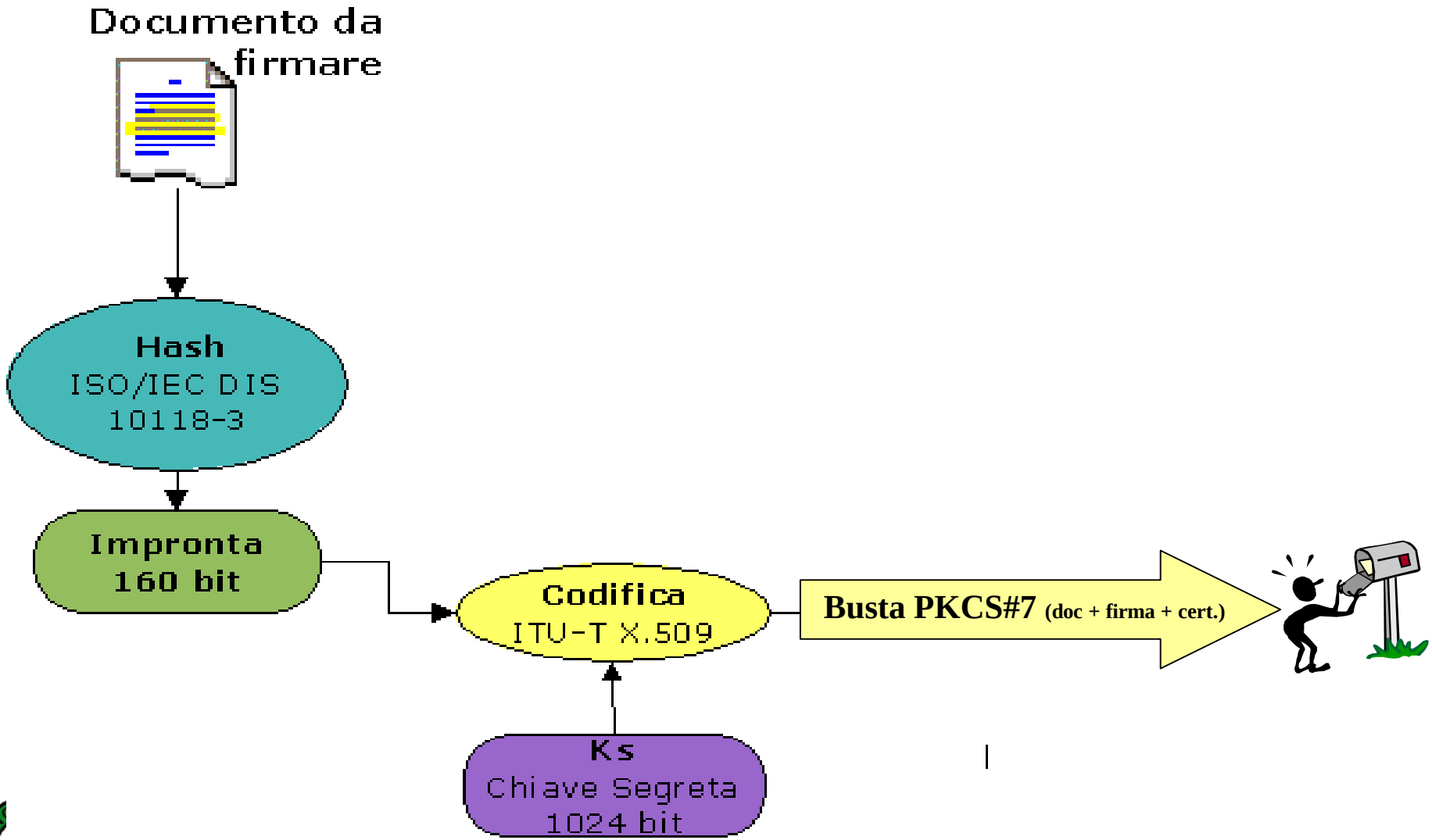
- La complessità degli algoritmi di crittografia asimmetrica è direttamente proporzionale alla dimensione del file da cifrare e alla lunghezza della chiave



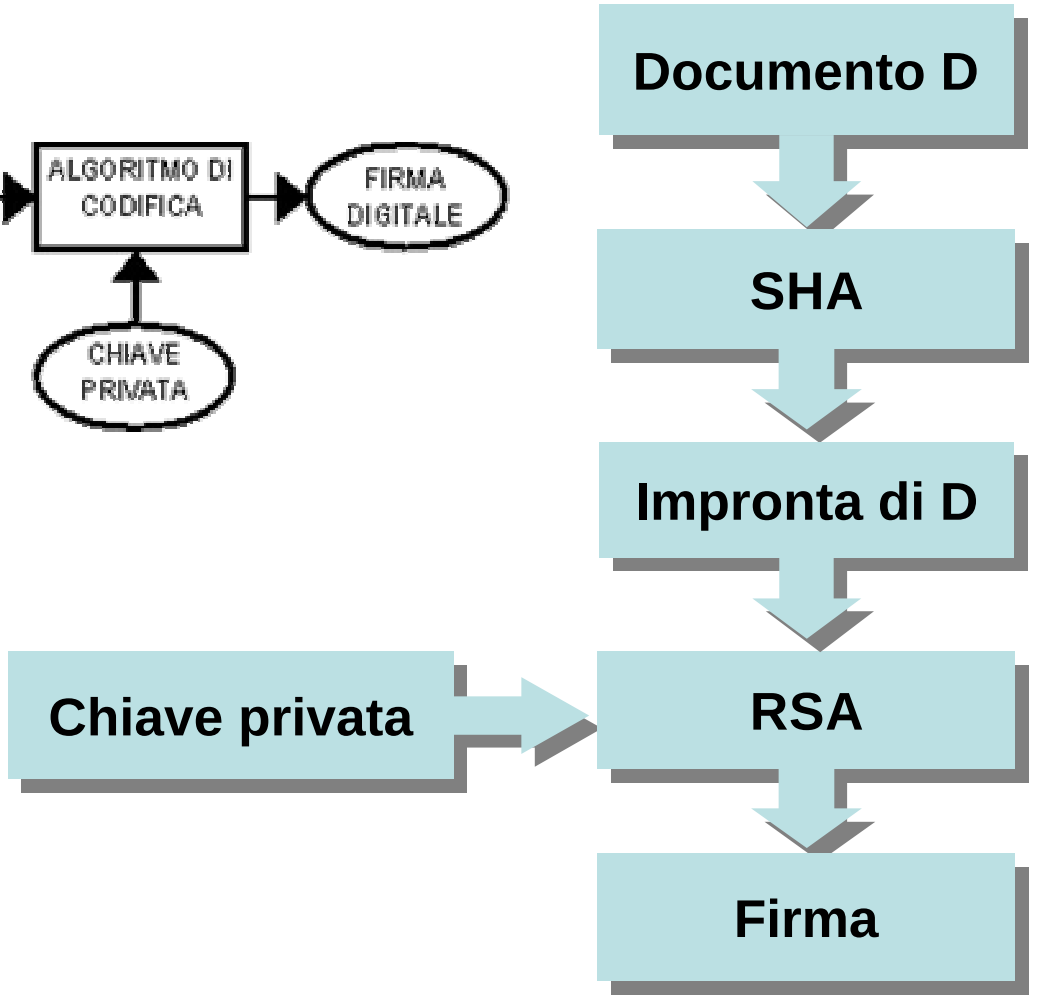
Si comprime il file in input con un algoritmo di hashing sicuro.

L'algoritmo di crittografia asimmetrica viene applicato all'impronta ottenuta.

