GUIDE FOR OBTAINING CERTIFICATES

Certification Authority (CA). The CA is authority trusted by one or more users to issue and manages certificates. The CA is the security solution for conducting business on the Internet. The CA ensures that electronic transactions are conducted with confidentiality, data integrity, proper user authentication, and protection against repudiation.

Certificate Policy (CP). The CP is the administrative policy for certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a certificate-based system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provisions of the security services required by a particular application.

Certificate Practices Statement (CPS). A CPS is an internal statement of practices that a CA employs in issuing certificates. A CPS is expected to be a detailed and comprehensive technical and procedural document regarding the operation of the supporting infrastructure.

Certificate Revocation List (CRL). The CRL is the CA's listing of invalid certificates. Revocation can occur due to time lapse, employment change, theft of a private key, or other reasons.

Digital Certificate. A Digital Certificate is a digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. A Digital Certificate is a data structure used in a public key system to bind a particular, authenticated individual to a particular public key.

E-mail Certificate. An e-mail certificate is a certificate used to create encrypted e-mail.

Encryption. Encryption is the mathematical process of transforming plain text into a less readable form. The less readable form is information that has been encrypted into seemingly meaningless code, and can be read by anyone who has the key that decrypts the code.

Passphrase. A Subscriber determined phrase used when connecting to the URL. The passphrase is used instead of a password. It must consist of no words or more than one word without spaces between the words. It shouldn't be a dictionary or name-based word. It must be alphanumeric and contain both upper and lower case letters.

Private Key. A Private Key is (1) the key of a signature key pair used to create a digital signature or (2) the key of an encryption key pair used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key. A Public Key is (1) the key of a signature key pair used to validate a digital signature or (2) the key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available.

Public Key Infrastructure (PKI). PKI is a set of policies, processes, server platforms, software, and workstations used to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA). The RA is responsible for the identification and authentication of certificate Subscribers before issuing certificates, but does not sign or issue the certificates.

Relying Party. The Relying Party is a person or agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. The Relying Party relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally-signed message to identify the creator of the message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use. The Relying Party is the owner of the application.

Subscriber. The Subscriber is

- the subject named or identified in a certificate,
- holds a private key that corresponds to the public key listed in the certificate, and
- does not issue certificates to another party.

This includes, but is not limited to, an individual or network device. The Subscriber's name appears as the subject in a certificate in accordance with Certificate Policy asserted in the certificate.

The MREN CA issues user (personal), host and service certificates. Subscribers eligible for certification from MREN CA are:

- Users and site administrators of Montenegro Research and Education Network (MREN)
- Computers used in activities of Montenegro Research and Education Network (MREN)
- Services or host applications which are running on computers used in Montenegro Research and Education Network (MREN).

There are two ways to issue a certificate:

1. Sign pkcs#10 request
2. Issue certificate directly withouth a request.

The first case is most common in case of server/service certificate.

Generating certificate request:

In order to obtain MREN certificate, you need to have a valid user account in one of the User Interface nodes (UI) of MREN to generate a certificate request.

You can use any SSH client to log to a User Interface with your username. In case you a re using Windows, you can use any SSH compatible terminal emulator.

Once your login is successful, you need to issue the following command:

>grid-cert-request

You may use "grid-cert-request -int" option if you want to override the defaults configured for your UI.

Important note: In order to be able to execute this command /opt/globus/bin/ must be in your PATH.

Three files will be generated in .globus directory after this command is executed, these files are:

- userkey.pem: contains the private key associated with the certificate: it must be kept readable only by the user requesting the certificate. Should this file be lost or deleted, you will have to request a new certificate.
- Usercert-request.pem: contains the request for the user certificate.
- usercert.pem: should be replaced by the actual certificate when you will receive it signed by MREN CA.

Note: When generating a re-key request, move these files to another directory to keep them from being overwritten.

Distinguished name (DN):

DC=me, DC=ac, DC=MREN, O=XXX, CN=Subject-name
Where XXX is the name or acronym of the institution.
DN for each certificate must be unambiguous and unique. To prevent name collisions between different entities, mainly in issuing personal certificates, a number or other allowed distinguishing characters can be added to the CN to ensure uniqueness. The subject names for the certificate applicants shall follow the X.500 standard:

- In case of user certificate the subject name must include the persons name in the CN field;
- In case of host certificate the subject name must include the DNS FQDN in the CN field;
- In case service certificate the subject name must include the service name and the DNS FQDN separated by a „/“ in the CN field.

A current list of O's is in table below.
DN must consist of: 'a'-'z', 'A'-'Z', '0'-'9', and the characters: '(', ')', '+', ',', '-', '.', ':', '?', ' ', that is, upper and lower case alphanumeric (english alphabet), left and right parentheses, plus, comma, minus/hyphen, dot (period), colon, question mark, and space.
Additionally, in case of grid host certificate and service certificate character '/' can be used. The maximal length of the CN is 128 characters for all types of certificates.
Private keys must not be shared among end entities.

See the table below for the list of names and acronyms to be used as Organization.

Faculty of Electrical Engineering	ETF
Faculty of Mechanical Engineering	MF
Faculty of Metallurgy and Technology	MTF
Faculty of Natural sciences and Mathematics	PMF
Faculty of Civil Engineering	GF
Faculty of Architecture	AF
Faculty of Economics	EF
Faculty of Law	PF
Faculty of Political Sciences	FPN
Faculty of Medicine	MDF

Faculty of Philosophy	FF
Faculty of Marine studies	FZP
Faculty of Tourism and Hotel Management	FTH
Music Academy	MA
Faculty of Drama	FDU
Faculty of Fine Arts	FLU
Faculty of Practical Physiotherapy	FPF
Institute of Foreign Languages	ISJ
Institute of Biotechnology	BTI
Institute of Marine Biology	IBM
Institute of History	II
Center of Information Technology	CIS
University Library	**UB**
Pharmacy	F
Geodesy	G
Schoolmaster literacy on Albanian	OUA

Authentication of individual entity:

Certificate of a person:
The subject should contact personally the RA or CA staff in order to validate his/her identity. The subject authentication is fulfilled by providing an official document (ID-card, driving license or a passport) declaring that the subject is a valid end entity.

