

# **GARR CERTIFICATION AUTHORITY**

**Corso per Utenti e Registration Authority**

# Agenda

- ▶ 09:30 – 11:00 Istruzioni per Utenti
- ▶ 11:00 Coffee break
- ▶ 11:30 – 12:45 Istruzioni per Registration Authority
- ▶ 12:45 – 13:00 Autenticazioni



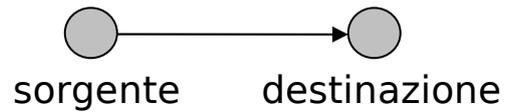
# Sessione Utenti

- ▶ Elementi di crittografia
- ▶ Certificati digitali X.509
- ▶ Procedure operative per gli utenti
- ▶ Uso dei certificati nei dispositivi client
- ▶ Comandi OpenSSL
- ▶ Procedure operative per i server
- ▶ SCS (per amministratori)

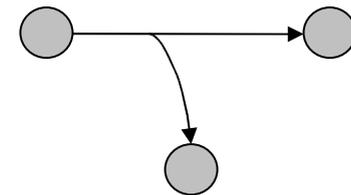
# Attacchi

- Azioni che compromettono la sicurezza dei dati

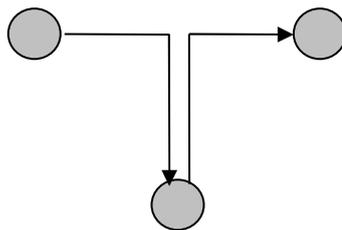
Trasmissione regolare



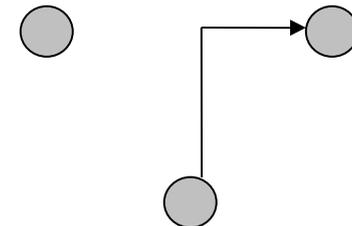
Interruzione



Intercettazione



Modifica



Fabricazione

# Servizi

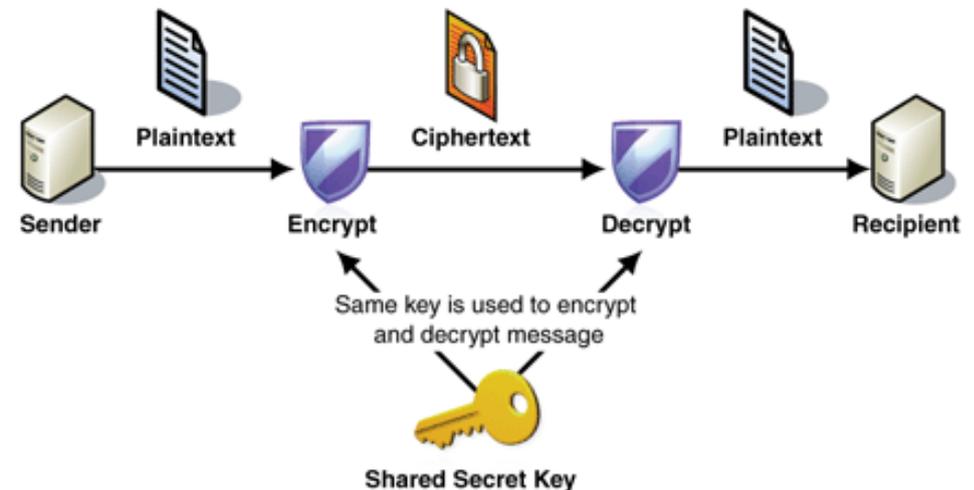
- **Autenticazione:** verificare l'identità di un soggetto
- **Autorizzazione:** controllo degli accessi
- **Non ripudio:** impedire al mittente e al destinatario di disconoscere i dati trasmessi
- **Riservatezza:** garantire che i dati in un sistema e i dati trasmessi siano accessibili solo a chi autorizzato
- **Integrità:** garantire che i dati in un sistema e i dati in transito non siano modificati da terzi
- **Disponibilità:** garantire che i dati siano disponibili ai soli autorizzati quando richiesto

# Meccanismi

- **Crittografia**
  - Convenzionale: a chiave segreta
  - Chiave pubblica: coppia di chiavi pubblica – privata
- **Funzioni di autenticazione del messaggio**
  - Cifratura del messaggio
  - Message Authentication Code (MAC)
  - Funzioni Hash
- **Firma digitale**

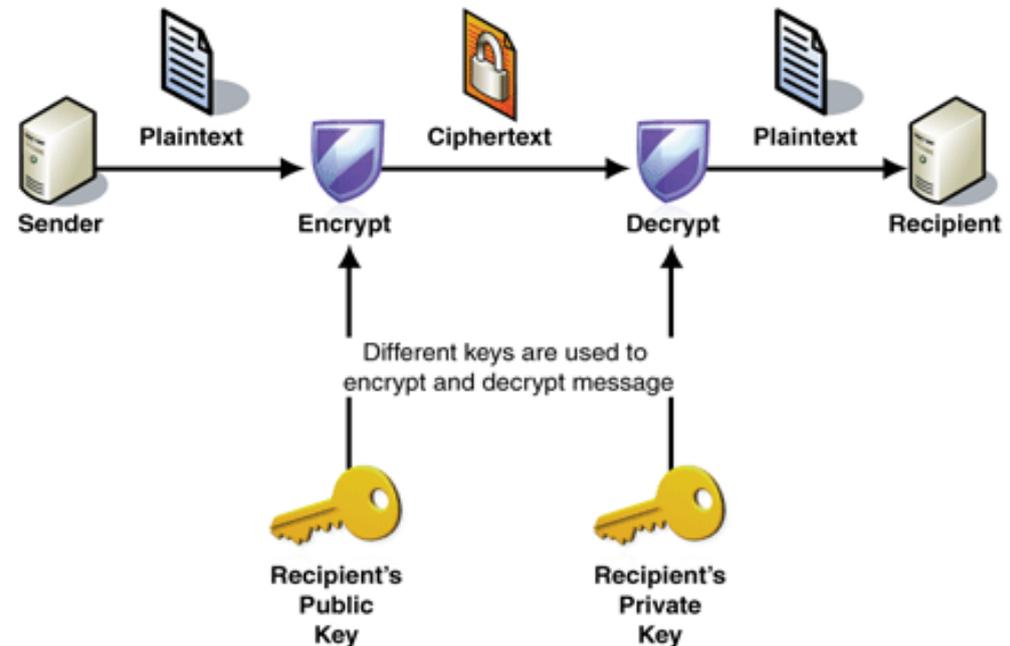
# La crittografia a chiave segreta

- ♦ Richiede una chiave *segreta* nota solo ai corrispondenti
- ♦ La stessa chiave è usata per cifrare e decifrare il messaggio
- ♦ Vantaggio: è veloce
- ♦ Problemi:
  - scambio sicuro di chiavi
  - il numero delle chiavi da gestire è  $O(n^2)$



# La crittografia a chiave pubblica

- ♦ Ogni utente ha due chiavi:
  - pubblica e privata
    - dalla chiave pubblica è praticamente impossibile scoprire quella privata
    - ciò che si cifra con una chiave si decifra solo con l'altra
- ♦ Vantaggi:
  - non c'è scambio di chiavi
  - le chiavi sono  $O(n)$
- ♦ Problema: è lento



# Autenticazione del messaggio: Cifratura del testo e MAC

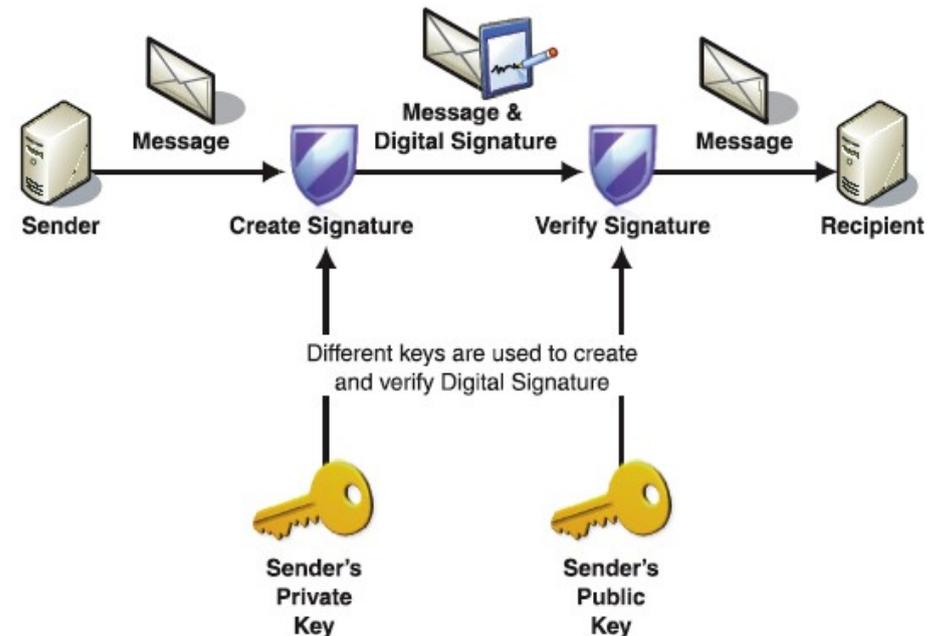
- Ha lo scopo di produrre un valore da usare per autenticare il messaggio (*authenticator*)
- **Message encryption:** il testo cifrato dell'intero messaggio funge da *authenticator*
  - crittografia convenzionale
  - crittografia a chiave pubblica
- **Message authentication code (MAC):** una funzione
  - applicata al messaggio e ad una chiave segreta -
  - funge da *authenticator*

# Autenticazione del messaggio: Funzioni Hash

- Lo scopo di queste funzioni è quello di produrre un'*impronta* di un messaggio (*authenticator*)
- Una funzione  $H$  deve avere le seguenti proprietà:
  - poter essere impiegata con blocchi di lunghezza variabile
  - produrre un output di **lunghezza fissa**
  - dato  $x$ , deve essere facile calcolare  $h = H(x)$
  - dato  $h$ , deve essere difficile calcolare  $x = H^{-1}(h)$  [**one-way**]
  - dato  $x$ , deve essere difficile trovare  $y$  tale che  $H(y) = H(x)$
  - deve essere computazionalmente impossibile trovare  $(x,y)$  t.c.  $H(y) = H(x)$

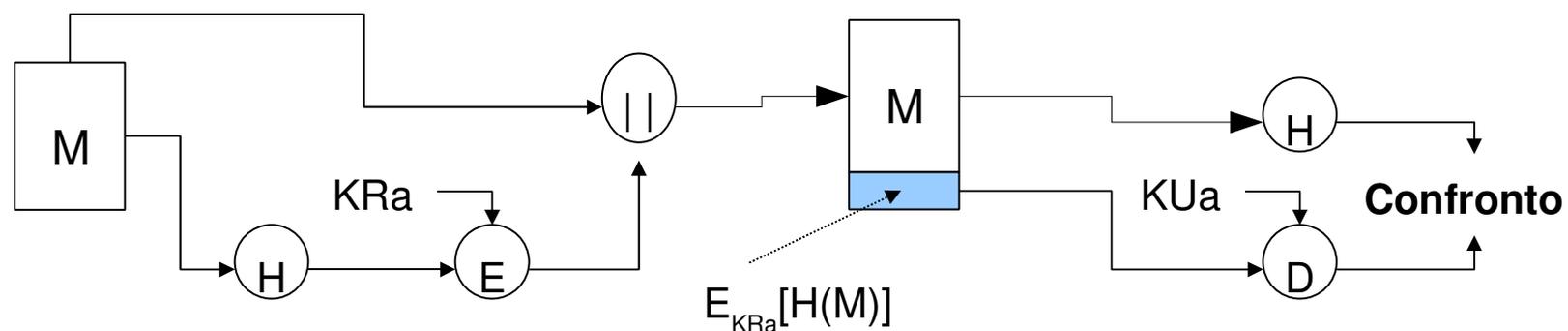
# Firma digitale: Cifratura + Hash

- Impiega il meccanismo di cifratura sull'hash del messaggio
- Garantisce:  
*Autenticazione* del messaggio e *Non Ripudio*
- Non garantisce:  
*Riservatezza*