Generazione della firma digitale



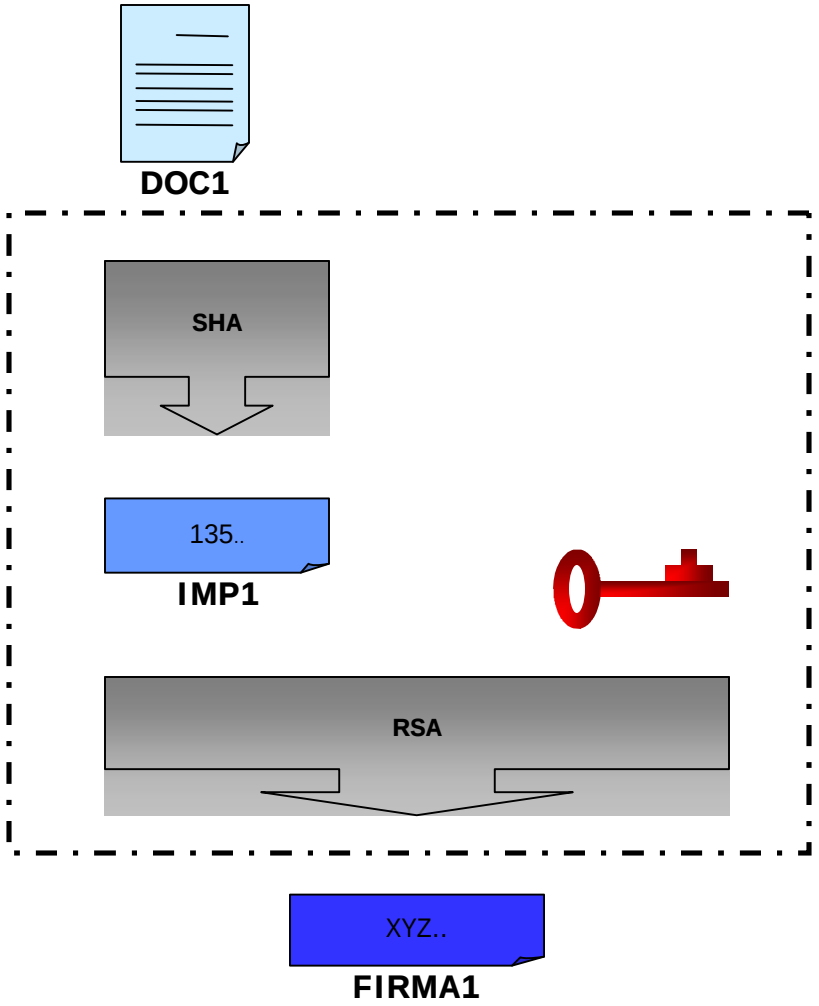
Firma di un documento



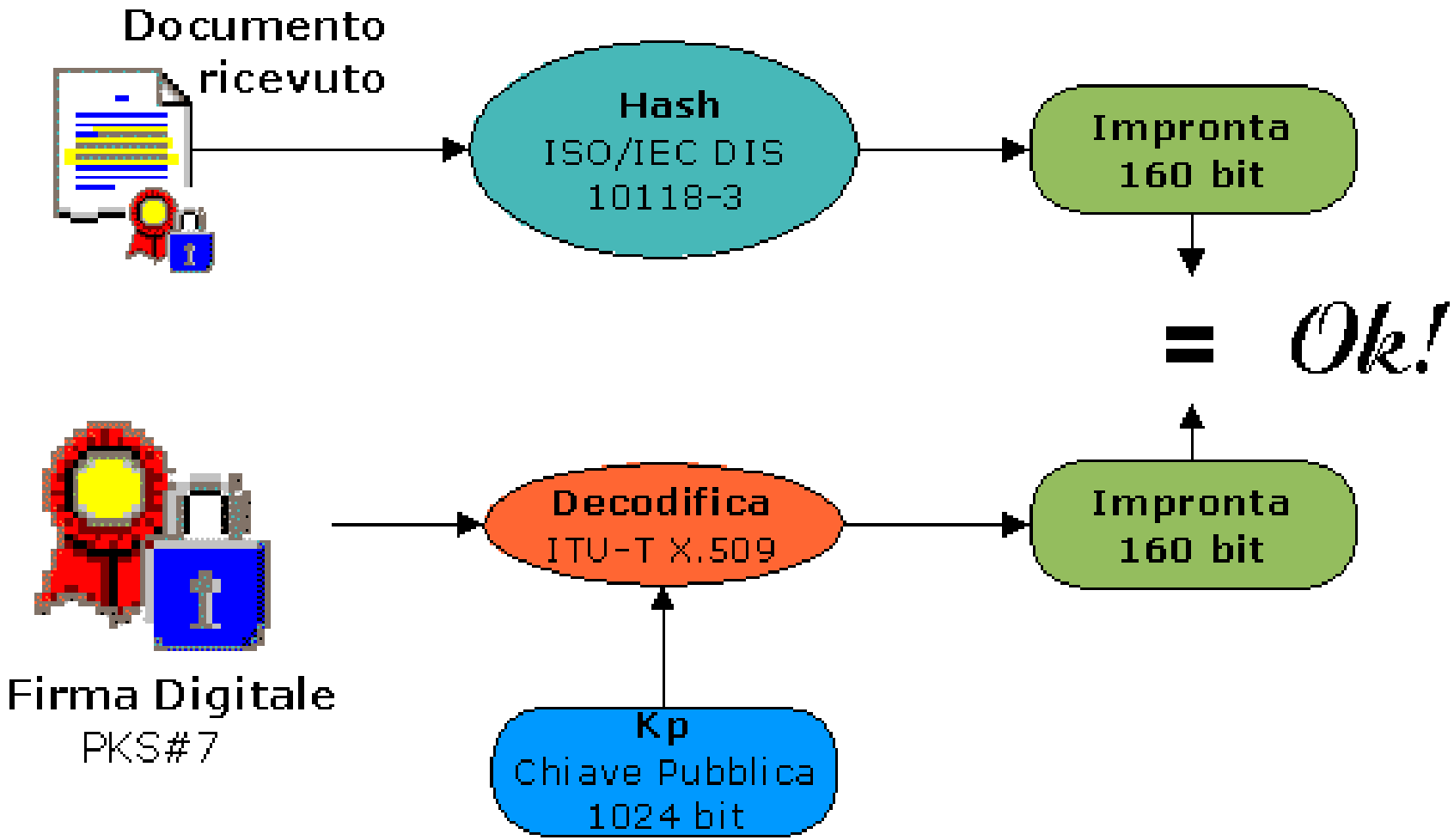
L’algoritmo di firma

- Algoritmo di compressione (SHA) ⇒ impronta univoca

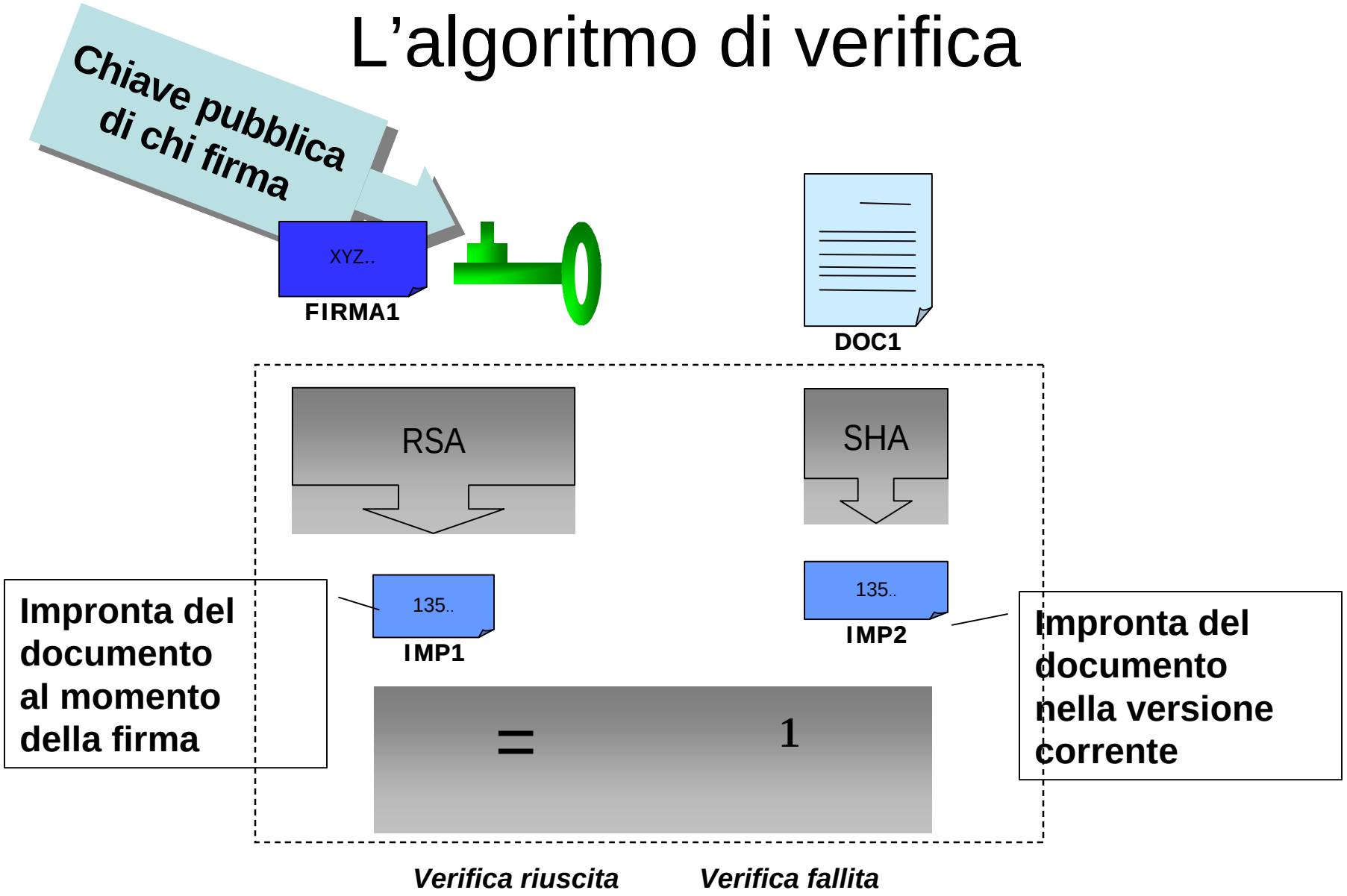
Algoritmo di crittografia (RSA) ⇒ firma



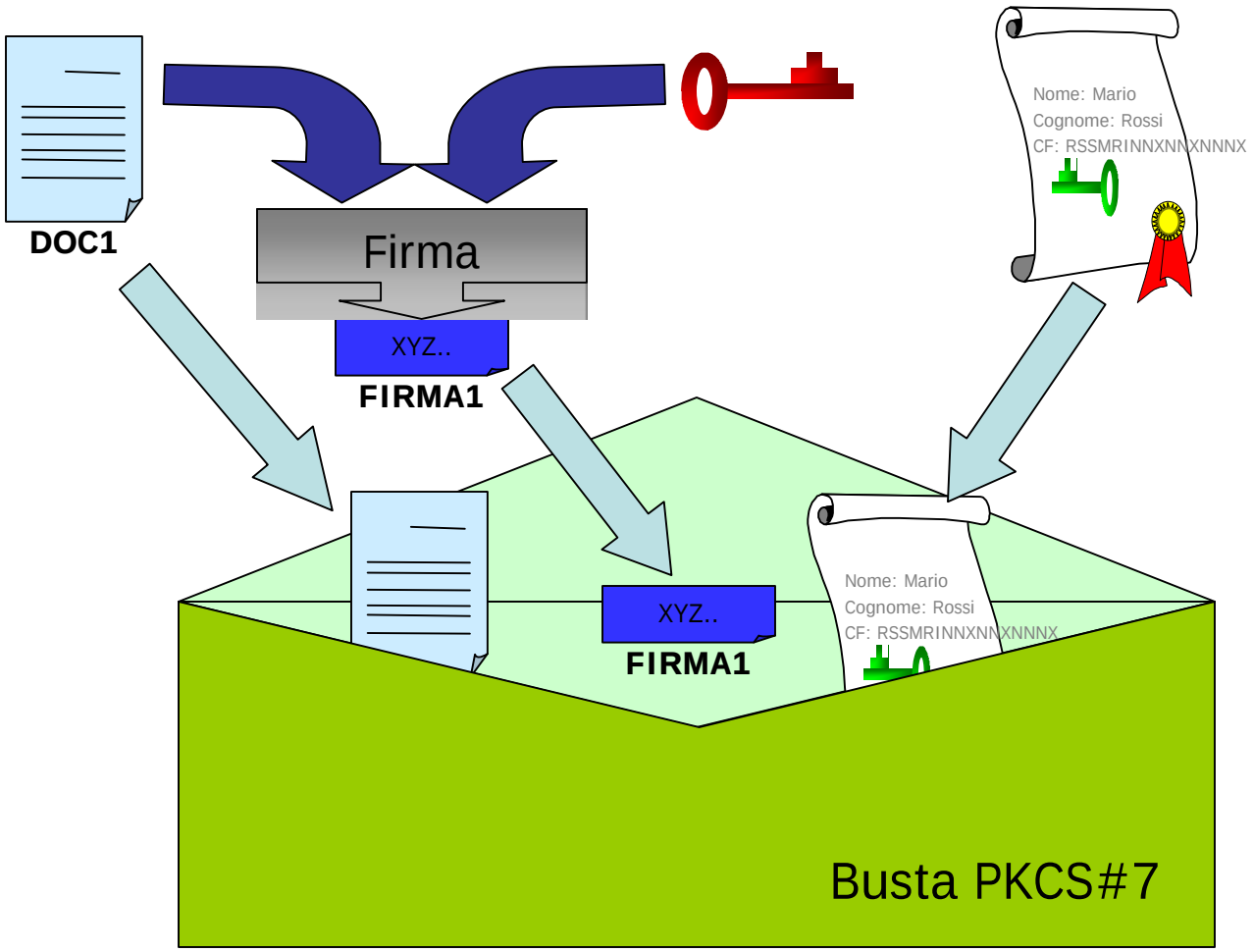
Verifica della firma digitale



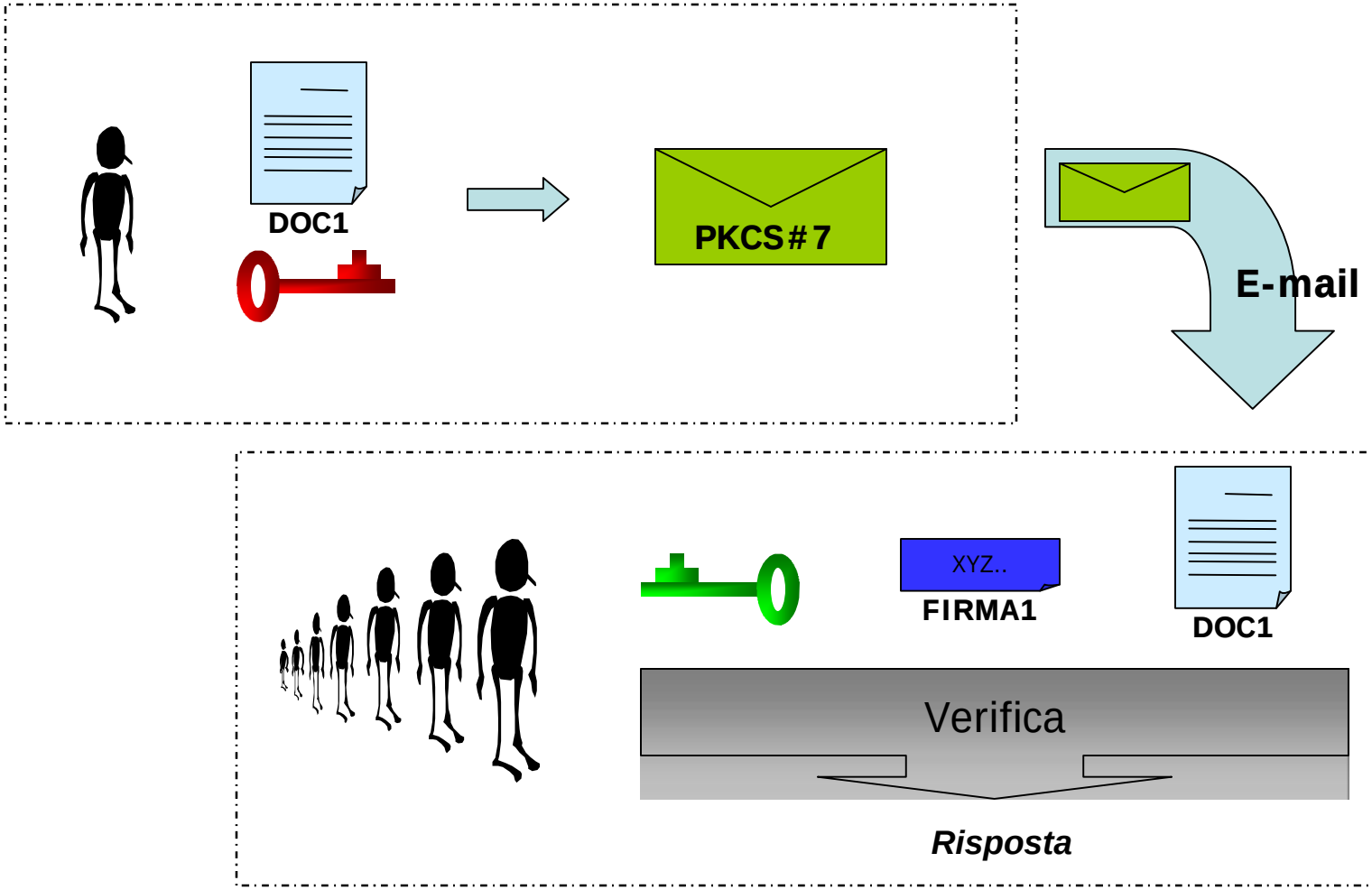
L'algoritmo di verifica



Il processo di firma



Il processo completo



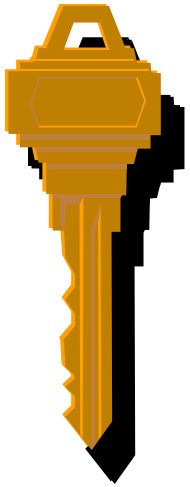
Lunghezza e validità delle chiavi

1.024 bit

2 anni

1.536 bit

3 anni



2.048 bit

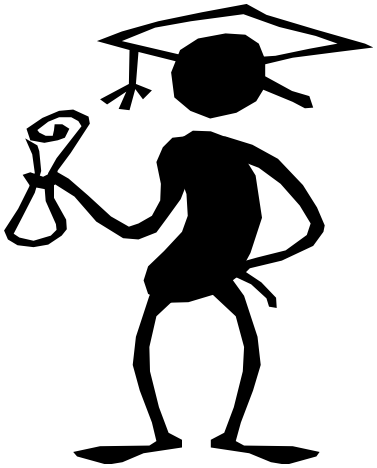
5 anni

Infrastruttura a chiave pubblica

Il termine infrastruttura a chiave pubblica (**PKI**, Public Key Infrastructure) è utilizzato per descrivere l'insieme di software, di attori e di criteri organizzativi che consente di gestire i certificati e le chiavi pubbliche e private

Autorità di Certificazione

L’Autorità di Certificazione (**CA**, Certification Authority) è una terza parte, considerata attendibile da tutti gli attori, che emette e gestisce i certificati



Autorità di Certificazione

- Principali attività:
  - Riceve le richieste di certificazione
  - Genera e sottoscrive i certificati
  - Riceve e gestisce richieste di sospensione e revoca
  - Mantiene aggiornata la CRL e la CSL (liste di revoca e sospensione)
  - Mantiene aggiornata la lista dei certificati emessi
  - Garantisce l'unicità dei certificati

Autorità di Registrazione

- Principali attività:
  - Verifica l’identità del richiedente
  - Eventualmente genera la coppia di chiavi per il richiedente
  - Genera la richiesta di certificazione e la invia alla CA
  - Eventualmente fornisce il dispositivo di firma

Rilascio di un certificato

- Il rilascio di un certificato si concretizza:
  - Prenotazione presso una CA
  - Riconoscimento fisico del richiedente