Certificate of a host or service:
Host or service certificates can only be requested by the administrator responsible for the particular host. In order to request a host certificate the following conditions must be met:

- The host must have a valid DNS name
- The administrator must already possess a valid personal MREN Certificate
- The administrator must provide a proof of his or her relation to the host itself.

The subscriber requesting service from the MREN CA must present valid documents for personal identification (ID-card, driving license or a passport), and a valid document proving host's or service's relation with an institute or organization.

MREN CA or RA will archive photocopies of ID documents in case of user certificates and digitally signed e-mails in case of host or service certificates.

Certificate acceptance:

The subscriber must send an e-mail on mren-ca@ac.me, within 5 working days from the day that his/her certificate was issued, in which he will be stating that:

- He or she has read this policy and accepts to adhere to it
- He or she accepts his/her certificate signed by the MREN CA
- He or she assumes the responsibility to notify the MREN CA immediately:
  - In case of possible private key compromise
  - When the certificate is no longer required
  - When the information in the certificate becomes invalid.

The e-mail which the user sends to the CA has to be signed with the key corresponding to the public key in certificate he or she received from the CA.
If the subscriber does not send the e-mail within 5 working days, the certificate becomes the subject for revocation.

You must cut the sample text below and replace the text under "" with your details.

For user certificates:

----------Cut here----------
To whom it may concern,

With this email I state that

1. I, "your name", accept my x509v3 digital certificate with

DN: /DC=me/DC=ac/ DC=MREN/O="your organization"/ CN="your name"

Serial Number: "your certificate serial number"
signed by /DC=me/DC=ac/DC=MREN/CN=MREN-CA

2. I adhere the MREN CA policy and usage rules found at:
http://mren-ca.ac.me/policy%20document.php
(O.I.D: 1.3.6.1.4.1. 29544.1.1.1.0)

----------Cut here----------

For host certificates:

----------Cut here----------
To whom it may concern,

With this email I state that

1. I am the person responsible for the network entity "host/FQDN", and I accept the x509v3 digital certificate with
   DN: /DC=me/DC=ac/ DC=MREN/O="your organization"/ CN="host/FQDN"
   Serial Number: "certificate serial number"
   signed by /DC=me/DC=ac/DC=MREN/CN=MREN-CA
2. I adhere the MREN CA policy and usage rules found at:
   http://mren-ca.ac.me/policy%20document.php
   (O.I.D: 1.3.6.1.4.1. 29544.1.1.1.0)

----------Cut here----------

Subscriber private key and certificate usage:

- Email signing/verifying and encryption/decryption (S/MIME)
- Server authentication and encryption of communications
- General purpose authentication (e.g. web site authentication)
- User authentication.

How do digital IDs work?

A digital ID is composed of a public key, a private key, and a digital signature. When you digitally sign your messages, you are adding your digital signature and public key to the message. The combination of a digital signature and public key is called a certificate. Recipients can use your digital signature to verify your identity, and they can use your public key to send you encrypted e-mail that only you can read by using your private key. To send encrypted messages, your Address Book must contain digital IDs for the recipients. That way, you can use their public keys to encrypt the messages. When a recipient gets an encrypted message, his or her private key is used to decrypt the message for reading.

Importing your certificate into Internet Explorer / Outlook Express

Step 1 of 3: Transferring PKCS#12 bundle to your computer

Your certificate and private key must be located in the .globus directory in your home. In the standard LCG setup your private key is found at: ~/.globus/userkey.pem and your certificate at: ~/.globus/usercert.pem.

In order to import your private key and certificate in your browser you must create a pkcs12 bundle. This can be achieved by issuing the command:

- openssl pkcs12 -export -in ~/.globus/usercert.pem -inkey ~/.globus/userkey.pem -name "My Certificate" -out mycertificate.p12

After issuing the above command, you will be asked to enter the pem pass phrase. This is the pass phrase you entered during the initial process of creating the certificate request. Next you will have to enter an export password for the pkcs12 bundle and you will have to use it during the import procedure.

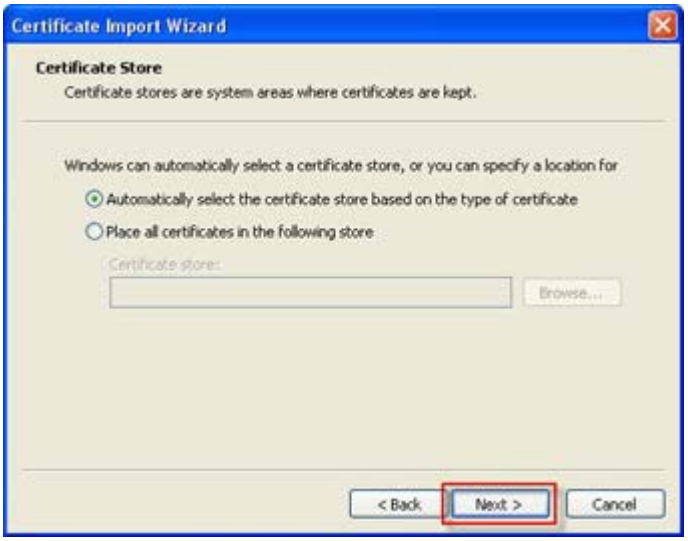
Transfer the pkcs12 bundle to your computer.

Step 2 of 3: Importing CA ROOT certificate into certificate store

- Open http://mren-ca.ac.me/ca%20root%20cert.php in Internet Explorer.
- Click on “CA certificate”
- A new window will popup, click open

- Start the import wizard by clicking "Install certificate"

- Click "Next" two times.



