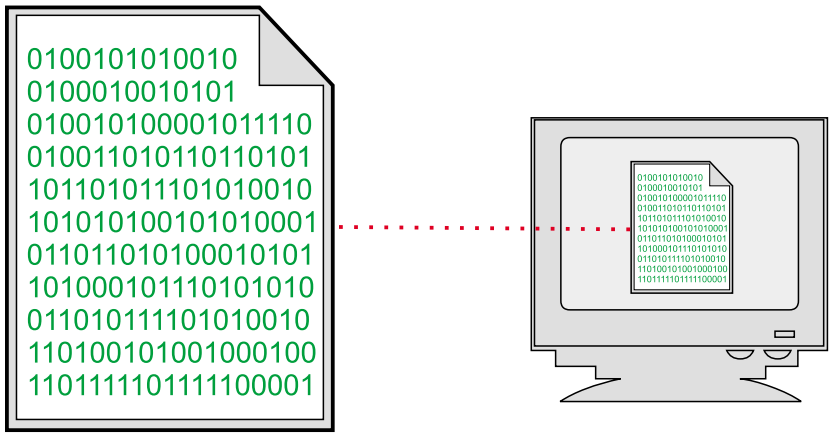
Concetto di “documento informatico”

Documento informatico
lunghezza n bit



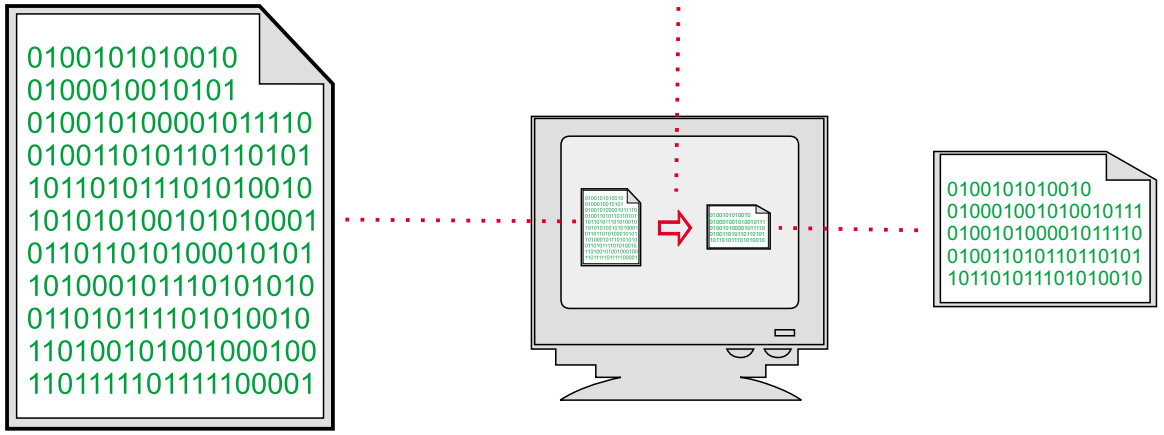
La legge definisce “documento informatico la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”
(DPR 513/97, art. 1/1)

Un documento informatico è una sequenza di caratteri binari (in generale n bit) e può contenere testo, immagini, sequenze audio e video.

Impronta di un documento informatico

Documento informatico
(lunghezza n bit)

