

Sicurezza: necessità

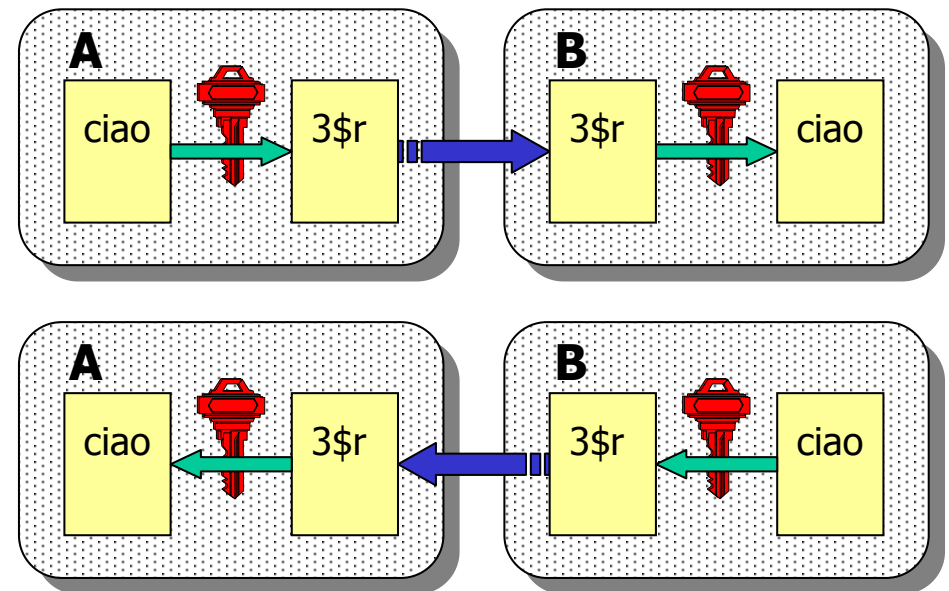
- **Riservatezza:** la comunicazione è stata intercettata?
- **Autenticazione:** l'utente è veramente chi dice di essere?
- **Autorizzazione:** ogni utente può accedere solo alle risorse cui ha diritto.
- **Integrità:** i dati ricevuti sono proprio quelli spediti?
- **Non ripudio:** il mio interlocutore può ritrattare quello che ha detto?
- **Disponibilità:** il mezzo di comunicazione è stato reso inutilizzabile?

Crittografia

- La crittografia risponde alle esigenze di sicurezza.
 - Riservatezza: cifratura.
 - Autenticazione: firma digitale e certificati.
 - Integrità: *one-way hash (message digest)*.
 - Non ripudio: integrità e autenticazione.

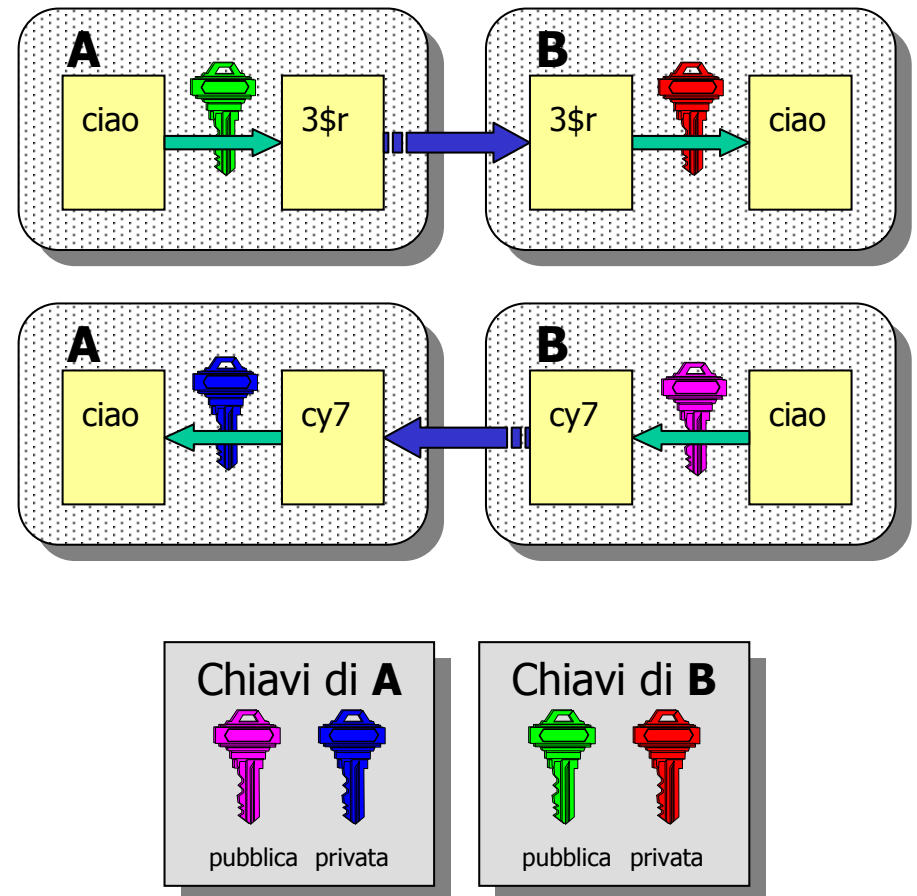
Cifratura a chiave privata

- Richiede una chiave *segreta* nota solo ai corrispondenti.
- La **stessa** chiave serve per cifrare e decifrare il messaggio.
- Pro
 - veloce;
 - fault tolerant.
- Contro
 - come distribuire le chiavi in modo sicuro?
 - il numero delle chiavi da gestire è $O(n^2)$.



