# Public-key Infrastructure

**Barbara Masucci**

Dipartimento di Informatica ed Applicazioni

Università di Salerno

**masucci@dia.unisa.it**
**http://www.dia.unisa.it/professori/masucci**

# Distribuzione chiavi pubbliche

- Come vengono distribuite le chiavi pubbliche?
- Chi ci assicura che una chiave pubblica è quella di un prefissato utente?

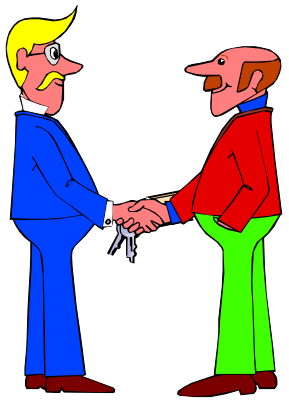
# Distribuzione chiavi pubbliche

Alcune tecniche:

- Invio point-to-point su canale fidato
- Annuncio pubblico
- Directory disponibile pubblicamente
- Autorità per le chiavi pubbliche
- Certificati per le chiavi pubbliche

# Invio point-to-point su canale fidato

- Esempi: scambio diretto, uso di un corriere fidato,…
- Oppure
  - invio su canale pubblico
  - autenticazione (per esempio: hash su canale fidato)



**Va bene se:**

- Uso non frequente
- Piccoli sistemi

# Annuncio pubblico

- Invio ad altri utenti / Broadcast chiave
- Esempio: aggiunta della chiave pubblica PGP ai messaggi inviati a forum pubblici

**Problema:** ci dobbiamo fidare dell'annuncio?

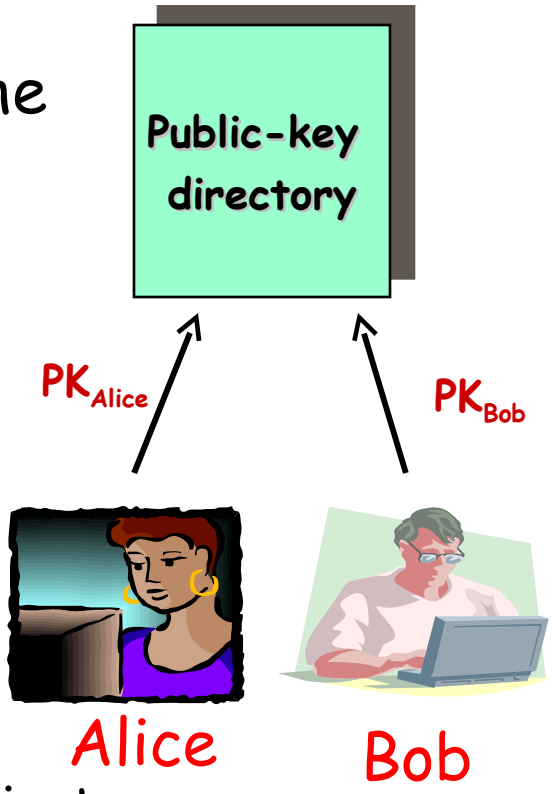
# Directory disponibile pubblicamente

## Entità fidata:

- Gestisce la directory di chiavi pubbliche

## Ogni partecipante:

- Registra la propria chiave pubblica
  - Di persona o in modo autenticato
- Può aggiornare la propria chiave
  - Se usata da troppo tempo o chiave privata compromessa
- Può accedere alla directory
  - Necessaria comunicazione sicura ed autenticata



# Autorità per le chiavi pubbliche

- Gestisce directory chiavi pubbliche
- Ha una chiave pubblica nota a tutti gli utenti
- Ogni utente chiede la chiave pubblica desiderata, l'autorità la invia
- Svantaggi:
  - server on-line
  - collo di bottiglia

Vediamo un possibile protocollo

# Autorità per le chiavi pubbliche

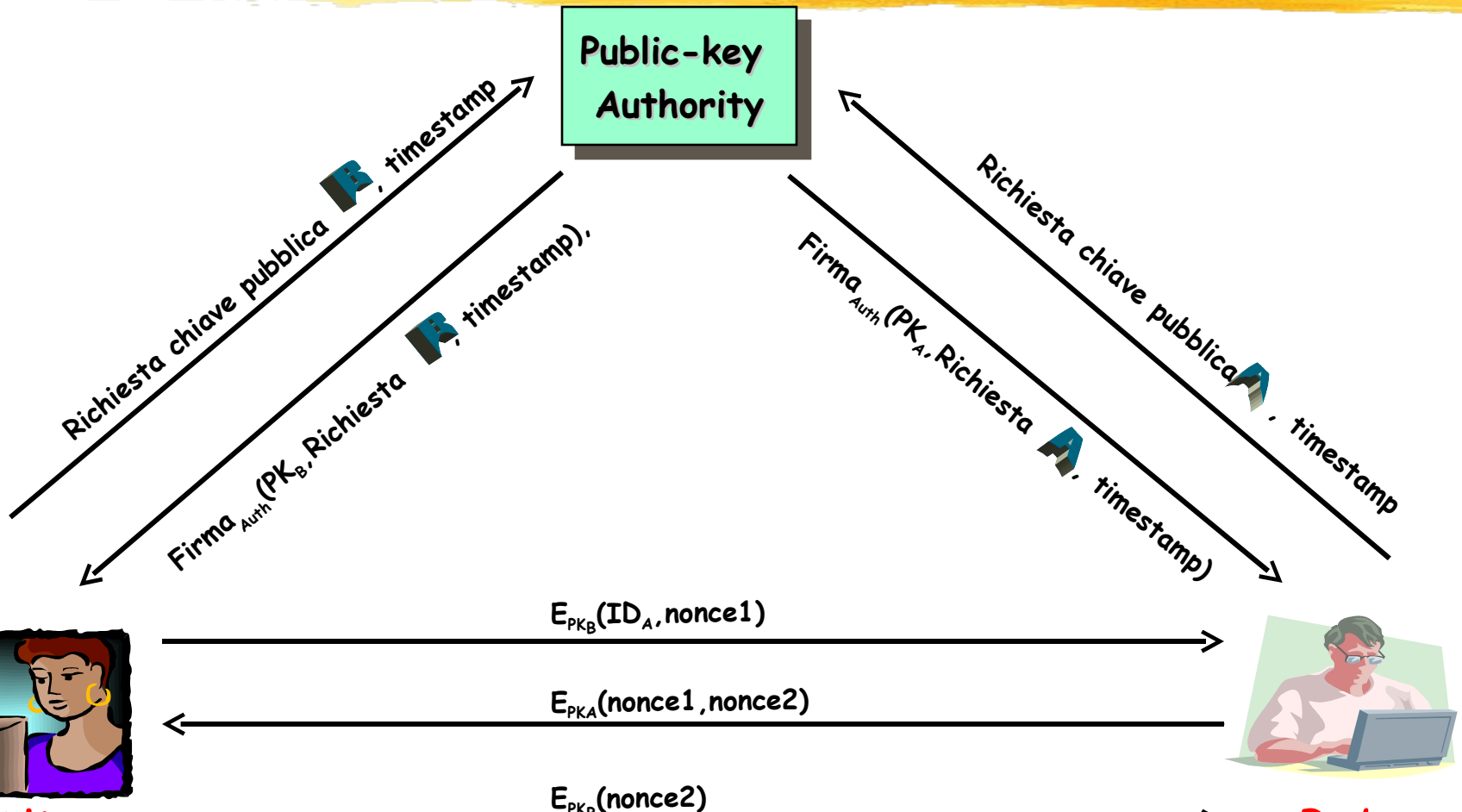
Public-key Authority

Voglio la chiave pubblica di Bob

Alice

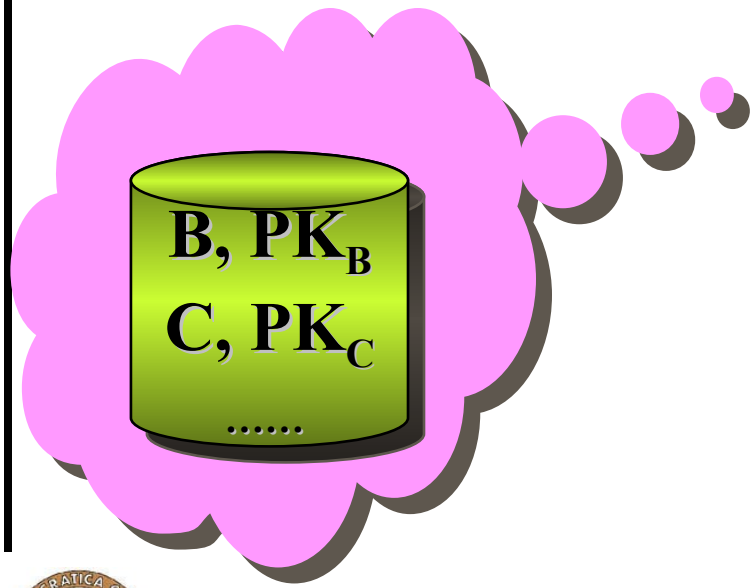
Bob

# Autorità per le chiavi pubbliche



# *Caching* chiavi pubbliche

Ottenuta una chiave pubblica, si memorizza




Alice

... ma occorre aggiornarla periodicamente

# Certificati

## Mondo fisico

- Carta di identità
  - Un'autorità riconosciuta lega un nome ad una foto

## Mondo digitale

- Certificato digitale
  - Un'autorità riconosciuta lega un nome ad una chiave pubblica

# Certificati


Autorità di Certificazione:
Terza parte fidata la cui firma garantisce il legame tra chiave ed identità

Alcune proprietà dei certificati:

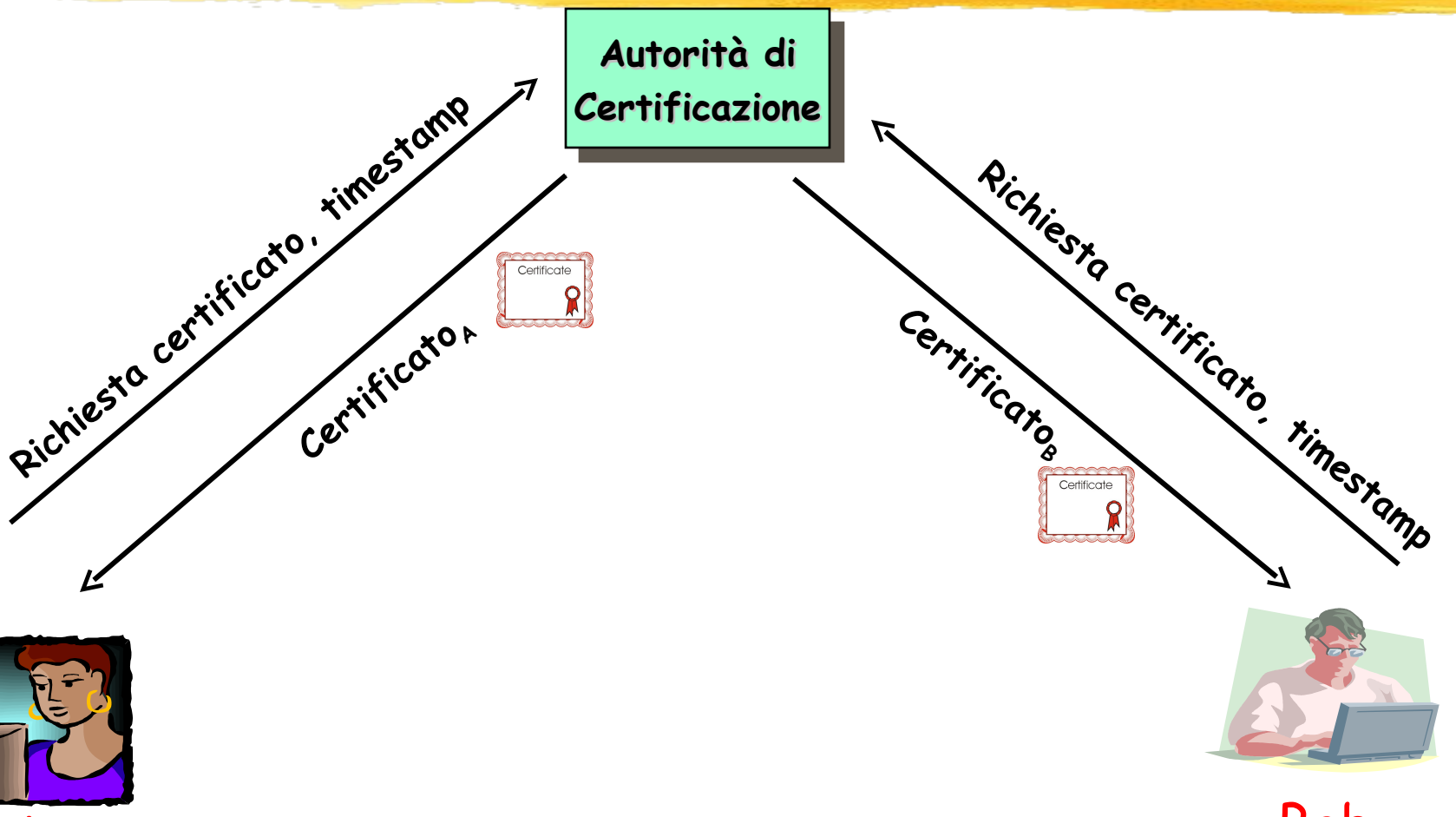
- Ognuno può leggerli e determinare nome e chiave pubblica
- Ognuno può verificarli ed assicurarsi dell'autenticità
- Solo l'Autorità può crearli ed aggiornarli

# Certificati

- Esempi di altri dati in un certificato:
  - periodo di validità chiave pubblica
  - numero seriale o identificatore chiave
  - info addizionali su chiave (ad es., algoritmi ed utilizzo)
  - info addizionali su utente
  - stato della chiave pubblica


- Formato più diffuso: definito dallo standard internazionale ITU-T X.509

# Richiesta Certificati



# Scambio Certificati

Autorità Certificazione

Alice


$Certificato_A$

Bob

$Certificato_B$

# Revoca di certificati

- Che succede se la chiave privata viene compromessa?
- L'utente può richiedere la revoca del certificato

# Revoca Certificati: Motivi

- Compromissione chiave privata
- Info non più valide (es., cambio affiliazione)
- Non più utile per lo scopo prefissato
- Compromissione algoritmo
- Perdita o malfunzionamento di security token, perdita di password o PIN
- Cambio politiche di sicurezza
  - (es., la CA non supporta più servizi per certificati)

# Revoca Certificati: Metodi

- Data scadenza dentro un certificato
  - Certificati "a breve scadenza"
- Notifica manuale
  - Informazione tramite canali speciali
  - Solo per sistemi piccoli o chiusi
- File pubblico di chiavi revocate
  - Certificate Revocation List (CRL)
- Certificato di revoca
  - Sostituisce certificato revocato nella directory

