



Roma, 2-3 Dicembre 2010

Ministero dell'Istruzione, dell'Università e della Ricerca

GARR Certificate Service & Federazione IDEM

Simona Venuti - GARR

Agenda

- I certificati offerti da GARR Certificate Service
- Introduzione ai sistemi di certificazione
 - Chiave simmetrica
 - Chiave asimmetrica
 - Catena di Certification Authority (CA)
- GARR-CA e TCS e-science (personal/server)
 - Procedure di adesione e policy
 - Caratteristiche dei certificati
 - Dettagli tecnici per ottenere certificati

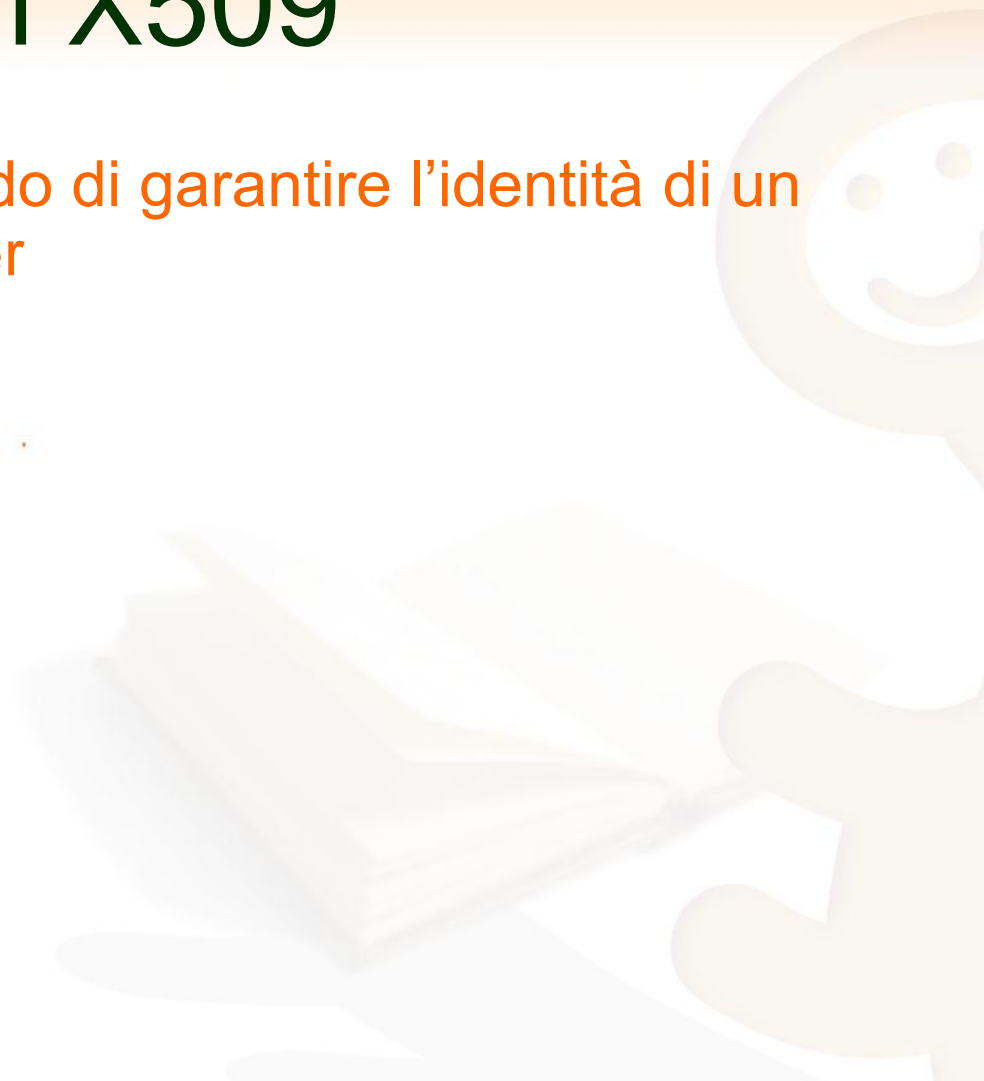
GARR Certificate Service

- Cosa è:
 - Emissione di certificati digitali
 - Certificati personali e certificati server
- Il servizio si rivolge a tutti gli Enti connessi con la rete GARR
- Il servizio è gratuito per tutti gli Enti di cui sopra indipendentemente dal numero di certificati richiesti ed emessi

