



# La Firma Digitale e le sue applicazioni



Ing. Francesca Merighi  
CINECA  
Tel. 051 6171916  
e-mail: [f.merighi@cineca.it](mailto:f.merighi@ cineca.it)

[www.cineca.it](http://www.cineca.it)



# 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

**Legge 59/27**

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

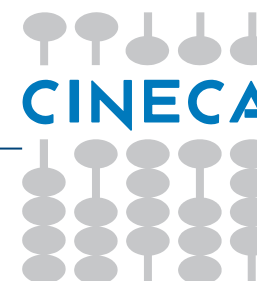
**Formati e regole tecniche**

**Strumenti a garanzia dell'affidabilità del documento informatico**

**Firma Digitale**

**Tecnologia abilitante della dematerializzazione**

**Know-how**





Organismo che opera

presso la Presidenza del Consiglio dei Ministri

a nome del Governo dal Ministro per le Riforme e le Innovazioni nella Pubblica Amministrazione

Fornisce supporto alle Pubbliche Amministrazioni nell'uso innovativo dell'informatica e dell'ICT (Information and Communication Technology).

- Svolge attività di consulenza e proposta
- Emette normative tecniche a livello secondario, quali linee guida e guide tecniche
- Svolge attività di valutazione e vigilanza

## Punto di vista giuridico

**Codice dell'Amministrazione Digitale**  
(Decreto Legislativo del 7 marzo 2005, n.82)

Norme e principi generali in materia di dematerializzazione

**Regole tecniche in materia di generazione apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici**  
(Decreto del Presidente del Consiglio dei Ministri del 30 Marzo 2009)

Regole tecniche di base per

Generazione e la verifica della firma

Profili e gestione dei certificati qualificati

Profili e gestione dei riferimenti temporali

**Regole per il riconoscimento e la verifica del documento informatico**  
(CNIPA Deliberazione 21 maggio 2009)

Algoritmi crittografici e funzioni di hash

Profili di firma XML e PKCS#7 (CADES)

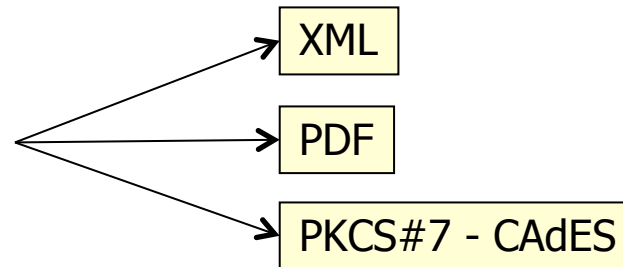
Specifiche per i profili dei certificati

Regole per la validazione temporale

## Punto di vista tecnico

**Utilizzo di standard** → **Interoperabilità**

## Standard per le buste crittografiche



## PKCS#1

Primitive di firma e verifica della **firma RSA**

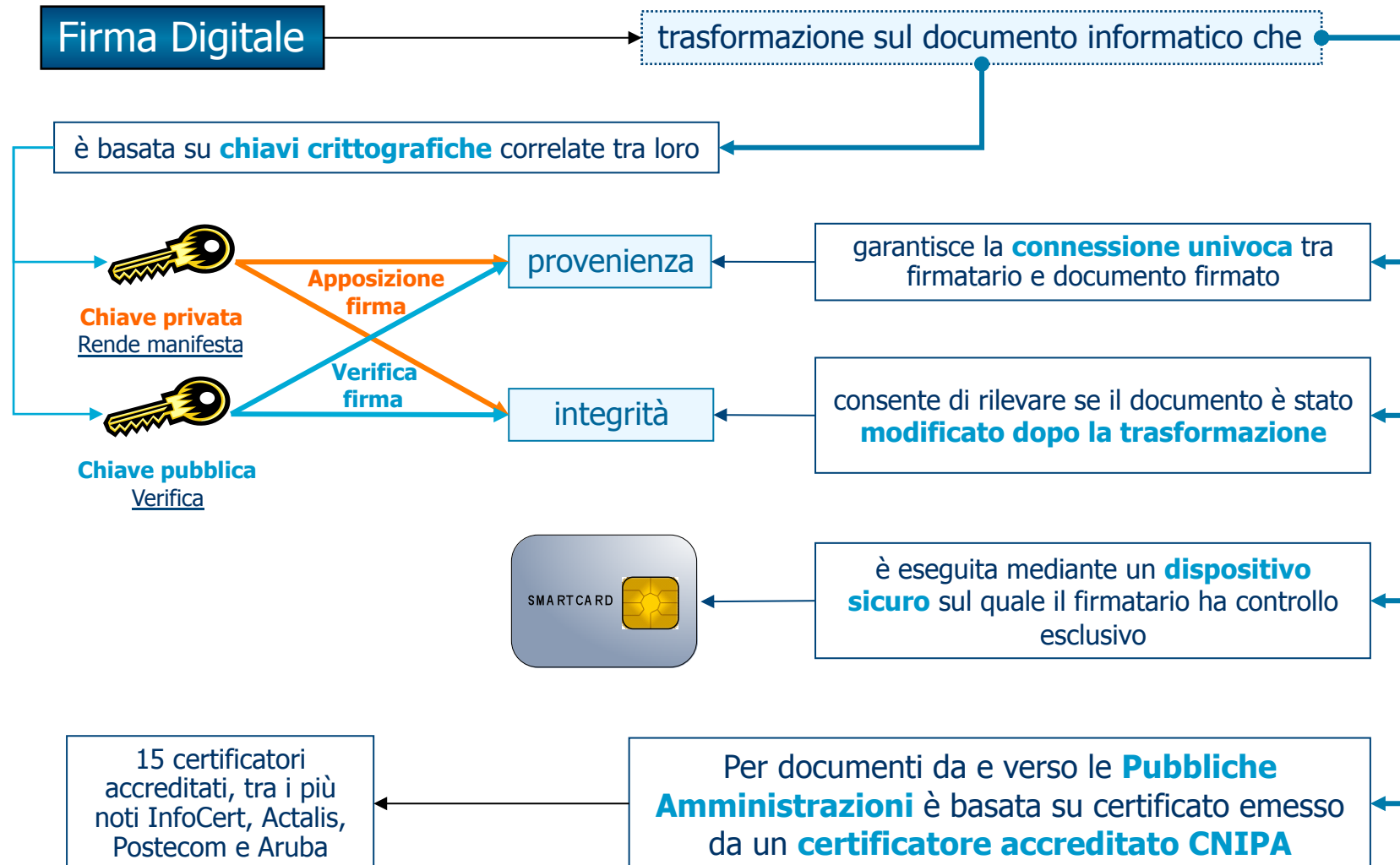
Primitive di cifratura e decifratura RSA