  - Rilascio del certificato (e del sw di firma)

Revoca e sospensione di un certificato

- Revoca del certificato elettronico:
  - l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi
- Sospensione del certificato elettronico:
  - l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo
- I certificati revocati e sospesi sono inseriti nell'elenco di revoche di certificati (**CRL**: Certificate Revocation List)

Firma e criptazione

- *Talvolta è necessario firmare e contemporaneamente criptare un documento (ad esempio una lettera, un messaggio di posta elettronica, un testamento ..). In generale documenti corti.*

- L'originatore applica la propria firma al documento ottenendo un file che contiene documento in chiaro e appendice firmata

1) Il file complessivo così ottenuto viene criptato con la chiave pubblica del destinatario e inviato
2) Il destinatario decodifica con la propria chiave privata il file ricevuto ottenendo il documento originale con l'appendice firmata
3) Verificando l'appendice con la chiave pubblica del mittente ne controlla la provenienza e l'integrità

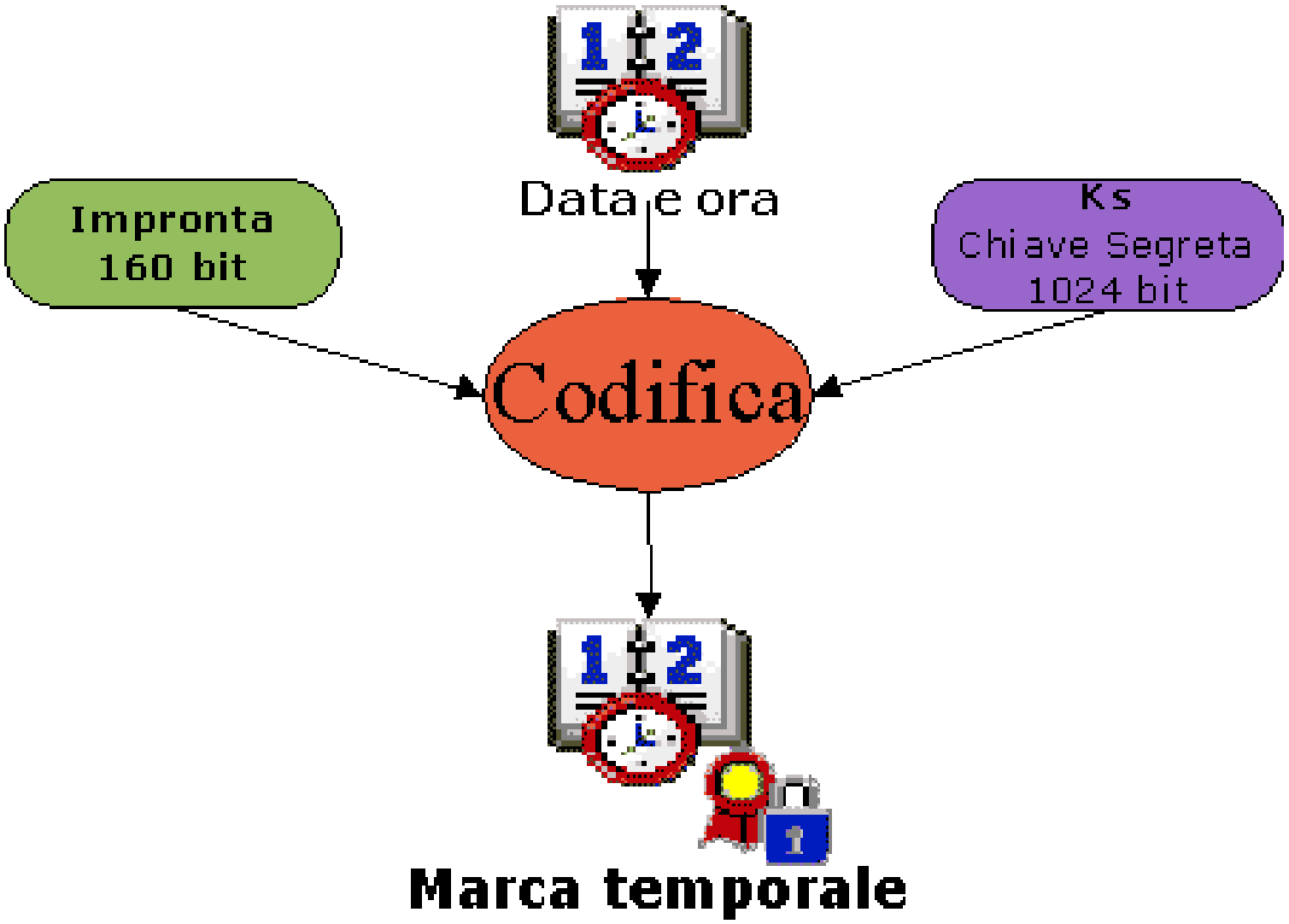
Utilizzo delle chiavi

Tipo azione	***Obiettivo principale raggiunto***
Codifica il messaggio con la key_{pub} destinatario	La **riservatezza** del documento in quanto solo il destinatario, che possiede la sua chiave privata può rimetterlo in chiaro.
Codifica il messaggio con la propria key_{pri}	La **autenticità** del documento in quanto il destinatario, accedendo alla chiave pubblica del mittente può rimetterlo in chiaro.
Codifica il messaggio con la key_{pub} destinatario e poi lo firma utilizzando la propria key_{pri}	La **autenticità** e la **riservatezza** del documento in quanto chiunque, accedendo alla chiave pubblica del mittente, può sapere da chi proviene il documento, ma solo il destinatario, può rimetterlo in chiaro.