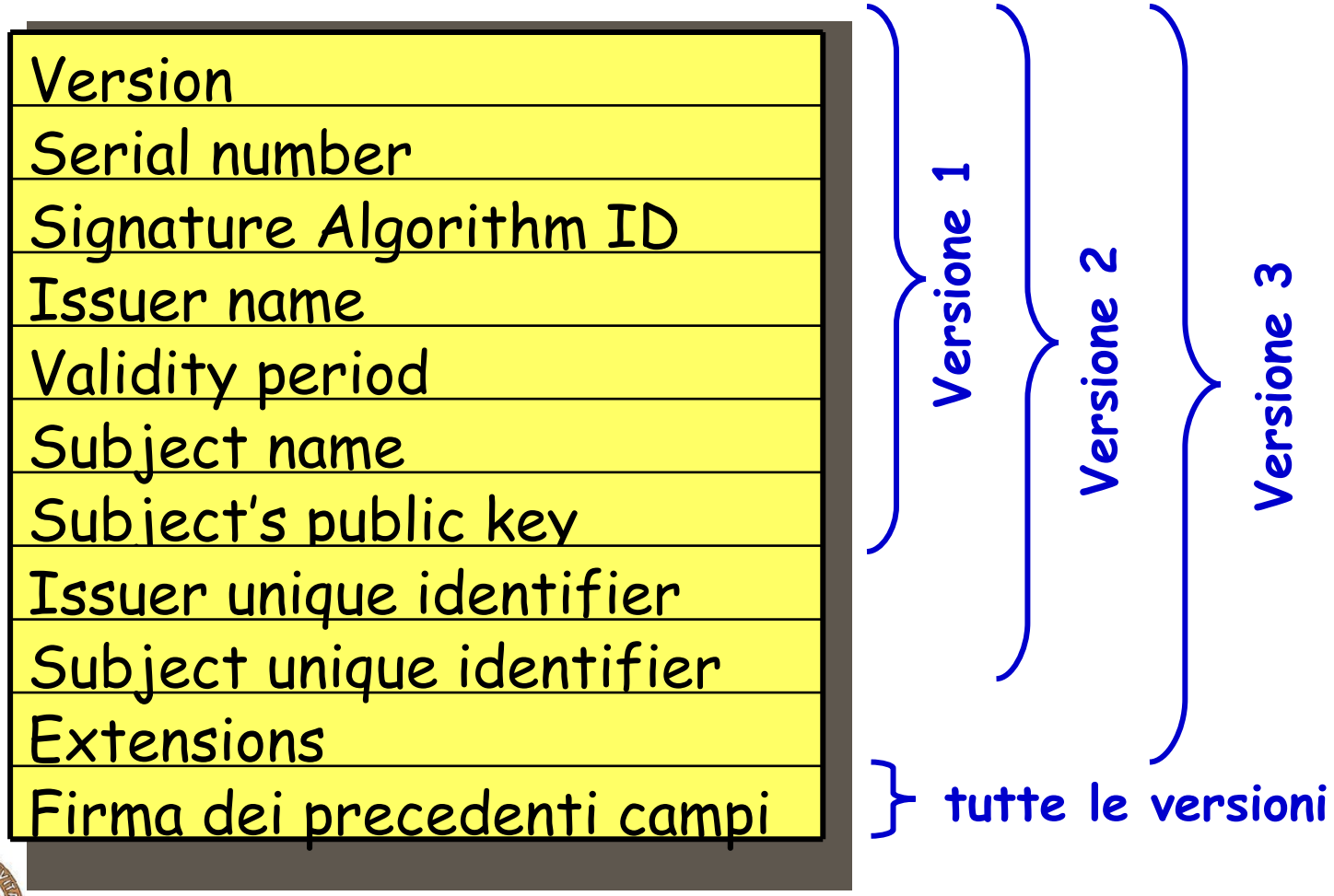
# Certificate Revocation List (CRL)

- Lista firmata dalla CA contenente:
  - numeri seriali dei certificati emessi revocati
    - (ma non ancora scaduti)
  - quando è avvenuta la revoca
  - altro (per es., motivi)
- La data della CRL indica quanto sia aggiornata

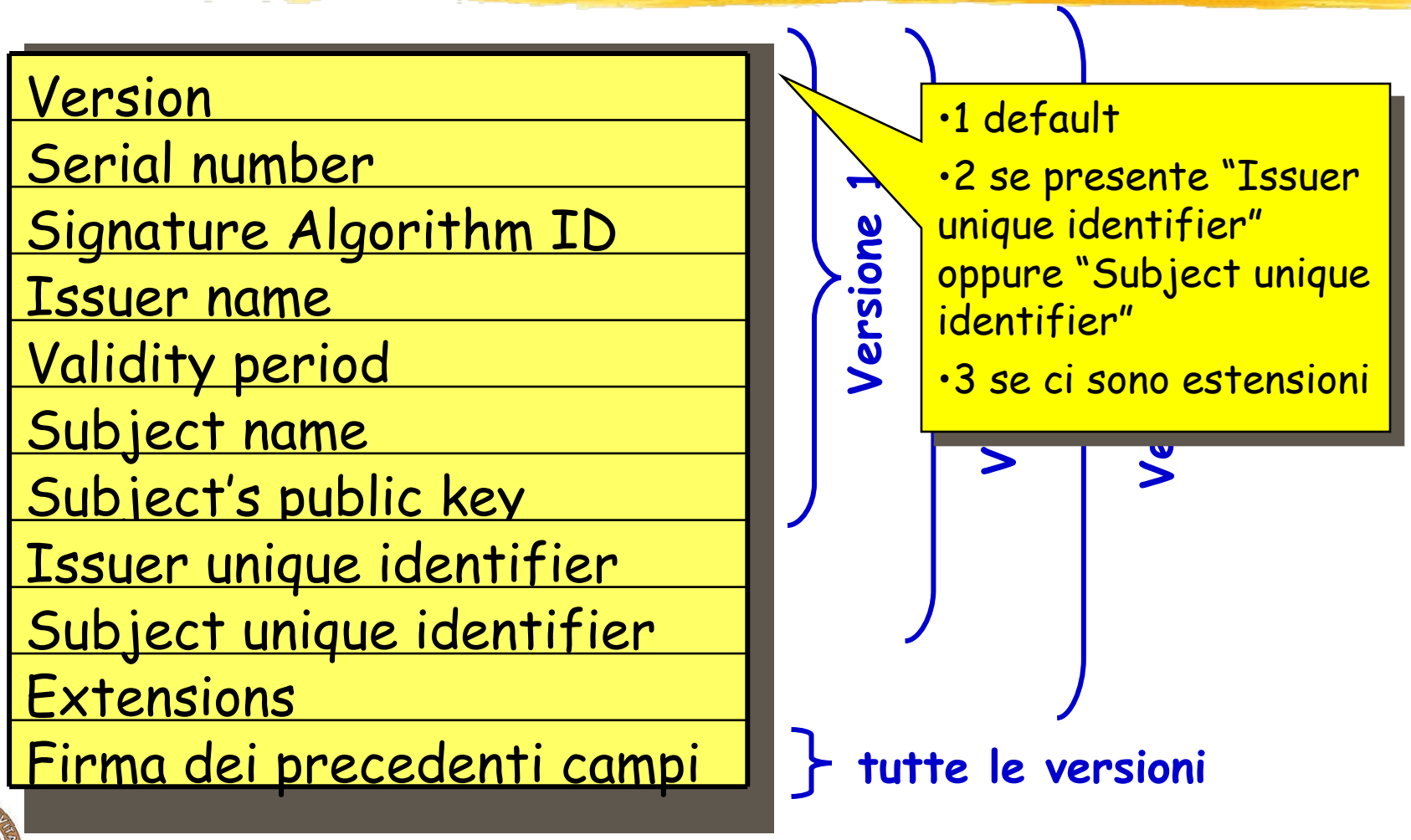
# Standard dei certificati X.509

- Più diffuso ed utilizzato standard per i certificati
- Parte della serie X.500 di raccomandazioni che definisce un "directory service"
  - directory: server o insieme distribuito di server che mantiene un database di informazioni su utenti
- Definito nel 1988 da ITU-T, modificato nel 1993 e 1995
  - International Telecommunication Union, Telecommunication Standardization Sector
- Usato in molte applicazioni
  - S/MIME, SSL/TLS, SET, IPSEC, …