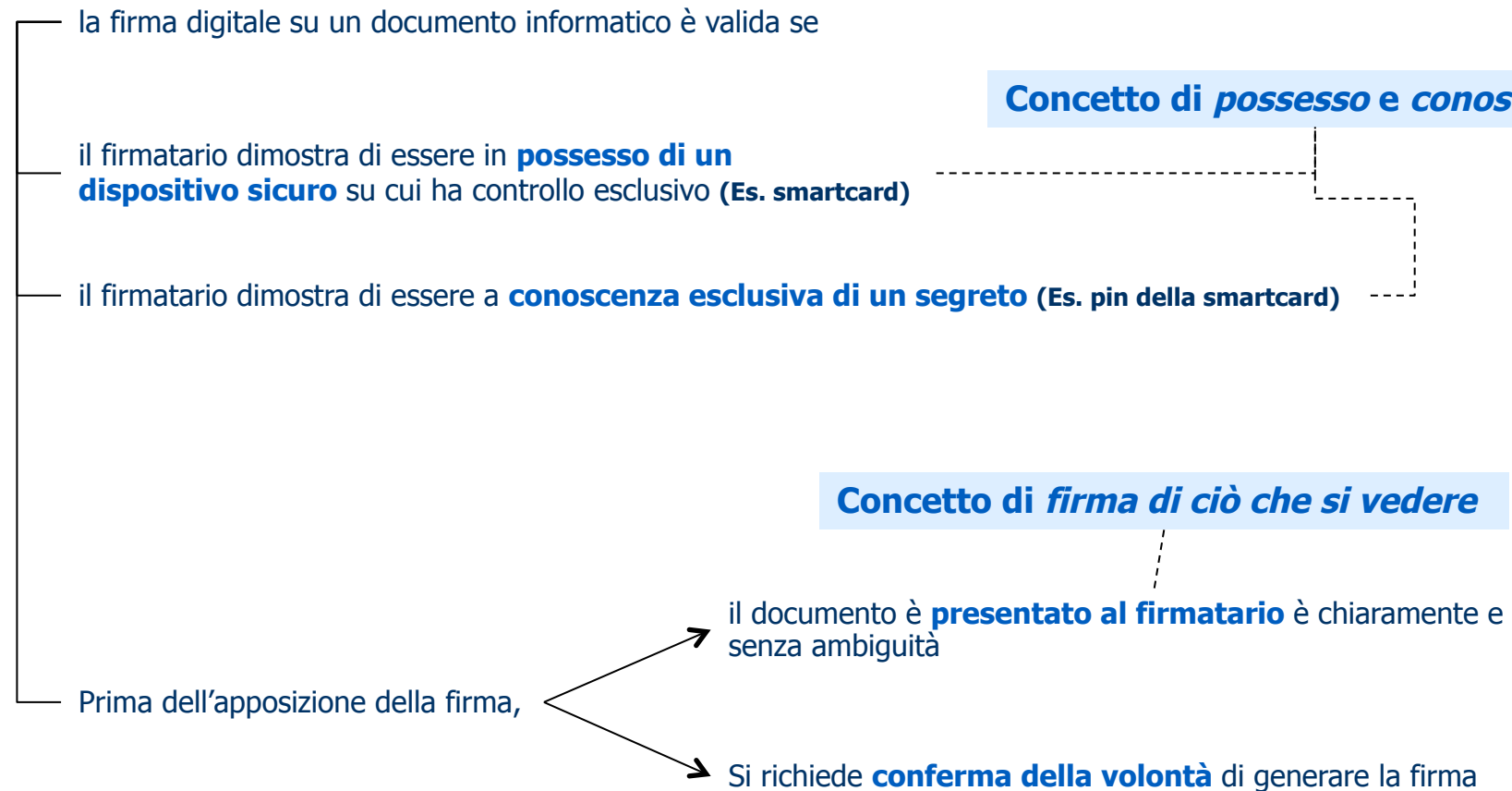
## X509

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

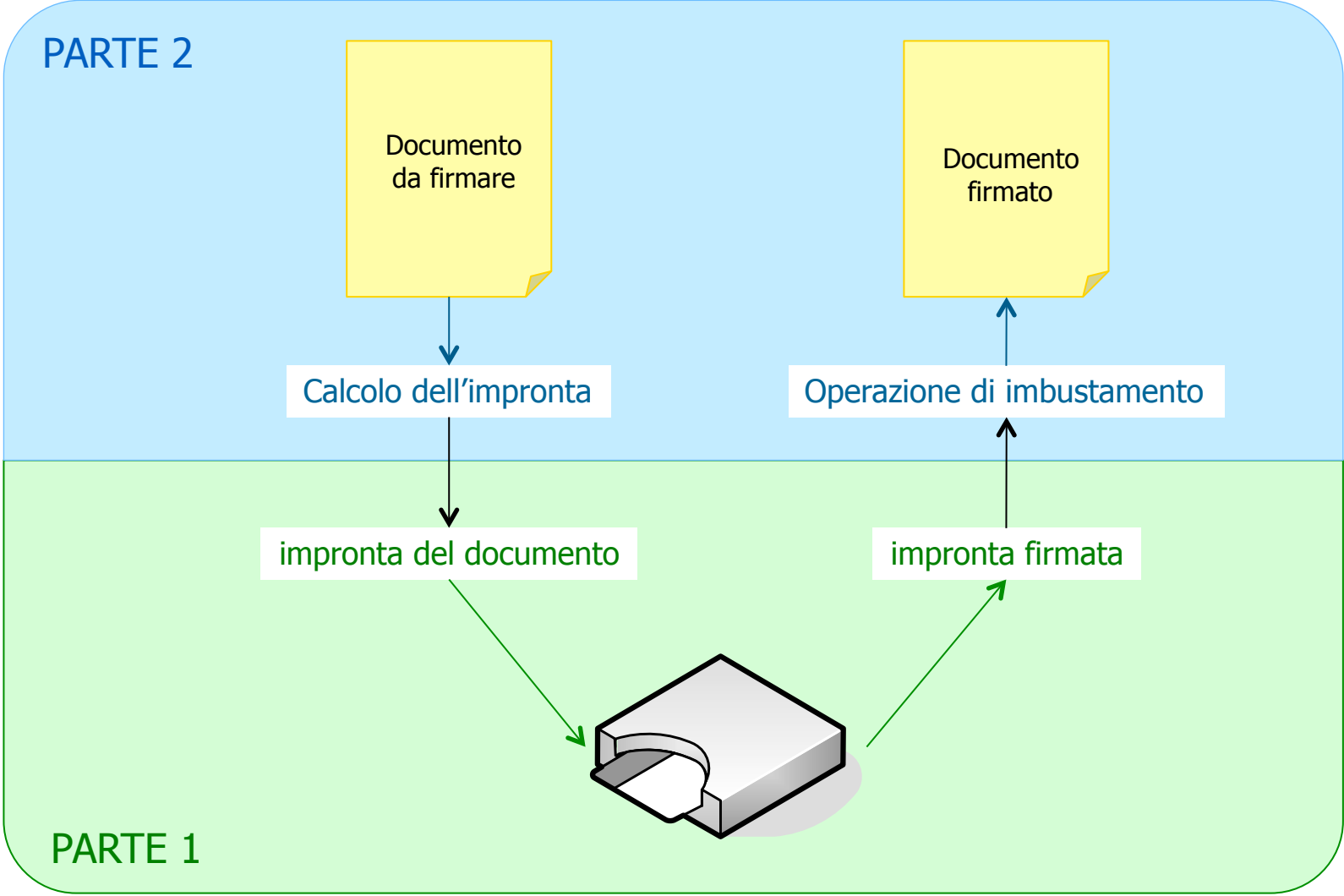
## PKCS#11

Interfaccia fra applicazione e **dispositivi di firma**











# Parte 1

## Dispositivi di Firma Digitale

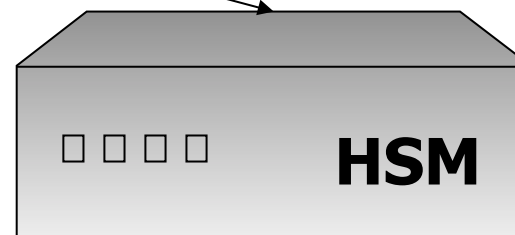
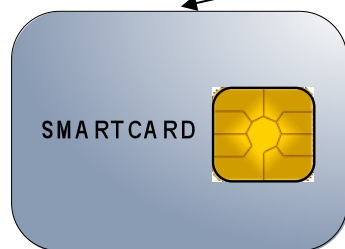
***Smartcard***  
***Interfaccia PKCS#11 ai dispositivi di firma***  
***Dispositivi di firma remota e automatica***

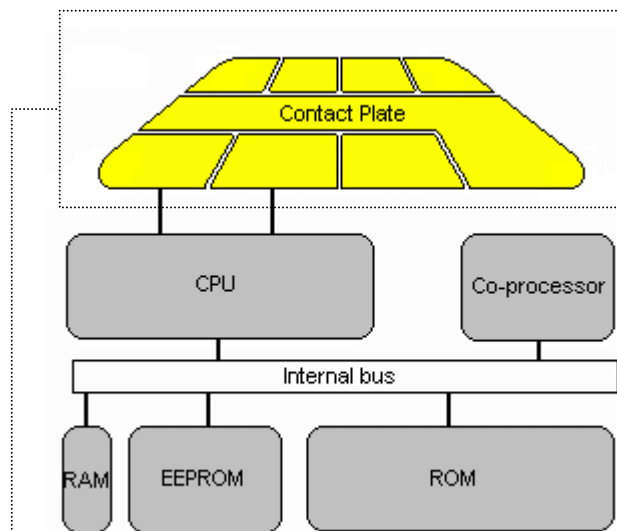
**Dispositivi fisici** che contengono oggetti (**chiavi private**, **chiavi pubbliche** e **certificati digitali**), attraverso i quali eseguono **operazioni crittografiche**

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

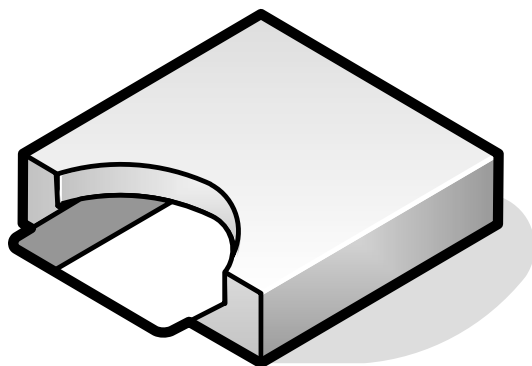
**Information Technology Security Evaluation Criteria (ITSEC)**  
Insieme strutturato di criteri di valutazione della sicurezza di un sistema