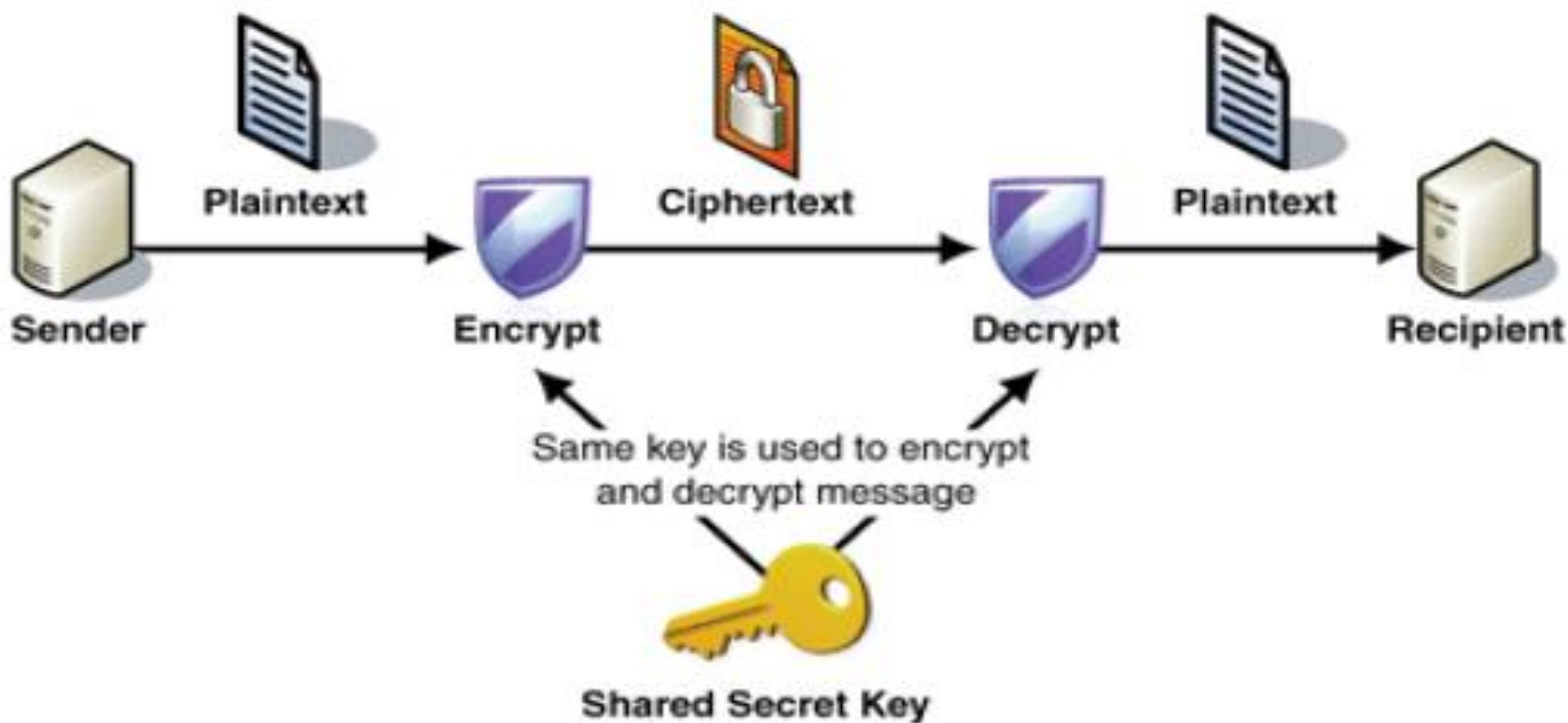
Certificati digitali X509

Sono file elettronici in grado di garantire l'identità di un soggetto, persona o server

- Autenticazione
- Autorizzazione
- Non ripudio
- Riservatezza
- Integrità
- Disponibilità

