GARR

The Italian Academic & Research Network

www.garr.it

GARR CA

Corso per Utenti e Registration Authority

Barbara Monticini

Corso GARR CA, Sesto Fiorentino, 11.02.2010

Consortium GARR

Agenda

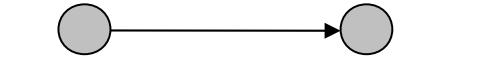
- 10:00 – 11:30 Istruzioni per utenti
- 11:30 Coffee break
- 12:00 – 13:00 Istruzioni per Registration Authority
- 13:00 Autenticazione delle future RA

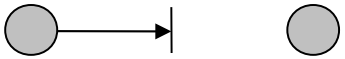
Sessione per Utenti

- Elementi di crittografia
- Certificati digitali X.509
- Procedure operative per gli utenti
- Uso dei certificati personali
- Comandi OpenSSL
- Procedure operative per i server
- Uso dei certificati server

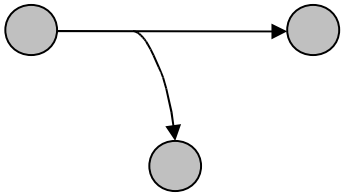
Attacchi

- Azioni che compromettono la sicurezza dei dati

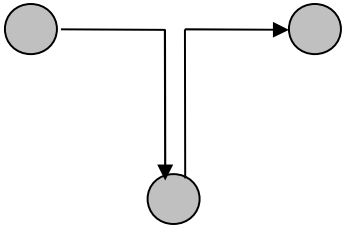




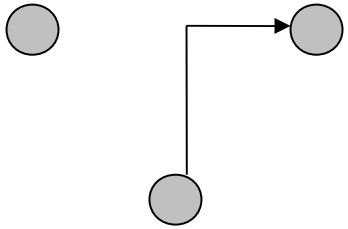
Interruzione



Intercettazione



Modifica



Fabbricazione

Servizi

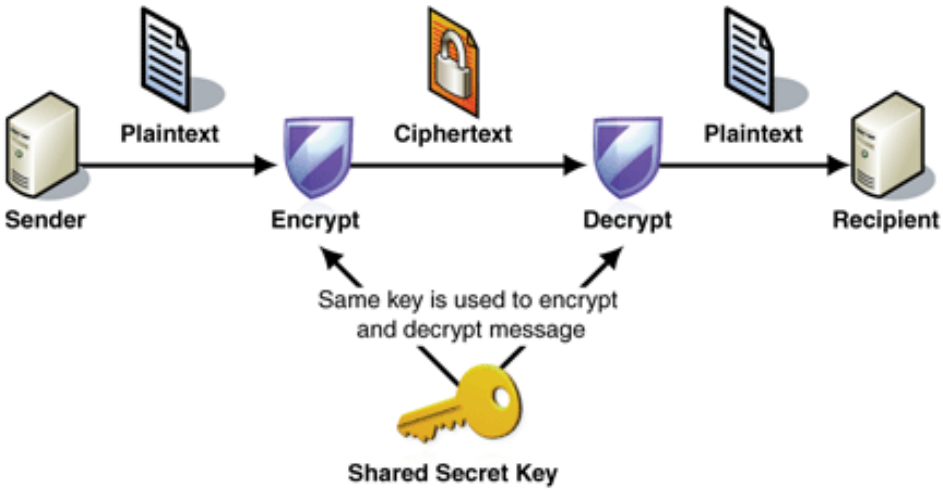
- **Autenticazione**: verificare l'identità di un soggetto
- **Autorizzazione**: controllo degli accessi
- **Non ripudio**: impedire al mittente e al destinatario di disconoscere i dati trasmessi
- **Riservatezza**: garantire che i dati in un sistema e i dati trasmessi siano accessibili solo a chi autorizzato
- **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**