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





Interfaccia Input/Output



**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)

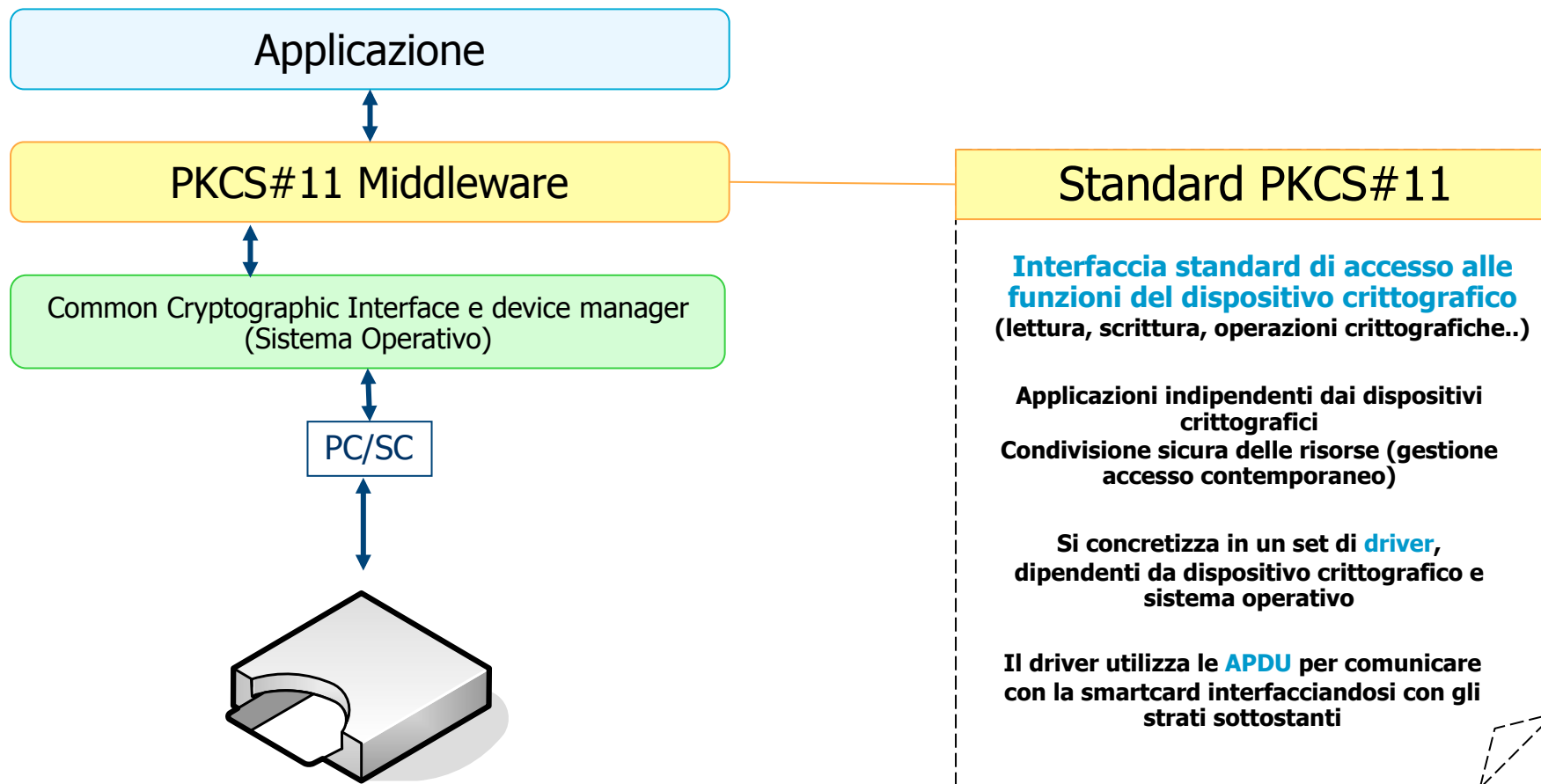
**Interfaccia Input/Output:** velocità del flusso dati 9600 bit/sec, protocolli T=0 e **T=1**

**ISO 7816** - Standard di riferimento per smartcard che definisce

- ✓ Caratteristiche fisiche ed elettriche
- ✓ I protocolli di comunicazione verso il lettore di smartcard (**T=0, T=1**)
- ✓ Comando di risposta al reset (**Answer To Reset**) → modello smartcard
- ✓ *Protocollo di comunicazione verso le applicazioni (**Application Protocol Data Unit**): spesso non rispettato dai produttori di smartcard*