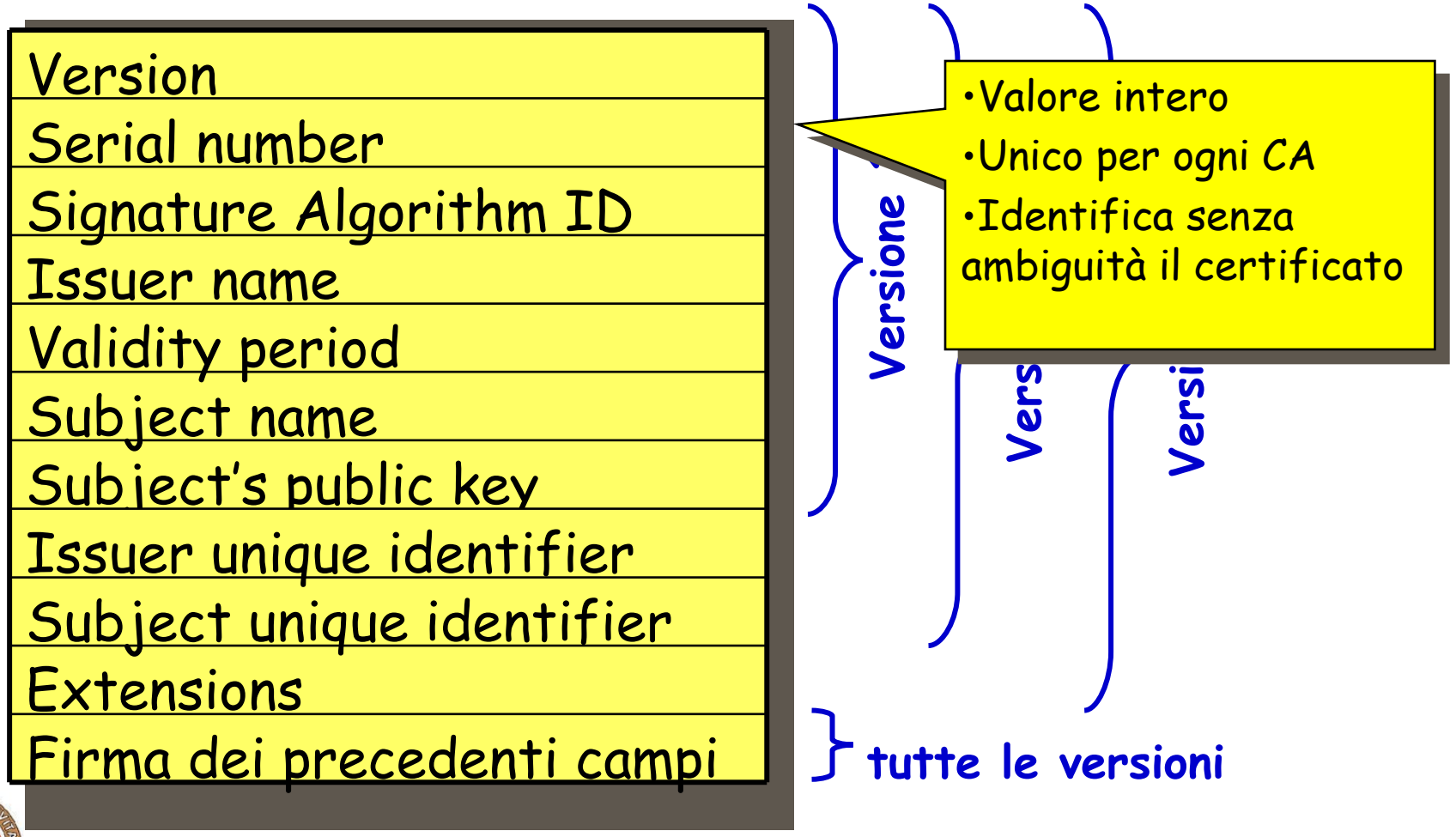
# Certificati X.509



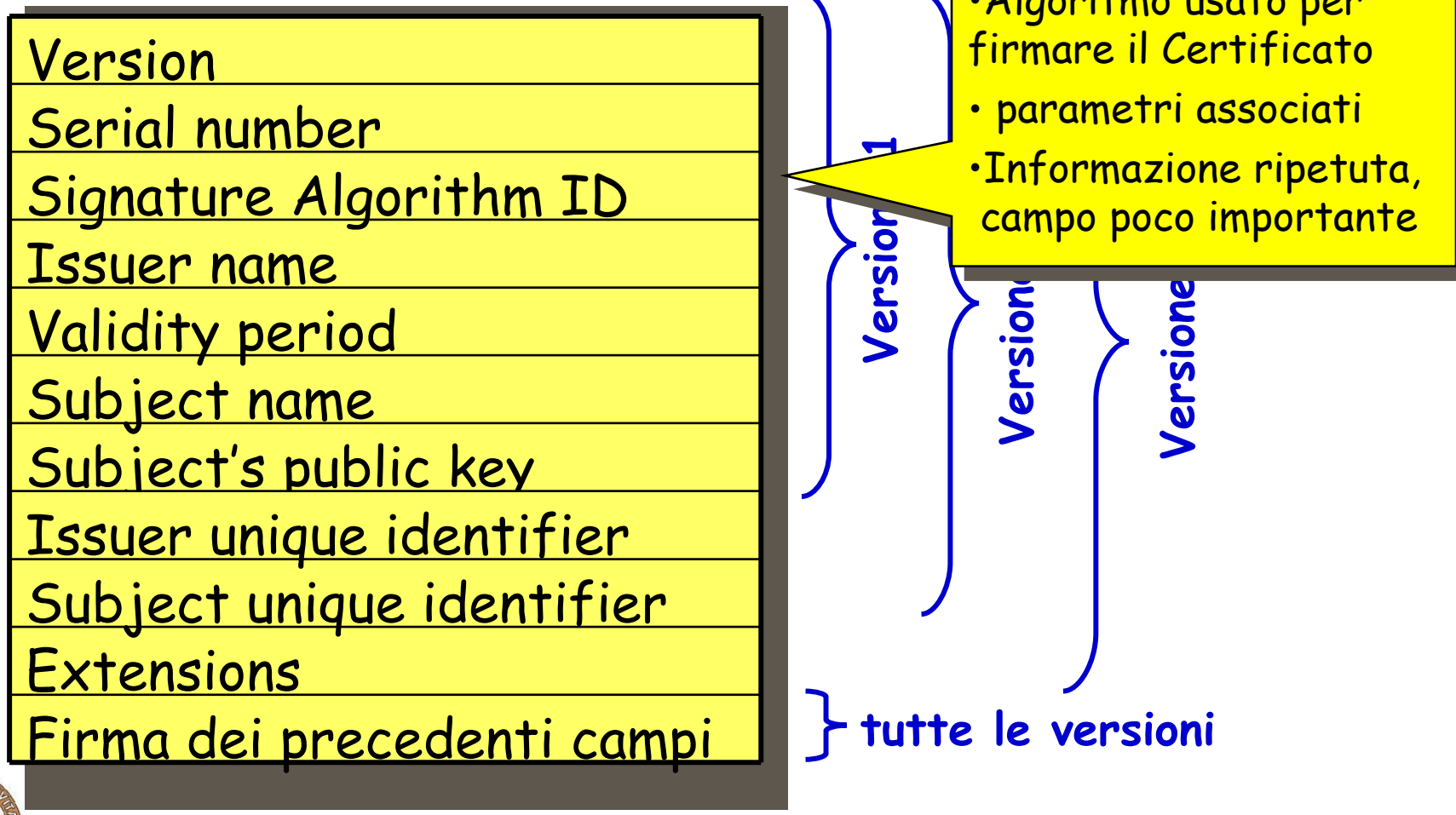
# Campi Certificati X.509



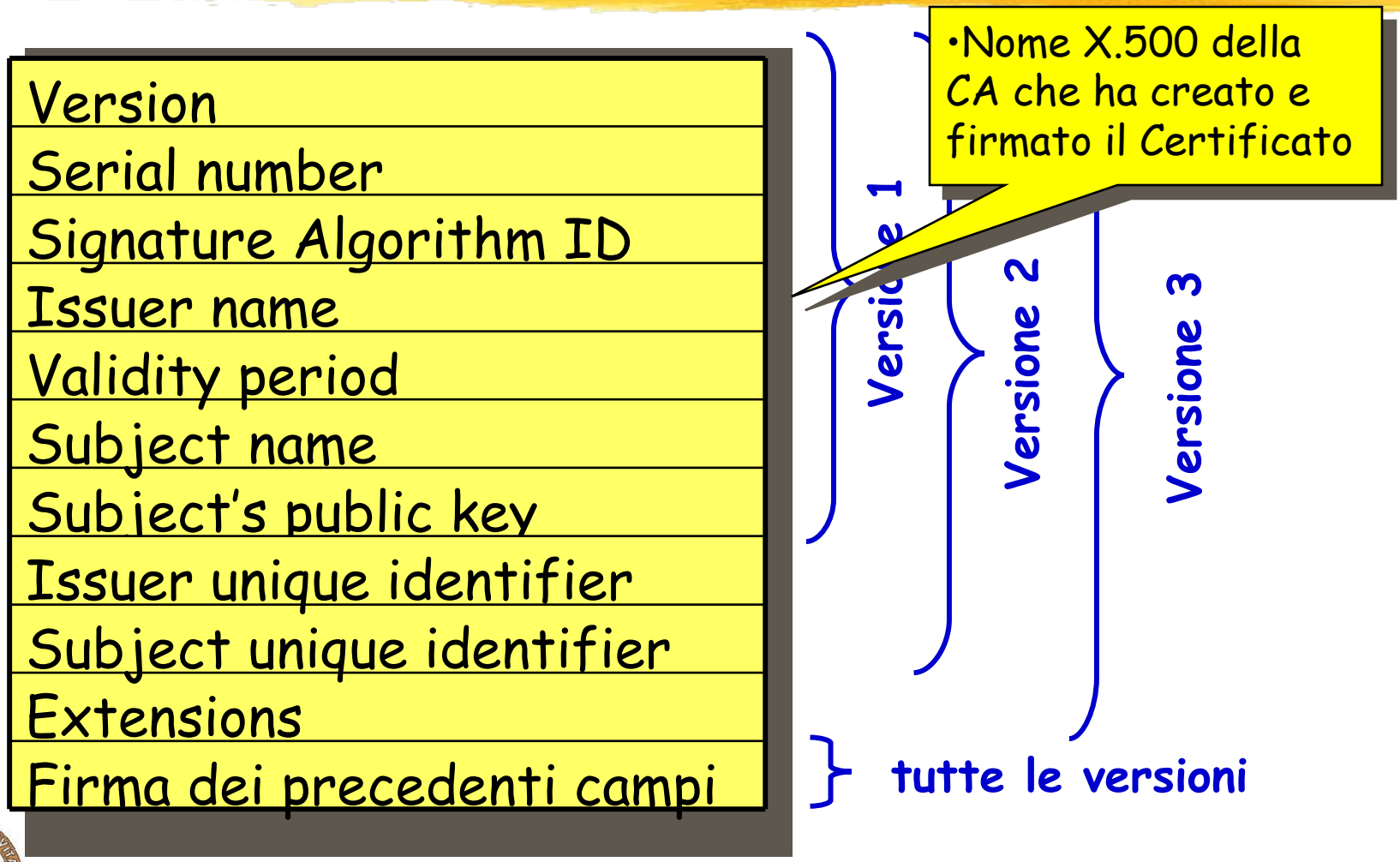
# Campi Certificati X.509



# Campi Certificati X.509



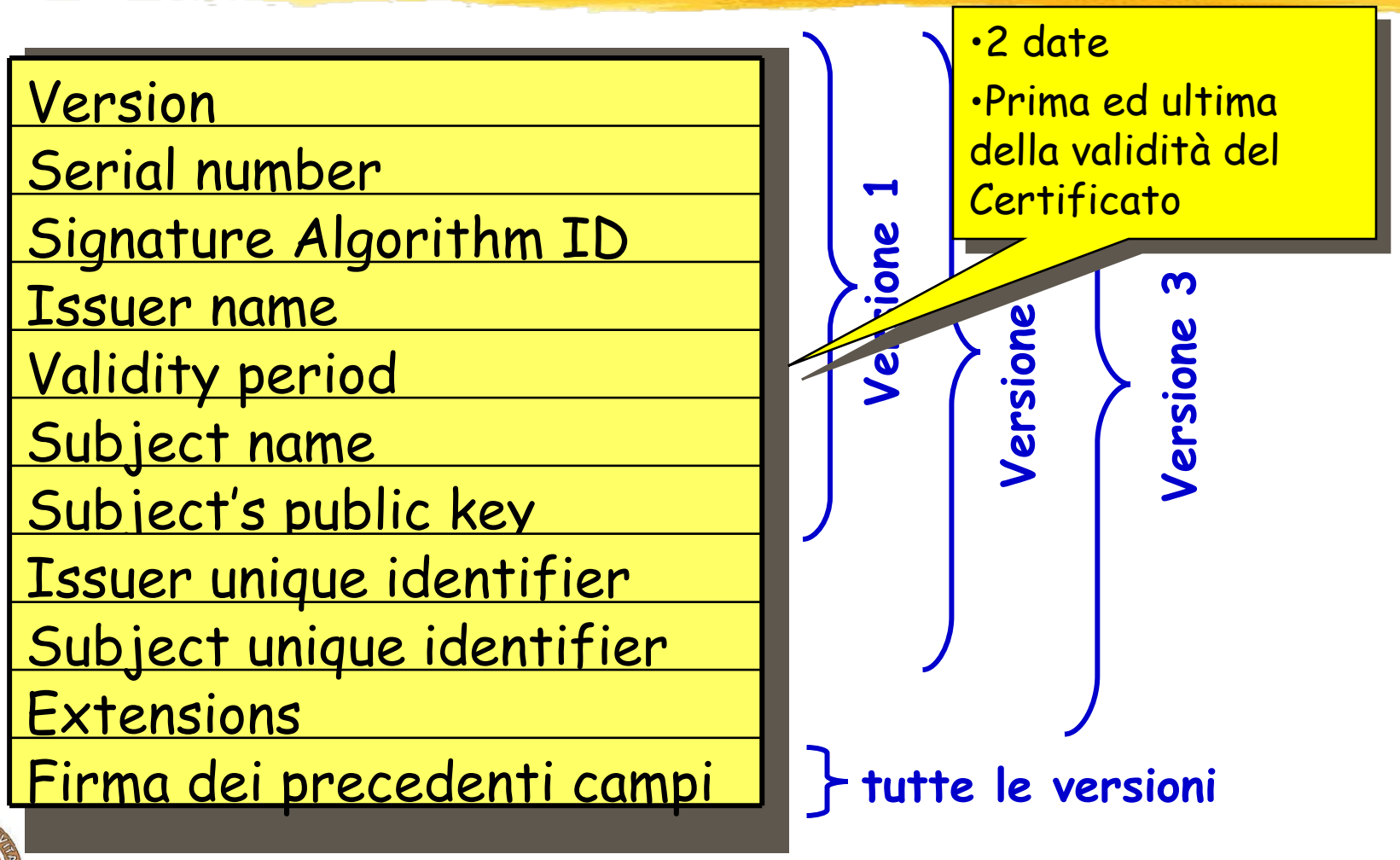
# Campi Certificati X.509



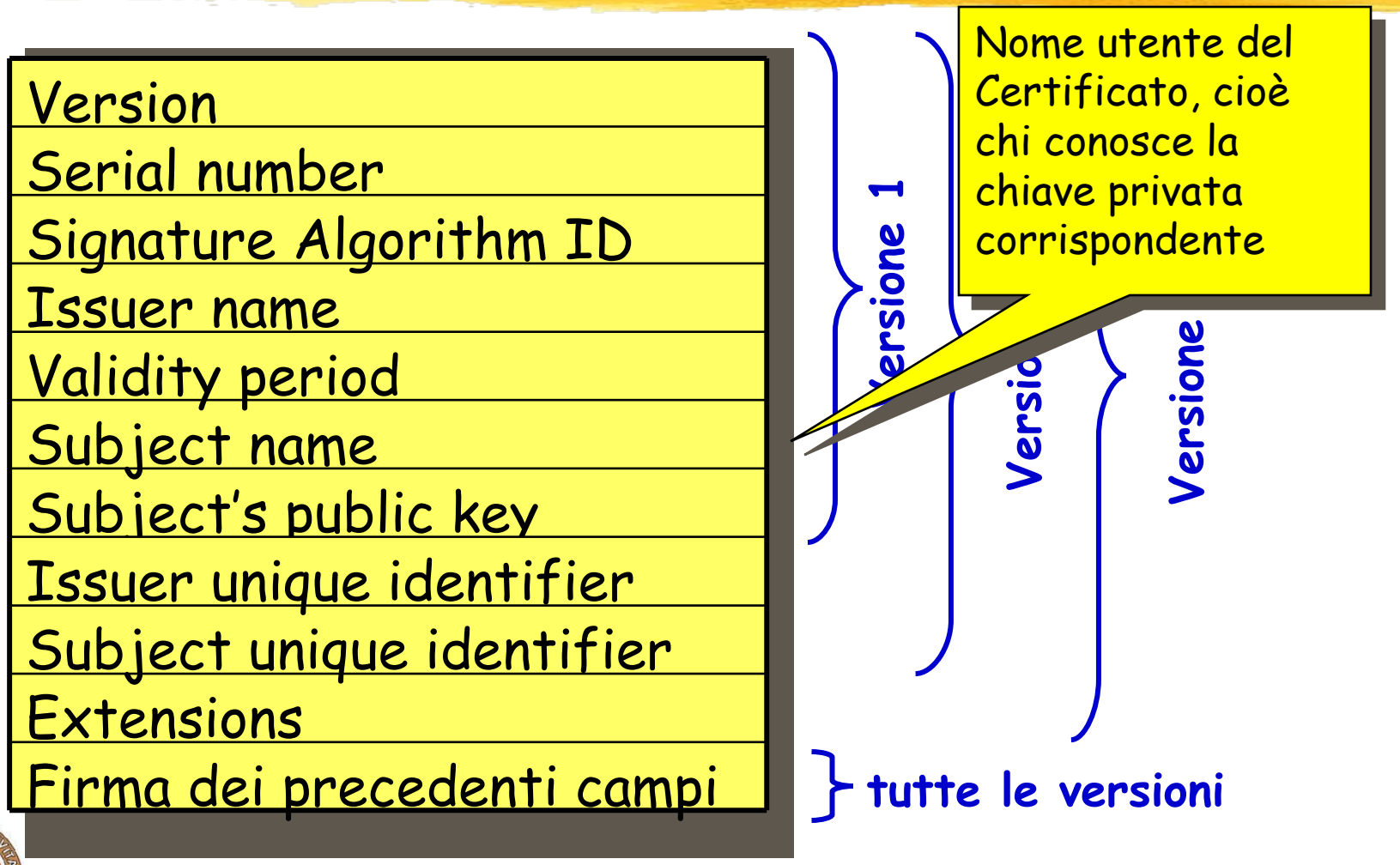
# Nome X.500

Sequenza di coppie nome-valore che identificano univocamente un'entità

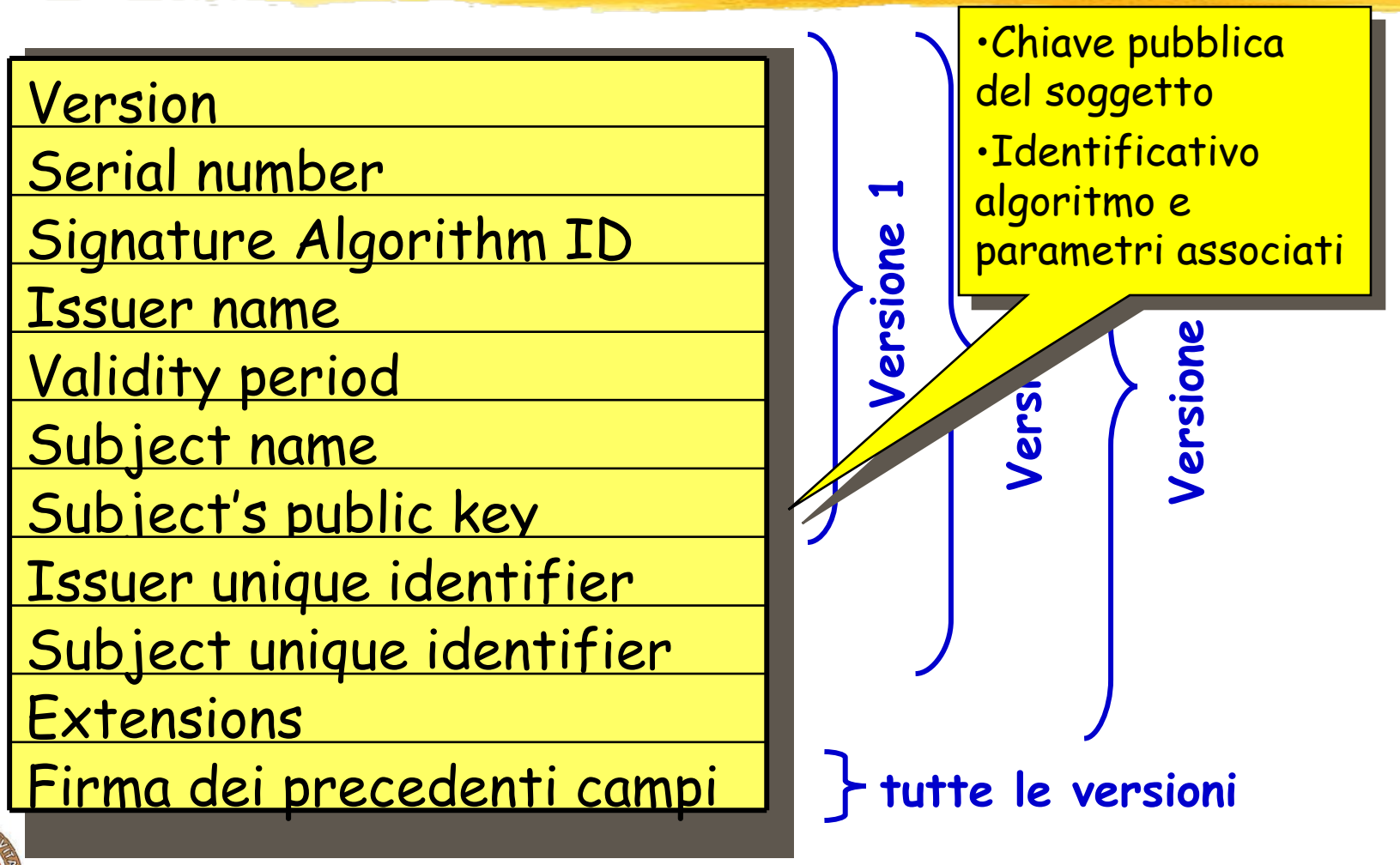

# Campi Certificati X.509



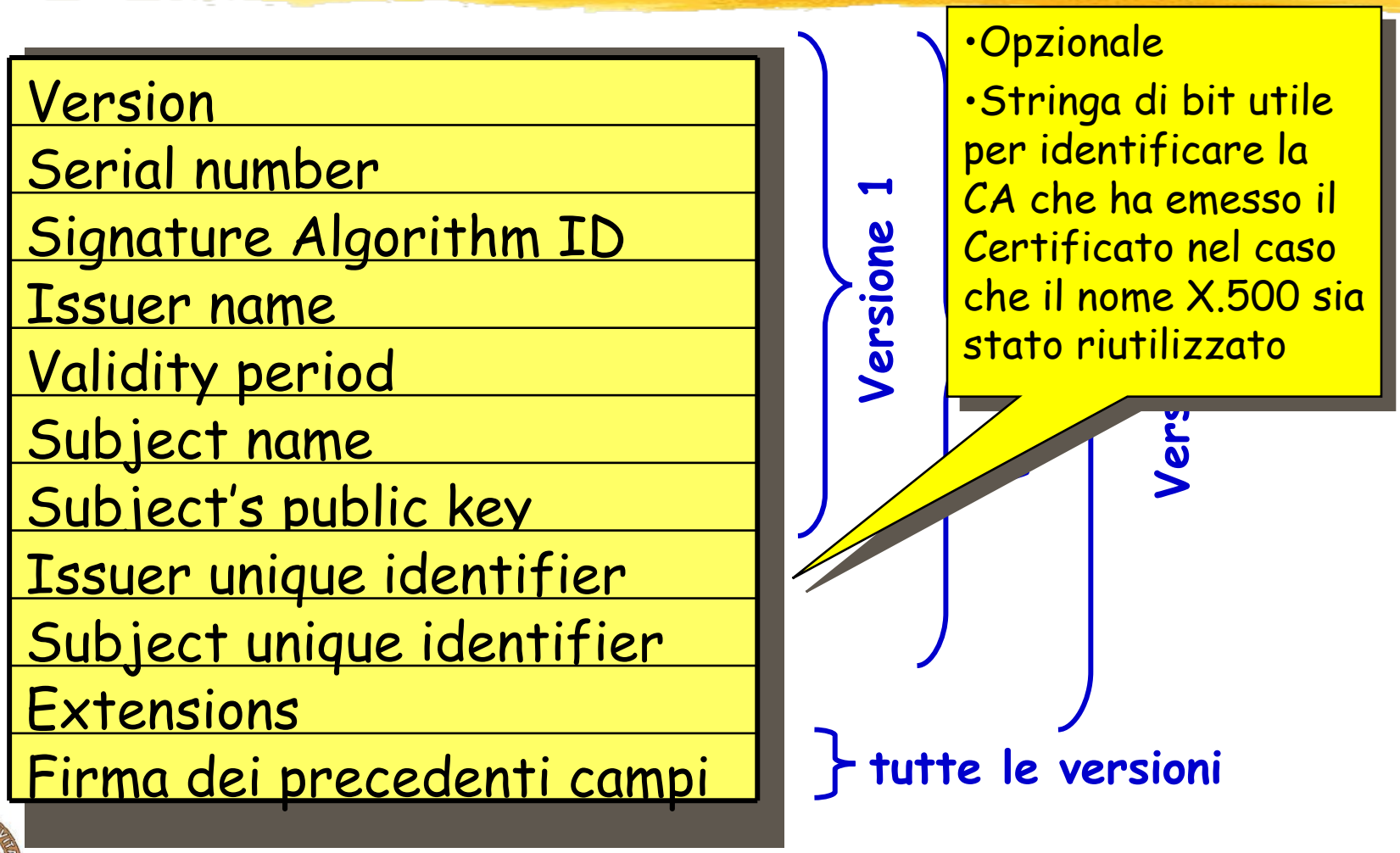
# Campi Certificati X.509



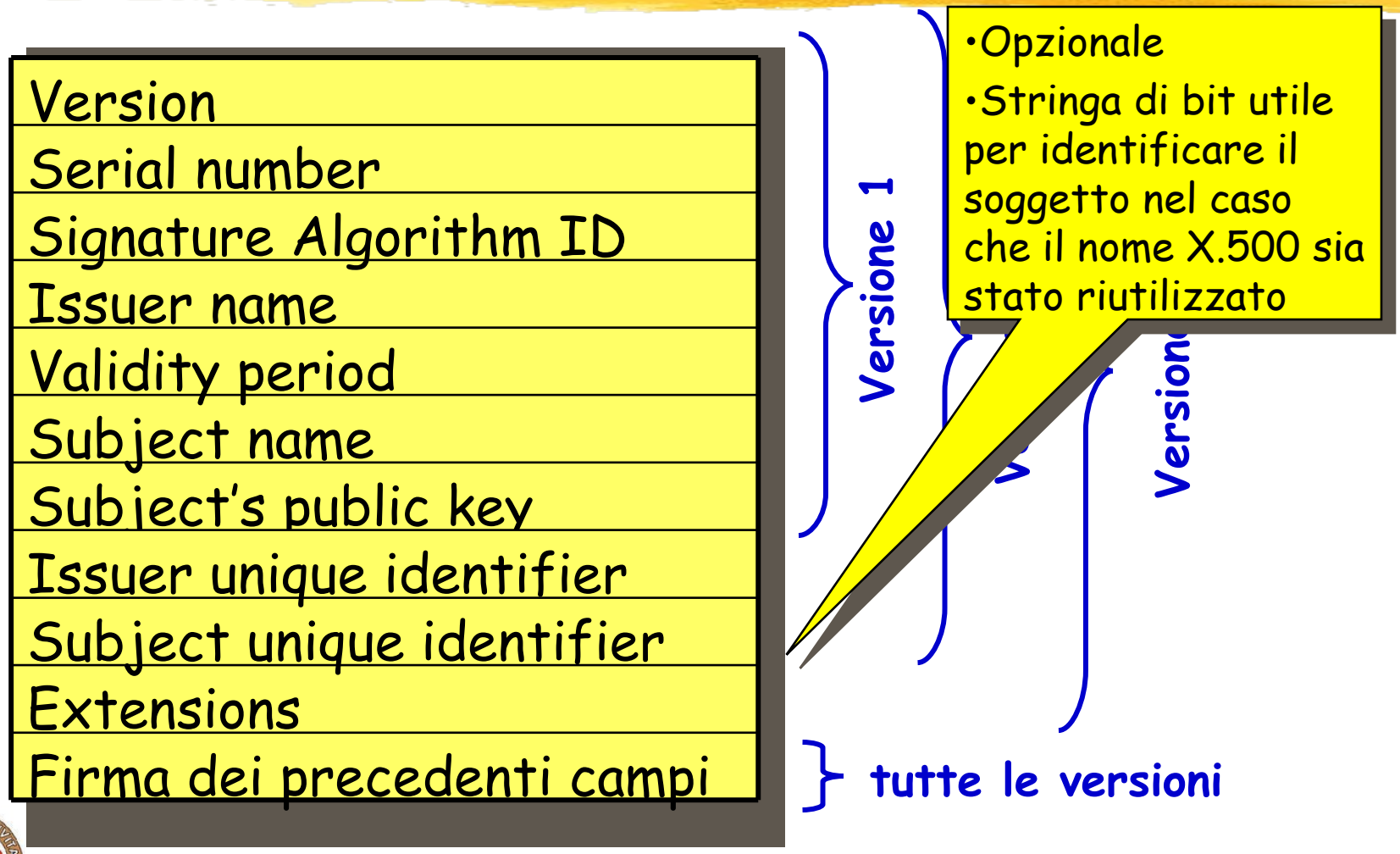
# Campi Certificati X.509



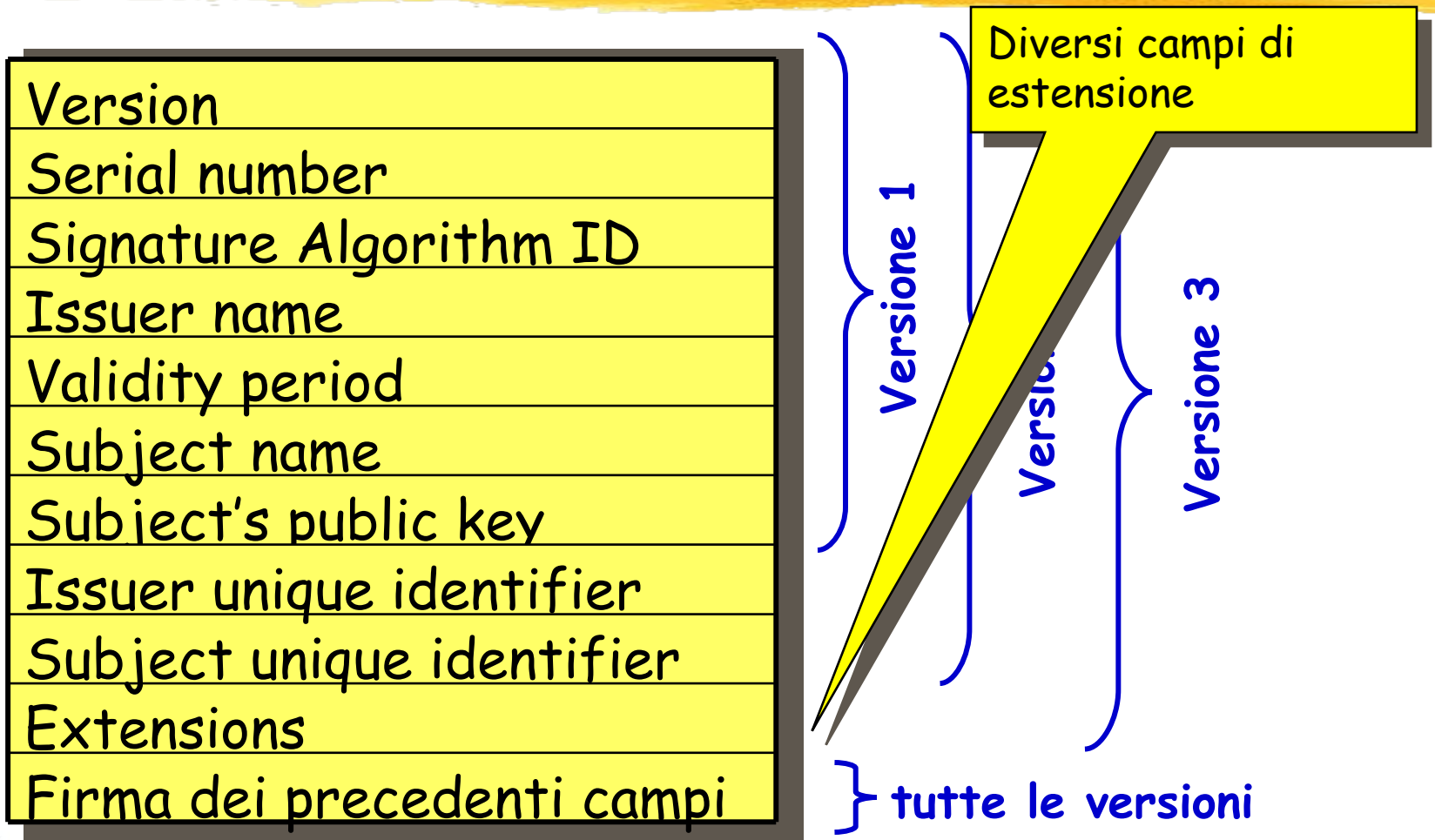