Cifratura a chiave pubblica

- Ogni utente ha due chiavi: una *privata* ed una *pubblica*:
 - dalla chiave pubblica è *praticamente impossibile* scoprire quella privata;
 - quello che si cifra con una, si può decifrare **solo** con l'altra.
- Pro
 - Non è necessario nessuno scambio di chiavi segrete: il mittente cifra con la chiave pubblica del destinatario e il destinatario decifra con la propria chiave privata;
 - le chiavi da gestire sono $O(n)$.
- Contro
 - lento.

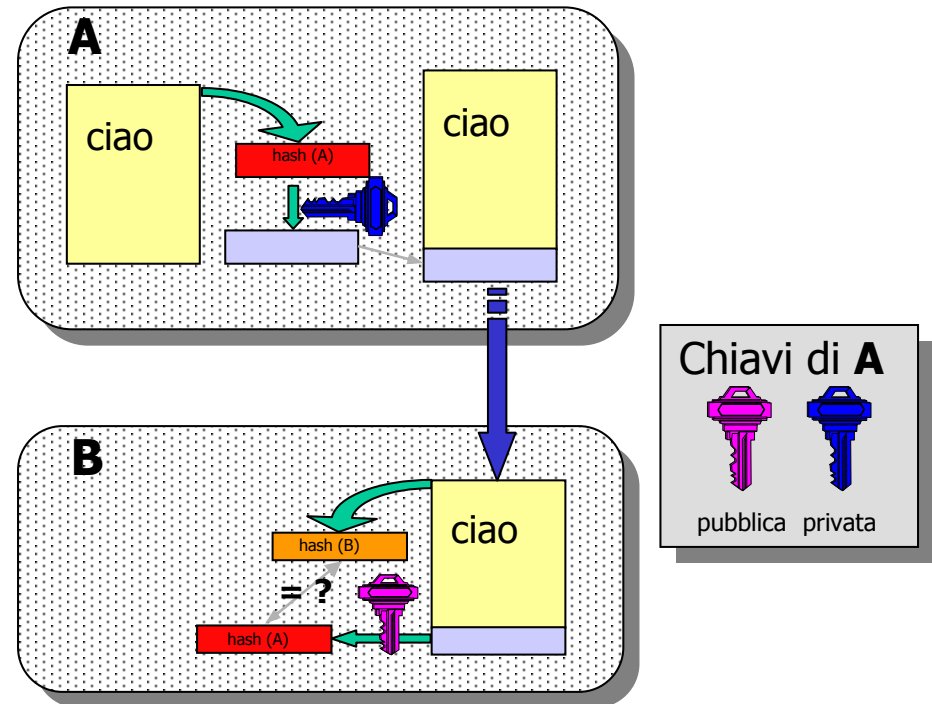


Integrità: *one-way hash*

- Funzioni (H) che hanno in ingresso un messaggio di lunghezza variabile (M) e producono una stringa di lunghezza **fissa**: *hash* (h);
 - dato M , deve essere facile calcolare $h = H(M)$;
 - dato h , deve essere difficile trovare $M = H^{-1}(h)$;
 - dato M , deve essere difficile trovare M' tale che: $H(M) = H(M')$.
 - h di almeno 128 bit (per resistere ai *birthday attack*).
- Algoritmi più comuni:
 - SNEFRU: hash di 128 o 256 bit;
 - MD4/MD5: hash di 128 bit;
 - SHA (Standard FIPS): hash di 160 bit.

Autenticazione: firma digitale

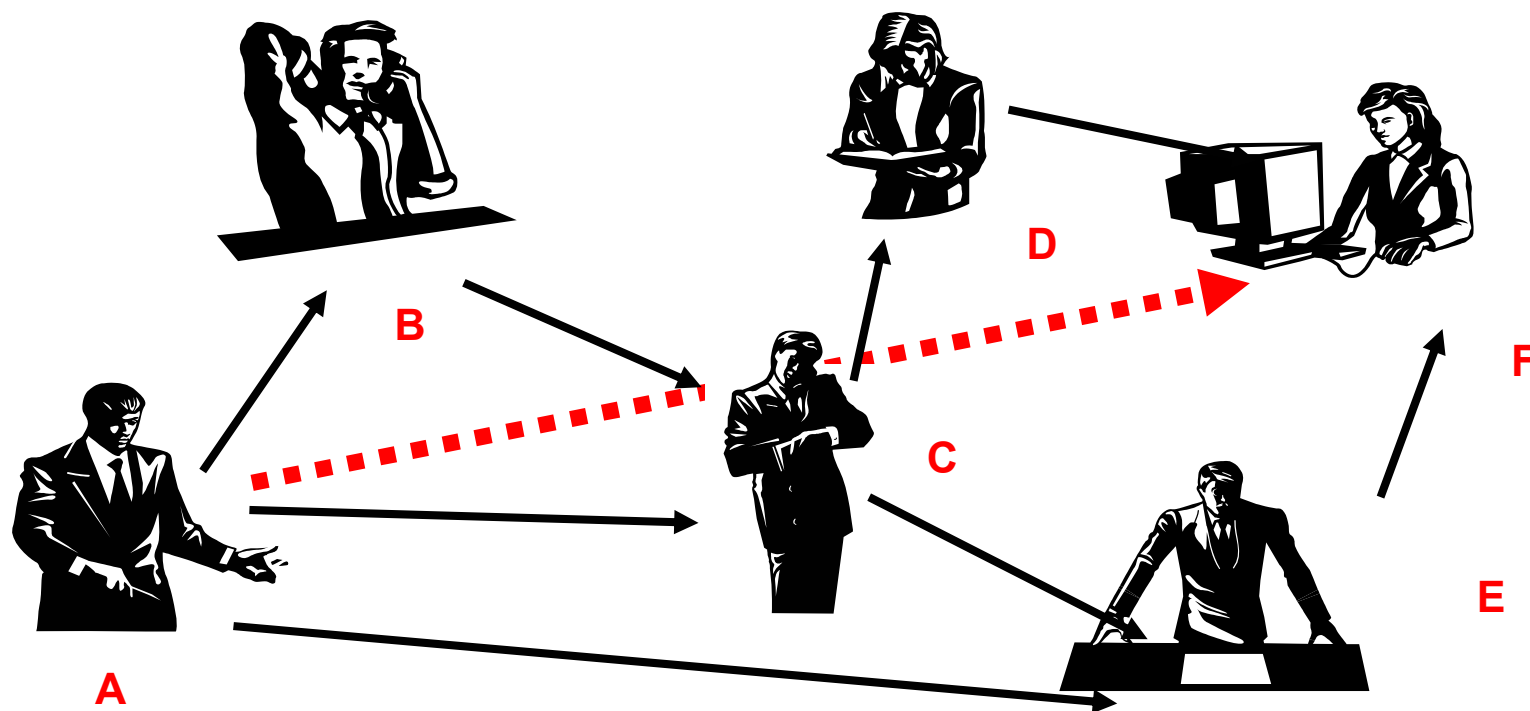
- **A** calcola l'hash del messaggio e lo cifra con la sua chiave **privata**: l'hash cifrato è la **firma digitale**.
- **A** invia il messaggio firmato a **B**.
- **B** ricalcola l'hash sul messaggio e lo confronta con quello inviato, dopo averlo decifrato con la chiave **pubblica** di A.
- Se i due hash sono uguali, il messaggio non è stato modificato e **A** non può ripudiarlo.