- Complete the wizard by clicking "Finish"

- Click "Yes" at the Security prompt.

Step 3 of 3: Importing your private key and certificate into Internet Explorer / Outlook Express

- Open Internet Explorer
- Click "File -> Open" and then browse to the location of your pkcs#12 bundle you previously transferred to your computer, and open it.

- A new window will appear, click "Next" in two next windows.

- In the next screen, enter your password. This is the export password you entered previously.
- Enable ONLY "Enable strong private key protection. You will be prompted every time the private key is used by an application, if you enable this option."
- DO NOT enable "Mark this key as exportable. This will allow you to backup or transport your keys at a later time."

- Select "Next" in the two following screen, and the "Finish".
- Select "Ok" when the following window appears.

Importing your certificate into Firefox / Thunderbird

Step 1 of 4: Transferring PKCS#12 bundle to your computer

Your certificate and private key must be located in the .globus directory in your home. In the standard LCG setup your private key is found at: ~/.globus/userkey.pem and your certificate at: ~/.globus/usercert.pem.

In order to import your private key and certificate in your browser you must create a pkcs12 bundle. This can be achieved by issuing the command:

- openssl pkcs12 -export -in ~/.globus/usercert.pem -inkey ~/.globus/userkey.pem -name "My Certificate" -out mycertificate.p12

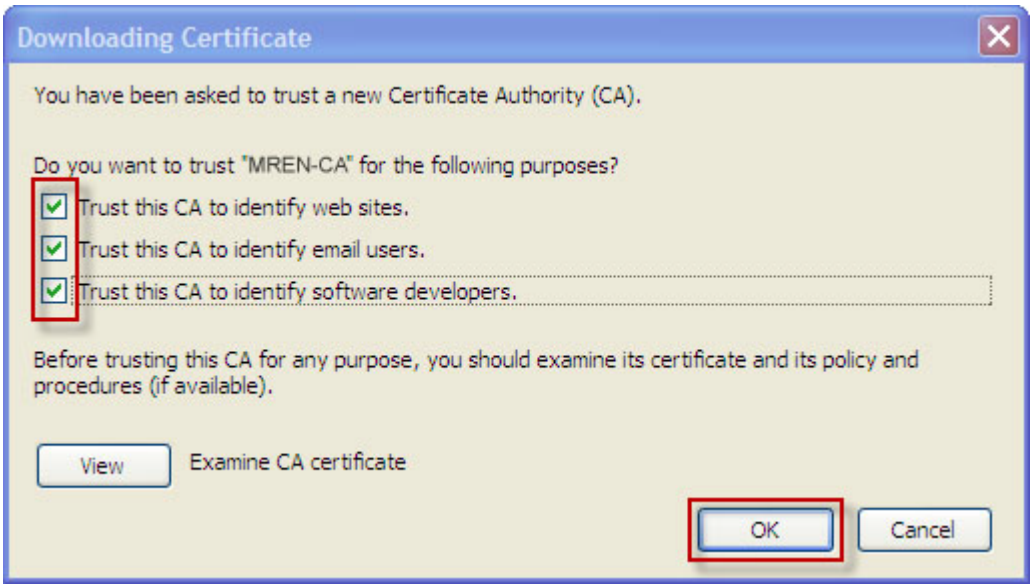
After issuing the above command, you will be asked to enter the pem pass phrase. This is the pass phrase you entered during the initial process of creating the certificate request. Next you will have to enter an export password for the pkcs12 bundle and you will have to use it during the import procedure.

Transfer the pkcs12 bundle to your computer.

Step 2 of 4: Importing CA ROOT certificate into Firefox

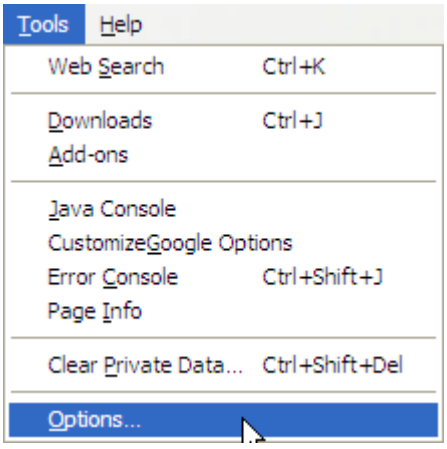
- Open http://mren-ca.ac.me/ca%20root%20cert.phpl in Firefox.

- Click on "CA certificate"
- A new window will popup, check all three boxes and click ok. Root certificate is installed in Firefox.