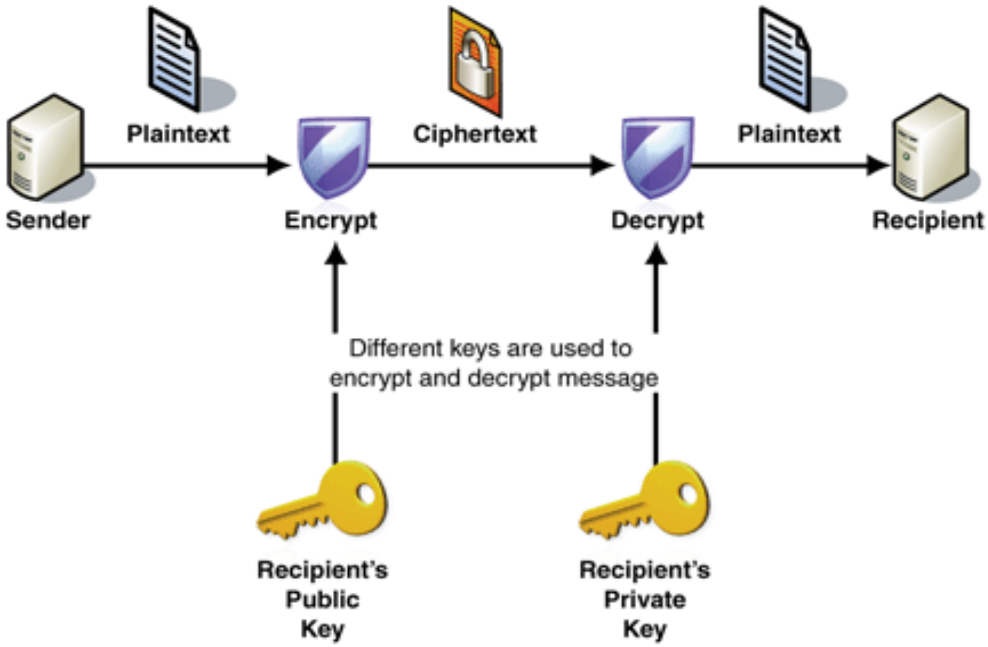
La crittografia a chiave segreta

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



Cifratura del testo e MAC

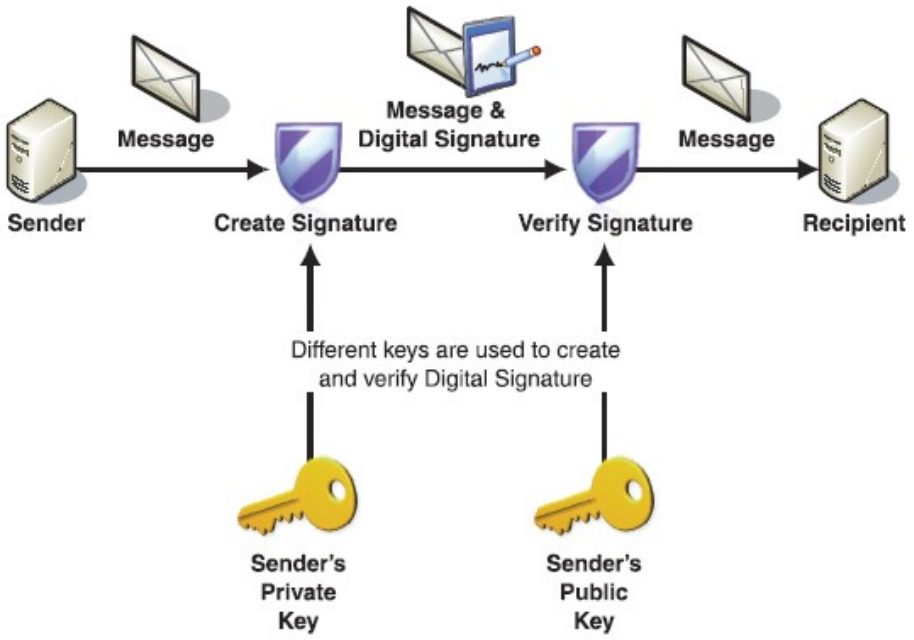
- Ha lo scopo di produrre un valore da usare per autenticare il messaggio (*authenticator*)
- **Message encryption**: il testo cifrato dell'intero messaggio funge da *authenticator*
  - crittografia convenzionale
  - crittografia a chiave pubblica
- **Message authentication code** (MAC): una funzione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

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. $H(y) = H(x)$

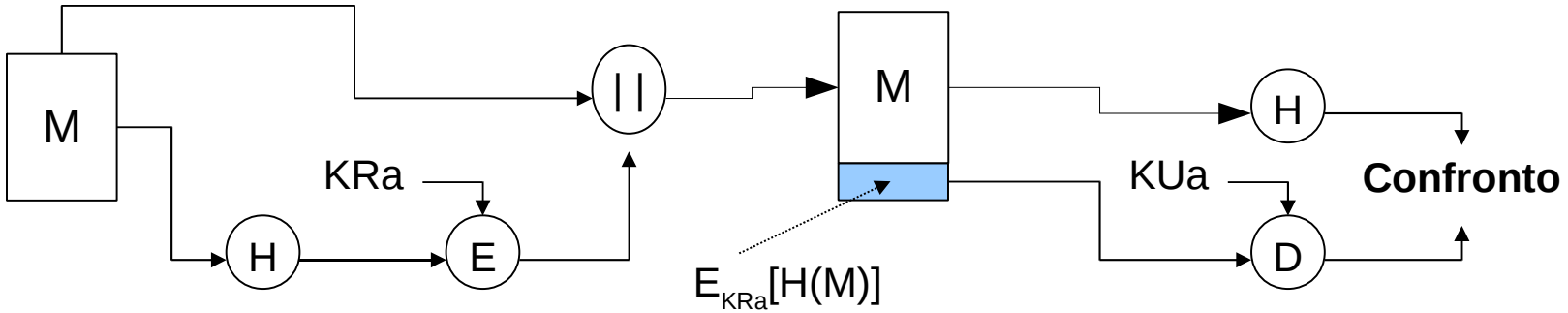
Firma digitale: Cifratura + Hash

- 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** KRa (*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** KUa del mittente
4. Se i due hash sono uguali il messaggio non è stato alterato