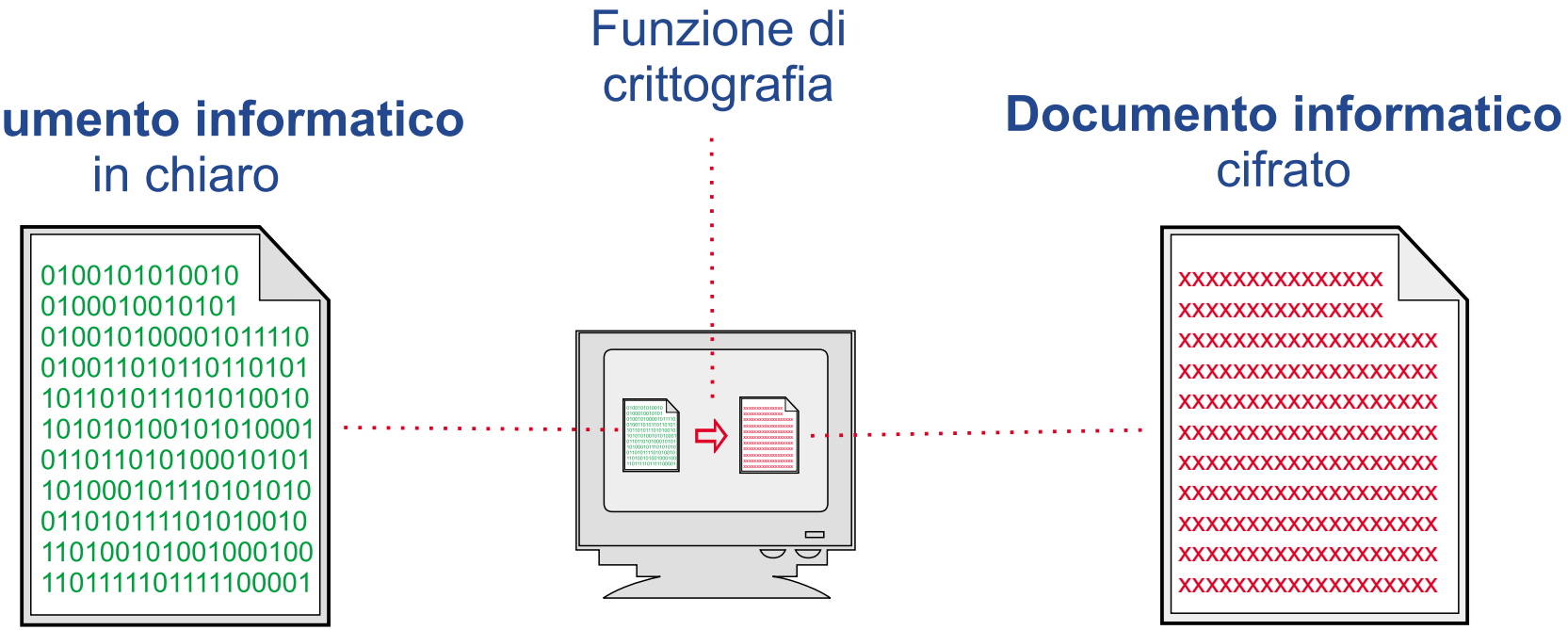
Funzione di hash
SHA-1 o RIPEMD-160



Impronta
del documento informatico
(lunghezza 160 bit)

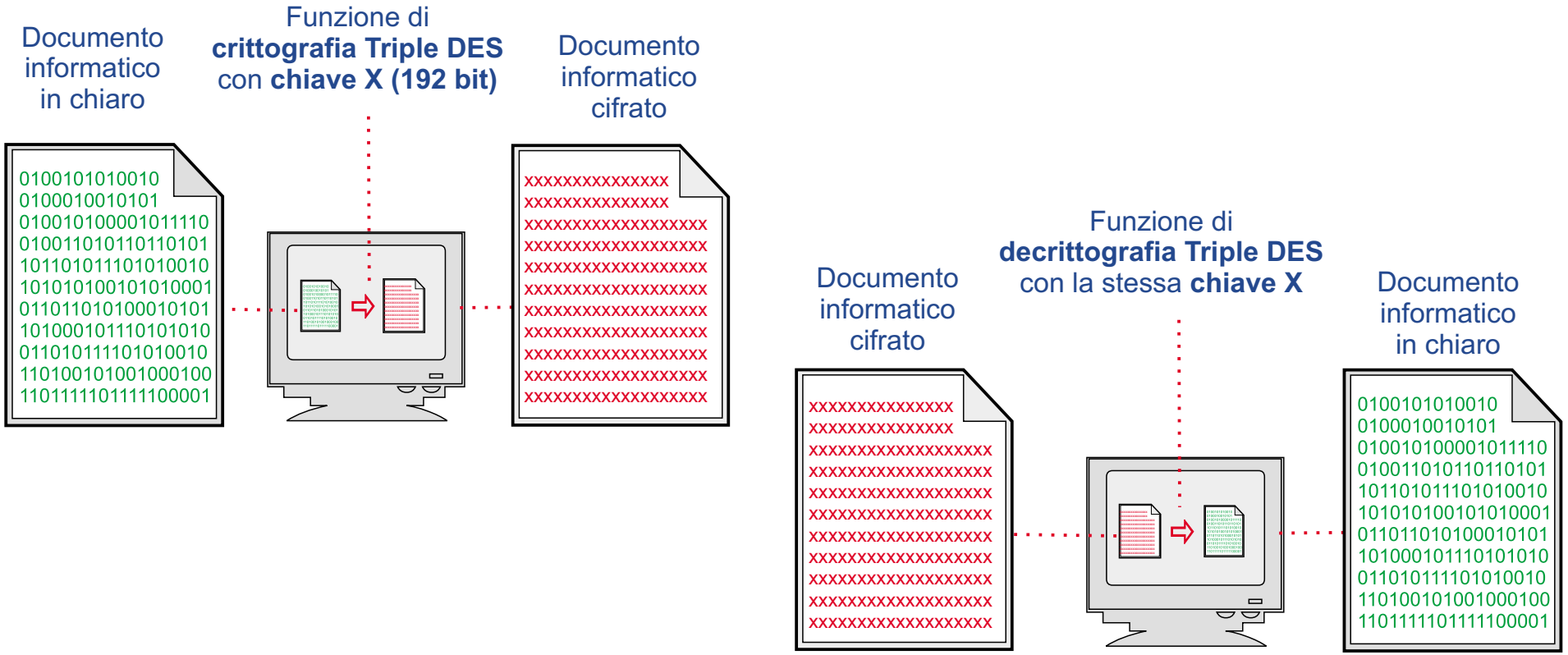
L'impronta è una rappresentazione sintetica del documento informatico. Essa è costruita in modo tale che risulti di fatto impossibile determinare una coppia di documenti informatici che generino la stessa impronta (e altresì impossibile dall'impronta risalire a un documento che la generi).

