

Certificati e Public-key Infrastructure

Corso di Sicurezza
a.a. 2019-20



Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

<http://www.di-srv.unisa.it/~ads>

Marzo 2020

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

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

Vediamo alcune tecniche



Distribuzione chiavi pubbliche

Alcune tecniche:

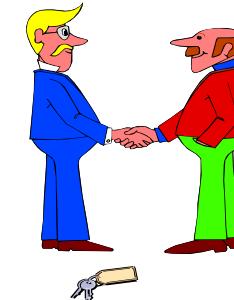
- Annuncio pubblico
- Directory pubblica
- Autorità per le chiavi pubbliche
- Certificati per le chiavi pubbliche



Annuncio pubblico

Pubblicizzare la proprio chiave pubblica

- Scambio diretto con la controparte
- Sul sito web
- In allegato alle email
- Bacheca elettronica



Problema

- Possiamo fidarci dell'annuncio?



Directory pubblica

Entità fidata:

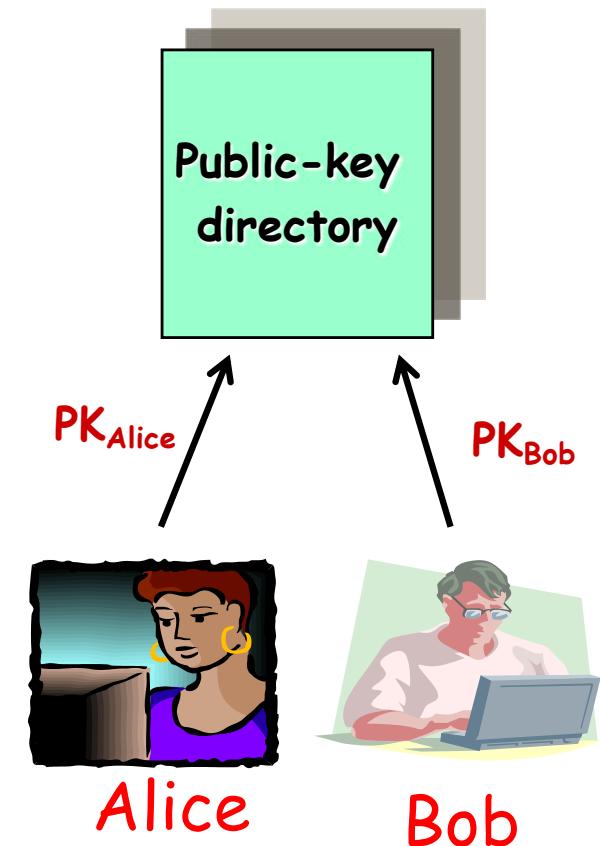
- Gestisce la directory di chiavi pubbliche

Ogni partecipante:

- Registra la propria chiave pubblica
 - Di persona o in modo autenticato
- Può aggiornare la propria chiave
 - Se usata da troppo tempo o compromessa

Problemi:

- Possiamo fidarci?
 - Valore di chiave di firma digitale
- Se viene violata l'entità fidata...



Autorità per le chiavi pubbliche

- Gestisce directory di 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

Autorità per le chiavi pubbliche

- Gestisce directory di 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



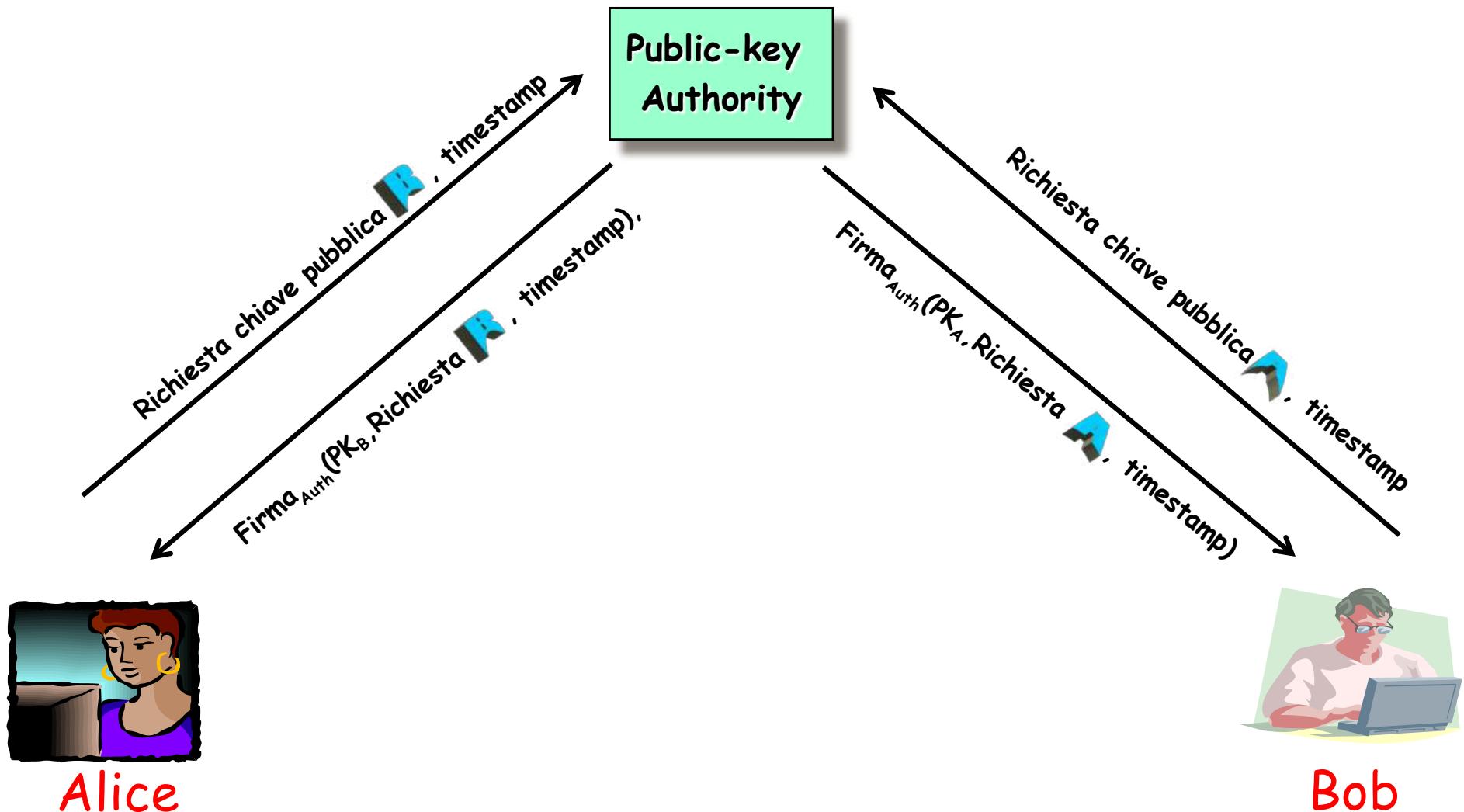
Alice

Voglio la chiave pubblica di Alice

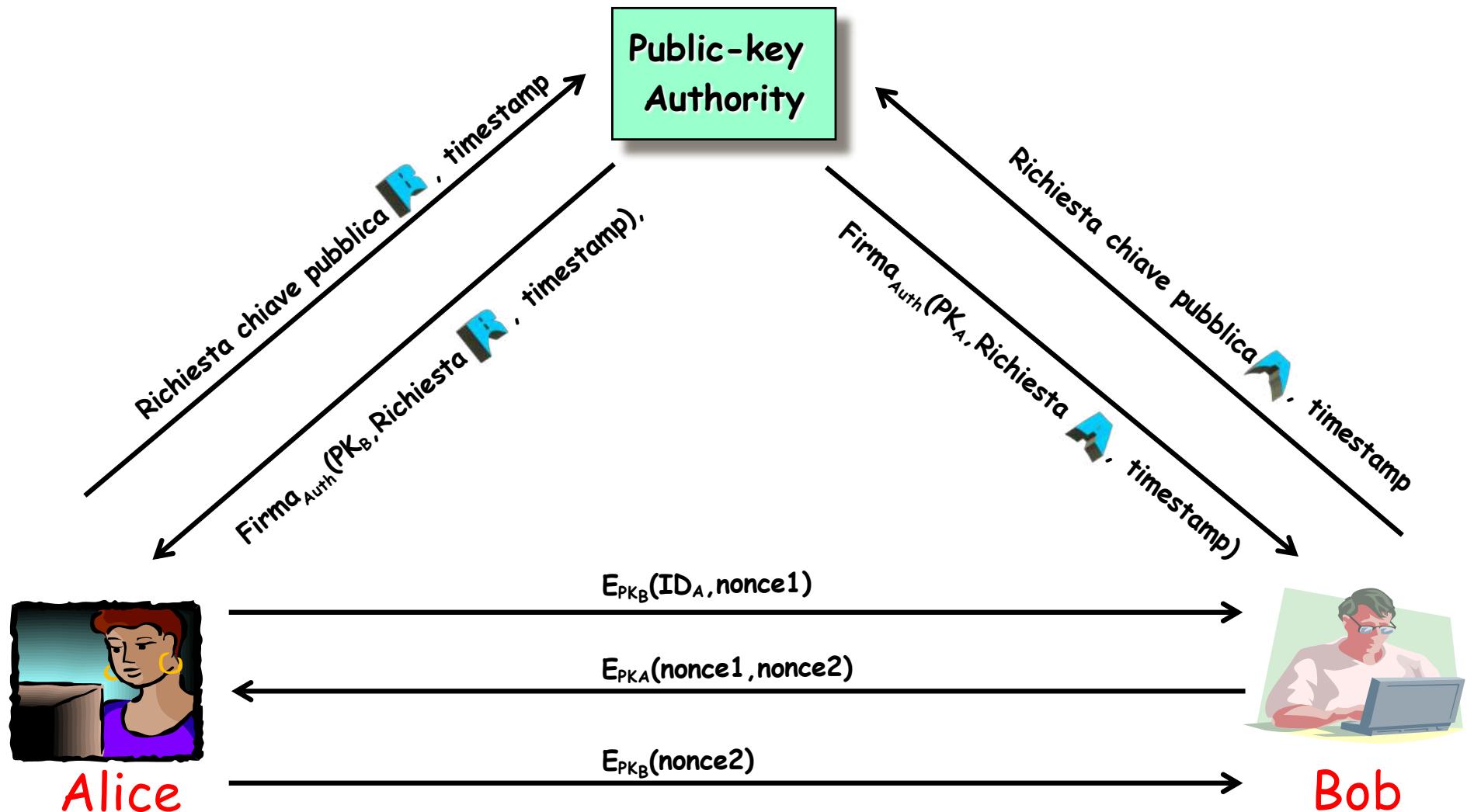


Bob

Autorità per le chiavi pubbliche



Autorità per le chiavi pubbliche



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:

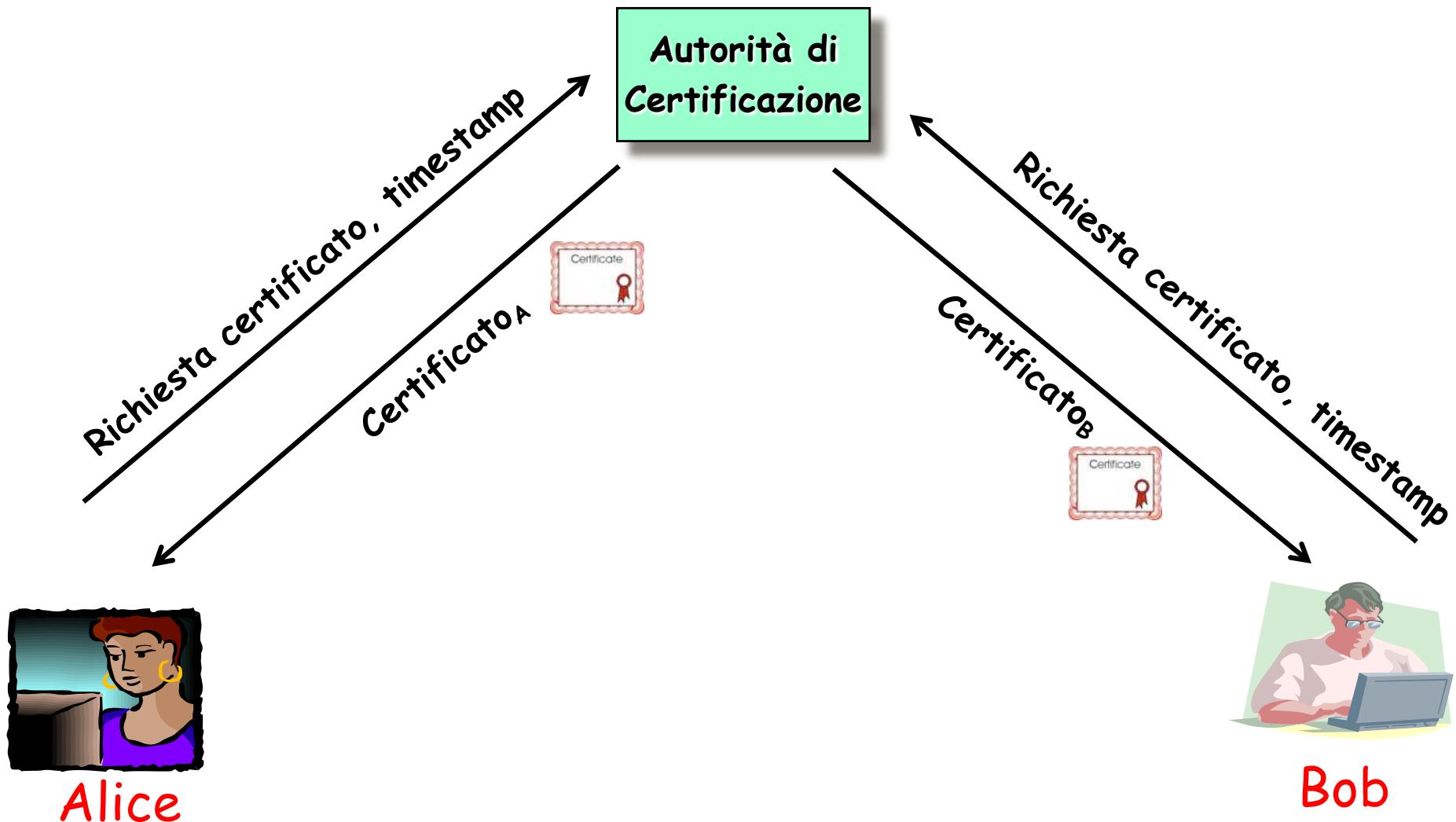
- Ognuno può leggerli e determinare nome e chiave pubblica
- Ognuno può verificarli ed assicurarsi dell'autenticità
- Solo l'Autorità può crearli ed aggiornarli

Certificati

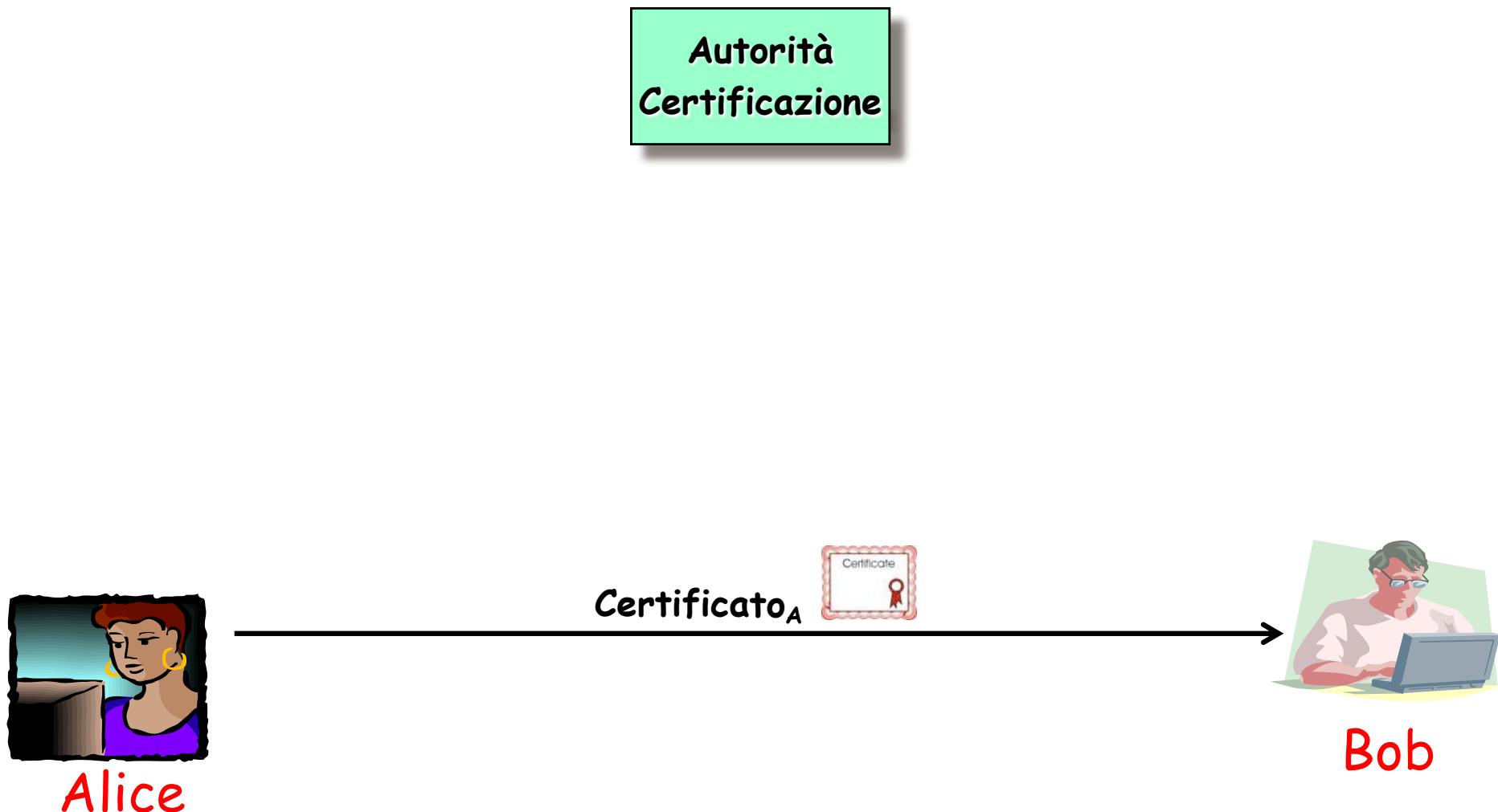
- Esempi di altri dati in un certificato:
 - periodo di validità chiave pubblica
 - numero seriale o identificatore chiave
 - info addizionali su chiave (ad es., algoritmi ed utilizzo)
 - info addizionali su utente
 - stato della chiave pubblica
- Formato più diffuso: definito dallo standard internazionale **ITU-T X.509**



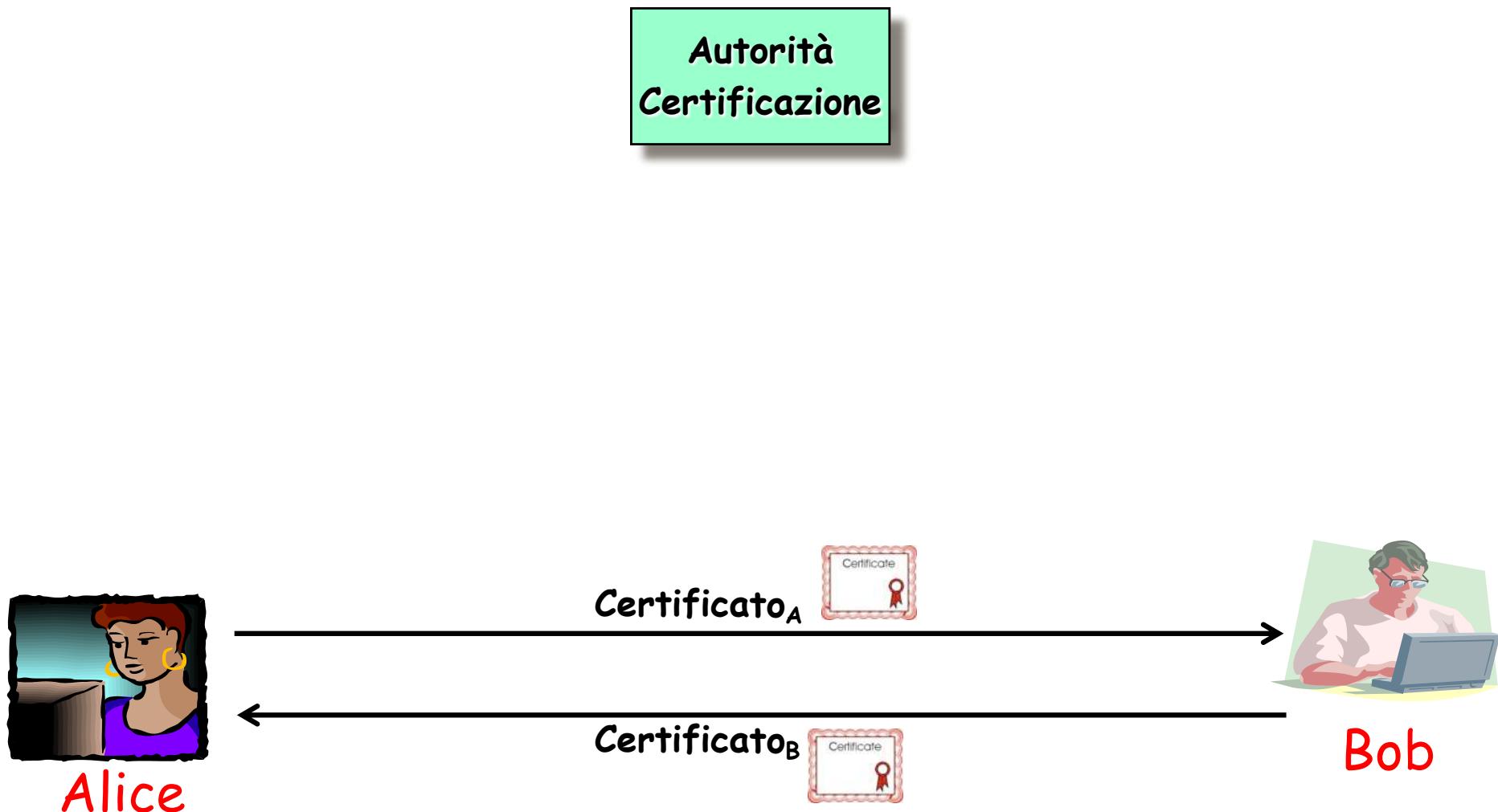
Richiesta Certificati



Scambio Certificati



Scambio Certificati



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 (ad 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
 - (ad 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

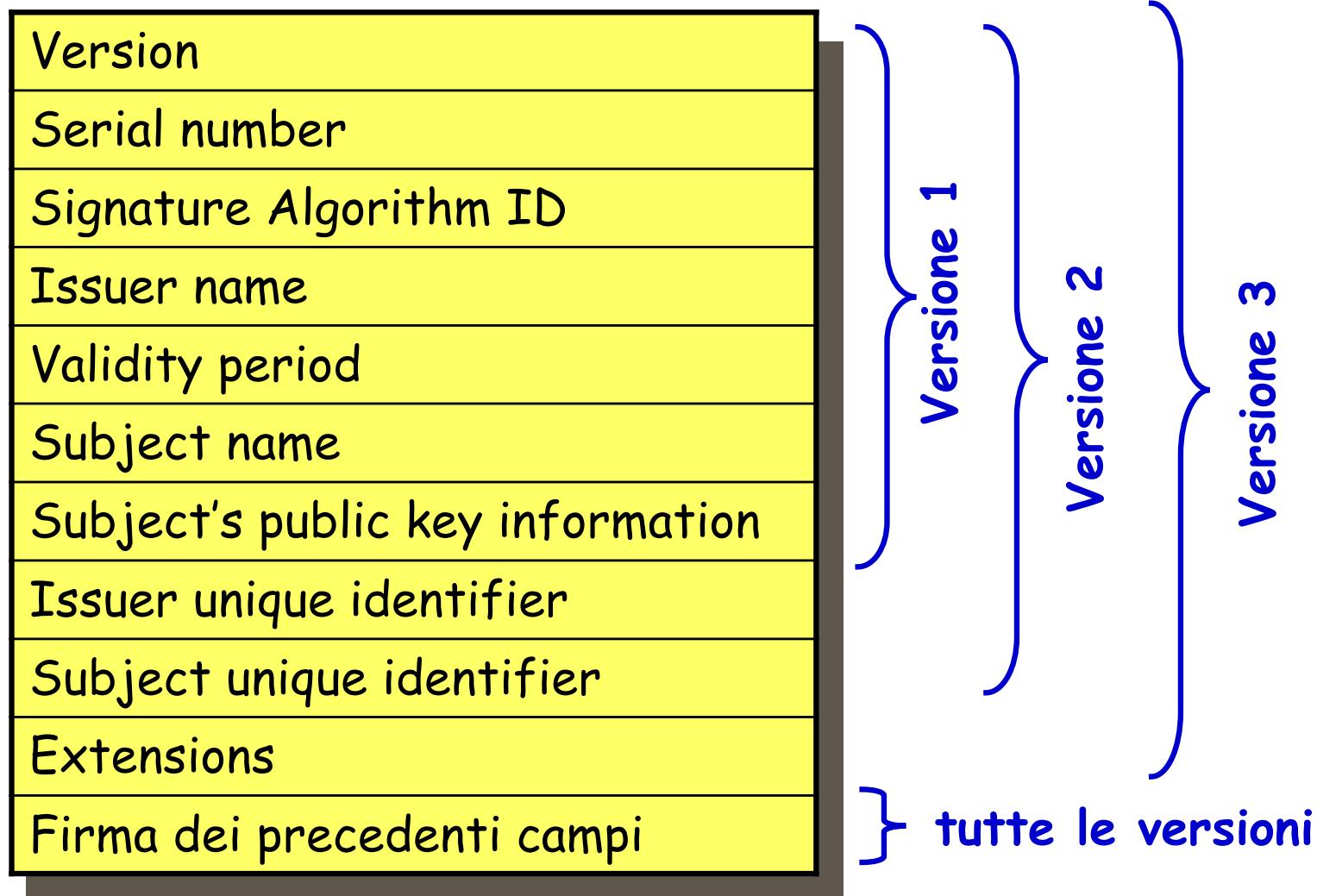
Certificate Revocation List (CRL)

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

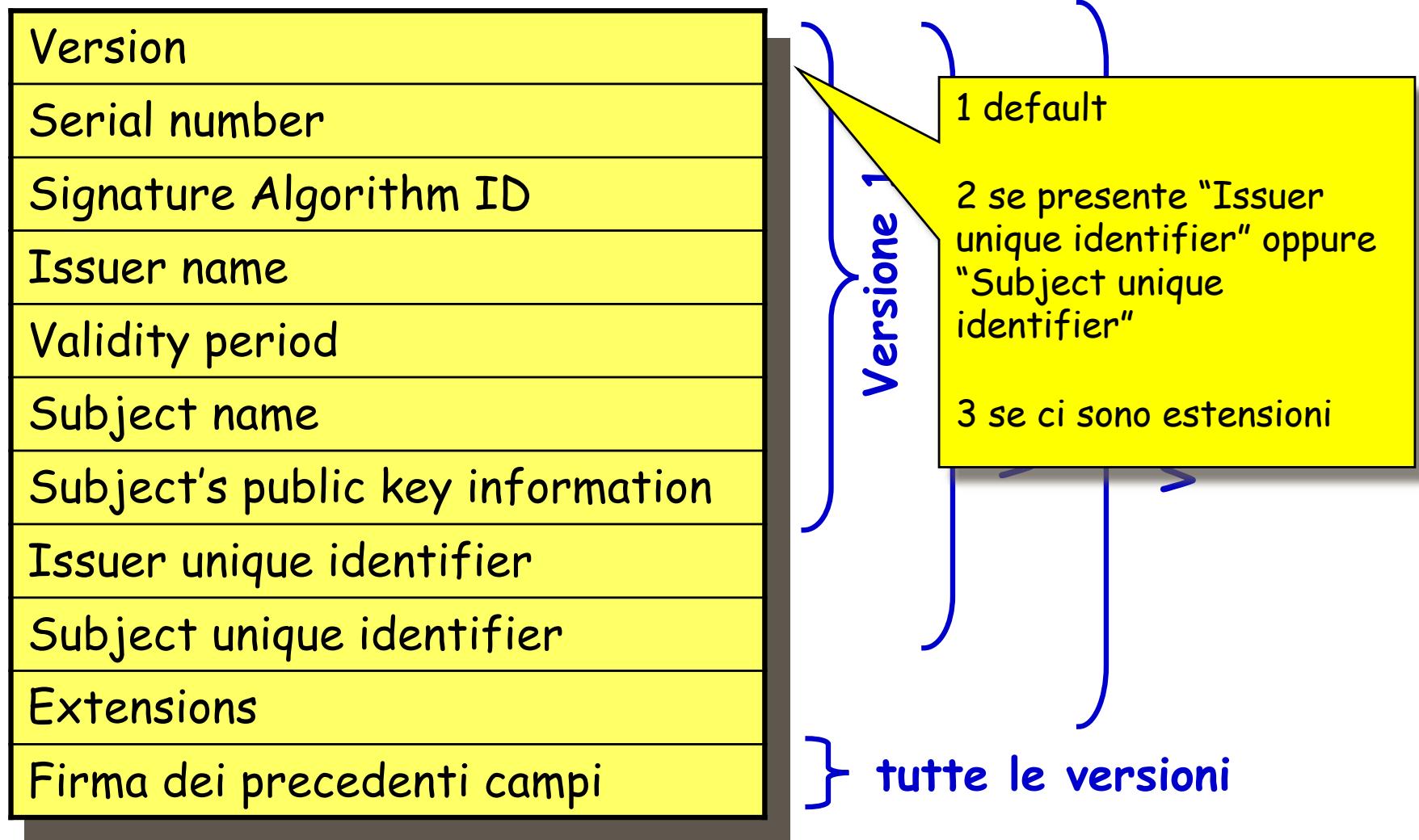
Standard dei certificati X.509

- 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, ...

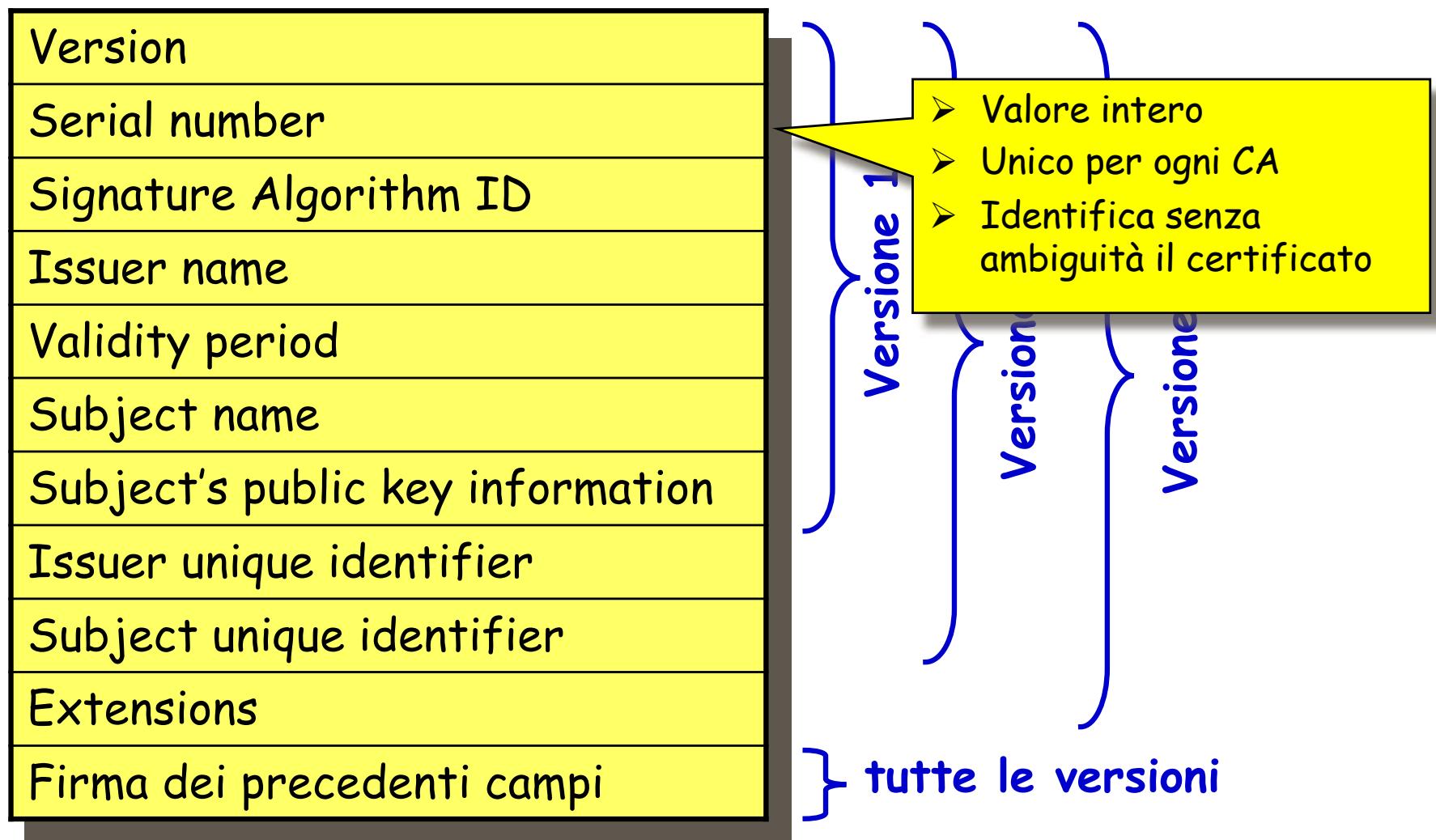
Campi Certificati X.509



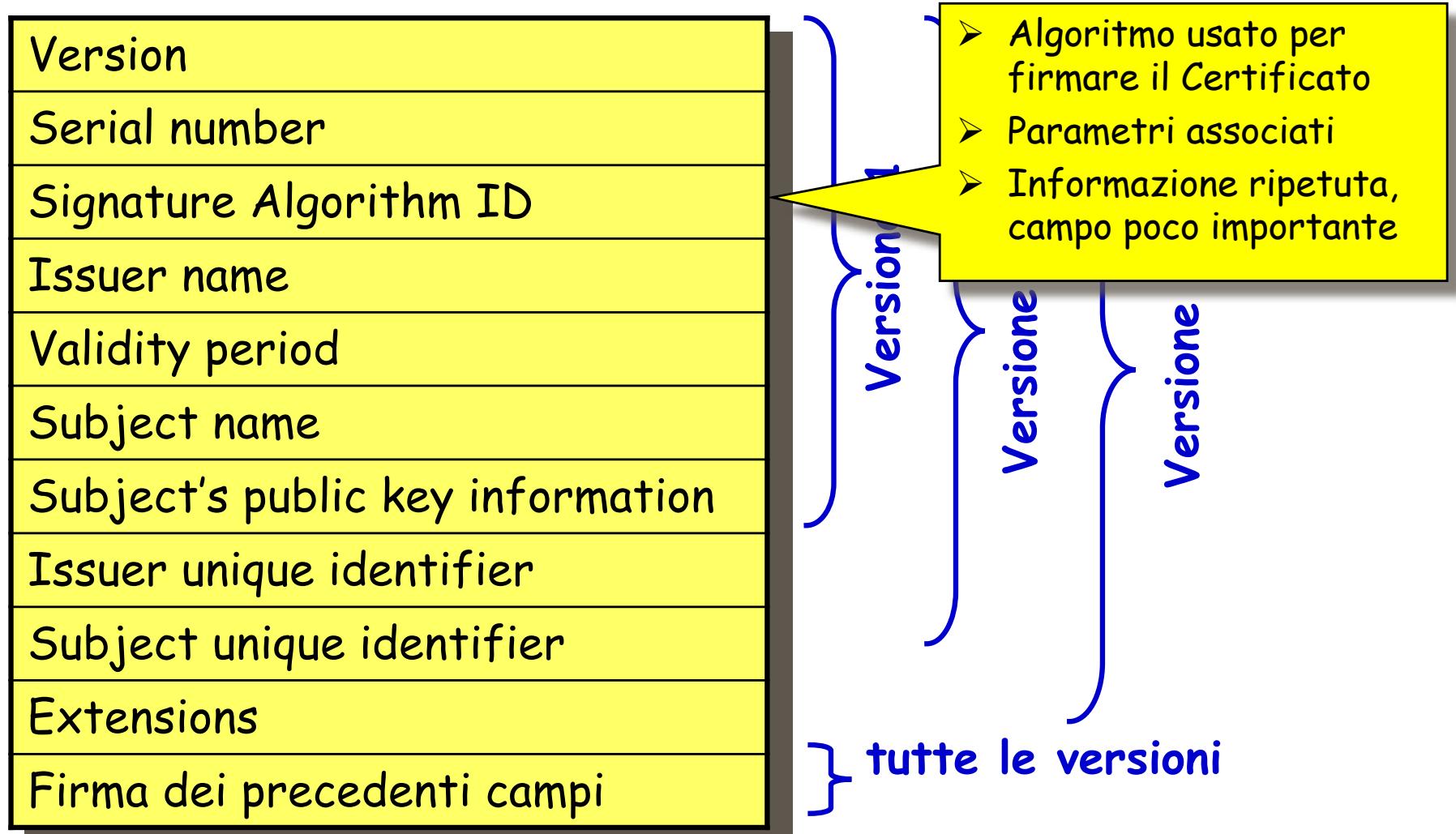
Campi Certificati X.509



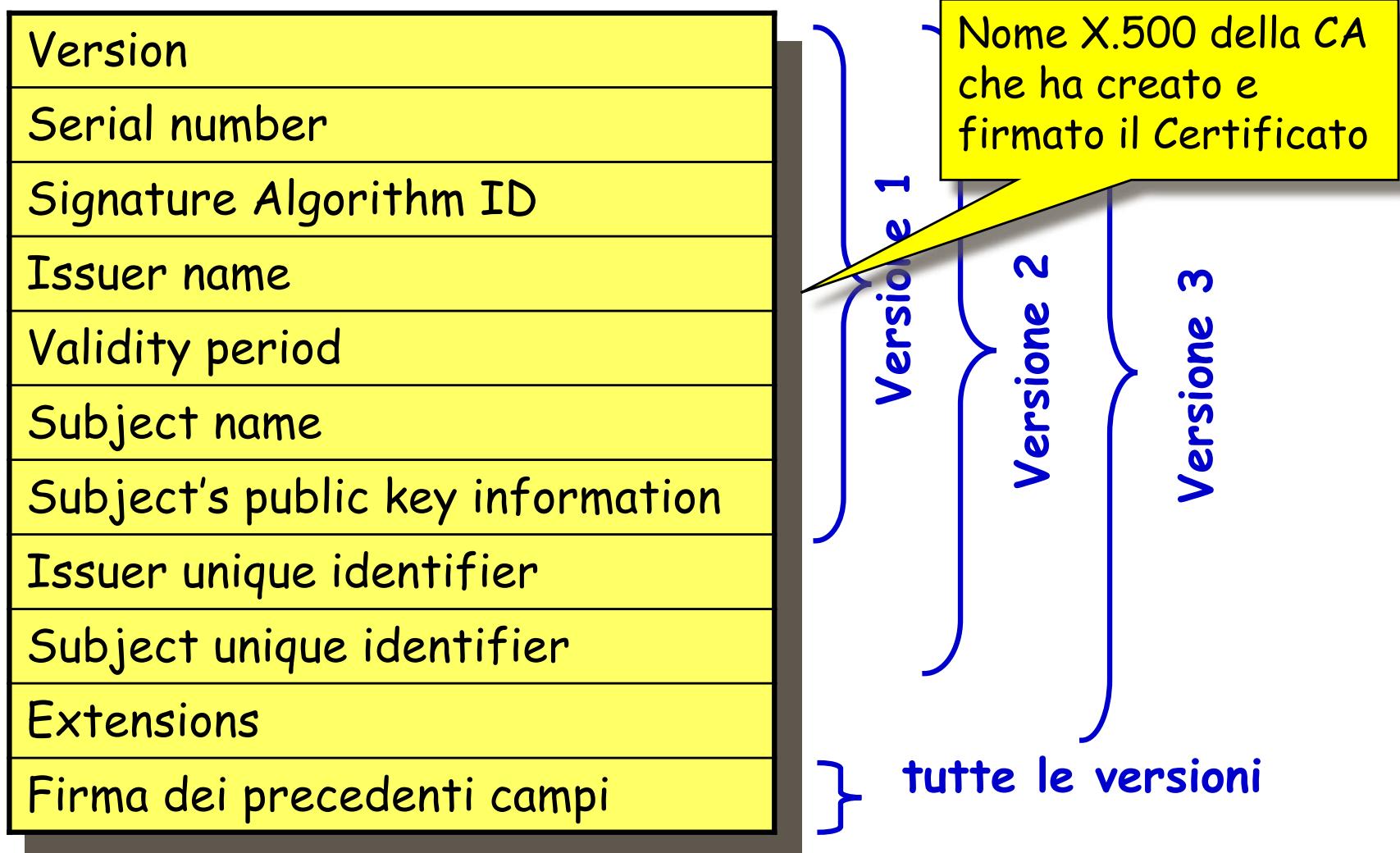
Campi Certificati X.509



Campi Certificati X.509



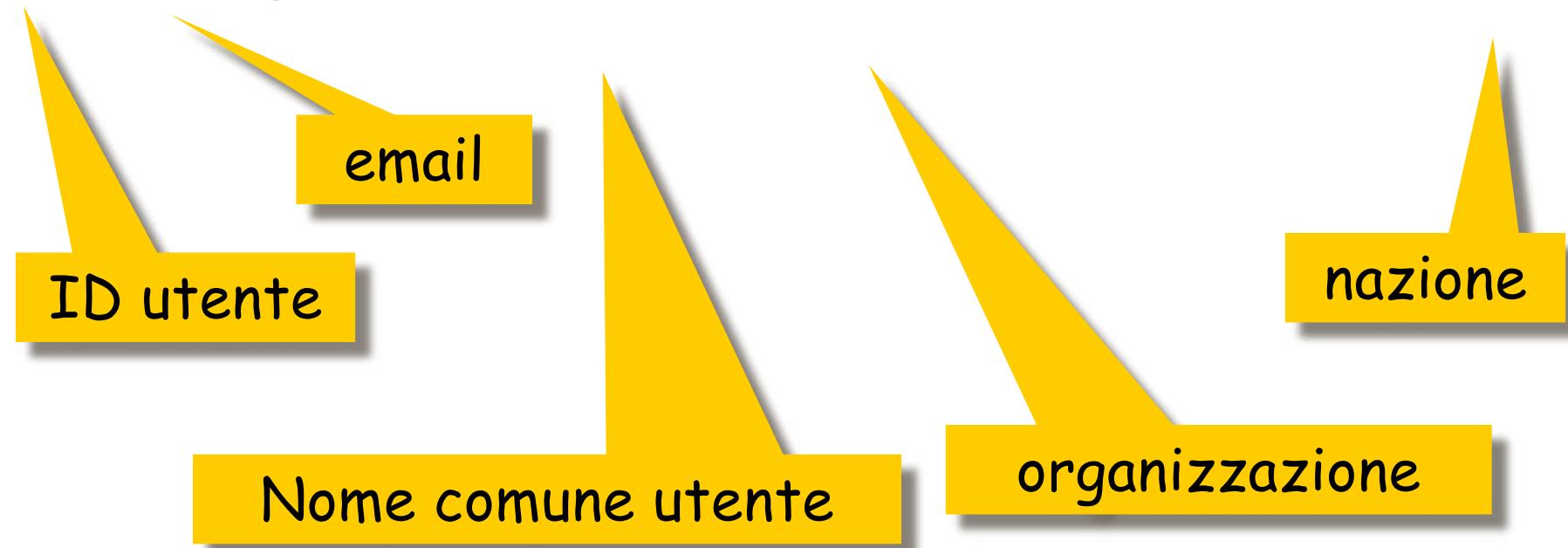
Campi Certificati X.509



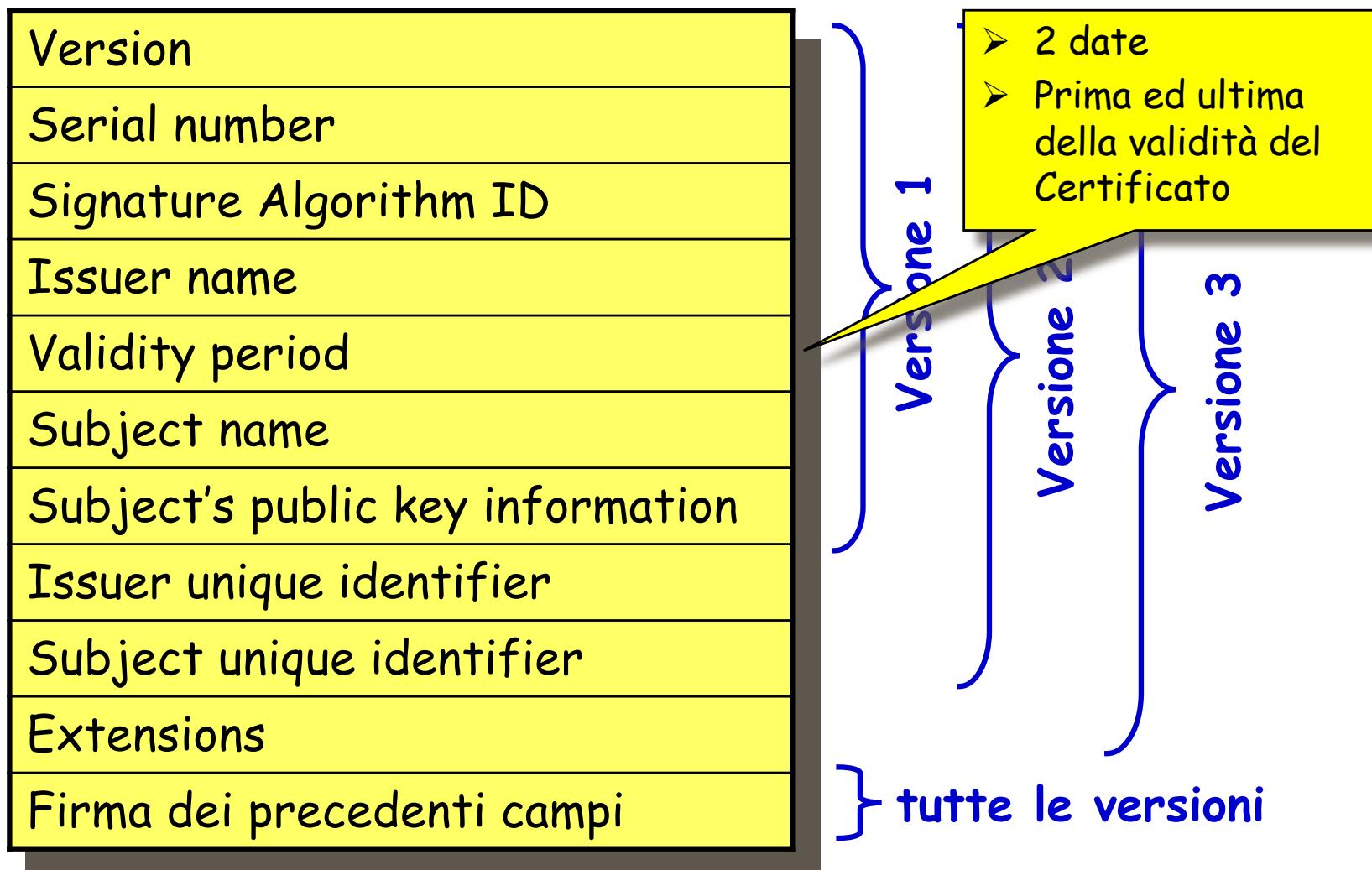
Nome X.500

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

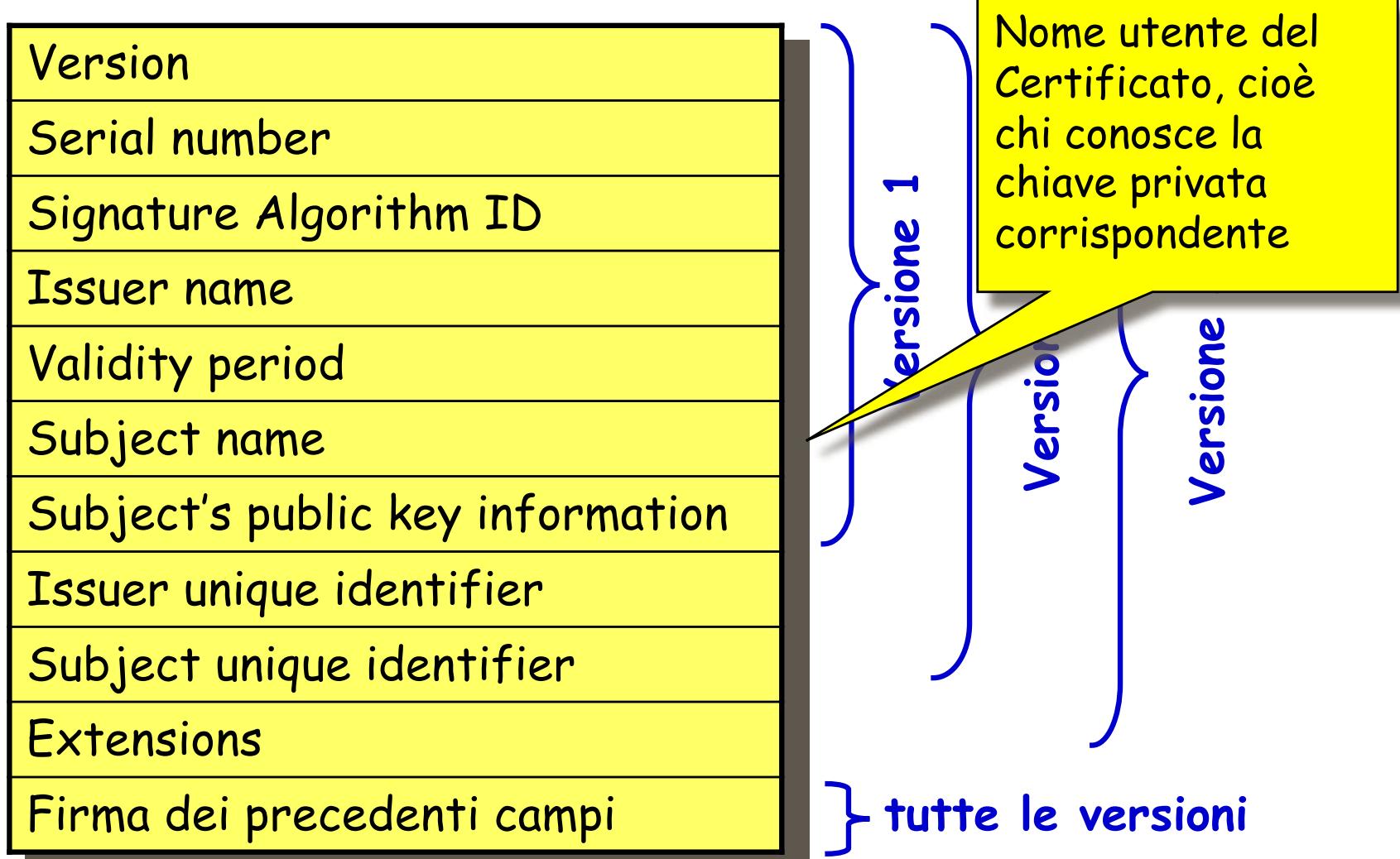
uid=doe,e=doe@netscape.com,cn=John Doe,o=Netscape Communications Corp.,c=US



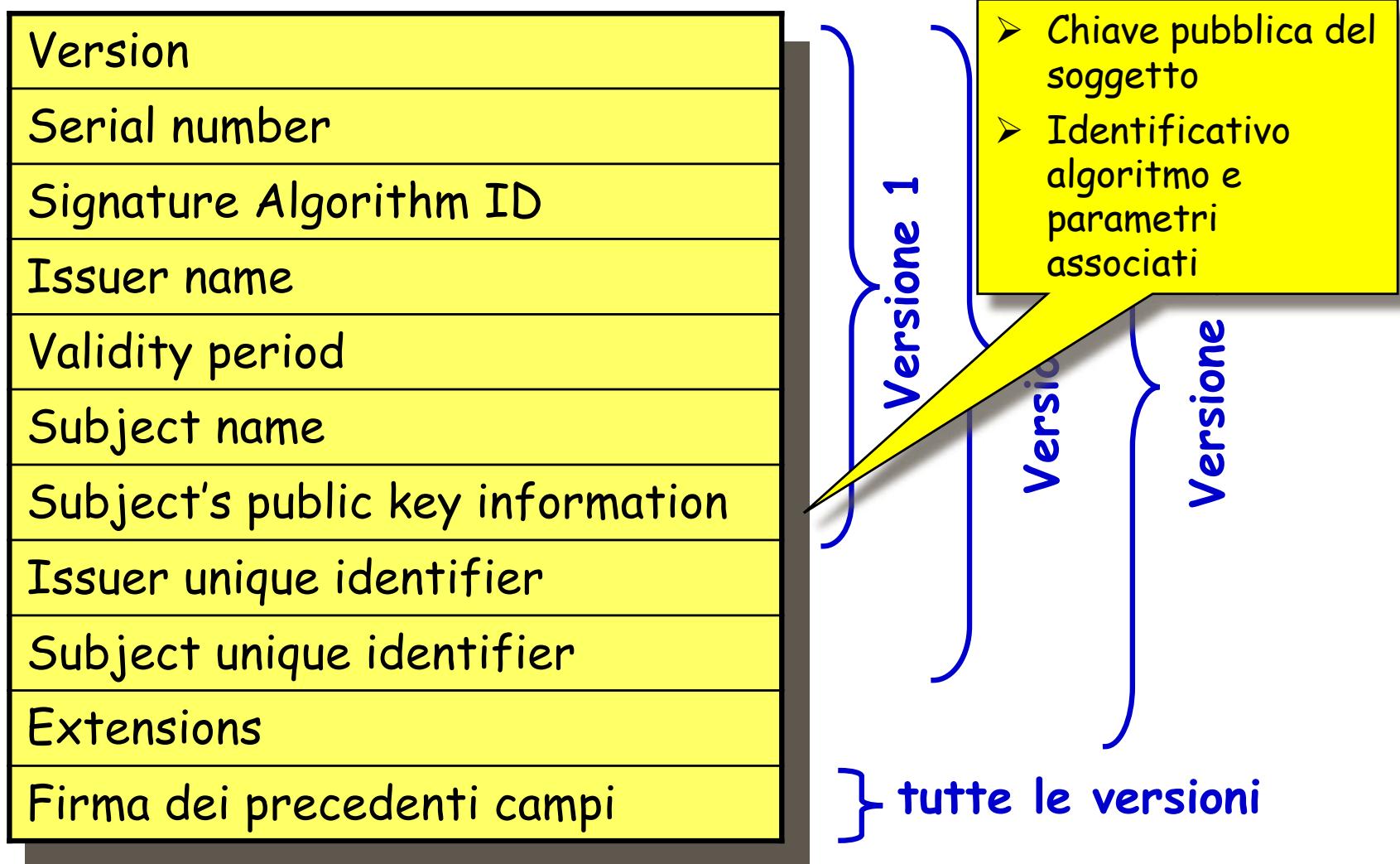
Campi Certificati X.509



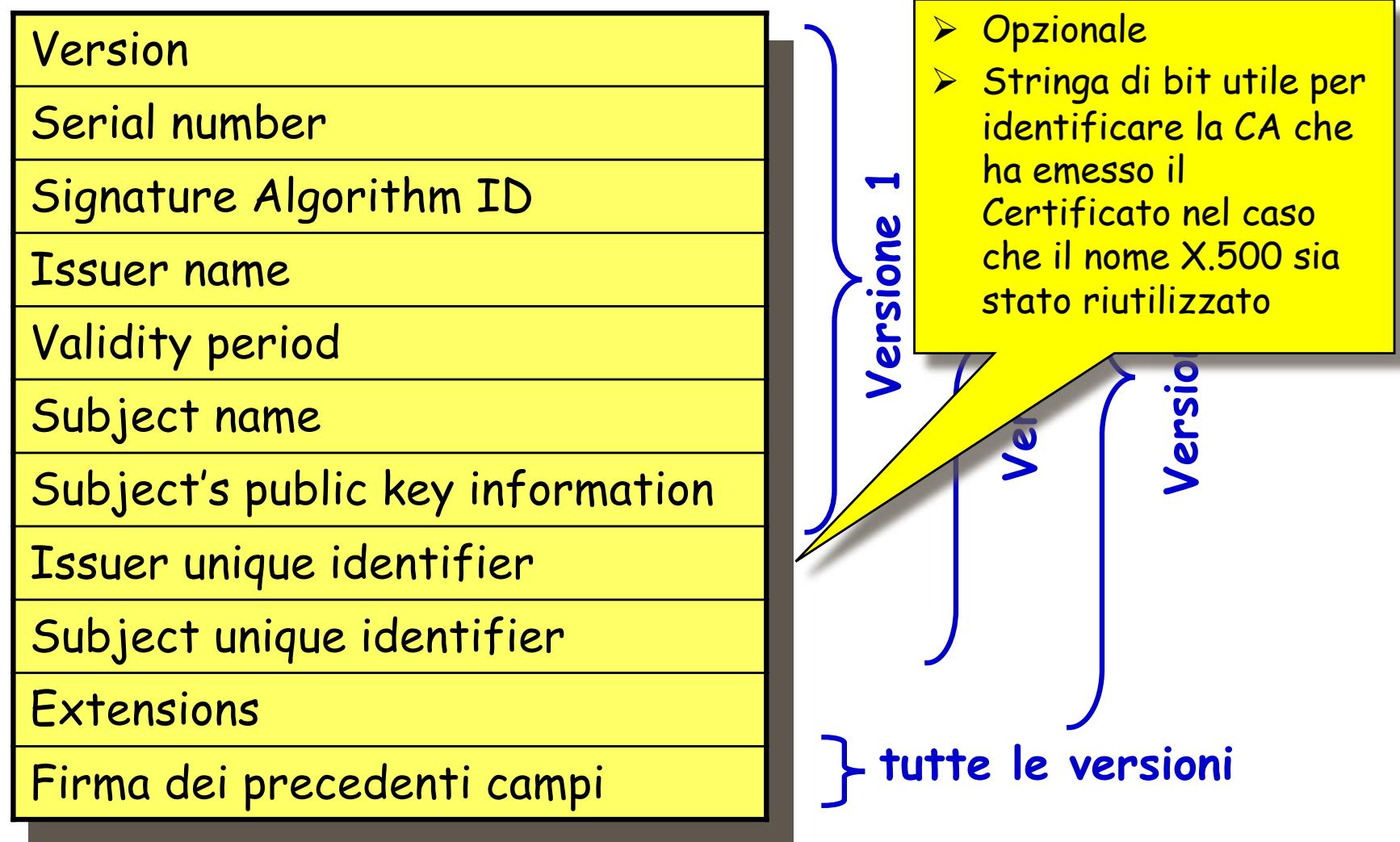
Campi Certificati X.509



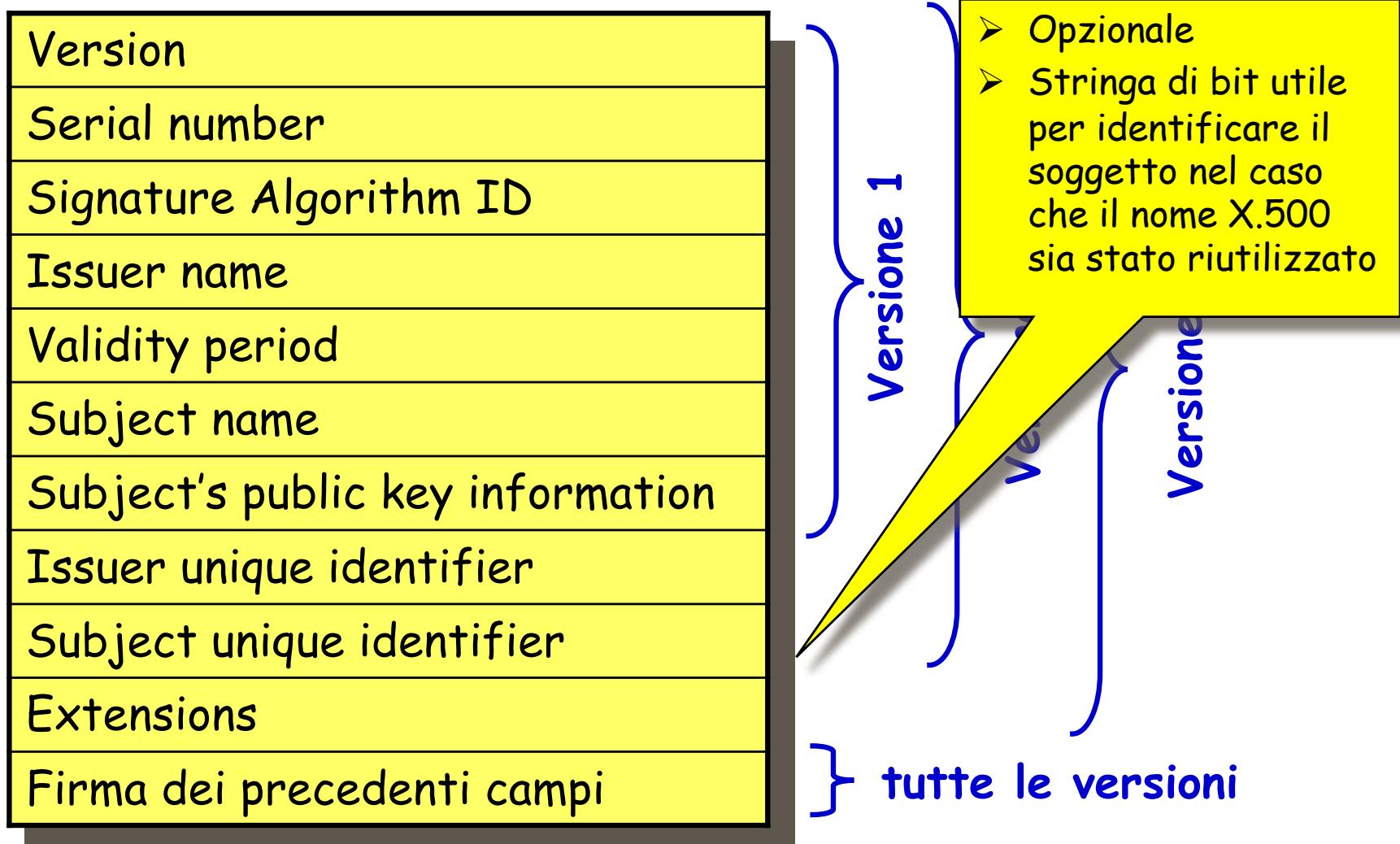
Campi Certificati X.509



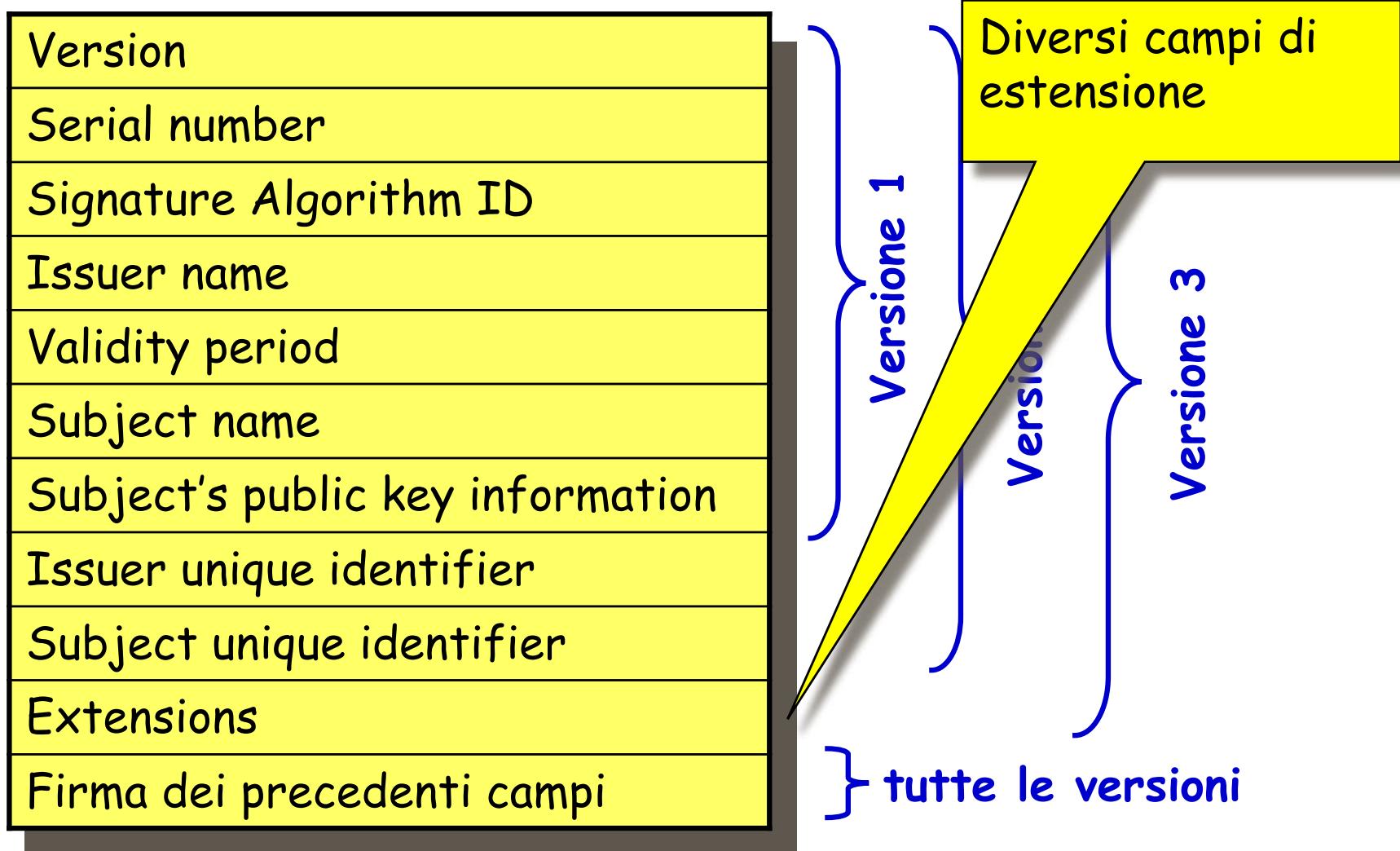
Campi Certificati X.509



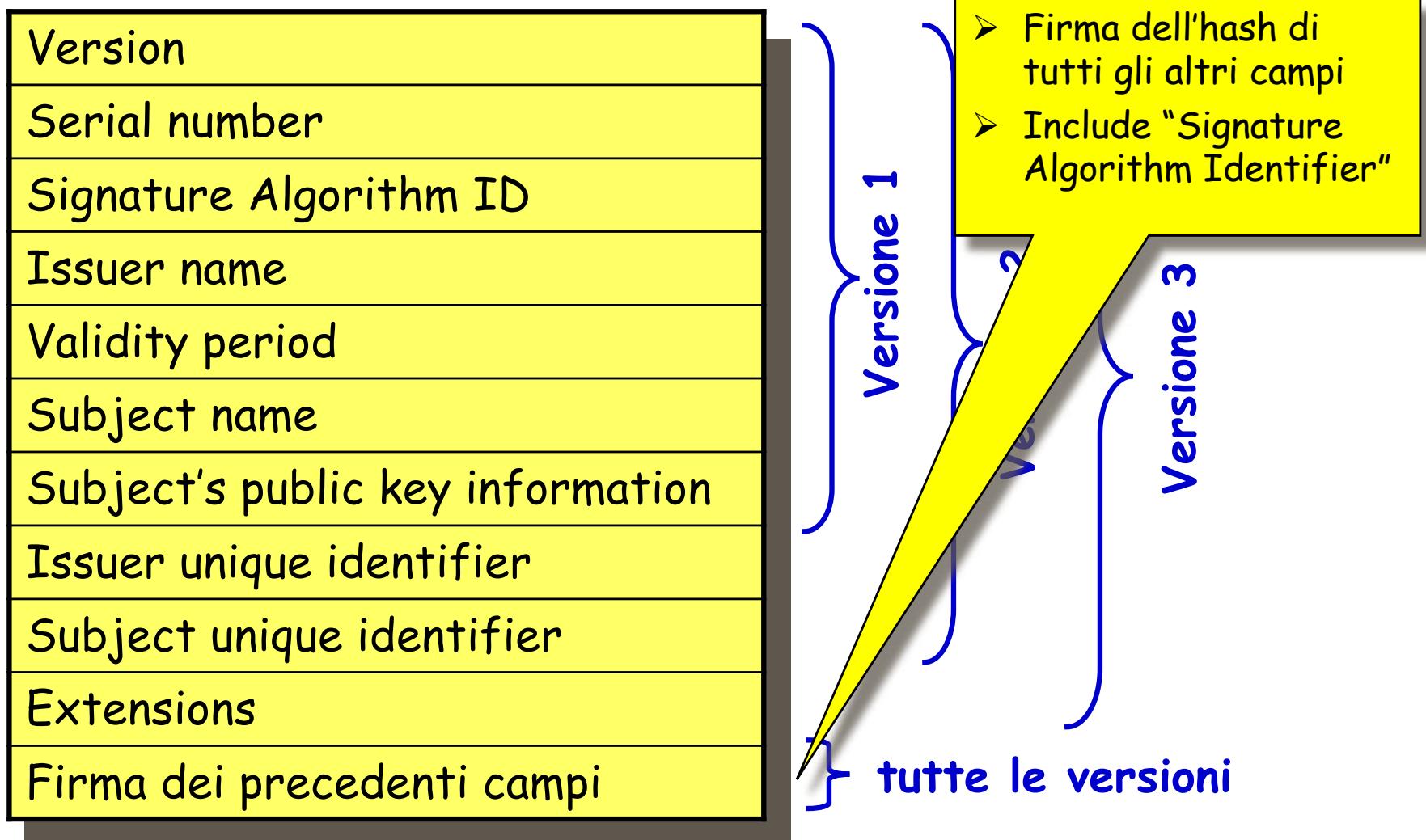
Campi Certificati X.509



Campi Certificati X.509



Campi Certificati X.509



Certificate:

Data:

Version: v3 (0x2)

Serial Number: 3 (0x3)

Signature Algorithm: PKCS #1 MD5 With RSA Encryption

Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US

Validity:

Not Before: Fri Oct 17 18:36:25 1997

Not After: Sun Oct 17 18:36:25 1999

Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US

Subject Public Key Info:

Algorithm: PKCS #1 RSA Encryption

Public Key:

Modulus:

00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
91:f4:15

Public Exponent: 65537 (0x10001)

Extensions:

Identifier: Certificate Type

Critical: no

Certified Usage:

SSL Client

Identifier: Authority Key Identifier

Critical: no

Key Identifier:

f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36: 26:c9

Signature:

Algorithm: PKCS #1 MD5 With RSA Encryption

Signature:

6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:dd:c4

Estensioni per i file contenenti certificati X.509

- **.CER .DER** - certificato codificato con DER
- **.PEM** - certificato codificato con Base64
- **.P7B .P7C** - struttura SignedData PKCS#7 senza dati, solo il/i certificato/i o la/le CRL (Certificate revocation list)
- **.PFX .P12** - PKCS#12, può contenere certificati e chiavi pubbliche e private (protette da password)

Certificato codificato con DER

- Distinguished Encoding Rules
 - Regola di codifica ASN.1 definita in ITU-T X.690, 2002
 - File binari, non si possono vedere con text editor

Certificato codificato in Base64

-----BEGIN CERTIFICATE-----

MIICKzCCAQSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJVUzER
MA8GA1UEChMITmV0c2NhcGUxFATBqNVBAsTDFN1cHJpeWEncyBDQTAeFw05NzEw
MTgwMTM2MjVaFw05OTEwMTgwMTM2MjVaMEgxCzAJBgNVBAYTAIVTMREwDwYDVQQK
EwhOZXRzY2FwZTENMAAsGA1UECxMEUHViczEXMBUGA1UEAxMOU3Vwcml5YSBTaGV0
dHkgZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRJgEjmKiG
7SdATYazBcABu1AVyd7chRkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7L
iQZBcrXpc0k4du+2Q6xJu2MPm/8WKuMOnTuvzpo+SGXelmHVChEqooCwfdiZwywZ
NMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCGSAGG+EIBAQQEAvIAaDAfBgNV
HSMEGDAWgBTy8gZZkBhHUfWJM1oxeuZc+zYm
I6/z07Z635DfzX4XbAFpjIRI/AYwQzTSYx8GfcNAqC
UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uv
hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpF

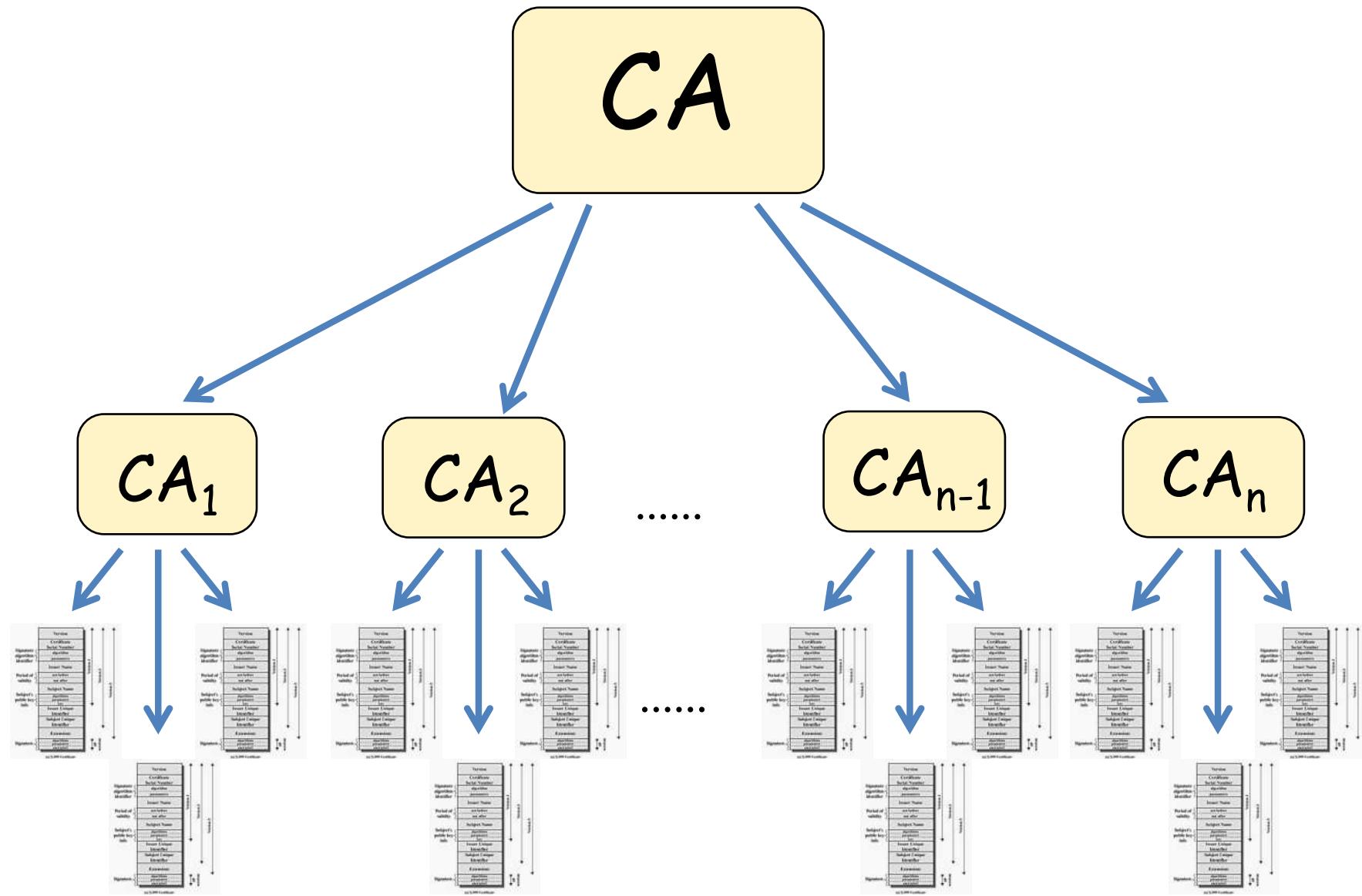
-----END CERTIFICATE-----

Binary	ASCII	Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/

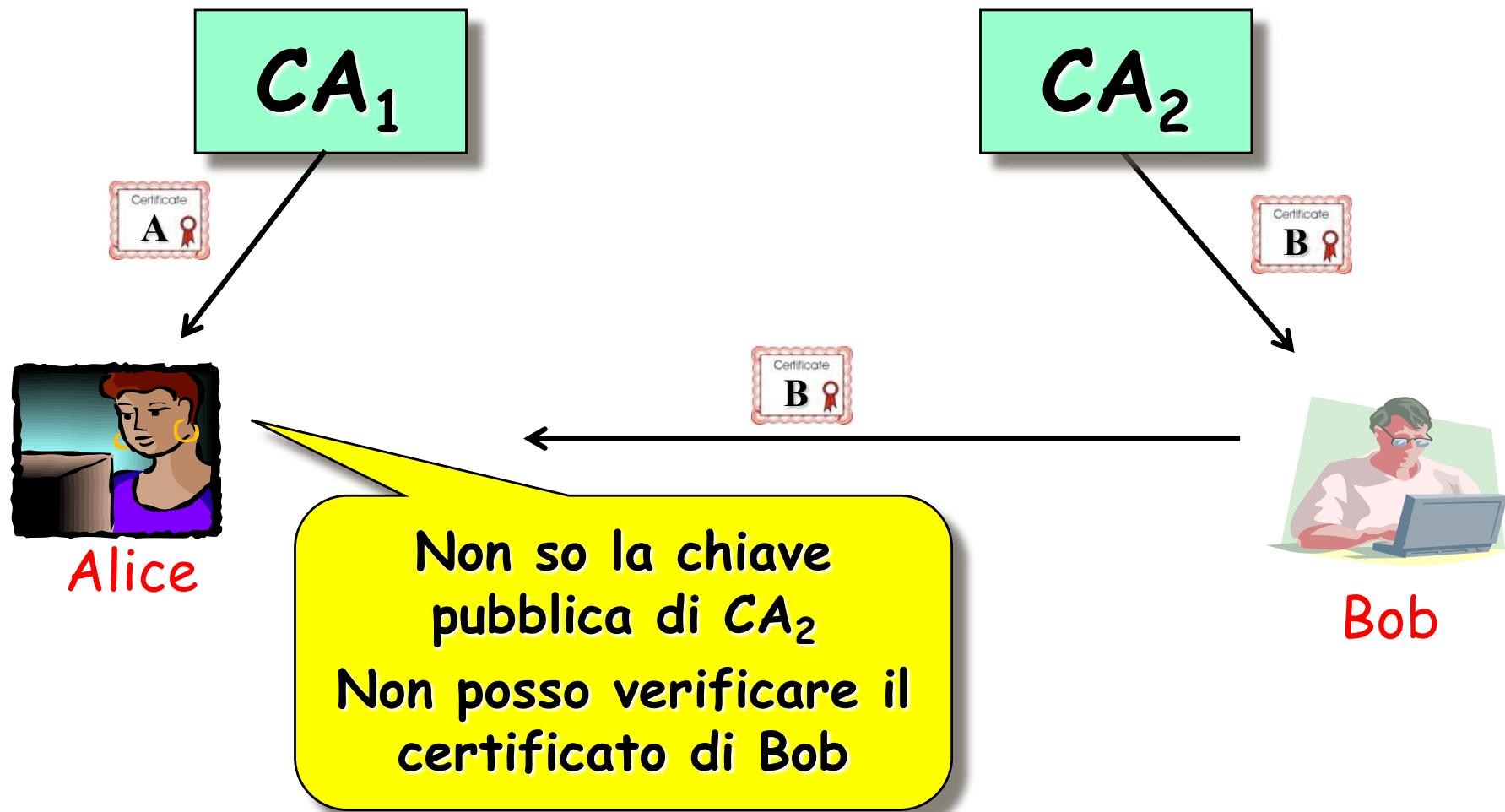
Public-Key Cryptography Standards (PKCS)

- PKCS #1: RSA Cryptography Specifications
- PKCS #2: ritirato
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #4: ritirato
- PKCS #5: Password-based Encryption Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Standard
- PKCS #11: Cryptographic Token Interface
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #14: Pseudo-random Number Generation
- PKCS #15: Cryptographic Token Information Format Standard

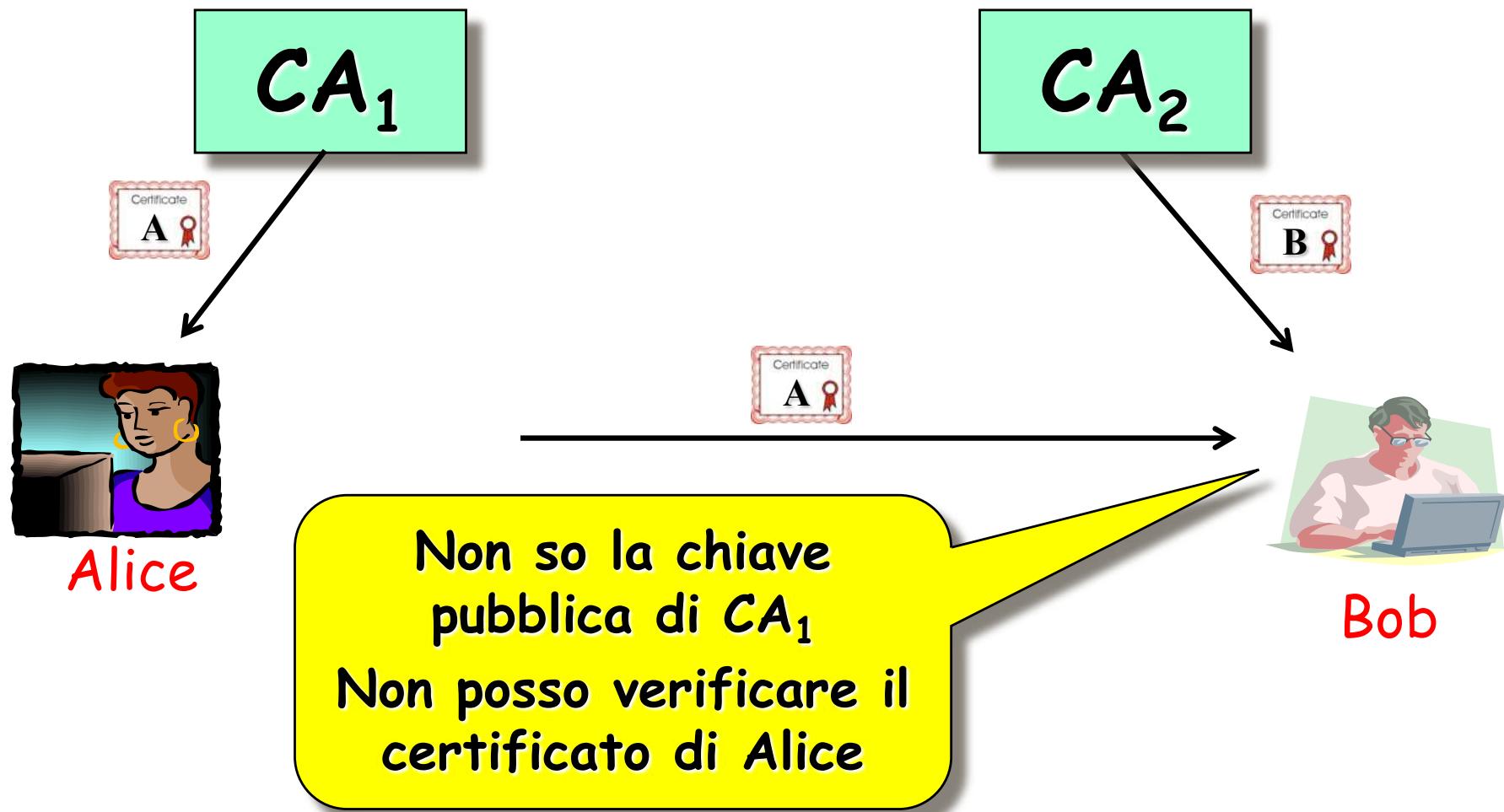
Gerarchia CA



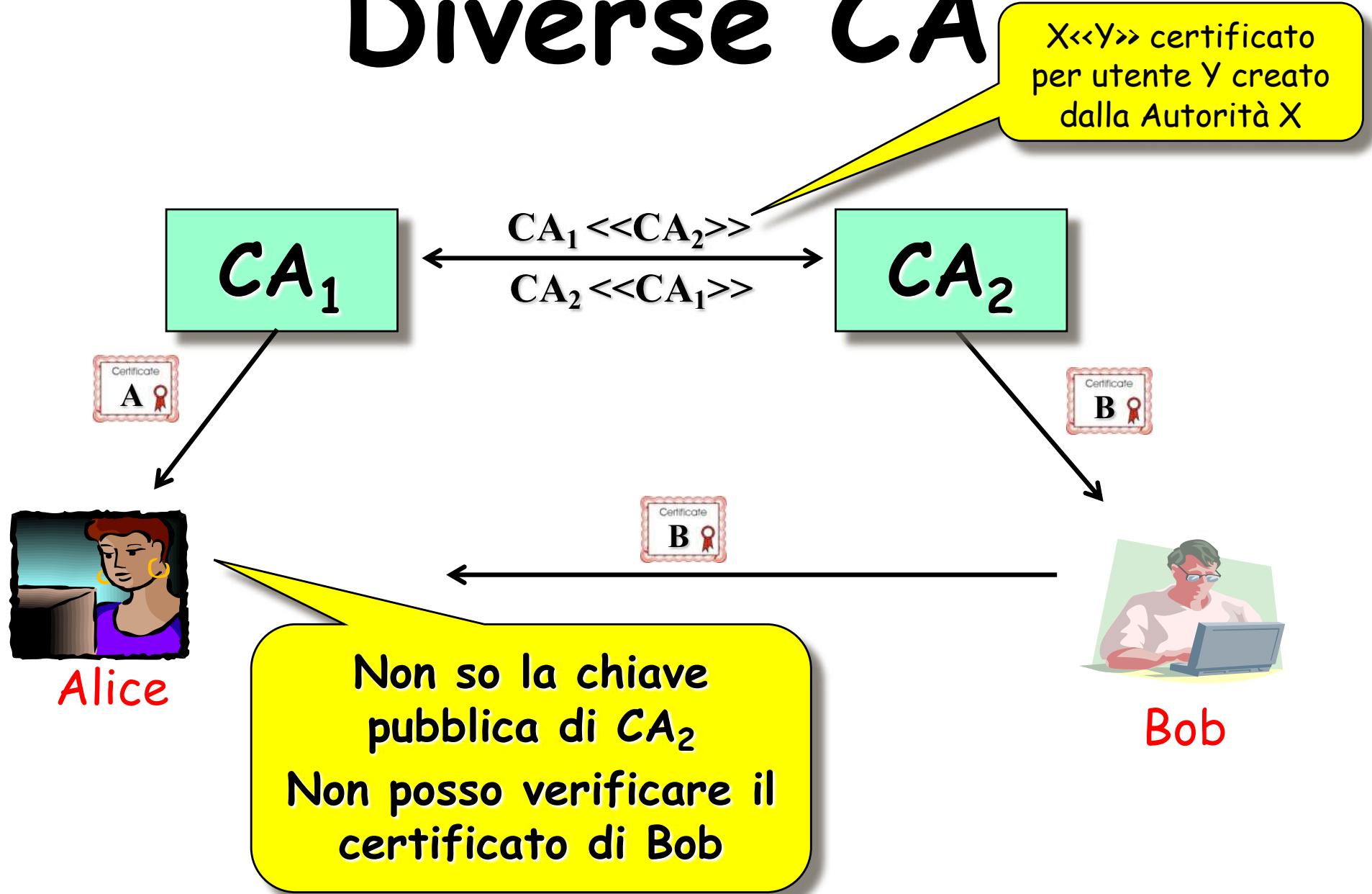
Diverse CA



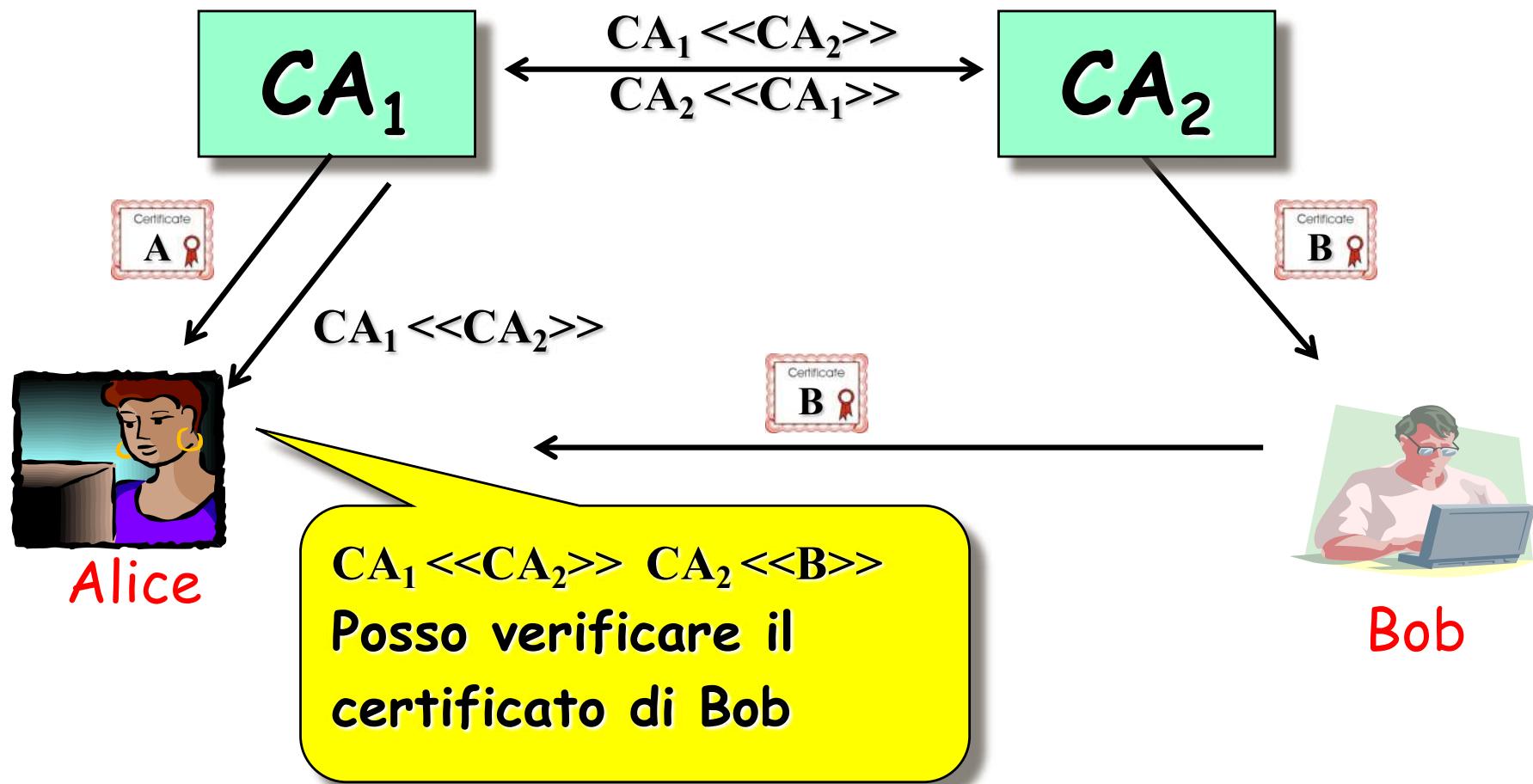
Diverse CA



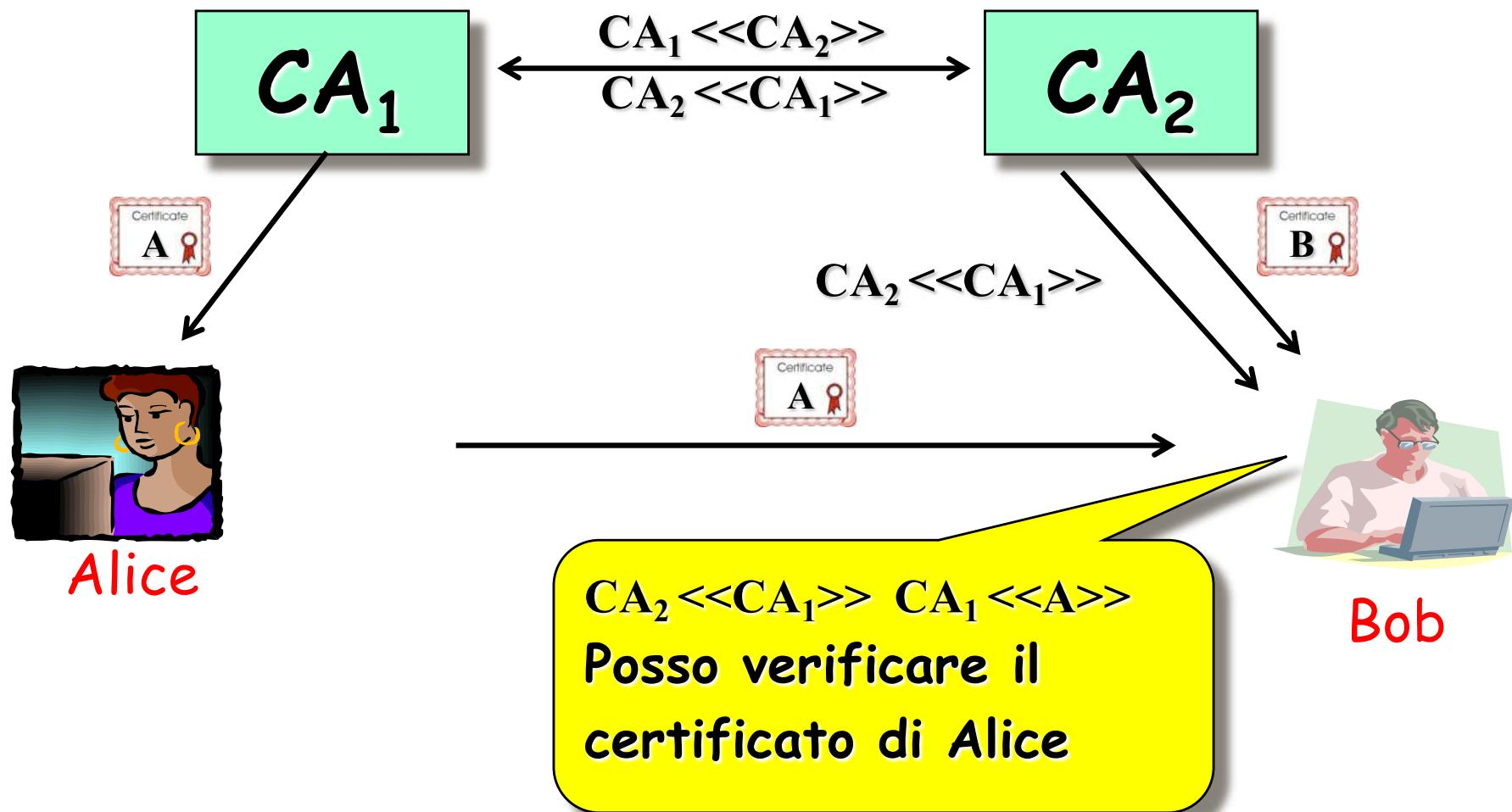
Diverse CA



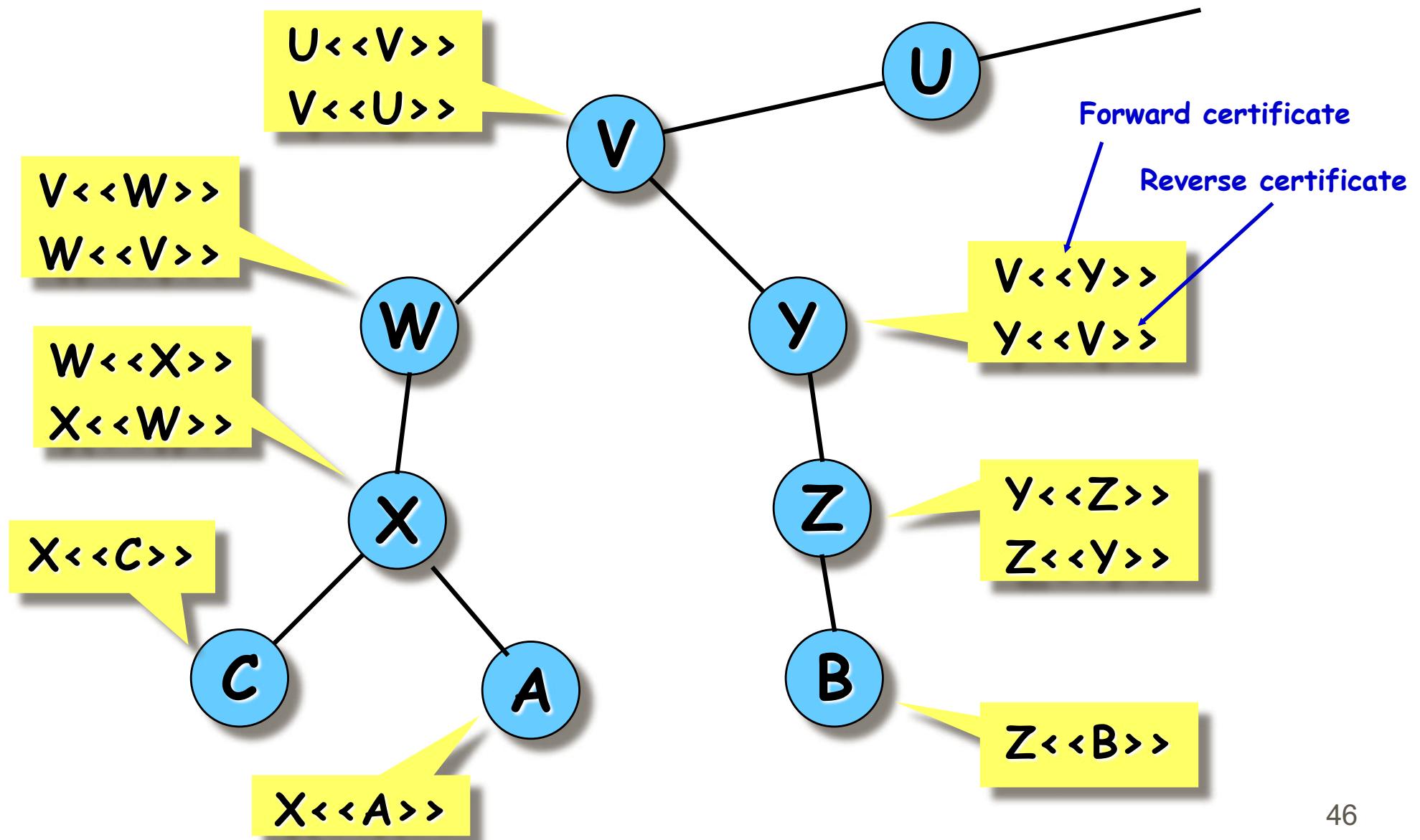
Diverse CA



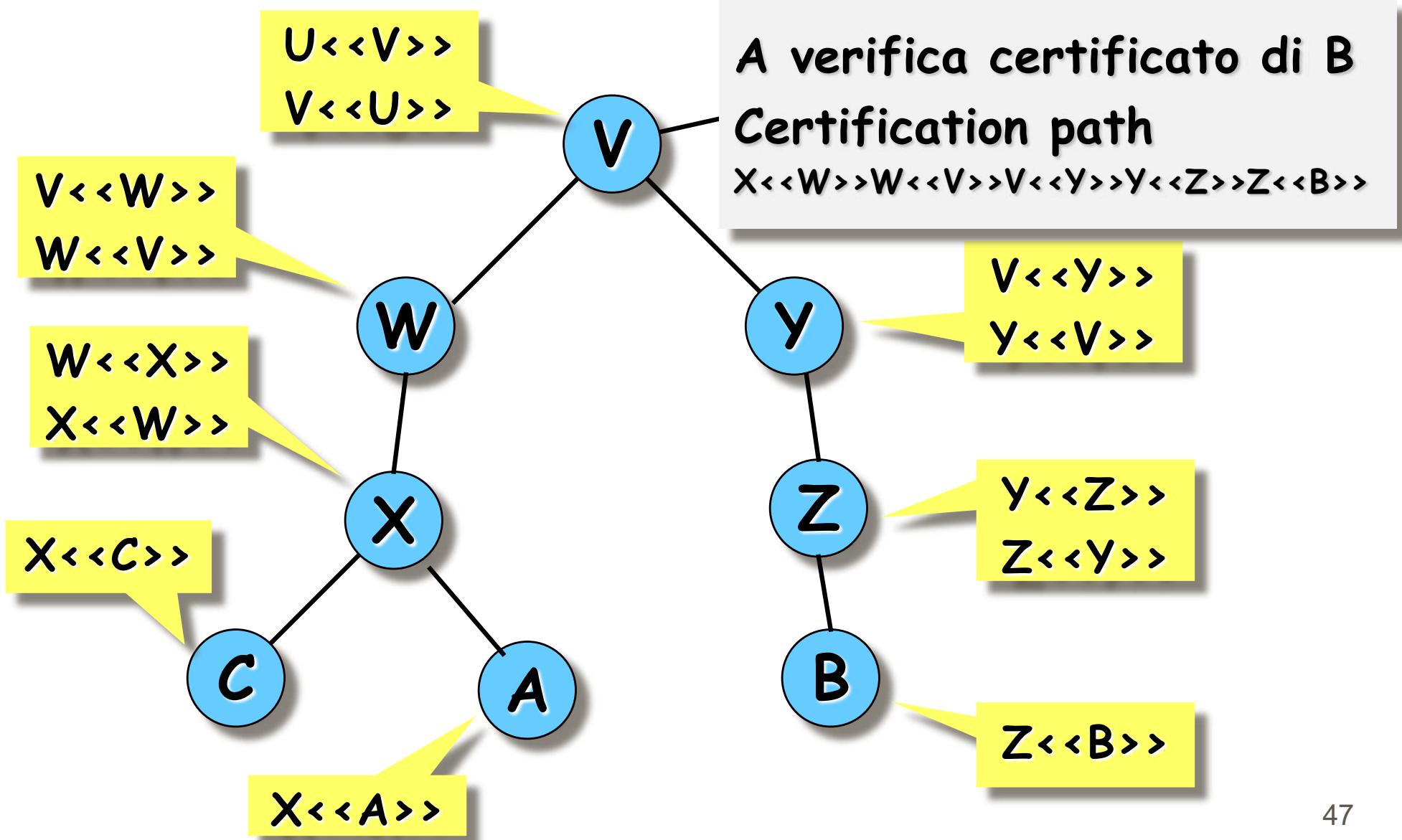
Diverse CA



Gerarchia X.509



Gerarchia X.509





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

Prestatori di servizi fiduciari attivi in Italia

Ragione sociale	Indirizzo della sede legale	Rappresentante legale	Man. oper. certificatore	Data iscrizione	Man. oper. sottoscritta AgID
Actualis S.p.A.	Via S. Clemente, 53 - 24036 Ponte San Pietro (BG), IT	Cecconi Giorgio	Link	28/03/2002	Manuali Operativi Data: 11/03/2019
Aruba Posta Elettronica Certificata S.p.A.	Via San Clemente n. 53 - 24036 Ponte San Pietro (BG)	Cecconi Giorgio	Link	06/12/2007	Manuali Operativi Data: 11/03/2019
Banca d'Italia	Via Nazionale, 91 - 00184 Roma, IT	il Governatore pro tempore	Link	23/01/2008	Manuali operativi
Cedacri S.p.A. (già Cedacrinord S.p.A.)	via del Conventino, 1 - 43044 Callecchia (PR), IT	Renato Dalla Riva, Presidente	Link	15/11/2001	Manuali operativi
Comando C4 Difesa - Stato Maggiore della Difesa	Via Stresa, 31/B - 00135 Roma, IT	Generale B. Calogero Massara, Comandante C4 Difesa	Link	20/09/2006	Manuali operativi
Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili	Piazza della Repubblica, 59 - 00185 Roma, IT	Il Presidente pro tempore	Link	10/07/2008	Manuali operativi
Consiglio Nazionale del Notariato	via Flaminia, 160 - 00196 Roma, IT	Il Presidente pro tempore	Link	12/09/2002	Manuali operativi
InTeSA S.p.A.	Strada Pianezza, 289 - 10151 Torino IT	Nicola Losito, Amministratore Delegato	Link	22/03/2001	Manuali operativi
InfoCert S.p.A.	Piazza Sallustio, 9 - 00187 Roma, IT	Daniele Vaccarino, Presidente CdA	Link	19/07/2007	Manuali operativi Data: 15/02/2019
Intesa Sanpaolo S.p.A. (già Sanpaolo IMI S.p.A. e Banca Intesa S.p.A.)	Piazza San Carlo, 156 - 10126 Torino, IT	Messina Carlo, Consigliere delegato e CEO	Link	07/04/2004	Manuali operativi
Intesi Group S.p.A.	Via Torino, 4B - 20123 Milano, IT	Paolo Sironi	Link	19/01/2018	Manuale operativo
Lombardia Informatica S.p.A.	via Don Minzoni, 24 - 20158 Milano, IT	Francesco Ferri, Presidente	Link	16/12/2010	Manuali operativi

Prestatori di servizi fiduciari attivi in Italia

<https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia>



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Lottomatica Holding S.r.l.	Via del Campo Boano, 56/d 00154 - Roma	Fabio Attilio Cairoli	Link	20/11/2018	Manuali operativi Data: 30/11/2018
Namirial S.p.A.	Via Caduti sul Lavoro, 4 - 60019 Senigallia (AN), IT	Davide Ceccucci, Amministratore Delegato.	Link	03/11/2010	Manuali operativi
NexiPayments S.p.A.	Corsa Semiponte 55 - 20149 Milano, IT	Marco Bassilichi, Presidente	Link	01/07/2018	Manuali operativi Data: 01/07/2018
Poste Italiane S.p.A.	Viale Europa, 190 - 00144 Roma IT	Matteo Del Fante	Link	29/03/2017	Manuali operativi
Telecom Italia Trust Technologies S.r.l.	S.S. 148 Pontina - Km 29.100 - 00040 Pomezia (RM), IT	Salvatore Nappi, Amministratore Delegato	Link	01/01/2014	Manuali operativi Data: 18/03/2019
Zucchetti S.p.A.	Via Selvettino, 1 - 26900 Lodi	Alessandro Zucchetti, Amministratore delegato	Link	22/10/2015	Manuali operativi

Prestatori di servizi fiduciari cessati in Italia

Ragione sociale	Data iscrizione	Data cessazione	Certificatore sostitutivo
Banca di Roma S.p.A.	08/09/2004	13/02/2008	nessuno
Banca Intesa S.p.A.	08/09/2004		Intesa San Paolo S.p.A.
Banca Monte dei Paschi di Siena S.p.A.	03/04/2008	31/08/2015	no 'Contenuto nei certificati'
BNL Multiservizi S.p.A.	29/03/2000	30/11/2003	Actalis
Cedacrinord S.p.A.	14/11/2001		Cedacri S.p.A.
Centro Tecnico per la RUPA	14/03/2001		confluito nel CNIPA
CNIPA	14/03/2001	31/08/2009	nessuno
Comando C4 - IEW (dal 10/04/2003 - Nuova denominazione Comando Trasmissioni e Informazioni Esercito) Comando Trasmissioni e Informazioni Esercito	09/04/2003	21/09/2007	nessuno
Consiglio Nazionale Forense	10/12/2003	01/07/2014	Nessuno 'Contenuto nei certificati'
Consorzio Certicomm	22/06/2005	15/12/2008	CNDCEC
ENELIT S.p.A.	16/05/2001	31/12/2004	nessuno
Finital S.p.A.	12/04/2000	31/12/2003	nessuno
I.T. Telecom S.p.A. (già Saritel S.p.A.)	05/02/2003	31/12/2004	I.T. Telecom S.r.l.
I.T. Telecom S.r.l.	13/01/2005	31/12/2013	Telecom Italia Trust Technologies S.r.l. 'Contenuto nei certificati'
ICBPI - Istituto Centrale delle Banche Popolari Italiane S.p.A. (Cambio denominazione)	17/12/2012	10/11/2017	NEXI S.p.A. 'Contenuto nei certificati'
Infocamere S.c.p.A.	05/04/2000	15/12/2007	Infocert
Lombardia Integrata S.p.A. Servizi Infotelematici per il Territorio	16/08/2004	21/04/2011	Lombardia Informatica S.p.A. 'Contenuto nei certificati'

Prestatori di servizi fiduciari cessati in Italia

<https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia>



Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

Lottomatica S.p.A. (in cessazione)	26/07/2017	30/11/2018	
NEXI S.p.A.	10/11/2017	01/07/2018	NexiPayments S.p.A.
Postecom S.p.A.	20/04/2000	01/04/2017	Poste Italiane S.p.A. 'Contenuto nei certificati'
S.I.A. S.p.A.	26/01/2000	01/03/2003	Actalis
Sanpaolo IMI S.p.A. (società fusa per incorporazione in Banca Intesa)	07/04/2004		
Saritel S.p.A. (società fusa per incorporazione nella I.T. Telecom S.p.A.)	19/04/2000		
Seceti S.p.A.	05/07/2000	31/07/2003	Actalis
SOGEI S.p.A.	26/02/2004	20/02/2013	Contenuto nei certificati
SSB S.p.A.	19/04/2000	01/01/2003	Actalis
Trust Italia S.p.A.	06/06/2001	20/02/2008	Aruba PEC S.p.A.

**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 una 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.

Uso dei certificati

Vediamo alcuni usi comuni dei certificati

- HTTPS
- Code Signing

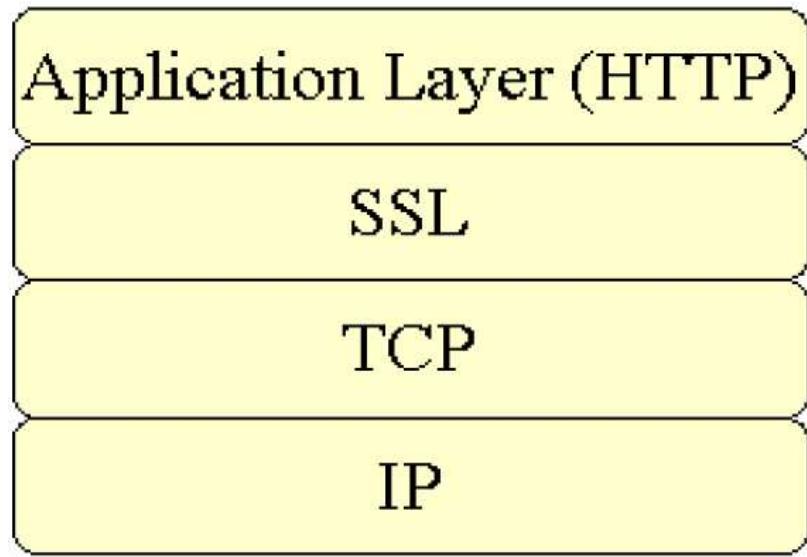
Certificati in HTTPS

Uso comune dei certificati

Accesso a siti web tramite HTTPS

➤ HTTP su SSL

Hypertext Transfer Protocol over Secure Socket Layer

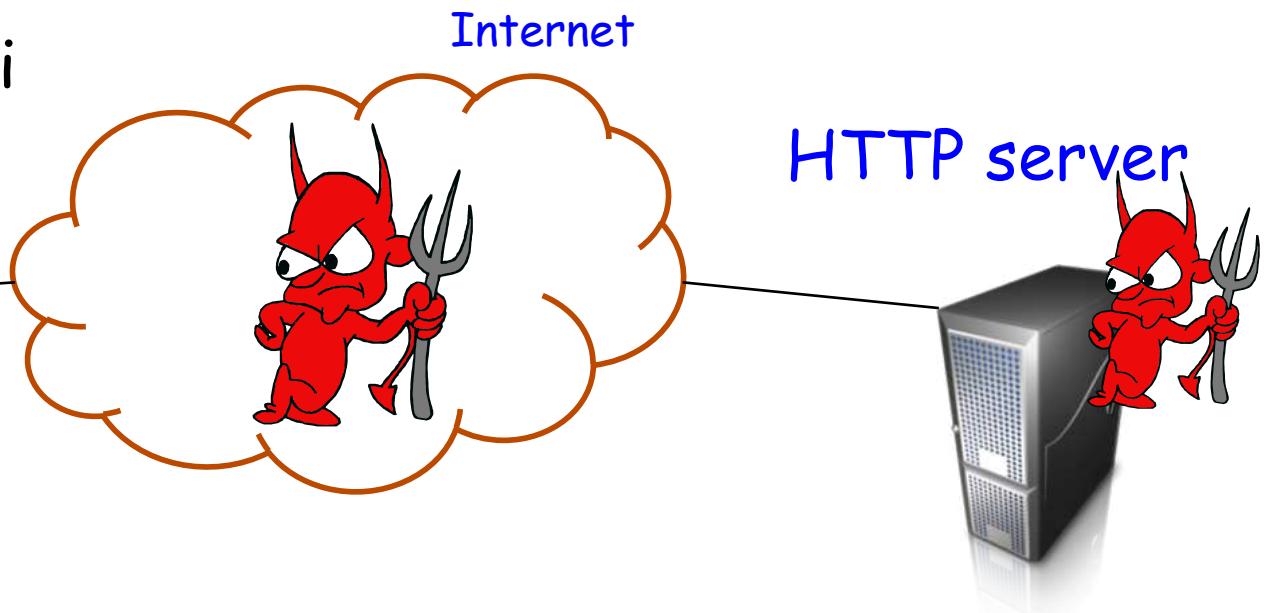


HTTP

Problemi di sicurezza

- Autenticazione
- Privacy
- Integrità dei dati

browser



HTTP

Problemi di sicurezza

- Autenticazione
- Privacy
- Integrità dei dati

L'attaccante può controllare il proprio sito web



Scenario:

- Link malevolo in una email di phishing
- Link malevolo in un'altra pagina web

HTTP

Problemi di sicurezza

- Autenticazione
- Privacy
- Integrità dei dati

L'attaccante controlla completamente

- Wi-Fi, DNS, router, il proprio sito web, può sniffare qualsiasi pacchetto, modificare pacchetti in transito, inserire propri pacchetti nella rete

Scenario:

- Tipicamente HotSpot
 - Accesso internet negli hotel (ISP non fidato)
 - Internet Café connesso tramite un Access Point Wi-Fi



HTTP

Problemi di sicurezza

- Autenticazione
- Privacy
- Integrità dei dati

L'attaccante può ottenere:

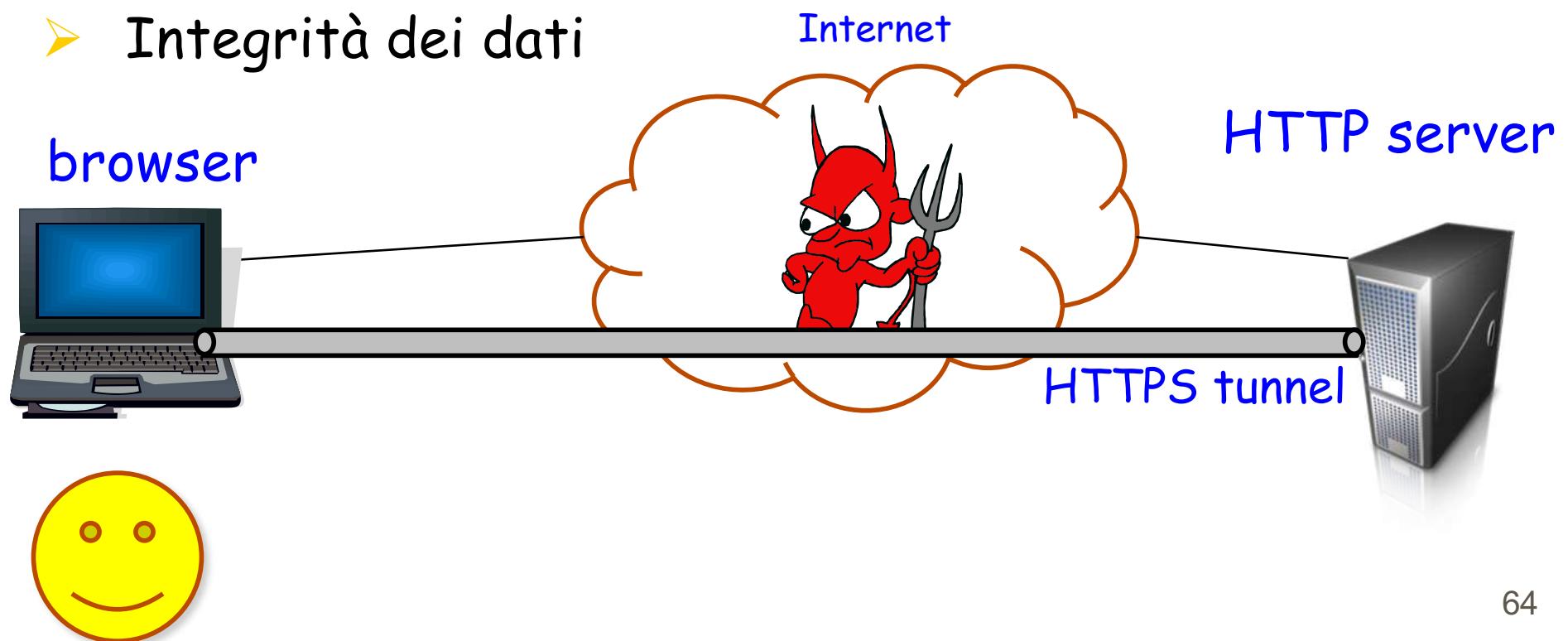
- login and password
- informazioni finanziarie (ad es., numeri di carta di credito, account bancari)
- dati personali (ad es., nomi, indirizzi, codici fiscali, date di nascita)
- informazioni proprietarie
- documenti legali e contratti
- liste dei clienti
- dati medici
- etc.



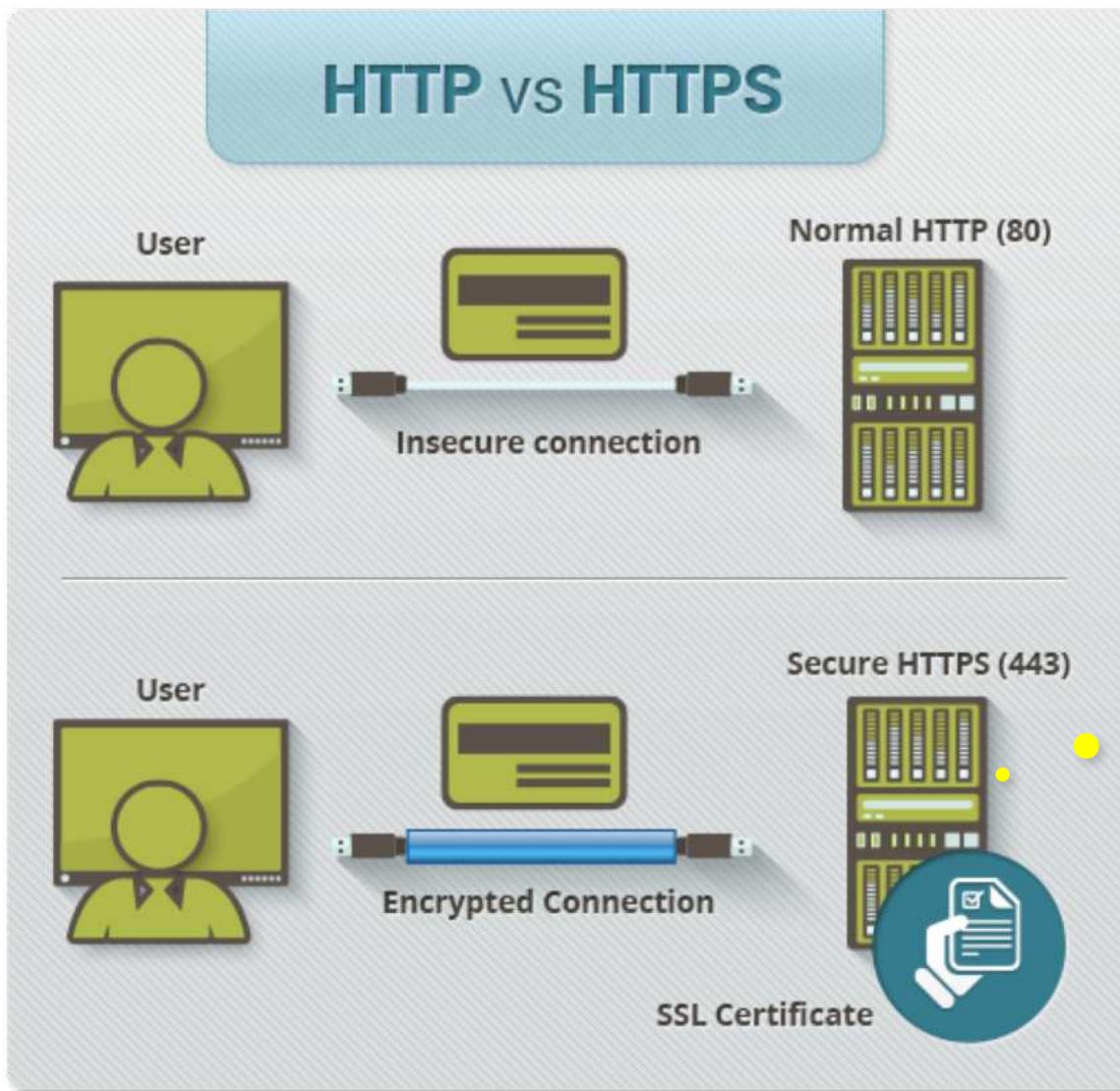
HTTP

Problemi di sicurezza

- Autenticazione
- Privacy
- Integrità dei dati



Certificati in HTTPS



<https://esse3web.unisa.it/unisa>

The screenshot shows a web browser window displaying the Unisa website (<https://esse3web.unisa.it/unisa>). The page is titled "UNISA" and features the University of Salerno logo and the text "UNIVERSITÀ DEGLI STUDI DI SALERNO CAMPUS VIVENDI". A navigation bar at the top includes links for "Home", "SERVIZI ON-LINE", and language options "Ita" and "Eng".

The main content area is titled "Guest" and contains a sidebar with links for "Area Riservata", "Registrazione", "Login", "Password dimenticata", "Comunità", "Didattica", "Offerta Didattica", "Facoltà / Dipartimenti", "Corsi di Laurea", "Corsi di Specializzazione", "Dottorati di ricerca", "Master 1° livello", "Master 2° livello", "Specialistica / Magistrale", "Specialistica / Magistrale a ciclo unico", "Segreterie Studenti on-line", "Sedi", "Bacheca Appelli", and "Bacheca Appelli di Laurea".

The central content area is titled "Area Struttura Didattica" and contains the following text:

DA QUESTA PAGINA E' POSSIBILE ACCEDERE ALL'AREA RISERVATA
GLI STUDENTI CHE ACCEDONO PER LA PRIMA VOLTA ALL'AREA RISERVATA DEVONO REGISTRARSI AL SITO SELEZIONANDO 'REGISTRAZIONE' DAL MENU' DI SINISTRA, PER OTTENERE I CODICI DI ACCESSO 'NOME UTENTE' E 'PASSWORD'
GLI STUDENTI CHE SONO GIA' REGISTRATI POSSONO ACCEDERE ALL'AREA RISERVATA SELEZIONANDO 'LOGIN' DAL MENU' DI SINISTRA

I DOCENTI DELL'ATENEO NON DEVONO REGISTRARSI: PER OTTENERE I CODICI DI ACCESSO, INVIARE EMAIL A: HELPDOCENTI@UNISA.IT

Didattica » Area Struttura Didattica

Come verificare che un sito abbia un certificato SSL



Come verificare che un sito abbia un certificato SSL

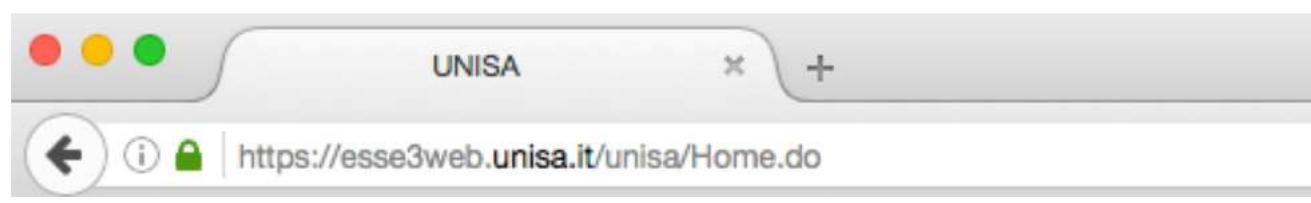
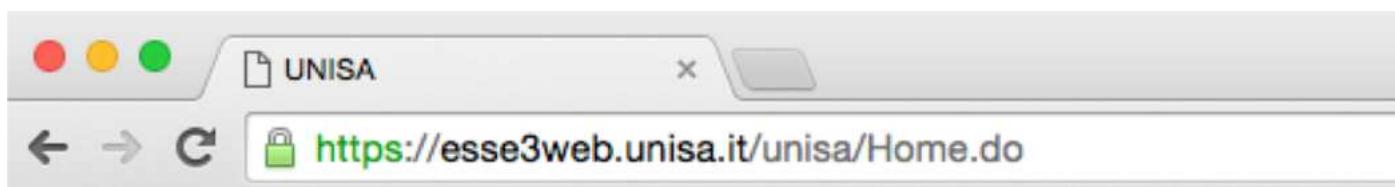
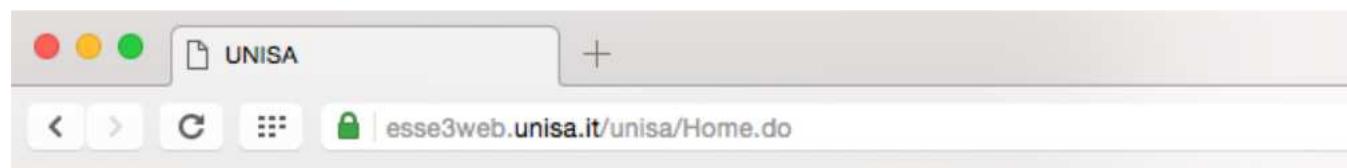
Ci sono quattro indizi visivi:

- Lucchetto a fianco di una URL
- Prefisso https dell'URL invece di http
- Un sigillo di fiducia



- Alcune componenti della barra degli indirizzi sono di colore verde
- Lucchetto, prefisso https, etc.

Barra degli indirizzi



Homepage area pubblica, Università di Salerno

Safari utilizza una connessione a esse3web.unisa.it codificata.

La codifica con un certificato digitale mantiene private le informazioni quando vengono inviate al/dal sito web https://esse3web.unisa.it.

MENU

Area Strutturale

DA QUESTA PAGINA E' POSSIBILE ACCEDERE ALLA SEZIONE DI CUI ALDO A DESTRA, PER OTTENERE I DOCUMENTI DI CUI ALLA NOTA.

GLI STUDENTI CHE ACCEDONO A QUESTA PAGINA SONO IDENTIFICATI DA UN COLORE DIVERSO DA QUELLO DEGLI STUDENTI CHE SONO IDENTIFICATI DA UN COLORE DIVERSO.

I DOCENTI NON DEVONO RICORDARSI DI ACCEDERE ALLA SEZIONE DI CUI ALDO A DESTRA.

Home

DigiCert Assured ID Root CA
└ TERENA SSL CA 3
└ esse3web.unisa.it

esse3web.unisa.it

Emesso da: TERENA SSL CA 3
Scade: mercoledì 19 maggio 2021 02:00:00 Ora legale dell'Europa centrale
Il certificato è valido

► Attendibilità

▼ Dettagli

Nome soggetto _____

Paese o regione IT
Località Fisciano
Società Università degli Studi di Salerno
Unità organizzativa unisa.it
Nome comune esse3web.unisa.it

Nome emittente _____

Paese o regione NL
Stato/Provincia Noord-Holland
Località Amsterdam
Società TERENA
Nome comune TERENA SSL CA 3

Numero di serie 07 2F 3A DC A6 FF A9 42 26 01 7C 24 C3 29 25 F0
Versione 3
Algoritmo firma SHA-256 con codifica RSA (1.2.840.113549.1.1.11)
Parametri Nessuno

Non valido prima di giovedì 14 febbraio 2019 01:00:00 Ora standard dell'Europa centrale
Non valido dopo mercoledì 19 maggio 2021 02:00:00 Ora legale dell'Europa centrale

Informazioni chiave pubblica _____

Algoritmo Codifica RSA (1.2.840.113549.1.1.1)
Parametri Nessuno

Chiave pubblica 256 byte: B1 2E F6 F3 4A B6 B8 0A E2 E5 43 4A 01 BB EF 38 BC AE 8F C3 5F 49 74
44 70 05 36 AE 6D DE 1B 18 EC 14 B8 4C 1B D9 44 18 BF 22 33 F2 7A 5C 21 B1 92
37 25 2E 0A BC 1F D3 C2 EC AB B8 14 9C E8 90 B5 31 58 2D D3 30 63 18 31 29 0C
FA CD E8 EE B0 D3 14 E5 7B F8 72 5C 01 61 97 65 A3 23 BB 6F 0D 9D 4A 3D 29

?

Nascondi certificato

OK

NE' DAL MENU' IN ALTO A DESTRA

'LOGIN' DAL MENU' IN ALTO A DESTRA

INFORMATIVA UTILIZZO COOKIE | © CINECA



UNIVERSITÀ



Safari utilizza una connessione a esse3web.unisa.it codificata.

La codifica con un certificato digitale mantiene private le informazioni quando vengono inviate al/dal sito web
https://esse3web.unisa.it.≡
MENU

Area Strutturale

DA QUESTA PAGINA E' POSSIBILE:

GLI STUDENTI CHE ACCEDONO AL SITO DA QUESTA PAGINA SONO AUTORIZZATI A:

GLI STUDENTI CHE SONO CONNETTI ALLA RETE SONO AUTORIZZATI A:

I DOCENTI NON DEVONO FAR ALTRO CHE ACCEDERE DA QUESTA PAGINA ALLA RETE DA ALTO A DESTRA

Home

DigiCert Assured ID Root CA

TERENA SSL CA 3

esse3web.unisa.it

TERENA SSL CA 3

Autorità di certificazione intermedia

Scade: lunedì 18 novembre 2024 13:00:00 Ora standard dell'Europa centrale

Il certificato è valido

► Attendibilità

▼ Dettagli

Nome soggetto

Paese o regione NL

Stato/Provincia Noord-Holland

Località Amsterdam

Società TERENA

Nome comune TERENA SSL CA 3

Nome emittente

Paese o regione US

Società DigiCert Inc

Unità organizzativa www.digicert.com

Nome comune DigiCert Assured ID Root CA

Numero di serie 08 70 BC C5 AF 3F DB 95 9A 91 CB 6A EE EF E4 65

Versione 3

Algoritmo firma SHA-256 con codifica RSA (1.2.840.113549.1.1.11)

Parametri Nessuno

Non valido prima di martedì 18 novembre 2014 13:00:00 Ora standard dell'Europa centrale

Non valido dopo lunedì 18 novembre 2024 13:00:00 Ora standard dell'Europa centrale

Informazioni chiave pubblica

Algoritmo Codifica RSA (1.2.840.113549.1.1.1)

Parametri Nessuno

Chiave pubblica 256 byte: C5 76 0F 0F D9 43 29 3B ...

Esponente 65537

Dimensione chiave 2.048 bit

Utilizzo chiave Verifica

?

Nascondi certificato

OK



UNIVERSITÀ



Safari utilizza una connessione a esse3web.unisa.it codificata.

La codifica con un certificato digitale mantiene private le informazioni quando vengono inviate al/dal sito web
https://esse3web.unisa.it.≡
MENU

Area Strutturale

DA QUESTA PAGINA E' POSSIBILE:

GLI STUDENTI CHE ACCEDONO DA QUESTA PAGINA SONO A DESTRA, PER OTTENERE I CERTIFICATI

GLI STUDENTI CHE SONO CONNETTI DA QUESTA PAGINA SONO A DESTRA

I DOCENTI NON DEVONO FARE NIENTE, SONO A DESTRA, ALTO A DESTRA

Home

DigiCert Assured ID Root CA

TERENA SSL CA 3

esse3web.unisa.it

DigiCert Assured ID Root CA
Autorità di certificazione principale
Scade: lunedì 10 novembre 2031 01:00:00 Ora standard dell'Europa centrale
Il certificato è valido

► Attendibilità

▼ Dettagli

Nome soggetto _____
Paese o regione US
Società DigiCert Inc
Unità organizzativa www.digicert.com
Nome comune DigiCert Assured ID Root CA

Nome emittente _____
Paese o regione US
Società DigiCert Inc
Unità organizzativa www.digicert.com
Nome comune DigiCert Assured ID Root CA

Numero di serie 0C E7 E0 E5 17 D8 46 FE 8F E5 60 FC 1B F0 30 39
Versione 3
Algoritmo firma SHA-1 con codifica RSA (1.2.840.113549.1.1.5)
Parametri Nessuno

Non valido prima di venerdì 10 novembre 2006 01:00:00 Ora standard dell'Europa centrale
Non valido dopo lunedì 10 novembre 2031 01:00:00 Ora standard dell'Europa centrale

Informazioni chiave pubblica
Algoritmo Codifica RSA (1.2.840.113549.1.1.1)
Parametri Nessuno
Chiave pubblica 256 byte: AD 0E 15 CE E4 43 80 5C ...
Esponente 65537
Dimensione chiave 2.048 bit
Utilizzo chiave Verifica

Firma 256 byte: A2 0F BC DF E2 FD F0 F3

?

Nascondi certificato

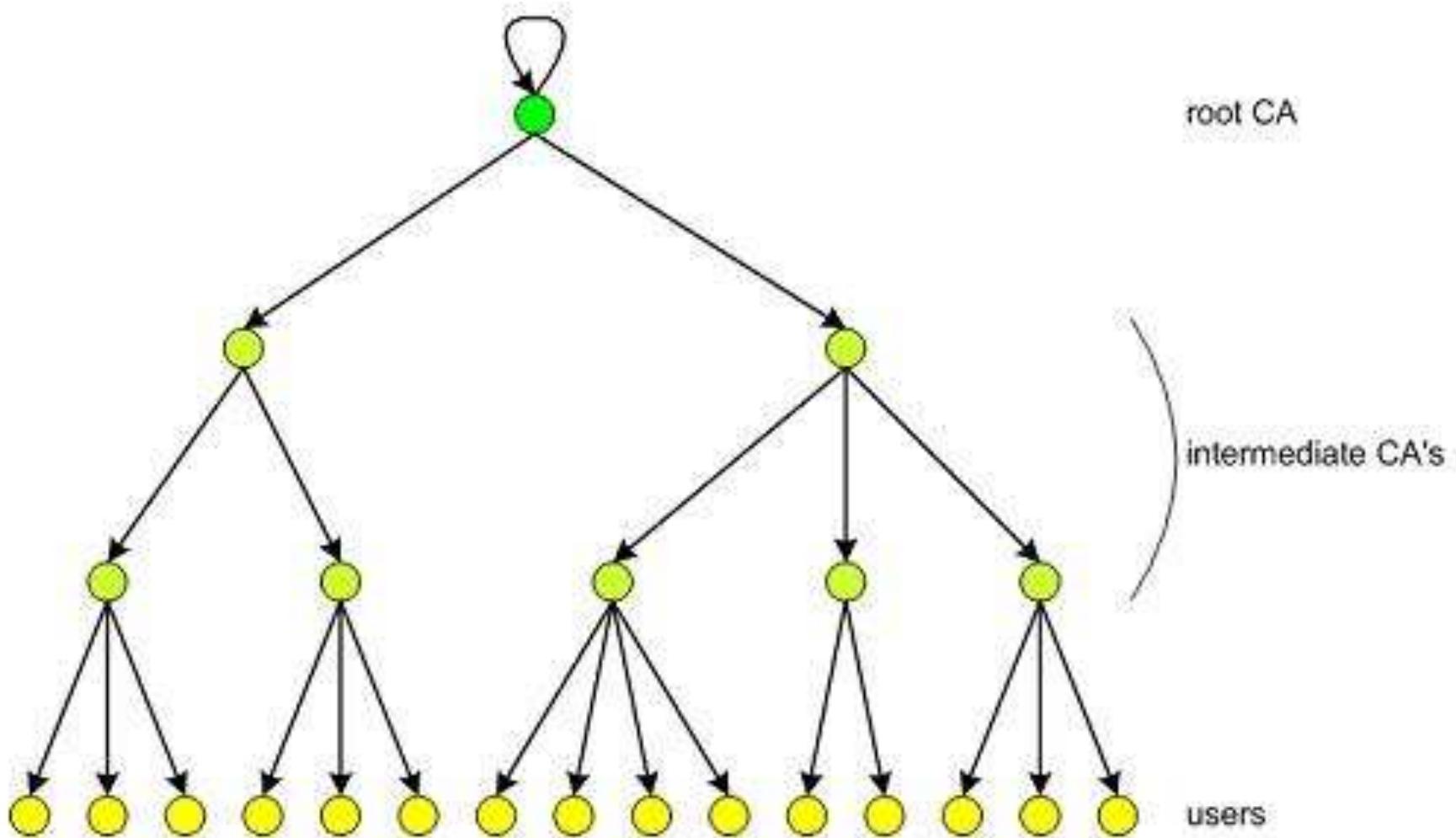
OK

NE' DAL MENU' IN ALTO A DESTRA

'LOGIN' DAL MENU' IN ALTO A DESTRA

Informativa utilizzo cookie | © CINECA

Gerarchia di Certificati



Chain of trust

End-entity Certificate

Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

reference

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

sign

reference

Root CA's name
Root CA's public key
Root CA's signature

sign

self-sign

Root Certificate

Quanti certificati?

Per esempio, la sola Let's Encrypt:



Let's Encrypt

[Documentation](#)

[Get Help](#)

[Donate](#) ▾

[About Us](#) ▾

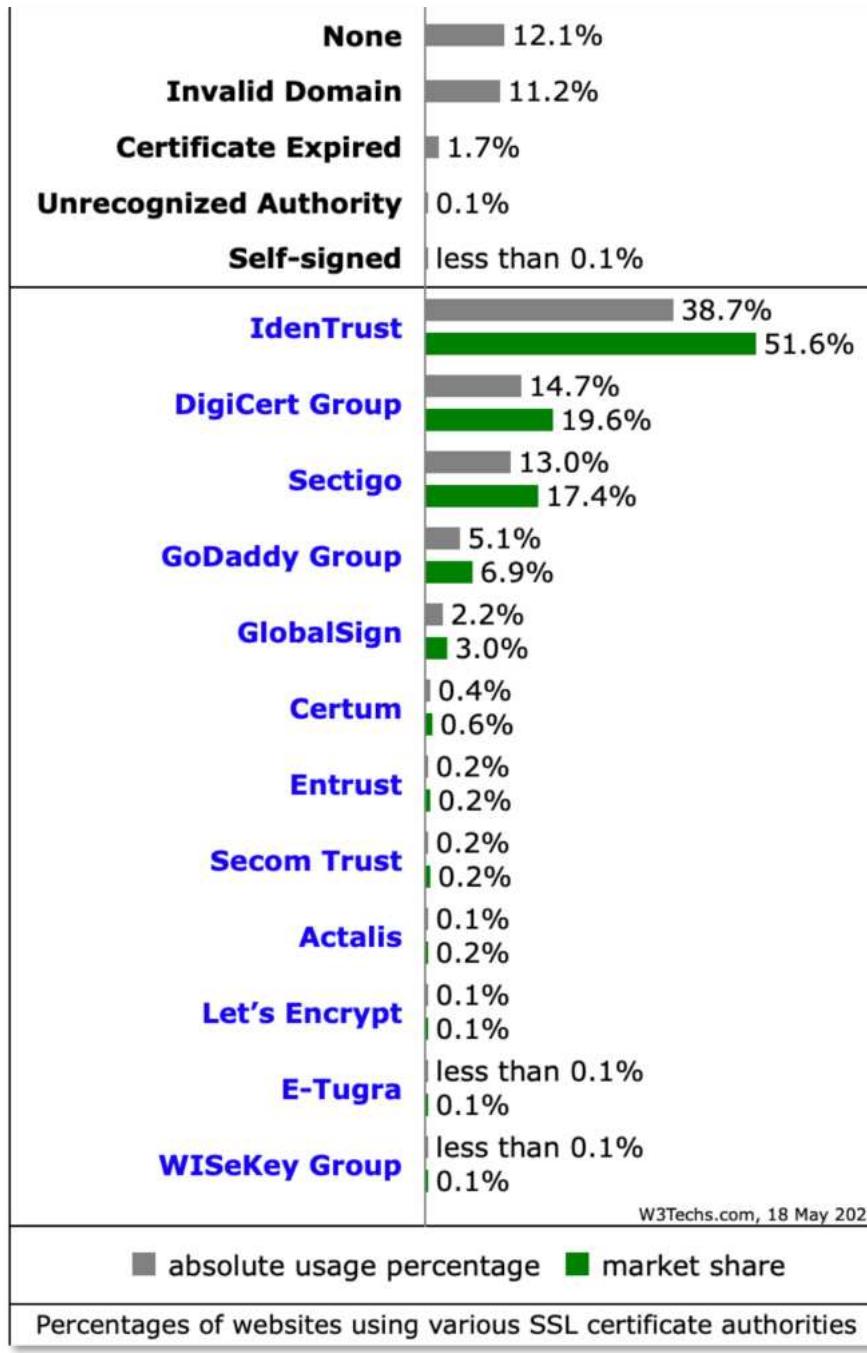
[Languages](#) ▾

Let's Encrypt Has Issued a Billion Certificates

Feb 27, 2020 • Josh Aas and Sarah Gran

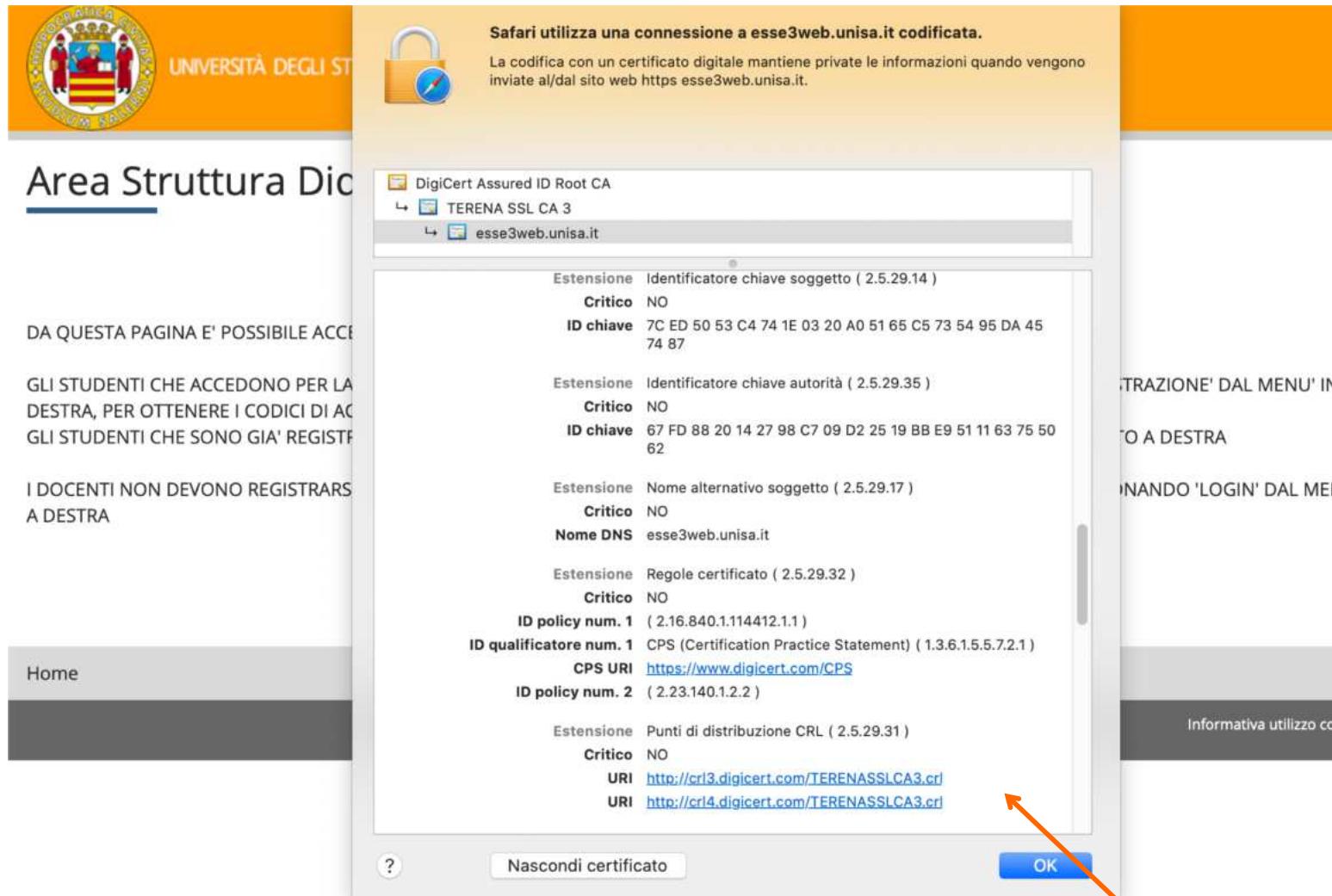
We issued our billionth certificate on February 27, 2020. We're going to use this big round number as an opportunity to reflect on what has changed for us, and for the Internet, leading up to this event. In particular, we want to talk about what has happened since the last time we talked about a big round number of certificates - [one hundred million](#).

One thing that's different now is that the Web is much more encrypted than it was. In June of 2017 approximately 58% of page loads used HTTPS globally, 64% in the United States. Today 81% of page loads use HTTPS globally, and we're at 91% in the United States! This is an incredible achievement. That's a lot more privacy and security for everybody.



18 maggio 2020

https://w3techs.com/technologies/overview/ssl_certificate



CRL



```
MacBook-Pro-di-Alfredo:Downloads alfredo$ ls -l TERENASSLCA3.crl
-rw-r--r--@ 1 alfredo  staff  70806 14 Mag 20:15 TERENASSLCA3.crl
MacBook-Pro-di-Alfredo:Downloads alfredo$ 
MacBook-Pro-di-Alfredo:Downloads alfredo$ openssl crl -inform DER -text -in TERENASSLCA3.crl
Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: /C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL CA 3
    Last Update: May 14 18:00:30 2016 GMT
    Next Update: May 21 17:00:00 2016 GMT
    CRL extensions:
        X509v3 Authority Key Identifier:
            keyid:67:FD:88:20:14:27:98:C7:09:D2:25:19:BB:E9:51:11:63:75:50:62

        X509v3 CRL Number:
            541
Revoked Certificates:
    Serial Number: 0E325FB7D306601FF0F41DD4F22E436E
        Revocation Date: Dec 3 10:22:58 2014 GMT
    Serial Number: 0BC08E69868107B1FA73F6BB9147504E
        Revocation Date: Dec 3 10:23:38 2014 GMT
    Serial Number: 01732DDDF0E66953687B8F4318884045
        Revocation Date: Dec 11 12:17:44 2014 GMT
    Serial Number: 031BC4CC55EB87FE9B4D5B0C6863EDBE
        Revocation Date: Jan 3 10:33:04 2015 GMT
```

Certificate Revocation List (CRL) Management

-inform DER|PEM

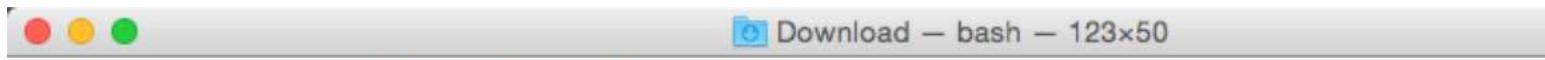
Specifica il formato di input. DER permette di codificare la struttura della CRL in formato DER. PEM (default) è una versione codificata in Base64 del formato DER, con l'aggiunta di alcune linee di header e di footer

-in filename

Specifica il nome del file da cui leggere oppure lo standard input se questa opzione non è specificata

-text

Stampa la CRL in formato testuale



```
Serial Number: 04D4EEFAE5013EA94A1E09F6126C1A49
    Revocation Date: May 13 05:31:04 2016 GMT
Serial Number: 0DA8CA483E6E9E2478E37E19E922E15B
    Revocation Date: May 13 07:44:48 2016 GMT
Serial Number: 0A3C551F61CB907296D9319D4D46D7BA
    Revocation Date: May 13 07:59:01 2016 GMT
Serial Number: 0526BD5A0B82AC056135483011A44F2C
    Revocation Date: May 13 08:34:22 2016 GMT
Serial Number: 02B185A6C7C9C08D2D1ED3CAB7974F13
    Revocation Date: May 13 08:49:22 2016 GMT
Serial Number: 0E228F90FCD18E597904A0D382A13F66
    Revocation Date: May 13 12:52:14 2016 GMT
Serial Number: 0C5976BA5FBABF94CB4AD98BF1FF116B
    Revocation Date: May 14 06:51:01 2016 GMT
Signature Algorithm: sha256WithRSAEncryption
5f:a8:65:70:a8:7d:70:5f:cd:1b:a0:79:df:5f:54:97:a6:81:
87:58:de:6a:1f:63:e3:1b:bd:78:22:b1:af:db:06:00:cf:f6:
1b:ac:6d:7a:50:9f:ed:d6:e5:ba:b0:cb:7a:ca:bb:ce:59:d3:
0e:e2:70:36:23:10:f4:7b:05:01:20:a1:20:a5:e8:29:77:7c:
72:ac:31:21:9c:03:68:c2:fb:1c:f6:02:ea:9e:46:44:af:44:
62:10:2c:72:e7:7f:7c:1e:af:84:36:7b:b9:de:00:9d:d3:1d:
ba:5a:d8:07:0d:64:d0:7f:39:d1:01:33:2e:29:66:f8:c9:81:
44:fd:e9:cb:a6:f7:e3:95:51:e1:9a:7a:93:f6:db:02:57:a6:
f0:b5:14:7b:13:51:34:a7:d0:17:86:2d:29:f5:16:47:b8:05:
4c:1e:11:d8:39:36:b0:62:2c:51:0a:48:e9:93:72:1d:1d:36:
f5:00:c1:74:e8:5e:98:fc:ae:b4:72:24:d3:21:ee:70:5a:2d:
1d:fb:0f:b7:c1:ff:05:19:0f:c0:20:2e:f2:fe:a8:f2:d5:48:
5f:35:e6:ba:52:71:74:44:f8:a1:0b:bf:90:8b:38:2c:ee:71:
72:62:1c:02:42:17:d3:2a:3d:96:70:1e:e4:f6:1e:99:2e:6c:
67:e4:cb:09
-----BEGIN X509 CRL-----
MIMBFJEWgwETeAIBATANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJOTDEWMBQG
A1UECBMNTm9vcmtSG9sbGFuZDESMBAGA1UEBxMJQW1zdGVyZGftMQ8wDQYDVQQK
EwZURVJFTkExGDAWBgNVBAMTD1RFUkVOQSBU0wgQ0EgMxcNMTYwNTE0MTgwMDMw
WhcNMTYwNTIxMTcwMDAwWjCDARKrMCECEA4yX7fTBmAf8PQd1PIuQ24XDTE0MTIw
MzEwMjI10FowIQIQC8C0aYaBB7H6c/a7kUdQThcNMTQxMjAzMTAyMzM4WjAhAhAB
cy3d80ZpU2h7j0MYiEBFFw0xNDEyMTExMjE3NDRaMCECEAMbxMxV64f+m01bDGhj
...
hi0p9RZHuAVMHhHY0TawYixRCKjkpk3IdHTb1AMF06F6Y/K60ciTTIe5wWi0d+w+3
wf8FGQ/AIC7y/qjy1UhfNea6UnF0RPihC7+Qizgs7nFyYhwCQhfTKj2WcB7k9h6Z
Lmxn5MsJ
-----END X509 CRL-----
MacBook-Pro-di-Alfredo:Downloads alfredo$
```

<https://www.openssl.org/docs/manmaster/apps/crl.html>

Maggiori dettagli in seguito!

86

Certificato che non può essere convalidato



Autorità di certificazione

- Commerciali
- Ad esempio

COMODO
Creating Trust Online®  Symantec



 **GlobalSign**
GMO INTERNET GROUP

IdenTrust  **digiCert**®

- Gratuite
- CAcert.org
- Let's Encrypt


 **Let's Encrypt**



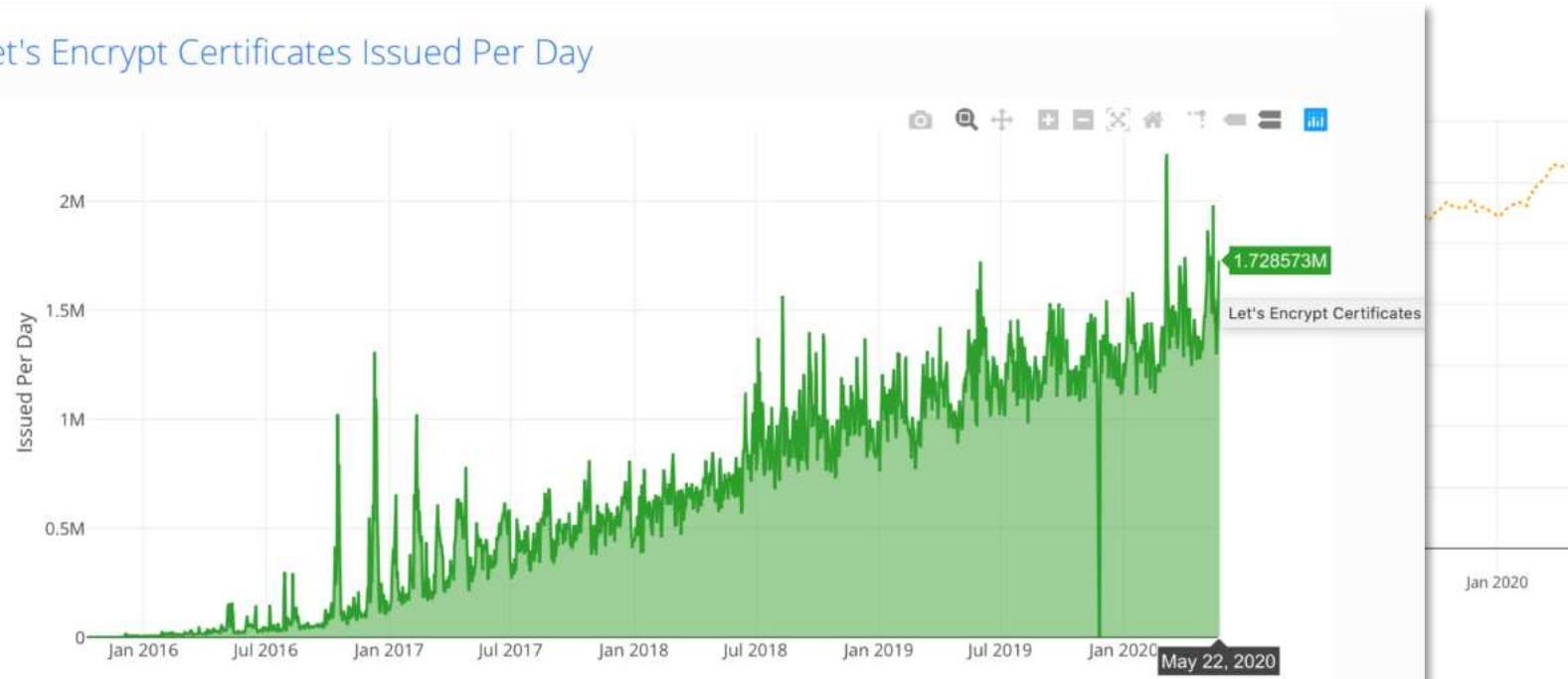
- Autorità di certificazione
- Rilascia gratuitamente certificati X.509 per TLS
- Attiva da 12 aprile 2016
- Solo domain-validated certificate
 - Identità validata con controllo su dominio DNS
- Numero certificati emessi





Let's Encrypt

- Autorità di certificazione
- Rilascia gratuitamente certificati X.509 per TLS
- Attiva da 12 aprile 2016
- Solo domain-validated certificate
 - Identità validata con controllo su dominio DNS
- Let's Encrypt Certificates Issued Per Day



Microsoft Security Advisory 2524375

Fraudulent Digital Certificates Could Allow Spoofing

Published: March 23, 2011 | Updated: July 06, 2011

Version: 5.0

General Information

Executive Summary

Microsoft is aware of nine fraudulent digital certificates issued by Comodo, a certification authority present in the Trusted Root Certification Authorities Store, on all supported releases of Microsoft Windows, Windows Mobile 6.x, Windows Phone 7, Microsoft Kin, and Zune HD devices. Comodo advised Microsoft on March 16, 2011 that nine certificates had been signed on behalf of a third party without sufficiently validating its identity. These certificates may be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against all Web browser users including users of Internet Explorer.

These certificates affect the following Web properties:

- login.live.com
- mail.google.com
- www.google.com
- login.yahoo.com (3 certificates)
- login.skype.com
- addons.mozilla.org
- "Global Trustee"

Comodo has revoked these certificates, and they are listed in Comodo's current Certificate Revocation List (CRL). In addition, browsers which have enabled the Online Certificate Status Protocol (OCSP) will interactively validate these certificates and block them from being used.

<https://technet.microsoft.com/en-us/library/security/2524375>

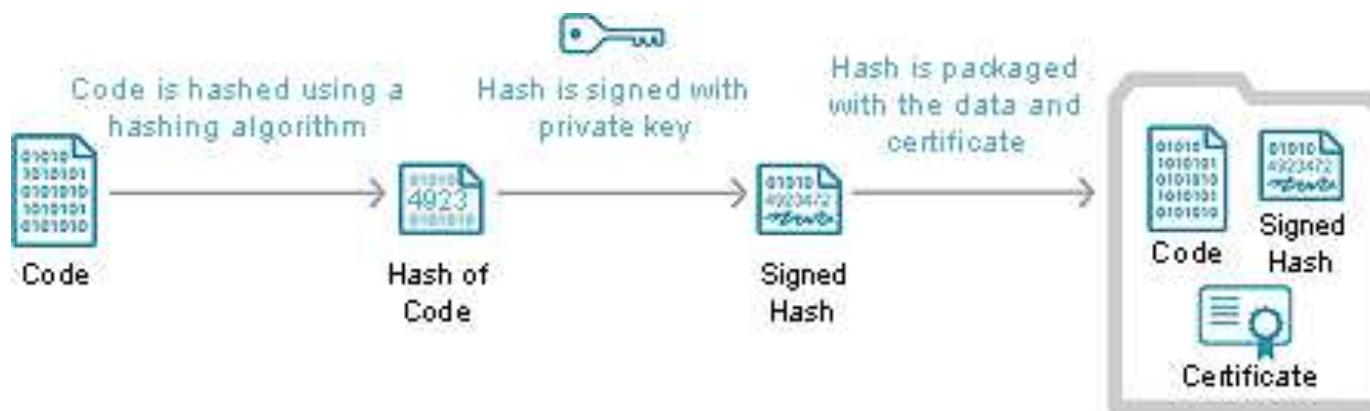
Uso dei certificati

Vediamo alcuni usi comuni dei certificati

- HTTPS
- Code Signing

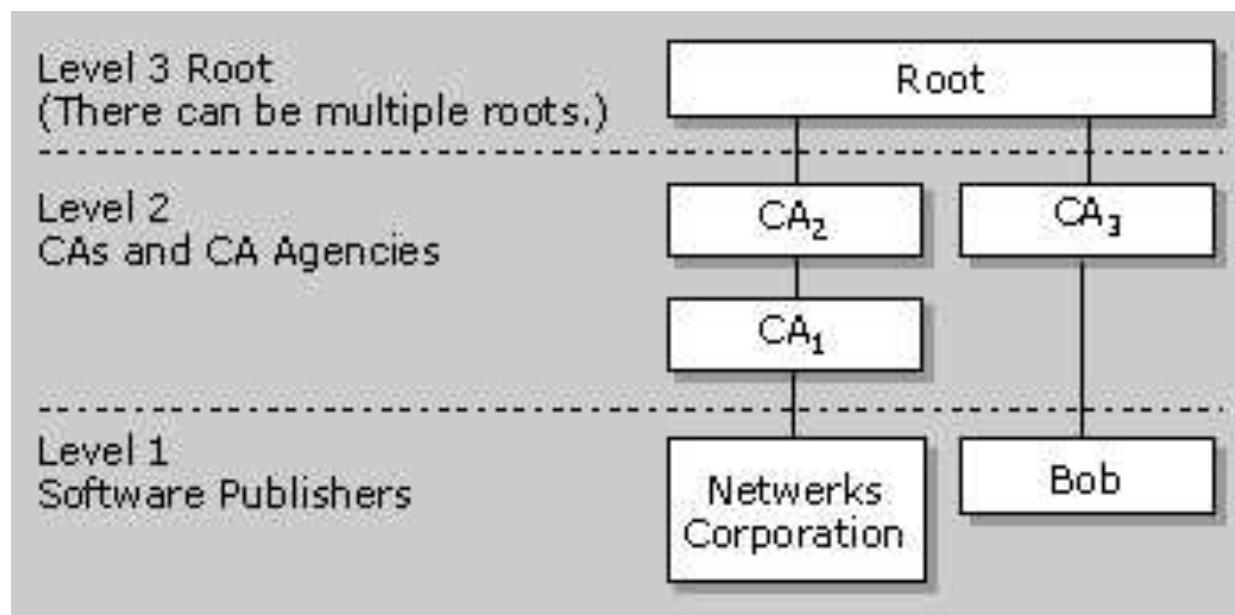
Code Signing

Un Code Signing Certificate permette agli sviluppatori di firmare digitalmente il loro software prima della distribuzione via web



- **Origine del Contenuto:** Gli utenti finali possono avere conferma che il software provenga proprio dalla legittima fonte che lo ha firmato
- **Integrità del Contenuto:** Gli utenti finali possono verificare che il software non è stato modificato da quando è stato firmato

Code Signing



[https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537361\(v=vs.85\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537361(v=vs.85)?redirectedfrom=MSDN)

Bibliografia

- Cryptography and Network Security
by W. Stallings (2005)
 - cap. 10 (Key Management)
 - cap. 14 (X.509 Authentication Service)

Domande?