Circa 1 operazione al secondo

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





## Dispositivo crittografico ad alte prestazioni

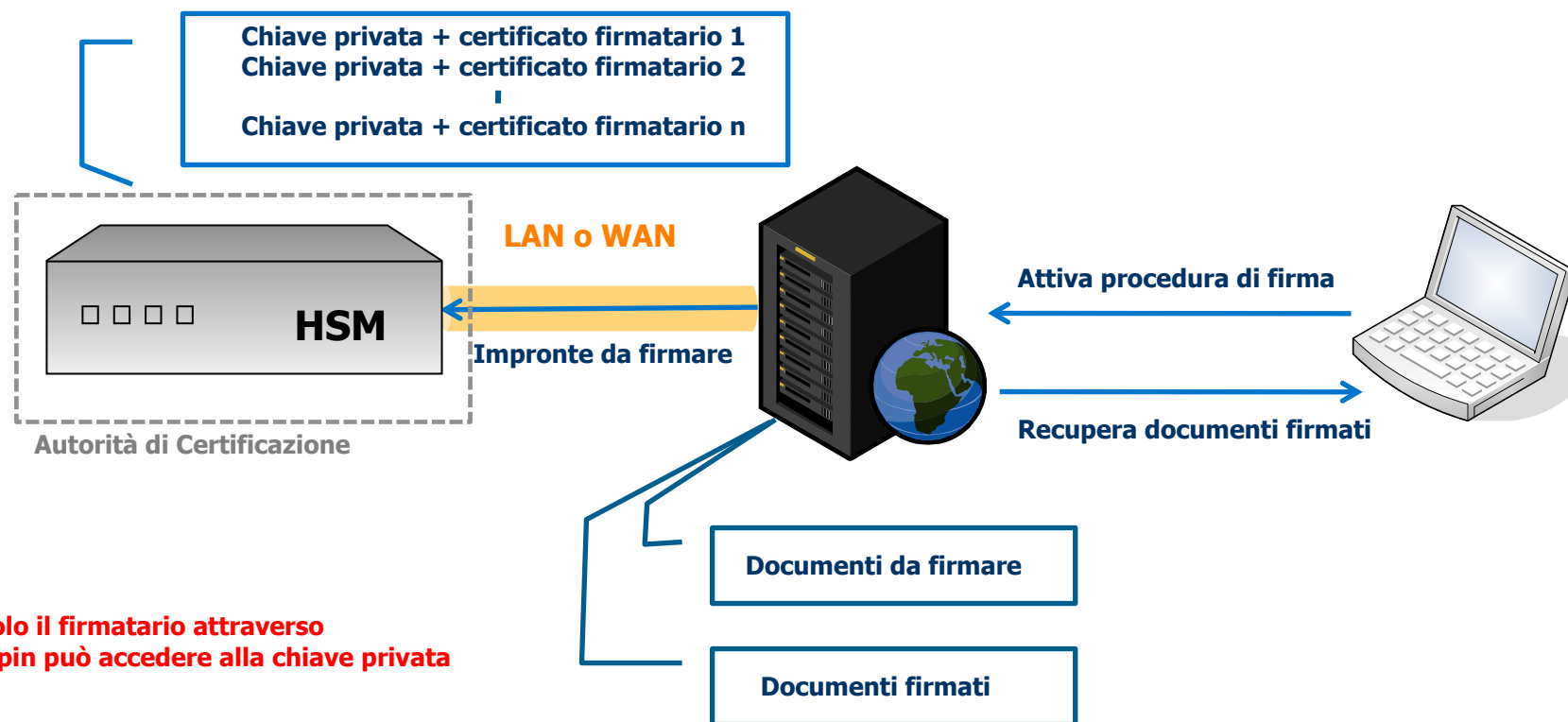
Sistema complesso con hardware dedicato

Stesse funzionalità delle smartcard

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

Dalle 200 alle 1000 operazioni al secondo

Costo dell' hardware dai 20.000 euro in su



**Solo il firmatario attraverso il pin può accedere alla chiave privata**

**Le chiavi di firma sono protette da procedure di sicurezza dell'autorità di certificazione**

**Il pin del firmatario è trasportato in rete in forma cifrata**

Pin = conoscenza

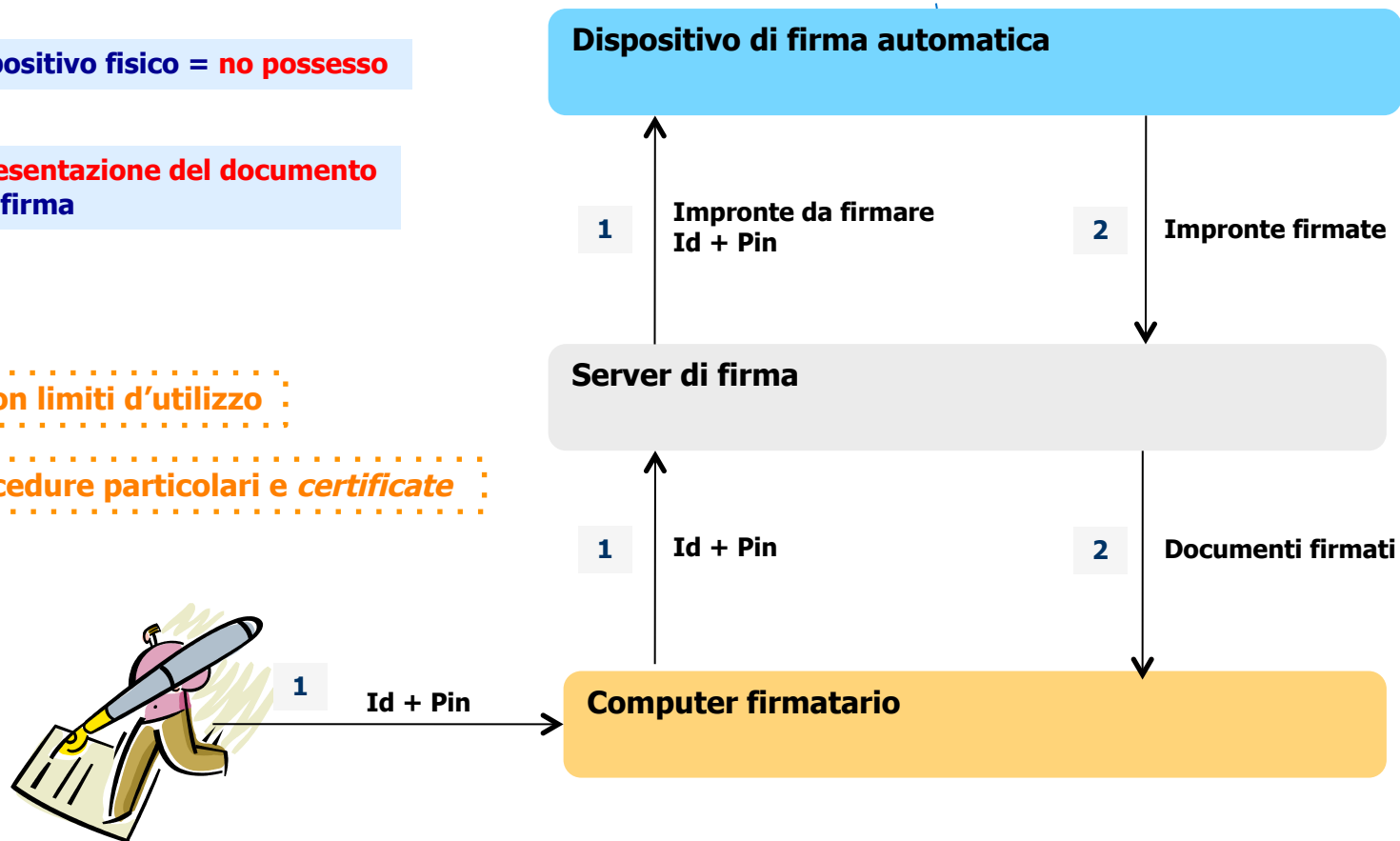
Nessun dispositivo fisico = **no possesso**