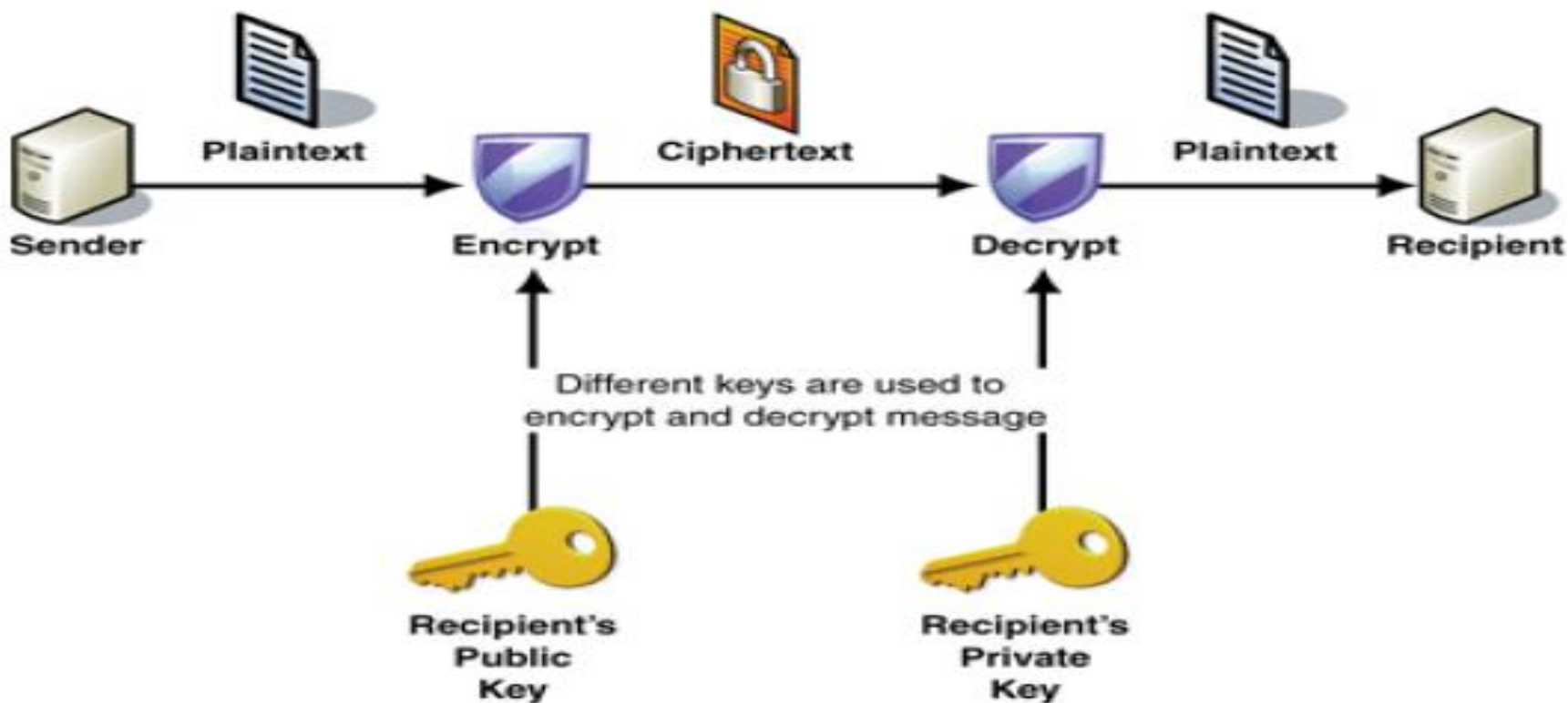


Chiave simmetrica



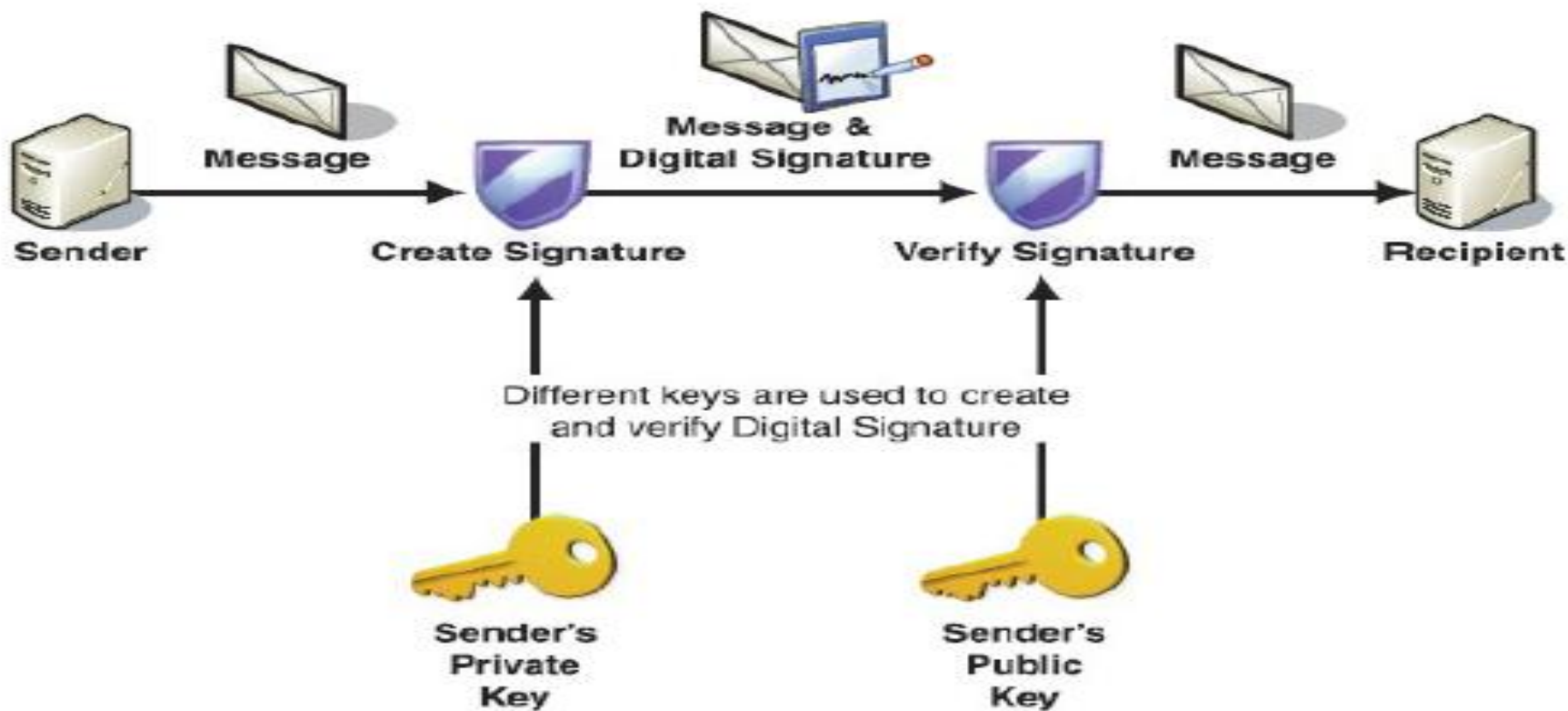
Slide gentilmente «rubata» a Barbara Monticini