# Campi Certificati X.509



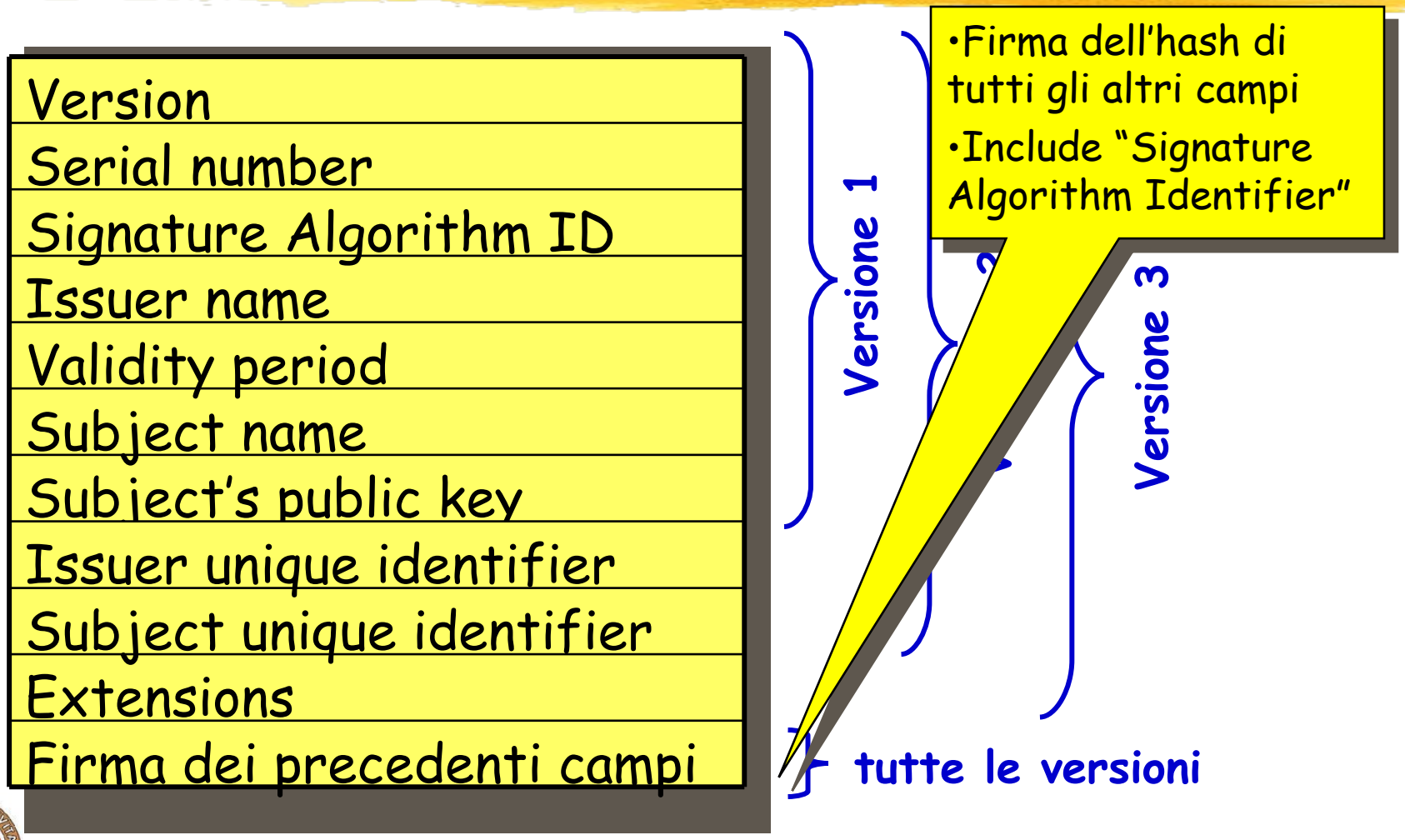
# Campi Certificati X.509



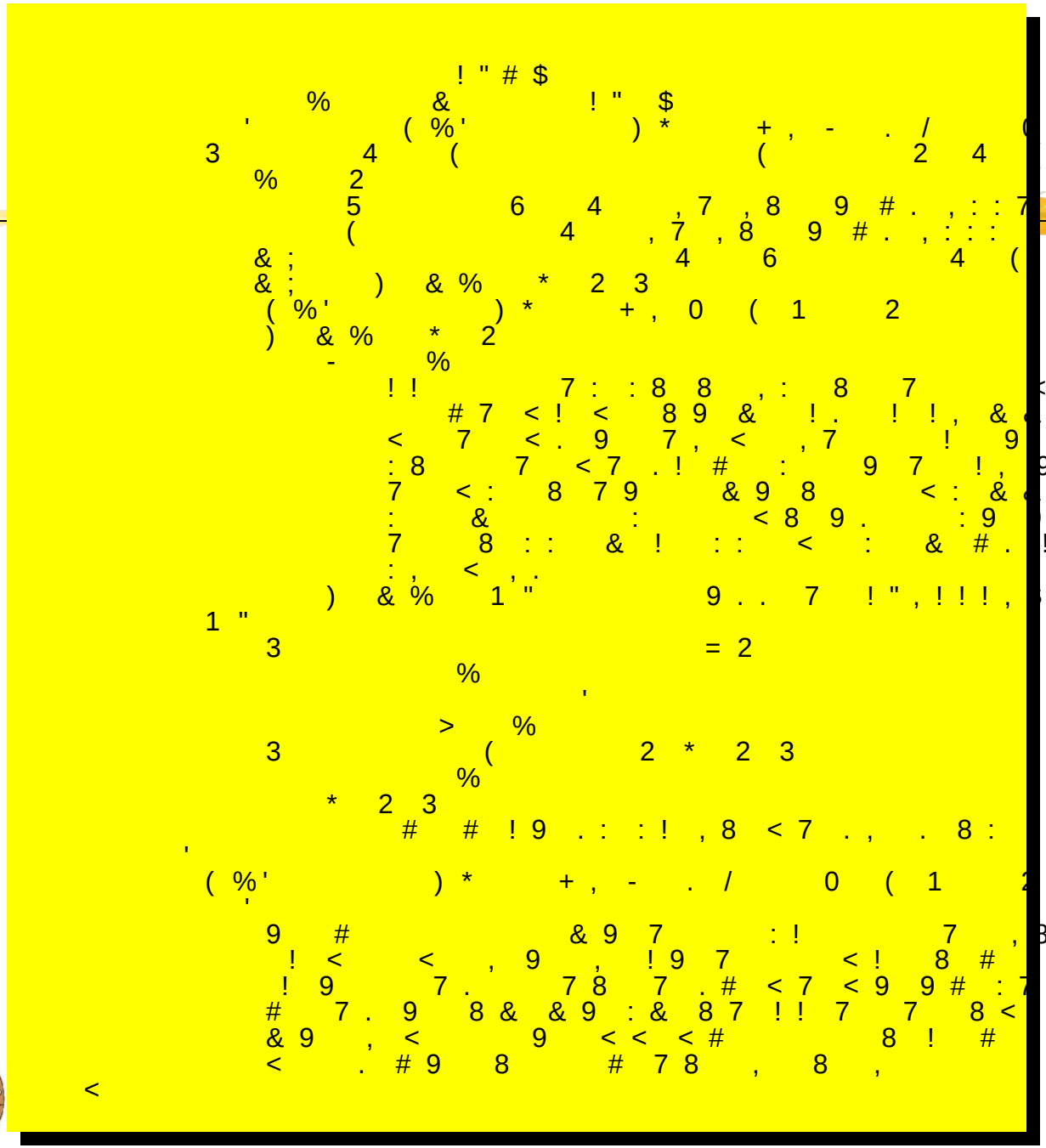
# Campi Certificati X.509



# Campi Certificati X.509



# Esempio



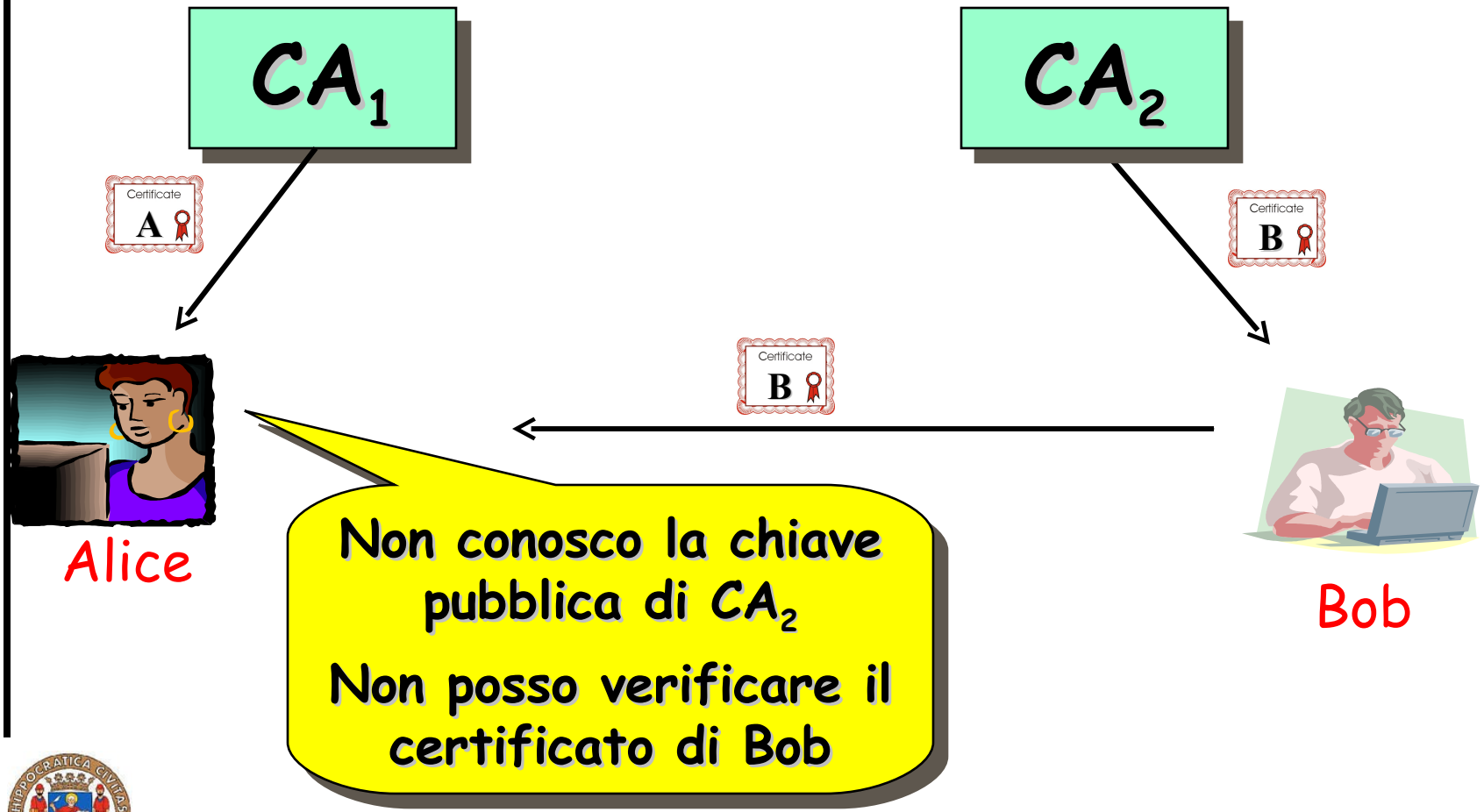
# Certificato in base64-encoded form

```
?????5 1 @ 3    1 0 = 36 3  ( = 1 ?????
 33  * A   ( B  ' ( C 35 ( ' 35 ( A (  5 ' D E  D  @  : C ! 5 ( F  F  6 (
 ( 8 @ ( ,  1   - 3 =   !  #   @  " 6 = ( = 5 '   5 (  =  6  ,  H
 = ' C - = - # - ;  6 C ! . 4 = 1 C - = ' C - = - # - ;  - 1 ' "  A (  5
1 C  4 B I 0 A G # 6 C B = 1  - (  @ ( ,  1  " - 1  H   A 1 I - 5
 H D C ' B 8 C  F  G  *  B 3   ( F 1 6 5 F (  ' G ! ( - 3 @  (  @