Autenticazione: Certificati

- La firma digitale rende sicuro un messaggio se:
 - la chiave privata di **A** non è stata compromessa;
 - **B** è in possesso della chiave pubblica di **A**;
 - **ma come può B essere certo di possedere la vera chiave di A?**
- La convalida dell'abbinamento tra dati anagrafici e chiavi pubbliche viene fatta tramite i **Certificati Digitali**: un'autorità esterna (*Certification Authority*) garantisce dell'autenticità delle chiavi pubbliche.
 - A e B devono fidarsi della Certification Authority.
- Due modelli principali:
 - X.509: organizzazione gerarchica;
 - PGP: "*web of trust*".

PGP "web of trust"



- F conosce D e E, che conosce A e C, che conosce A e B.
- F è ragionevolmente sicura che la chiave provenga da A.

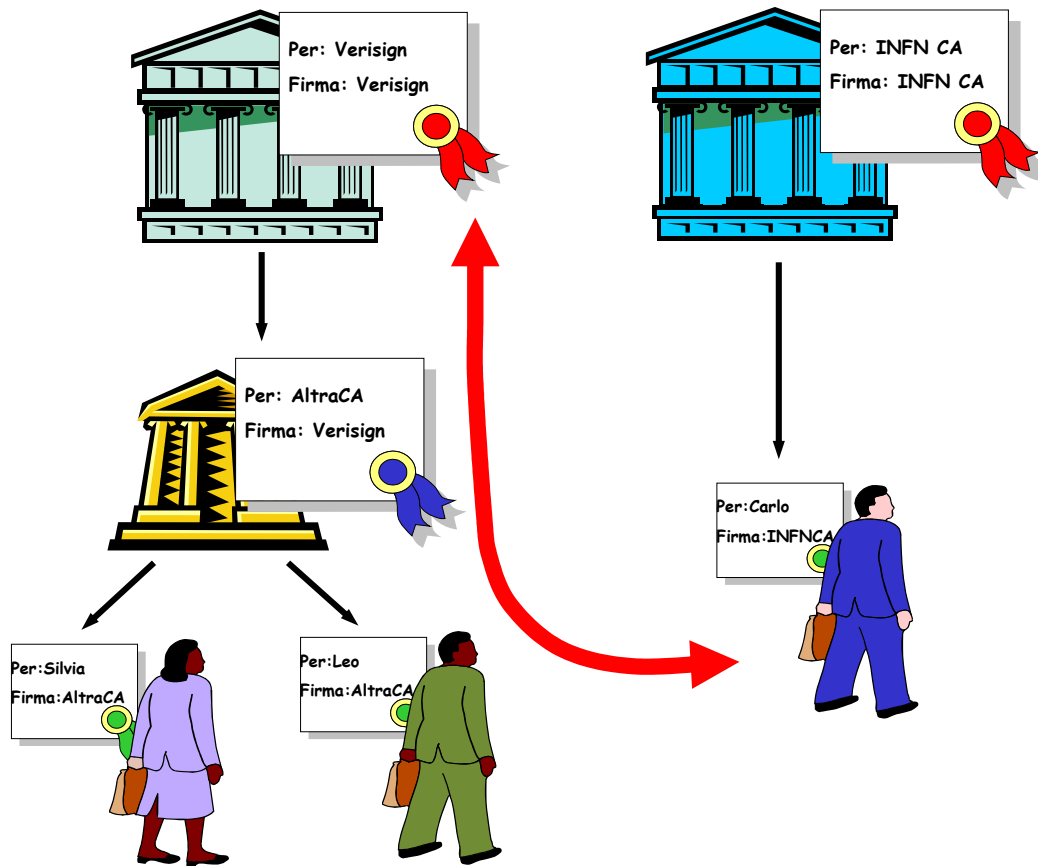
Certificati X.509

- Un certificato X.509 è composto fundamentalmente da:
 - informazioni sul proprietario;
 - la *data di scadenza*;
 - la chiave pubblica del proprietario;
 - informazioni sull'autorità garante (la *Certification Authority* o *CA*);
 - la firma della CA.
- I certificati sono pubblicati in una directory pubblica (ad es. LDAP o WWW) gestita dalla CA.