Crittografia



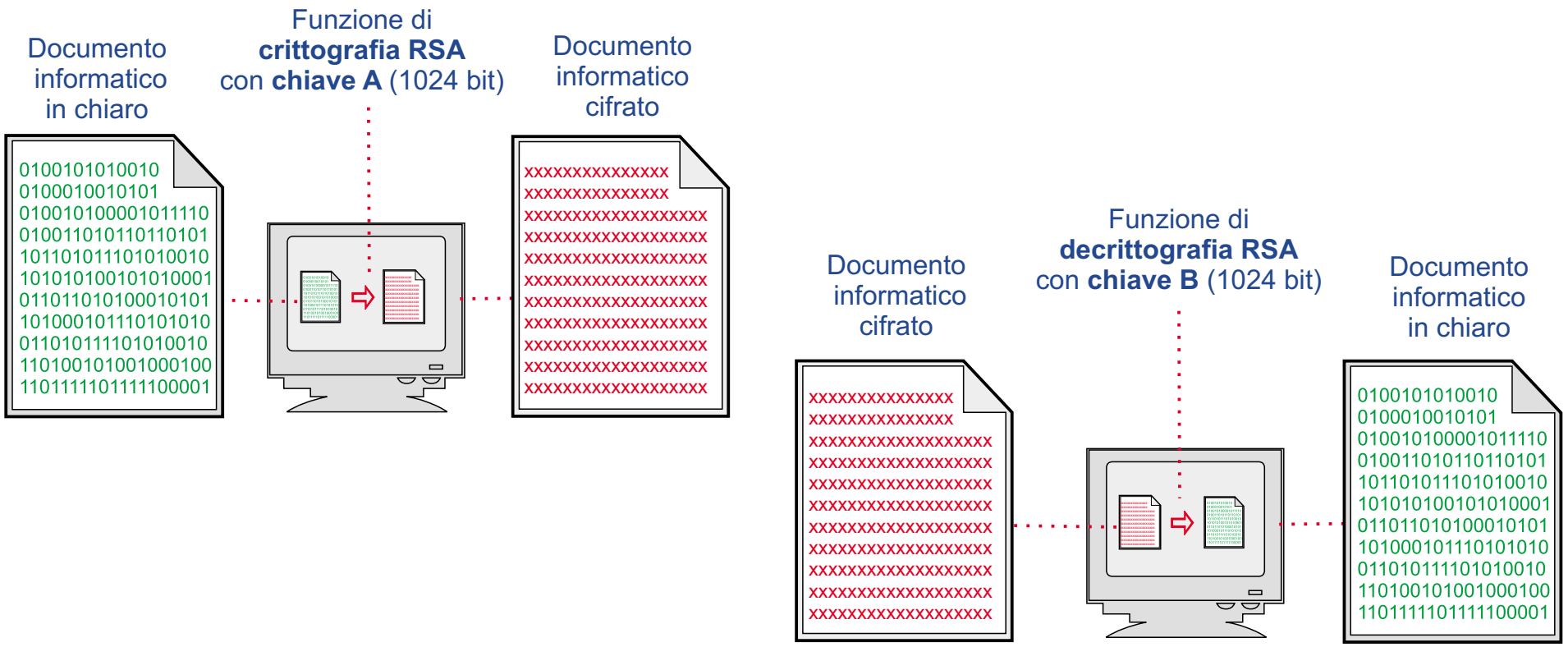
Un’apposita procedura informatica genera a partire da un documento in chiaro un documento cifrato.

Crittografia a chiavi simmetriche



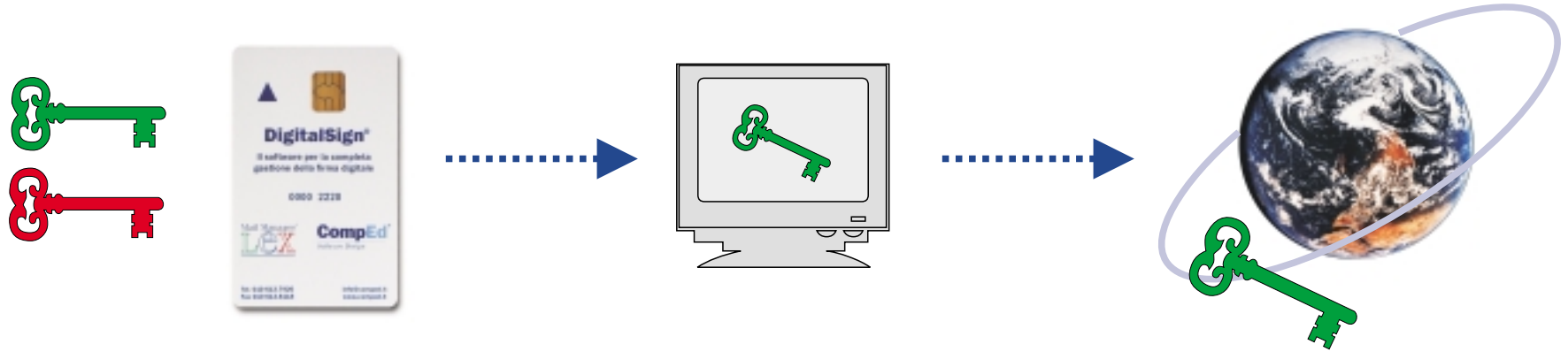
La tecnica di crittografia a **chiavi simmetriche (Triple DES)** utilizza la medesima chiave (codice di 192 bit) sia per cifrare che per decifrare il documento informatico