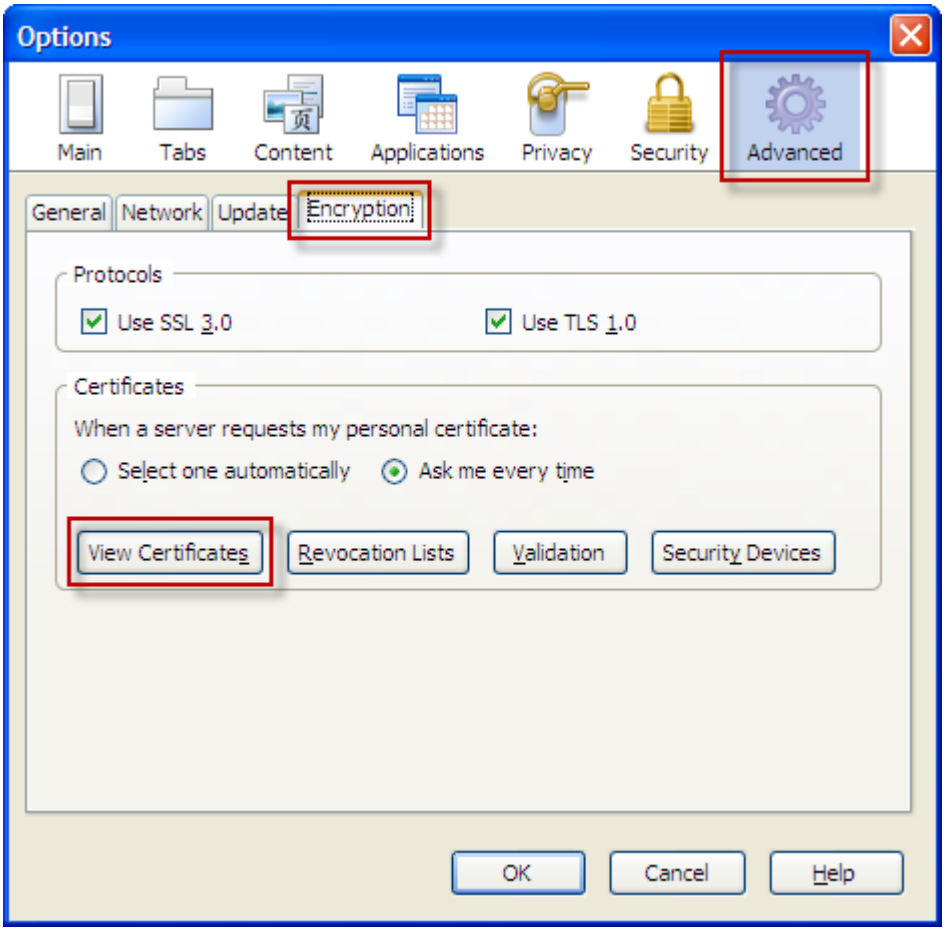


Step 3 of 4: Importing your private key and certificate into Firefox

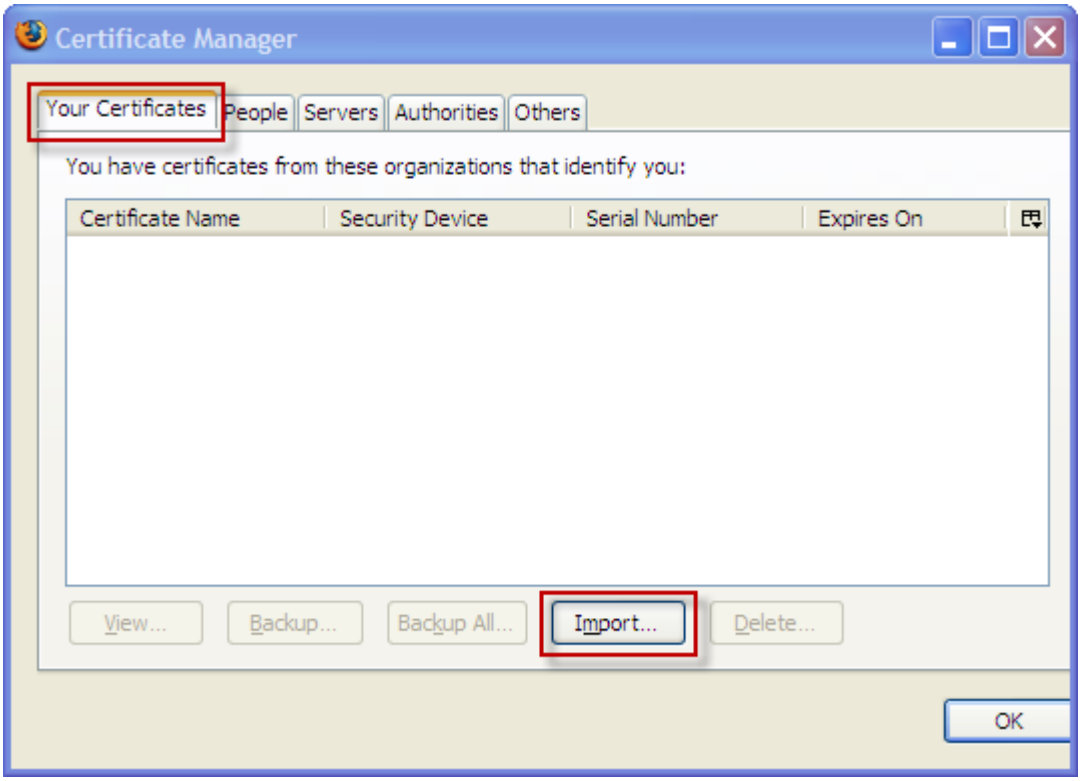
- Open menu "Tools / Options"



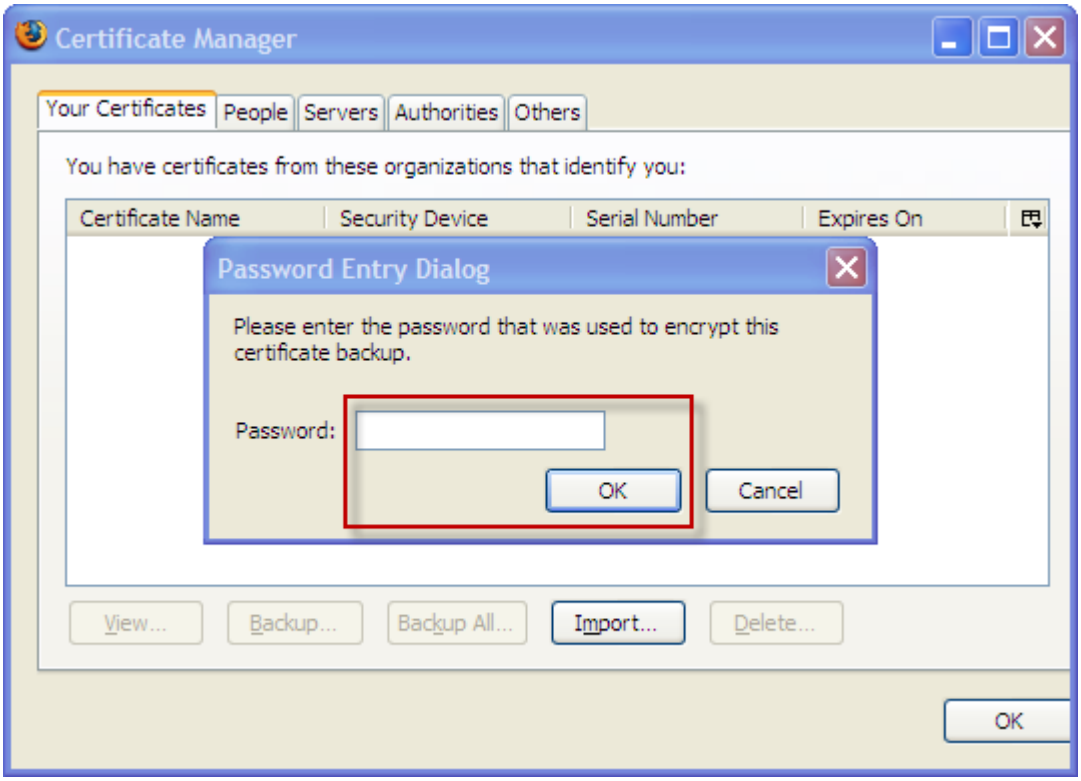
- New window will open, click "Advanced / Encryption / View Certificates"