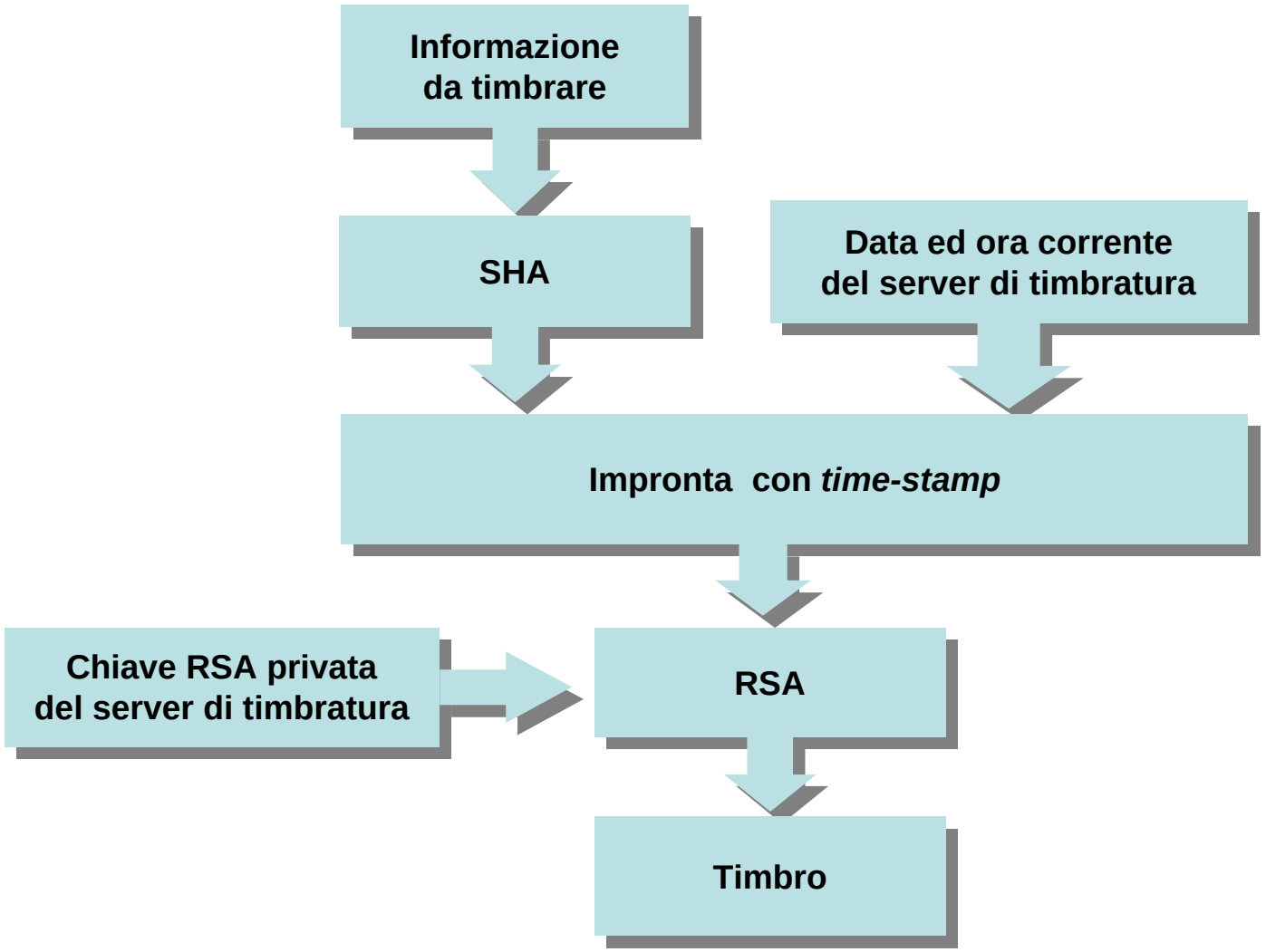
Time stamping

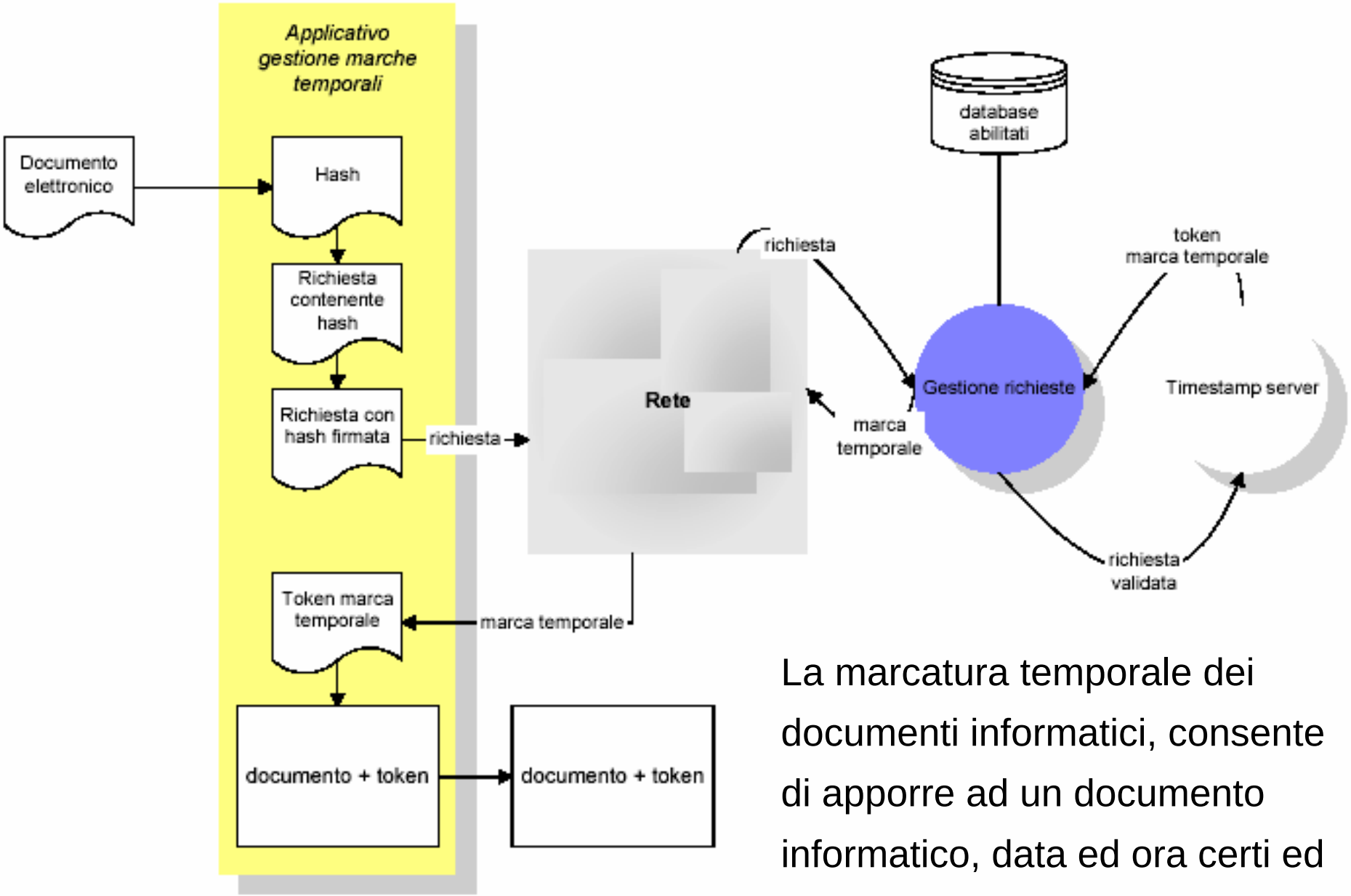
- Nell'ambito del processo di firma è possibile inserire un "time stamping" ovvero l'indicazione certa della data e dell'ora in cui un file è stato firmato, da parte di terzi
- La marca temporale è applicata all'hash in modo da non rivelare il contenuto del documento al "terzo"
- La marcatura temporale serve a validare firme "scadute" ma valide al momento dell'apposizione della firma oppure a garantire l'apposizione in data e ora certe

Marcatura temporale



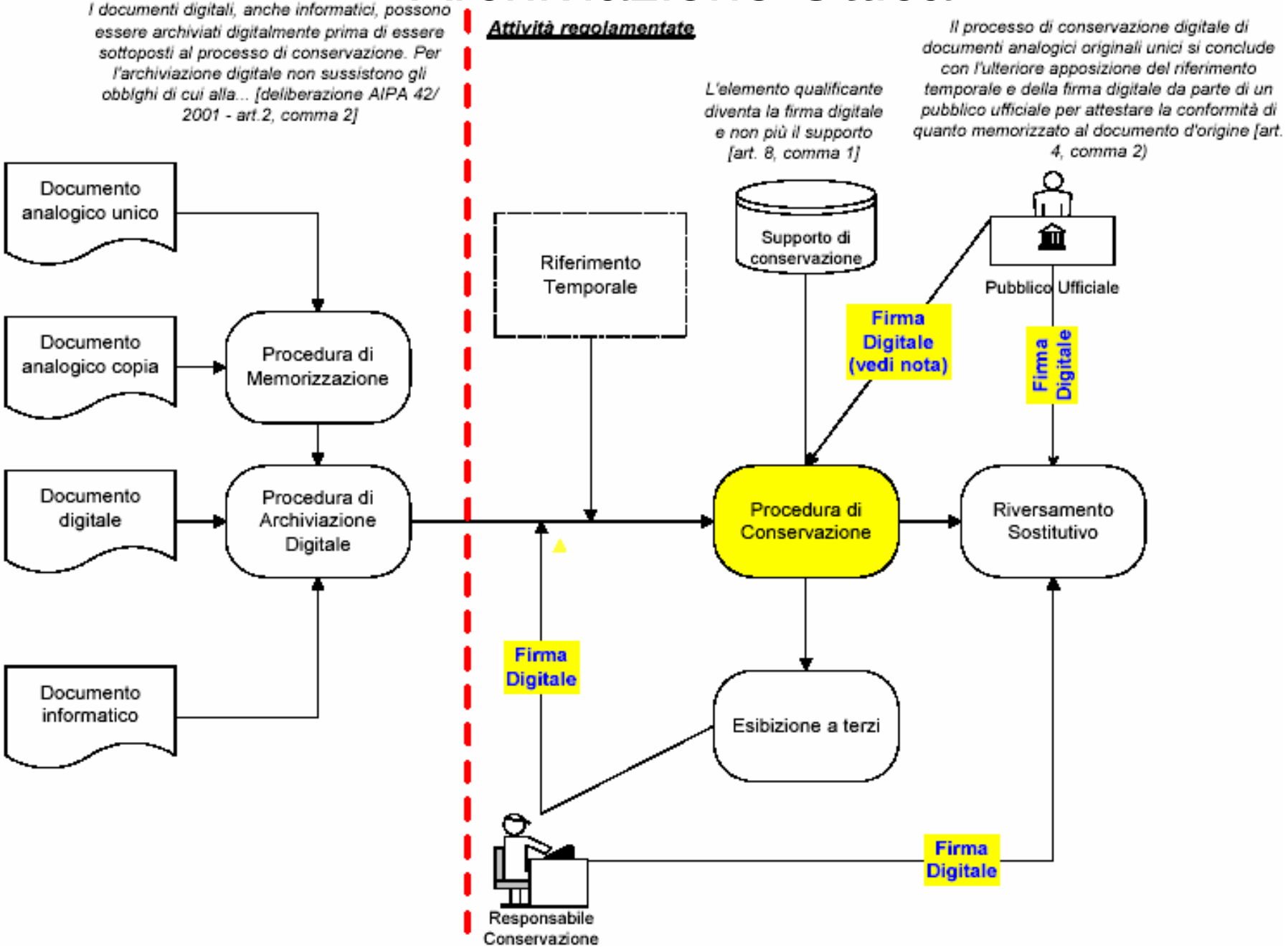
Certificazione temporale



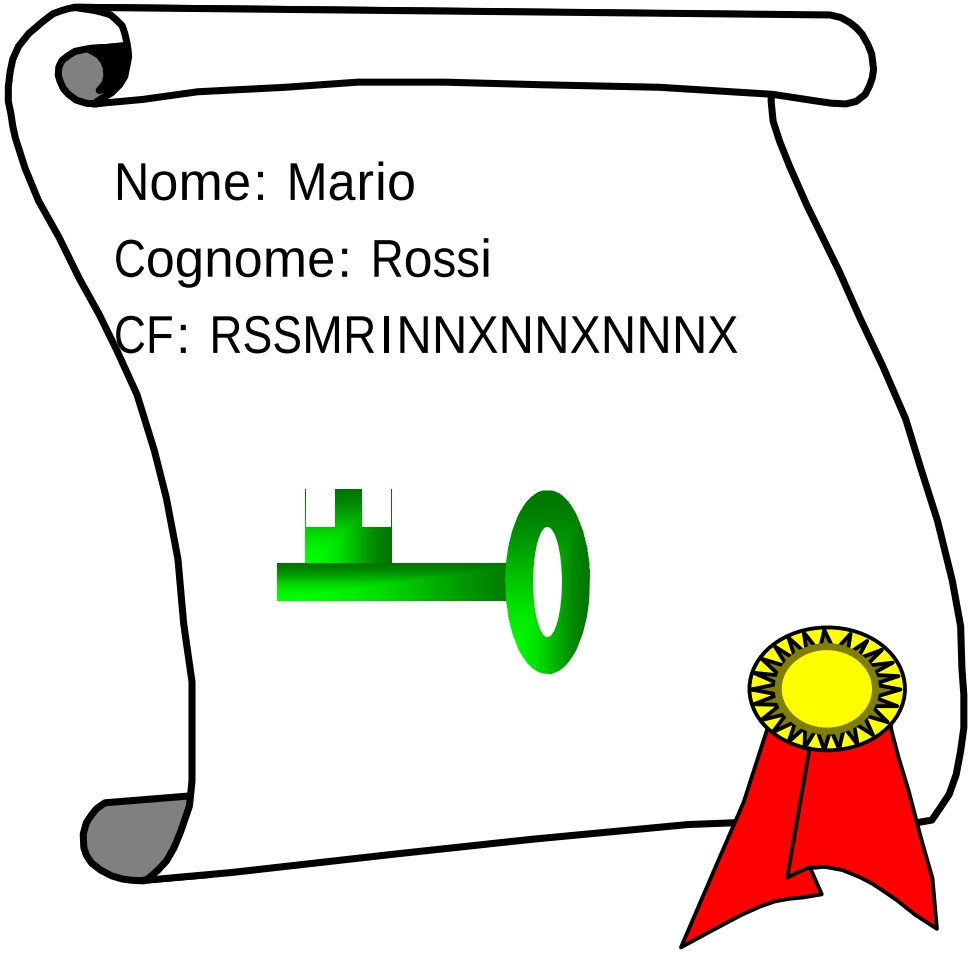


La marcatura temporale dei documenti informatici, consente di apporre ad un documento informatico, data ed ora certi ed opponibile ai terzi.