Crittografia a chiavi asimmetriche



La crittografia a **chiavi asimmetriche (RSA)** utilizza una coppia di chiavi (diverse) strettamente correlate.
Utilizzando la chiave A per cifrare si deve usare la B per decifrare. Viceversa è possibile usare la chiave B per cifrare e in tal caso è necessaria A per decifrare.

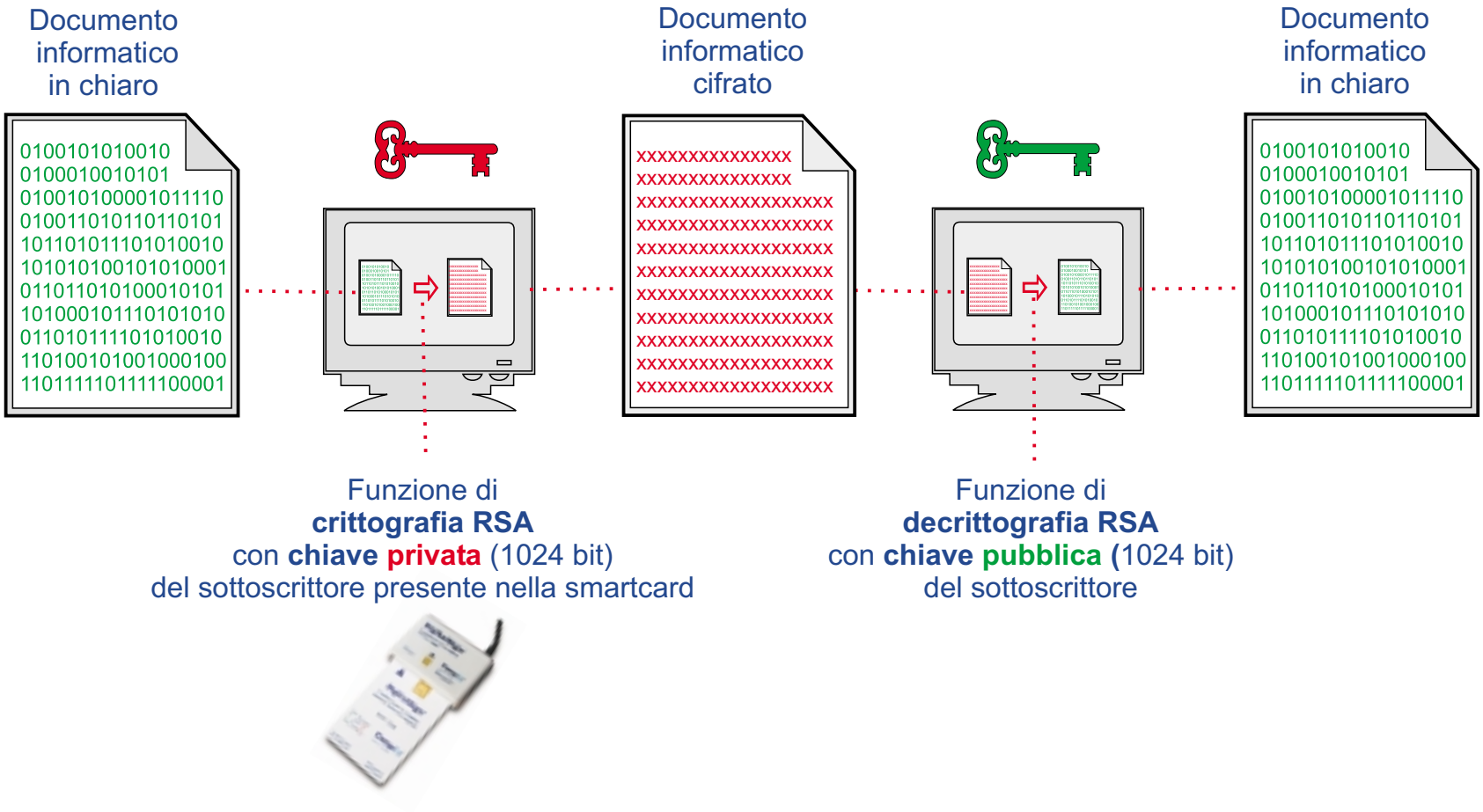
Chiave pubblica e chiave privata



Chiave pubblica e Chiave privata.
Lunghezza minima per la
legge italiana 1024 bit

Per la legge italiana la coppia di chiavi può essere generata dal titolare; in questo caso la generazione deve avvenire all'interno del dispositivo di firma, apparato elettronico programmabile solo all'origine (es: smartcard). Una delle due chiavi, quella privata, non uscirà mai dal dispositivo; l'altra, quella pubblica, verrà resa nota.