Revoca dei certificati

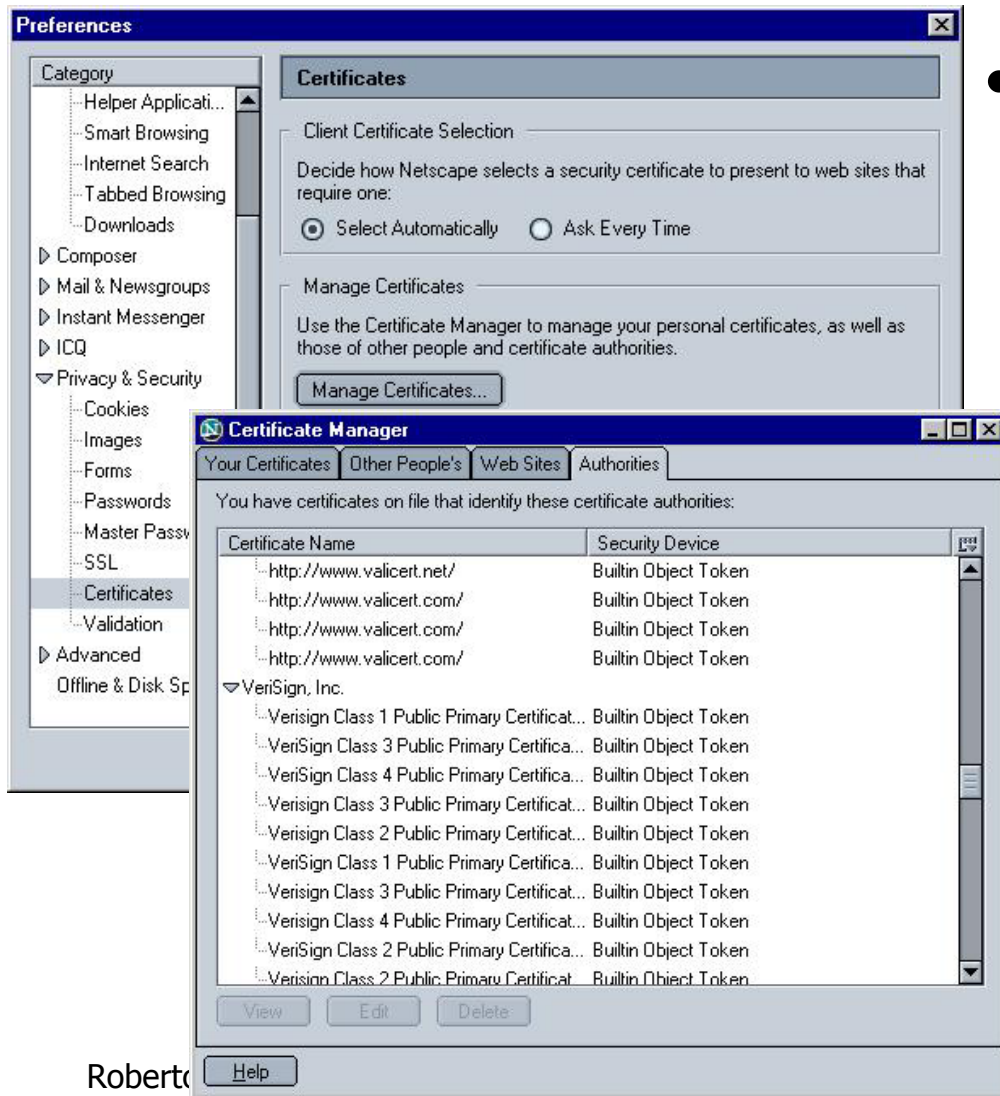
- Normalmente il legame tra identità e chiave pubblica vale per l'intero periodo di validità del certificato.
- Può essere necessario rescindere questo legame in anticipo (ad es. la chiave privata è stata persa).
- Una CA può (e **deve**) *revocare* un certificato non più valido:
 - **Certificate Revocation Lists** (CRL): liste di certificati revocati *firmate* dalla CA
 - possono essere scaricate nei browser
 - meccanismi di controllo interattivo dello stato del certificato, ad es. **Online Certificate Status Protocol** (OCSP).
- Fondamentale la diffusione dell'informazione.

CA: catene gerarchiche e fiducia



- Anche le CA hanno un proprio certificato.
- Una CA può garantire anche altre CA, di livello inferiore:
 - catene gerarchiche di certificati.
- All'origine della catena c'è una **Root CA**, che ha un certificato *auto-firmato* (**root certificate**).
- I certificati delle CA sono largamente pubblicizzati, quindi difficili da falsificare.