Archiviazione Ottica



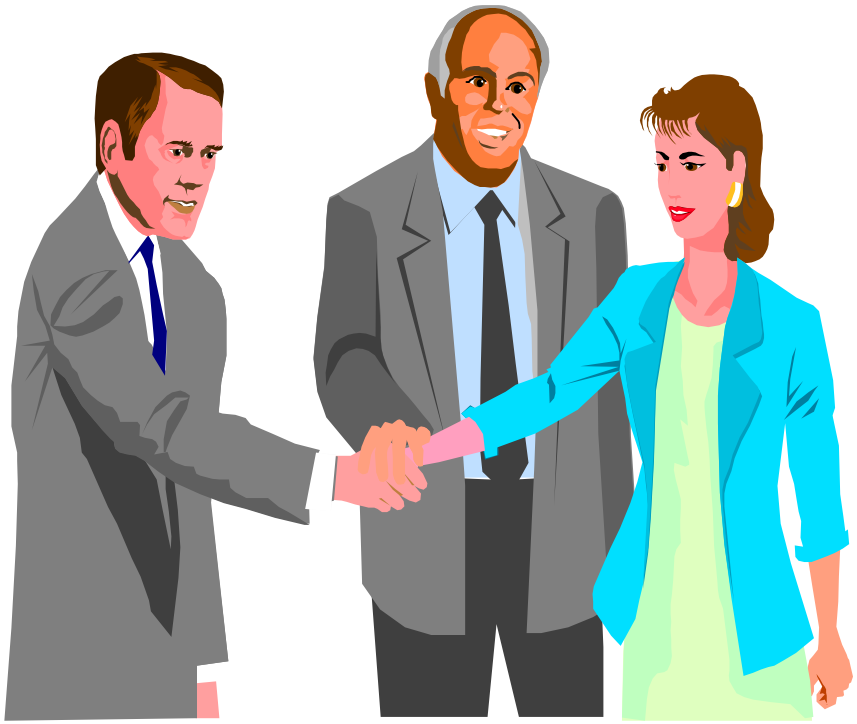
Certificato



Il Certificatore

Indispensabile la presenza di un Certificatore come:

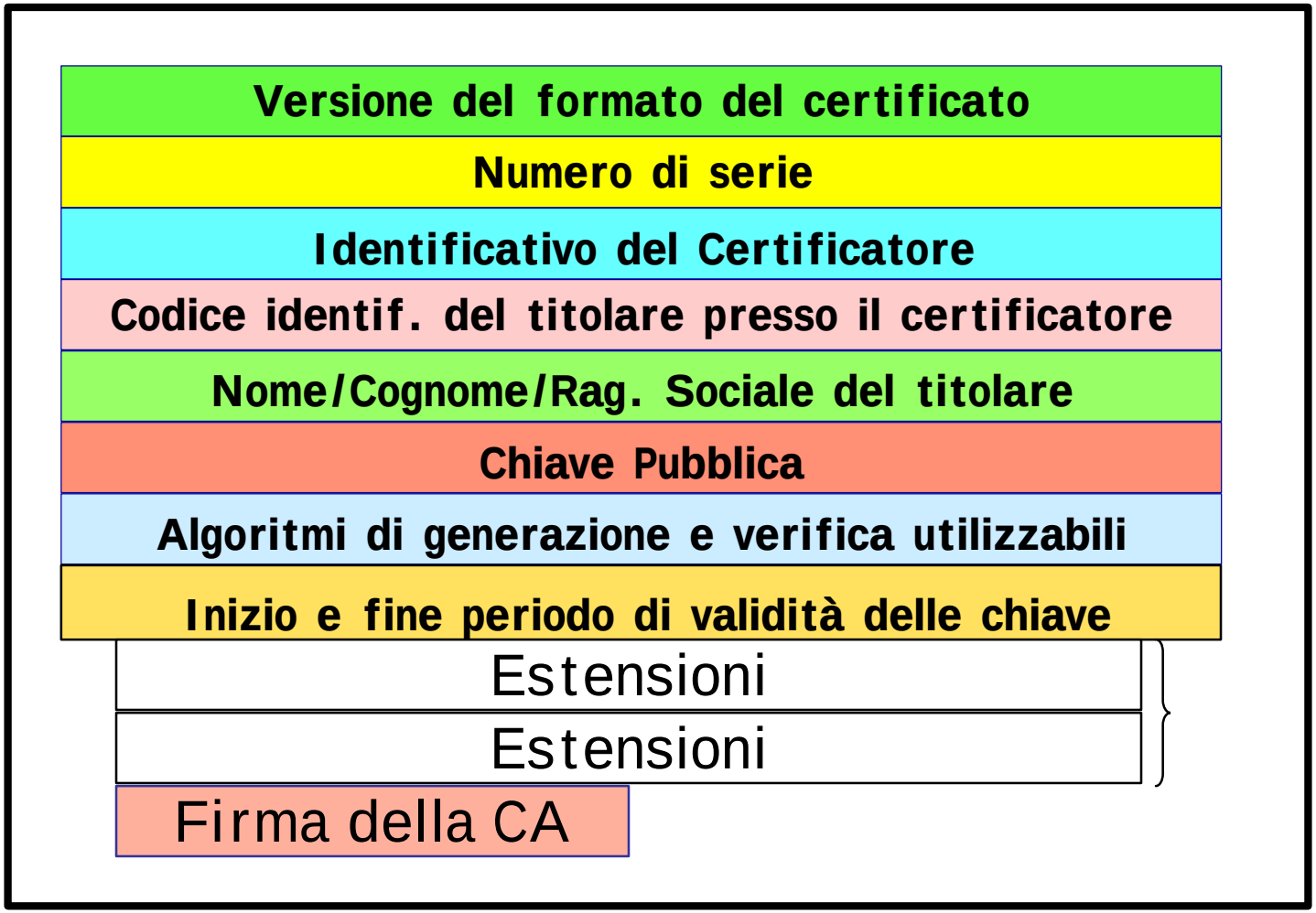
- soggetto che effettua **l'abbinamento inscindibile e biunivoco tra la chiave pubblica ed il soggetto certificato**
- elemento indispensabile e **TERZA PARTE FIDATA** di una transazione tra due potenziali sconosciuti (il **certificatore**);



Certificato

- Il Certificato include:
  - Il nome dell'Autorità di Certificazione
  - La data di emissione del certificato
  - La data di scadenza del certificato
  - Il nominativo del soggetto
  - La chiave pubblica del soggetto

Certificato X509



Revoche

Ove per qualsiasi motivo il possessore ritenga compromesso (ad esempio smarrimento) il suo certificato può “revocarlo” tramite semplice telefonata alla RA o alla CA.

Revocation list

E’ la lista dei certificati non più validi mantenuta e aggiornata dalla CA. (CRL)
N.B. Anche se un certificato può non essere più valido (ad esempio perché scaduto) la CA è comunque in grado di verificare la validità di una firma apposta utilizzando il “time stamping”
Esistono anche i certificati “sospesi” (CSL)

LE LEGGI SULLA FIRMA ELETTRONICA

- **Art. 10 DPR n. 445/2000**
- **DLgs. 23 febbraio 2002, n. 10**
- **DPR 31 gennaio 2003 (Reg.coordinamento firme elettroniche a norma dell'art.13 Dlgs. n. 10/2002).**

Documento Informatico art. 2712 c.c.
(= fotocopia)

Documento Informatico <u>firma elettronica</u>
(= forma scritta)

Documento Informatico <u>firma elettronica qualificata</u>
(= scrittura privata riconosciuta) piena prova

Cosa è la Firma digitale

- firma digitale: il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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 elettronica**

l'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**

Firma digitale

Firma elettronica avanzata

basata su certificato qualificato **& generata** mediante dispositivo di creazione firma sicura

-**riservatezza** della transazioni
-**integrità** del contenuto delle transazioni
-**autenticità** della provenienza dei messaggi
-**non ripudiabilità** del documento

I vari tipi di firma

- Regolamento 137/03:
  - FIRMA ELETTRONICA: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
  - FIRMA ELETTRONICA AVANZATA: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
  - FIRMA ELETTRONICA QUALIFICATA: la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;

Certificato

- Regolamento 137 / 03:
  - certificati elettronici: (…) gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi
  - certificati qualificati: (…) i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva

Cos'è un documento informatico?

- **D.P.R. 28 dicembre 2000, n. 445**

TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE AMMINISTRATIVA

Testo coordinato con le modifiche apportate dal D.Lgs. 10/02 e dal DPR 137/03

per: DOCUMENTO INFORMATICO

Si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

Documento informatico

Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del Testo Unico.

Il documento informatico

- In sé considerato, il documento informatico come sopra definito prescinde dal requisito di una firma digitale o elettronica.

  Infatti:

  A ciascun documento informatico, o a un gruppo di documenti informatici, nonchè al duplicato o copia di essi, **può** essere apposta, o associata con separata evidenza informatica, una firma digitale.

Firma elettronica o Firma digitale

E’ una informazione formata da un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, il fine è di ottenere un metodo di autenticazione informatica che viene aggiunta ad un documento informatico al fine di garantirne integrità (messaggio non manipolato) e provenienza (che il mittente sia effettivamente quello dichiarato).

E’ il risultato di una operazione matematica applicata al documento informatico

Forma ed efficacia del documento informatico

- Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.
- Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di firma sicura in modo sicuro, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

Il documento informatico con firma elettronica

Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.

Contratti stipulati con strumenti informatici o per via telematica

- I contratti stipulati e sottoscritti con strumenti informatici o per via telematica, mediante l'uso della firma elettronica qualificata, sono validi e rilevanti a tutti gli effetti di legge.
- Ai contratti indicati si applicano le vigenti disposizioni in materia di contratti negoziati al di fuori dei locali commerciali.

Trasmissione del documento informatico

- Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato.
- La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del Testo Unico, sono opponibili ai terzi.
- La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Copie di atti e documenti informatici

- I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se conformi alle disposizioni del presente Testo Unico.
- I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma elettronica qualificata.

.

Copie su supporto informatico di documenti origine su supporto cartaceo

- Le copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico.

NON OCCORRONO PIU' TIMBRI

- L'apposizione di firma digitale integra e sostituisce, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

Firma digitale

- La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
- Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
- L'apposizione ad un documento informatico di una firma elettronica basata su un certificato revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
- L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

Firma digitale autenticata

- Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato.
- L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'arti-colo 28, primo comma, n. 1 della legge 6 febbraio 1913, n. 89.

Firma di documenti informatici delle pubbliche amministrazioni

- In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale, in conformità alle norme del presente Testo Unico.

- L’uso della firma digitale integra e sostituisce ad ogni fine di legge l’apposi-zione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

Schema di decreto del Presidente della Repubblica recante disposizioni per l'utilizzo della posta elettronica certificata L'articolo 16

- Dispone l'abrogazione dell'articolo 25, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2002, n. 445.
  Essendo stato riconosciuto alla firma digitale valore analogo alla firma autografa, ma ha anche riconosciuto che il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.
- In tal modo è stata prevista una modalità di sottoscrizione che seppur non assimilabile alla firma autografa, ad essa può essere riconosciuta validità *ad probationem.*
  Alla luce di tale previsione, peraltro conforme al dettato comunitario non appare più necessario prevedere che in tutti i documenti delle pubbliche amministrazioni debba essere utilizzata la firma digitale.

Certificatore

- Regolamento 137 / 03:
  - CERTIFICATORE ai sensi dell'articolo 2, comma 1, lettera b), del decreto legislativo 23 gennaio 2002, n. 10, il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

Chiavi

- chiavi asimmetriche: la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici
- chiave privata: l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica
- chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi

Possibilità di avere più firme

- A differenza di quanto accade per la firma tradizionale – che è sottoscrizione autografa sempre uguale a sé stessa, si potranno avere, per uno **stesso soggetto**, **più firme elettroniche**, diversificate in relazione a diversi **livelli di uso** cui sono destinate ed abilitate, soprattutto in relazione al **valore** delle transazioni commerciali per le quali sono destinate ad essere adoperate
- I consumatori potranno dotarsi di dispositivi di firma, alcuni con ristretti limiti d'uso o di valore, da adoperarsi per acquisti su reti pubbliche ed intrinsecamente poco sicure.

Dispositivi di firma

La normativa italiana prevede che il processo di firma sia eseguito internamente ad un dispositivo caratterizzato da elevati livelli di sicurezza e di protezione della chiave privata.