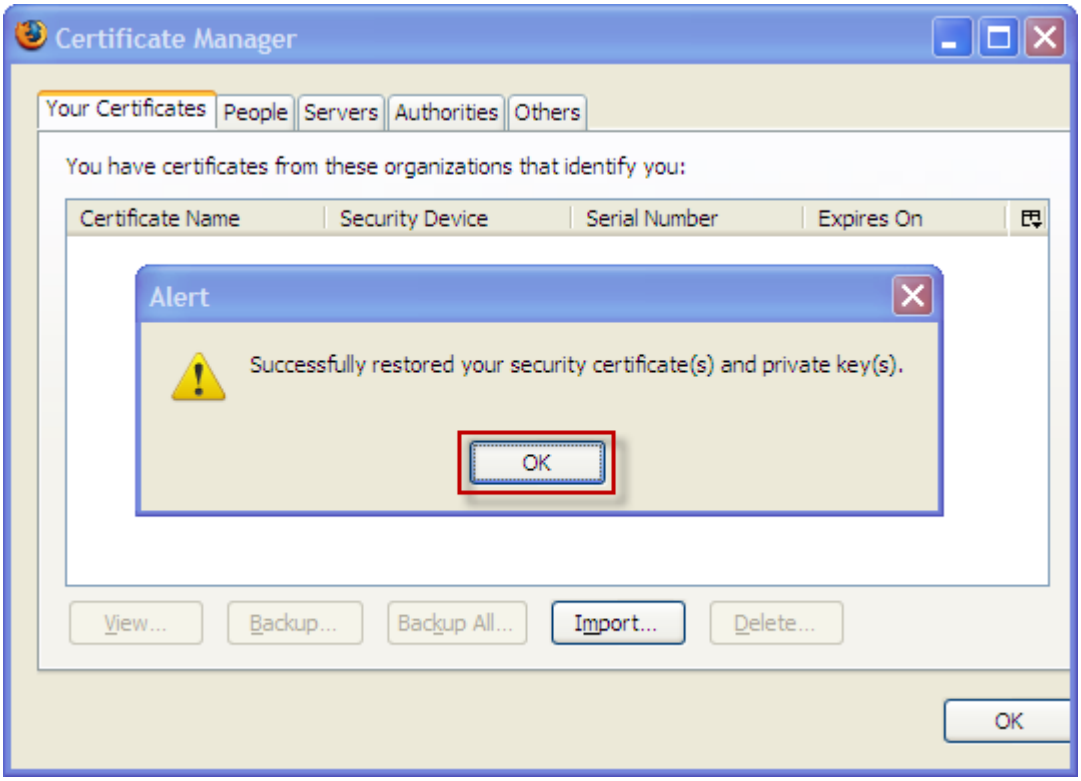
- New window will open, click "Your certificates / Import"



- Browse to location of your PKCS#12 certificate, click "Open", enter your password and click "Ok"

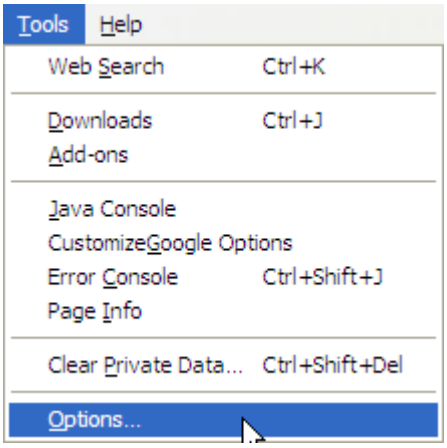


- Your certificate is now imported, click "Ok"

