La Firma Digitale
e le sue applicazioni

Ing. Francesca Merighi
CINECA
Tel. 051 6171916
e-mail: f.merighi@cineca.it

www.cineca.it

Sommario

Introduzione

Dematerializzazione documentale
Definizione e normativa sulla Firma Digitale

Dematerializzazione

Sostituzione dei documenti cartacei con **documenti informatici**

Ciclo di vita del documento

- **Creazione**
- **Protocollazione**
- **....**
- **Trasmissione**
- **Conservazione**

Costi → **Riorganizzazione** dei processi amministrativi, riorganizzazione e formazione del personale

Benefici → **Efficienza ed efficacia**, in termini di **risparmio** di carta, spazio, tempo

Strumenti a garanzia dell'affidabilità del documento informatico

Firma Digitale

Legge 59/27

Documento informatico con **Firma Digitale**
stesso valore
documento cartaceo con **firma autografa**

Formati e regole tecniche

Tecnologia abilitante della dematerializzazione

Know-how

CINECA

Firma Digitale → trasformazione sul documento informatico che

- è basata su **chiavi crittografiche** correlate tra loro
  - **Chiave privata** — Rende manifesta
  - **Chiave pubblica** — Verifica
  - **Apposizione firma**
  - **Verifica firma**
- provenienza ← garantisce la **connessione univoca** tra firmatario e documento firmato
- integrità ← consente di rilevare se il documento è stato **modificato dopo la trasformazione**
- SMARTCARD ← è eseguita mediante un **dispositivo sicuro** sul quale il firmatario ha controllo esclusivo
- Per documenti da e verso le **Pubbliche Amministrazioni** è basata su certificato emesso da un **certificatore accreditato CNIPA**
  - 15 certificatori accreditati, tra i più noti InfoCert, Actalis e Postecom

Parte 1

Operazioni di apposizione e verifica della Firma Digitale

Operazione di firma RSA
Operazione di imbustamento
Operazione di verifica della firma RSA

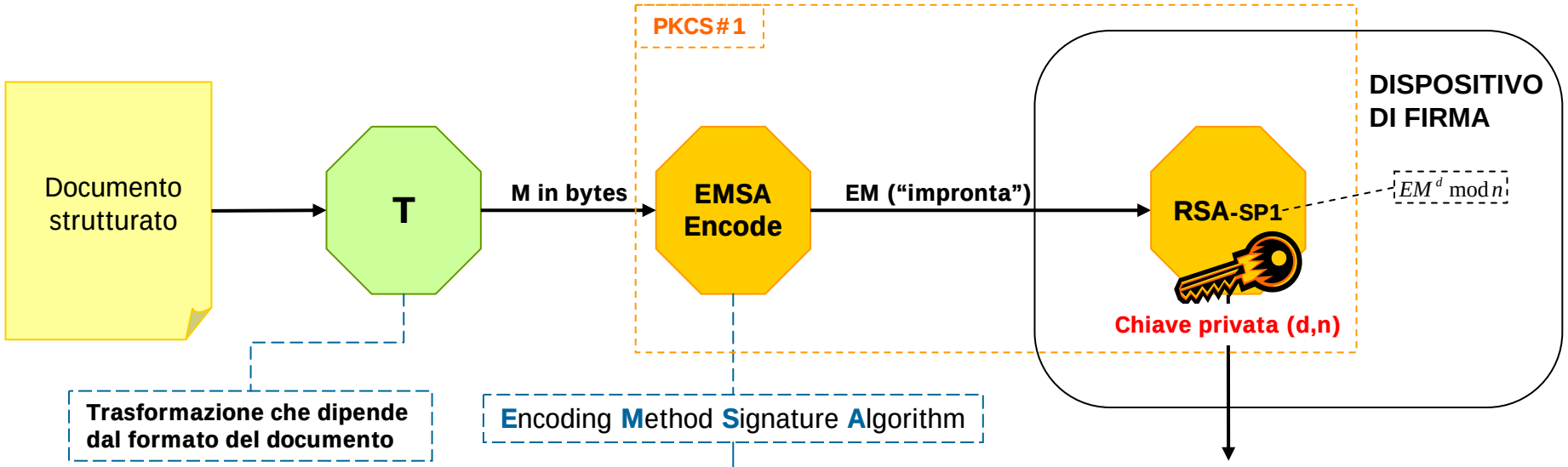
Utilizzo di standard → **Interoperabilità**

PKCS#1
- Primitive di firma e verifica della **firma RSA**
- Primitive di cifratura e decifratura RSA

X509 → Formato dei **Certificati Digitali** e degli oggetti ad essi correlati (CRL, ecc.)

PKCS#11 → Interfaccia fra applicazione e **dispositivi di firma**

Operazione di firma (RSA)



Funzione basata su Hash che protegge da attacchi di **contraffazione**

EMSA-PKCS1-v1_5

(deterministico)

EM = 0x00 | | 0x01 | | 0xff | | 0xff...0xff | | 0x00 | | Hprefix | | H

(0xff: p volte)

H = impronta di EM

HPrefix = prefisso distintivo per ogni algoritmo di hash

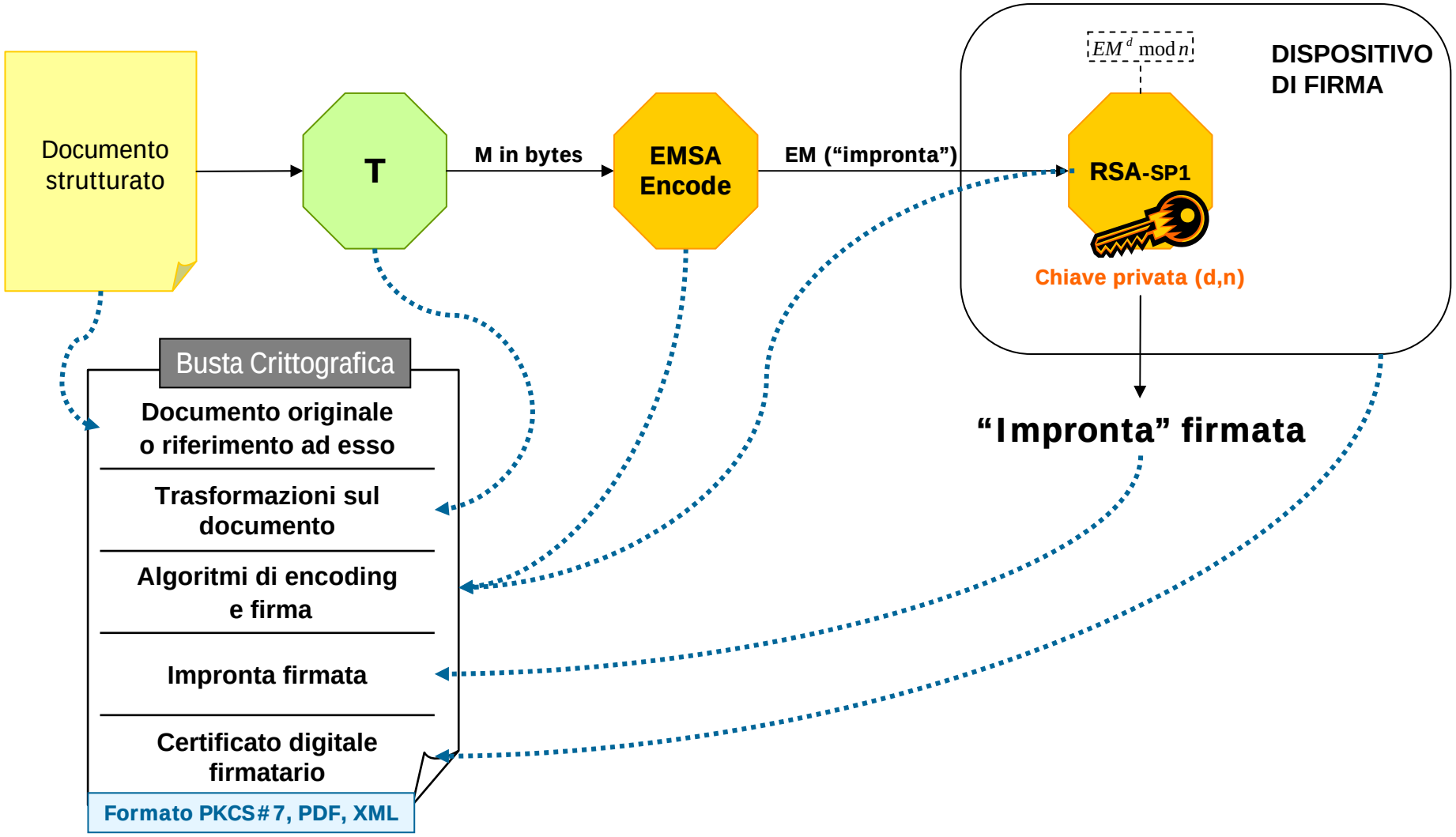
p= *nLen – emLen – hLen - hPrefixLen*

EMSA-PSS

(probabilistico)

Impronta "mascherata" con un numero casuale, allegato in EM

Operazione di imbustamento



Operazione di verifica della firma (RSA)
Controllo di integrità e provenienza

Busta Crittografica

Documento originale
o riferimento ad esso

Trasformazioni sul
documento

Algoritmi di encoding
e firma

Impronta firmata

Certificato digitale
firmatario

T

M

PKCS#1

EMSA
Verify

Firma valida

Firma non valida

EM'

$S^e \bmod n$

RSA-VP1

Chiave pubblica (e,n)

EMSA-PKCS-v1_5 Verify

M

EMSA
PKCS-v1_5
Encode

EM

EM'

=?

si

Firma valida

no

Firma non valida

EMSA-PSS Verify

- "Smaschera" EM' ottenendo l'impronta H'

- Confronta H' con H=Hash(M):
  se sono uguali firma valida

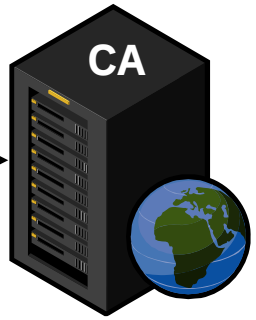
Controllo certificato di Firma Digitale

Standard X509

Busta Crittografica

- **Documento originale o riferimento ad esso**
- **Trasformazioni sul documento**
- **Algoritmi di encoding e firma**
- **Impronta firmata**
- **Certificato digitale firmatario**

- **Controllo integrità e affidabilità ente emettitore**
  - **Controllo firma CA**
  - **Controllo CA affidabile**
- **Controllo scadenza**
- **Controllo stato di revoca**
  - **O**nline **C**ertificate **S**tatus **P**rotocol
  - Controllo **C**ertificate **R**evocation **L**ist



Parte 2

Dispositivi di Firma Digitale

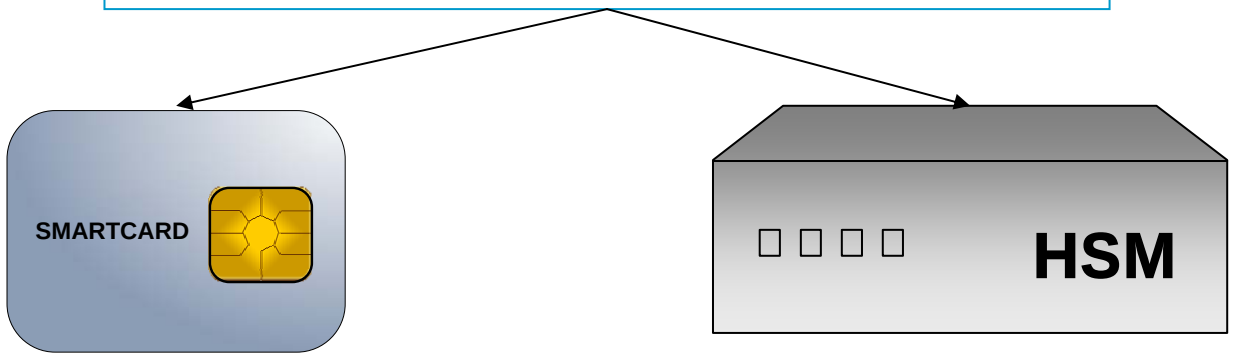
Smartcard
Hardware Security Module
Interfaccia PKCS#11 ai dispositivi di firma

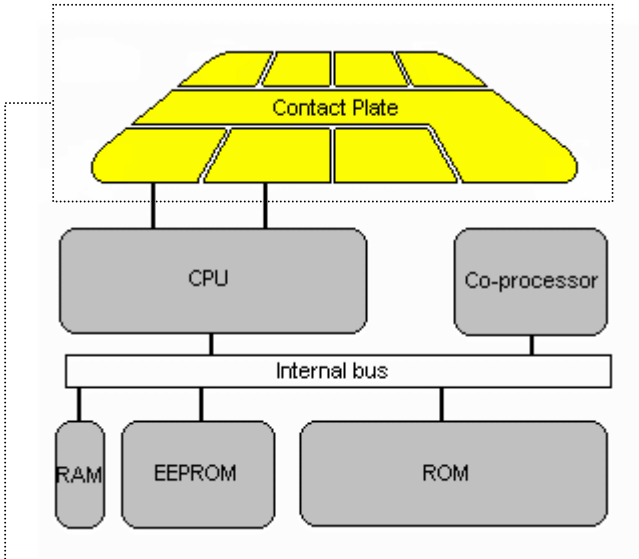
Dispositivi fisici che
contengono oggetti (**chiavi private**, **chiavi pubbliche** e **certificati digitali**),
attraverso i quali eseguono **operazioni crittografiche**

Operazioni che coinvolgono la **chiave privata** avvengono **all'interno del dispositivo**
Non è possibile estrarre le chiavi private dai dispositivi

Information Technology Security Evaluation Criteria (ITSEC)
Insieme strutturato di criteri di valutazione della sicurezza di un sistema

Normativa italiana : Firma Digitale ottenuta con
dispositivi certificati ITSEC Livello 3





CPU: CISC a 5 Mhz

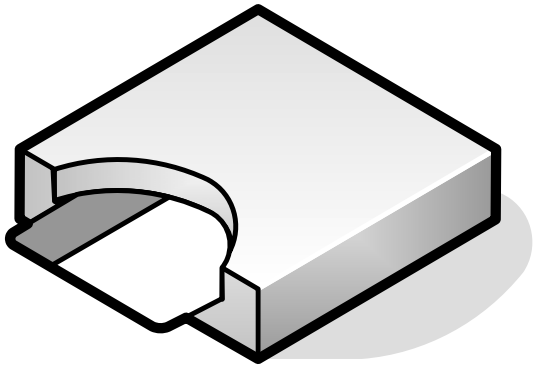
ROM: Contiene **sistema operativo** e programmi "fissi" (2k/64k)

PROM: Contiene il **numero seriale** della smartcard (32/64 bytes)

RAM: utilizzata per **dati temporanei**, si cancella quando si estrae la smartcard dal lettore (128/1024 byte)

EEPROM: Memorizza informazioni variabili (**chiavi e certificati**) (circa 128k)

Interfaccia Input/Output: velocità del flusso dati 9600 bit/sec, protocolli T=0 e **T=1**



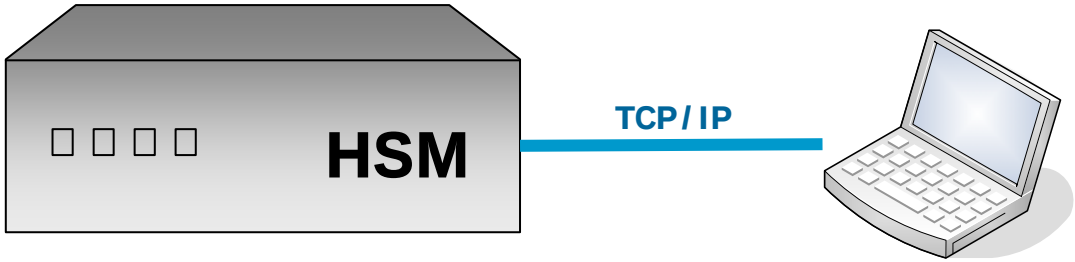
ISO 7816 - Standard di riferimento per smartcard che definisce

- ✓ Caratteristiche fisiche ed elettriche
- ✓ I protocolli di comunicazione verso il lettore di smarcard (**T=0**, **T=1**)
- ✓ Comando di risposta al reset (**A**nswer **T**o **R**eset) ➡ modello smartcard
- ✓ *Protocollo di comunicazione verso le applicazioni (**A**pplication **P**rotocol **D**ata **U**nit): spesso non rispettato dai produttori di smartcard*

Circa 1 operazione al secondo

Costo 10-50 euro **(+ circa 25 euro per il lettore)**

Hardware Security Module



Dispositivo crittografico ad alte prestazioni

Sistema complesso con hardware dedicato

Stesse funzionalità delle smartcard

Dispositivo di rete con interfaccia TCP/IP

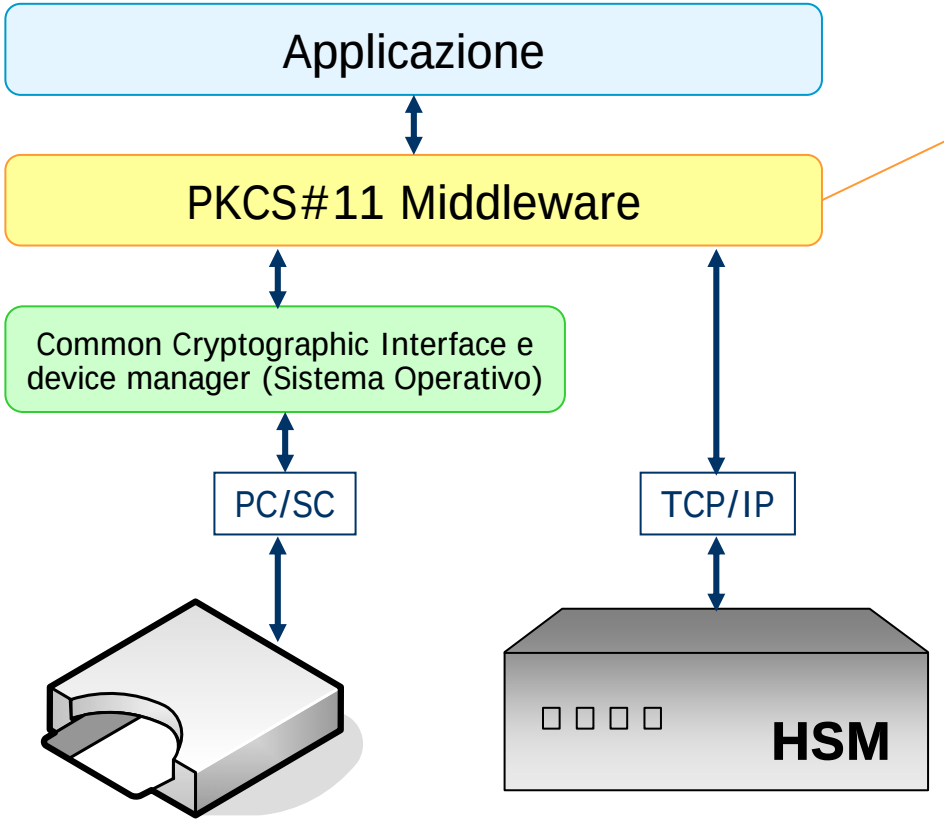
Accesso via rete con autenticazione

Collegabili in cascata

Tipicamente utilizzato da Certification Authority e
sistemi di firma massiva (es. conservazione documentale)

Dalle 200 alle 1000 operazioni al secondo

Costo dai 20.000 euro in su



Standard PKCS#11

Interfaccia standard di accesso alle funzioni del dispositivo crittografico
(lettura, scrittura, operazioni crittografiche..)

Applicazioni indipendenti dai dispositivi crittografici
Condivisione sicura delle risorse (gestione accesso contemporaneo)

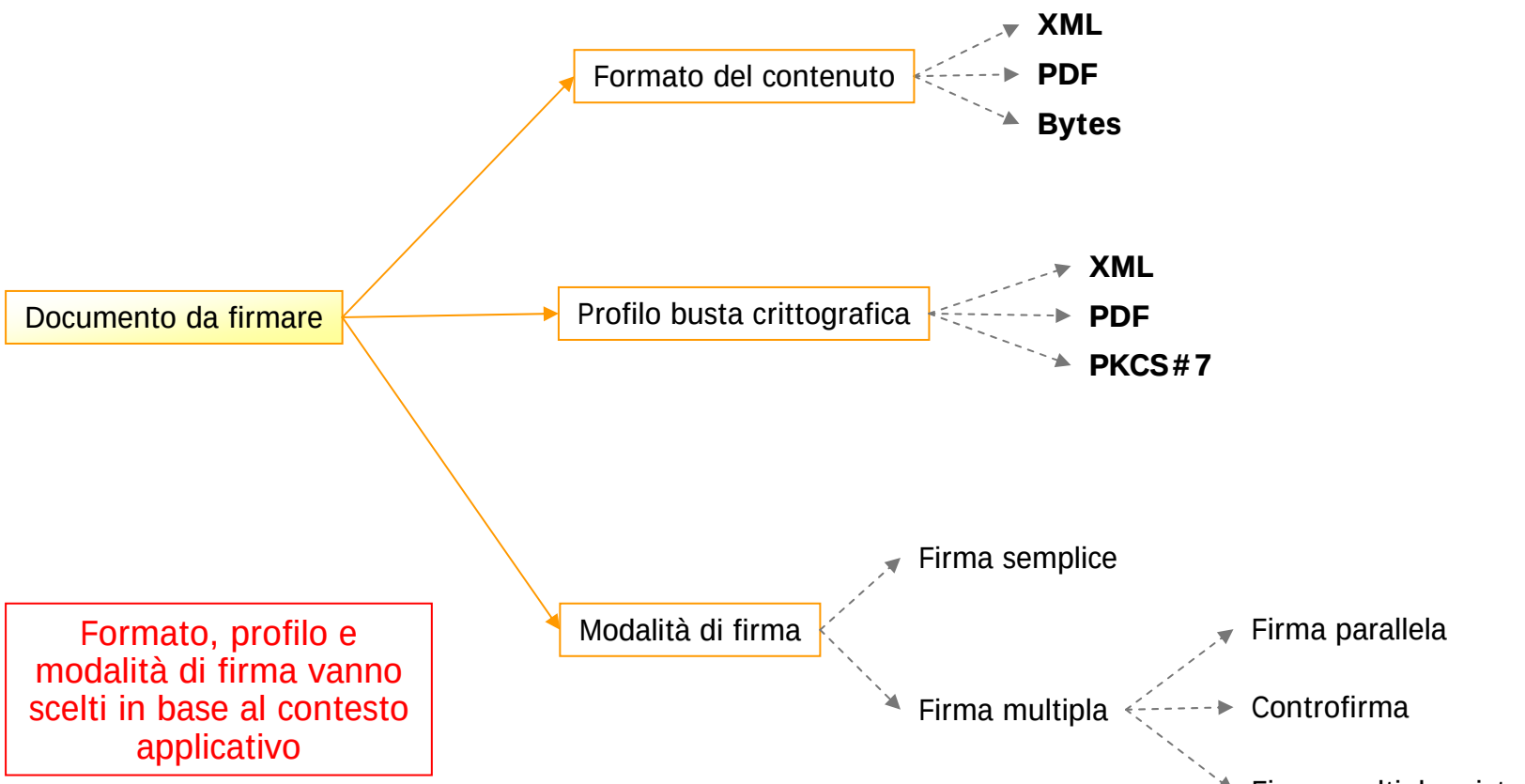
Si concretizza in un set di driver, dipendenti da dispositivo crittografico e sistema operativo

Il driver utilizza le APDU per comunicare con la smartcard interfacciandosi con gli strati sottostanti

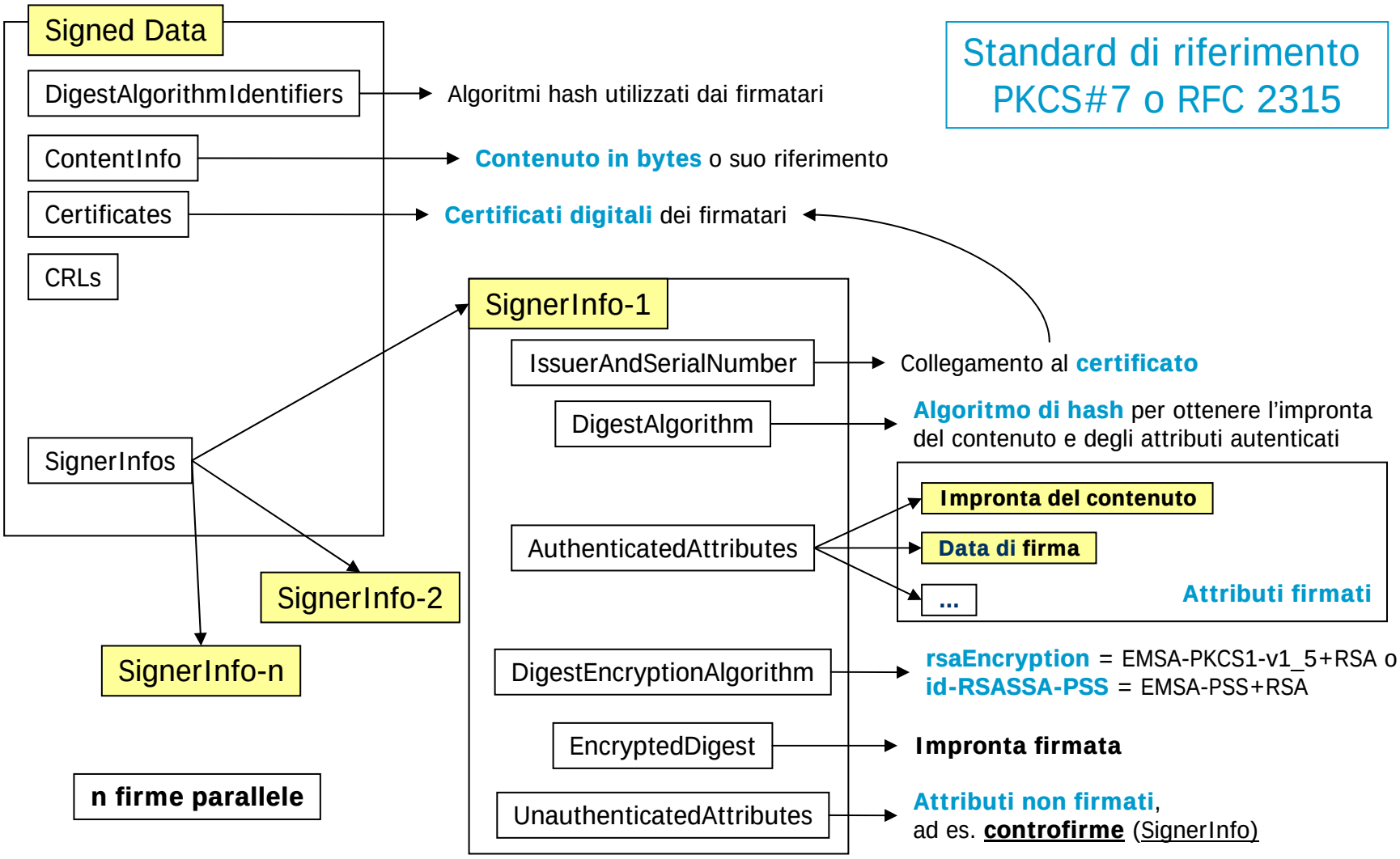
Parte 3

Profili di Firma Digitale

PKCS#7
PDF
XML

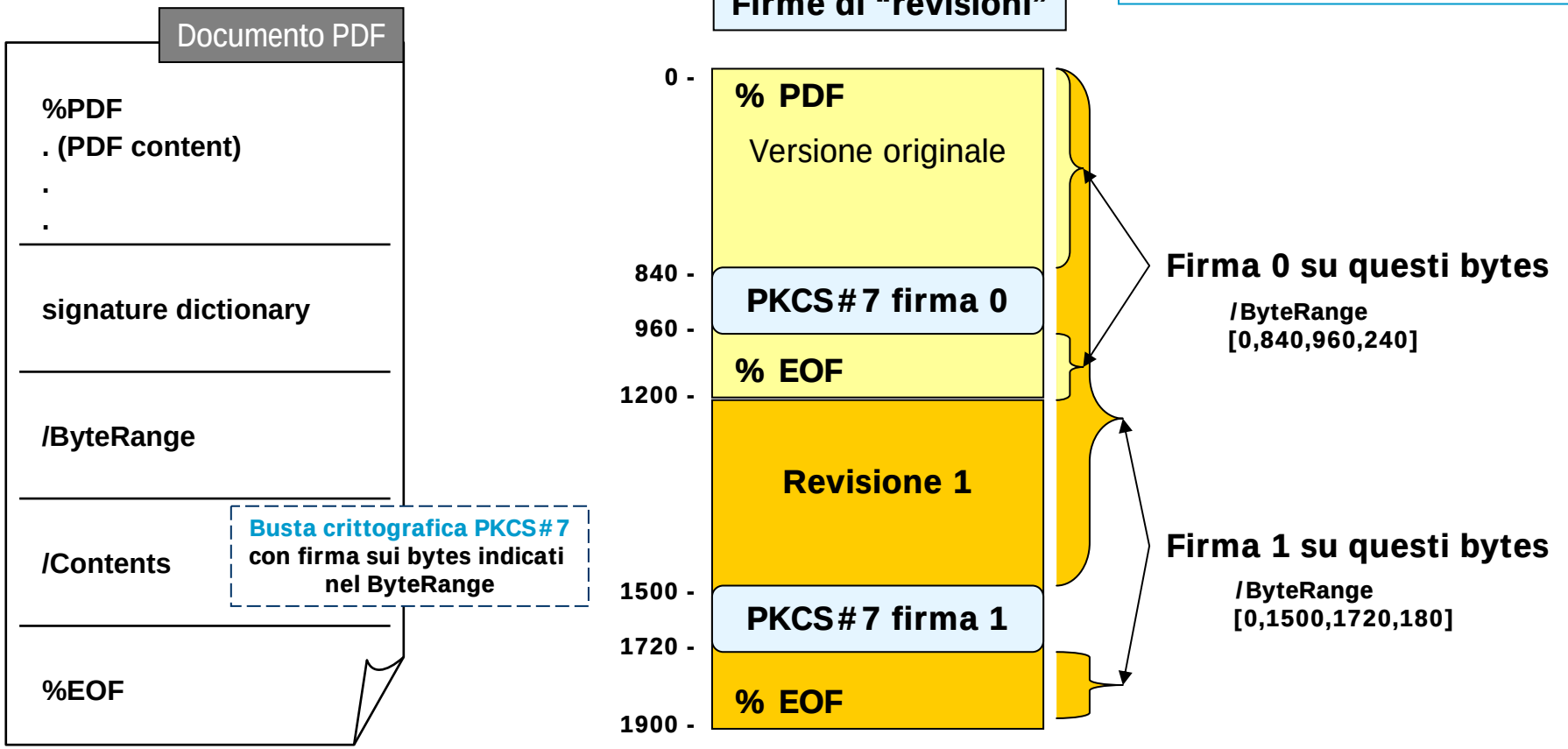


Formato, profilo e modalità di firma vanno scelti in base al contesto applicativo

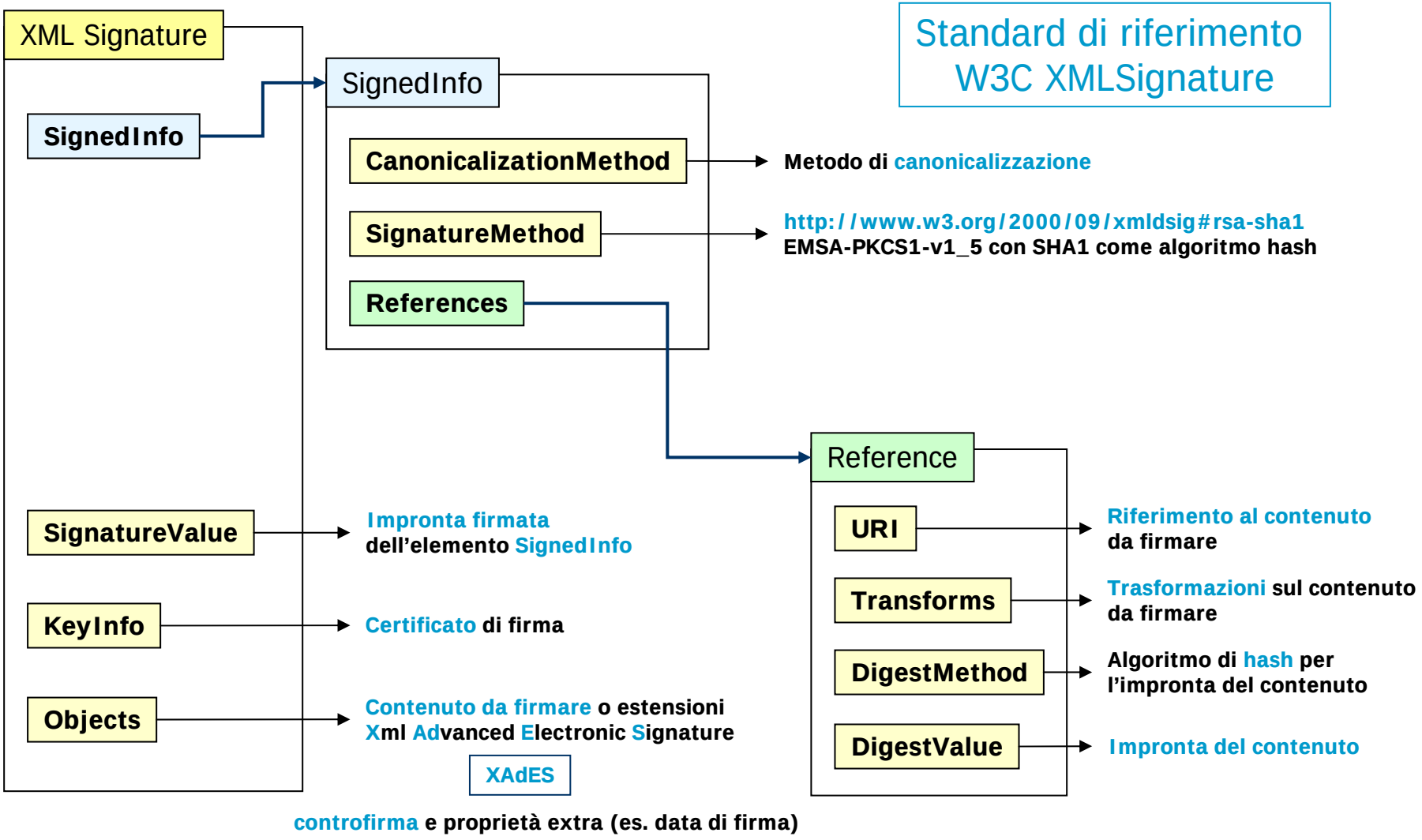

Signed Data
DigestAlgorithmIdentifiers
Algoritmi hash utilizzati dai firmatari
ContentInfo
Contenuto in bytes o suo riferimento
Certificates
Certificati digitali dei firmatari
CRLs
SignerInfo-1
IssuerAndSerialNumber
Collegamento al certificato
DigestAlgorithm
Algoritmo di hash per ottenere l'impronta del contenuto e degli attributi autenticati
SignerInfos
Impronta del contenuto
Data di firma
...
Attributi firmati
AuthenticatedAttributes
SignerInfo-2
SignerInfo-n
DigestEncryptionAlgorithm
rsaEncryption = EMSA-PKCS1-v1_5+RSA o
id-RSASSA-PSS = EMSA-PSS+RSA
EncryptedDigest
Impronta firmata
UnauthenticatedAttributes
Attributi non firmati,
ad es. controfirme (SignerInfo)
n firme parallele
Standard di riferimento
PKCS#7 o RFC 2315

Profilo di busta crittografica PDF

Standard di riferimento
PDF Reference e
ISO 19005-1

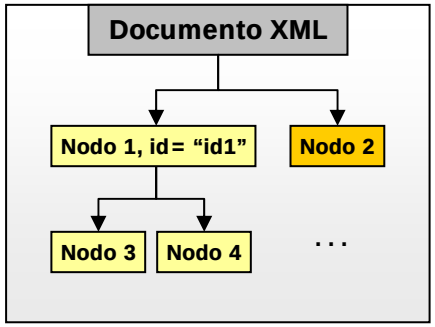


Profilo di busta crittografica XML (1)



Standard di riferimento
W3C XMLSignature

Profilo di busta crittografica XML (2)
Modalità enveloped, enveloping, detached



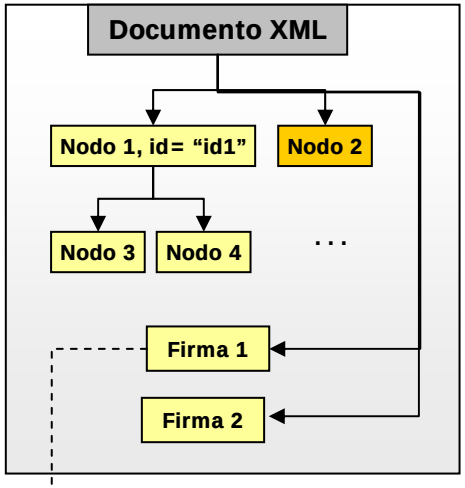
Reference

URI=“#id1” → **Riferimento al nodo (con l’ id indicato) contenuto nello stesso documento in cui è inclusa la firma**

URI=“percorso/file.xml” o “http://..” → **Riferimento ad una risorsa esterna al documento in cui è inclusa la firma**

Modalità Enveloped

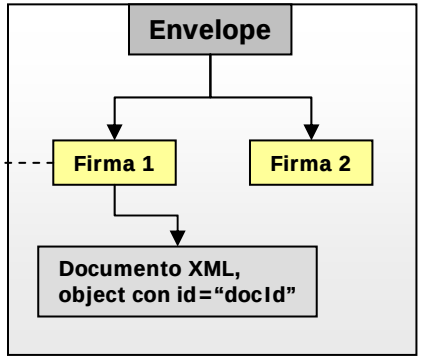
Firma inclusa nel documento da firmare



Es. Reference URI=“#id1”

Modalità Enveloping

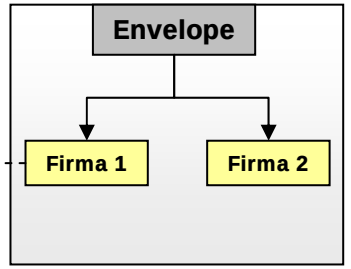
Documento da firmare incluso nella firma



Es. Reference URI=“#docId”

Modalità Detached

Documento da firmare esterno al documento che include la firma



Es. Reference URI=“documento.xml”

Parte 4

La Firma Digitale in Java

Provider Crittografici

- Racchiudono primitive crittografiche e utilità (Hash, algoritmi simmetrici e asimmetrici, ecc)
- Vengono utilizzati per funzionalità crittografiche di base o avanzate (handshake SSL, PKCS#7, XMLSignature, ecc.)
- Disponibili implementazioni open source (SunJCE, BouncyCastle, ecc.) o commerciali (IAIK)

Librerie consigliate per i vari formati e profili

Profilo PKCS#7	Package incluso nella jre **sun.security.pkcs**
Profilo PDF	Librerie open source **iText**
Profilo XML	Librerie open source **apache XML-SEC v 1.4**