In pratica questo requisito si traduce nell'uso di speciali smart card certificate ITSEC 4

Dispositivi di firma

- Le normali card contengono un chip non duplicabile in grado di memorizzare in modo inalterabile informazioni di interesse per l'utente e/o necessarie per l'utilizzo di specifiche applicazioni.
- La card dialoga con la stazione di lavoro attraverso un apposito lettore, ed software applicativo può interrogarla per ottenere le informazioni in essa memorizzate.
- La card fornisce le informazioni memorizzate solo se riceve dalla applicazione (e quindi dall'utente) un PIN (Personal Identification Number) segreto.
- In definitiva l'accesso alle applicazioni é subordinato sia alla conoscenza del PIN, sia al possesso fisico della card

Dispositivi sicuri di firma (smart card)

•Memorizzano in modo inalterabile la chiave privata dell'utente e, inoltre, dispongono di firmware, micro-processore e memoria con caratteristiche sufficienti a eseguire on-board:

- un algoritmo di inizializzazione in grado di generare e memorizzare stabilmente una coppia di chiavi pubblica/privata (quest'ultima in una zona di memoria inaccessibile dall'esterno);
- un algoritmo di cifratura asimmetrica in grado di cifrare i dati in ingresso con la chiave privata memorizzata internamente

Non richiedono il trasferimento della chiave privata dell'utente sulla stazione di lavoro. La chiave viene creata dalla smart-card e rimane sempre stabilmente memorizzata nella sua memoria interna

Tipi di Smart Card: a sola memoria

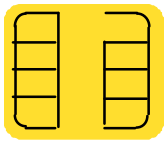
- Non hanno la CPU
- L’accesso ai dati è gestito da un modulo di sicurezza nel chip che non permette che questi vengano scritti o cancellati.
- Costano poco (meno di un Euro).
- Sono tipicamente usate come carte telefoniche prepagate

Tipi di Smart Card: a microprocessore

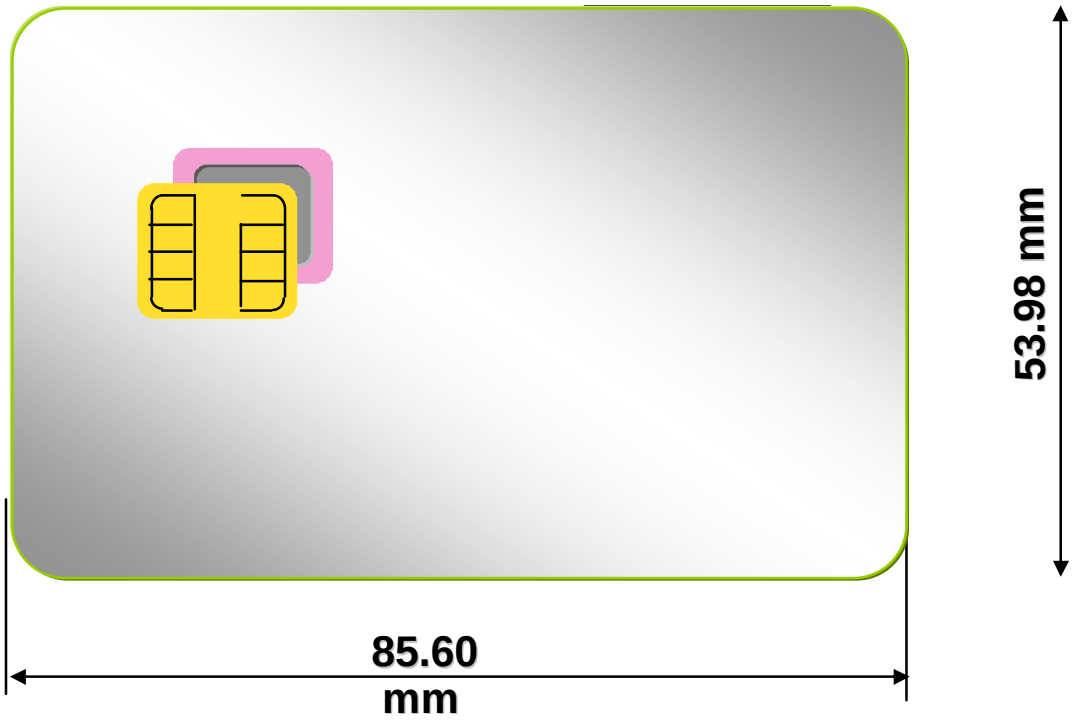
- Sono in tutto simili ad un vero computer, ma con prestazioni ridotte
- Ospitano un vero sistema operativo
- Contengono dati che vengono aggiornati di frequente
- Possono disporre di un coprocessore crittografico
- Hanno un costo un po' più elevato: da 5 a 15 Euro (con un forte effetto quantità)
- Garantiscono elevati gradi di sicurezza fisica e logica, grazie alla presenza del sistema operativo

Com’è fatta una Smart Card

Il chip, completo di CPU, ROM, RAM ed EEPROM viene incastonato in un circuito stampato, la cui struttura è conforme allo standard ISO 7816-3.
In seguito l’insieme circuito/processore viene incollato sul supporto



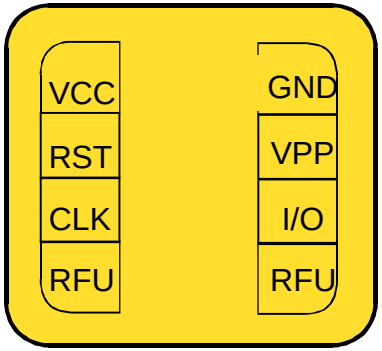
La struttura fisica (dimensioni) di una smart card è specificata negli standard ISO 7810, 7816-1, 2



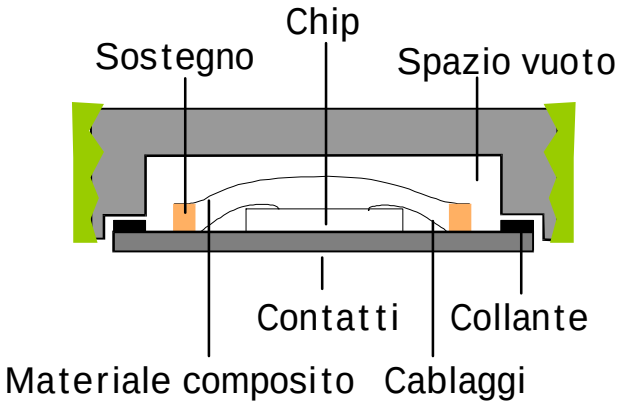
Un collante viene applicato nella posizione prevista dallo standard.

Schema costruttivo

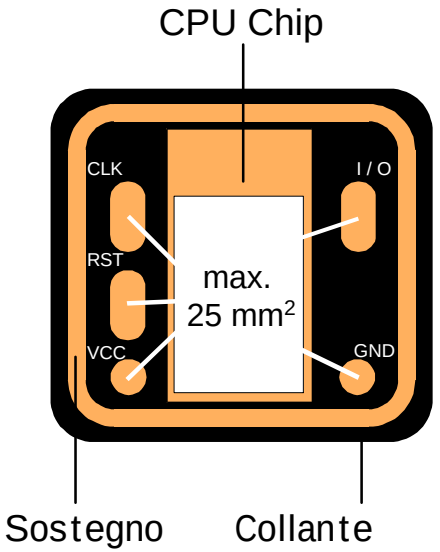
Pianta



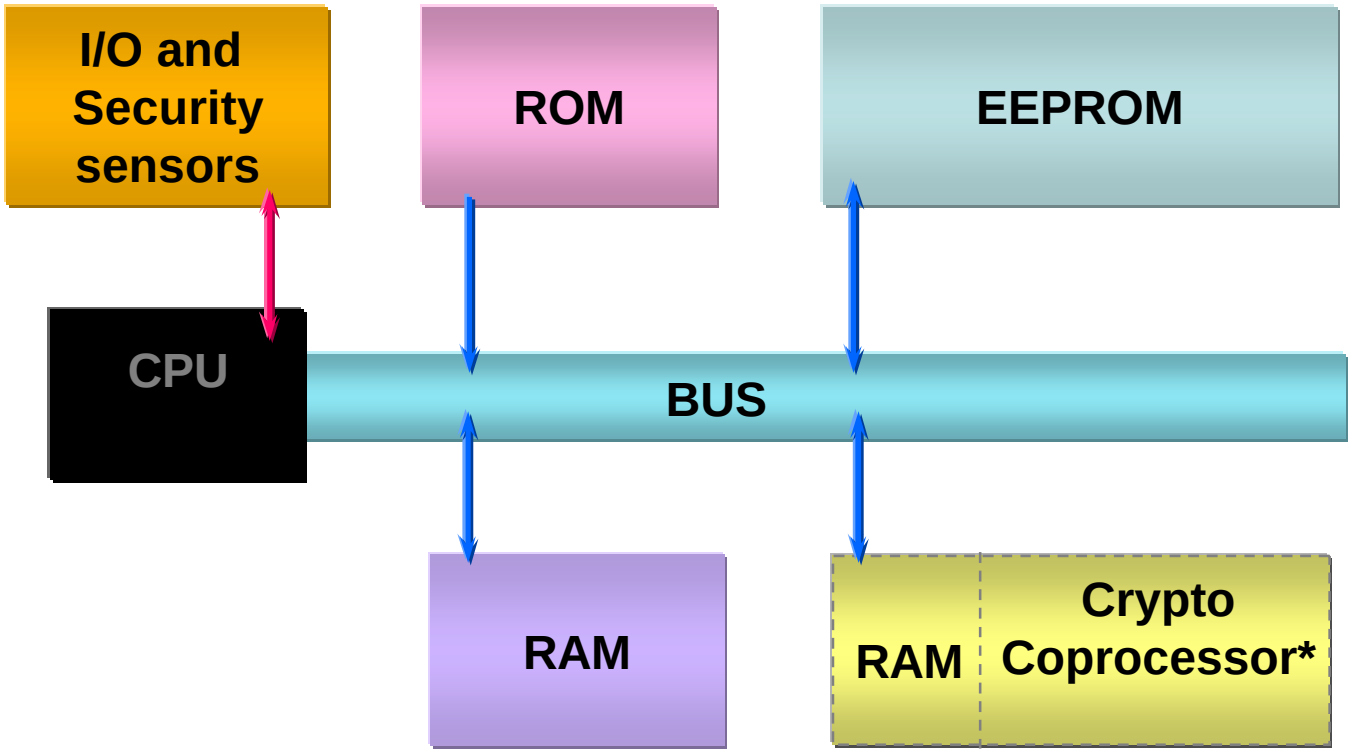
Laterale



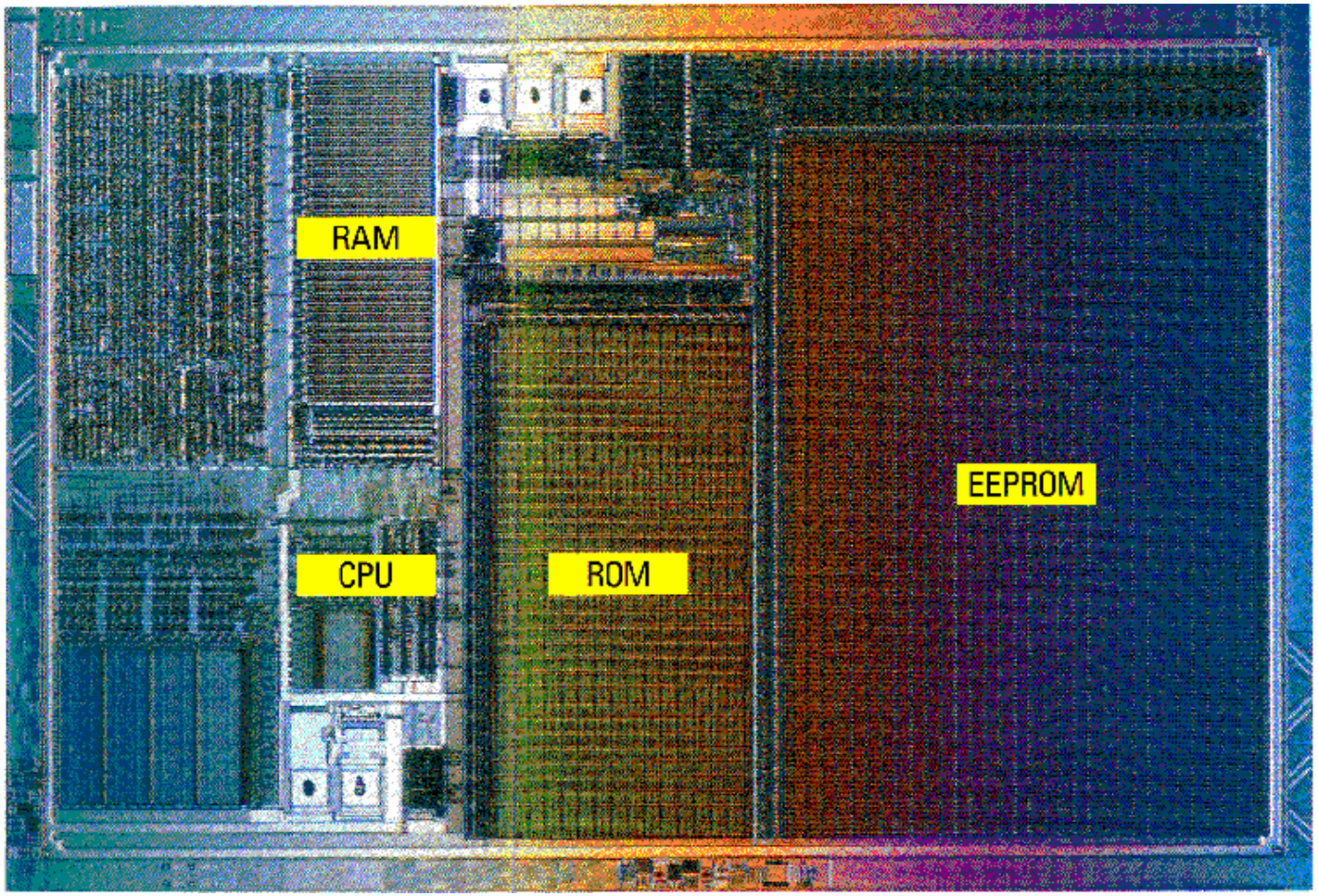
Posteriore



Smart Card: architettura logica del chip



Smart Card: architettura fisica del chip



Lettori

La carta di identità elettronica

I principi ispiratori

la sicurezza:

- **del dispositivo fisico,**
- **del circuito di emissione, formazione e rilascio,**
- **del processo di riconoscimento dei titolare "a vista" ed in rete**

la carta servizi:

- **possibilità di fruire i servizi a carattere nazionale (sanità, finanze, certificato elettorale…)**
- **possibilità di fruire dei servizi a livello locale (trasporti, musei, sportello unico, …)**

l'interoperabilità:

- **su tutto il territorio nazionale**

La soluzione tecnologica

Supporto in policarbonato

numero assegnato al documento in bianco

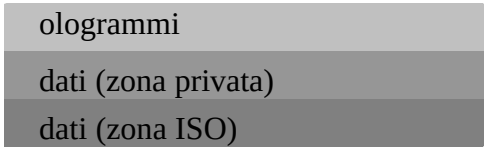
microcircuito

ologramma

banda ottica

La soluzione tecnologica

La Banda ottica



È un mezzo di elevata sicurezza e di difficile contraffazione dotato di ampie capacità di memorizzazione:

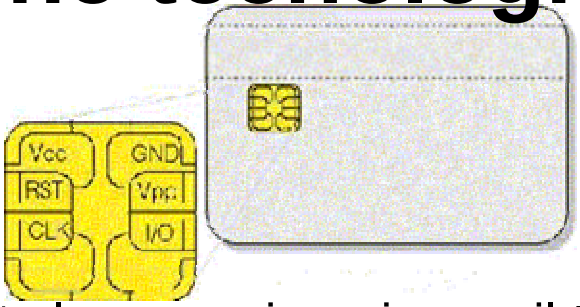
- Permette di memorizzare, in formato digitale, la fotografia, la firma e – con il consenso del titolare – anche le impronte digitali

- Permette, grazie alla tecnica dell'***embedded hologram***, di sostituire logicamente il "timbro a secco" che il Comune appone, al momento del rilascio, al documento d'identità (la carta "filigranata" è invece logicamente sostituita dall'apposizione di un ologramma a caldo da parte dell'IPZS).

- Permette, nella verifica a vista (in assenza di lettori), di controllare la rispondenza dei dati stampati sulla plastica con quelli riportati nell'embedded hologram, garantendo così la loro autenticità.

- Permette di verificare a vista il danneggiamento eventualmente subito dal supporto informatico.

La soluzione tecnologica



Il Microchip

- È un dispositivo che permette la memorizzazione e il **trattamento delle informazioni** con elevate caratteristiche di sicurezza.
- Attraverso un coprocessore crittografico gestisce gli algoritmi basati su chiave pubblica e privata che

  consentono tramite l'identificazione in rete, **la erogazione di servizi**
- La capacità di elaborazione e, in particolare, la capacità di svolgere algoritmi quali la generazione

  delle chiavi, la codifica e decodifica, senza scambi di dati sensibili (es: la chiave privata) con il mondo

  esterno, rendono il microprocessore lo strumento ideale per le transazioni che richiedono un alto livello

  di sicurezza
- L'accesso alla memoria del microprocessore è protetto da sicurezze fisiche e logiche .

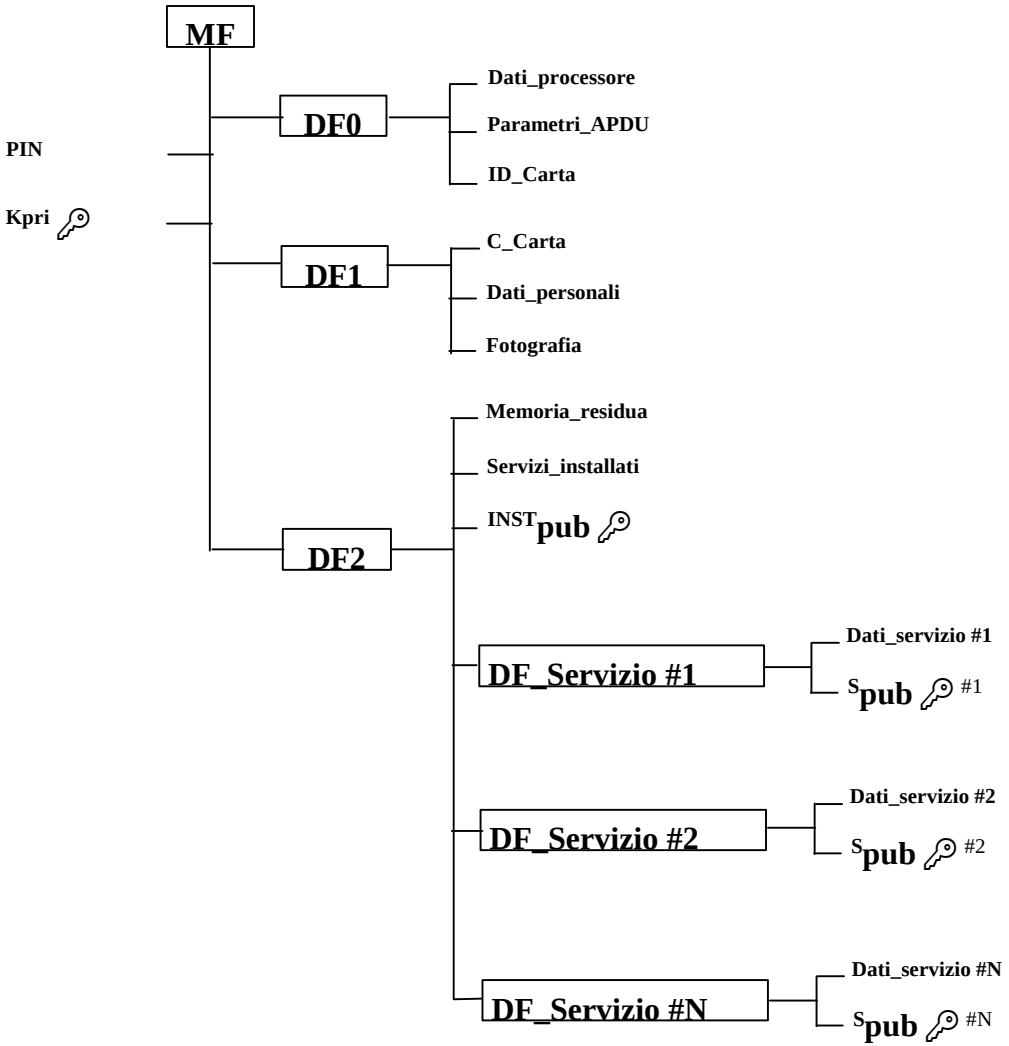
La firma digitale e la carta di identità elettronica

La carta di identità elettronica non è uno strumento di firma del titolare anche se utilizzata per l'identificazione a vista (supporto plastico) ed in rete (supporto chip) del possessore.

Per l'identificazione in rete del titolare si utilizzano tecnologie simili a quelle della firma digitale, ma l'infrastruttura PKI ed i certificati emessi afferiscono soltanto ed esclusivamente alla carta come supporto fisico e mai al titolare, la cui identità non si conosce se non al momento del rilascio a vista presso i Comuni.

La carta di identità elettronica è fornita di chip la cui strutturazione (maschera) consente di inserire dei servizi sia a valenza nazionale che locale. Tra questi ultimi è possibile prevedere la firma digitale del titolare rilasciata da una CA.

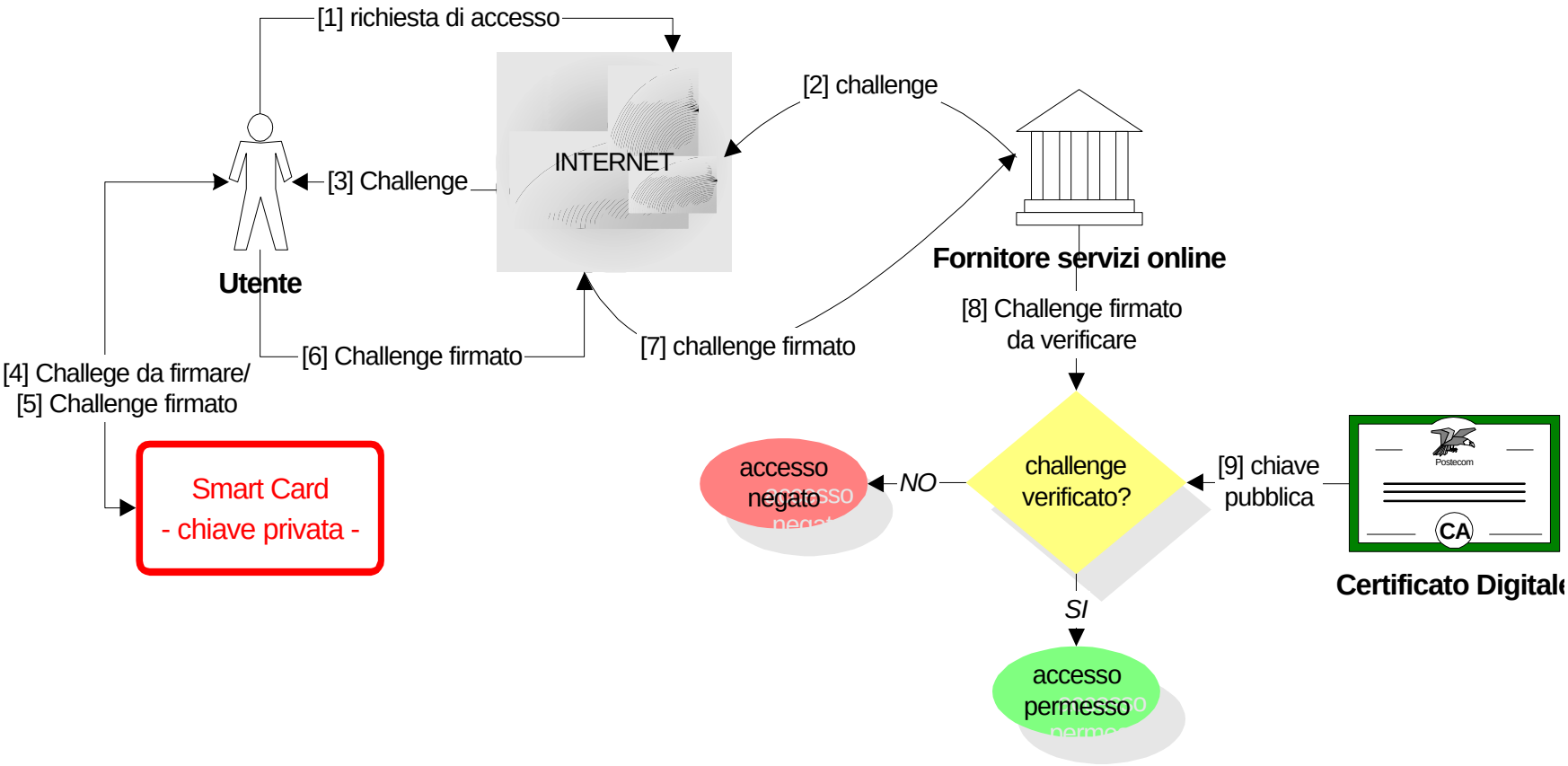
Struttura dati del microprocessore



La Carta Nazionale dei Servizi

- La CNS non identifica “a vista”.
- Le caratteristiche del micro chip sono equivalenti a quelle della CIE.
- Il certificato di autenticazione ha un formato standardizzato.
- Esiste un documento di Assocertificatori su questo standard.
- La CNS è conforme allo standard Netlink nella sua funzione di tesserasanitaria