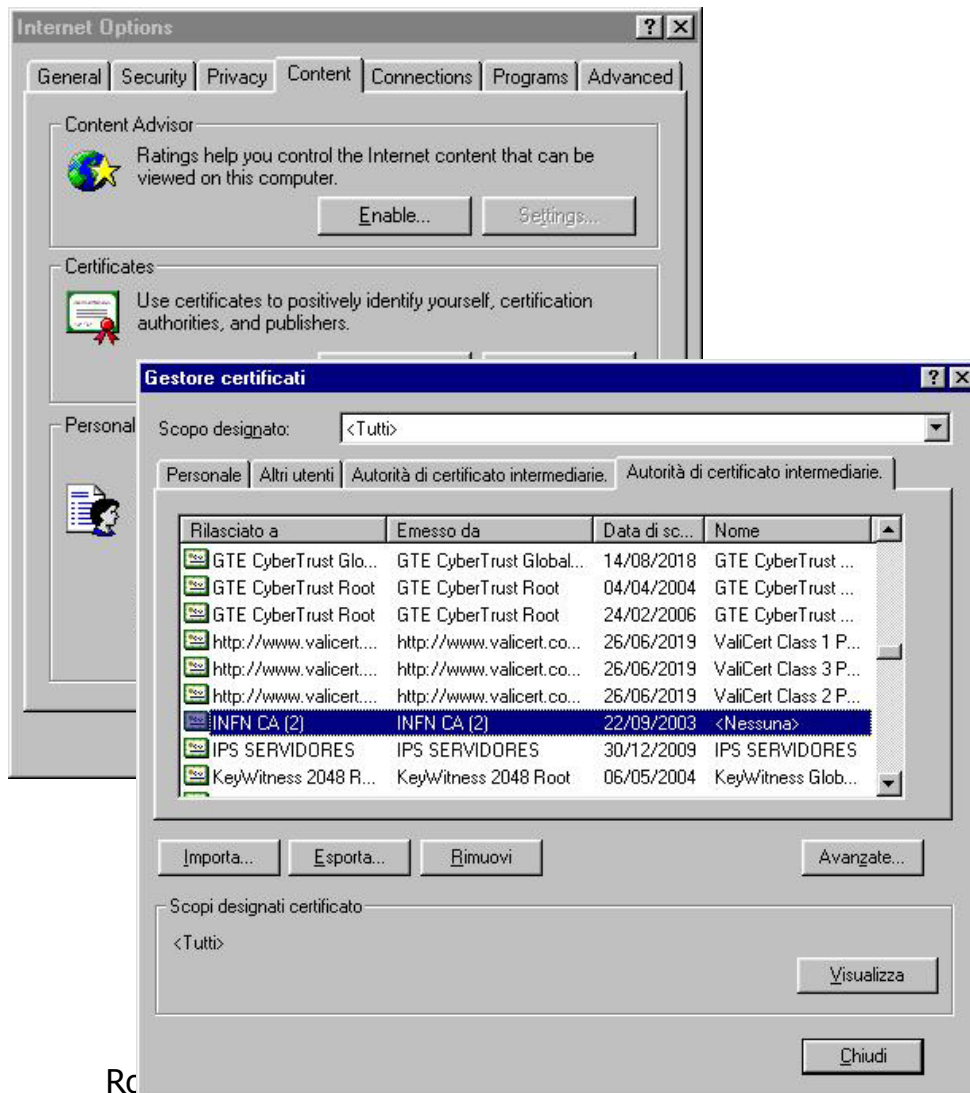
Certificati X.509: root CA (Netscape)



- I browser contengono preinstallati alcuni *root certificates*, visibili sotto **Certificates** nel menu **Edit/Preferences**.

Si possono aggiungere, eliminare e modificare i certificati.

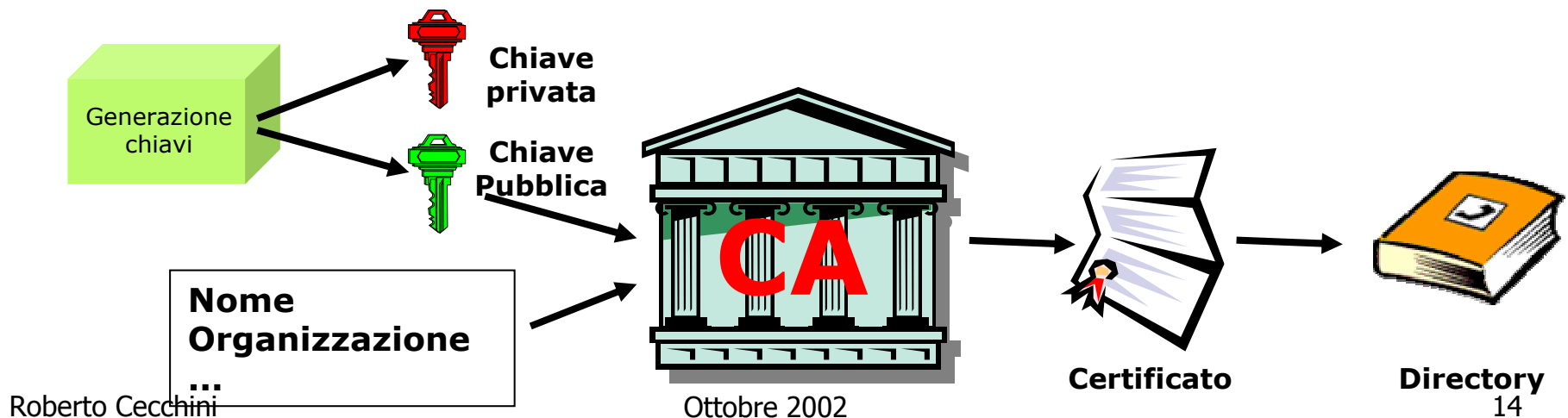
Certificati X.509: root CA (Explorer)



- I browser contengono preinstallati alcuni *root certificates*, visibili sotto **Certificates** nel menu **Tools/Internet Options**.
- Si possono aggiungere, eliminare e modificare i certificati.

Certificati X.509: come si ottengono

- ❶ **A** sceglie una Certification Authority e se ne procura il certificato;
- ❷ **A** genera una coppia di chiavi: pubblica e privata;
- ❸ **A** sottopone una richiesta di certificato alla CA scelta;
- ❹ la CA verifica che la richiesta provenga veramente da **A**;
- ❺ la CA emette il certificato per **A** e lo pubblica.



