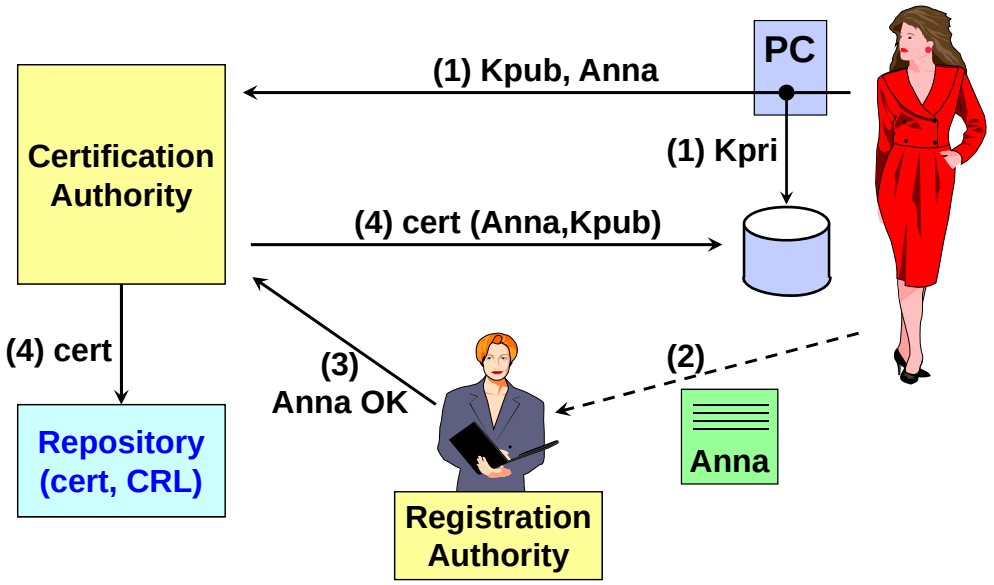
Lo standard X.509, le PKI ed i documenti elettronici

Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dipartimento di Automatica e Informatica

Autorità di certificazione



Certificati X.509

- **standard ITU-T X.509:**
  - v1 (1988)
  - v2 (1993) = minore
  - v3 (1996) = v2 + estensioni + cert. di attributo v1
  - v3 (2001) = v3 + certificati di attributo v2
- **è parte integrante dello standard X.500 per i servizi di directory (pagine bianche)**
- **è una soluzione al problema dell'identificazione del possessore di una chiave crittografica**
- **specifica in ASN.1 (Abstract Syntax Notation 1)**

X.509 versione 3

- **standard ultimato nel giugno 1996**
- **raccoglie in un unico documento le modifiche necessarie a estendere le definizioni dei certificati e delle CRL**
- **esistono estensioni di due tipi:**
  - pubbliche, ossia definite nello standard e quindi note a tutti
  - private, uniche per una certa comunità di utenti

Estensioni critiche

- **un'estensione può essere definita critica o non critica:**
  - nel processo di verifica devono essere rifiutati i certificati che contengono un'estensione critica non riconosciuta
  - un'estensione non critica può essere ignorata se sconosciuta
- **il differente trattamento è interamente a carico di chi effettua la verifica: il Relying Party (RP)**

Estensioni pubbliche

- **X.509v3 definisce quattro categorie di estensioni:**
  - key and policy information
  - certificate subject and certificate issuer attributes
  - certificate path constraints
  - CRL distribution points

Key and policy information

- **authority key identifier**
- **subject key identifier**
- **key usage**
- **private key usage period**
- **certificate policies**
- **policy mappings**

Key and policy information

- **key usage**
  - identifica lo spazio delle applicazioni per il quale la chiave pubblica può essere usata
  - può essere critica o non critica
  - se è critica allora il certificato può essere usato solo per gli scopi per cui la corrispondente opzione è definita