Crittografia a chiavi asimmetriche: chiave privata e chiave pubblica



Utilizzando la chiave privata per cifrare si deve usare la chiave pubblica per decifrare.

Le Autorità di Certificazione (CA) delle chiavi pubbliche

Le autorità di certificazione (CA) hanno il compito di garantire, in modo opponibile a terzi, l'associazione tra il soggetto titolare e la chiave pubblica e che non esistano due chiavi pubbliche identiche.

Allo scopo le CA effettuano la registrazione del titolare, opportuni controlli ed emettono un apposito certificato della chiave pubblica (documento informatico).

Pubblicano gli elenchi dei certificati validi, ne garantiscono la consultazione per via telematica e pubblicano gli elenchi dei certificati revocati o sospesi.

Requisiti delle autorità di certificazione

- Forma di società per azioni
- Capitale sociale non inferiore a quello necessario all'autorizzazione all'attività bancaria, se soggetti privati
- Altri requisiti (onorabilità dei rappresentanti legali e dei soggetti preposti all'amministrazione, competenza ed esperienza del personale, qualità dei processi informatici).

Il certificato della chiave pubblica

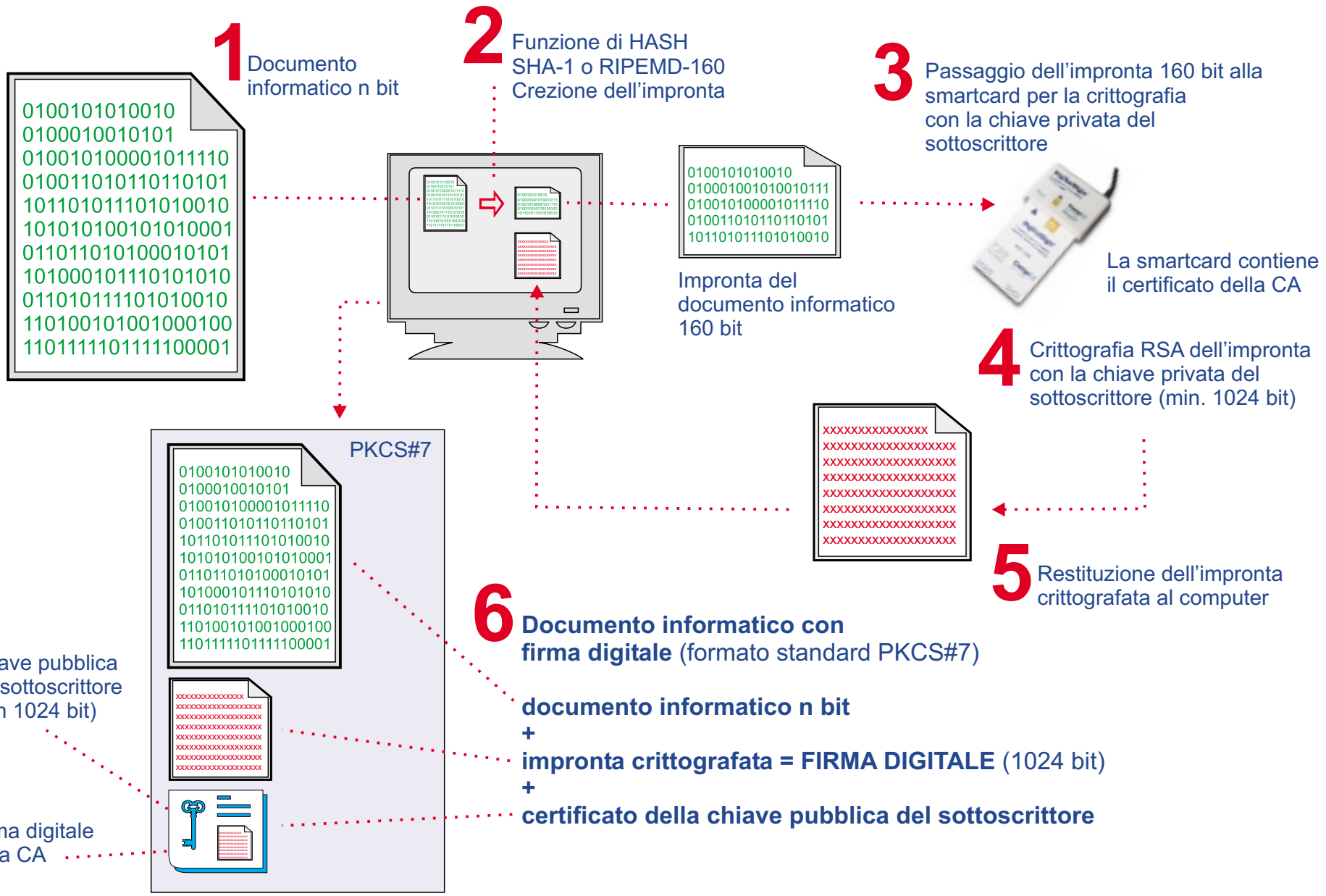
- Contiene, tra le altre informazioni:
  numero di serie del certificato
  ragione sociale del certificatore
  codice identificativo del titolare presso il certificatore
  nome, cognome e data di nascita del titolare
  valore della chiave pubblica
  inizio e fine del periodo di validità delle chiavi