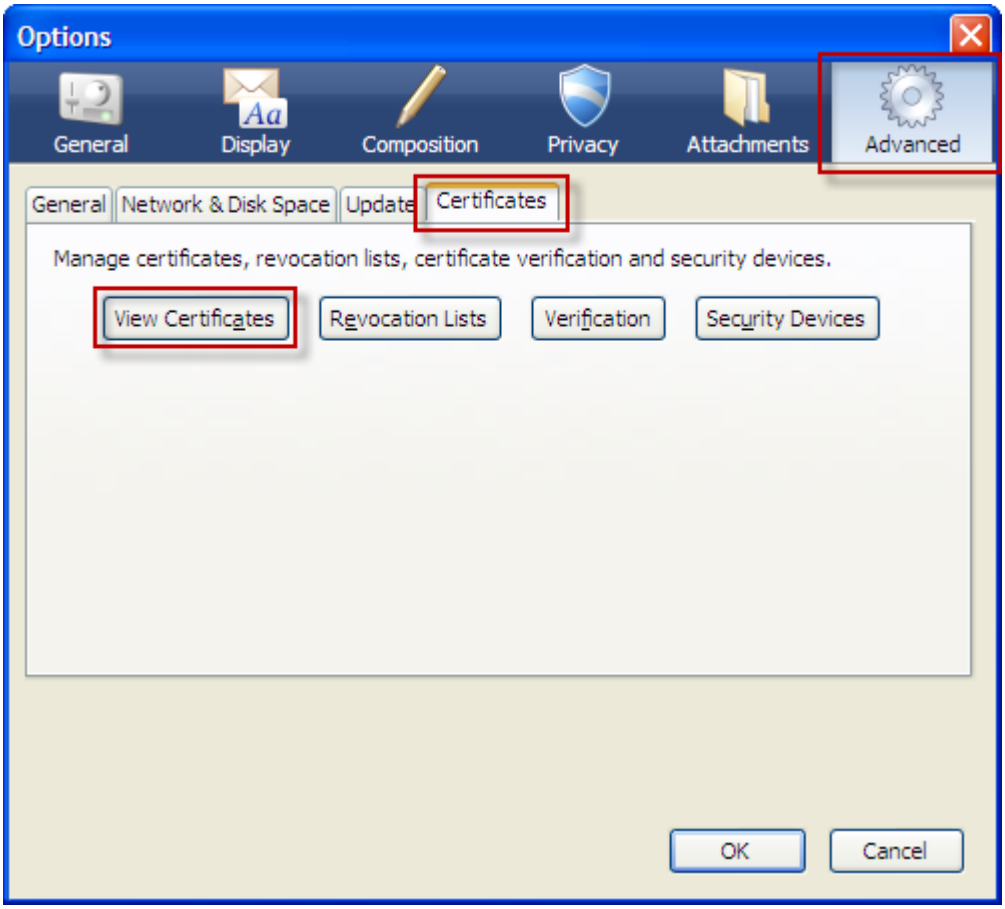


Step 4 of 4: Importing your private key and certificate into Thunderbird

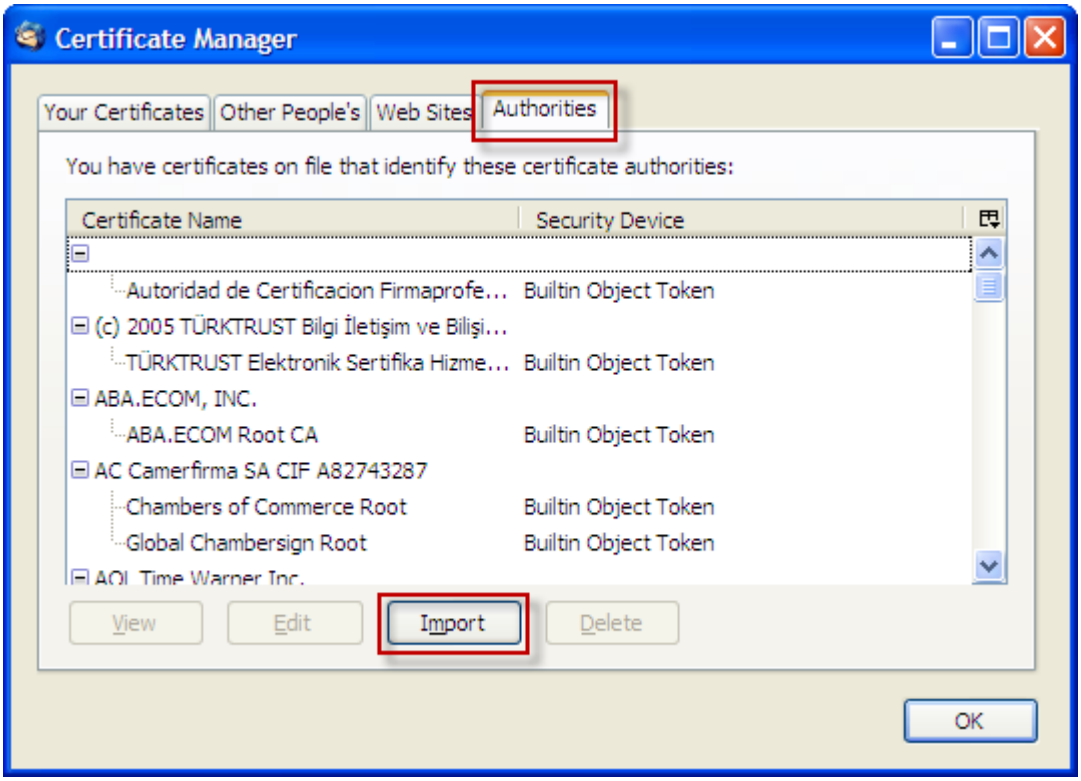
- Open http://mren-ca.ac.me/ca%20root%20cert.php in your browser
- Click on “CA certificate”, and save to desired location
- Open Thunderbird and open menu "Tools / Options"