Key and policy information

- ***key usage* - le applicazioni definibili sono:**
  - digitalSignature (CA, user)
  - nonRepudiation (user)
  - keyEncipherment (user)
  - dataEncipherment
  - keyAgreement (encipherOnly, decipherOnly)
  - keyCertSign (CA)
  - cRLSign (CA)

Certificate subject and certificate issuer attributes

- **subject alternative name**
- **issuer alternative name**
- **subject directory attributes**

Certificate subject and certificate issuer attributes

- **subject alternative name**
  - consente di usare diversi formalismi per identificare il possessore del certificato (es. indirizzo e-mail, indirizzo IP, URL)
  - sempre critica se il campo subject-name è vuoto

X.509 alternative names

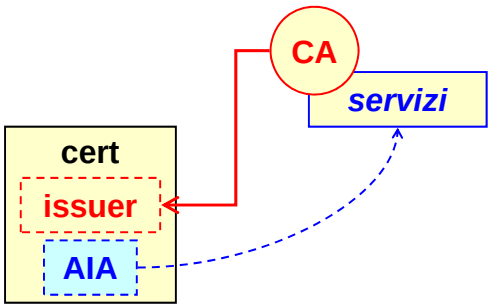
- **varie possibilità:**
  - rfc822Name
  - dNSName
  - iPAddress
  - uniformResourceIdentifier
  - directoryName
  - X400Address
  - ediPartyName
  - registeredID
  - otherName

CRL distribution point

- **CRL distribution point**
  - identifica il punto di distribuzione della CRL da usare nella verifica della validità di un certificato
  - può essere:
    - directory entry
    - e-mail o URL
  - critica o non critica

Estensioni private PKIX

- **authority information access**
  - indica come accedere ad informazioni e servizi della CA che ha emesso il certificato:
    - certStatus
    - certRetrieval
    - cAPolicy
    - caCerts
  - critica o non critica



Extended key usage

- **in aggiunta o in sostituzione di keyUsage**
- **valori possibili [bit compatibili]:**
  - (id-pkix.3.1) serverAuth [DS, KE, KA]
  - (id-pkix.3.2) clientAuth [DS, KA]
  - (id-pkix.3.3) codeSigning [DS]
  - (id-pkix.3.4) emailProtection [DS, NR, KE, KA]
  - (id-pkix.3.8) timeStamping [DS, NR]
  - (id-pkix.3.9) ocspSigning [DS, NR]

CRL X.509

- **Certificate Revocation List**
- **elenco dei certificati revocati**
- **le CRL sono emesse periodicamente e mantenute dagli emettitori dei certificati**
- **le CRL sono firmate:**
  - dalla CA che ha emesso i certificati
  - da una revokation authority delegata dalla CA (indirect CRL, iCRL)

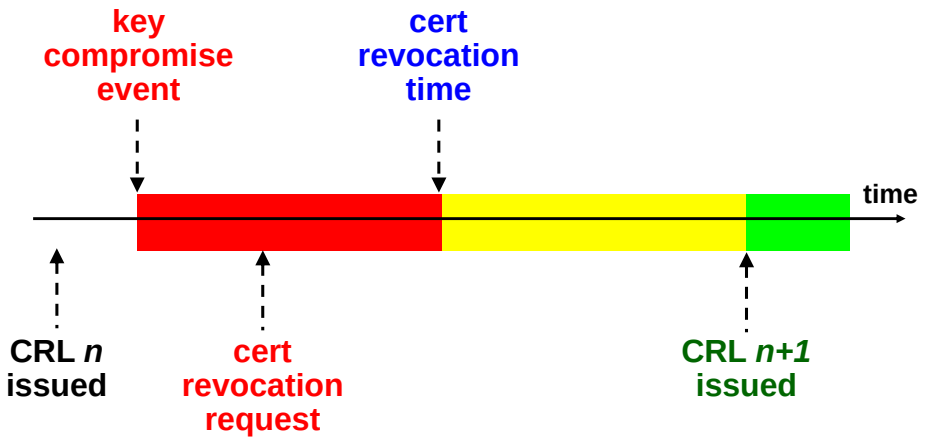
CRL X.509 versione 2

```
CertificateList ::= SEQUENCE {
   tbsCertList          TBSCertList,
   signatureAlgorithm   AlgorithmIdentifier,
   signatureValue       BIT STRING }
TBSCertList ::= SEQUENCE {
   version              Version OPTIONAL,
                        -- if present, version must be v2
   signature            AlgorithmIdentifier,
   issuer               Name,
   thisUpdate           Time,
   nextUpdate           Time OPTIONAL,
   revokedCertificates  SEQUENCE {
      userCertificate   CertificateSerialNumber,
      revocationDate    Time,
      crlEntryExtensions Extensions OPTIONAL
   } OPTIONAL,
   crlExtensions        [0] Extensions OPTIONAL
}
```

Estensioni delle CRLv2

- **crlEntryExtensions:**
  - reason code
  - hold instruction code
  - invalidity date
  - certificate issuer (importante per iCRL)
- **crlExtensions:**
  - authority key identifier
  - issuer alternative name
  - CRL number
  - delta CRL indicator
  - issuing distribution point

Certificate revocation timeline

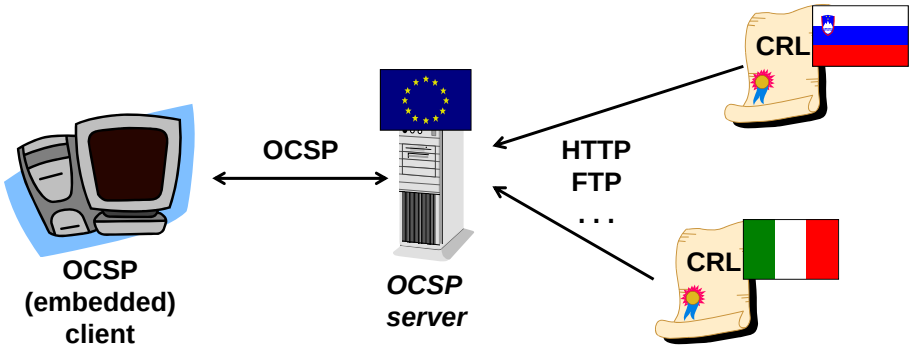


OCSP

- **RFC-2560: On-line Certificate Status Protocol**
- **standard IETF-PKIX per verificare in linea se un certificato è valido:**
  - good
  - revoked
    - revocationTime
    - revocationReason
  - unknown
- **risposte firmate dal server (non dalla CA!)**
- **certificato del server non verificabile con OCSP!**

Architettura di OCSP

- **possibili risposte pre-calcolate**
  - diminuisce il carico sul server … ma rende possibili attacchi di tipo replay!
- **possibile attingere informazioni non da CRL**

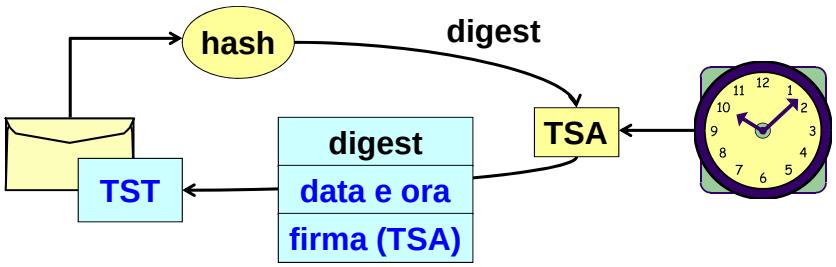


Modelli di OCSP responder

- **Trusted Responder**
  - il server OCSP firma le risposte con una coppia chiave:cert indipendente dalla CA per cui sta rispondendo
  - responder aziendale o TTP pagata dagli utenti
- **Delegated Responder**
  - il server OCSP firma le risposte con una coppia chiave:cert diversa in base alla CA per cui sta rispondendo
  - TTP pagata dalle CA

Time-stamping

- **prova della creazione dei dati prima di un certo istante di tempo**
- **TSA (Time-Stamping Authority)**
- **RFC-3161:**
  - protocollo di richiesta (TSP, Time-Stamp Protocol)
  - formato della prova (TST, Time-Stamp Token)

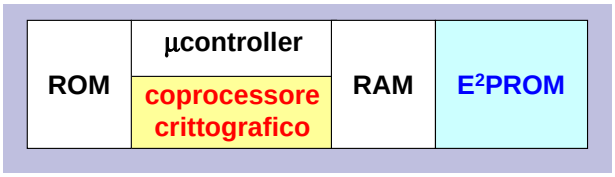


PSE (Personal Security Environment)

- **ogni utente dovrebbe proteggere:**
  - la propria chiave privata (segreta!)
  - i certificati delle root CA fidate (autentiche!)
- **software PSE:**
  - file (cifrato) della chiave privata
- **hardware PSE:**
  - passivo = chiavi protette
  - attivo = chiavi protette + operazioni crittografiche
- **mobilità possibile (ma con problemi) in entrambi casi**

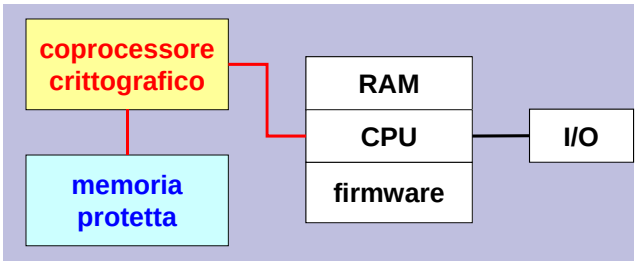
Smart-card crittografiche

- **carte a chip a memoria e con capacità crittografiche autonome**
- **semplici: DES**
- **complesse: RSA**
  - lunghezza della chiave?
  - generazione della chiave privata a bordo?
- **poca memoria (EEPROM): 4 - 32 Kbyte**



HSM (HW Security Module)

- **acceleratore crittografico per server**
  - memoria protetta (chiave privata)
  - capacità crittografiche autonome (RSA, talvolta anche algoritmi simmetrici)
- **sotto forma di scheda PCI o dispositivo esterno (USB, IP, SCSI, …)**



API di sicurezza (basso livello)

- **PKCS-11 = (solo) crypto engine**
  - in software
  - in hardware
    - smart card
    - scheda crittografica
  - parte dell'architettura CDSA
- **MS-CAPI CSP (Crypto Service Provider)**
  - stesse funzioni di PKCS-11 ma proprietario di MS

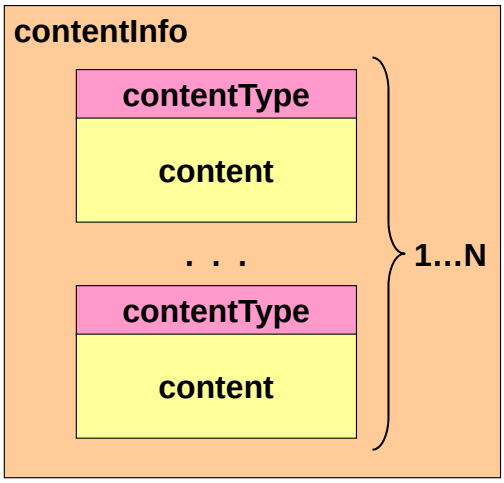
Formati sicuri per i dati

- **PKCS-7 = busta sicura**
  - firmata e/o cifrata
- **PKCS-10 = richiesta di certificati**
  - nel colloquio tra client e CA / RA
- **PKCS-12 = software PSE (Personal Security Environment)**
  - portabilità di chiavi e certificati
- **non sono formati applicativi:**
  - S/MIME? IDUP-GSS-API? XML-DSIG?
  - documenti elettronici a norme di legge?

Formati PKCS-7 e CMS

- cryptographic message syntax
- PKCS-7 è lo standard RSA per la busta sicura (v1.5 è anche RFC-2315)
- CMS è l'evoluzione di PKCS-7 in seno alla IETF, codificato come RFC-2630
- permette firma e/o cifratura dei dati, con algoritmi simmetrici o asimmetrici
- permette di apporre più firme su uno stesso oggetto (gerarchiche o parallele)
- può includere i certificati usati per la firma
- è un formato recursivo

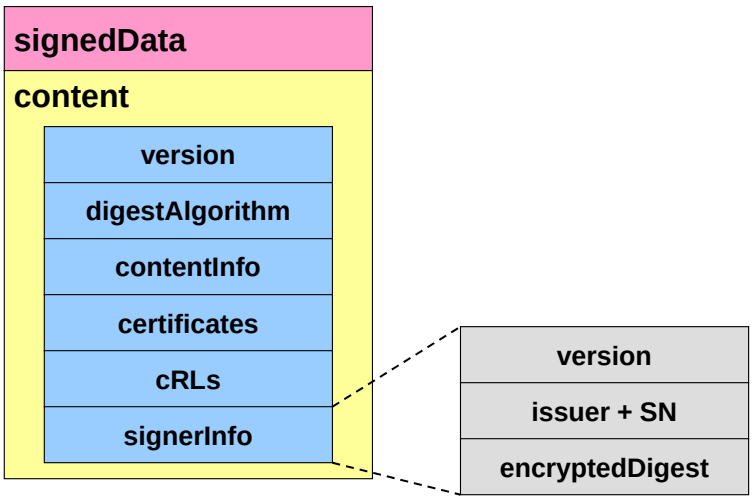
PKCS-7: struttura



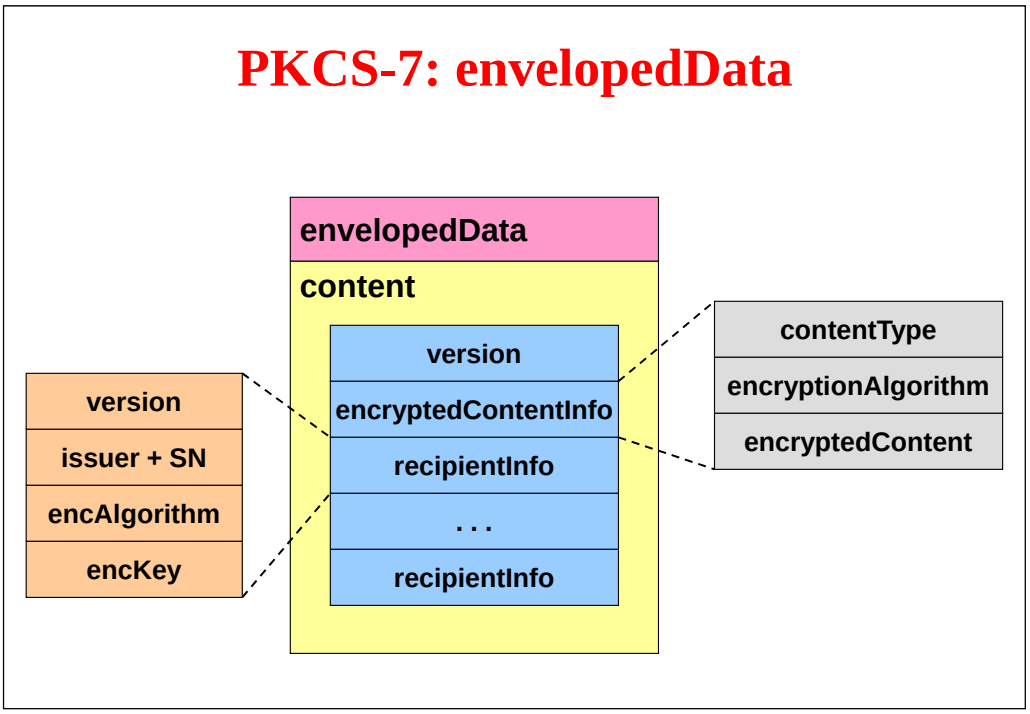
PKCS-7: contentType

- ***data***
  codifica di una generica sequenza di byte
- ***signedData***
  dati + firme digitali (1..N) parallele
- ***envelopedData***
  dati cifrati simm. + chiave cifrata con RSA
- ***signedAndEnvelopedData***
  cifratura RSA di (dati + firme digitali)
- ***digestData***
  dati + digest
- ***encryptedData***
  dati cifrati con algoritmo simmetrico

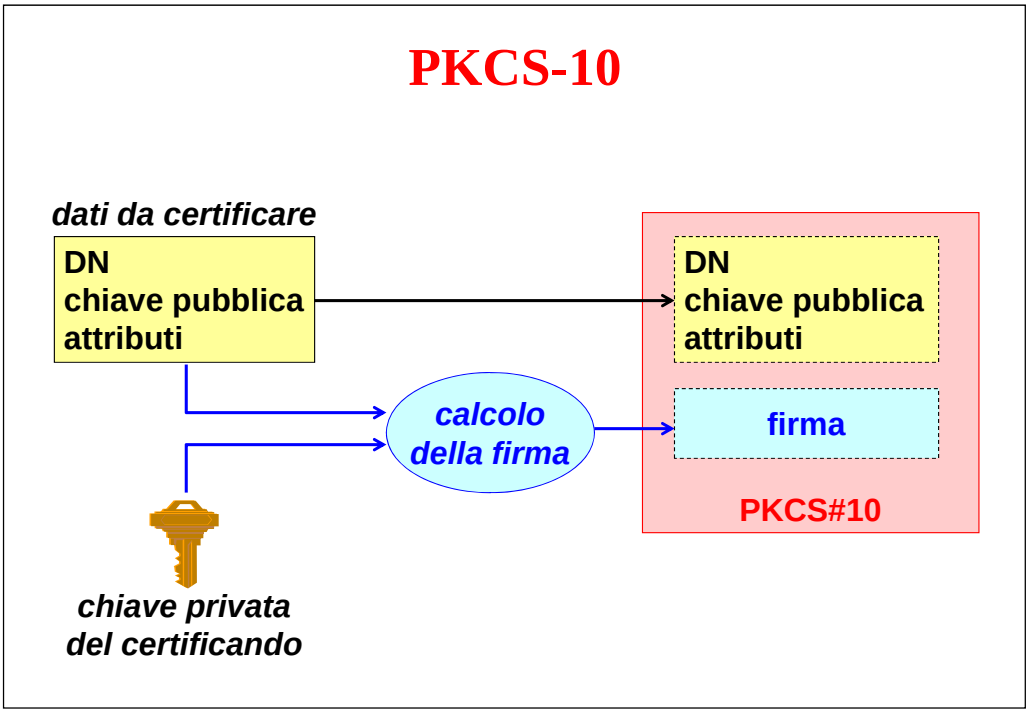
PKCS-7: signedData



PKCS-7: envelopedData

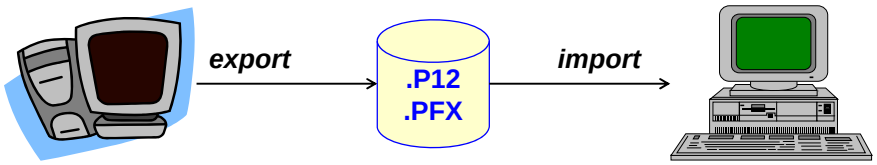


PKCS-10

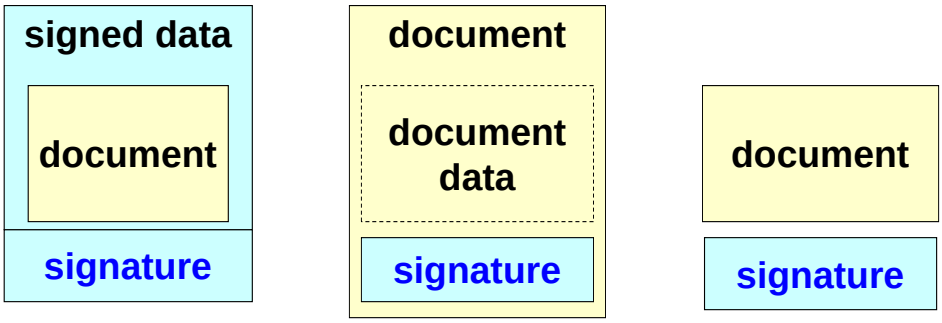


Formato PKCS-12 (security bag)

- trasporto di materiale crittografico (personale) tra applicazioni / sistemi diversi
- trasporta una chiave privata e uno o più certificati
- trasporto dell'identità digitale di un utente
- usato da Netscape, Microsoft, Lotus, …
- criticato dal punto di vista tecnico (specie nell'implementazione MS) ma molto diffuso



Formati di documenti firmati

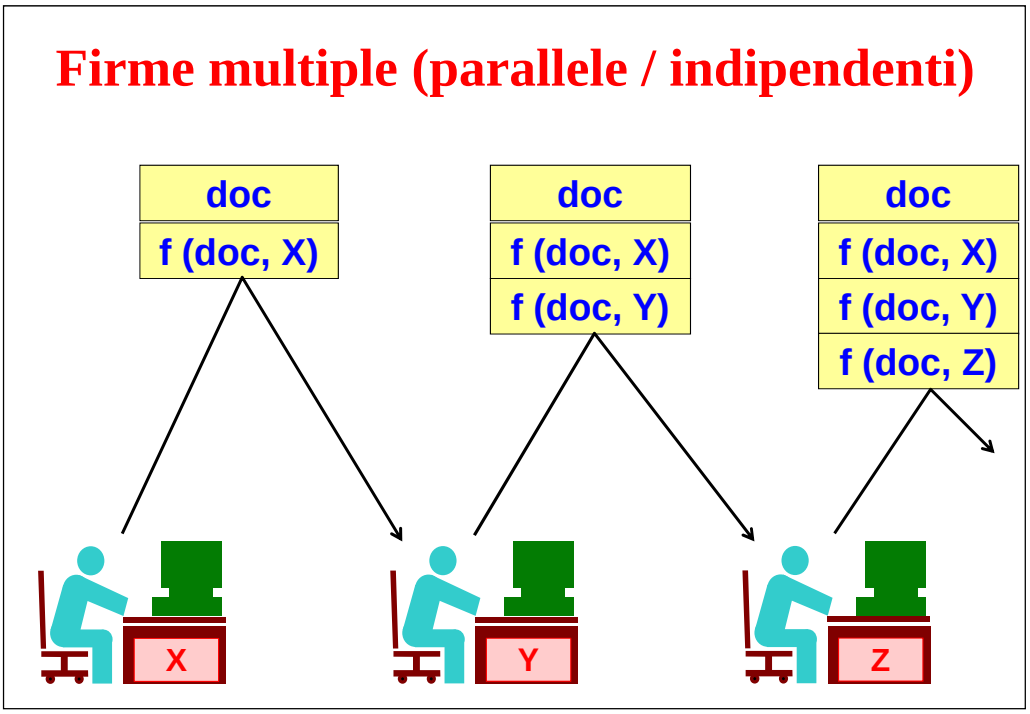


enveloping signature (es. PKCS-7)

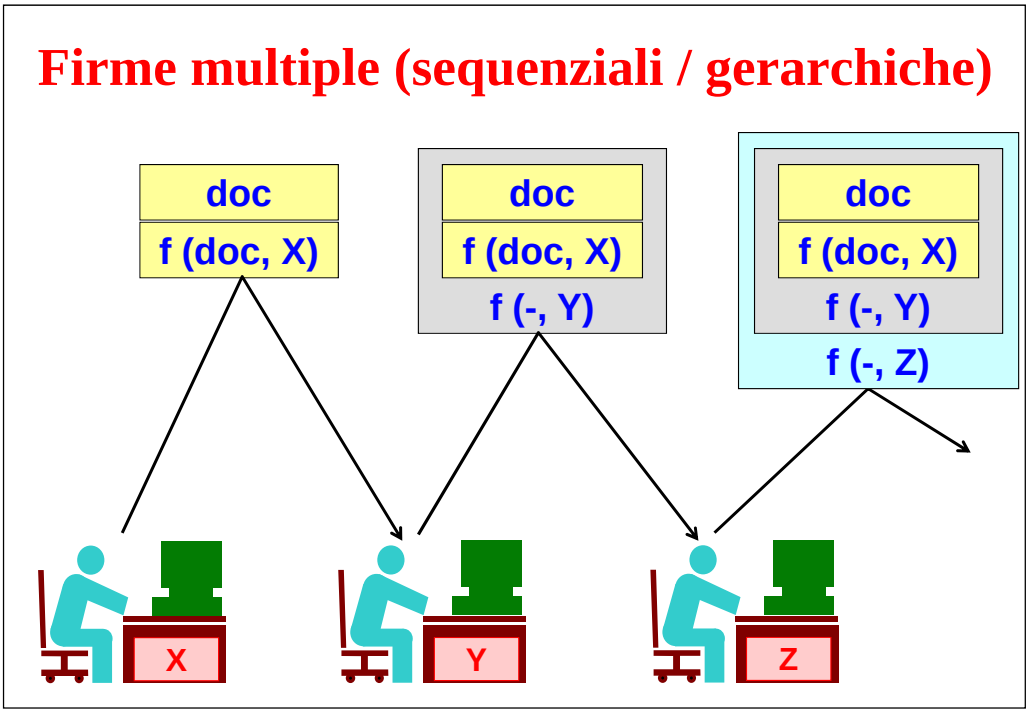
enveloped signature (es. PDF)

detached signature (es. PKCS-7)

Firme multiple (parallele / indipendenti)



Firme multiple (sequenziali / gerarchiche)

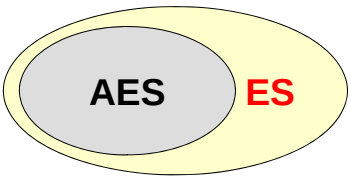


Electronic Signature (ES) europea

- **dati in formato elettronico attaccati o logicamente associati con altri dati in formato elettronico che ne forniscono un mezzo di autenticazione**
- **ATTENZIONE: una firma scannerizzata è una Electronic Signature (!)**
- **non può essere negato valore legale ad una firma elettronica solo perché:**
  - è in forma elettronica
  - non è basata su *qualified certificate*
  - non usa certificati emessi da certificatori autorizzati
  - non è stata creata con un dispositivo di firma sicuro

Advanced Electronic Signature (AES)

- **una ES che soddisfa i seguenti requisiti:**
  - è in relazione univoca con il firmatario
  - consente di identificare il firmatario
  - è creata usando strumenti che il firmatario può mantenere sotto il suo controllo
  - è in relazione con i dati ai quali si riferisce in modo che ogni successiva modifica dei dati possa essere individuata



Qualified Certificate (QC)

- **è un certificato che garantisce l'identità di una persona e contiene:**
  - l'indicazione che si tratta di un QC
  - l'indicazione del certificatore e dello stato in cui è stato emesso
  - indicazioni sulle limitazioni di utilizzo del certificato
  - indicazioni sul limite delle transazioni commerciali effettuabili con quel certificato
- **RFC-3739 = profilo IETF-PKIX per QC**

Qualified Electronic Signature (QES)

- **è una advanced electronic signature apposta usando:**
  - qualified certificate
  - dispositivi di firma sicuri
- **ha valore legale equivalente alla firma autografa**