- Una coppia di chiavi a 1024 bit può avere validità massima 2 anni.

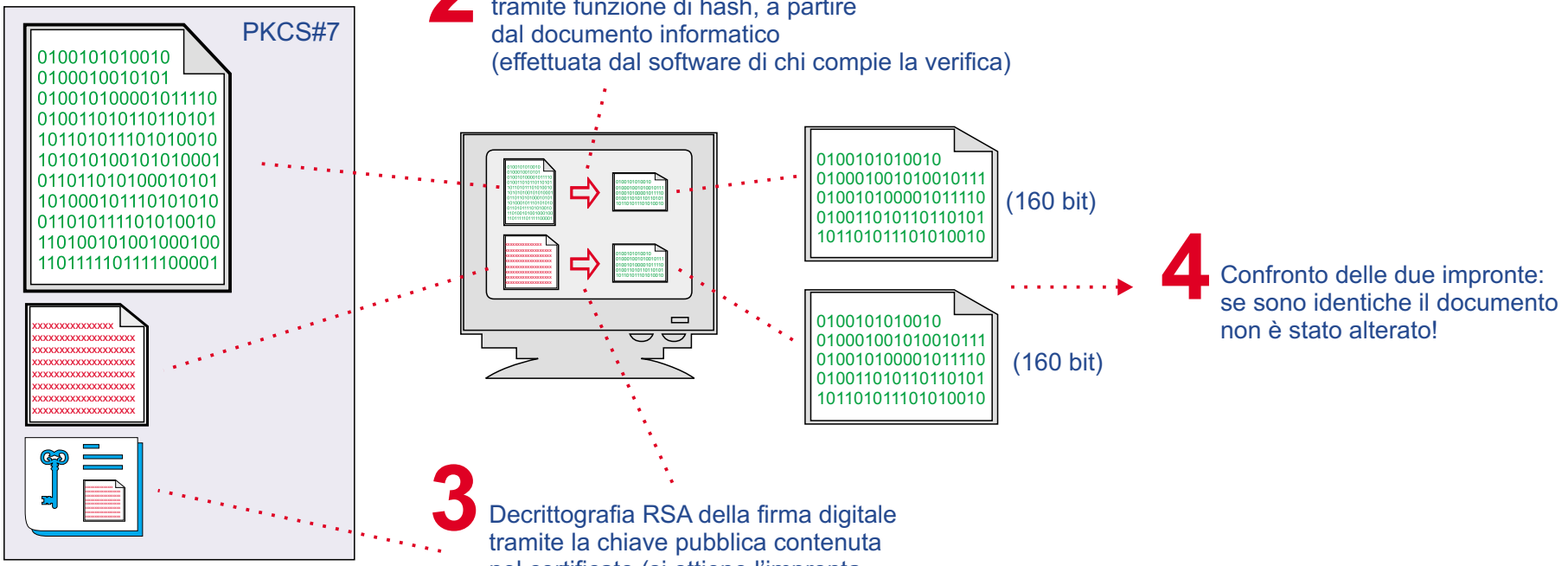
- Il termine di scadenza del certificato e il periodo di validità delle chiavi possono essere anticipati dal certificatore.

- Il certificato è un documento informatico firmato digitalmente dal certificatore.

Firma digitale di un documento informatico



Verifica di un documento informatico firmato digitalmente (documento non alterato)



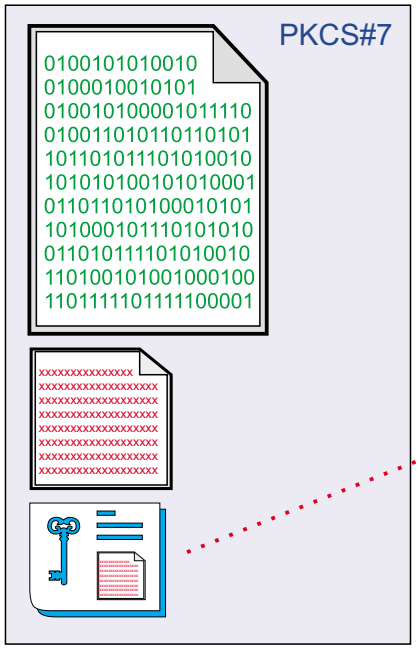
2 Creazione locale dell'impronta, tramite funzione di hash, a partire dal documento informatico (effettuata dal software di chi compie la verifica)

3 Decrittografia RSA della firma digitale tramite la chiave pubblica contenuta nel certificato (si ottiene l'impronta calcolata dal sottoscrittore).