Meccanismi di autenticazione



Sottoscrizione e identificazione

Carta di Identità Elettronica (e CNS)

Tutte le istanze e le dichiarazioni da presentare alla Pubblica Amministrazione o ai gestori o esercenti di pubblici servizi, inviate per via telematica sono valide se sottoscritte mediante firma digitale, basata su di un certificato qualificato, rilasciato dal un certificatore accreditato e generata mediante un dispositivo per firma sicura… (D.L. vo 23.01.02 n° 10, art. 9, comma 2, lett. a)

Firma Elettronica Avanzata

Tutte le istanze e le dichiarazioni da presentare alla Pubblica Amministrazione o ai gestori o esercenti di pubblici servizi, inviate per via telematica sono valide:

…ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi (D.L. vo 23.01.02 n° 10, art. 9, comma 2, lett. b)

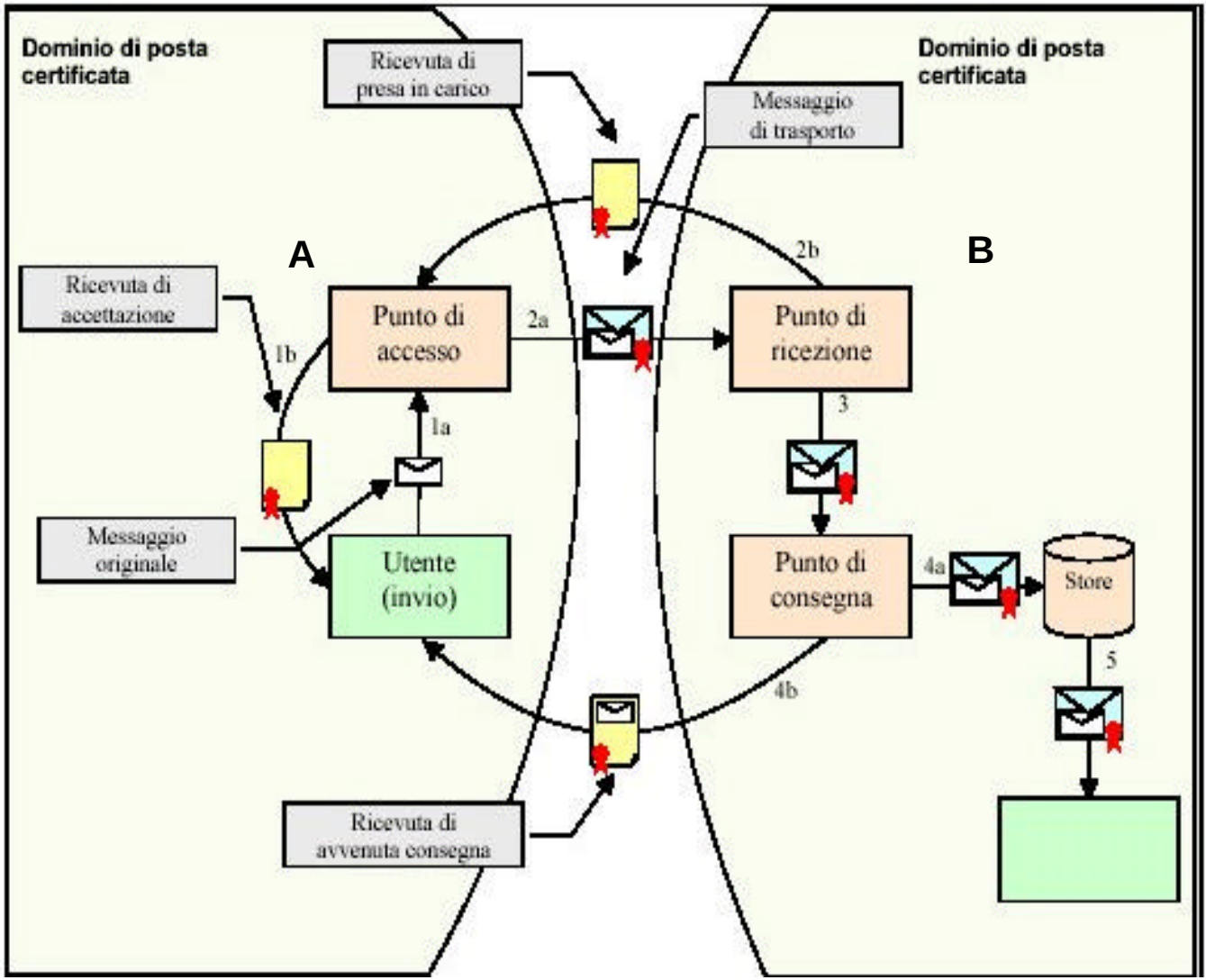
La posta certificata

- La Posta Elettronica Certificata (PEC) è un servizio di messaggistica, basato sugli standard della posta elettronica, che consente la trasmissione di documenti prodotti mediante strumenti informatici nel rispetto dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, quindi in grado di fornire attestazioni di recapito con garanzia di identificazione del mittente e del destinatario.
- Il servizio prevede anche funzionalità accessorie per garantire:
  - la confidenzialità
  - l'integrità
  - il non ripudio
  - la tracciabilità e la storicizzazione del flusso dei messaggi.

Posta Elettronica Certificata

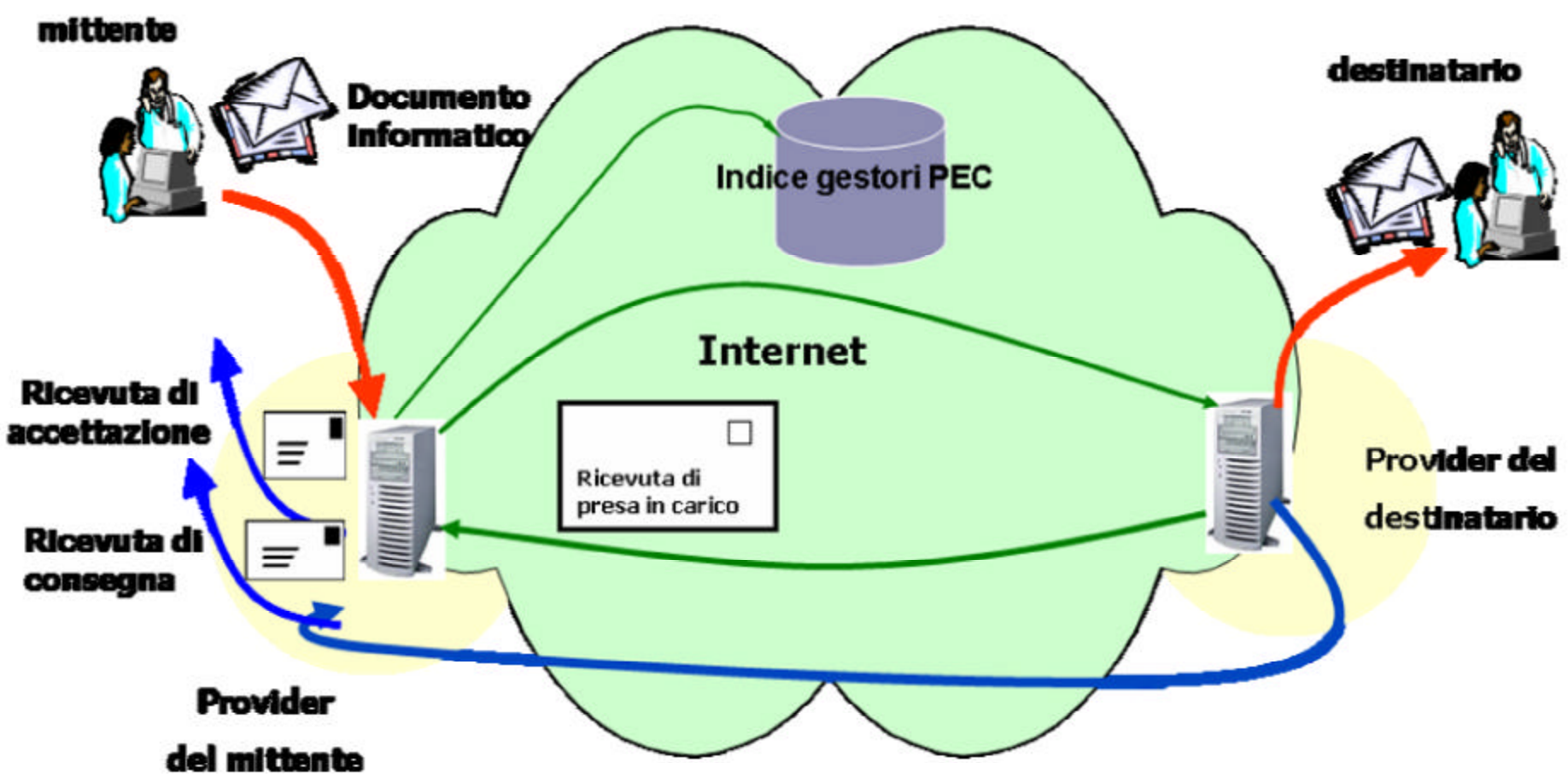
Nel caso la trasmissione del messaggio avvenga tra diversi gestori, deve essere assicurata l'interoperabilità dei medesimi.

Alla ricezione del messaggio, il gestore ricevente emette una ricevuta di presa in carico nei confronti del gestore mittente.



Schematizzazione grafica dell'invio di un messaggio di posta certificata attraverso l'interazione di due gestori A e B.

La posta certificata



Trasmissione del documento informatico nel T.U.

- Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato.
- La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del Testo Unico, sono opponibili ai terzi.
- La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Attori

- **Mittente**: è l'utente iniziale che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
- **Destinatario**: è l'utente finale che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
- **Gestore del servizio**: è il soggetto, pubblico o privato che eroga il servizio di posta elettronica certificata e che gestisce uno o più domini di posta certificata. Il generico gestore del servizio è presente in un registro informatico dedicato, denominato indice dei gestori di posta certificata. I gestori del servizio di posta elettronica certificata devono garantire l'utilizzo di metodi per la verifica che il messaggio sia trasportato dal mittente al destinatario integro nelle sue parti.

Compiti del gestore

- Il gestore del servizio di posta certificata deve:
- mantenere traccia delle operazioni svolte su un apposito registro; i dati contenuti nel suddetto registro devono essere conservati per un periodo di almeno due anni e devono essere disponibili ed accessibili per la consultazione a fini ispettivi
- adottare le soluzioni tecniche e organizzative che garantiscano la riservatezza e la sicurezza (autenticità ed inalterabilità nel tempo) delle informazioni in esso contenute.

Tipi di ricevuta

- Ricevuta di accettazione: attesta l'invio di un messaggio; è generata dal gestore di riferimento del mittente
- Ricevuta di avvenuta consegna: attesta il recapito di un messaggio presso la casella di posta certificata del destinatario; è generata dal gestore di riferimento del destinatario e contiene anche la copia completa del messaggio recapitato; indica al mittente che il suo messaggio è effettivamente pervenuto al destinatario, indipendentemente dall'avvenuta lettura
- Ricevuta di presa in carico: quando la trasmissione del documento avviene tra due diversi gestori, il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio
- Ricevuta di errore di consegna: quando il messaggio non risulta consegnabile il gestore del ricevente fornisce ricevuta di errore di consegna al mittente.

Indice delle PA

- E' l'Anagrafe, gestita da un sistema informatico accessibile tramite un sito internet, presso la quale una Amministrazione che intenda trasmettere documenti informatici soggetti alla registrazione di protocollo si deve accreditare, fornendo almeno le seguenti informazioni identificative relative alla amministrazione:
  - denominazione della amministrazione;
  - codice identificativo proposto per la amministrazione
  - indirizzo della sede principale della amministrazione
  - elenco delle proprie aree organizzative omogenee