# Firma digitale: come funziona

1. Il mittente calcola l'hash del messaggio e lo cifra con la propria chiave **privata**  $K_{Ra}$  (*firma*)
2. Il mittente inoltra il messaggio e la firma digitale al destinatario
3. Il destinatario ricalcola l'hash del messaggio in chiaro e lo confronta con quello ricevuto, dopo averlo decifrato con la chiave **pubblica**  $K_{Ua}$  del mittente
4. Se i due hash sono uguali il messaggio non è stato alterato



# Distribuzione delle chiavi

- Necessità:
  - diffondere liberamente le chiavi pubbliche
  - associare l'identità di un soggetto con la relativa chiave pubblica in maniera sicura
- Due modelli di fiducia principali:
  - **user-centric**: certificati PGP
  - **gerarchico**: certificati a chiave pubblica X.509

# I certificati digitali X.509

- Contengono varie informazioni
  - ad es.: nome, cognome, e-mail, città di residenza, affiliazione
  - la chiave pubblica (quella privata è conosciuta solo dal soggetto stesso)
  - la firma della CA che lo ha emesso
  - informazioni sulla CA
  - la durata del certificato in termini di validità
- Sono pubblicati su elenchi pubblici
  - server LDAP, server WEB ... gestiti dalla CA

# Struttura del certificato X.509 1/2

Firmata dalla CA  
(Issuer)

|         |               |           |        |          |         |                         |            |
|---------|---------------|-----------|--------|----------|---------|-------------------------|------------|
| Version | Serial Number | Signature | Issuer | Validity | Subject | Subject Public Key Info | Extensions |
|---------|---------------|-----------|--------|----------|---------|-------------------------|------------|

- **Version:** indica la versione del certificato (v1, v2, v3)
- **Serial Number:** identificativo univoco dato dalla CA emittente
- **Signature:** identifica l'algoritmo impiegato per calcolare la firma del certificato. Ad es. `sha1WithRSAEncryption`
- **Issuer:** il *Distinguished Name* DN di chi ha emesso il certificato (obbligatorio)

# Struttura del certificato X.509 2/2

- **Validity:** la finestra temporale durante la quale il certificato è valido a meno di revoca.
- **Subject:** il DN del proprietario del certificato (non nullo)
- **Subject Public Key info:** la chiave pubblica e l'identificativo dell'algoritmo
- **Extensions:** estensioni opzionali presenti solo nella v3
  - GARR-CA: Basic Constraints, Key Usage, Extended Key Usage, CRL Distribution Point, Certificate Policies, Subject Key Identifier, Authority Key Identifier, Subject Alternative Name.

# I formati dei file di certificato 1/3

- .CER - certificato codificato con metodo DER, talvolta può essere anche una sequenza di certificati
- .DER - certificato codificato con metodo DER
- DER acronimo di *Distinguished Encoding Rules* è un metodo per la codifica di oggetti contenenti dati, quali le richieste per certificati X.509, destinati ad essere firmati digitalmente o a subire un processo di verifica della firma digitale.

# I formati dei file di certificato 2/3

- .PEM - certificato codificato con schema Base64 e racchiuso dalle stringhe "-----BEGIN CERTIFICATE-----" e "-----END CERTIFICATE-----". Può contenere la chiave privata del certificato debitamente racchiusa da apposite linee BEGIN/END
- .PFX o .P12 - PKCS#12, può contenere sia il certificato che la chiave privata (protetta da password)
- PKCS #12 è uno standard nato come evoluzione del formato PFX (*Personal inFormation eXchange*) ed è utilizzato per lo scambio di oggetti pubblici e privati all'interno di un singolo file.

# I formati dei file di certificato 3/3

- PKCS #10 è uno standard per il formato dei messaggi di richiesta certificato (*Certification Request Standard*)
- .P7C - PKCS#7 conosciuto con il nome di Cryptographic Message Syntax è uno standard che definisce la struttura generale per i messaggi contenenti elementi crittografici quali firme digitali ed cifratura
- PKCS #7 è uno standard per "l'imbustamento" della firma o dell'oggetto cifrato. Per verificare un oggetto di tipo firma digitale è richiesto il certificato, il quale può essere incluso all'interno del file .P7C

# Revoca dei certificati

- Esistono circostanze che annullano la validità dei certificati prima della scadenza
  - cambiamento nei dati identificati
  - sospetta compromissione della chiave privata
- E' necessario revocare certificati non più validi:
  - **Certificate Revocation Lists - CRL**: liste di certificati revocati *firmate* dalla CA (integrità e autenticità)
    - Version 1: forma piu' semplice
    - Version 2: comprende estensioni (es. Reason Code, Invalidity Date)
  - meccanismi di controllo interattivo dello stato dei certificati (**Online Certificate Status Protocol – OCPS**)

# Struttura di una CRL

Firmata dalla CA  
(Issuer)

|                |                  |               |                    |                    |   |
|----------------|------------------|---------------|--------------------|--------------------|---|
| <b>Version</b> | <b>Signature</b> | <b>Issuer</b> | <b>Last Update</b> | <b>Next Update</b> | <b>... List of revoked Certificates ...</b> |
|----------------|------------------|---------------|--------------------|--------------------|---|

- **Version:** indica la versione della CRL (v1, v2)
- **Signature:** identifica l'algoritmo usato per calcolare la firma digitale della CRL
- **Issuer:** indica il DN di chi firma ed emette la CRL
- **Last - Next Update:** indica la data di emissione della CRL
- **Revoked Certificates:** riporta la lista dei certificati revocati indicandone il *Serial Number* e la data di avvenuta revoca

# GARR Certification Authority

- Sito internet <http://ca.garr.it/>
- Indirizzo e-mail [garr-ca@garr.it](mailto:garr-ca@garr.it)
- Spazio dei nomi (*Subject nel certificato*)

/C=IT/O=GARR/OU=<>/CN=<>

/C=IT/O=GARR/OU=<>/OU=<>/CN=<>

- Rilascia certificati: **personali** e per **server**
- Validità dei certificati: **1 anno**
- CRL: **Version 1**
- CP/CPS: disponibile in <https://ca.garr.it/CPS/>
- LDAP server: ca.garr.it

# Installazione certificato GARR CA

Home

Documentazione

Policy and CPS

Certificato GARR CA

Richiesta certificati **personali**

Rinnovo certificati **personali**

Consultazione certificati

Certificate Revocation List

Registration Authority (RA)

Statistiche

## Scarico Certificato GARR CA

Questi sono i fingerprint del certificato:

**FD:25:9C:0F:25:ED:1A:89:77:2D:18:45:CF:B0:95:EF (MD5)**  
**35:A1:4F:70:8D:35:4F:29:25:B9:7D:28:77:04:CF:0A:BD:C5:FE:CB (SHA1)**

### Istruzioni

- Per l'installazione automatica nel browser, premete il bottone "Scarica Certificato".  
In Netscape, Mozilla, Firefox e Camino nella finestra che comparirà abilitate *tutte* le funzionalità proposte:
  - network sites
  - e-mail users
  - software developersIn Opera procedete all'installazione seguendo le istruzioni nella finestra di dialogo che comparirà
- In alternativa il certificato è disponibile anche in formato PEM.

Scarica Certificato

- Selezionare il link **Certificato GARR CA**
- Seguire le istruzioni in base al browser impiegato
- Controllare nei Root Certificates

# Richiedere un Certificato Personale Autenticazione

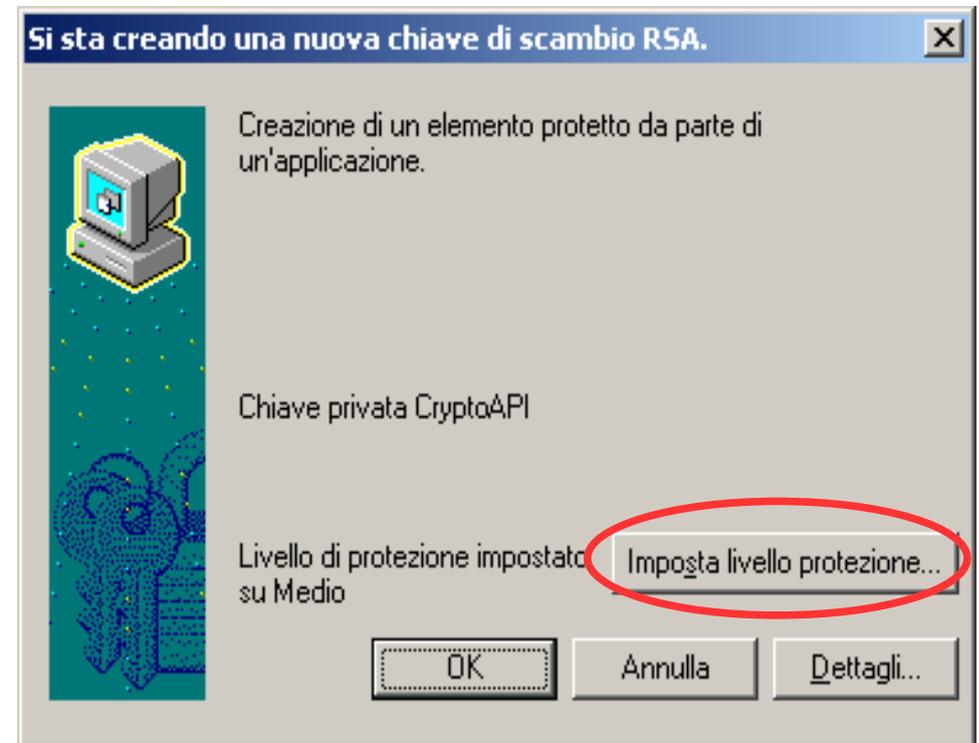
- L'utente si rivolge alla RA della struttura (o Unità Organizzativa **OU**) a cui afferisce
  - avviene un'autenticazione de-visu in cui l'utente comunica i propri dati e riceve un **codice numerico** di identificazione
  - il codice servirà per la richiesta on-line
- La lista delle RA abilitate è consultabile in <https://ca.garr.it/RA/>





# Richiesta con Internet Explorer

- Impostare il livello di protezione della chiave privata nel browser su **Alto**
- Quando richiesto immettere una nuova password di almeno 12 caratteri (doppia immissione)
- Annotare la password (in maniera sicura) per gli usi futuri del certificato



# Richiesta con Firefox

- Firefox possiede un Security Device da proteggere con una **Master Password**
- Quando richiesto immettere una nuova password di almeno 12 caratteri (doppia immissione)
- Annotare la password (in maniera sicura) per gli usi futuri del certificato



# Richiedere un Certificato Personale

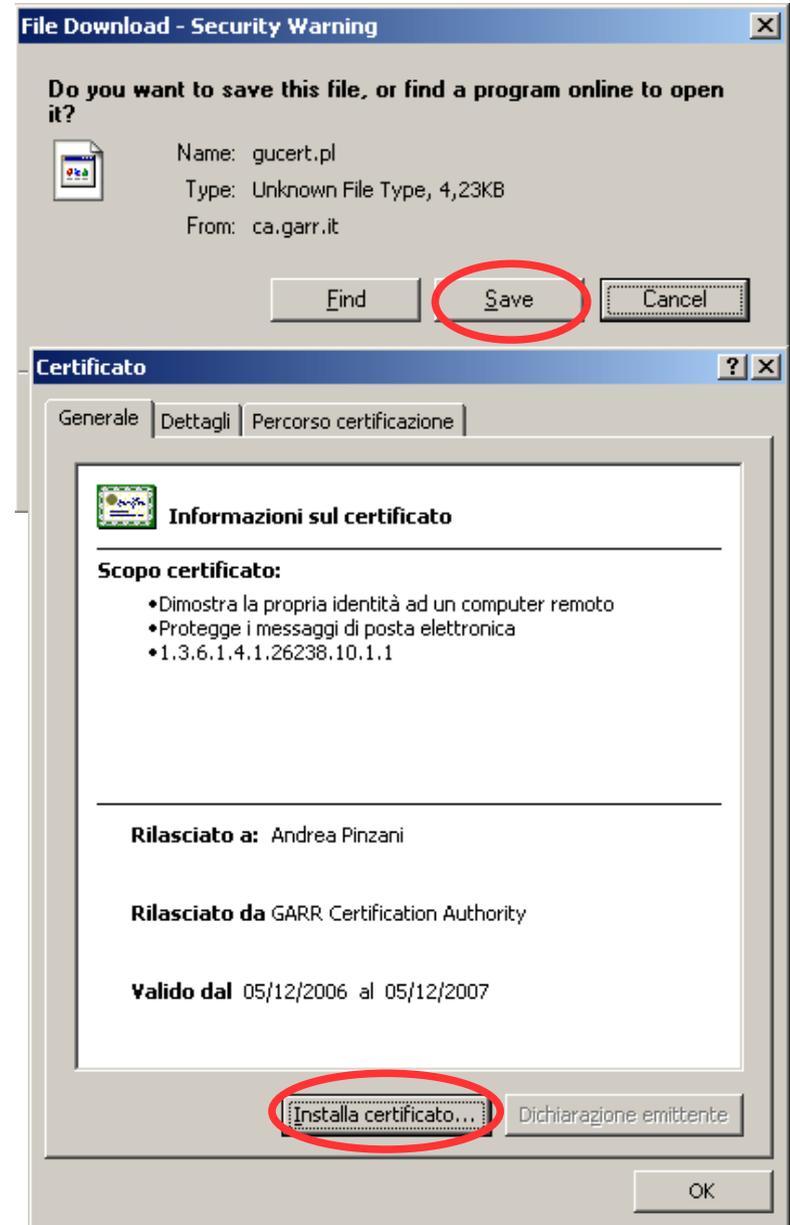
## Installazione

- Le istruzioni per scaricare il certificato sono contenute in una mail inviata dalla CA con oggetto:  
[GARR CA #n] Certificato per ...
- Il certificato emesso deve essere scaricato nel **browser** (lo stesso impiegato per la richiesta) da cui potrà essere successivamente esportato



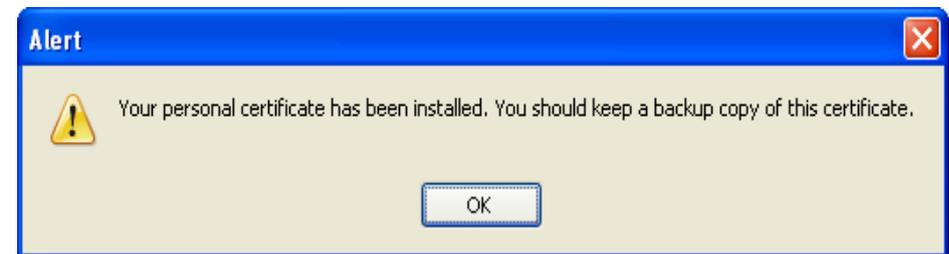
# Installazione in Internet Explorer

- Seguire il link indicato in fondo alla mail di istruzioni
- Salvare il file su disco come **<cert>.der** e riaprirlo con doppio click
- Nella finestra “Certificato” premere Installa ... per importare il certificato
- Inserire la password scelta in fase di richiesta se necessario



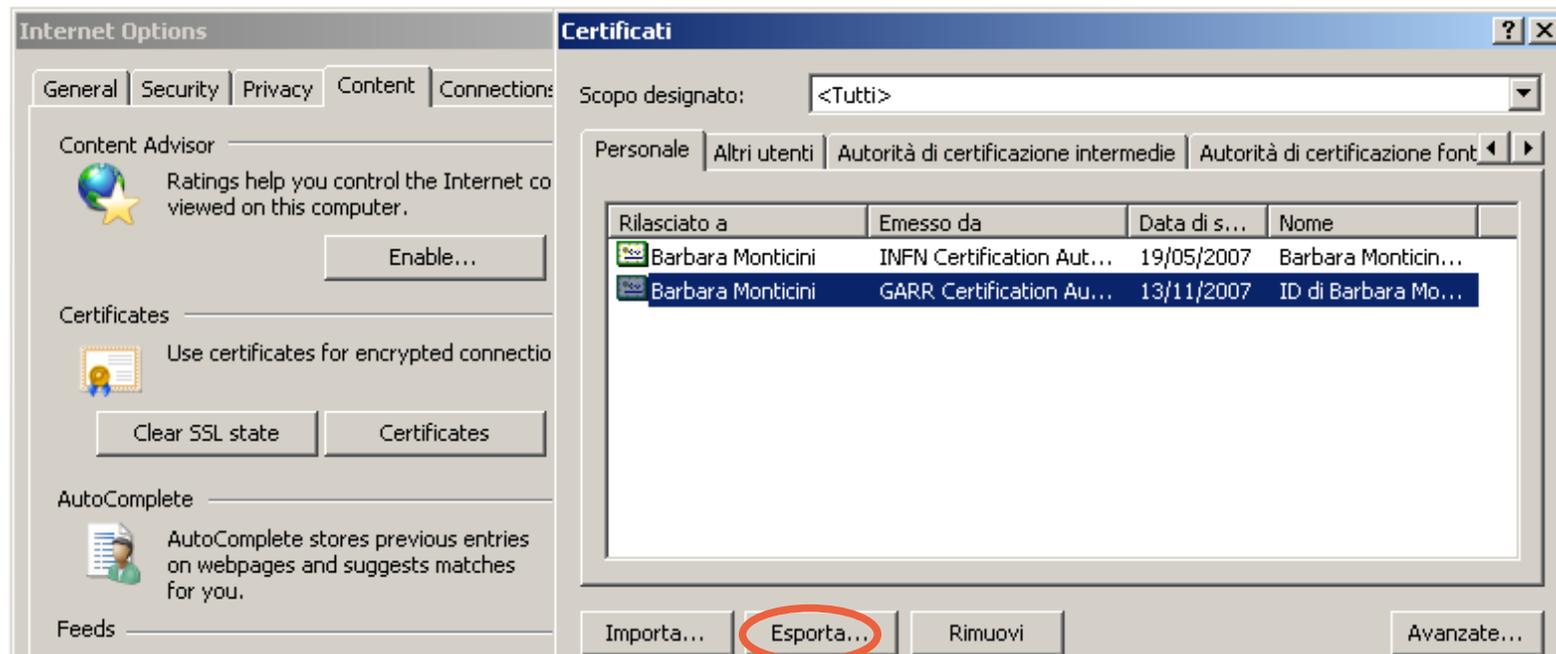
# Installazione in Firefox

- Seguire il link indicato in fondo alla mail di istruzioni
- Inserire la password se necessario
- Firefox 2 *notifica* la corretta importazione del certificato al contrario di Firefox 1 che visualizza una *pagina bianca*



# Backup del certificato

- Procedere immediatamente al **backup** salvando su floppy-disc, cd-rom o penna usb
- Cifrare la chiave privata (creazione di password)
- Solo in IE: abilitare esportazione chiave privata e protezione avanzata della chiave



# Trovare le informazioni sui certificati

- <http://ca.garr.it/> alla pagina

## ► Consultazione certificati

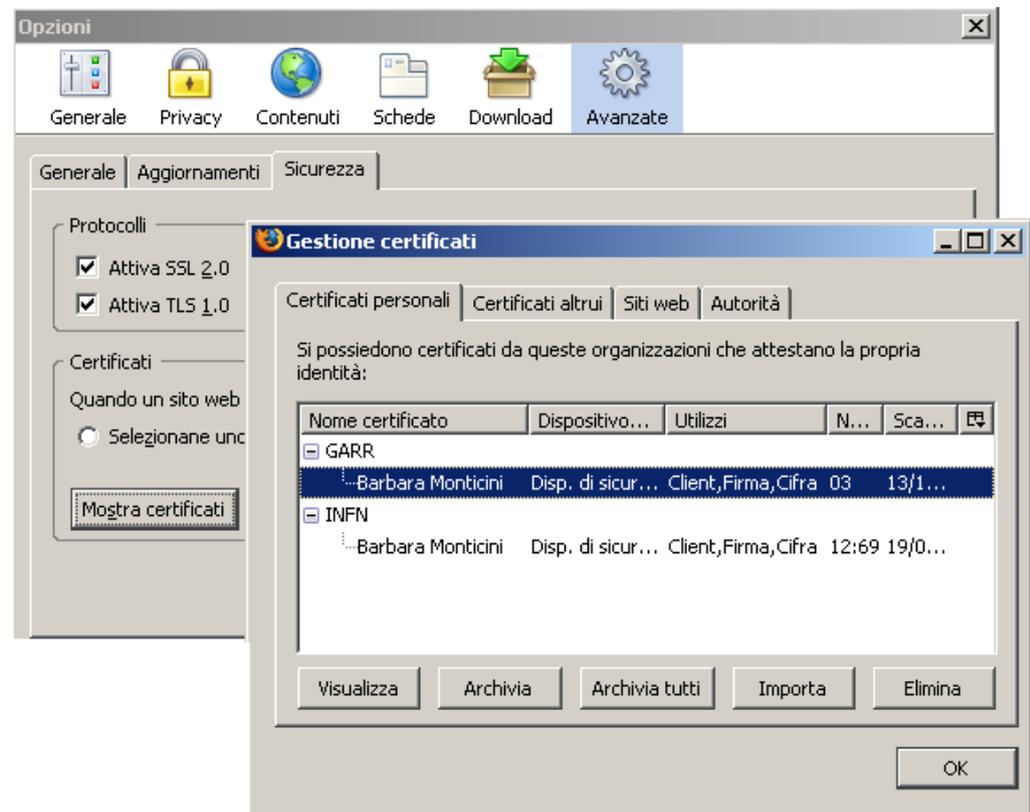
- All'interno del browser:

### – Internet Explorer:

Strumenti -> Opzioni ->  
Contenuto / Certificati SSL

### – Firefox:

Strumenti -> Opzioni -> Avanzate  
/ Sicurezza / Mostra Certificati



# Pubblicazione dei certificati su LDAP

- Parametri necessari
  - server ca.garr.it
  - porte: 389 (ldap) 636 (ldaps)
  - nessun utente (anonymous bind)
- Pubblicazione certificati: utente, server e CA (con aggiornamento della CRL)
- Rubrica LDAP su client di posta

# Rinnovo Certificato Personale

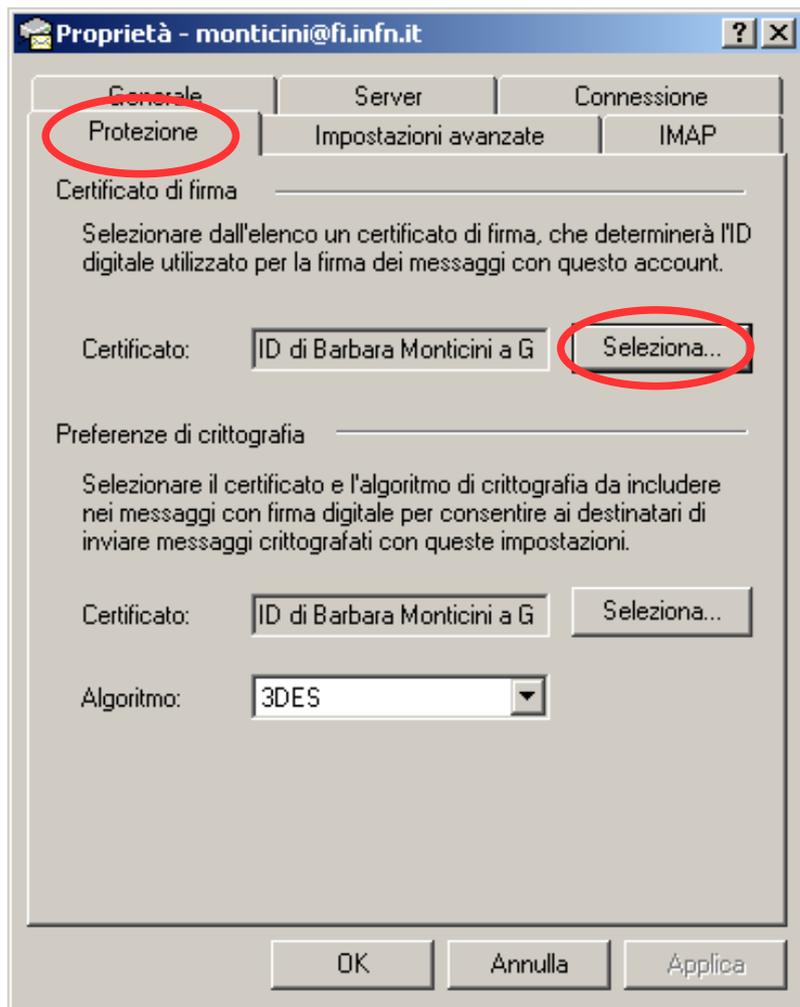
- Disponibile solo per chi è già in possesso di un *certificato valido* ovvero non scaduto e non revocato
- Si richiede on-line, da un **browser** che contiene il certificato da rinnovare, non prima di 20 giorni dalla scadenza
- Il rinnovo, una volta richiesto, è subordinato all'**approvazione della RA** per la struttura di riferimento
- Il certificato sarà emesso solo dopo l'approvazione della RA
- Il certificato emesso deve essere scaricato nel **browser** da cui in seguito potrà' essere esportato (**backup** – importazione in altro browser/client di posta elettronica)

# Revoca Certificato Personale

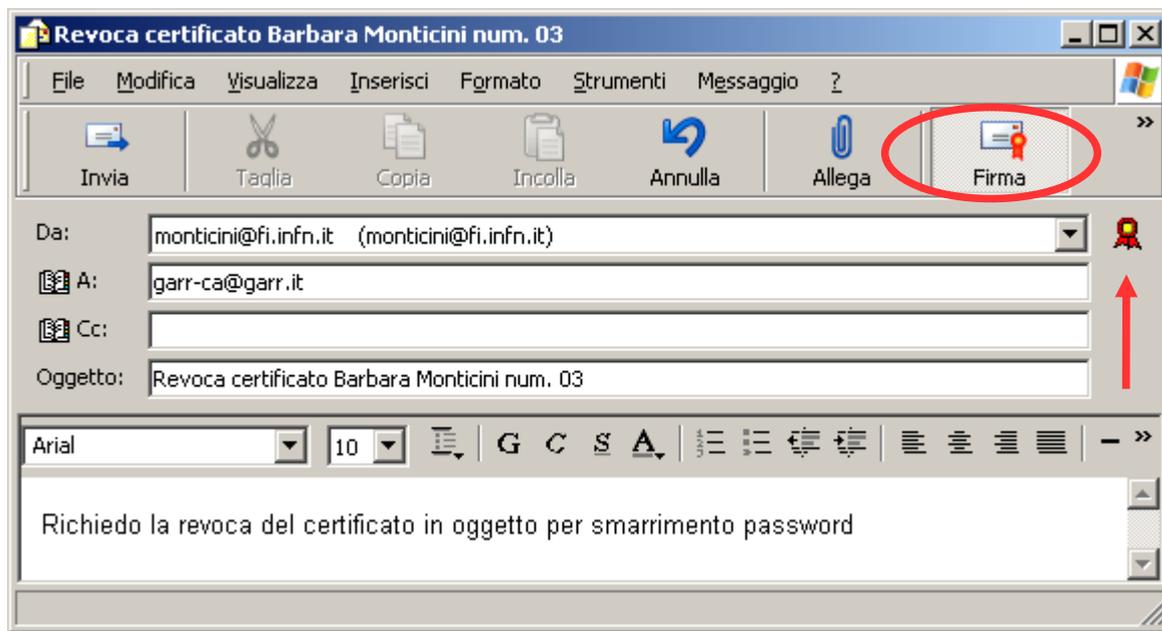
- Deve essere richiesta nei seguenti casi:
  - smarrimento o distruzione della chiave privata
  - smarrimento della password di protezione della chiave privata
  - variazione dei dati riportati nel certificato
- Chi la deve richiedere
  - l'**utente** con mail **firmata** indicando il motivo e specificando nel soggetto il *numero di serie* del certificato
  - la **RA**, con le stesse modalità, se l'utente non è più in grado
- Il *numero di serie* del certificato revocato sarà contenuto nella CRL emessa dalla CA



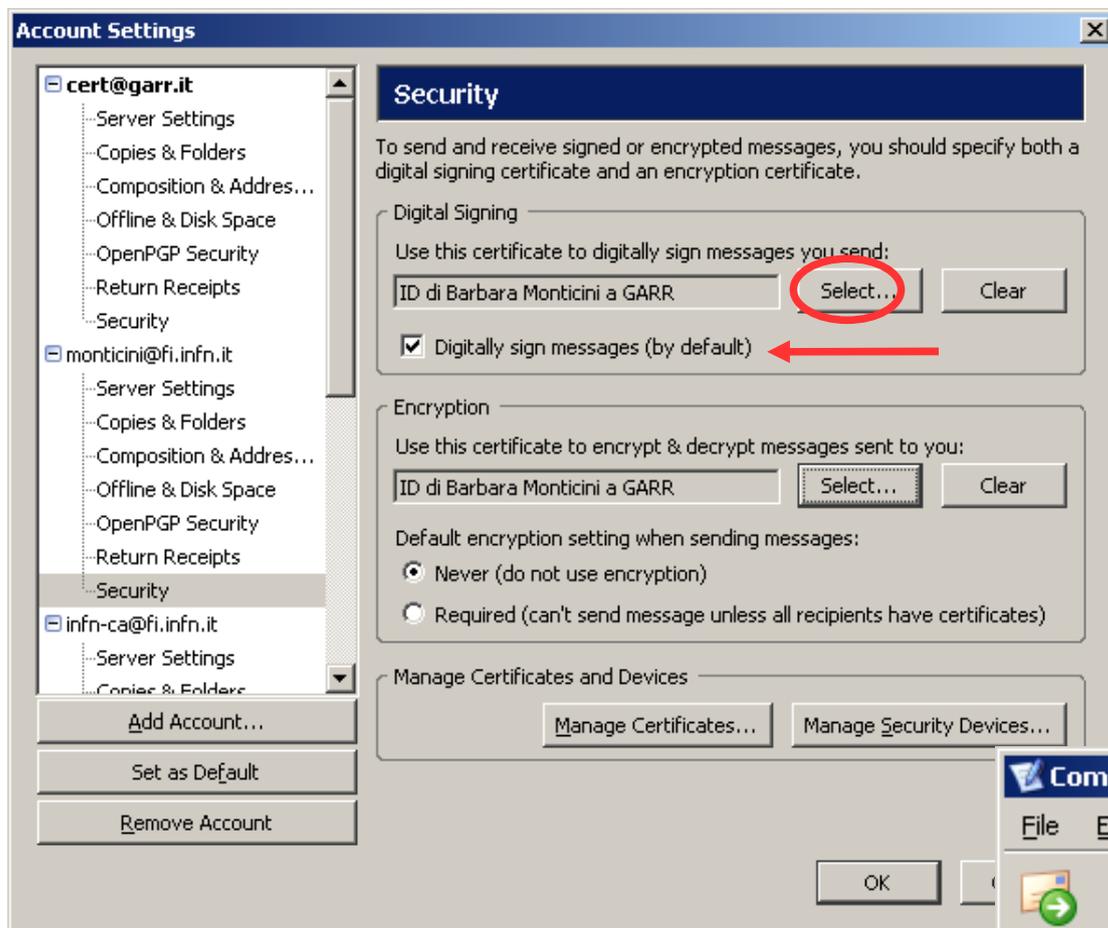
# Firmare la posta con Outlook Express



- Per ogni account, alla voce *Protezione*, selezionare il certificato desiderato
- Creare un messaggio ed abilitare la firma

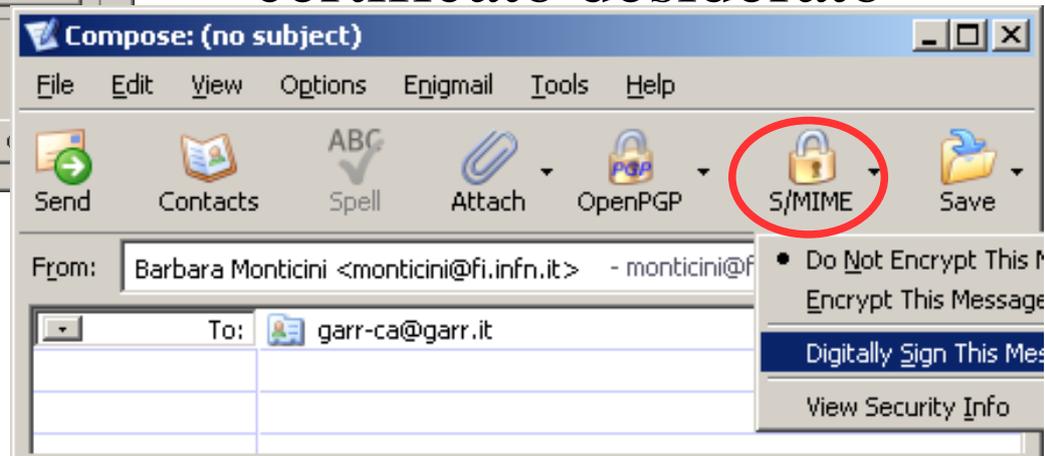


# Firmare la posta con Thunderbird



- In *Options/Advanced /Manage Certificates* importare il certificato
- Per ogni account, alla voce *Security*, selezionare il certificato desiderato

- Creare un nuovo messaggio ed abilitare la firma



# Comandi Openssl: req

- Creazione di una richiesta con nuova chiave senza password

```
[user@localhost]# openssl req -new -nodes -out req-server.pem -keyout key-server.pem  
-config host.conf  
Generating a 1024 bit RSA private key  
.....++++++  
.....++++++  
writing new private key to 'key-server.pem'
```

- Consultazione di una richiesta certificato per server

```
[user@localhost]# openssl req -text -noout -in req-ca.garr.it.pem  
Certificate Request:  
Data:  
Version: 0 (0x0)  
Subject: C=IT, O=GARR, OU=GARR Firenze, CN=ca.garr.it/emailAddress=cecchini@fi.infn.it  
.....
```

- Creazione di un certificato self-signed (per le prove)

```
[user@localhost]# openssl req -x509 -new -keyout key.pem -out cert.pem
```

# Comandi OpenSSL: x509

- Stampa del contenuto del certificato (.pem)

```
[user@localhost]# openssl x509 -text -noout -in ca.garr.it.pem
```

```
Certificate:
```

```
  Data:
```

```
    Version: 3 (0x2)
```

```
    Serial Number: 4 (0x4)
```

```
    Signature Algorithm: sha1WithRSAEncryption
```

```
    Issuer: C=IT, O=GARR, CN=GARR Certification Authority
```

```
    Validity
```

```
      Not Before: Nov 14 15:59:11 2006 GMT
```

```
      Not After  : Nov 14 15:59:11 2007 GMT
```

```
    Subject: C=IT, O=GARR, OU=GARR Firenze, CN=ca.garr.it
```

- Variante: stampa su file .pem dal formato .der

```
openssl x509 -noout -inform DER -in ca.garr.it.der -outform PEM -out  
ca.garr.it.pem
```

- Altre opzioni utili: `-enddate` `-subject` `-serial`

# Richiesta Certificato Server

Viene fatta dall'amministratore del server impiegando comandi **OpenSSL** ed un opportuno file di configurazione (fornito sul sito)

```
openssl req -new -nodes -out req.pem -keyout key.pem -config host.conf
```

## Iter di richiesta

- La richiesta <req.pem> va spedita con **e-mail firmata**, indicando nel soggetto il nome del server, alla RA che la inoltrerà alla CA 
- La CA invia - all'indirizzo contenuto nella richiesta - una e-mail per verificarne la validità e resta in attesa di una mail di conferma
- Il certificato sarà emesso e spedito a suddetto indirizzo e-mail
- E' fondamentale eseguire il **backup** della chiave privata

# Esempio di richiesta

- Preparare i seguenti dati:
  - Nome del server registrato sul DNS
  - Valore del campo **OU** ed email della RA competente
- Generare la richiesta

```
[user@localhost]# openssl req -new -nodes -out req-foo.pem -keyout key-foo.pem
  -config cnf/host.conf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'key-foo.pem'
-----
Nazione []:IT
Organizzazione []:GARR
Unita Organizzativa []:GARR Firenze
FQDN del Server [ ]:foo.fi.infn.it
Email del Server Manager [ ]:monticini@fi.infn.it
```

- Inviare req-foo.pem via mail firmata alla RA
- Salvare key-foo.pem in maniera opportuna

# Richiesta Certificato Server con Nomi Multipli

```
openssl req -new -nodes -out req.pem -keyout key.pem  
-reqexts server_cert -config host_multi.conf
```

- File di configurazione `host_multi.conf` da editare per inserire i nomi alternativi (registrati sul DNS)

```
[ server_cert ]
```

```
subjectAltName = DNS:serverAltname1.your.dom, DNS:serverAltname2.your.dom,  
DNS:serverAltname3.your.dom
```

- Riga di comando con opzione: **-reqexts server\_cert**
- Seguire lo stesso iter delle richieste tradizionali

# Rinnovo Certificato Server

- Segue lo stesso procedimento di una nuova richiesta:
  - generazione delle richiesta
  - inoltro alla RA
  - verifica della correttezza dell'indirizzo e-mail
- Non può essere richiesto prima di 20 giorni dalla scadenza del certificato esistente
- E' fondamentale eseguire il **backup** della chiave privata
- Nel caso di smarrimento della chiave privata di un certificato esistente **non** deve essere richiesto il rinnovo bensì una REVOCA!

# Revoca Certificato Server

- Deve essere richiesta nei seguenti casi:
  - distruzione o smarrimento della chiave privata
  - violazione del sistema
- Deve essere richiesta dall'amministratore ed  inoltrata alla RA di competenza con **e-mail firmata**
- L'oggetto dell'e-mail deve specificare il **numero di serie** del certificato ed il **nome del server**
- Nel corpo del messaggio deve essere specificato il **motivo** della revoca

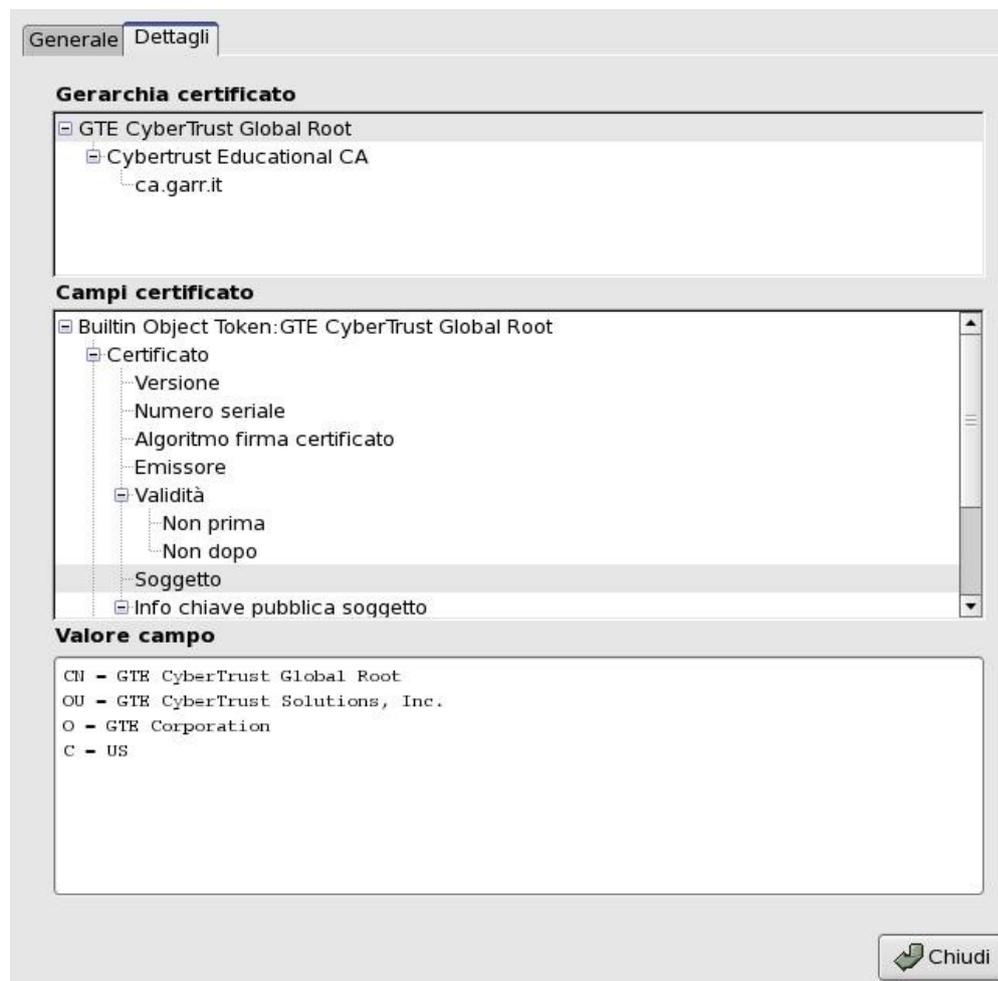
# Terena Server Certificate Service

- Servizio dedicato alle NREN per l'emissione di **certificati server**
- Emessi da **GlobalSign**
- Risolve il cosiddetto *pop-up problem*
- Richieste per “server istituzionali”



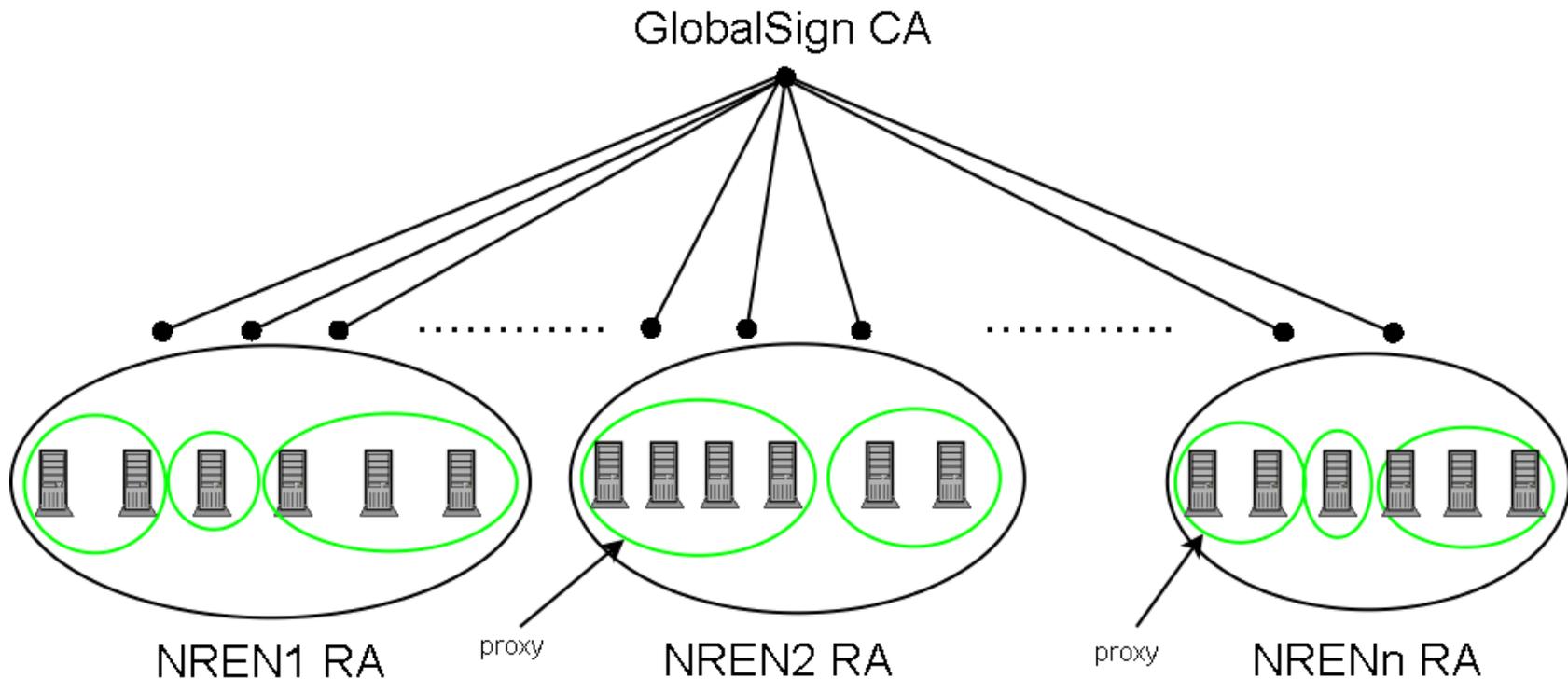
# SCS: Root certificates pre-installati

- La radice della catena dei certificati SCS è **GTE Cybertrust Global Root**
- Emissione fatta dalla CA intermedia **Cybertrust Educational CA**



# Infrastruttura SCS

- Ogni NREN attiva una Registration Authority
- Ogni RA identifica un certo numero di “proxy”



# L'offerta SCS

- Solo certificati per **server**
- **Validità di 1, 2, o 3 anni**
- Tipologie
  - **SureServerEDU TLS emailserver** (**non** per Mail Server)
    - Campi obbligatori: countryName (C), organizationName (O), commonName (CN), [emailAddress \(E\)](#)
  - **SureServerEDU TLS**
    - Campi obbligatori: countryName (C), organizationName (O), commonName (CN)
  - **SureServerEDU**
    - Tipo standard usato da Globalsign (estens. *Netscape-cert-type*)
    - Sconsigliato: da non richiedere!

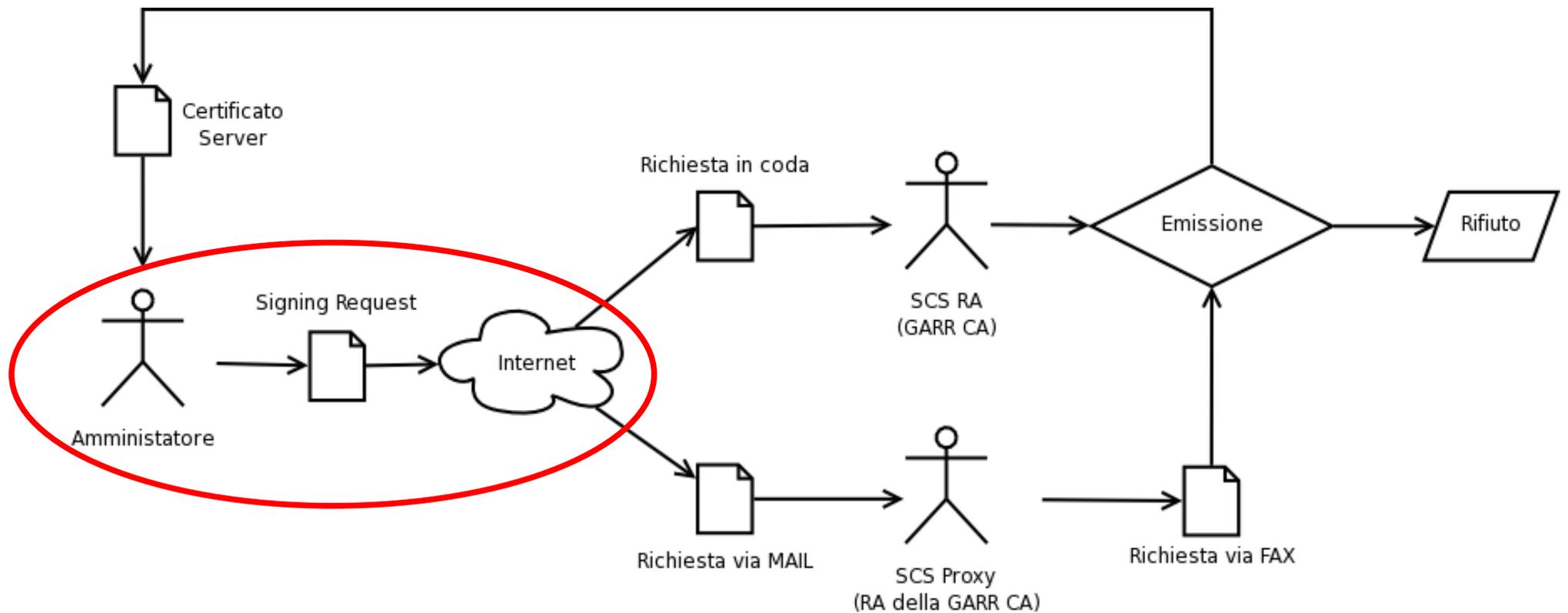
# Iter di richiesta certificati server

- Il richiedente crea una richiesta di certificato CSR generando la coppia di chiavi pubblica-privata (openssl)
- Il richiedente completa un'apposita *form on-line* indicando i propri dati (**contatto tecnico**) e quelli relativi al **contatto amministrativo** (*proxy*)
- Il *proxy* riceve la richiesta, la controlla e stampa il contenuto per firmarlo e inoltrarlo alla RA (via fax, per posta ordinaria, pdf via e-mail o con e-mail firmata con certificato “PersonalSign 2 Pro”)
- Se tutto va bene la RA autorizza l'emissione ed il certificato viene spedito al richiedente

# Come generare una richiesta

- Seguire le stesse istruzioni della GARR CA per server con nome unico
- Per **nomi multipli** impiegare gli appositi file di configurazione (<http://ca.garr.it/SCS/istruzioni.php>)
  - La richiesta avrà tanti CN quanti sono i nomi multipli
  - Il primo CN sarà il CN effettivo
  - Gli altri diventeranno subjectAltNames
- Sottomettere la richiesta all'indirizzo <https://ca.garr.it/SCS/>

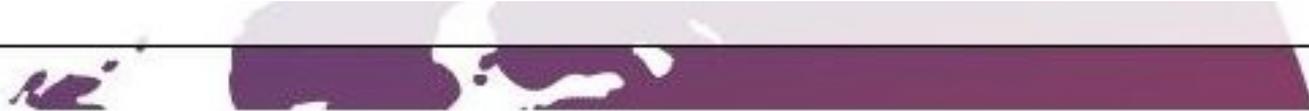
# Iter di richiesta certificati server



# Richiesta SCS: step 1

- <https://ca.garr.it/SCS/> (sito GARR CA)
- <https://www.globalsign.net/ra/terena/garr/edu.cfm>

---



SureServerEDU Certificate Procedure

Step 1: Enter CSR       Step 2: Enter corporate Information       Step 3: Confirm Information

---

STEP 1: SUBMIT CERTIFICATE SIGNING REQUEST

|                            |   |
|----------------------------|---|
| <b>1. Options</b>          |   |
| No. Years:                 | <input checked="" type="radio"/> 1 year <input type="radio"/> 2 years <input type="radio"/> 3 years |
| Type of Server Certificate | <input type="text" value="Please Select:"/>   |
| Webserver Type:            | <input type="text" value="Please Select:"/>   |

# Richiesta SCS: step 1

## 2. Certificate Request File (CSR)

You can do a copy & paste. Open the CSR in a text editor:

1. Locate the section in the file that looks like

```
-----BEGIN CERTIFICATE REQUEST-----  
(...)  
-----END CERTIFICATE REQUEST-----
```

2. Paste it in the input field below (including the BEGIN and END- lines).

OR

1. Enter here the Certificate Signing Request (CSR) that you have created.

You can use the 'browse' button below : this activates the standard File Upload dialog box that allows you to select the archive containing the CSR you want to upload.

[Go to step 2](#)

# Richiesta: step 1

- Procedendo è possibile controllare il contenuto
- Attenzione: è visualizzato solo il 2° campo OU

**1. Options**

No. Years:  1 year  2 years  3 years

Type of Server Certificate: SureServerEDU TLS emailserver

Webserver Type: Apache-ModSSL

**2. Certificate Request File (CSR)**

**Certificate Signing Request (CSR) contents**

Common Name :test-ca.garr.it  
E-mail address :monticini@fi.infn.it  
Organization :GARR  
Organization Unit :Firenze ←  
Country code :IT

Key type:RSA  
Key size:2048

*Please verify the above information is correct before proceeding.  
If not you can enter a new CSR in the box below.*

## Richiesta SCS: step 2

- **Contatto tecnico:** inserire i propri dati (amministratore del server)
- **Contatto amministrativo (*proxy*):** inserire i dati di una delle RA della struttura a cui il server afferisce
- **Password per revoca:** da memorizzare per utilizzare il meccanismo della revoca on-line
- **Nota:** sostituire GARR con il nome della vostra Organizzazione nel *contatto tecnico*



# Emissione certificato SCS

- Il certificato arriva per mail all'indirizzo specificato nel contatto tecnico
- Lasciar perdere il sigillo (*seal*)

☐ **Oggetto:** Your SureServerEDU TLS emailserver Certificate

**Da:** [ca@globalsign.net](mailto:ca@globalsign.net)

**Data:** 06/04/2007 13:04

**A:** [monticini@fi.infn.it](mailto:monticini@fi.infn.it)

Hi,

Following your request for a GARR SCS certificate with subject:

countryName=IT, organizationName=GARR, organizationalUnitName=GARR,  
organizationalUnitName=Firenze, commonName=ca.garr.it, [emailAddress=monticini@fi.infn.it](mailto:monticini@fi.infn.it)

Please find the signed certificate in attachment.

**Allegati:**

cert\_1788042192.pem

# Revoca di certificati SCS

<http://secure.globalsign.net/phoenixng/services.cfm?id=2658624481&reset=yes>

## REVOKE YOUR CERTIFICATE !

A certificate should be revoked if:

there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key  
there has been a modification of the information contained in the certificate

Once revoked, the serial number of the certificate will be published in our CRL (Certificate Revocation List).

To revoke your certificate, free of charge, just proceed with the following 4 steps

Please keep in mind that you will be asked to provide your password (supplied to us at the time of request).

**This will only take 2 minutes!**

### **Step 1. CHECK ROOT**

First, you need to install GlobalSign's Root Certificate.

### **Step 3. SELECT THE CERTIFICATE**

Choose one of the certificates from the list.

### **Step 2. SELECT SEARCH METHOD**

We ask you to retrieve your certificate by providing us the  
E-mail, Name or Serialnumber of the certificate.

### **Step 4. ENTER YOUR PASSWORD**

As a security check, we ask you to enter your password.

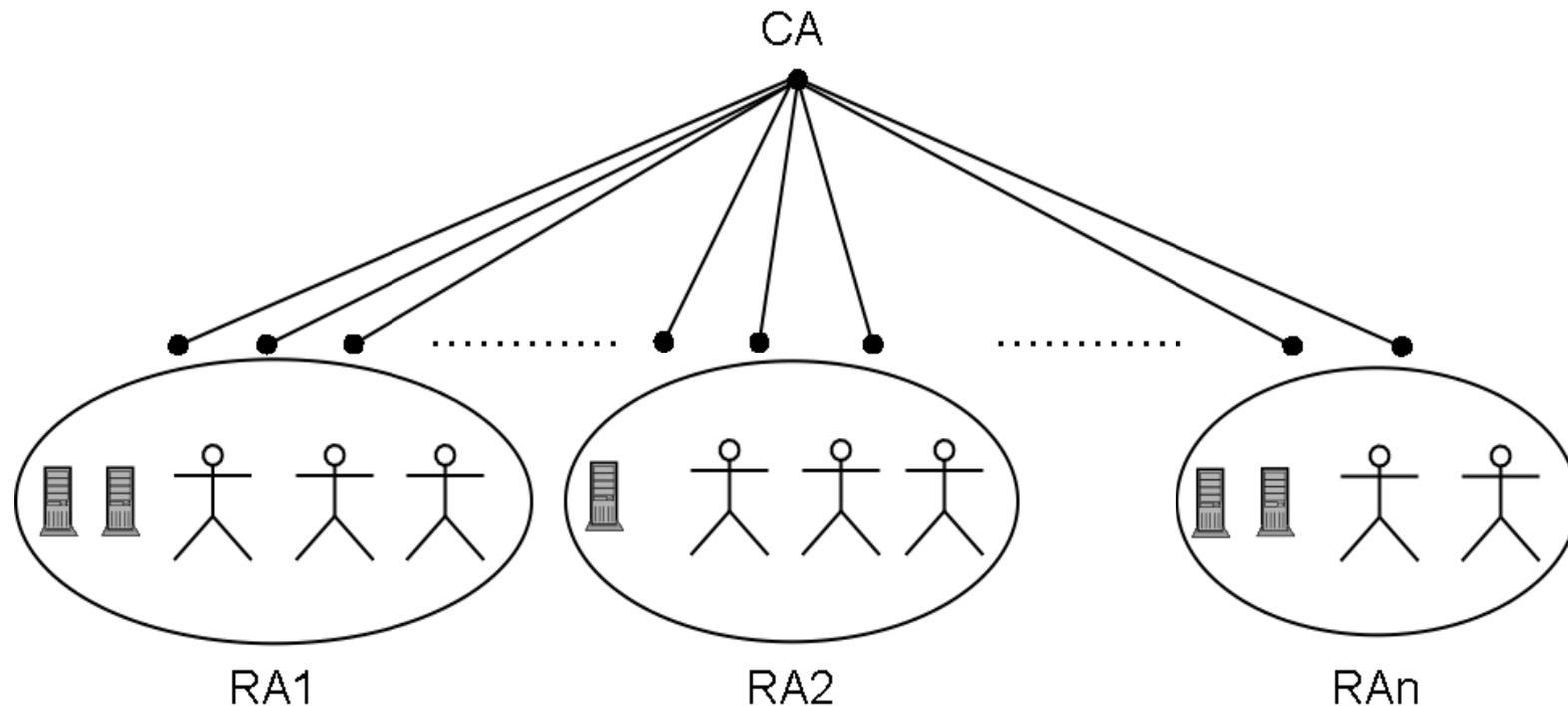
[Go to step 1](#)

# Sessione Registration Authority

- Attivare una Registration Authority
- Il primo certificato
- Altri comandi OpenSSL
- I compiti del ruolo di RA
- Quali sono gli aventi diritto?
- Certificati SCS

# Cos'è una Registration Authority

- La RA rappresenta per la CA un **punto di fiducia** a cui demandare il compito dell'autenticazione delle utenze
- La RA opera nell'ambito di un determinato dominio di competenza, stabilito nella **lettera di nomina**



# Iter di abilitazione al ruolo di RA

- Contattare il gestore della CA per prendere accordi
- Definire il dominio di competenza a cui associare un valore detto campo **OU**; tale valore identifichera' univocamente tutti i certificati emessi per le entità che vi afferiscono
- Richiesta formale su **carta intestata, protocollata e firmata** dal direttore della struttura, **spedita** per posta ordinaria (il fac-simile è disponibile sul sito)
- La richiesta dovrà specificare:
  - i nomi delle persone che svolgeranno il ruolo (**almeno due**)
  - il valore del campo **OU** (che identificherà tutti i certificati emessi)

# Il certificato personale di una RA

- Ottenere un certificato personale per la **prima** RA
  - autenticazione presso la CA
  - richiedere un certificato on-line 
  - dimostrare di aver scaricato il certificato inviando un mail firmato
- Le **successive** RA per la stessa Unità Organizzativa (OU)
  - autenticazione presso la RA già abilitata
  - richiedere un certificato on-line 
  - dimostrare di aver scaricato il certificato inviando un mail firmato

# Altri adempimenti

- Dichiarazione della RA alla GARR CA
  - lettera su carta intestata in cui ogni RA sottoscrive l'impegno a ricoprire il ruolo (disponibile in appendice al documento [https://ca.garr.it/RA/Istruzioni\\_RA.pdf](https://ca.garr.it/RA/Istruzioni_RA.pdf))
- Mantenimento della documentazione
  - archiviazione di tutta la corrispondenza intercorsa con la GARR CA (richieste, approvazioni, revoche ...)
  - *auditing* dell'attività da parte della GARR CA

# Comandi OpenSSL: req

- Consultazione di una richiesta certificato per server

```
[user@localhost]# openssl req -text -noout -in req-ca.garr.it.pem
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=IT, O=GARR, OU=GARR Firenze, CN=ca.garr.it/emailAddress=cecchini@fi.infn.it
    .....
```

- Variante: consulta solo il *subject*

```
[user@localhost]# openssl req -subject -noout -in req-ca.garr.it.pem
subject=/C=IT/O=GARR/OU=GARR Firenze/CN=ca.garr.it/emailAddress=cecchini@fi.infn.it
```

- Variante: consulta la versione .pem

```
[user@localhost]# openssl req -in req-ca.garr.it.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIBrDCCARUCAQAwbDELMAkGA1UEBhMCSVQxDTALBgNVBAoTBEdBU1IxFTATBgNV
.....
s1QbfFTnkkmQIjkI3iVFza5by9u2Tx522SMXnwN/+Kx7G06Qf+Zf/Ch5DqE98g28
-----END CERTIFICATE REQUEST-----
```

# Comandi OpenSSL: x509

- Stampa del contenuto del certificato (.pem)

```
[user@localhost]# openssl x509 -text -noout -in ca.garr.it.pem
```

```
Certificate:
```

```
Data:
```

```
Version: 3 (0x2)
```

```
Serial Number: 4 (0x4)
```

```
Signature Algorithm: sha1WithRSAEncryption
```

```
Issuer: C=IT, O=GARR, CN=GARR Certification Authority
```

```
Validity
```

```
Not Before: Nov 14 15:59:11 2006 GMT
```

```
Not After : Nov 14 15:59:11 2007 GMT
```

```
Subject: C=IT, O=GARR, OU=GARR Firenze, CN=ca.garr.it
```

- Variante: stampa su file .pem dal formato .der

```
openssl x509 -noout -inform DER -in ca.garr.it.der -outform PEM -out  
ca.garr.it.pem
```

- Altre opzioni utili: `-enddate -subject -serial`

# Ambiti di intervento di una RA

- ▶ Richiesta di un nuovo certificato personale
- ▶ Richiesta di rinnovo di un certificato personale
- ▶ Richiesta di un certificato per server
  - nuovo
  - rinnovo
- ▶ richiesta di revoca di un certificato
  - personale (solo in particolari casi)
  - server

# Autenticazione degli utenti

- Incontro **faccia a faccia** con l'utenza
- Possono essere autenticati solo gli utenti che afferiscono alla struttura per la quale si è ricevuto la nomina
- E' richiesto il possesso del certificato personale
- La procedura fornisce un **codice numerico** che dovrà essere comunicato all'utente



Registration Authority: **GARR, Firenze**  
**Barbara Monticini** (<monticini@fi.infn.it>)

---

Dichiaro che la persona di cui riporto i dati qui sotto

- è in mia presenza,
- ne ho accertato l'identità per mezzo di un documento legalmente valido,
- ha diritto ad ottenere un certificato dalla GARR CA.

|                 |                      |
|-----------------|----------------------|
| Nome e Cognome: | <input type="text"/> |
| E-mail:         | <input type="text"/> |

# Approvazione al rinnovo dei Certificati Personali

- Tutti i rinnovi di certificati personali necessitano del **consenso** della RA competente
- Ad ogni richiesta di rinnovo la CA inoltra un messaggio di richiesta approvazione a tutte le RA competenti
- Per approvare è sufficiente rispondere affermativamente al suddetto messaggio con **mail firmata**



# Inoltro Certificati Server

1. Controllare nelle richieste pervenute:
  - ✓ FQDN nel soggetto della mail
  - ✓ la correttezza dei campi del certificato
  - ✓ la **firma digitale** dell'amministratore richiedente
2. Inoltrare le richieste di certificato alla CA:
  - ✓ firmare il messaggio
  - ✓ attendere la notifica dell'emissione



# Revoca certificati personali

- Necessaria per utenti che **non** accedono più alla chiave privata
- Modalità:
  - **e-mail firmata** 
  - nell'oggetto indicare sia il **numero di serie** del certificato sia il **nome e cognome** del soggetto
  - nel body indicare il **motivo** della revoca

# Revoca certificati server

- Controllare che la richiesta di revoca provenga dall'amministratore del server
- Inoltrare la richiesta alla CA in un'e-mail firmata:
  - nell'oggetto indicare sia il **numero di serie** del certificato sia il **nome fqdn** del server
  - nel body indicare il **motivo** della revoca

Oggetto: Revoca Certificato num **AB03** rilasciato  
a rt.garr-ca.garr.it

Salve,

Si richiede la revoca del certificato in oggetto per smarrimento della chiave privata.



# Identificare la comunità

- L'insieme degli *aventi diritto* all'identificazione è definito puntualmente nella **lettera di nomina**
- Per un server è necessario capire:
  - a quale rete appartiene
  - da chi è gestito
- E' obbligatorio rifiutare richieste di autorizzazione e richieste per server provenienti da soggetti non appartenenti alla comunità identificata nella lettera di nomina
- In caso di dubbio contattare il gestore della CA

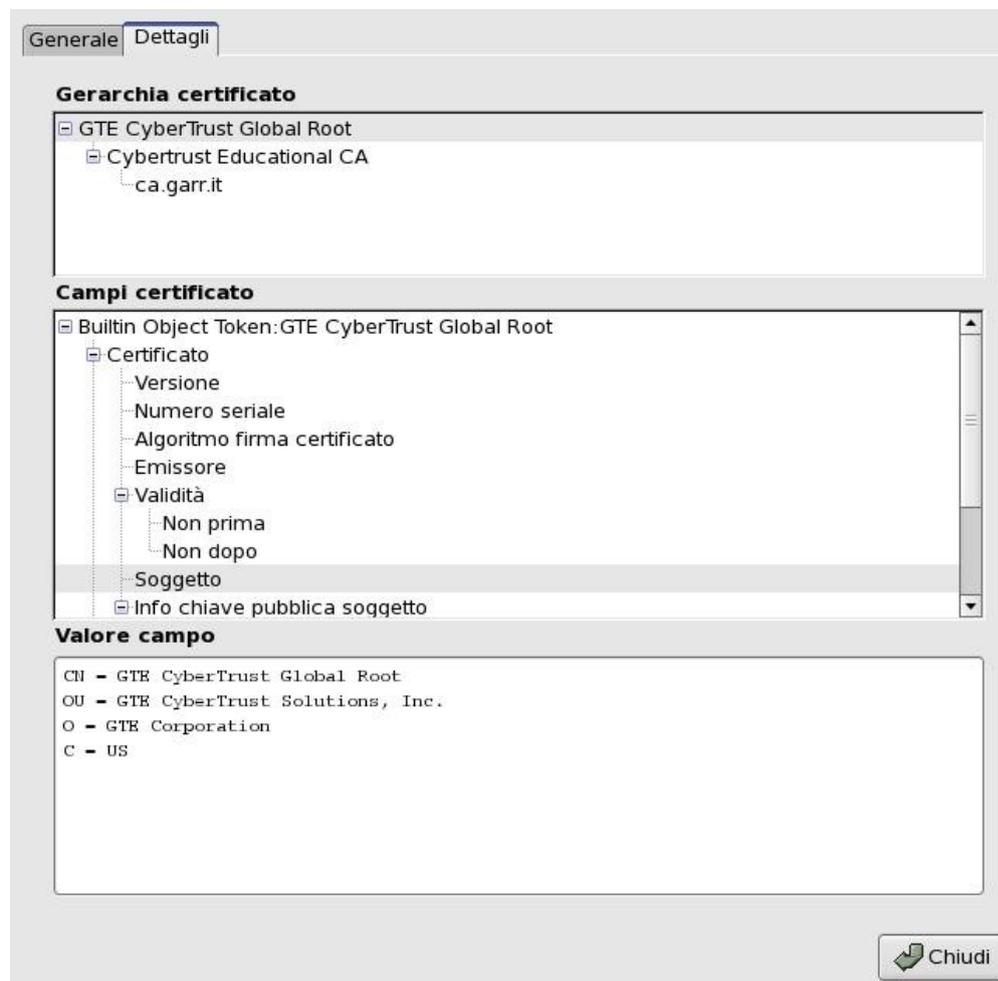
# Terena Server Certificate Service

- Servizio dedicato alle NREN per l'emissione di **certificati server**
- Emessi da **GlobalSign**
- Risolve il cosiddetto *pop-up problem*
- Richieste per “server istituzionali”



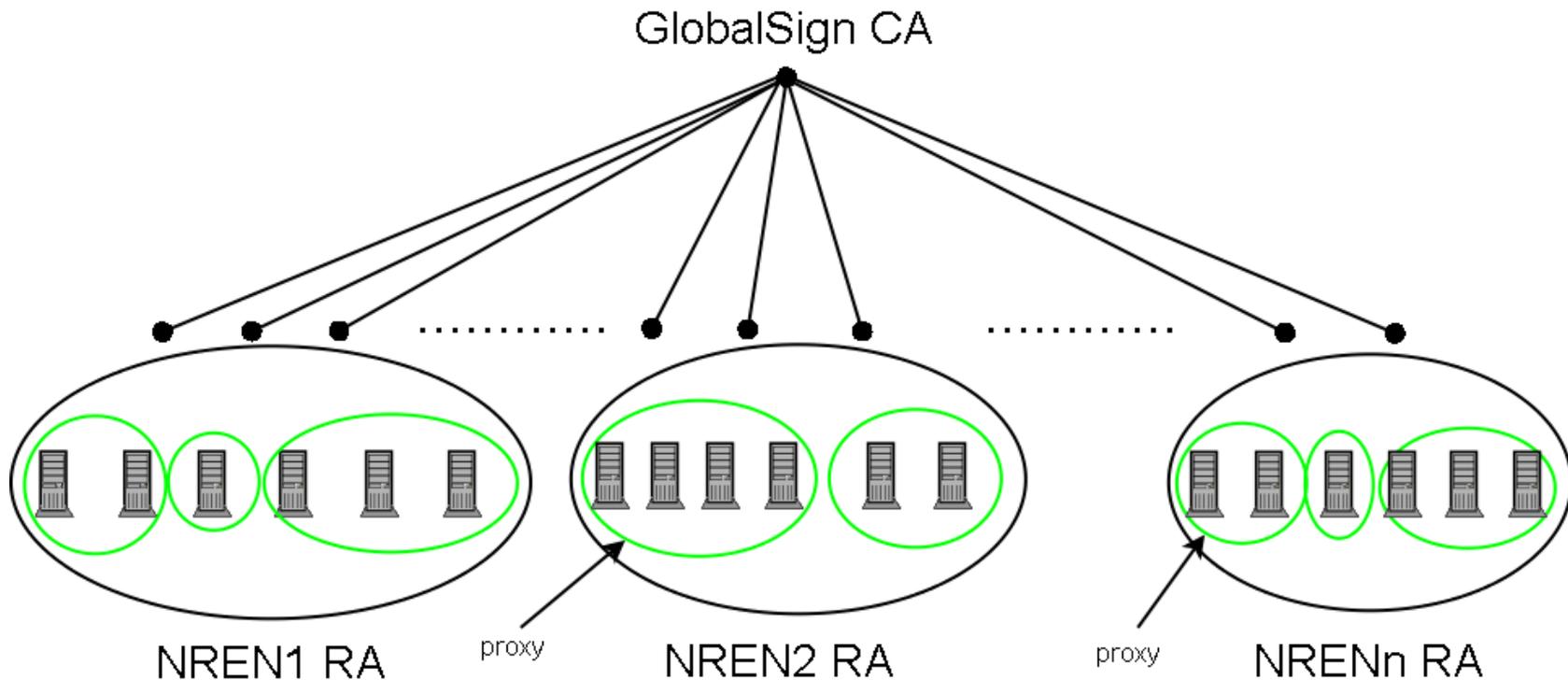
# SCS: Root certificates pre-installati

- La radice della catena dei certificati SCS è **GTE Cybertrust Global Root**
- Emissione fatta dalla CA intermedia **Cybertrust Educational CA**



# Infrastruttura SCS

- Ogni NREN attiva una Registration Authority
- Ogni RA identifica un certo numero di “proxy”



# Il ruolo di proxy

- Nell'infrastruttura GARR-CA il ruolo di *proxy* coincide con il ruolo di **RA** di unità organizzativa
- Per svolgere il ruolo di *proxy* per una unità organizzativa è necessario presentare apposita documentazione (cartacea e firmata da un rappresentante legale)
  - Documento di *Nomina dei proxy* (= lettera nomina di RA)
  - Documento di *autorizzazione dei nomi di dominio* (sottoscritto dall'Access Port Administrator)

# L'offerta SCS

- Solo certificati per **server**
- **Validità di 1, 2, o 3 anni**
- Tipologie
  - **SureServerEDU TLS emailserver** (**non** per Mail Server)
    - Campi obbligatori: countryName (C), organizationName (O), commonName (CN), [emailAddress \(E\)](#)
  - **SureServerEDU TLS**
    - Campi obbligatori: countryName (C), organizationName (O), commonName (CN)
  - **SureServerEDU**
    - Tipo standard usato da Globalsign (estens. *Netscape-cert-type*)
    - Sconsigliato: da non richiedere!

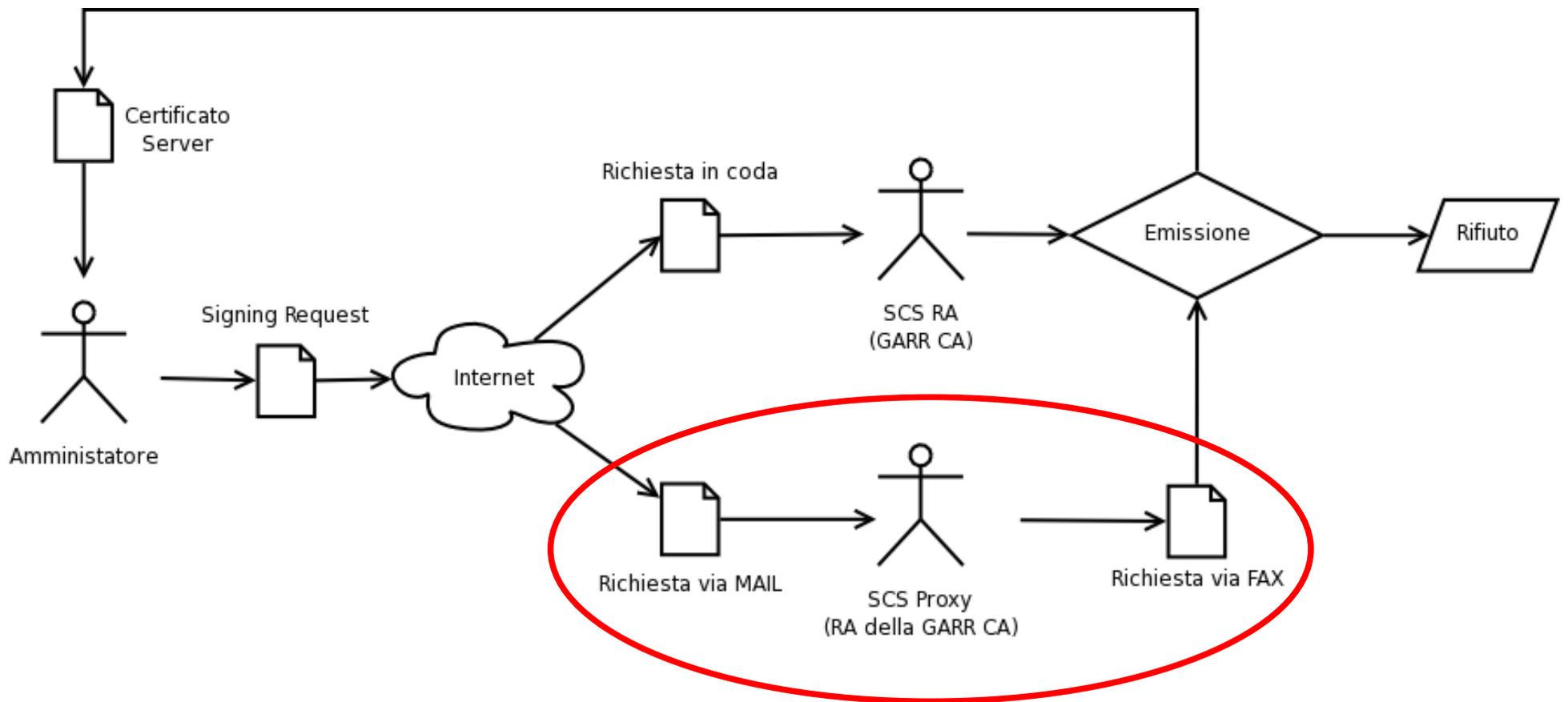
# Iter di richiesta certificati server

- Il richiedente crea una richiesta di certificato CSR generando la coppia di chiavi pubblica-privata
- Il richiedente completa un'apposita *form on-line* indicando i propri dati (**contatto tecnico**) e quelli relativi al **contatto amministrativo** (*proxy*)
- Il *proxy* riceve la richiesta, la controlla e stampa il contenuto per firmarlo e inoltrarlo alla RA (via fax, per posta ordinaria, scansione / pdf via e-mail o con e-mail firmata con certificato “PersonalSign 2 Pro”)
- Se tutto va bene la RA autorizza l'emissione ed il certificato viene spedito al richiedente

# Come generare una richiesta

- Seguire le stesse istruzioni della GARR CA
- Per **nomi multipli** impiegare gli appositi file di configurazione (<http://ca.garr.it/SCS/istruzioni.php>)
  - La richiesta avrà tanti CN quanti sono i nomi multipli
  - Il primo CN sarà il CN effettivo
  - Gli altri diventeranno subjectAltNames
- Sottomettere la richiesta all'indirizzo <https://ca.garr.it/SCS/>

# Iter di richiesta certificati server



# Richiesta SCS: step 1

- <https://ca.garr.it/SCS/> (sito GARR CA)
- <https://www.globalsign.net/ra/terena/garr/edu.cfm>

---



SureServerEDU Certificate Procedure

Step 1: Enter CSR       Step 2: Enter corporate Information       Step 3: Confirm Information

---

STEP 1: SUBMIT CERTIFICATE SIGNING REQUEST

**1. Options**

No. Years:       1 year     2 years     3 years

Type of Server Certificate     

Webserver Type:

# Richiesta SCS: step 1

## 2. Certificate Request File (CSR)

You can do a copy & paste. Open the CSR in a text editor:

1. Locate the section in the file that looks like

```
-----BEGIN CERTIFICATE REQUEST-----  
(...)  
-----END CERTIFICATE REQUEST-----
```

2. Paste it in the input field below (including the BEGIN and END- lines).

OR

1. Enter here the Certificate Signing Request (CSR) that you have created.

You can use the 'browse' button below : this activates the standard File Upload dialog box that allows you to select the archive containing the CSR you want to upload.

[Go to step 2](#)

# Richiesta: step 1

- Procedendo è possibile controllare il contenuto
- Attenzione: è visualizzato solo il 2° campo OU

**1. Options**

No. Years:  1 year  2 years  3 years

Type of Server Certificate: SureServerEDU TLS emailserver

Webserver Type: Apache-ModSSL

**2. Certificate Request File (CSR)**

**Certificate Signing Request (CSR) contents**

Common Name :test-ca.garr.it  
E-mail address :monticini@fi.infn.it  
Organization :GARR  
Organization Unit :Firenze ←  
Country code :IT

Key type:RSA  
Key size:2048

*Please verify the above information is correct before proceeding.  
If not you can enter a new CSR in the box below.*

## Richiesta SCS: step 2

- **Contatto tecnico:** inserire i propri dati (amministratore del server)
- **Contatto amministrativo (*proxy*):** inserire i dati di una delle RA della struttura a cui il server afferisce
- **Password per revoca:** da memorizzare per utilizzare il meccanismo della revoca on-line
- **Nota:** sostituire GARR con il nome della vostra Organizzazione nel *contatto tecnico*



# Emissione certificato SCS

- Il certificato arriva per mail all'indirizzo specificato nel contatto tecnico
- Lasciar perdere il sigillo (*seal*)



# Revoca di certificati SCS

<http://secure.globalsign.net/phoenixng/services.cfm?id=2658624481&reset=yes>

## REVOKE YOUR CERTIFICATE !

A certificate should be revoked if:

there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key  
there has been a modification of the information contained in the certificate

Once revoked, the serial number of the certificate will be published in our CRL (Certificate Revocation List).

To revoke your certificate, free of charge, just proceed with the following 4 steps

Please keep in mind that you will be asked to provide your password (supplied to us at the time of request).

**This will only take 2 minutes!**

### **Step 1. CHECK ROOT**

First, you need to install GlobalSign's Root Certificate.

### **Step 3. SELECT THE CERTIFICATE**

Choose one of the certificates from the list.

### **Step 2. SELECT SEARCH METHOD**

We ask you to retrieve your certificate by providing us the  
E-mail, Name or Serialnumber of the certificate.

### **Step 4. ENTER YOUR PASSWORD**

As a security check, we ask you to enter your password.

[Go to step 1](#)

# Riferimenti e Bibliografia

- W. Stallings: Cryptography and Network Security (Principles and Practice) - Prentice Hall
- C. Adams - S. Lloyd: Understanding Public Key Infrastructure - MacMillian Technical Publishing
- OpenSSL: <http://www.openssl.org/>
- GARR-CA: <http://ca.garr.it/>
- GARR-CA: CP/CPS <http://ca.garr.it/CPS/>
- GlobalSign: <http://www.globalsign.net/>