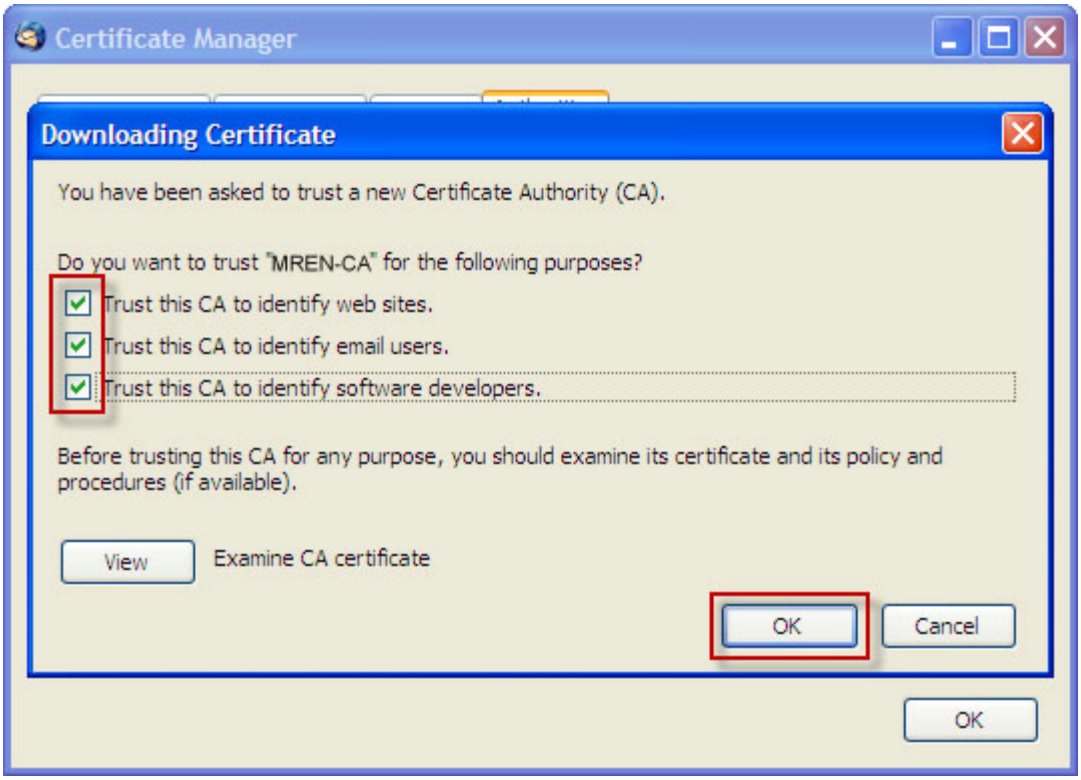
- Click "Advanced / Certificates / View certificates"



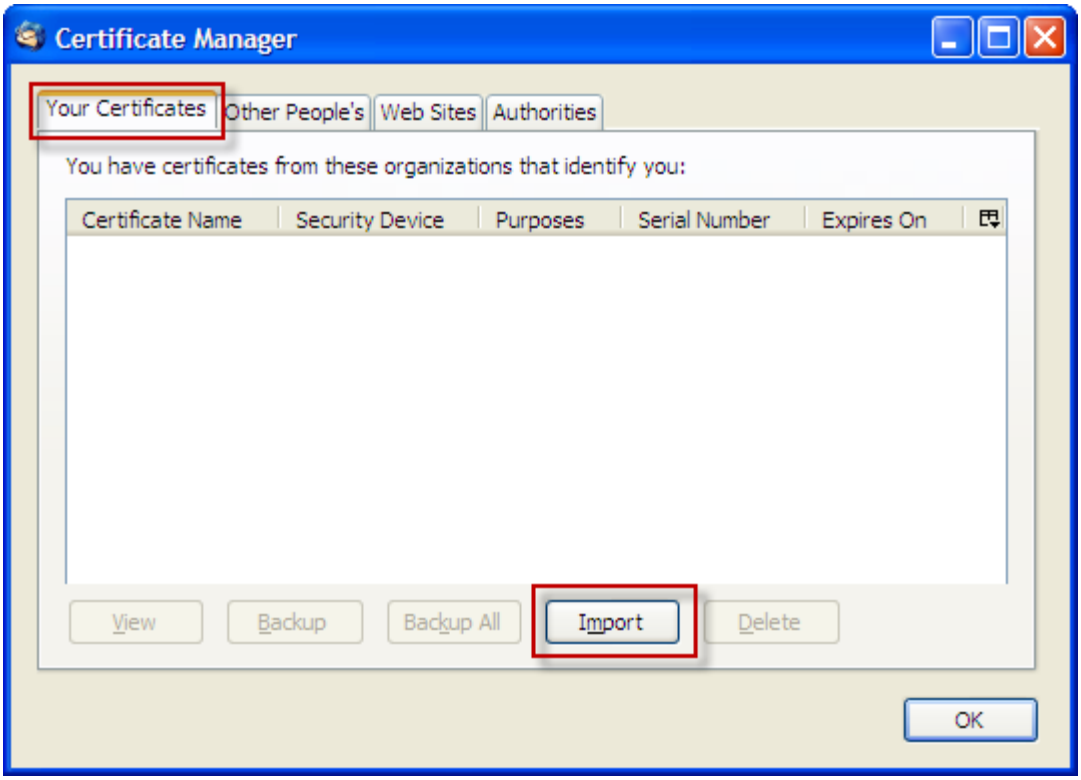
- New window will open, click "Authorities / Import"