Certificati X.509: come si usano

- **B** vuole scambiare messaggi “sicuri” con **A**:
 - si procura il certificato di **A** (e i certificati della catena di CA di **A** che ancora non possiede);
 - verifica la validità del certificato di **A** (una tantum):
 - decifra l’hash del certificato di **A** con la chiave pubblica della CA di **A** (ricavata dal certificato di quest’ultima);
 - calcola l’hash del certificato di **A**;
 - controlla che i due hash, quello calcolato e quello decifrato, siano uguali;
 - controlla la data di scadenza;
 - verifica che il certificato di **A** non sia revocato o sospeso;
 - usa il certificato di **A** per:
 - verificare la firma dei messaggi che riceve da **A**;
 - cifrare i messaggi per **A**.

La pratica (X509)

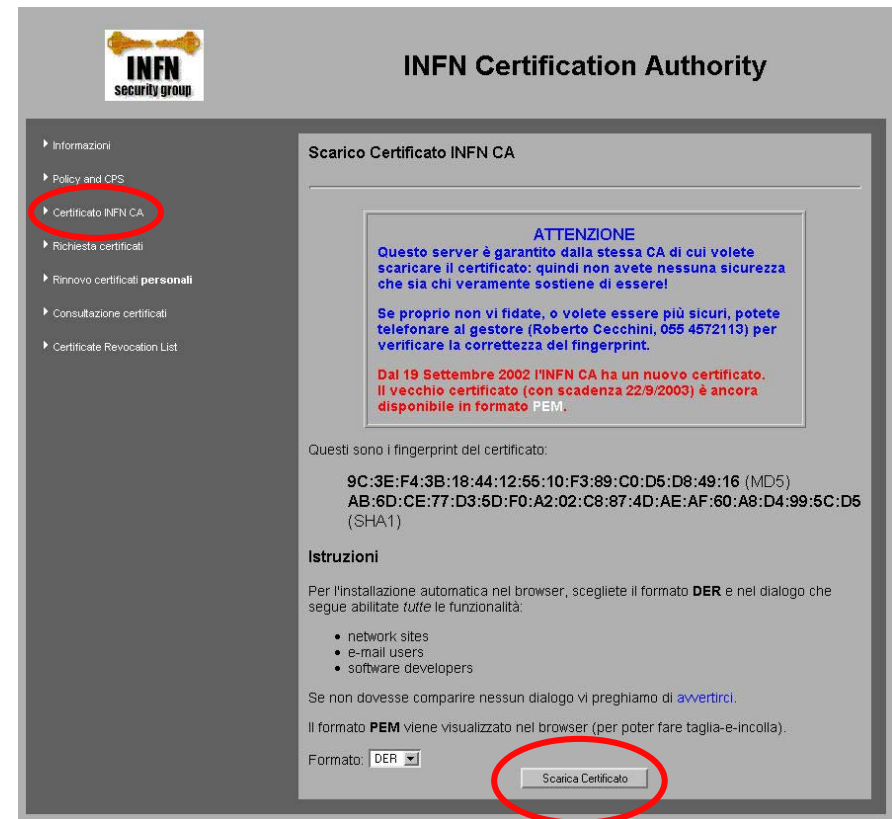
- Applicazioni:
 - autenticazione di un server web da parte dei clienti e cifratura dei dati trasmessi:
 - pagamenti online;
 - autenticazione dei clienti da parte del server web e cifratura dei dati trasmessi:
 - accesso a dati riservati senza dover digitare password;
 - autenticazione e cifratura di messaggi.

Ottenere un certificato personale

- Scaricare il certificato dell'INFN CA
- Richiedere il certificato utente
- Attendere la verifica da parte dell'INFN CA
- Scaricare il certificato via web
- Proteggere il certificato
- Fare una copia di salvataggio

Scaricare il certificato dell'INFN CA 1/2

- <http://security.fi.infn.it/CA/>
- Cliccare su **Certificato INFN CA**
 - ignorare eventuali messaggi di avvertimento sul fatto che ci si sta collegando ad un sito di cui non si possiede il certificato
- Cliccare su Scarica Certificato



INFN Certification Authority

Scarico Certificato INFN CA

ATTENZIONE
Questo server è garantito dalla stessa CA di cui volete scaricare il certificato: quindi non avete nessuna sicurezza che sia chi veramente sostiene di essere!
Se proprio non vi fidate, o volete essere più sicuri, potete telefonare al gestore (Roberto Cecchini, 055 4572113) per verificare la correttezza del fingerprint.

Dal 19 Settembre 2002 l'INFN CA ha un nuovo certificato. Il vecchio certificato (con scadenza 22/9/2003) è ancora disponibile in formato PEM.

Questi sono i fingerprint del certificato:

9C:3E:F4:3B:18:44:12:55:10:F3:89:C0:D5:D8:49:16 (MD5)
AB:6D:CE:77:D3:5D:F0:A2:02:C8:87:4D:AE:AF:60:A8:D4:99:5C:D5 (SHA1)

Istruzioni

Per l'installazione automatica nel browser, scegliete il formato **DER** e nel dialogo che segue abilitate tutte le funzionalità:

- network sites
- e-mail users
- software developers

Se non dovesse comparire nessun dialogo vi preghiamo di avvertirci.

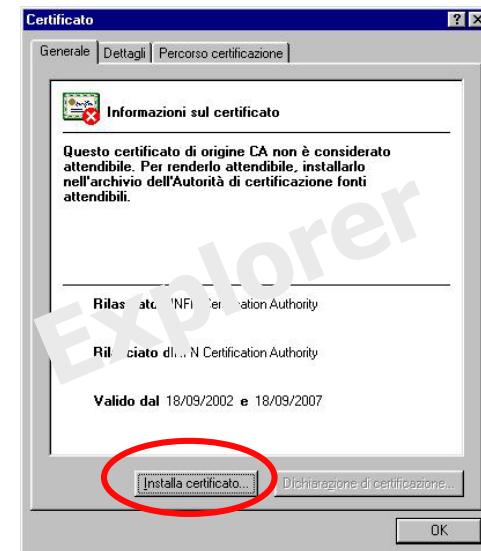
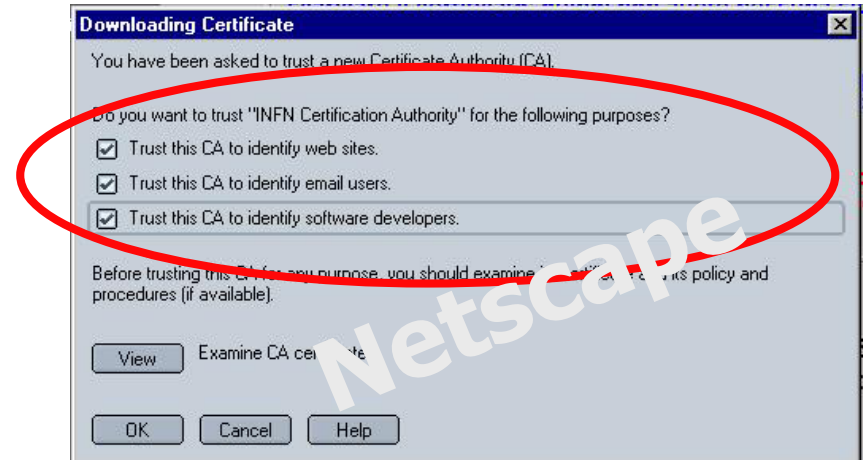
Il formato **PEM** viene visualizzato nel browser (per poter fare taglia-e-incolla).

Formato: DER

Scarica Certificato

Scaricare il certificato dell'INFN CA 2/2

- Netscape:
 - sulla finestra che compare abilitare tutte e tre le opzioni
- Explorer:
 - salvare su disco con estensione **.der**
 - aprire il file salvato e selezionare **Installa certificato** sulla finestra che compare
 - proseguire scegliendo sempre il default
- Controllare che il certificato compaia tra i "root certificates"



Richiedere il certificato utente

- Recarsi dalla propria RA (<https://security.fi.infn.it/CA/RA>) per l'autenticazione
- <http://security.fi.infn.it/CA/>
- Cliccare su **Richiesta certificati**
- Riempire i dettagli del certificato:
 - Nome sezione;
 - Nome e Cognome;
 - Indirizzo di e-mail: **deve** essere quello ufficiale, Nome.Cognome@sezione.infn.it.
 - Numero di autenticazione fornito dalla RA (non visibile in figura)
- Cliccare **Sottometti Richiesta**.
- Se va tutto bene compare una pagina che informa dell'avvenuta sottomissione.
- All'indirizzo della richiesta verrà spedito un messaggio con l'URL da aprire per completare lo scarico.

Richiesta certificato personale

Chi non lo avesse ancora fatto deve [scaricare il certificato della INFN Certification Authority](#).

Per richiedere un certificato è necessario riempire *tutti* i campi seguenti e premere il bottone "**Sottometti richiesta**".

Per i dipendenti e associati INFN l'indirizzo di e-mail **deve** essere della forma *[Nome.]Cognome@sezione.infn.it*.

ATTENZIONE

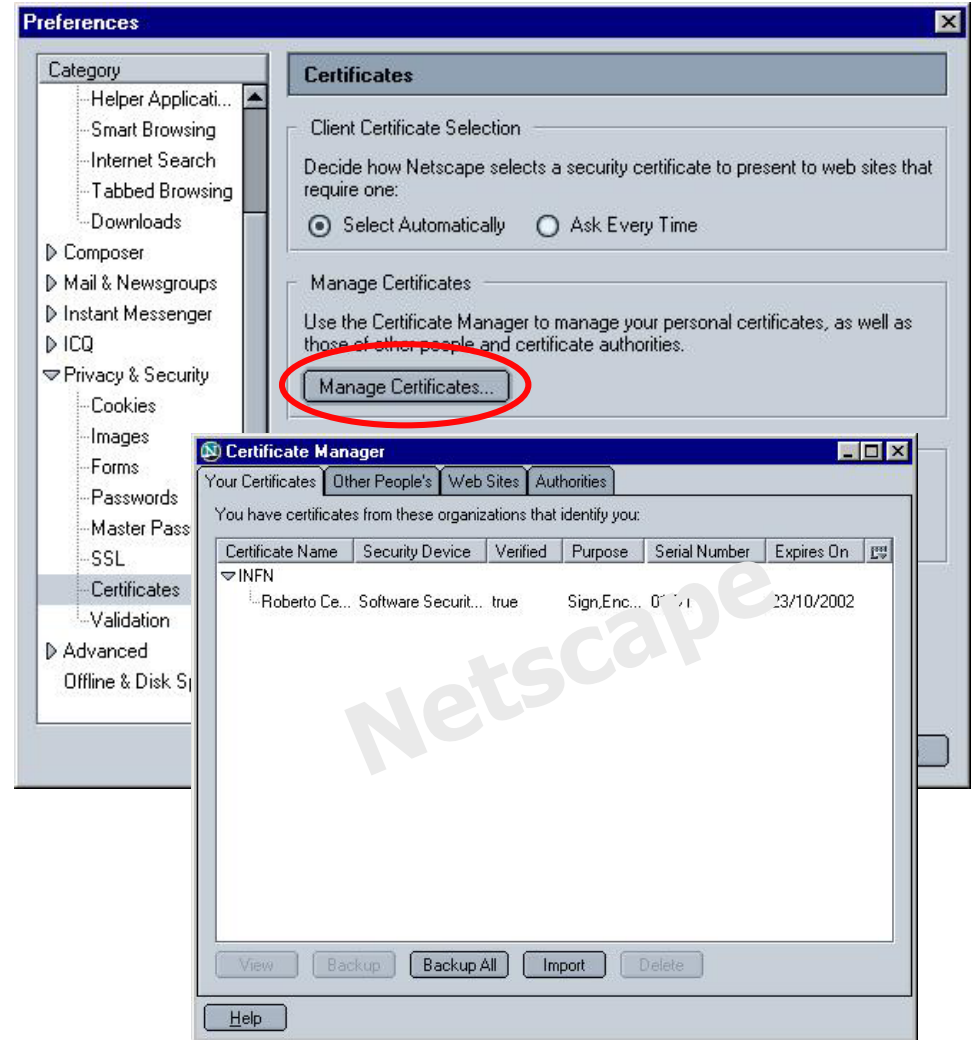
L'attuale CPS prevede un controllo telefonico da parte nostra prima del rilascio del certificato. Se il nominativo del richiedente non compare in un elenco telefonico ufficiale, è richiesto un messaggio di conferma **firmato** da un possessore di certificato rilasciato da questa CA, da inviare a <infn-ca@fi.infn.it>.

