Distribuzione chiavi pubbliche

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

Possibilità per distribuzione chiavi pubbliche

- Annuncio pubblico
- Directory disponibile pubblicamente
- Autorità per le chiavi pubbliche
- Certificati per le chiavi pubbliche

Annuncio pubblico

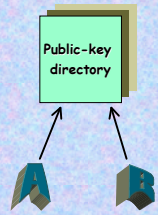
- Invio ad altri utenti / Broadcast chiave
- Esempio: aggiunta della chiave pubblica PGP ai messaggi inviati a forum pubblici (USENET newsgroup, mailing list)

Problema: ci dobbiamo fidare dell'annuncio?

Directory disponibile pubblicamente

Entità fidata:
- Gestisce la directory
- Periodicamente pubblica la directory o gli aggiornamenti

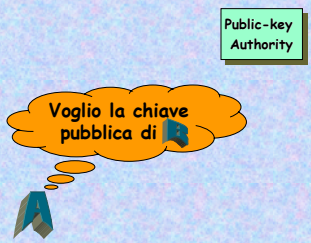
Ogni partecipante:
- Registra la propria chiave pubblica con l'autorità (registrazione di persona, o in modo autenticato)
- Può aggiornare la propria chiave (usata da troppo tempo, o chiave privata compromessa)
- Può accedere alla directory elettronicamente ⇒ bisogna prevedere comunicazione sicura ed autenticata



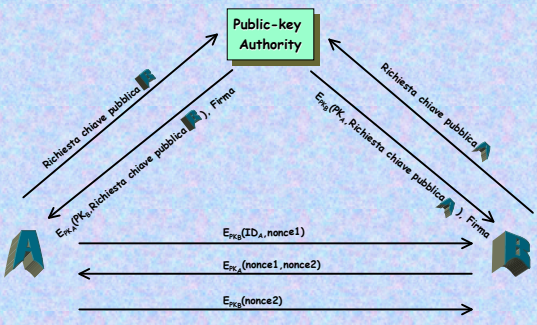
Autorità per le chiavi pubbliche

- Gestisce directory chiavi pubbliche
- Ha una chiave pubblica per la cifratura ed una per la firma conosciute da tutti gli utenti
- Ogni utente chiede la chiave pubblica desiderata
- Problema: autenticazione
- Vediamo un possibile protocollo

Autorità per le chiavi pubbliche

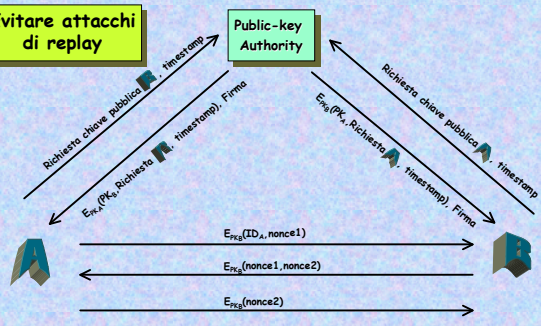


Autorità per le chiavi pubbliche



Autorità per le chiavi pubbliche

Evitare attacchi di replay



Caching chiavi pubbliche

Ottenuta una chiave pubblica, si memorizza

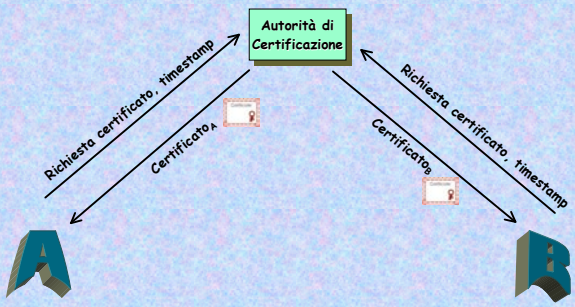
... ma occorre aggiornarla periodicamente

Certificati

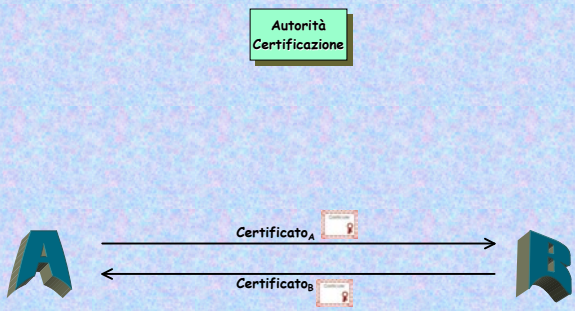
Alcune proprietà dei certificati:

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

Richiesta Certificati



Scambio Certificati



Problemi coi certificati

- Chi invia il certificato è il legittimo possessore?
  Cattura, Replay, …
- Validità certificato
- Se la chiave privata è compromessa?

Cryptoperiodi

- Limitare info per crittoanalisi
- Limitare pericoli in caso di compromissione chiave privata
- Limitare uso della tecnologia al suo tempo di possibile effettivo utilizzo

Ciclo di vita di una chiave

[W. Ford 1994]

- Generazione
  e possibile registrazione (chiave pubblica)
- Distribuzione
- Attivazione
- Aggiornamento
- Revoca
- Terminazione (inclusa distruzione ed archiviazione)

Certificati

- **Certificato**: struttura dati composta da
  - dati (in chiaro): almeno una chiave pubblica ed una stringa identificativa (subject entity)
  - firma di una autorità che *lega* chiave e identità
- **Autorità di Certificazione**: Terza parte fidata la cui firma *garantisce* il legame tra chiave ed identità
- Esempi di altri dati di un certificato:
  - periodo di validità chiave pubblica
  - numero seriale o identificatore chiave
  - info addizionali su subject entity (ad es., indirizzo fisico o rete)
  - info addizionali su chiave (ad es., algoritmi ed utilizzo)
  - stato della chiave pubblica (revoca certificati)

Revoca Certificati

- **Data scadenza dentro un certificato**
- **Notifica manuale**
- **File pubblico di chiavi revocate**
  - **Certificate Revocation List** (CRL)
- **Certificato di revoca**

Certificate Revocation List (CRL)

- Lista firmata da CA contenenti i numeri seriali dei certificati emessi revocati (ma non ancora scaduti), quando è avvenuta la revoca, ed altro (per es., motivi)
  - la data della CRL indica quanto sia aggiornata
- **Distribuzione CRL**:
  - modello **pull**: download da CA quando necessario
  - modello **push**: CA la invia ad intervalli regolari
  - approccio **ibrido**: CA la invia a repository intermediari da cui il verificatore fa il download quando necessario
- **Segmentazione CRL** Se troppo grandi:
  - Invio solo degli aggiornamenti (*delta-CRL*)
  - Partizione lista per motivi della revoca
  - Partizione in segmenti pre-assegnati

Funzioni di terze-parti

- Certification Authority (CA) gestione certificati, CRL, serial number
- Name Server gestione spazio nomi, identificativo unico per ogni utente relativo ad una CA
- Registration Authority
- Key Generator crea chiavi. Può essere parte dell'entità utente, parte della CA, o componente indipendente
- Certificate Directory database o server accessibile in lettura da utenti. La CA può fornire certificati (e gestire) al database

Raccomandazioni X.509

- Parte della serie X.500 di raccomandazoni che definisce un "directory service"
  - directory: server o insieme distribuito di server che mantiene un database di informazioni (come mapping da nome utente ad indirizzo rete) su utenti
- Servizi di autenticazione della directory X.500 ad utenti
- Standard X.509 usato in: S/MIME, SSL/TLS, SET, IP Security, …
- X.509 definito nel 1988 da ITU-T
  - Modificato nel 1993
  - Terza versione nel 1995

International Telecommunication Union Telecommunication Standardization Sector

Certificati X.509

- Cuore delle raccomandazioni X.509
- Creati da una Certification Authority (CA)

Campi Certificati X.509

Version
Serial number
Signature Algorithm ID
Issuer name
Validity period
Subject name
Subject's public key information
Issuer unique identifier
Subject unique identifier
Extensions
Firma dei precedenti campi

Versione 1

- 1 default
- 2 se presente "Issuer unique identifier" oppure "Subject unique identifier"
- 3 se ci sono estensioni

tutte le versioni

Campi Certificati X.509

Version
Serial number
Signature Algorithm ID
Issuer name
Validity period
Subject name
Subject's public key information
Issuer unique identifier
Subject unique identifier
Extensions
Firma dei precedenti campi

Versione 1

- Valore intero
- Unico per ogni CA
- Identifica senza ambiguità il Certificato

tutte le versioni

Campi Certificati X.509

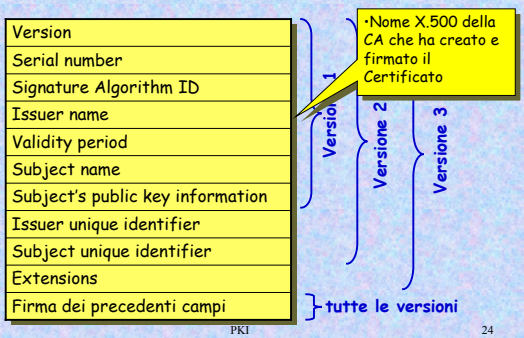
Version
Serial number
Signature Algorithm ID
Issuer name
Validity period
Subject name
Subject's public key information
Issuer unique identifier
Subject unique identifier
Extensions
Firma dei precedenti campi

Versione 1

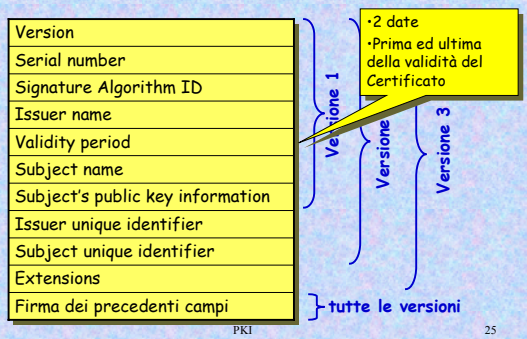
- Algoritmo usato per firmare il Certificato
- parametri associati
- Informazione ripetuta, campo poco importante

tutte le versioni

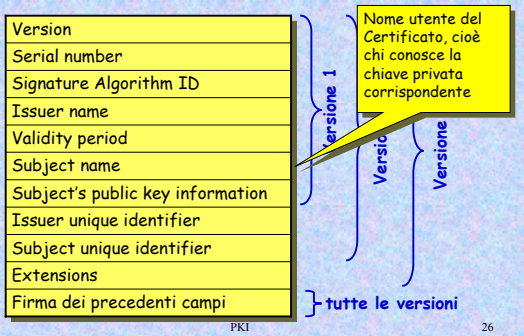
Campi Certificati X.509



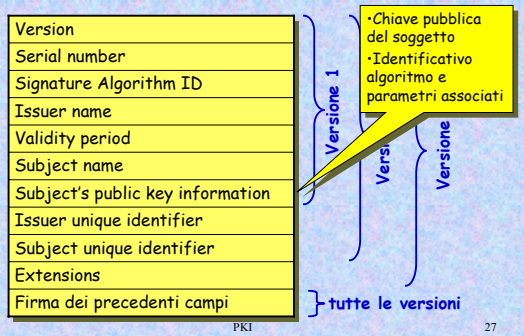
Campi Certificati X.509



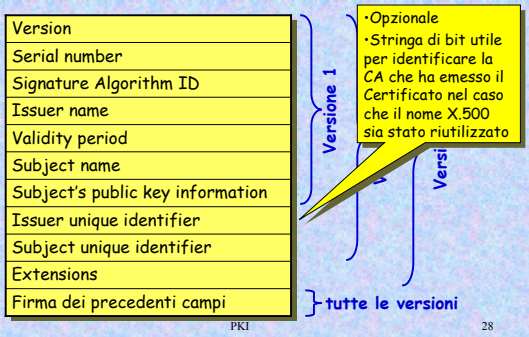
Campi Certificati X.509



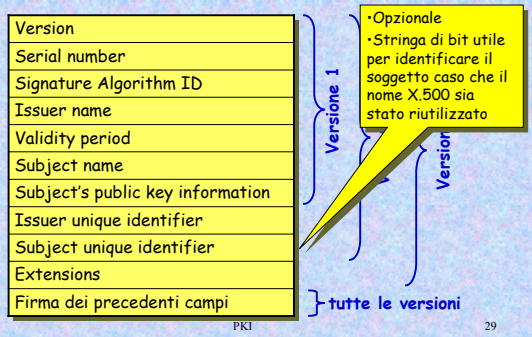
Campi Certificati X.509



Campi Certificati X.509



Campi Certificati X.509



Campi Certificati X.509

Version
Serial number
Signature Algorithm ID
Issuer name
Validity period
Subject name
Subject's public key information
Issuer unique identifier
Subject unique identifier
Extensions
Firma dei precedenti campi

Versione 1

Versione 3

Diversi campi di estensione

tutte le versioni

Campi Certificati X.509

Version
Serial number
Signature Algorithm ID
Issuer name
Validity period
Subject name
Subject's public key information
Issuer unique identifier
Subject unique identifier
Extensions
Firma dei precedenti campi

Versione 1

Versione 3

- Firma dell'hash di tutti gli altri campi
- Include "Signature Algorithm Identifier"

tutte le versioni

Esempio

```
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:a3:0e:
                    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:
            8d: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
```


Certificato in 64-byte-encoded form

```
-----BEGIN CERTIFICATE-----
MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJVUzER
MA8GA1UEChMITmV0c2NhcGUxFTATBgNVBAsTDFN1cHJpeWEncyBDQTAeFw05NzEw
MTgwMTM2MjVaFw05OTEwMTgwMTM2MjVaMEgxCzAJBgNVBAYTAlVTMREwDwYDVQQK
EwhOZXRzY2FwZTENMAsGA1UECxMEUHViczEXMBUGA1UEAxMOU3Vwcml5YSBTaGV0
dHkwgZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRJgEjmKiqG
7SdATYazBcABu1AVyd7chRkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7L
iQZBcrXpc0k4du+2Q6xJu2MPm/8WKuMOnTuvzpo+SGXelmHVChEqooCwfdiZywyZ
NMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCGSAGG+EIBAQQEAwIAgDAfBgNV
HSMEGDAWgBTy8gZZkBhHUfWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAOBgQBt
I6/z07Z635DfzX4XbAFpjlRl/AYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf91o3j3
UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uvi00mJYw8W2wUOsY0RC/a/IDy84
hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd1A==
-----END CERTIFICATE-----
```


Notazione dello standard

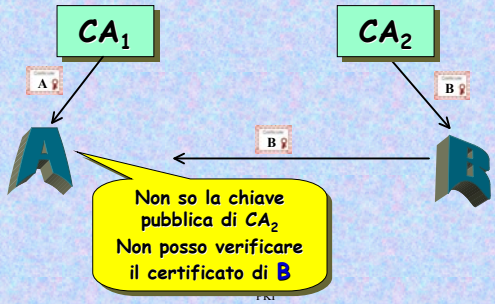
Y<<X>>

certificato utente X creato dalla Autorità Y

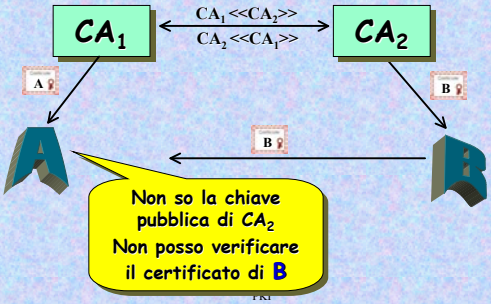
Y{I}

I con firma del proprio hash da parte di Y

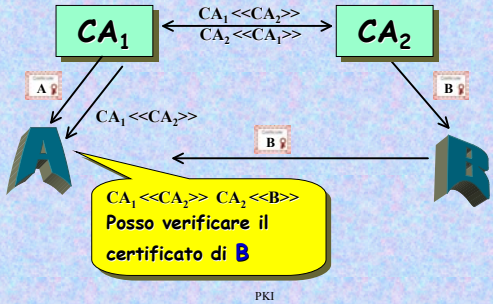
Diverse CA



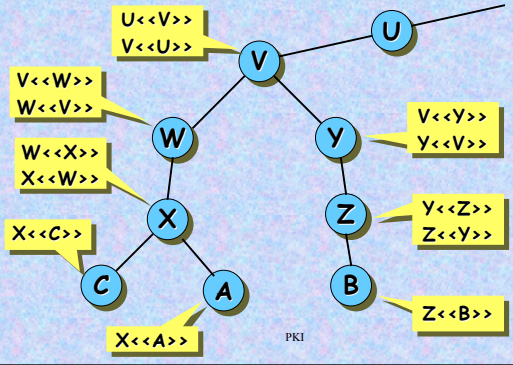
Diverse CA



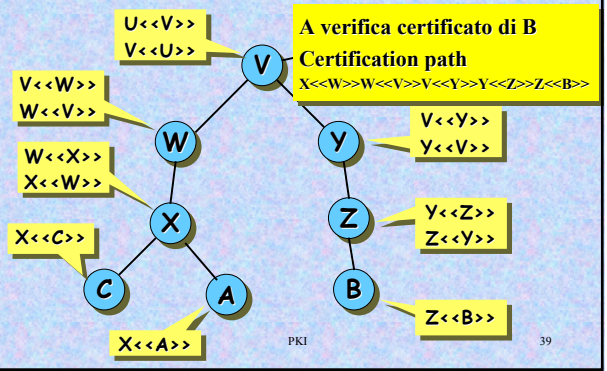
Diverse CA



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 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

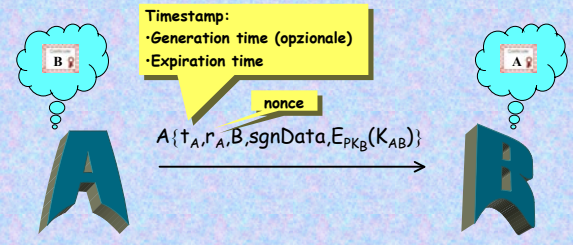
Certificato revocato

Certificato revocato

Autenticazione X.509

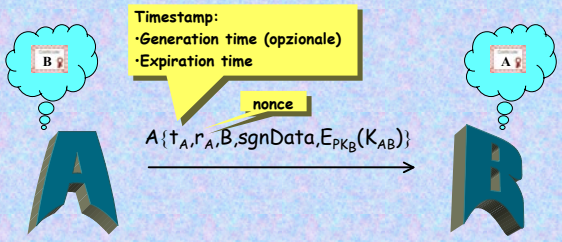
- Tre procedure di autenticazione:
  - Autenticazione One-way
  - Autenticazione Two-way
  - Autenticazione Three-way
- Assumiamo che A e B conoscano le chiavi pubbliche
  - Scambio dei certificati come primo messaggio
  - Certificati ottenuti dalla directory

Autenticazione One-way



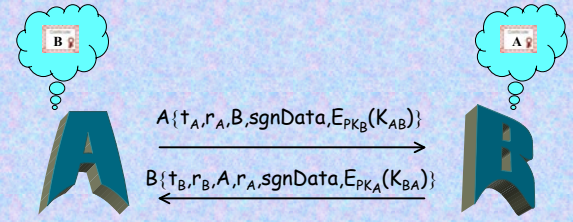
Nonce unico fino all'expiration time, per evitare attacchi di replay

Autenticazione One-way



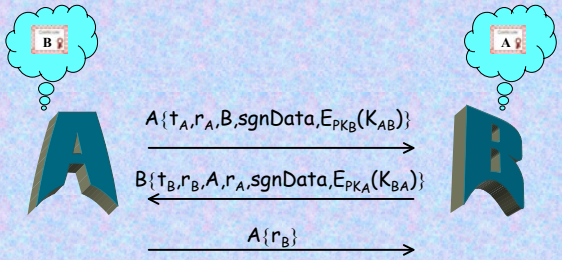
Messaggio di A
Diretto a B
Integrità ed originalità messaggio

Autenticazione Two-way



Messaggio di B
Diretto ad A
Integrità ed originalità messaggio

Autenticazione Three-way



Timestamp inutili ora

X.509 versione 3

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

- Subject field non adequato: nomi X.509 sono corti, e mancano dettagli identificativi che potrebbero essere utili
- Subject field non adequato per le applicazioni che riconoscono entità dall'indirizzo email, URL, o identificazione collegata ad Internet
- 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 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, nonrepudation, 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., mail elettronica, EDI, 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

Public Key Infrastructures (PKI)

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

NIST, Introduction to Public Key Technology and the Federal PKI Infrastructure, feb 2001

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

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 – Definizioni

1. Ai fini del presente regolamento s'intende:

a) per firma digitale, il 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) per certificazione, il 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) per certificatore, il 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 - Efficacia probatoria del documento informatico

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 - Certificazione

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.

Certificatori attivi

- **Società Interbancaria per l'Automazione - Cedborsa S.p.A. (SIA S.p.A.)** (Iscritto dal 27/01/2000)
- **SSB S.p.A.** (Iscritto dal 24/02/2000)
- **BNL Multiservizi S.p.A.** (Iscritto dal 30/03/2000)
- **Infocamere SC.p.A.** (Iscritto dal 06/04/2000)
- **Finital S.p.A.** (Iscritto dal 13/04/2000)
- **Saritel S.p.A.** (Iscritto dal 20/04/2000)
- **Postecom S.p.A.** (Iscritto dal 20/04/2000)
- **Società per Azioni Servizi Centralizzati - Seceti S.p.A.** (Iscritto dal 06/07/2000)
- **Centro Tecnico per la RUPA** (Iscritto dal 15/03/2001)
- **In.Te.S.A. S.p.A.** (Iscritto dal 22/03/2001)

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.