**Nessuna presentazione del documento prima della firma**

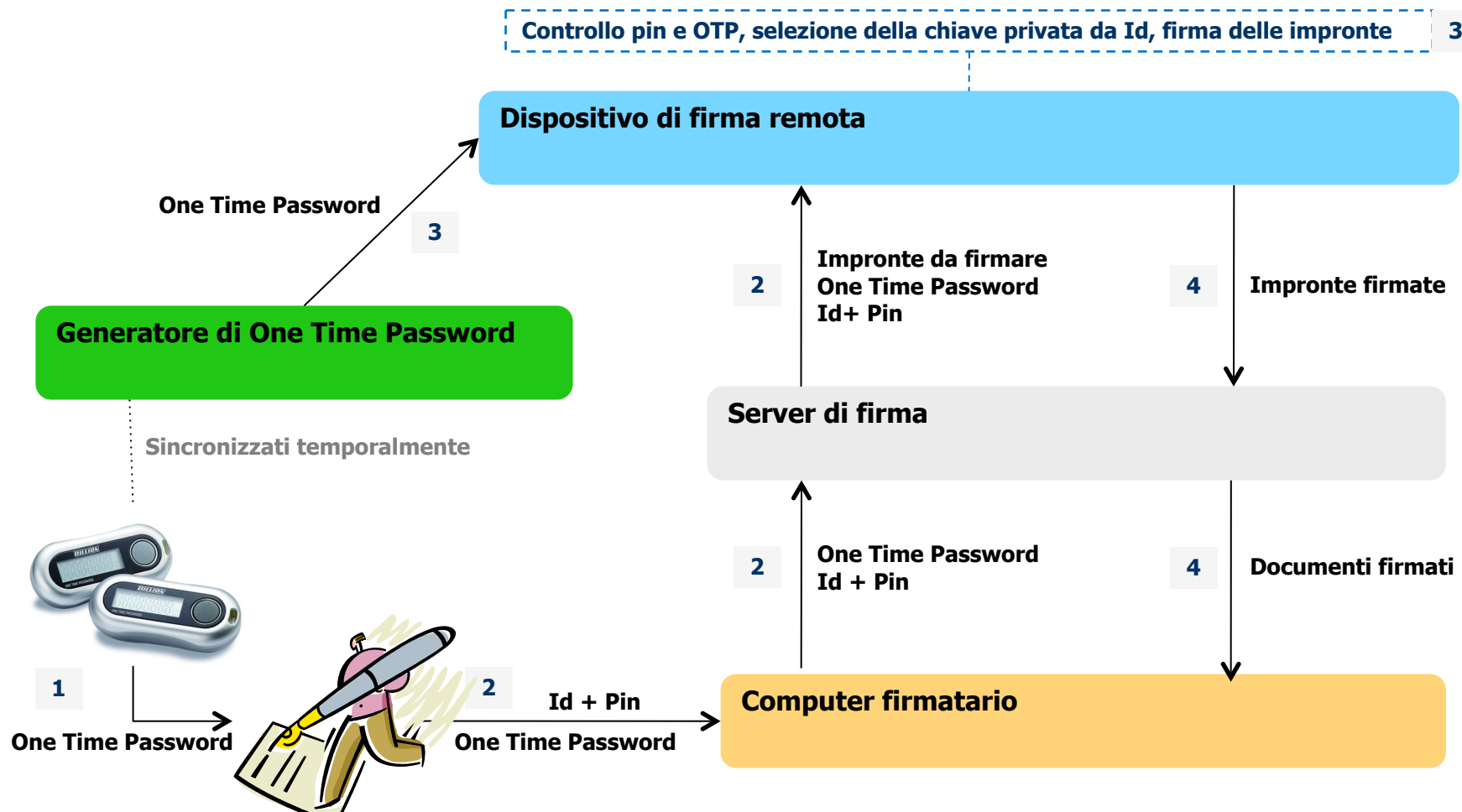
Certificato con limiti d'utilizzo

Solo per procedure particolari e *certificate*

Controllo pin, selezione chiave privata da Id, firma delle impronte 1







One Time Password = possesso  
Pin = conoscenza

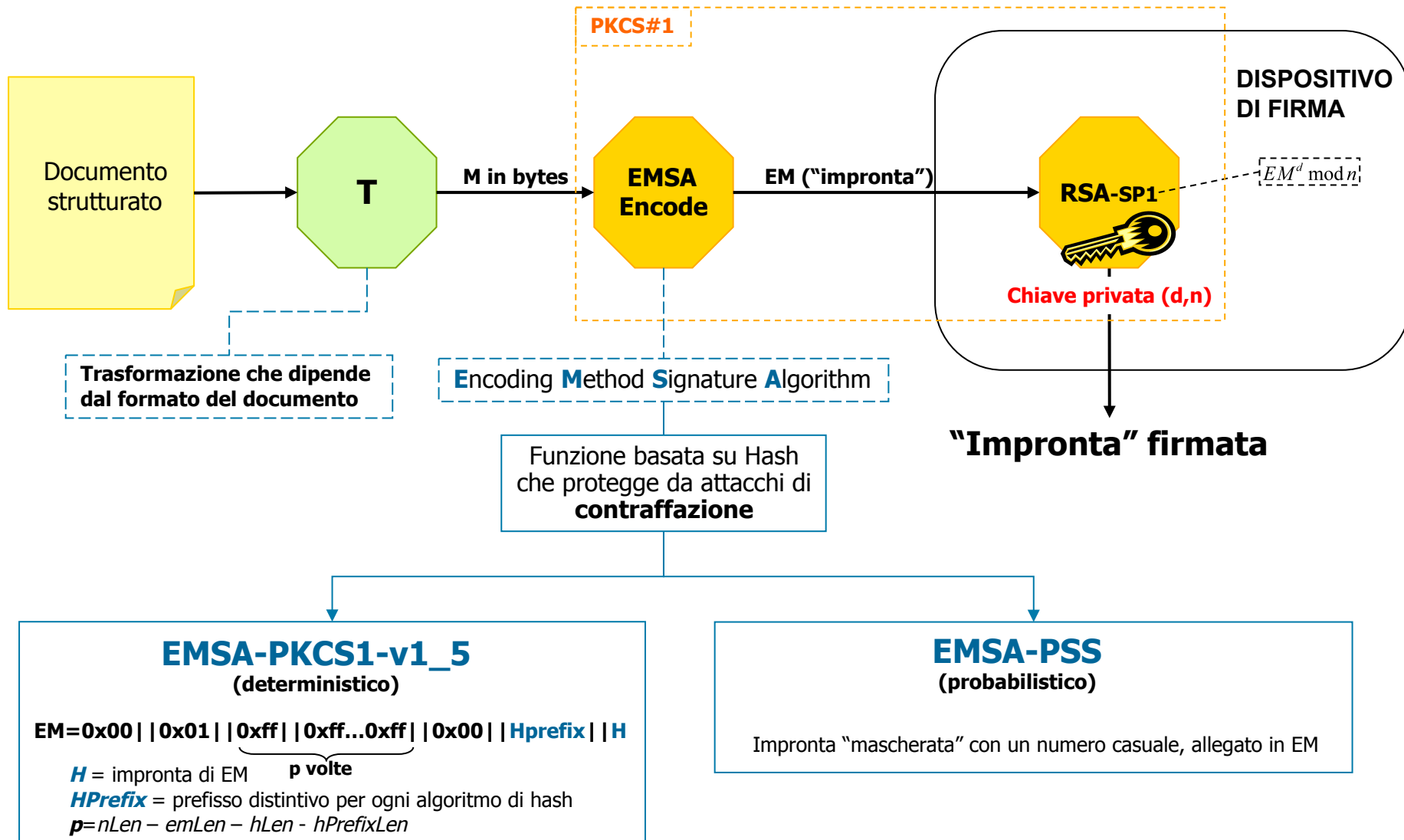
Presentazione del documento prima della firma