A firma avvenuta verrà inviato un messaggio di e-mail con le istruzioni per lo scarico del certificato.

Sezione:	<input type="text"/>
Nome e Cognome:	<input type="text"/>
E-mail:	<input type="text"/>
KeySize:	2048 (High Grade) <input type="text"/>

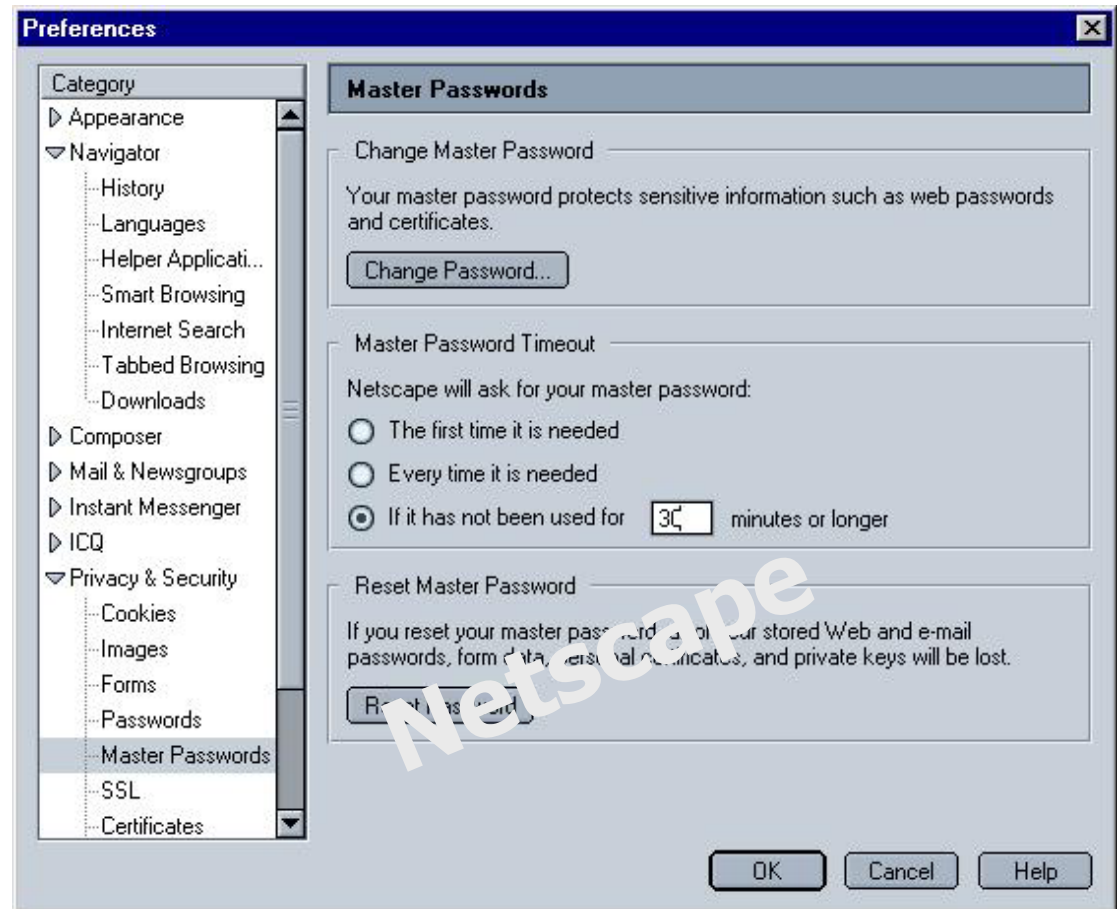
Scaricare il certificato personale

- Aprire l'URL comunicata nel mail dall'INFN-CA **con lo stesso browser da cui è stata fatta la richiesta**
- Controllare che il certificato appaia nel database del proprio browser



Proteggere il certificato

- Per evitare l'uso non autorizzato del proprio certificato è opportuno proteggerlo con una password (da non dimenticare!)



Fare una copia di salvataggio

- Salvare il proprio certificato su un floppy (meglio due...)
- Proteggere la copia salvata con una password (viene richiesta durante la procedura di export)
- La copia salvata può essere poi importata in un altro browser