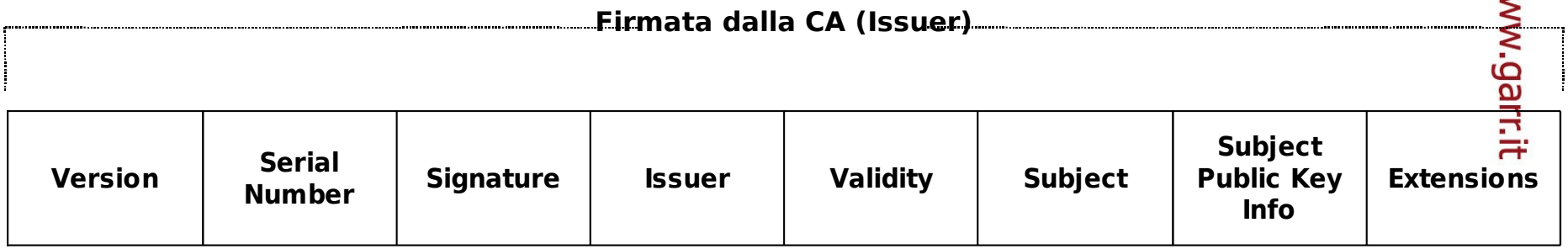
Distribuzione delle chiavi pubbliche

- 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)



- **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** - 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 anche la chiave privata del certificato.
- **.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 identificativi
  - sospetta compromissione della chiave privata
- Revocare certificati non più validi:
  - Certificate Revocation Lists - CRL: liste di certificati revocati firmate dalla CA
    - 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)

Version	Signature	Issuer	Last Update	Next Update	... List of revoked Certificates ...

- **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
- 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 di GARR CA (root cert.)

- Selezionare il link Certificato GARR CA
- Seguire le istruzioni a video e premere "scarica certificato"
  - Firefox: dare la fiducia a GARR CA per tutti gli utilizzi
    - FAQ - https://ca.garr.it/docs/faq.php#impexpMZ
  - IE: wizard di importazione automatica
    - FAQ - https://ca.garr.it/docs/faq.php#impexpIE

Certificati personali: Autenticazione

- L'utente si reca dalla RA della OU a cui afferisce:
  - 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

Certificati Personali: Richiesta

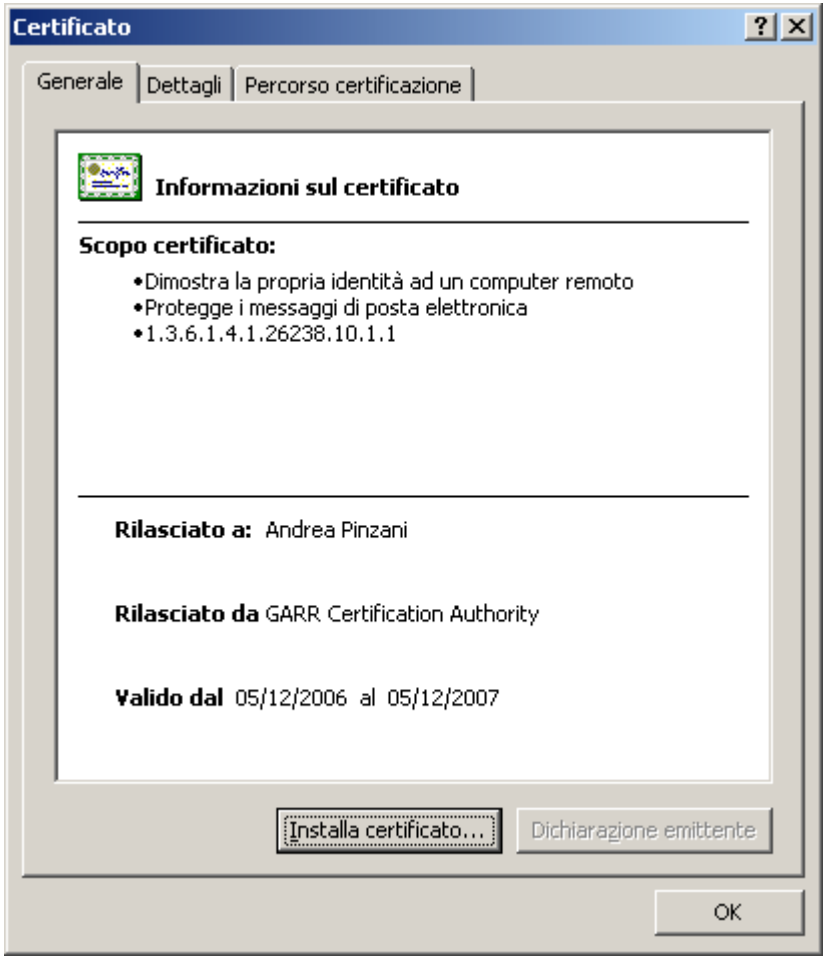
- Installare il certificato root GARR CA
- Sottomettere la richiesta on-line
  - https://ca.garr.it/mgt/restricted/ucert.php
  - Con Firefox
    - Impostare la **Master Password** per il Security Device
  - Con Internet Explorer
    - Impostare il **livello di protezione** della chiave privata su **alto** immettendo una nuova password
  - Con Safari
    - Impostare una **password** per il **Keychain**

Certificati Personali: Installazione

- Le istruzioni per scaricare il certificato sono inviate per **email dalla CA**
  - Oggetto: [GARR CA #n] Certificato per ...
- Aprire il link proposto nelle istruzioni usando lo stesso browser impiegato nella richiesta
- Installare il certificato nell'archivio dei certificati personali all'interno del browser
- Effettuare il backup del certificato
  - http://ca.garr.it/docs/faq.php#impexpIE
  - http://ca.garr.it/docs/faq.php#impexpMZ