Chiave pubblica: crypt



Slide gentilmente «rubata» a Barbara Monticini

Chiave pubblica: firma



Slide gentilmente «rubata» a Barbara Monticini

Problemi di «identità»

- Un certificato digitale è una coppia di file che mi garantisce identità del soggetto richiedente
- Può essere chiesto ed emesso da chiunque a nome di chiunque

Serve un «**Ente Certificatore**» (CA)

che stabilisca modalità e procedure

in grado di rendere validi e utilizzabili i certificati

Compiti di una CA:

- Garantire e divulgare le procedure di identificazione (persona|server)/certificato
- Stabilire e divulgare le policy del servizio
- Stabilire e divulgare le caratteristiche dei certificati
- Mantenere i certificati sul sito web
- Mantenere e firmare la CRL

A seconda del tipo di politica e procedure cambia l'affidabilità di una CA: i certificati possono essere utilizzati in contesti diversi a seconda del grado di affidabilità richiesto da un servizio

GARR-CA

■ Sistema di CA gerarchico

■ GARR-CA (Certification Authority)

- Stabilisce le procedure
- emette i certificati

■ GARR-RA (Registration Authority)

- Delegati all'identificazione degli utenti
- Delegati all'autorizzazione al rilascio di certificati personali e server

■ Procedure di identificazione

- Identificazione dell'utente «de visu» con la RA tramite un documento di identità valido
- Registrazione del codice fiscale dell'utente

Certificati GARR-CA

- Spazio dei nomi:
 - C=IT, O=GARR, OU=GARR, OU=Firenze, CN=Simona Venuti
 - C=IT, O=GARR, OU=GARR, OU=Direzione, CN=www.garr.it
- Validità un anno dalla emissione
- Servizi che richiedono certificati GARR:
 - GARR-RA
 - Alcuni servizi critici GARR
 - Contatti Amministrativi per il servizio TCS

Adesione GARR-CA

(Tutti i documenti dovranno essere scritti su carta intestata, protocollati e spediti in originale)

- Lettera di nomina del Rettore o Direttore
 - Nomina di almeno due membri RA
 - Scelta del campo o dei campi OU
- Dichiarazioni giurate dei membri RA
- Rilascio dei certificati personali per le RA
 - Incontro «de visu» con la CA
 - Consegna del codice identificativo
- Richiesta mail firmato RA
 - Ogni membro RA è tenuto ad installare il certificato nel client di posta e mandarci un mail firmato per dimostrare che sa usare il certificato

Emissione cert. Personali (1/3)

- L'utente si reca di persona dalla sua RA con un documento di riconoscimento e codice fiscale
- La RA inserisce i dati dell'utente (nome, cognome, documento, CF, mail) in una form web
- Il sistema restituisce un numero che deve essere consegnato di persona all'utente: non è ammesso l'invio per mail, telefono, skype...