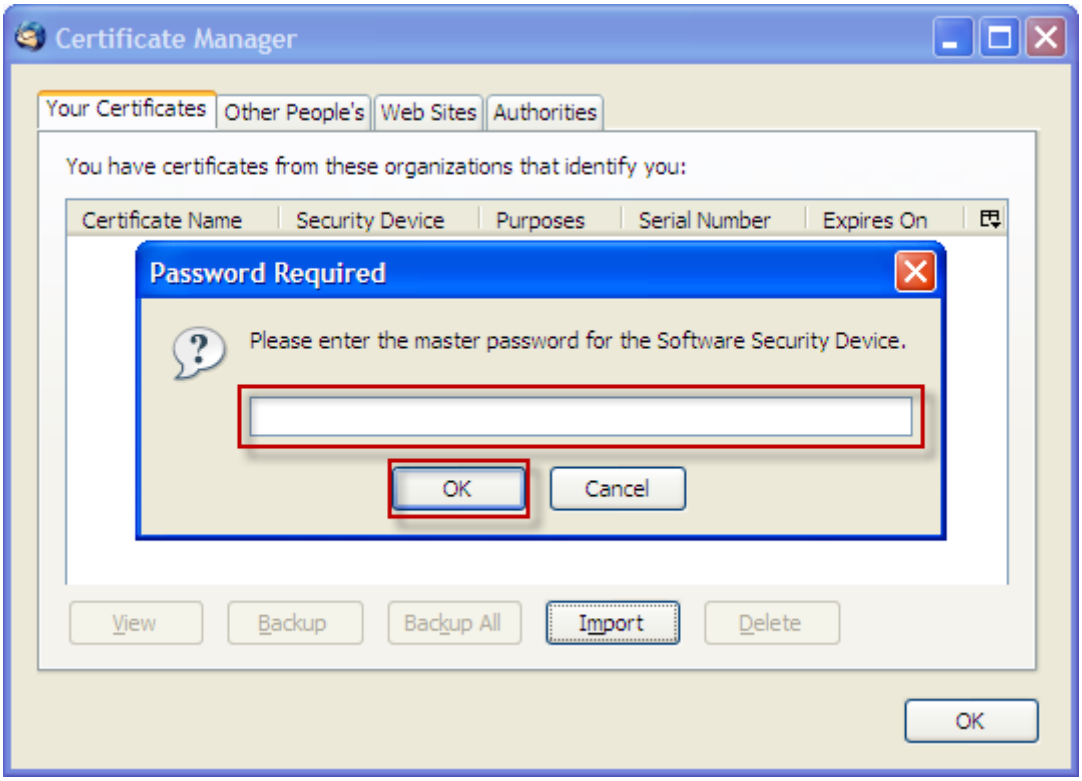
- Browse to location you previously saved ROOT certificate and click "Open", check all three boxes and click "Ok"



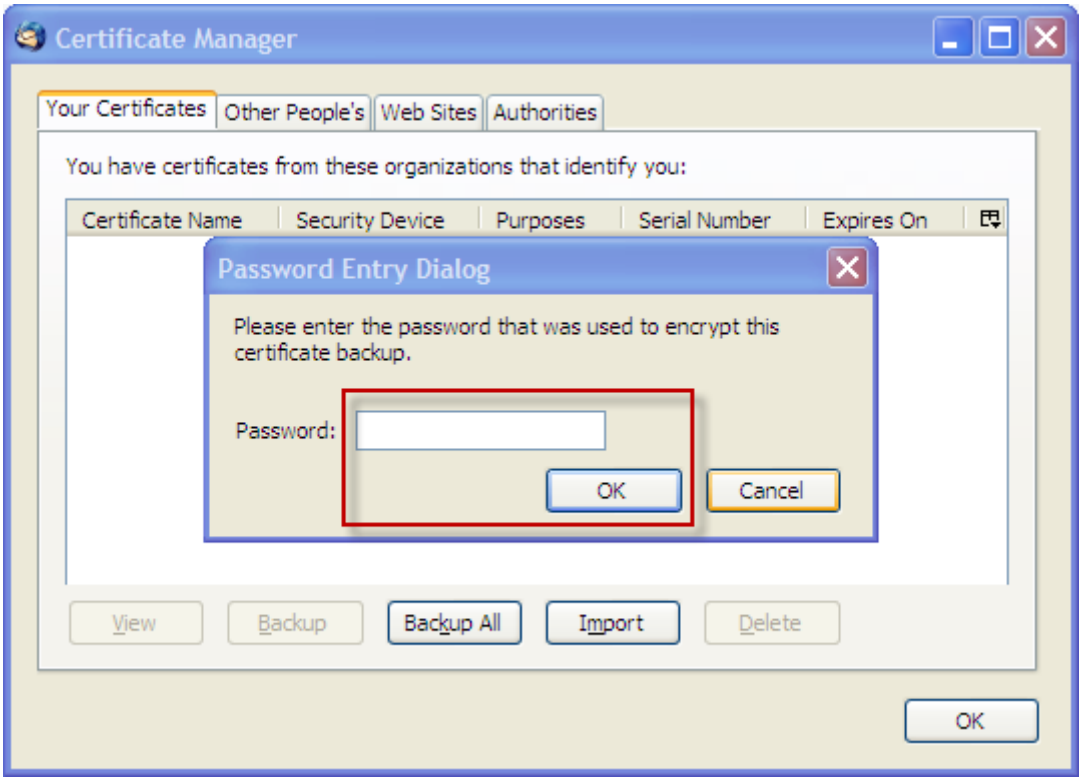
- Click "Your certificates / Import", browse to location of your PKCS#12 bundle and click "Open"



- Enter a master password for Thunderbird security device (you choose a master password which will be used to open all stored certificates in Thunderbird)



- Enter your certificate password



Certificate conversion

PKC12 (browser friendly) -> PEM (Globus friendly)

- user certificate
  $ openssl pkcs12 -in usercert.p12 -out usercert.pem -nokeys -clcerts
  Enter Import Password:
  MAC verified OK

- user key (key is encrypted)
  $ openssl pkcs12 -in usercert.p12 -out userkey.pem -nocerts
  Enter Import Password:
  MAC verified OK
  Enter PEM pass phrase:
  Verifying - Enter PEM pass phrase:

- host & service certificate
  $ openssl pkcs12 -in hostcert.p12 -out hostcert.pem -nokeys -clcerts
  Enter Import Password:
  MAC verified OK

- host & service key (key is not encrypted)
  openssl pkcs12 -in hostcert.p12 -out hostkey.pem -nocerts -nodes
  Enter Import Password:
  MAC verified OK

PEM (Globus friendly) -> PKC12 (browser friendly)

- $ openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -certfile /etc/grid-security/certificates//serial-number.pem -out usercert.p12
  Enter pass phrase for userkey.pem:
  Enter Export Password:
  Verifying - Enter Export Password: