GARR
CERTIFICATION AUTHORITY

VII Workshop GARR
Roma 16 Novembre 2006
Barbara Monticini

Agenda

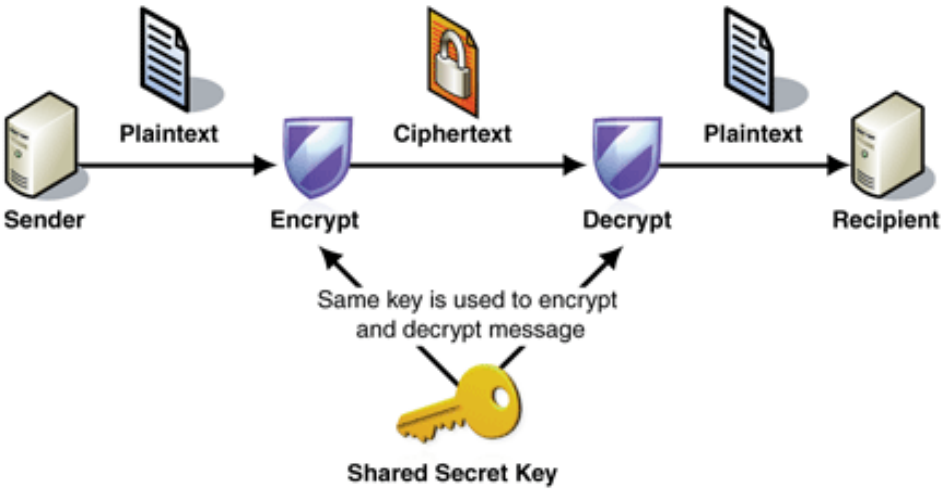
- Overview
- Sezione dedicata agli Utenti
- Sezione dedicata alle Registration Authority
- Terena Server Certificate Service (SCS)

Introduzione

- Problematiche relative alla sicurezza:
  - Autenticazione: verificare l'identità di un soggetto
  - Autorizzazione: accesso controllato a determinate risorse
  - Non repudiation: impedire al mittente di disconoscere i dati trasmessi
  - Riservatezza: garantire che i dati in transito non siano intercettati
  - Integrità: garantire che i dati in transito non siano modificati
- La crittografia:
  - A chiave segreta: crittografia simmetrica
  - A chiave pubblica: crittografia asimmetrica

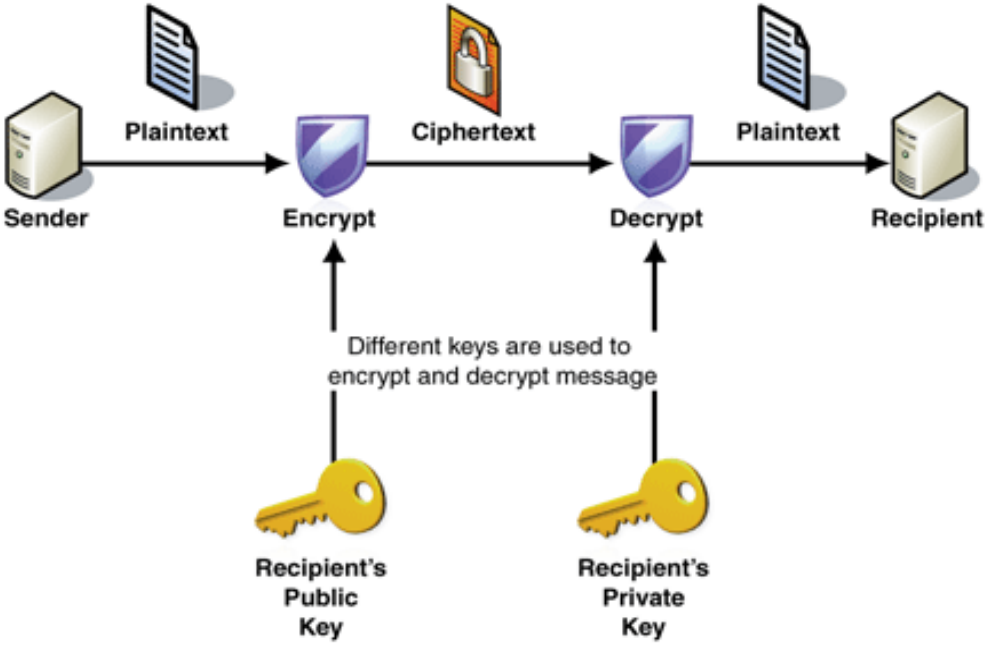
La crittografia a chiave segreta

- 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 può decrifrare solo con l'altra
- Vantaggi:
  - non c'è scambio di chiavi
  - le chiavi sono O(n)
- Problema: è lento