4 Confronto delle due impronte: se sono identiche il documento non è stato alterato!

1 Documento informatico con firma digitale e certificato della chiave pubblica del sottoscrittore

Verifica di un documento informatico firmato digitalmente (verifica del certificato della chiave pubblica)



1 Il certificato è anch'esso un documento informatico, firmato digitalmente da un'autorità di certificazione. Il software dell'utente deve verificare la validità della firma digitale apposta sul certificato dalla CA. La verifica avviene tramite il certificato della chiave pubblica della CA, pubblicato nell'Elenco Pubblico dei certificatori a cura dell'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione).

2 E' necessario anche verificare che il certificato della chiave pubblica del sottoscrittore non sia stato sospeso o revocato dalla CA. Ciò avviene tramite un collegamento con protocollo LDAP al sito della CA (Registro dei certificati).

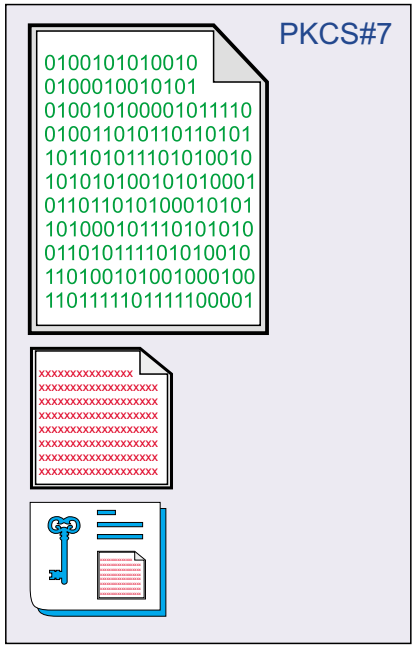
3 La validità del certificato della chiave pubblica attesta la validità della firma digitale, l'identità del sottoscrittore e i suoi poteri.

Validità temporale di una coppia di chiavi di firma digitale

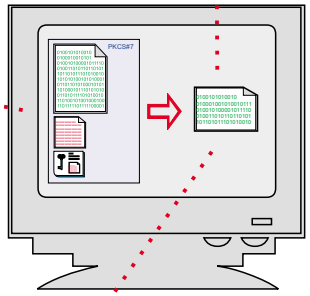
Per la legge italiana la validità massima di una coppia di chiavi di lunghezza 1024 bit non può superare i 2 anni, trascorsi i quali è necessario munirsi di una nuova coppia di chiavi di firma digitale.
Il periodo di validità della coppia è stabilito dal certificatore e specificato nel certificato della chiave pubblica.

Datazione certa (opponibile a terzi) di un documento informatico: la marca temporale

Le autorità di certificazione possono fornire anche un servizio per attribuire data certa (opponibile a terzi) a un documento informatico.

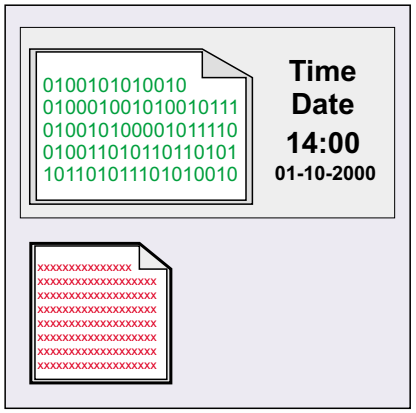


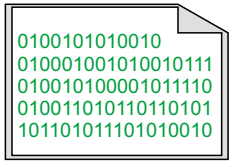
2 Invio della richiesta di marca temporale alla CA, allegando l'impronta (o più di una, calcolate con diverse funzioni di hash) del documento informatico



3 La CA restituisce la marca temporale, un documento informatico che contiene una serie di informazione tra cui:

- identificativo dell'emittente
- numero di serie della marca temporale
- algoritmo di firma della marca temporale
- identificativo del certificato della chiave pubblica con cui la CA ha firmato la marca
- **data e ora** di generazione della marca (entro un minuto dalla ricezione della richiesta)
- identificativo della funzione di hash usata per generare l'impronta della sequenza di simboli binari sottoposta a validazione temporale
- **impronta** calcola dalla CA a partire dall'impronta fornita dal richiedente
- **firma digitale** della marca apposta dalla CA





1 Generazione dell'impronta (calcolata sull'intero documento, firma e certificato inclusi)

Conservazione della validità dei documenti informatici nel tempo

Ipotizzando che si riceva un documento informatico con firma digitale, in che modo è possibile dimostrare che la firma è stata apposta in un momento di validità della chiave di sottoscrizione?