7   ( = G  A 5  ( 5  , (  2  7   0 D  F  , 6 & I 6 4 @   C  D  &  9
 F B 5  I  ! D <  K # F 9 "  # - )  J 8 / *  - 4  =  A  K  @
 -  '  -  # -  9  D  F  ( ' - 5 ( ( @ ;  ; ( ! - 5 1 @  /  @  (
H  - 1 @  ( / ' 5 = 2 8 ' B B D 5  H  /  - ,  "  B  K A G  2 = (
39 JA ! 7 B 9  .  A I < I & ( 6  ;%0 %J( G C F A =  G " 8 @  ( E
 D  @  G  #  G 0  ' *  < - C E  / 2 >  H ( H , 8  H B .  ! !
 /  / /  5  E  * .  G < JA  <  = ;" 7  C  -  @ C & /  0 E ;  , (
?????1  1 0 = 36 3  ( = 1 ?????
```

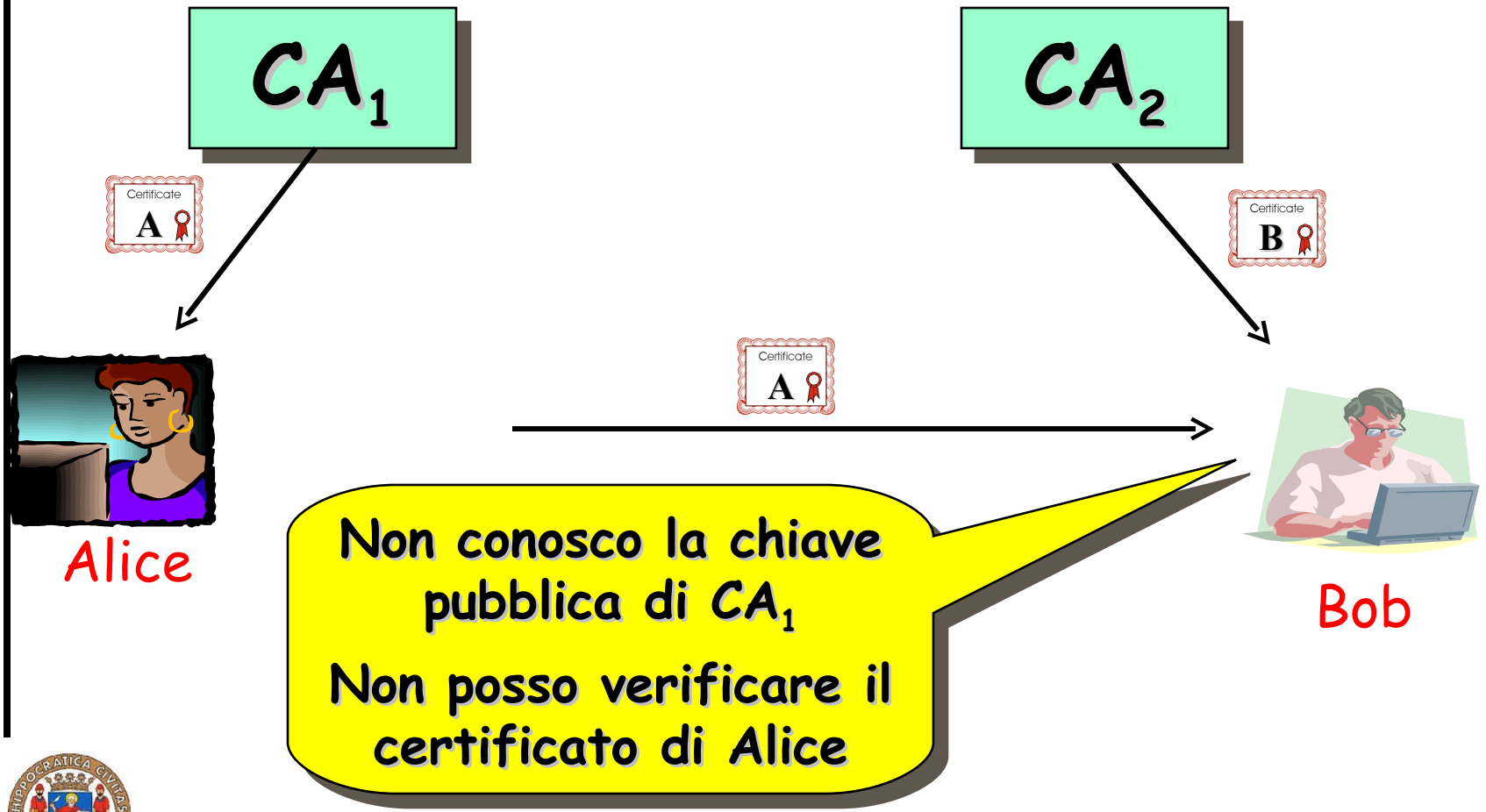
# Notazione dello standard

- Y<<X>>
  - certificato utente X creato dalla Autorità Y
- Y{I}
  - Firma dell'hash di I da parte di Y

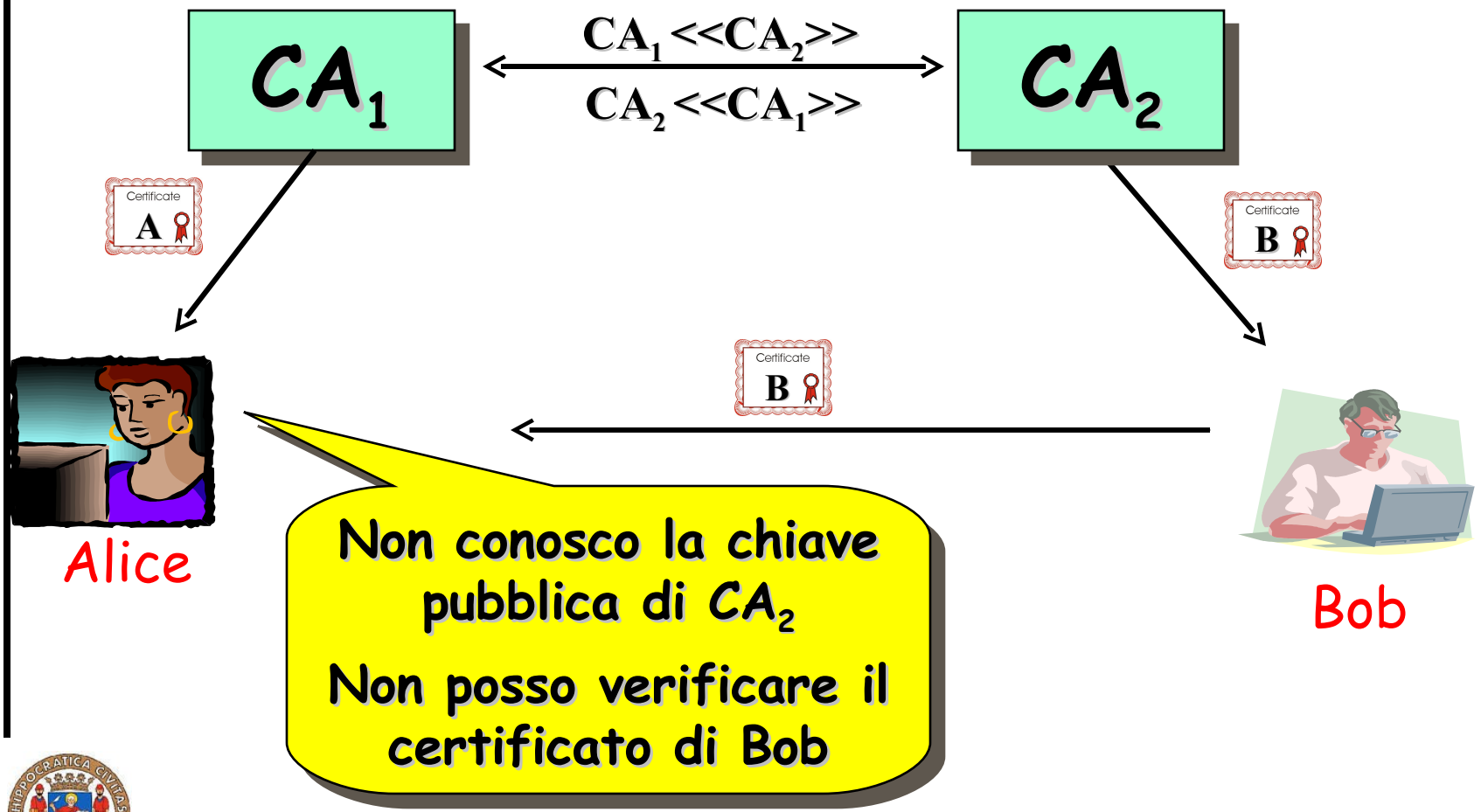
# Diverse CA


$CA_1$
$CA_2$
Certificate A
Certificate B
Certificate B
Alice
Bob
Non conosco la chiave pubblica di $CA_2$
Non posso verificare il certificato di Bob

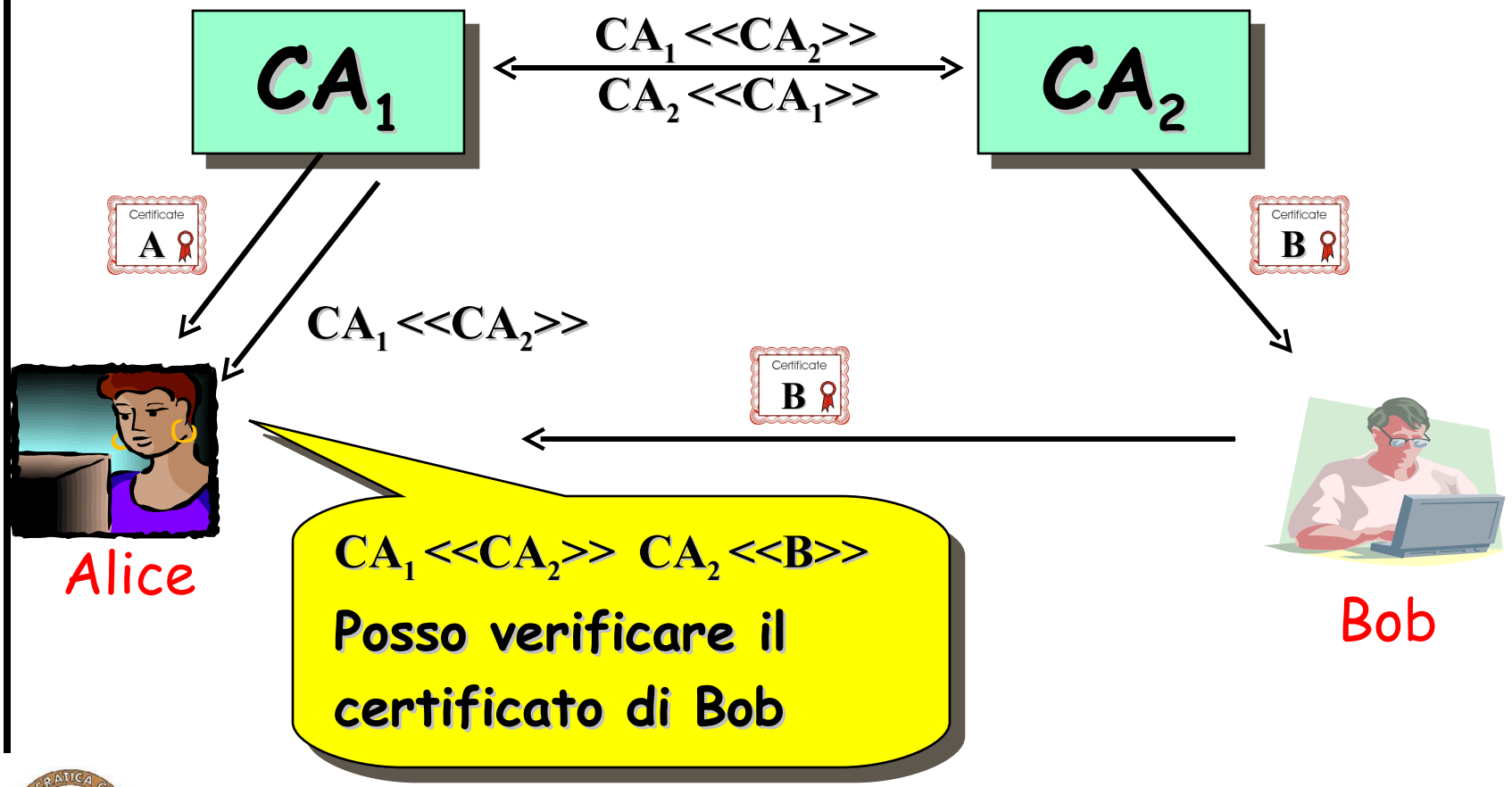
# Diverse CA


$CA_1$
$CA_2$
Certificate A
Certificate B
Certificate A
Alice
Bob
Non conosco la chiave pubblica di $CA_1$
Non posso verificare il certificato di Alice

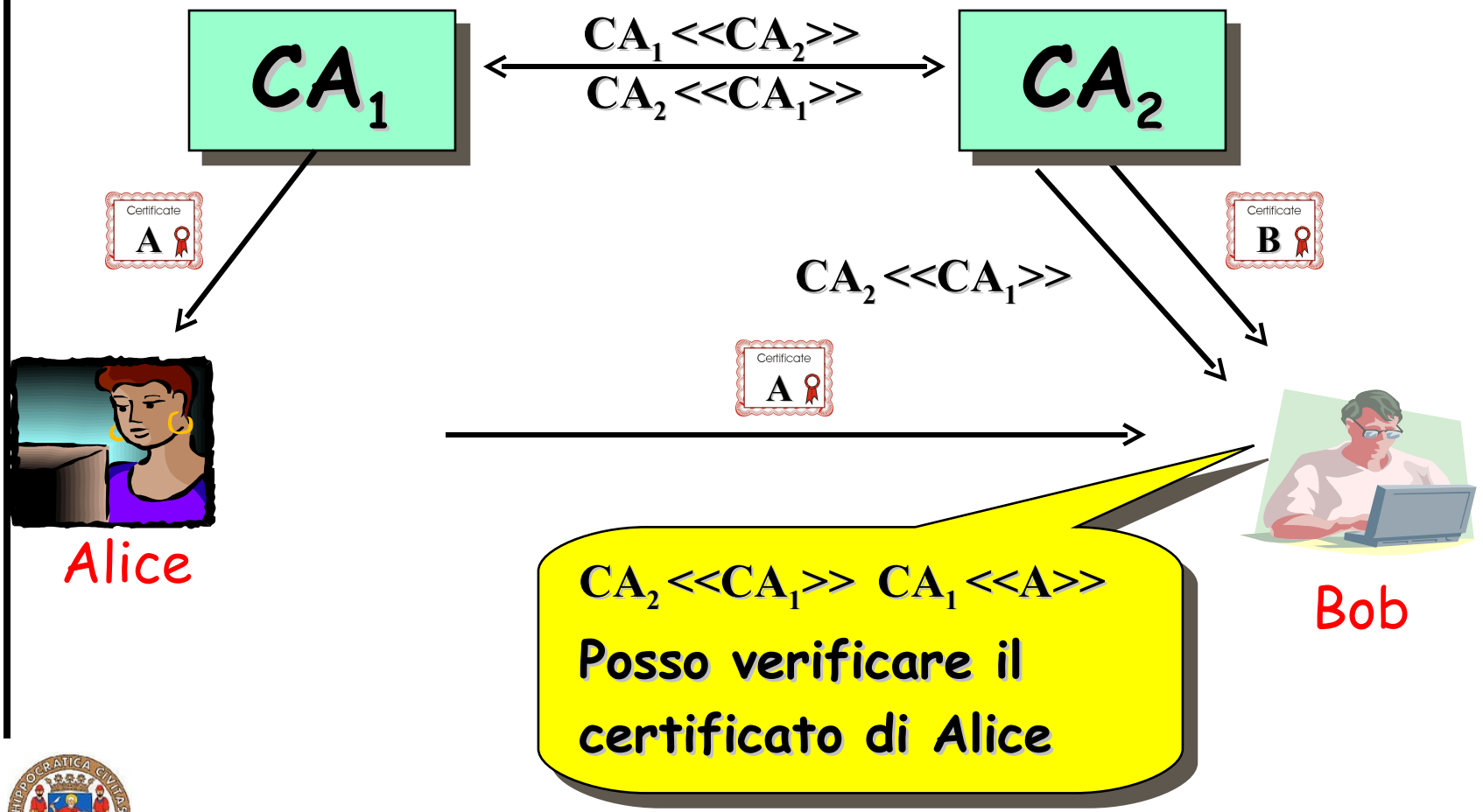
# Diverse CA


$CA_1$
$CA_1 <<CA_2>>$
$CA_2 <<CA_1>>$
$CA_2$
Certificate A
Certificate B
Certificate B
Alice
Bob
Non conosco la chiave pubblica di $CA_2$
Non posso verificare il certificato di Bob

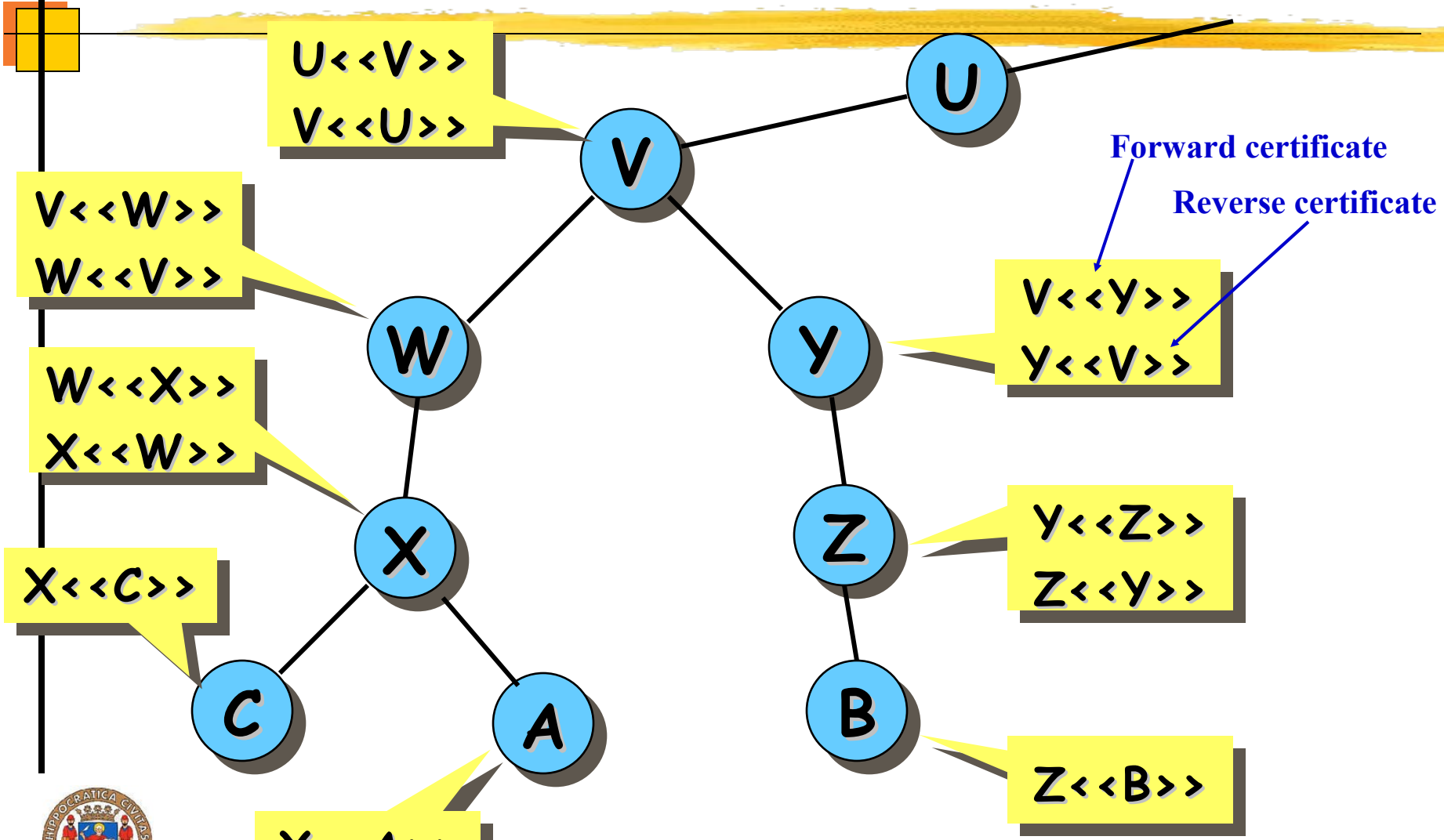
# Diverse CA


$CA_1$
$CA_1 <<CA_2>>$
$CA_2 <<CA_1>>$
$CA_2$
Certificate A
Certificate B
$CA_1 <<CA_2>>$
Certificate B
Alice
Bob
$CA_1 <<CA_2>>$ $CA_2 <<B>>$
Posso verificare il certificato di Bob

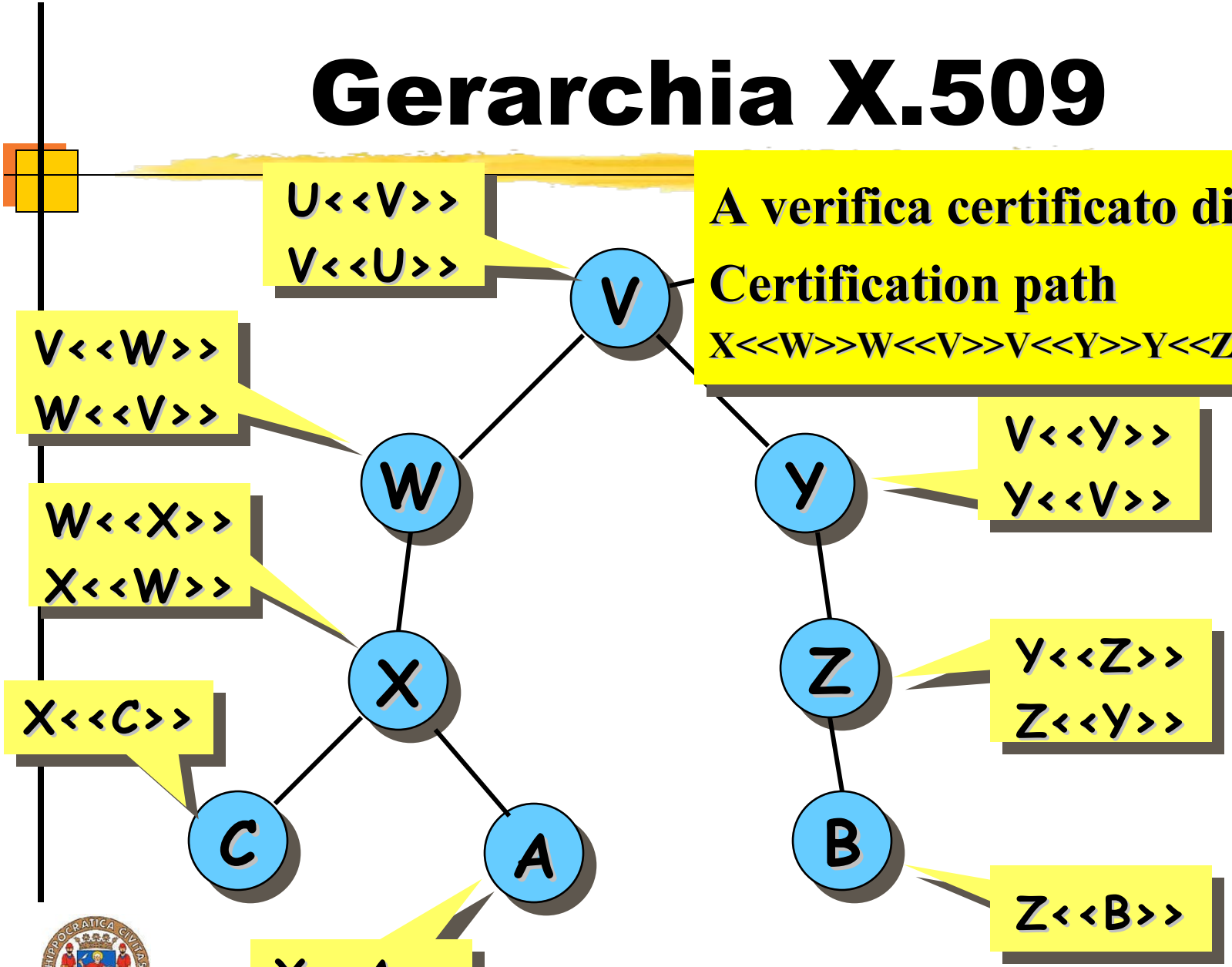
# Diverse CA


$CA_1$
$CA_1 <<CA_2>>$
$CA_2 <<CA_1>>$
$CA_2$
Certificate A
Certificate B
$CA_2 <<CA_1>>$
Certificate A
Alice
Bob
$CA_2 <<CA_1>>$ $CA_1 <<A>>$
Posso verificare il certificato di Alice

# Gerarchia X.509



# Gerarchia X.509



# Revoca di certificati

- Ogni CA mantiene lista dei propri certificati che sono stati revocati ma non scaduti
- Bisogna controllare se un certificato non sia stato revocato
- Caching dei certificati revocati

# CRL

| |
|---|
| Signature Algorithm Identifier |
| Issuer name |
| Data di questo aggiornamento |
| Data del prossimo aggiornamento |
| User certificate serial number |
| Data della revoca |
| … |
| User certificate serial number |
| Data della revoca |
| Firma |

Certificato revocato

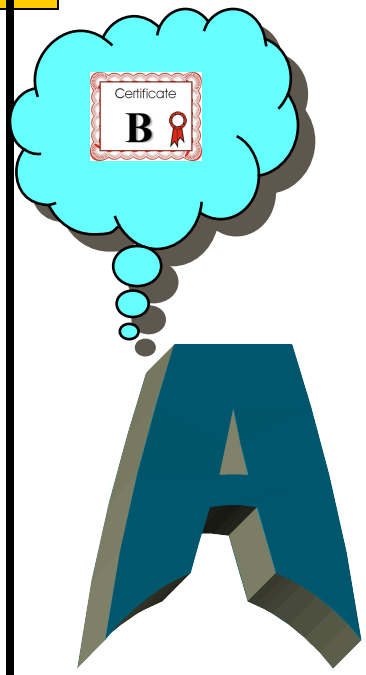
Certificato revocato

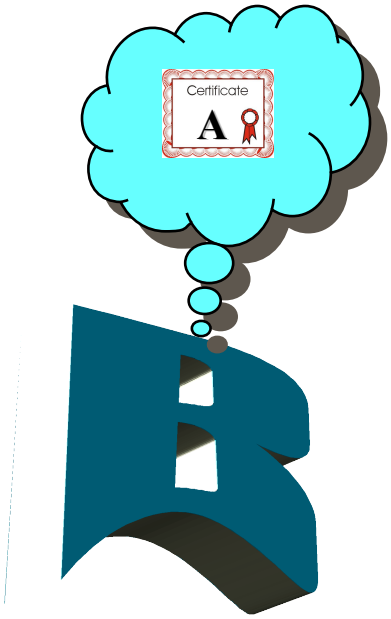
# Autenticazione X.509

X.509 fornisce anche tre procedure di autenticazione:

- Autenticazione One-way
- Autenticazione Two-way
- Autenticazione Three-way

# Autenticazione X.509



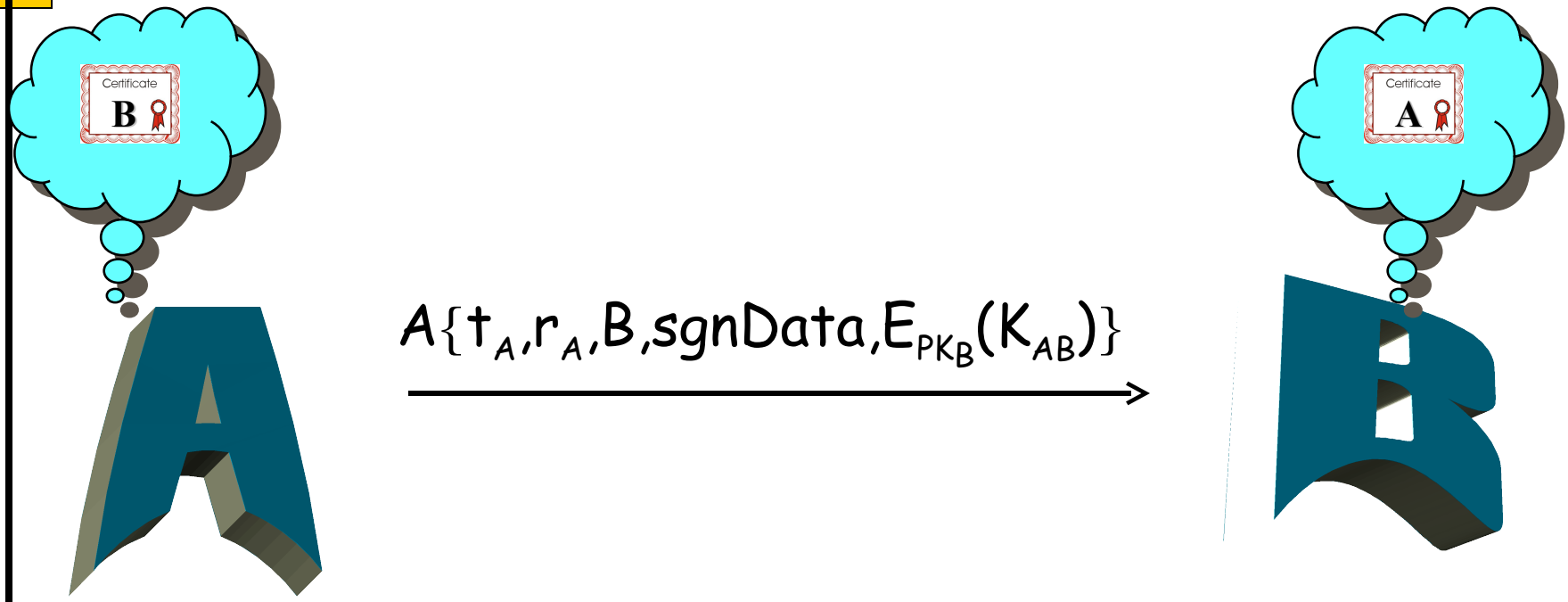




Assumiamo che entrambi conoscano le chiavi pubbliche

-Scambio dei certificati come primo messaggio, oppure

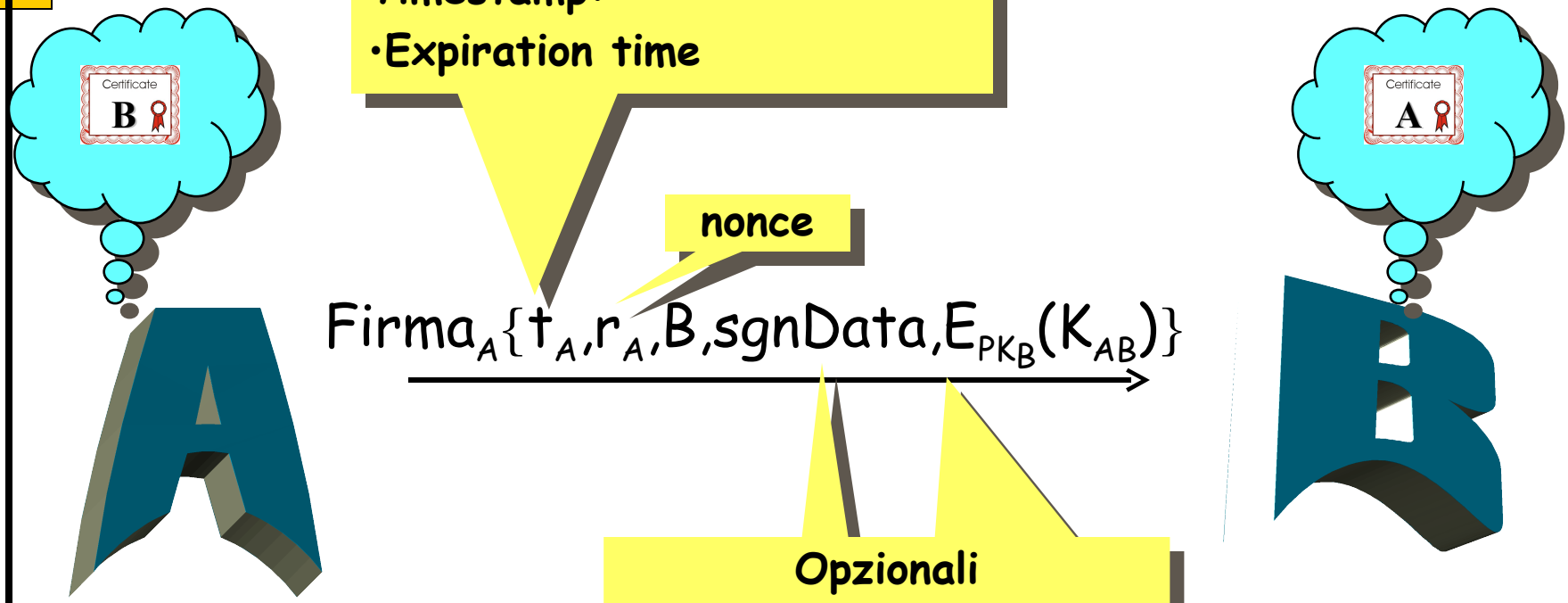
-Certificati ottenuti dalla directory

# Autenticazione One-way

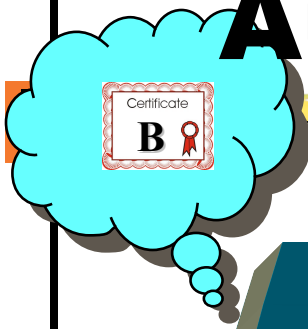



- Messaggio di *A*
- Diretto a B
- Integrità ed originalità (non inviato più volte) messaggio

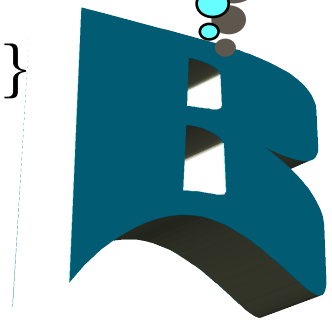
# Autenticazione One-way



# Autenticazione One-way

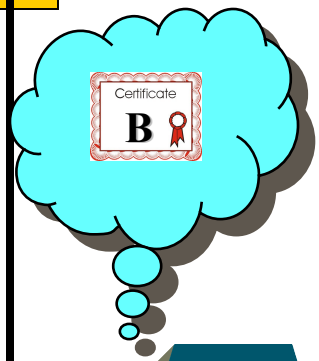



$Firma_A\{t_A, r_A, B, sgnData, E_{PK_B}(K_{AB})\}$


$Firma_A\{t_A, r_A, B, sgnData, E_{PK_B}(K_{AB})\}$

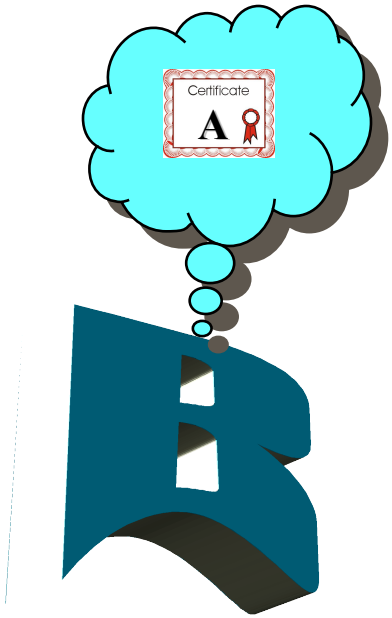
# Autenticazione One-way




Timestamp:
·Expiration time

nonce

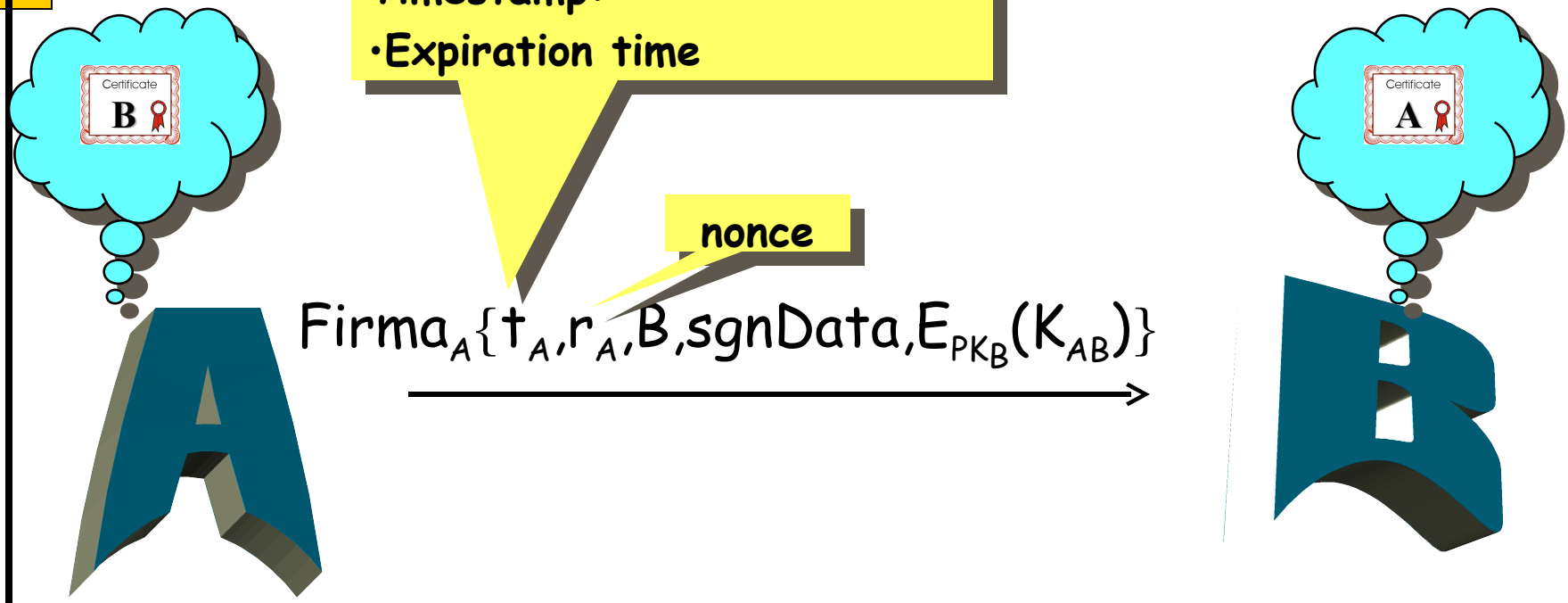
$Firma_A\{t_A, r_A, B, sgnData, E_{PK_B}(K_{AB})\}$




Devo conservar e il nonce

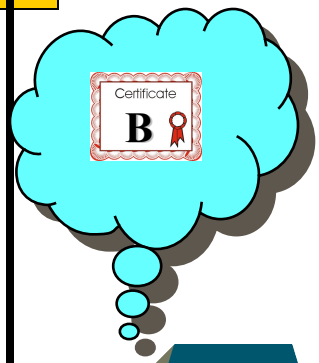
Nonce unico fino all'expiration time, per evitare attacchi di replay

# Autenticazione One-way

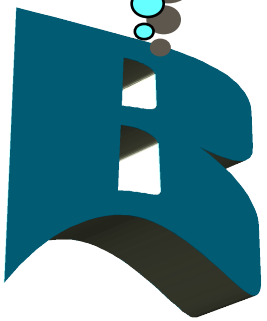



- Messaggio di *A*
- Diretto a B
- Integrità ed originalità (non inviato più volte) messaggio

# Autenticazione Two-way







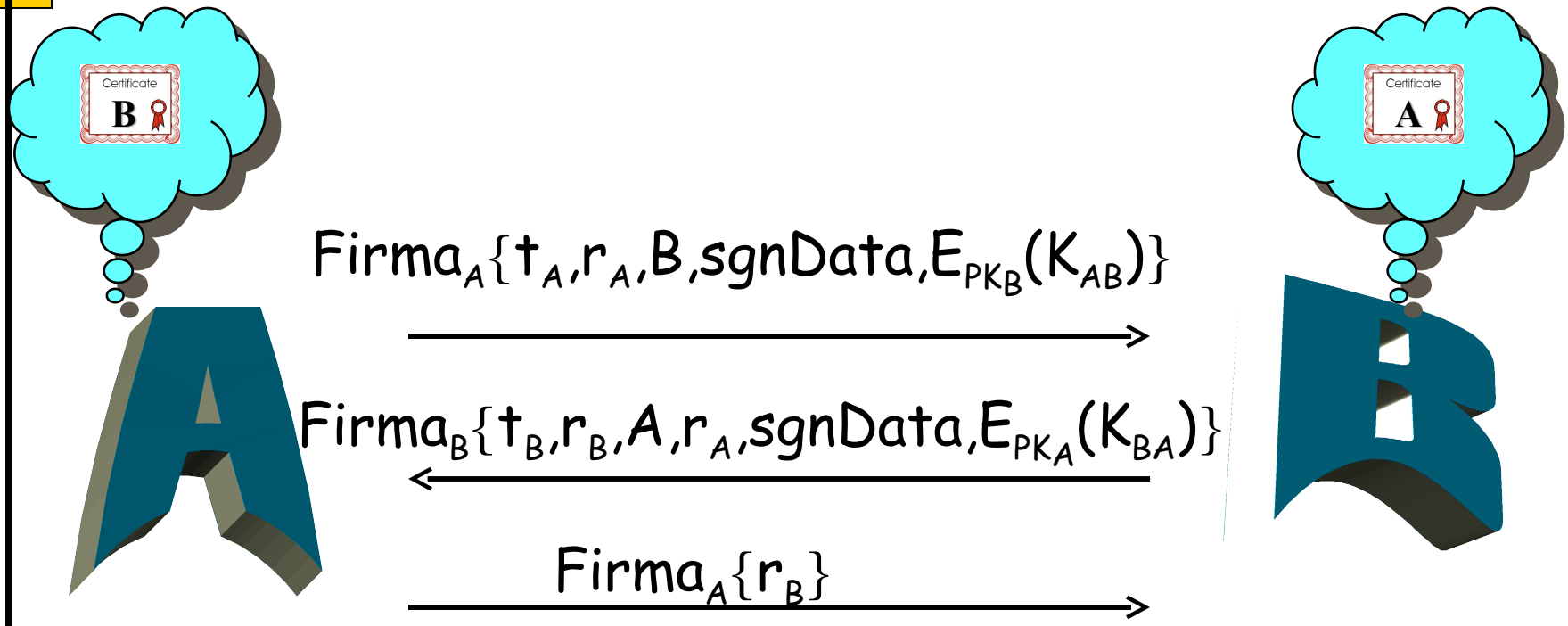
$Firma_A\{t_A, r_A, B, sgnData, E_{PK_B}(K_{AB})\}$ →

$Firma_B\{t_B, r_B, A, r_A, sgnData, E_{PK_A}(K_{BA})\}$ ←

**opzionali**

Messaggio di B
Diretto ad A
Integrità ed originalità messaggio di B

# Autenticazione Three-way




Scopo: Eliminare il check dei timestamp

Necessario in assenza di clock sincronizzato

# X.509 versione 3

Requisiti non soddisfatti dalla versione 2 [W. Ford 1995]

- Subject field non adeguato: nomi X.509 sono corti, e mancano dettagli identificativi che potrebbero essere utili
- Subject field non adeguato per le applicazioni che riconoscono entità dall'indirizzo email, URL
- Vi è necessità di indicare politiche di sicurezza
- Vi è necessità di limitare il danno che potrebbe fare una CA maliziosa, ponendo vincoli all'applicabilità di un particolare certificato
- E' importante distinguere chiavi diverse usate dallo stesso utente in tempi diversi

# X.509 versione 3

Estensioni opzionali nella versione 3

- Soluzione flessibile
- Meglio dell'aggiungere altri campi fissi alla versione 2

Ogni estensione contiene:

- Identificatore estensione
- Indicatore di criticità
- Valore estensione

**·Indica se l'estensione può essere ignorata**

**·Se TRUE e l'implementazione non riconosce l'estensione allora deve trattare il certificato come non-valido**

# Categorie Estensioni

Tre categorie principali per le estensioni:

- Key and Policy Information
- Certificate Subject and Issuer Attributes
- Certification Path Constraints

# Key and Policy Information

## Authority key identifier

indica quale di più chiavi pubbliche della CA usare per verificare la firma di un certificato o della CRL

## Subject key identifier

identifica quale di più chiavi pubbliche viene certificata

## Key usage

restrizione sull'uso della chiave certificata, come scopo:
(digital signature, key encryption, data encryption, key agreement, CA signature verification on certificates, CA signature verification on CRL)

# Key and Policy Information

## Private-key usage period

periodo uso della chiave privata (per la firma, diverso periodo per chiave privata e pubblica)

## Certificate policy

insieme di regole che indica l'applicabilità di un certificato ad una comunità e/o classi di applicazioni con requisiti di sicurezza comuni

## Policy mappings

usato solo per CA da altre CA. Permette ad una CA di indicare che una propria politica può essere considerata equivalente ad un'altra politica usata dalla CA soggetto.

# Certificate Subject and Issuer Attributes

## Subject alternative name

contiene uno o più nomi alternativi, in formati alternativi.

Importante per le applicazioni che hanno formati propri per i nomi (ad es., email, IPSec)

## Issuer alternative name

contiene uno o più nomi alternativi, in formati alternativi

## Subject directory attributes

contiene attributi della directory X.500 per il soggetto del certificato

# Certification Path Constraints

## Basic constraints

indica se il soggetto può agire come CA. Se si, si possono specificare vincoli sulla lunghezza della certification path

## Name constraints

indica uno spazio dei nomi in cui tutti i seguenti certificati in un certification path devono essere

## Policy constraints

inibisce policy mappings per la parte rimanente della certification path

# Legislazione italiana

- Legge 15 marzo 1997 n. 59 "Bassanini 1" art. 15 comma 2:
  - *gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici e telematici, sono validi e rilevanti ad ogni effetto di legge*
- Regolamento attuativo DPR 513/97, G.U. n° 60 13/3/1998
- Regolamento tecnico *"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici..."* Decreto del Presidente del Consiglio dei Ministri, G.U. n° 87 del 15/4/1999

# DPR 513/97, Art. 1

*a)firma digitale: 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;*

*…*

*h) certificazione: risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;*

*…*

*k) certificatore: soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;*

# DPR 513/97, Art. 5


*1. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.*

*2. Il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.*

# DPR 513/97, Art. 8

*3. … le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all'articolo 3:*

*a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;*
*b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;*
*c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 3;*
*d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.*

# Regolamento Tecnico

I. Regole di base

RSA, DSS, chiave ≥1024 bit, SHA-1, RIPEMD-160

II. Regole per la certificazione delle chiavi

III. Regole per la validazione temporale e per la protezione dei documenti informatici

IV. Regole tecniche per le Pubbliche Amministrazioni

V. Disposizioni finali

## Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche

### Art. 2 – Definizioni

*1) "firma elettronica", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione;*

*2) "firma elettronica avanzata", una firma elettronica che soddisfi i seguenti requisiti:*

*a) essere connessa in maniera unica al firmatario;*

*b) essere idonea ad identificare il firmatario;*

*c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;*

*d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.*

# Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche G.U. n. 39 del 15 febbraio 2002

## Art. 2

*a) "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;*

*d) "certificati elettronici" gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;*

*e) "certificati qualificati" i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva;*

*g) "firma elettronica avanzata" la firma elettronica ottenuta attraverso un 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;*

# Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche G.U. n. 39 del 15 febbraio 2002

## Art. 6

...

*3. 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 una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.*

# Problemi con PKI

- Public (Key Infrastructure) o (Public Key) Infrastructure?
  - Privato: OK; Pubblico???
  - SWIFT è privato
- Il Naming è hard
- CRL assume accesso continuo
  - diverso dalle hot cards
- Gli utenti devono essere educati
- I certificati legano nome a DNS, ma la CA non controlla il DNS

# Problemi con PKI

- Vi sono barriere all'ingresso per le CA
  - Necessario inserire il proprio root certificate nei browser
- Chi realizza la transazione può essere diverso dal titolare del certificato
- L'utente si può fidare del proprio sistema?
- Liability??

# Bibliografia

- Cryptography and Network Security
  by W. Stallings (2003)
  - cap. 10 (Key Management)
  - cap. 14 (X.509 Authentication Service)
- Tesina di Sicurezza su reti
  - PKI