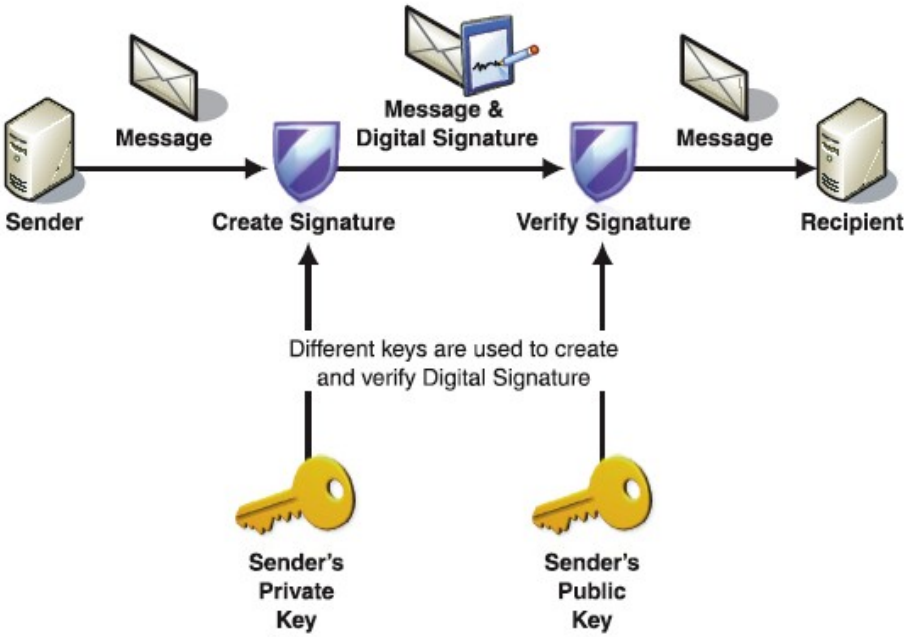


Funzioni Hash

- Lo scopo di queste funzioni è quello di produrre un'*impronta* di un messaggio
- 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 computazionalmete impossibile trovare (x,y) t.c. $H(y) = H(x)$