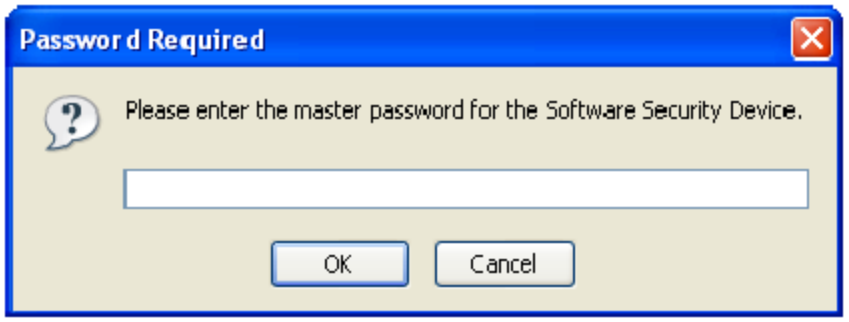
Installazione in Internet Explorer

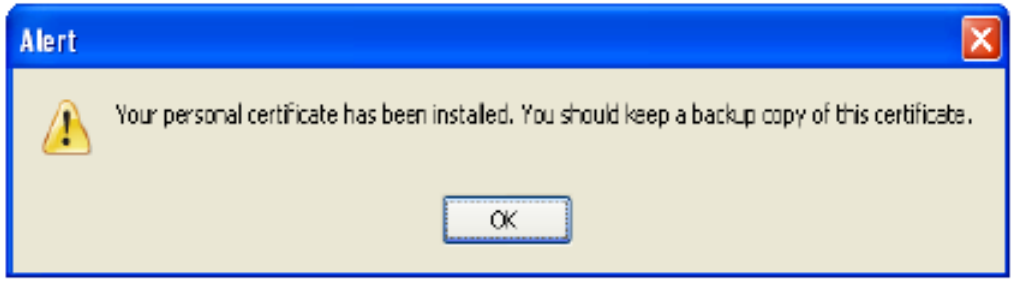
- Salvare il file come cert.pem e riaprirlo con doppio click
- "*installa certificato*"
- Seguire le istruzioni di windows
- Importante: **Chiave privata esportabile**



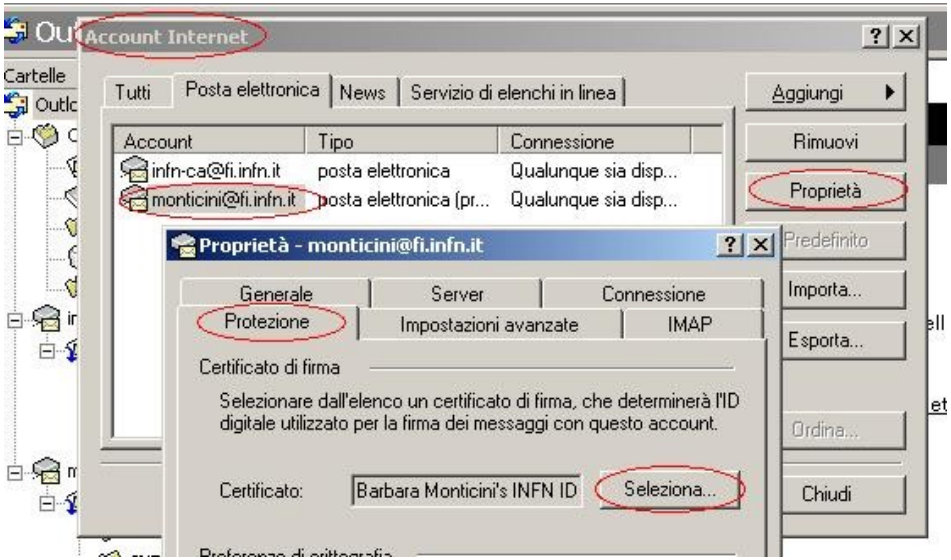
Installazione in Firefox

- Inserire la password se richiesto
- Firefox 1*:* pagina bianca, controllare tra i certificati
- Firefox 2 e 3*:* popup che notifica se l'instazione ha successo o meno



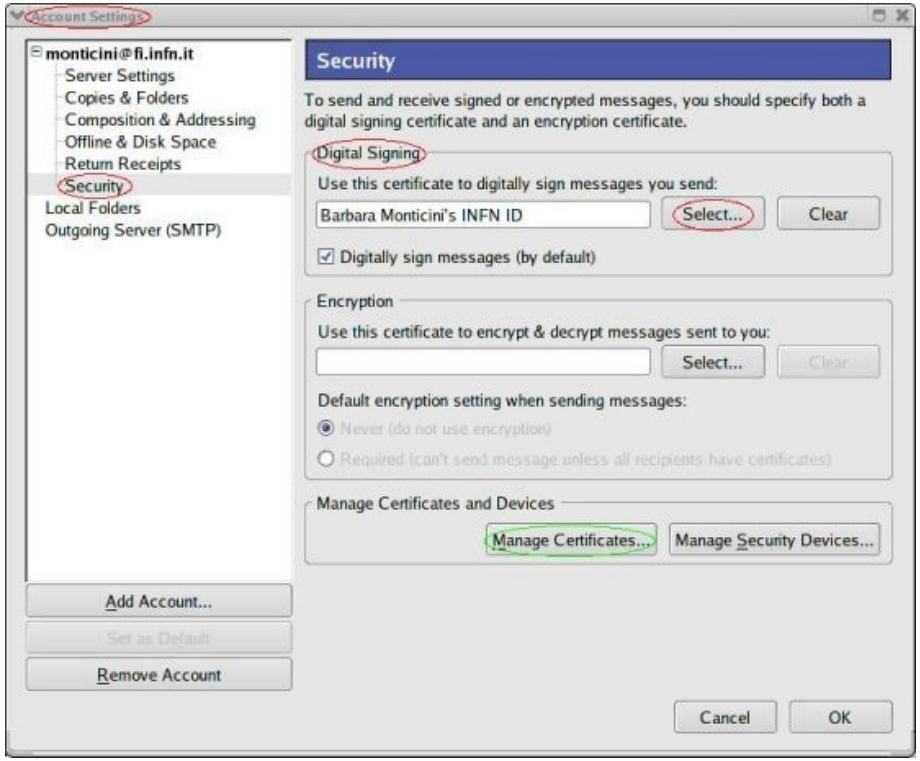


Firmare la posta con Outlook E.



- Nelle proprietà dell'acount alla voce **Protezione** selezionare un certificato
- Creare un messaggio ed abilitare la firma

Firmare la posta con Thunderbird



- Importare il certificato da *Opzioni/Avanzate/ Gestione certificati*
- Nelle proprietà dell'account alla voce **Sicurezza** selezionare il certificato
- Creare un messaggio ed abilitare la firma

Certificati personali: Rinnovo

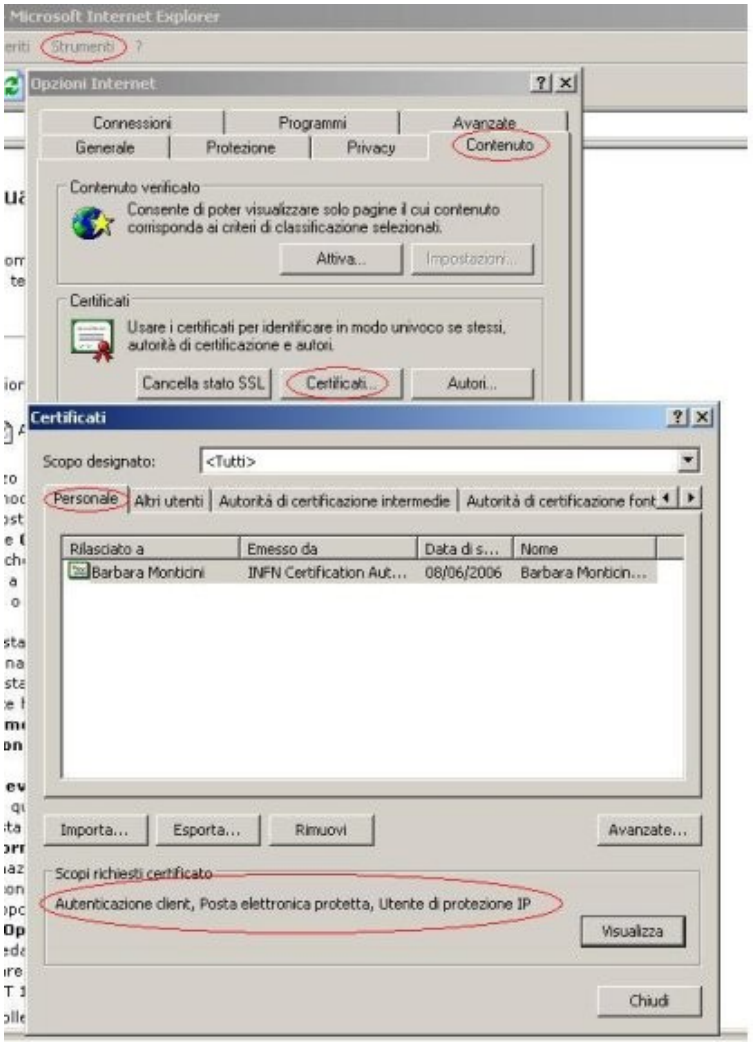
- Disponibile solo per chi possiede un **certificato valido** (non scaduto, non revocato)
- Richiesta **on-line da browser** che contiene il certificato non prima di 20 gg dalla scadenza
- Il rinnovo è subordinato all'**approvazione della RA** a cui si afferisce
- Una volta emesso si installa come in precedenza e si effettua il **backup**

Certificati personali: Revoca

- Deve essere richiesta nei seguenti casi:
  - Smarrimento o distruzione della chiave privata
  - Smarrimento della password di protezione della chiave privata
- Chi la richiede:
  - L'utente con **email firmata** indicando il *motivo* ed il *numero di serie*
  - La RA se l'utente non è più in grado
- Il *numero di serie* del certificato revocato sarà contenuto nella CRL

Trovare informazioni sui certificati

- http://ca.garr.it Consultazione certificati
- All'interno del browser:
  - IE da *Strumenti/Opzioni/ Contenuto/ Certificati SSL*
  - Firefox da *Strumenti/Opzioni/ Avanzate/Sicurezza/Mostra Certificati*



Certificati su LDAP

- Parametri necessari:
  - Server ca.garr.it
  - Porte: 389 (ldap) / 636 (ldaps)
  - Nessun utente (anonymous bind)
- Pubblicazione certificati:
  - utenti
  - server
  - CA (con aggiornamento della CRL)
- Rubrica LDAP su client di posta

Comandi Openssl: req

- Creare una richiesta con nuove chiavi senza password
  - openssl req -new -nodes -out req-server.pem -keyout key-server.pem -config host.conf
- Consultare una richiesta generata
  - openssl req -text -noout -in req-server.pem
- Creazione di un certificato self-signed
  - openssl req -x509 -new -out cert-server.pem -keyout key-server.pem

Comandi Openssl: x509

- Consultare un certificato:
  - openssl x509 -text -noout -in cert.pem
- Convertire dal formato .der a .pem
  - openssl x509 -noout -inform DER -in cert.der -outform PEM -out cert.pem
- Altre opzioni utili:
  - -enddate
  - -subject
  - -serial

Certificati server: Richiesta

- Generata dall'amministratore del server con comandi openssl
  - File di configurazione openssl fornito da GARR CA e disponibile sul sito
  - openssl req -new -nodes -out req.pem -keyout key.pem -config host.conf
  - Sono indicati:
    - C=IT
    - O=GARR
    - OU= <RA>
    - CN= <fqdn del server>
    - Email dell'amministratore del server

Certificati server: Nomi multipli

- Generata dall'amministratore del server con comandi openssl
  - Speciale file di configurazione openssl fornito da GARR CA (sul sito) denominato **host_multi.conf** che deve essere editato
    - Sezione **[server_cert]**
    - SubjectAltName = DNS:serverAltName1.your.dom, DNS:serverAltName2.your.dom, DNS:serverAltName3.your.dom
  - openssl req -new -nodes -out req.pem -keyout key.pem -config **host_multi.conf -reqexts server_cert**

Iter richiesta certificati server

1. La richiesta generata (**req.pem**) viene inviata con email **firmata** alla RA indicando nel soggetto il **fqdn** del server
2. La RA con email **firmata** inoltra alla CA
3. La CA invia, all'indirizzo indicato nella richiesta, una email per verificarne il funzionamento e **attende** una risposta
4. Il certificato viene emesso e spedito all'email specificata nella richiesta
5. L'amministratore che gestisce il certificato deve provvedere al **backup**

Certificati server: Rinnovo

- Consiste nella rigenerazione di una nuova richiesta di certificato (**req.pem**)
  - Anche per i nomi multipli
- Non può essere richiesto prima di 20 giorni dalla scadenza del certificato
- Segue lo stesso iter di una nuova richiesta
- A certificato emesso effettuare un backup
- Nel caso di smarrimento della chiave privata:
  - Chiedere prima la revoca e poi generare la richiesta

Certificati server: Revoca

- Deve essere richiesta nei seguenti casi:
  - Smarrimento della chiave privata
  - Violazione del sistema
- Richiesta dall'amministratore del server e inoltrata alla RA con email **firmata**:
  - Oggetto: indicare il **fqdn** del server ed il numero di serie del certificato da revocare
  - Body: indicare il **motivo** della revoca

Sessione Registration Authority

- Attivare una RA
- Il primo certificato
- Altri comandi openssl
- Procedure di una RA
- Certificati TCS

Iter di abilitazione al ruolo

- Contattare il gestore della CA per prendere accordi
- Definire il dominio di competenza a cui associare il cosiddetto campo **OU**
- Richiesta formale su **carta intestata**, **protocollata** e **firmata** dal responsabile della struttura, in originale
- La richiesta deve indicare:
  - Minimo due persone per il ruolo di RA
  - Il valore del campo OU

Il certificato personale di una RA

- Ottenere un certificato personale per la prima RA:
  - Autenticazione presso la CA
  - Richiesta certificato on-line
  - Inviare una mail firmata alla CA
- Le altre RA della stessa OU:
  - Autenticazione presso la RA abilitata
  - Richiesta certificato on-line
  - Inviare una mail firmata alla CA

Ambiti di intervento di una RA

- Richiesta di un nuovo certificato personale
- Richiesta di rinnovo certificati personali
- Richiesta di certificati per server
  - Nuove richieste
  - Rinnovi di certificati esistenti
- Richiesta di revoca di certificati
  - Personale
  - Per server

Autenticazione degli utenti

- Riconoscimento **de-visu** dell'utente
- Accesso on-line con certificato personale
- La procedura fornisce un **codice numerico** da comunicare di persona all'utente

Rinnovo certificati personali

- Ogni rinnovo è sottoposto all'**approvazione** della RA competente
- La RA riceve dalla CA un'email per ogni richiesta di rinnovo di certificato utente
- Per approvare il rinnovo è sufficiente rispondere affermativamente al suddetto messaggio con **email firmata**

Inoltro richieste certificati server

- Controllare le richieste ricevute dagli amministratori dei server
  - Fqdn del server nel soggetto della mail
  - Firma digitale del richiedente
  - Presenza del file PEM
- Inoltrare le richieste alla CA
  - Inoltro come **attachment** (non in-line)
  - Firmare digitalmente il messaggio
  - Attendere la notifica dell'emissione

Revoca certificati personali

- Necessaria per utenti che non possiedono più il certificato personale
- Come richiere la revoca:
  - **Email firmata** alla CA
  - Oggetto:
    - **Nome e cognome** dell'intestatario
    - **Numero di serie** del certificato
  - Body:
    - Descrivere il **motivo** della revoca

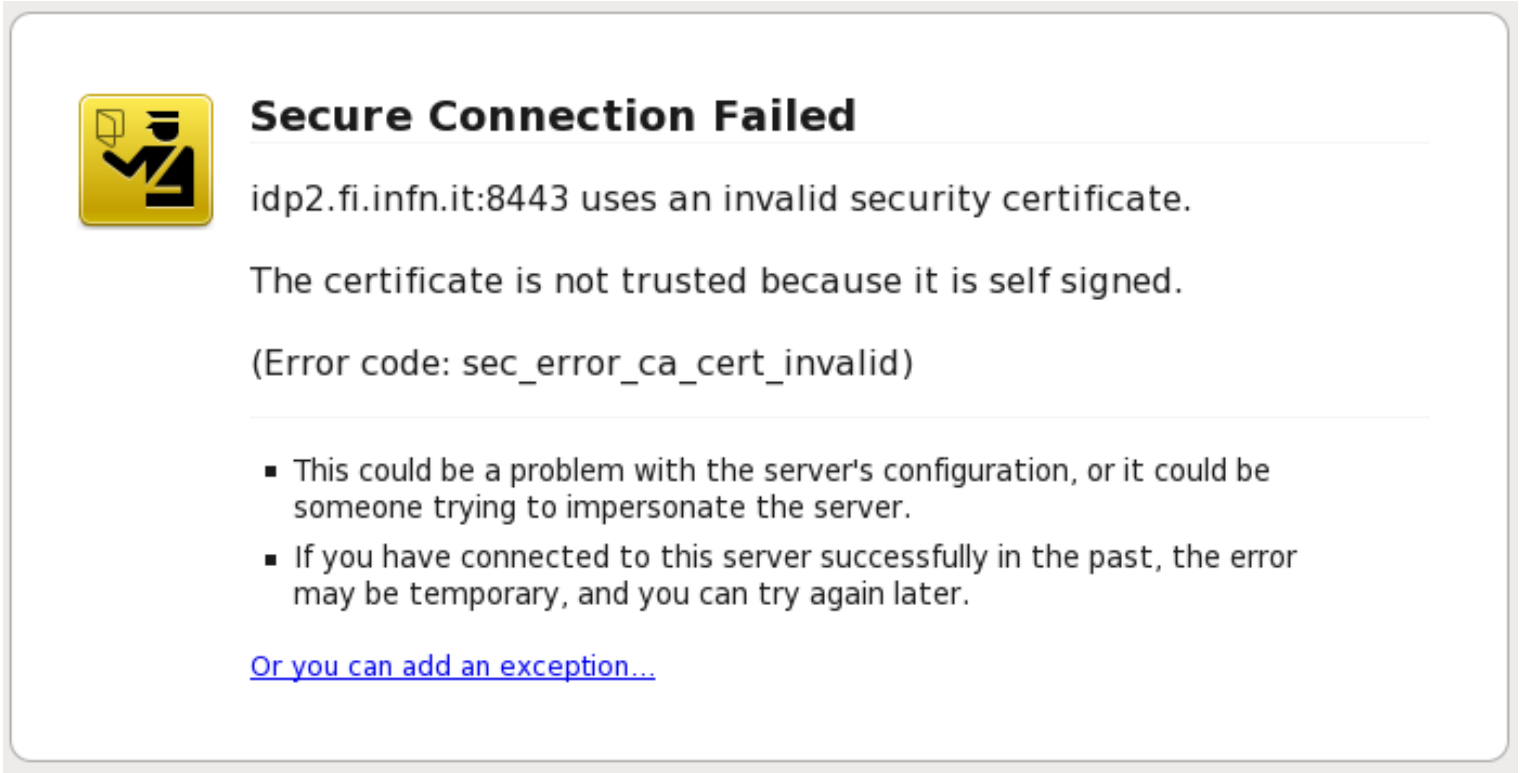
Revoca certificati server

- Può essere richiesta alla CA solo da parte di una RA (su richiesta dell'amministratore del server)
- Come richiedere la revoca:
  - **Email firmata**
  - Oggetto:
    - **Numero di serie** del certificato
    - **Fqdn** del server a cui è rilasciato
  - Body:
    - Indicare il **motivo** della revoca

Terena Certificate Service (TCS)

- Servizio di rilascio certificati X.509 per server, emessi da una Certification Authority commerciale (**COMODO CA)** riconosciuta dalla grande maggioranza dei browser web attualmente in uso
- Risolve il cosiddetto problema del *pop-up*
- E' offerto *gratuitamente* da **GARR** alla Comunità delle Università e della Ricerca Scientifica
  - I certificati non possono essere usati per proteggere transazioni monetarie

Pop-up problem



La catena dei certificati TCS

- Certificati emessi da **Terena SSL CA**
  - /C=NL/O=TERENA/CN=TERENA SSL CA
- Terena CA è subordinata di una delle CA di COMODO
- E' importante **configurare** correttamente la catena dei certificati sul server
  - https://ca.garr.it/mgt/Terena-chain.pem
  - https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=95&pcid=1&nav=0,1

Figure coinvolte in TCS

- *Subscriber*
  - Ente a cui viene emesso il certificato, individuato nel suo **legale rappresentante**
- *Administrative Contact*
  - Persona di fiducia eletta dal Subscriber
  - Responsabile effettivo delle procedure di richiesta certificati
- *Access Port Administrator*
  - APA della rete GARR responsabile dei nomi a dominio intestati all'Ente

Documenti per l'adesione

- Facsimili scaricabili da http://ca.garr.it/TCS
  - Subscriber Agreement
    - Sottoscritto dal legale rappresentante dell'Ente (Rettore, Prorettore, Dirigente Amministrativo ...)
  - Dichiarazione dei Contatti Amministrativi
    - Una per ogni Contatto nominato
  - Dichiarazione di responsabilità dei domini
    - Sottoscritta dall'APA
    - Elenco dei domini di secondo livello per i quali saranno richiesti certificati

Richieste di certificato TCS

- Le richieste sono sottomesse dai *Contatti Amministrativi* su apposita **form on-line** accessibile tramite **certificato** abilitato
- Le richieste possono essere generate dagli amministratori dei server e poi inoltrate agli opportuni *Contatti Amministrativi*
- Le richieste saranno evase solo dopo l'**approvazione firmata** (con certificato personale) di un *Contatto Amministrativo*
  - Il contatto è obbligato a conservare tutta la corrispondenza che riguarda TCS

Generare una richiesta TCS

- E' possibile usare il comando
  - openssl req -new -nodes ...
- Comodo fornisce una serie di istruzioni per generare le richieste su vari dispositivi:
  - Microsoft IIS
  - Apple Mac OS X Server
  - Java-based Webservers (using keytool)
  - ...
    - https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1

Contenuto di una richiesta TCS

- Tutte le richieste saranno processate secondo queste regole:
  - **C = IT**
  - **O =** <nome legale dell'Ente>
    - Entrambi sovrascritti automaticamente
  - *OU = <facoltativo>*
  - L = rimosso automaticamente
  - ST = rimosso automaticamente
  - **CN =** <fqdn del server>
    - Appartente ai domini dichiarati dall'APA

Richiesta via form on-line

www.garr.

Certificate Request in PEM format:

```
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMSqHcKMAhNQpfc7TcDMezjdToCBdUpR
/bwc6Di9YGglHKZ2zKap9Yhr+Xxf08yAMaJx9CYlMPld7yG/JPA4khrmTl3NdQzZ
IT83PBBT6uK1GPHeXE0Meh8KyYyqMQwIZHSKFICJxUXUKnljjR7jaJCp20ruldyB
kT38AgvxLU+arVCsM8Xx9FAESLncYrawgW7HJWroo/QWLXyPyY21mlCyZ7yJIDLl
hVLaEqVwHd23fIEtuczwW443udL/e7VjsQ9+SRB7rghY+FqqaJvKnUFf2w4YJeui
nJCJIXX+7POCFTu+meTnitVoBTQM8C50Nlr6Hhy+MlbsirQeqc8FlzkCAwEAAaAA
MA0GCSqGSIb3DQEBBAUAA4IBAQClH/joH62dMPnddbp/g0Fn9mHeRbRMKFzIP+ZJ
LBkqxRCSubvOGCfAiGAUEREMJSFkbFxmhItTjlJWKipxp9gVxW9Clhck08N94tYD
ySisVkhFwC3DYTY5EuS7dbip1YSNtQwoULabfnfmNkahVKJNXlZ1mDVi4MN6iCkZ
cQEIF/goosX1Iz4UbFt2srPEbzQxJHTJt5kGwiVY07Vf3J8c9xZmRKiEu70PFOgx
daQiQTXlvanRd3cYtVr9mV4FTYja1Cinfa43Oy/9cgYwvSahGoJ8iqvfeX8vg9qo
5A2Vg7mxfxnhXuh1i6iMqAxUE6q27+A5XdF+gpQkiK2wiqeU
-----END CERTIFICATE REQUEST-----
```

Alternatively, a file containing the CSR: Browse...

Certificate Valid for: 3 years

Certificate Variant: Normal certificate (Unicode)

Requestor Email: admin@garr.it

Check and Update

subjectAltNames

Key Size:	2048
Certificate Valid for:	3 years
Certificate Variant:	Normal certificate (Unicode)
Name components from the request:	
Common Name:	sp2.fi.infn.it
Subject Alternative Names: (one per line)	
Organizational Unit:	Sede di Firenze
Name components from the customer information:	
Organization:	Consortium GARR
Country:	IT
Additional Information:	
Requestor email:	admin@garr.it

* wildcards

- E' possibile richiedere nomi con wildcard
  - Nel CN
  - Nel subjectAltName
- * non fa matching con il punto
  - *.domain.it non autentica www.subd.domain.it
  - Firefox mostra un messaggio di errore

Revoca di certificati TCS

- E' richiesta da uno dei Contatti Amministrativi
  - **Email firmata** con il proprio certificato personale a tcs-ra@garr.it
    - **CN** del certificato
    - Il **numero** (o il serial number) del certificato
    - Il **motivo** della revoca
  - Il numero del certificato è contenuto nell'e-mail di conferma di emissione.

Riferimenti TCS

- TERENA
  - http://www.terena.nl/tcs
- GARR CA
  - http://ca.garr.it/TCS/
  - http://ca.garr.it/TCS/FAQ.php
- COMODO : istruzioni per generare una csr ed installare un certificato
  - https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1
  - https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=95&pcid=1&nav=0,1

Riferimenti

- 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/