Emissione cert. Personali (2/3)

- L'utente dal proprio PC inserisce in una form web i propri dati, insieme al codice ricevuto, per sottomettere la richiesta di certificato
- La chiave privata del certificato viene generata automaticamente nel browser
- La chiave pubblica viene automaticamente spedita alla CA per la firma

Emissione cert. Personali (3/3)

- La CA verifica che l'utente sia stato in persona dalla RA
- La CA verifica che i dati inseriti dall'utente corrispondano con quelli della RA
- La CA verifica che il codice inserito dall'utente sia effettivamente quello assegnato dal sistema
- La CA firma il certificato
- La CA spedisce un mail all'utente con un link dove scaricarsi il proprio certificato firmato

Emissione cert. Server (1/2)

- L'amministratore del server genera una richiesta di certificato server (CSR)
- L'amministratore del server manda la CSR alla propria RA tramite mail firmato con il proprio certificato personale
- La RA inoltra alla CA, con mail firmato, la CSR in modo da verificare la doppia firma nel messaggio (sia amministratore che RA)

Emissione cert. Server (2/2)

- La CA verifica la doppia firma
- La CA verifica che il server abbia una risoluzione valida nel DNS
- La CA verifica la correttezza dei campi nel certificato (OU di appartenenza, nome host)
- La CA spedisce un mail di conferma all'indirizzo contenuto all'interno della CSR per verificare che esista
- La CA emette il certificato
- La CA spedisce il certificato server alla RA e al «requestor address» inserito nella CSR

Terena Certificate Service-TCS

- Sistema di CA gerarchico
 - Comodo-CA Limited (Certification Authority)
 - Stabilisce le procedure
 - emette i certificati
 - CN=AddTrust External CA Root
 - Certification Authority Intermedia
 - UTN-USERFirst-Hardware
 - TERENA SSL CA (Certification Authority)
 - Tramite fra Comodo CA e le NREN
 - TCS-RA (Registration Authority – GARR)
 - Valuta le procedure di adesione
 - Approva l'emissione dei certificati

Certificati TCS (1/2)

- Eliminano il «problema del pop-up»
- 4 tipi di certificati diversi
 - TCS server } general purpose
 - TCS personali } general purpose
 - TCS e-science server } accesso alle GRID
 - TCS e-science personal } accesso alle GRID
- Validità da uno a tre anni
- Servizi o possibilità di utilizzo
 - universalmente riconosciuti dai comuni browser e client che supportano protocollo SSL (client mail etc)

Certificati TCS (2/2)

- Spazio dei nomi

- TCS server

C=IT/O=Nome ufficiale dell'Organizzazione/OU=Unità (facoltativo) /CN=FQDN del server

- TCS personali

C=IT/O=GARR/CN=Simona

Venuti/unstructuredName=venuti@garr.it

- TCS e-science server

DC=org/DC=terena/DC=tcs/C=IT/O=Nome ufficiale dell'Organizzazione/OU=Unità (facoltativo) /CN=FQDN del server

- TCS e-science personal

/DC=tcs/DC=terena/DC=org/C=IT/O=GARR/CN=Simona

Venuti venuti@garr.it

e-science e UNICODE

- **Certificati e-science server**
 - Eventuali caratteri non ASCII nel campo «O» saranno eliminati a «monte» da GARR
 - Non è possibile inserire un carattere non ASCII nel nome del server, indipendentemente da TCS
- **Certificati e-science personali**
 - Eventuali caratteri non ASCII nel campo «O» saranno eliminati a «monte» da GARR
 - Caratteri non ASCII in nome e cognome dell'utente sul back-end verranno trasformati in lettere semplici (senza apostrofo) in automatico

Adesione a TCS (1/4)

(Tutti i documenti dovranno essere scritti su carta intestata, protocollati e spediti in originale)

■ Lettera di adesione:

- Firmata dal Rettore, Direttore, Legale Rappresentante con delega alla firma
- Nome “legale” dell'Ente (quello registrato ufficialmente) che diventerà il campo “O”
- Dichiarata di aver letto il CP/CPS
- Dichiarata di non usare i certificati per transazioni monetarie
- Nomina almeno 2 contatti amministrativi

Adesione a TCS (2/4)

- Dichiarazione dei Contatti Amministrativi
 - Legge e comprende i termini del servizio
 - Si impegna a seguire il CP/CPS
 - Si impegna a conservare copia comunicazioni con la CA
 - Si impegna a collaborare auditing
 - Dichiara di non utilizzare i certificati per transazioni monetarie
 - Si impegna ad approvare solo richieste della sua struttura
 - Si impegna a non installare i certificati prima di aver visto i contenuti
 - Si impegna a prevenire la compromissione della chiave privata
 - Si impegna a comunicare immediatamente la compromissione a GARR-CA
 - Assiste gli utenti e amministratori dei server per problemi di gestione
 - Si impegna a far cessare l'utilizzo di certificati scaduti o revocati

Adesione a TCS (3/4)

- Dichiarazione Access Port Administrator
 - Dichiarare quali sono i domini di competenza della struttura
 - Solo per i domini che hanno macchine che stanno su IP assegnati sulla rete GARR

Adesione a TCS (4/4)

- Tutti i contatti amministrativi devono possedere un certificato personale della GARR-CA
 - **Autorizzazione/Autenticazione**
 - Devono recarsi fisicamente presso la GARR-CA a Sesto Fiorentino oppure farsi autenticare di persona a eventi o convegni da membri della CA
 - Possono fare autenticazione tramite una sessione skype registrata in audio e video
 - **Una volta autenticati ricevono il codice per fare la richiesta di certificato**

Adesione a TCS Personal ed e-science Personal

- Dichiarazione del Legale Rappresentante (Rettore o delegato alla firma o Direttore, o Referente Amministrativo IDEM)
 - dichiara, **sotto la propria responsabilità**, che verranno abilitati a richiedere certificati personali e personali e-Science, **nell'ambito del servizio Terena Certificate Service**, solamente quegli utenti la cui identità è stata accertata **de visu**, dietro presentazione di un documento di identità con validità legale.
 - **Indica il valore dell'attributo EduPersonOrgDN**
 - Concordato precedentemente con il servizio GARR-CS

La struttura deve avere un IdP in Federazione IDEM

Configurazioni per Cert. personali

- Aderire a TCS
- Compilare la documentazione (RL)
- Ottenere certificati personali GARR-CA per i Contatti Amministrativi
- Aderire alla Federazione IDEM
- Configurare IdP e back-end db degli utenti come segue

Configurazione IdP IDEM

- E' necessario aderire alla Federazione IDEM
- Configurare attribute-resolver.xml e attribute-filter.xml in modo da rilasciare i seguenti attributi
 - eduPersonOrgDN
 - cn
 - eduPersonPrincipalName
 - eduPersonEntitlement
 - mail

Configurazione back-end

- eduPersonOrgDN:
 - Stesso valore per tutti gli utenti dell'Organizzazione
 - Concordato con la GARR-CA
 - Per convenzione: l'attributo “scope”
 - Nella forma dc=scope, dc=it
- Per chi può ottenere il certificato personale:
 - eduPersonEntitlement:
 - urn:mace:terena.org:tcs:personal-user
 - urn:mace:terena.org:tcs:escience-user

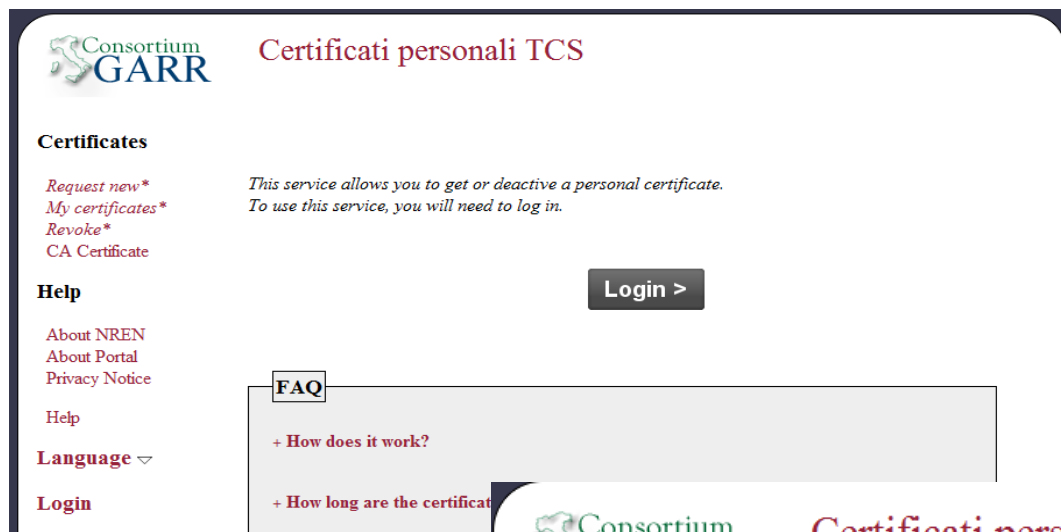
Esempio pratico: IdP GARR

```

<AttributeFilterPolicy id="TCSPERSONAL">
  <PolicyRequirementRule xsi:type="basic:AttributeRequesterString« value="https://tcs-personal-portal.terena.org/simplesamlphp/module.php/saml/sp/metadata.php/default-sp"/>
    <AttributeRule attributeID="eduPersonEntitlement">
      <PermitValueRule xsi:type="basic:OR" />
        <basic:Rule xsi:type="basic:AttributeValueString"
          value="urn:mace:urn:mace:terena.org:tcs:personal-user" ignoreCase="true" />
        <basic:Rule xsi:type="basic:AttributeValueString"
          value="urn:mace:urn:mace:terena.org:tcs:escience-user" ignoreCase="true" />
      </PermitValueRule></AttributeRule>
    <AttributeRule attributeID="mail">
      <PermitValueRule xsi:type="basic:ANY" /></PermitValueRule></AttributeRule>
    <AttributeRule attributeID="transientId">
      <PermitValueRule xsi:type="basic:ANY" /> </PermitValueRule></AttributeRule>
    <AttributeRule attributeID="eduPersonOrgDN">
      <PermitValueRule xsi:type="basic:ANY" /></PermitValueRule></AttributeRule>
    <AttributeRule attributeID="cn">
      <PermitValueRule xsi:type="basic:ANY" /> </PermitValueRule></AttributeRule>
  </AttributeFilterPolicy>
    
```

Richiesta certificati personali 1/2

l'utente finale è autonomo nella richiesta del certificato



Consortium GARR Certificati personali TCS

Certificates

- Request new*
- My certificates*
- Revoke*
- CA Certificate

This service allows you to get or deactivate a personal certificate. To use this service, you will need to log in.

Help

- About NREN
- About Portal
- Privacy Notice
- Help

Language ▾

Login

Login >

FAQ

- + How does it work?
- + How long are the certificates valid?



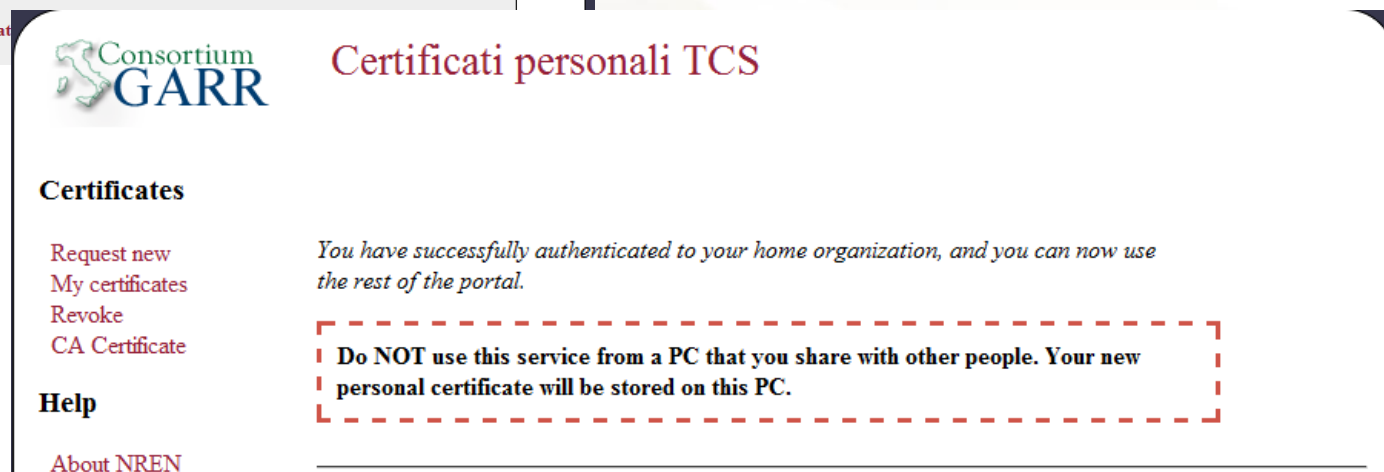
idem garr

Selezioni la sua Home Organisation

È necessario autenticarsi per poter accedere alla risorsa sull' host 'tcs-personal.garr.it'.

GARR

Ricorda la selezione per questa sessione.



Consortium GARR Certificati personali TCS

Certificates

- Request new
- My certificates
- Revoke
- CA Certificate

Help


- About NREN

You have successfully authenticated to your home organization, and you can now use the rest of the portal.

Do NOT use this service from a PC that you share with other people. Your new personal certificate will be stored on this PC.

Richiesta certificati personali 2/2

l'utente finale scarica subito il certificato che ha richiesto



Certificati personali TCS

Certificates

[Request new](#)

[My certificates](#)

[Revoke](#)

[CA Certificate](#)

Help

[About NREN](#)

[About Portal](#)

[Privacy Notice](#)

[Help](#)

View menu

[User](#)

[NREN-Admin](#)

Language ▾

Please choose one of the options available below to create your certificate.

You have several different ways of creating the certificate, ranging from a complete in-browser experience to different ways of uploading an existing CSR.

If you are unsure about what an CSR is, you probably want the in-browser approach.

Browser generation
Upload CSR
Paste CSR

Acceptable Use Policy (AUP)

I hereby state that I will adhere to the Requester's obligations as stated in the CPS.

[+ more](#)

Privacy notice:
Per l'utilizzo del servizio sono necessa ... ▾

Log out

Apply for a certificate in browser

*Press the start button **once** to generate a certificate request in your browser.*

Sometimes it will take a little while until you can see a browser reaction and there can be delays between browser actions.

Each certificate can contain zero, one or more of your email-addresses depending on how the portal has been configured. We have registered that you have 1 registered addresses.

*With the current settings, you can choose freely how many of your registered addressed you want in the certificate. Note, if you uncheck **all**, no address will be added to the certificate. This is most likely **not** what you want.*

[simona.venuti@garr.it](#)

Apply

Richiesta certificati server

- L'amministratore del server genera la richiesta di certificato (CSR)
 - **openssl req -new -nodes -out req-server.pem **
-keyout key.pem
- Campi da impostare
 - **Organizational Unit Name (eg, section) []:** *(opt.)*
 - **Common Name (eg, YOUR name) []:** *(FQDN)*
 - **Email Address []:** *(Opt. Requestor)*
- L'amministratore del server non è autonomo, ma deve mandare la CSR al proprio Contatto Amministrativo
- Il Contatto Amministrativo inserisce la CSR in una web form accessibile solo per i CA tramite certificato personale GARR-CA
- Contestualmente i CA ricevono una mail con gli attributi del certificato a cui devono rispondere con un messaggio firmato

Sottomissione certificato server

Apply for Certificate

Compilare tutti i campi sottostanti.

Generare la CSR seguendo le istruzioni in [COMODO CSR Generation instructions](#)

[FAQ sul sito GARR CA](#)

Certificate Request in PEM format:

Alternatively, a file containing the CSR:

Certificate Valid for:

Certificate Variant:

Requestor Email:

Apply for Certificate

Compilare tutti i campi sottostanti.

Generare la CSR seguendo le istruzioni in [COMODO CSR Generation instructions](#)

[FAQ sul sito GARR CA](#)

Key Size:

1024

Certificate Valid for:

Certificate Variant:

Name components from the request:

Common Name:

pleppy.garr.it

Subject Alternative Names:
(one per line)

Organizational Unit:

Name components from the customer information:

Organization:

Consortium GARR

Country:

IT

Additional Information:

Requestor email:

Emissione

- Viene mandata in una mail al Contatto Amministrativo ed eventualmente il requestor
 - Il link ad il file.pem con il certificato firmato
 - I link ai certificati della catena delle CA

Installazione/configurazione CA

- Esempi di configurazione CA:
 - Apache
 - SSLCertificateChainFile
/usr/local/apache/conf/ssl.crt/CA.crt
 - SSLCertificateFile
/usr/local/apache/conf/ssl.crt/server.pem
 - Keystore Tomcat:
 - keytool -import -alias root -keystore storage \ -trustcacerts -file ca.crt
 - keytool -import -alias tomcat -keystore storage \ -trustcacerts -file server.pem

La catena corretta della CA

- La catena di CA COMODO-TERENA:

- `openssl s_client -connect ca.garr.it:443`

0 s:/C=IT/O=Consortium GARR/CN=ca.garr.it

i:/C=NL/O=TERENA/CN=TERENA SSL CA

1 s:/C=NL/O=TERENA/CN=TERENA SSL CA

i:/C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network
/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware

2 s:/C=US/ST=UT/L=Salt Lake City/O=The USERTRUST

Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware

i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network /CN=AddTrust
External CA Root

3 s:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network /CN=AddTrust
External CA Root

i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network /CN=AddTrust
External CA Root

Riferimenti

- <https://ca.garr.it>
- <https://ca.garr.it/TCS>
- <https://terena.org/activities/tcs/>
- <http://www.idem.garr.it>
- <http://www.openssl.org>
- **Contatti**
 - **GARR-CA: garr-ca@garr.it**
 - **TCS: tcs-ra@garr.it**
 - **IDEM: idem@garr.it, idem-help@garr.it**