La firma digitale

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

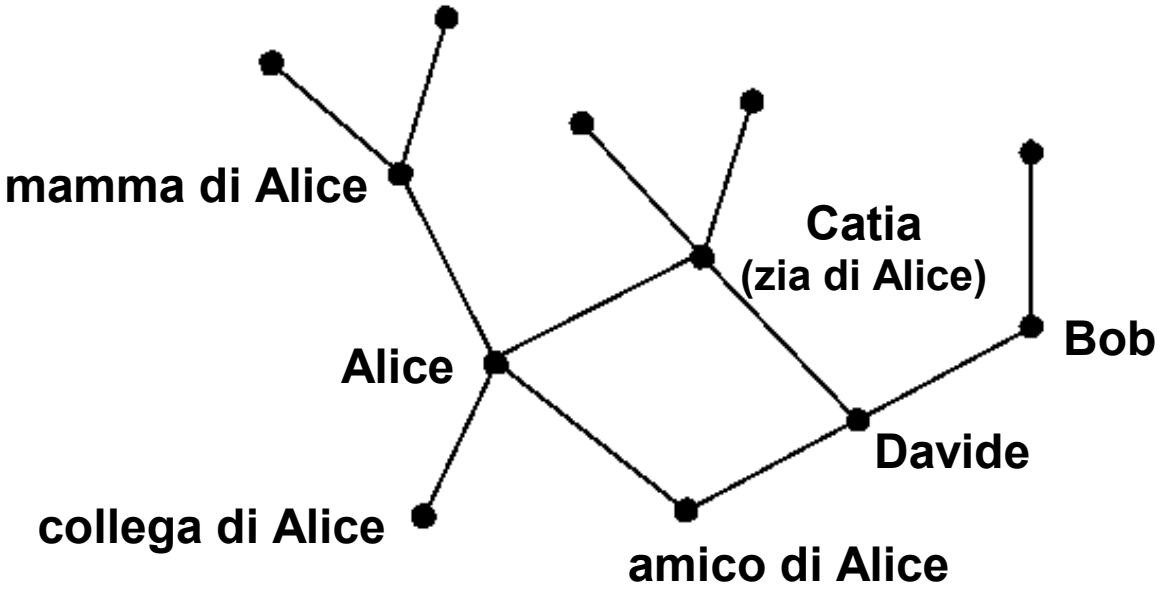


Distribuzione delle chiavi

- 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

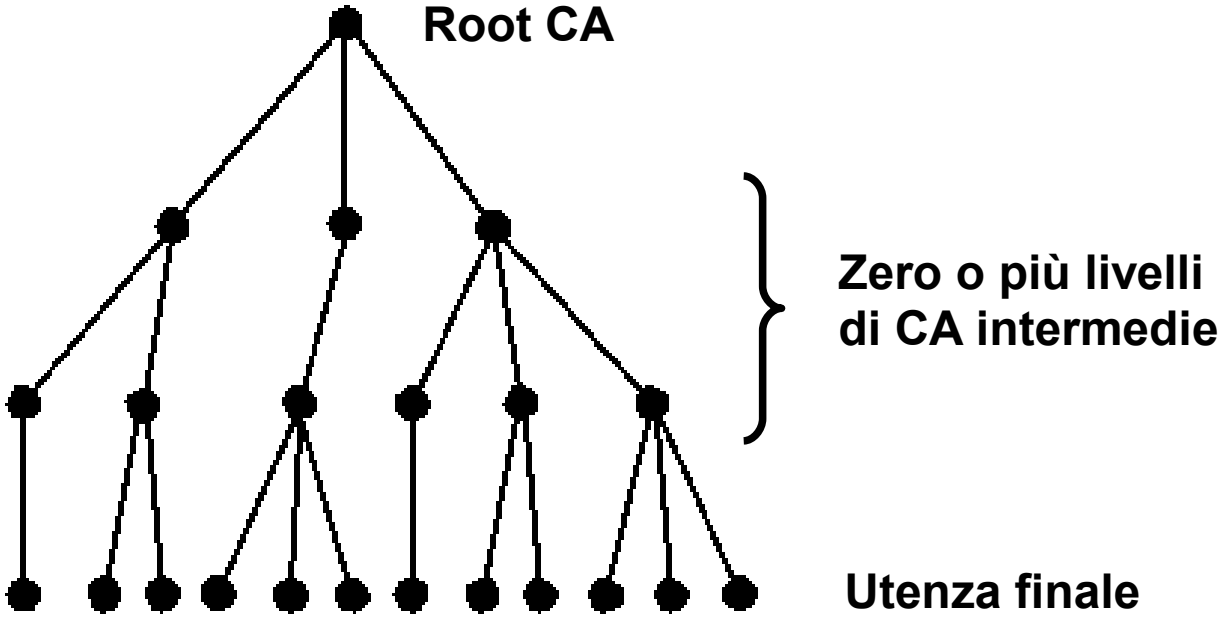
Modello user-centric

- L'utente:
  - decide a quali certificati accordare o meno la fiducia
  - agisce come una CA firmando i certificati di altre entità



Modello gerarchico

- La root CA “certifica” zero o più CA intermedie
- Le CA intermedie “certificano” zero o più CA sottostanti
- All'ultimo livello le CA “certificano” gli utenti finali



I certificati digitali X.509

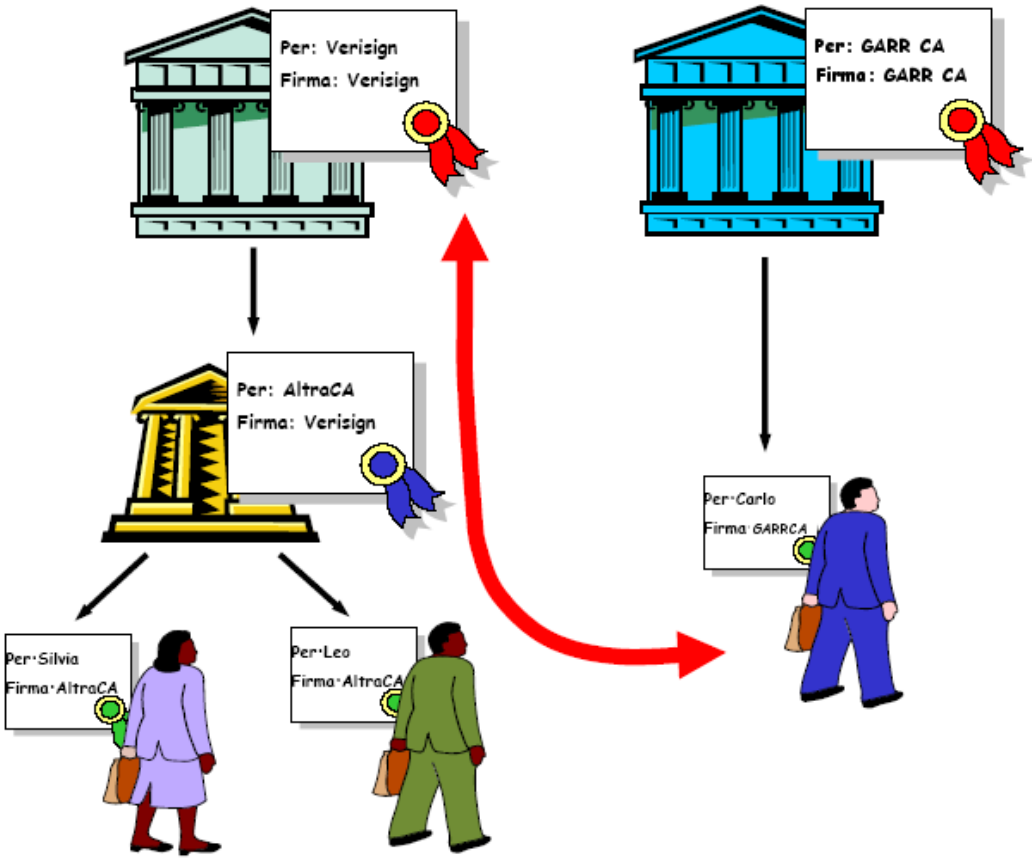
- Contengono varie informazioni
  - ad es.: nome, cognome, e-mail, città di residenza, affiliazione
  - la chiave pubblica (quella privata è conosciuta solo dal soggetto stesso)
  - la firma della CA che lo ha emesso
  - informazioni sulla CA
  - la durata del certificato in termini di validita da –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

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**)

Root Certification Authority

- E' all'apice dell'infrastruttura (**root**)
- Può istituire CA subordinate
- Si affida a *Registration Authority* per l'autenticazione dell'utenza
- Ha un certificato auto-firmato (**root certificate**)

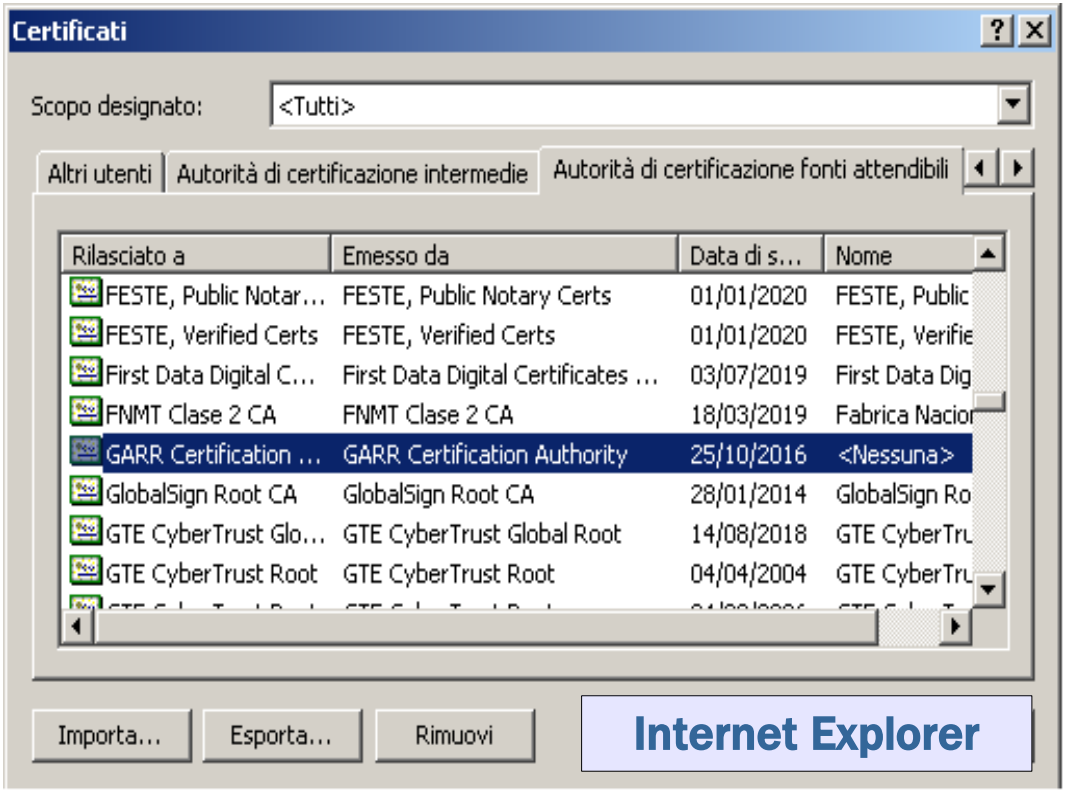


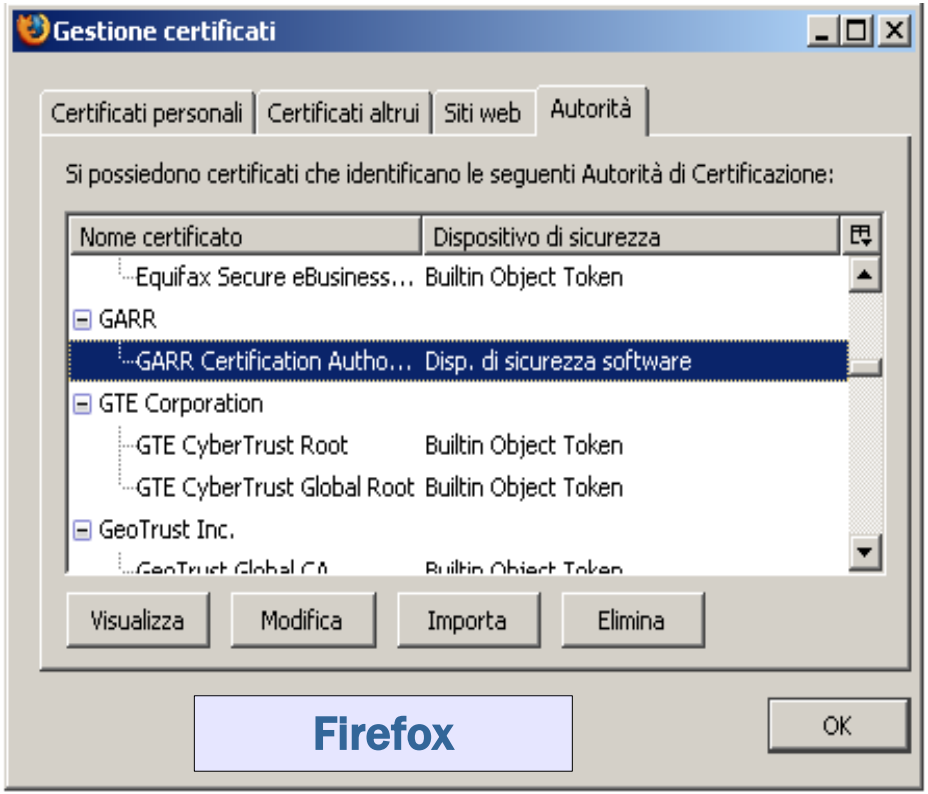
I compiti della CA

- Emissione di Certificate Policy (CP)
  - insieme di regole indicante il campo di applicazione dei certificati
- Emissione di Certification Practice Statement (CPS)
  - dichiarazione delle procedure impiegate dalla CA per l'emissione dei certificati
- Garantire il rispetto della policy
- Emissione di certificati a chiave pubblica
- Pubblicazione dei certificati in repository pubblici
- Emissione di Certificate Revocation List

Root Certificates

- Alcuni root certificates sono preinstallati nei browser
- Da qui possono essere aggiunti, eliminati e modificati



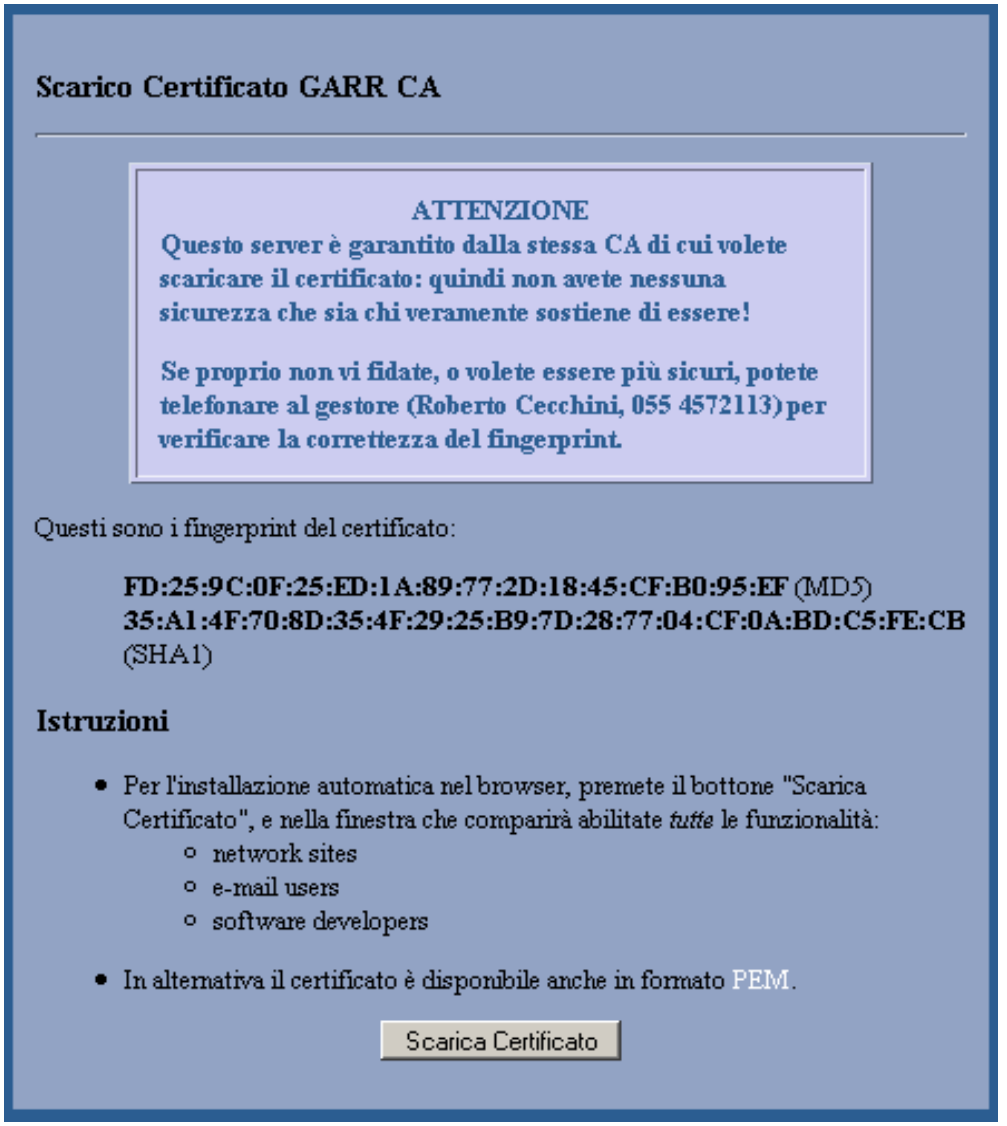


GARR Certification Authority

- Sito internet http://ca.garr.it/
- Indirizzo e-mail garr-ca@garr.it
- Spazio dei nomi /C=IT/O=GARR/OU=<>/CN=<>
- Rilascia certificati: *personali* e per *server*
- Validità dei certificati: un anno
- CRL: Version 1
- CP/CPS: disponibile in pdf - https://ca.garr.it/CPS/

Installazione certificato GARR CA

- Selezionare il link
  - Certificato GARR CA
- In Mozilla Firefox:
  - Abilitare le funzionalità come da istruzioni
- In Internet Explorer:
  - Apri ed installa
  - Problemi di accesso (IE7):
    - → installa e riavvia
- Controllare nei Root Certificates



End-Users

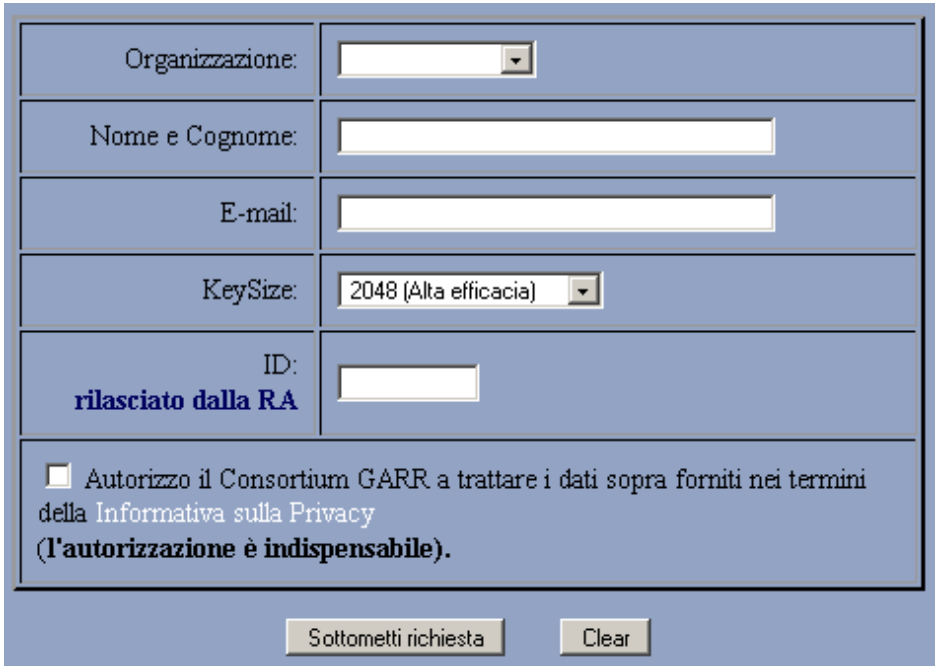
- Richiedere un certificato personale
  - nuovo
  - rinnovo
- Revocare un certificato personale
- Richiedere un certificato per server
  - nuovo
  - rinnovo
- Revocare un certificato per server

Richiedere un Certificato Personale Autenticazione

- L'utente si rivolge alla RA della struttura 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

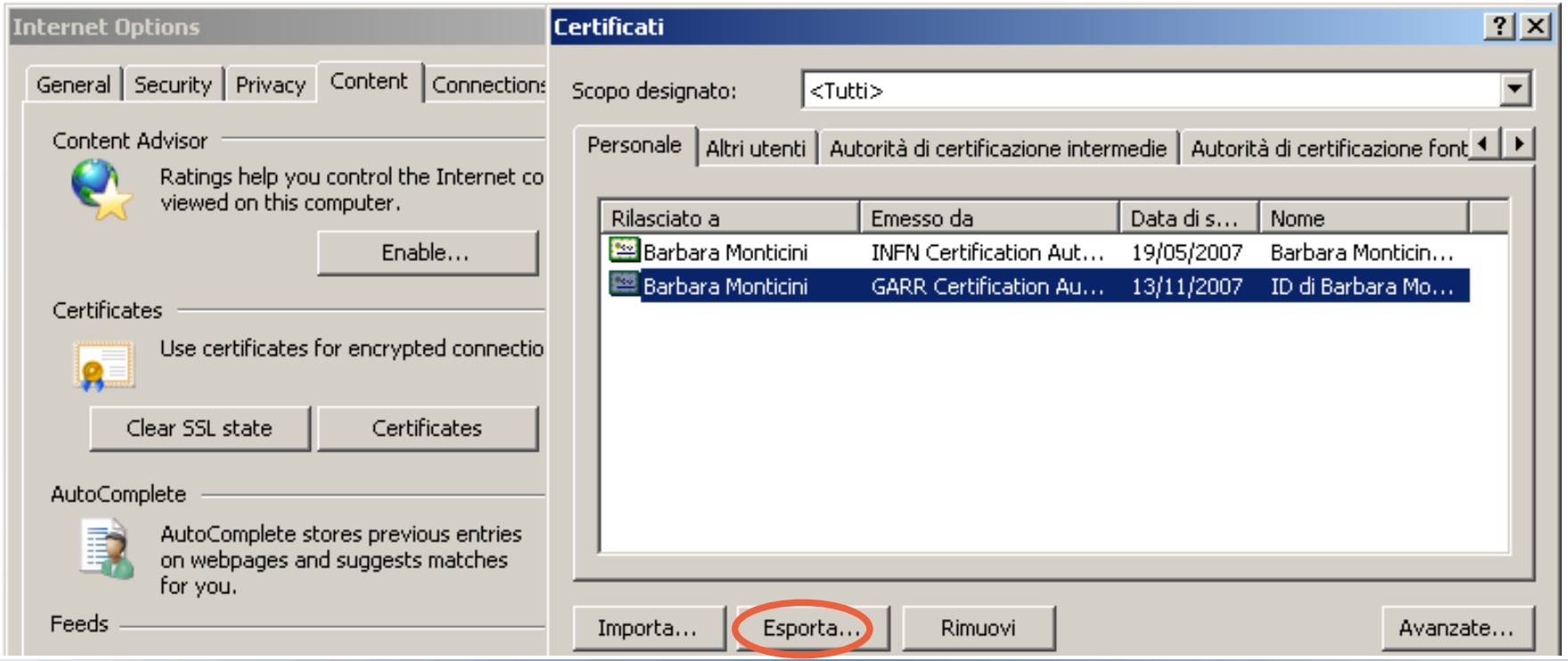
Richiedere un Certificato Personale Richiesta

- Installazione ed abilitazione del certificato della CA
- Nel **browser** avviene la generazione della coppia di chiavi:
  - la richiesta (chiave pubblica) arriva alla CA per la firma
  - la chiave privata è conservata nel browser
- Autorizzazione al Trattamento Dati Personali



Richiedere un Certificato Personale Installazione

- Il certificato emesso deve essere scaricato nel **browser** (lo **stesso** impiegato per la richiesta) da cui potrà essere successivamente esportato
- Procedere immediatamente al **backup**



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 competente per la struttura di riferimento
- Solo dopo l'approvazione della RA sarà emesso il certificato dell'utente
- Il certificato emesso deve essere scaricato nel **browser** da cui in seguito potra' 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
- Chi la deve richiedere
  - l'utente con mail firmata indicando il motivo e specificando nel soggetto il *numero di serie* del certificato
  - la RA se l'utente non è più in grado

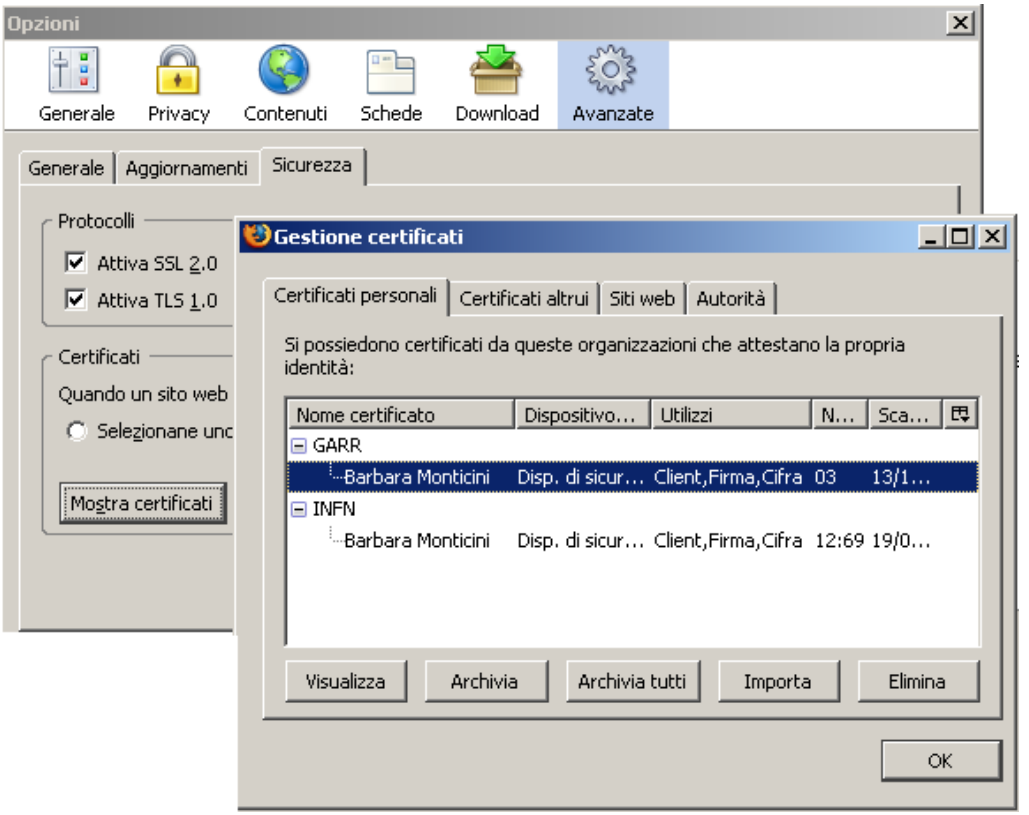
- Il *numero di serie* del certificato revocato sarà contenuto nella CRL emessa dalla CA

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



Richiesta Certificato Server

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

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

Iter di richiesta

- La richiesta <req.pem> deve essere spedita con e-mail firmata alla RA di competenza che la inoltrerà alla CA

- La CA invia - all'indirizzo contenuto nella richiesta - una e-mail per verificarne la validità
- Il certificato sarà emesso e spedito a suddetto indirizzo e-mail
- E' fondamentale eseguire il backup della chiave privata

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

Abilitazione al ruolo di RA

- Contattare il gestore della CA per prendere accordi
- Richiesta su carta intestata, protocollata e firmata dal direttore della struttura, spedita per posta ordinaria
- 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)
- Ottenere un certificato per la prima RA
  - autenticazione presso la CA
  - richiedere un certificato on-line
  - dimostrare di aver scaricato il certificato inviando un mail firmato

I compiti 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
  - 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

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 una e-mail firmata

Inoltro Certificati Server

1. Controllare le richieste pervenute:
   - FQDN nel soggetto
   - Controllare la correttezza dei campi del certificato
   - Firma nel messaggio
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.

Terena Server Certificate Service

- Servizio dedicato alle NREN per l'emissione di **certificati server**
- Risolve il cosiddetto *pop-up problem*
- Attivo da gennaio 2007
- Richieste per “server istituzionali”
- Attivare una RA locale