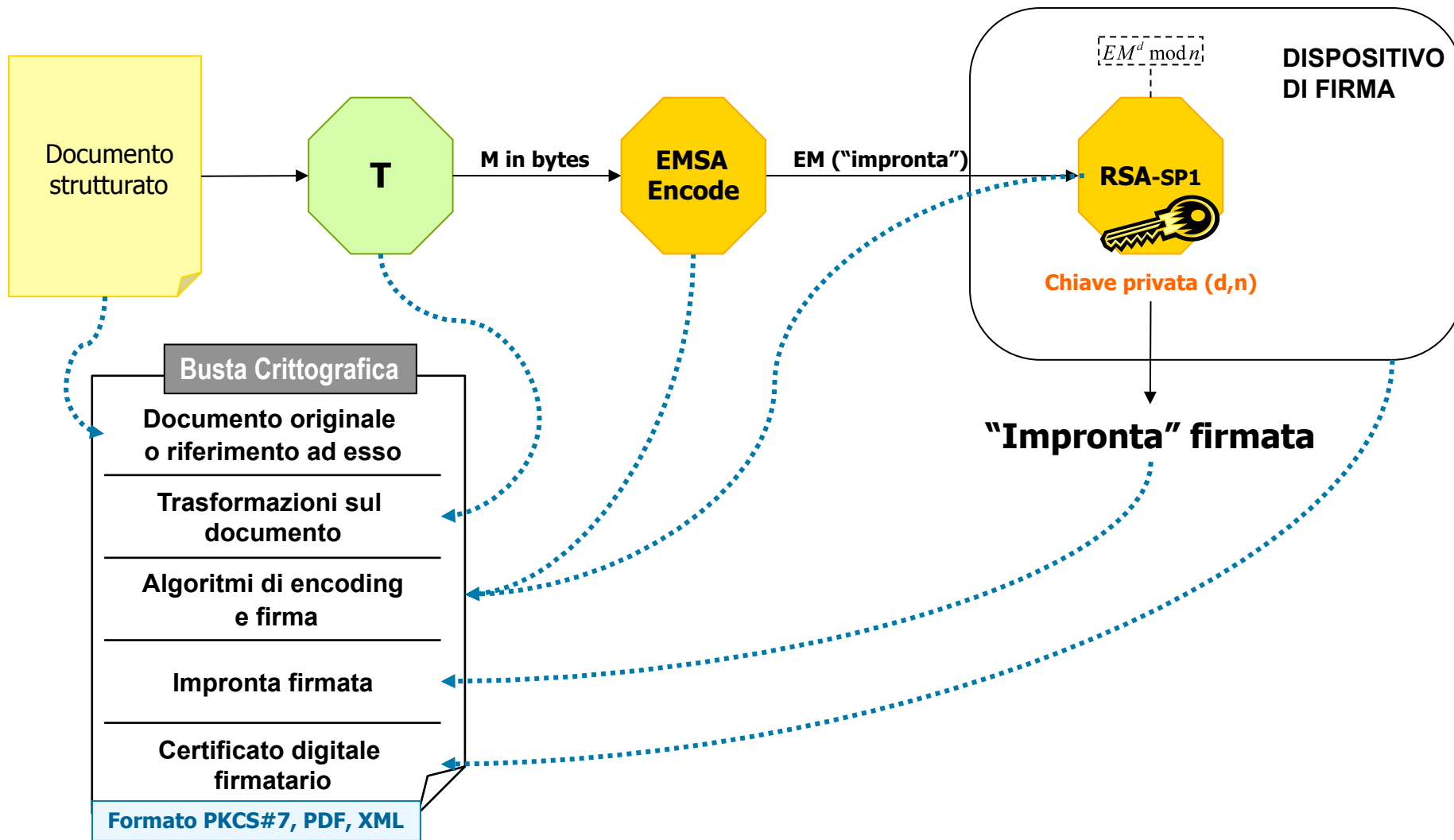


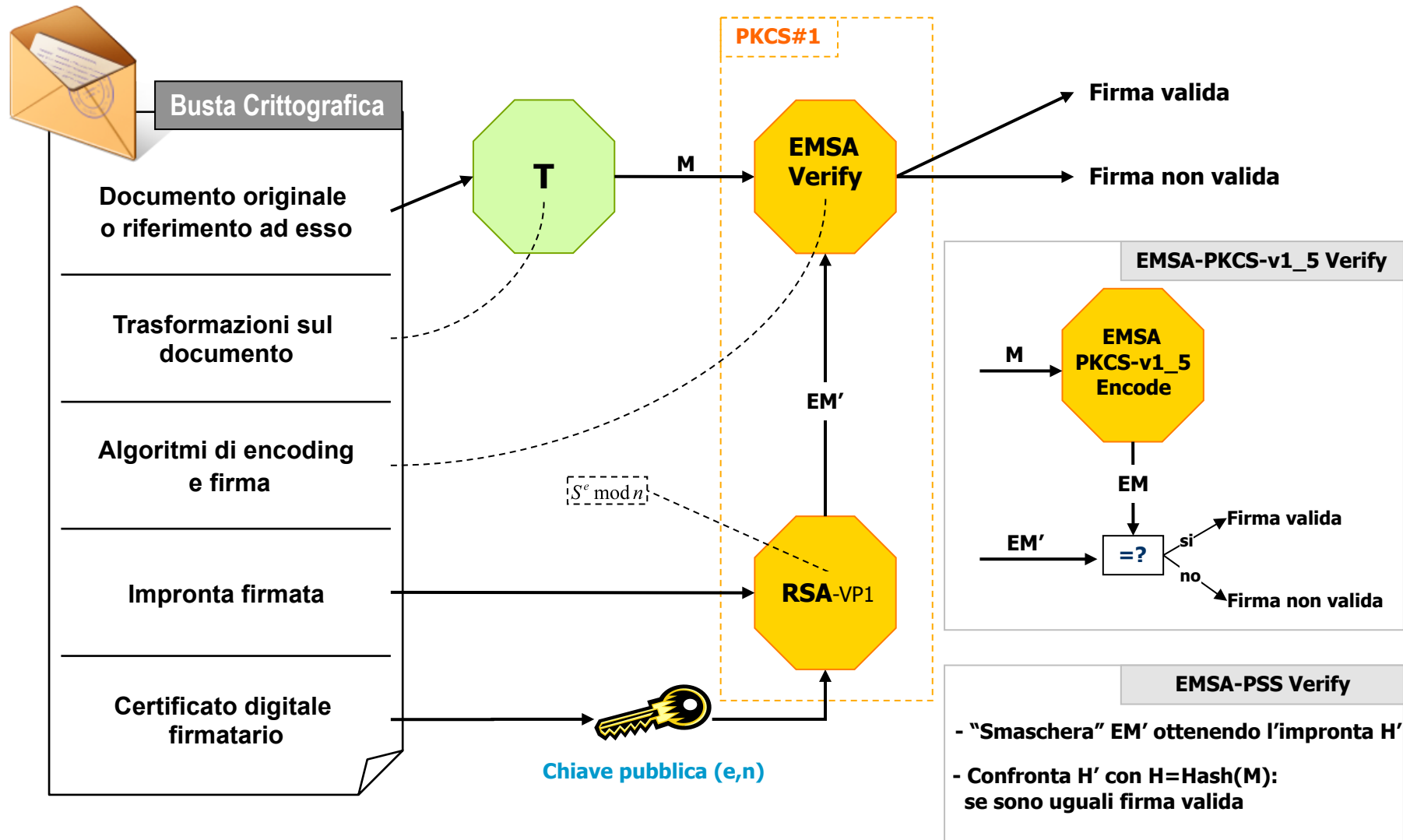
# Parte 2

## Operazioni di apposizione e verifica della Firma Digitale

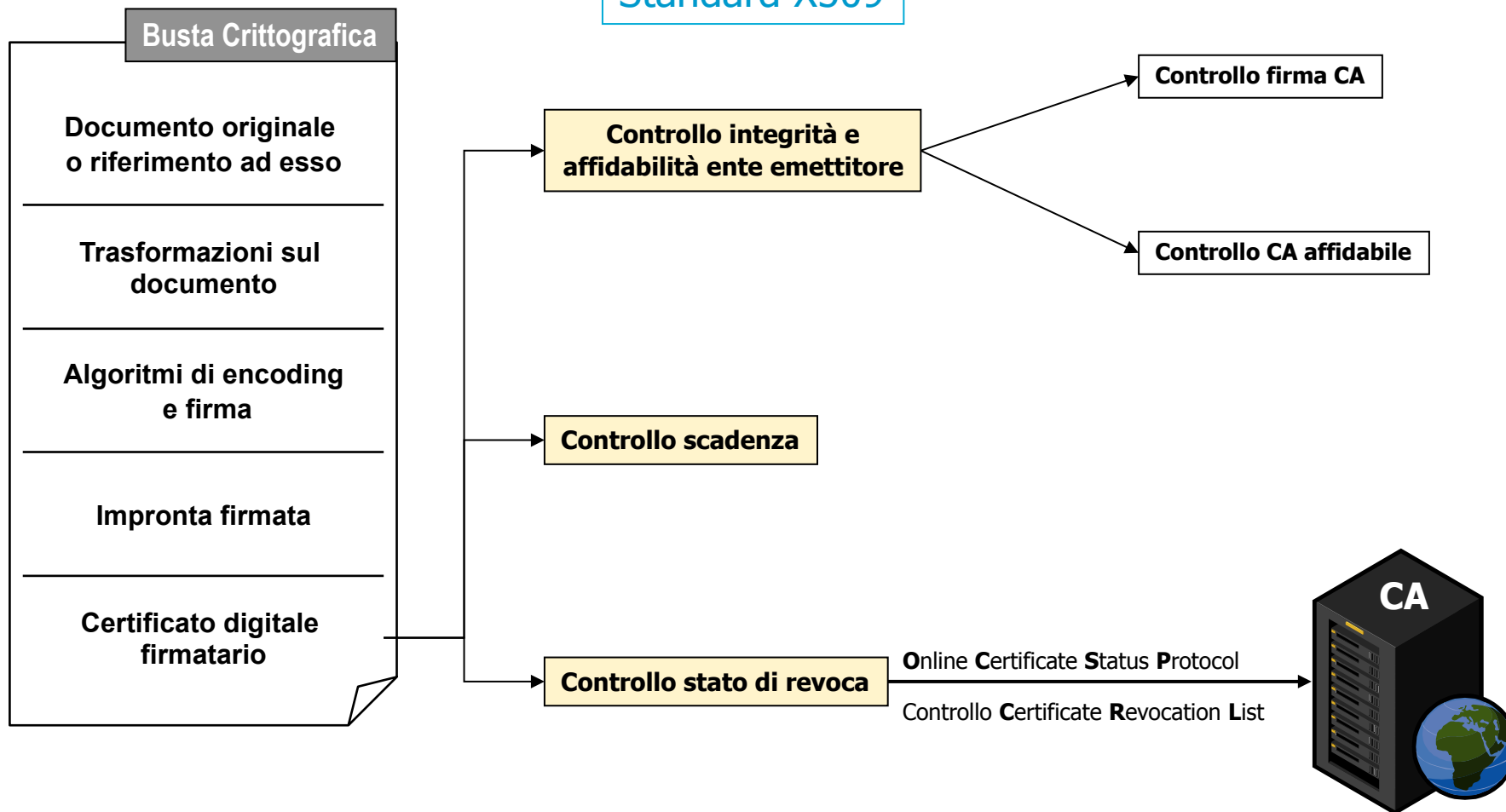
*Operazione di firma RSA*  
*Operazione di imbustamento*  
*Operazione di verifica della firma RSA*