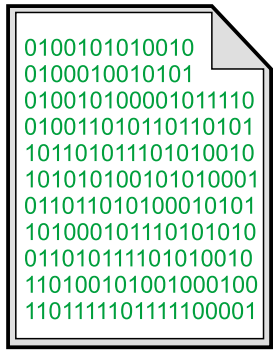
In che modo è possibile estendere la validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione?

Vi sono due possibilità:

1) Associazione di una o più marche temporali (e così via, alla scadenza di queste)

2) Conservazione su supporti ottici secondo le regole tecniche di cui alla deliberazione AIPA 24/98

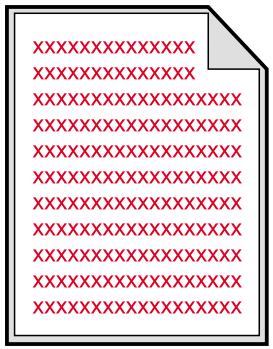
Operazione di cifratura di un documento informatico

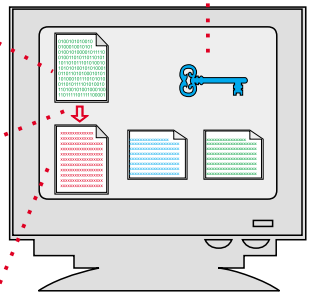


1 Documento informatico n bit

2 Crittografia simmetrica Triple DES con chiave generata casualmente dal sistema (192 bit)

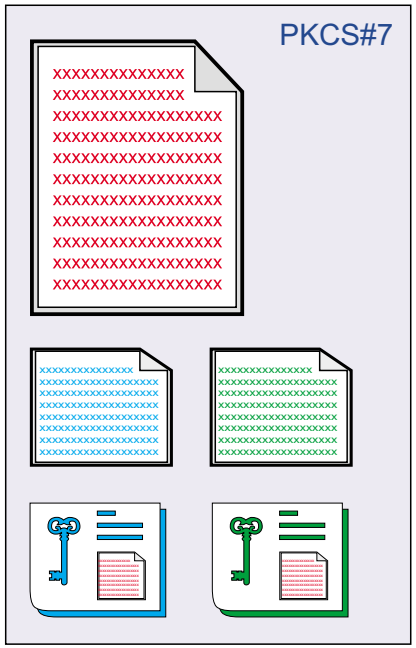
3 Documento informatico crittografato con funzione Triple DES e chiave casuale a 192 bit





4 Crittografia della chiave Triple DES tramite procedura RSA con la chiave pubblica del sottoscrittore e, se il documento è destinato a essere trasmesso, anche con la chiave pubblica del destinatario.

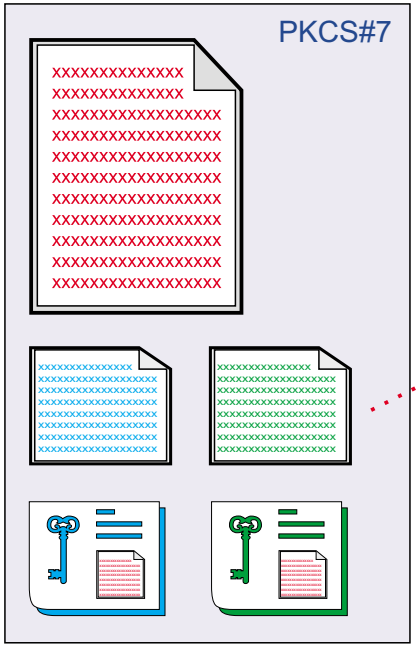
5 **Documento informatico cifrato (formato standard PKCS#7)**

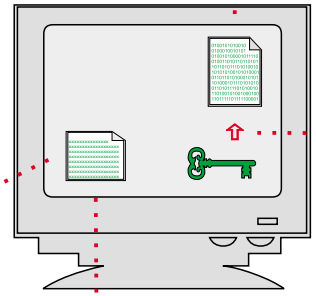


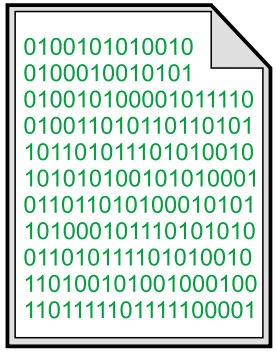
documento informatico n bit cifrato con chiave Triple DES
+
chiave Triple DES cifrata con chiave pubblica del sottoscrittore
+
chiave Triple DES cifrata con chiave pubblica del destinatario
+
chiave pubblica del sottoscrittore
+
chiave pubblica del destinatario

Operazione di decifratura di un documento informatico

1 Documento cifrato
con algoritmo Triple DES
e chiave casuale cifrata
(formato standard PKCS#7)







6 Documento informatico
in chiaro.
Il documento può ovviamente
contenere firma digitale e
certificato relativo.

5 Il documento viene
decifrato con la chiave
decifrata dalla smartcard
e algoritmo standard RSA

2 La chiave casuale cifrata viene
trasmessa alla smartcard

4 Restituzione della chiave
casuale decifrata al
computer

3 La chiave casuale viene
decifrata utilizzando
la propria chiave privata