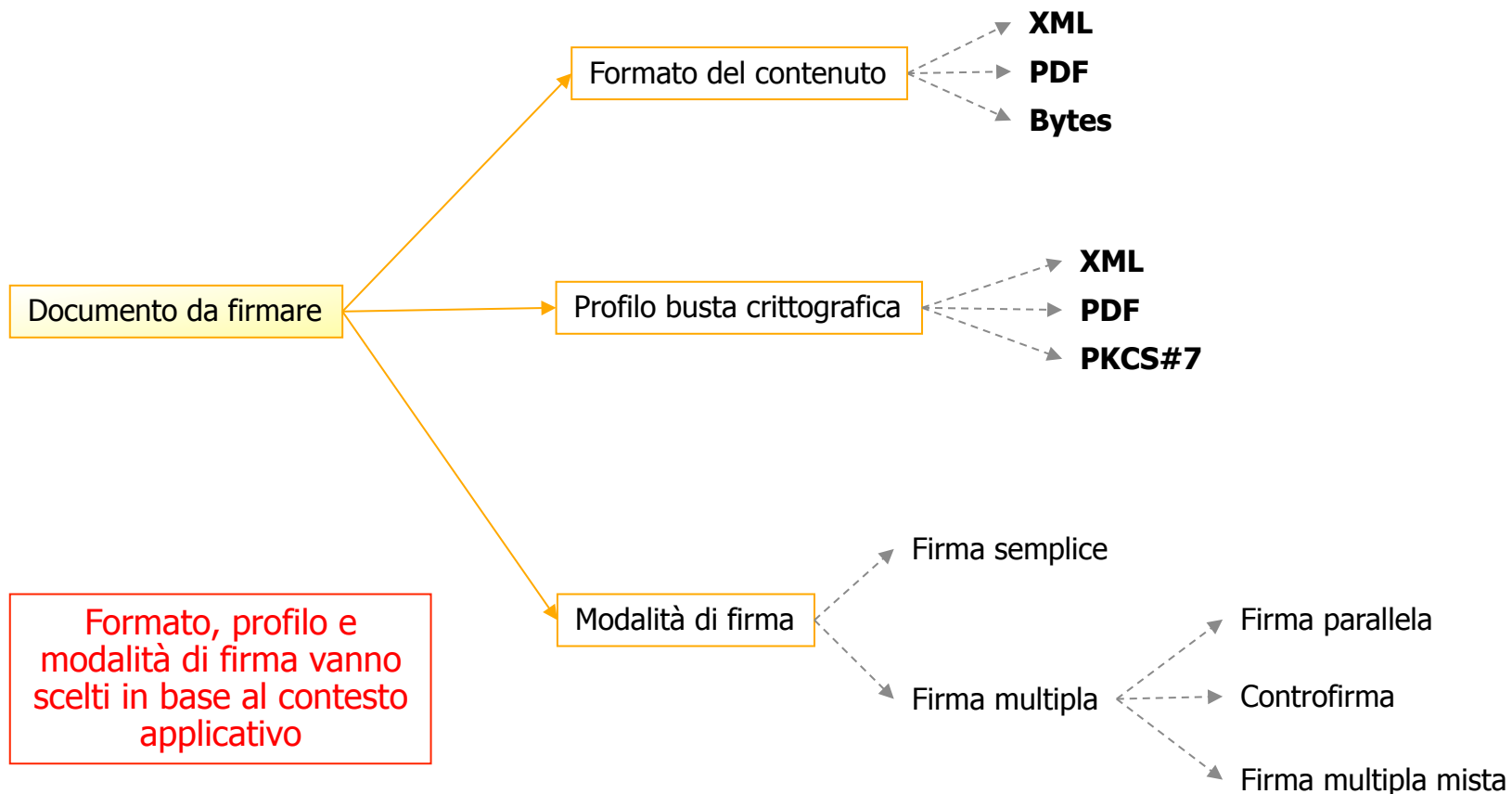


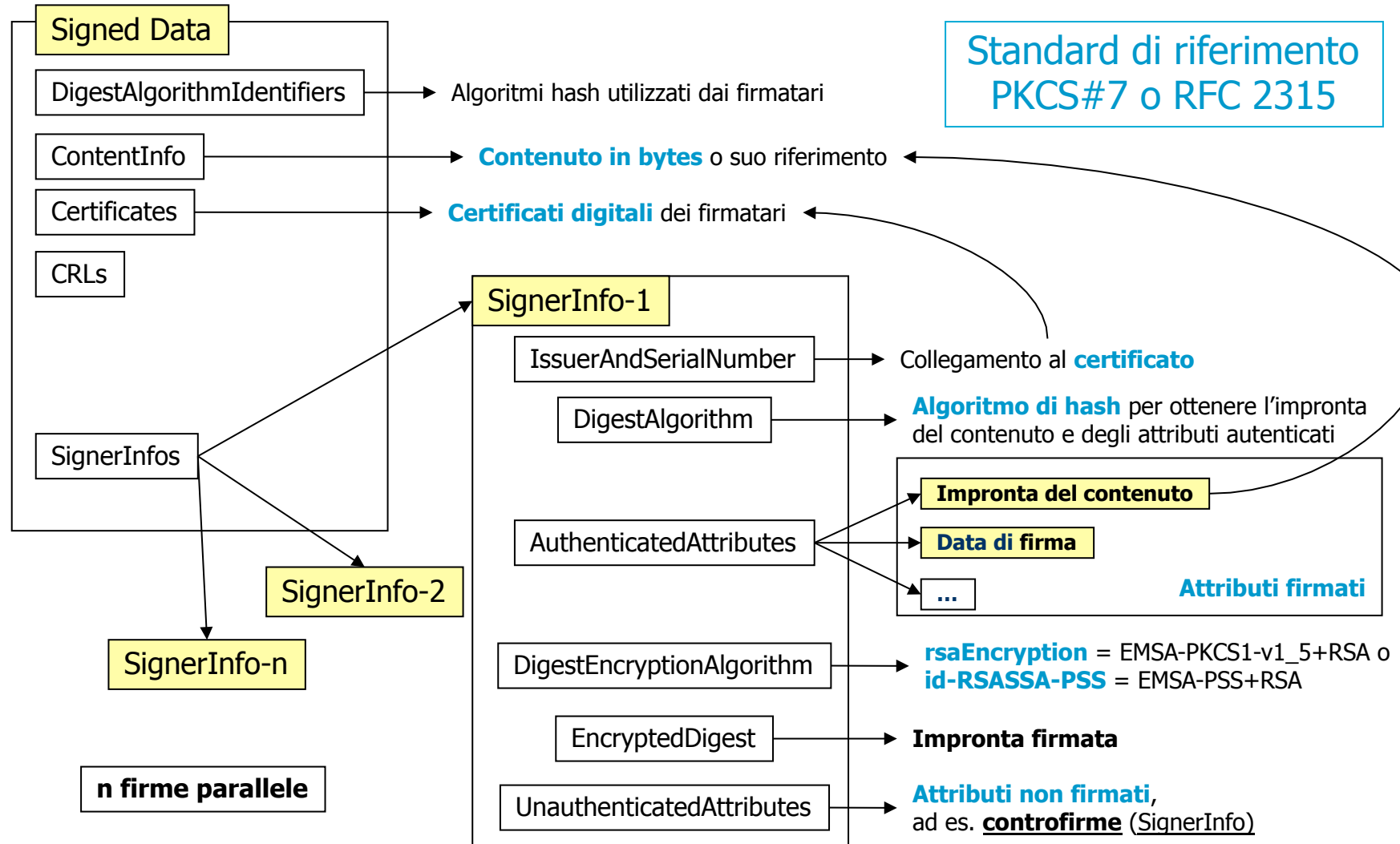




## Standard X509

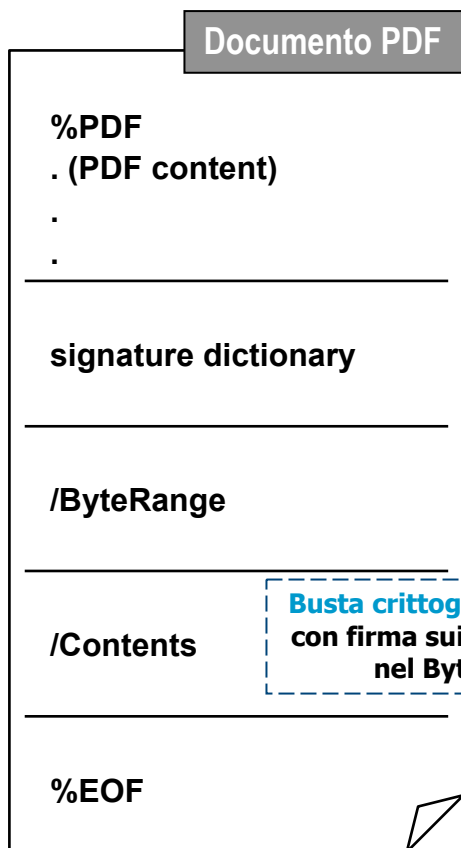




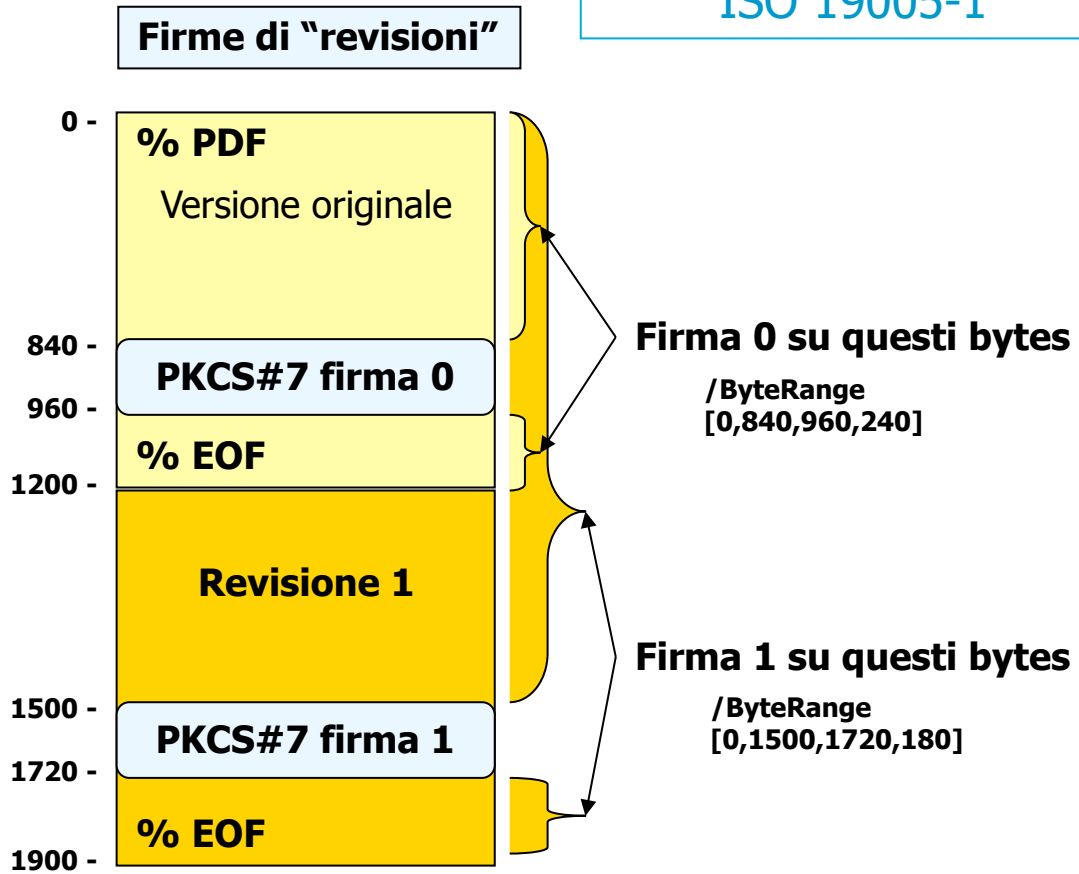


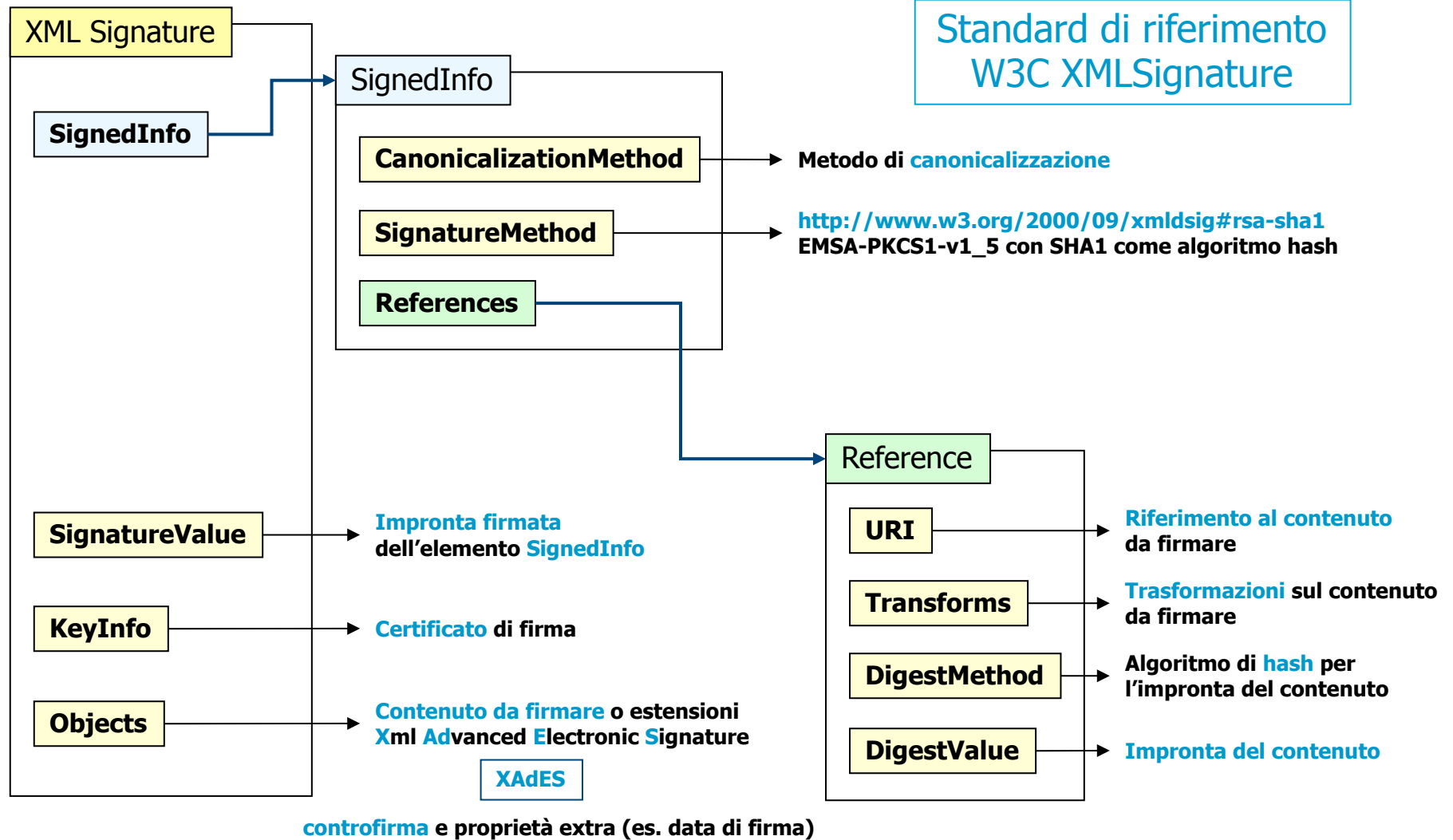


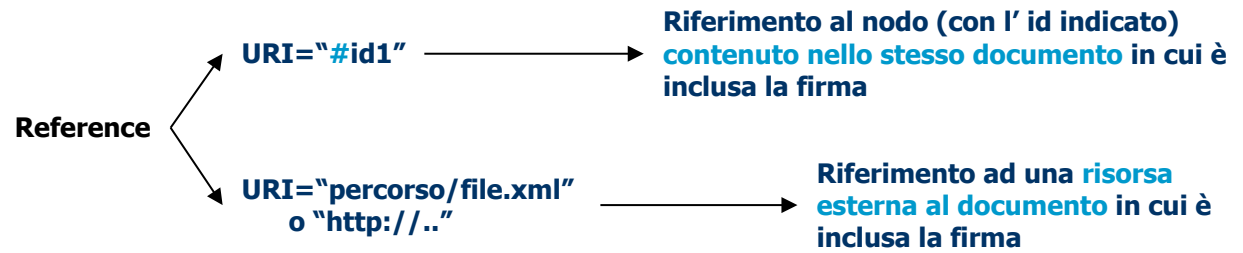
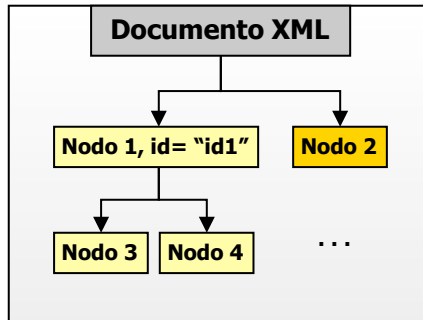
Standard di riferimento  
PDF Reference e  
ISO 19005-1



Busta crittografica PKCS#7  
con firma sui bytes indicati  
nel ByteRange

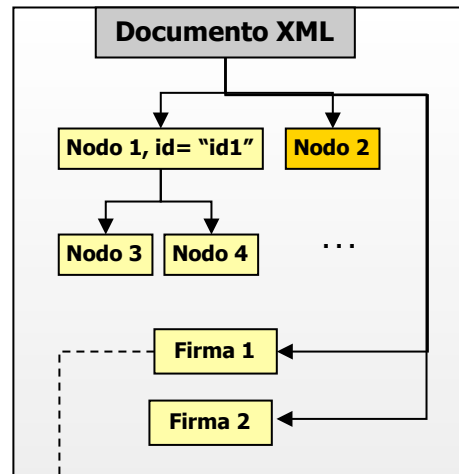






### Modalità Enveloped

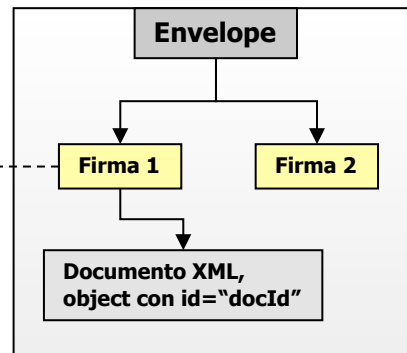
Firma inclusa nel documento da firmare



Es. Reference URI="#id1"

### Modalità Enveloping

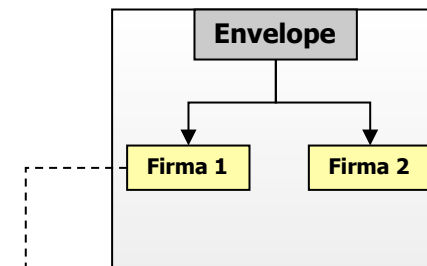
Documento da firmare incluso nella firma



Es. Reference URI="#docId"

### Modalità Detached

Documento da firmare esterno al documento che include la firma



Es. Reference URI="documento.xml"

**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**