Security Services

- Forms the underlying communication medium for all the services
- Secure Authentication and Authorization
- Single Sign-on
  - User need not explicitly authenticate himself every time a service is requested
- Uniform Credentials
- Ex: GSI (Globus Security Infrastructure)
Creates a proxy for single-sign on

User → Proxy

A

GSI enabled GRAM

Plain unix authentication

B

GSI enabled GRAM

Kerberos authentication
A GSI certificate includes four primary pieces of information:

- A subject name, which identifies the person or object that the certificate represents.
- The public key belonging to the subject.
- The identity of a *Certificate Authority (CA)* that has signed the certificate to certify that the public key and the identity both belong to the subject.
- The digital signature of the named CA.

A third party (a CA) is used to certify the link between the public key and the subject in the certificate. In order to trust the certificate and its contents, the CA's certificate must be trusted. The link between the CA and its certificate must be established via some non-cryptographic means, or else the system is not trustworthy.
Grid certificate

- Simply speaking, you need a certificate that authenticates you and which can be used as a single sign-on in systems like Globus.

- To get a personal grid certificate, usually the following steps are involved:
  - Import the CA certificate into your browser.
  - Request your certificate.
  - Retrieving your certificate.
  - Exporting your key pair for use by Globus grid-proxy-init.
DOEGrids certificate

- Import the DOEGrids Certificate Chain
  1. Go to: http://pki1.doegrids.org
  2. Select "Retrieval" tab
  3. Select "Import CA Certificate Chain" from the menu.
  4. Under "Users", select the radio button "Import CA Certificate Chain into your browser".
  5. Click the "Submit" button.

source: http://www.doegrids.org
Requesting a Grid Certificate

- Request your certificate.
  - Point your browser to https://pki1.doegrids.org
  - Select Enrollment tab.
  - Fill in the New User Form.
  - When you click 'submit' the key pair will be generated.

Instructions for obtaining Grid3 user certificate were prepared for Grid Summer Workshop 2005
Retrieving your Grid Certificate

- Go to http://pki1.doe grids.org/srchCert.html
  - This is a search interface to locate your certificate in the DOEGrids CA repository.
  - You MUST use the same browser on the same computer that you used to request the certificate, because it is this browser that is holding your private key in its certificate repository.

- In the "Subject Name" section, check the box marked “Show certificates with a subject name matching the following”, and enter your last name in the “Common Name” box. Make sure Match Method of Partial is selected. Scroll (way down) to the bottom of the page and click Find.

- At least one certificate - hopefully yours! - should be listed. Click Details next to your certificate. At the very bottom of the Details page, click "Import Your Certificate".
Export your Grid Certificate

- The interface for this varies from browser to browser.
  - Internet Explorer starts with "Tools -> Internet Options -> Content";
  - Netscape Communicator has a "Security" button on the top menu bar;
  - Mozilla starts with "Edit -> Preferences -> Privacy and Security -> Certificates".

- The exported file will probably have the extension .p12 or .pfx. Guard this file carefully. Store it off your computer, or remove it once you are finished with this process.
Exporting your key pair for use by Globus grid-proxy-init.

Copy the above PKCS#12 file to the computer where you will run *grid-proxy-init*.

Extract your certificate (which contains the public key) and the private key:

- Certificate:
  ```bash
  openssl pkcs12 -in YourCert.p12 -clcerts -nokeys -out $HOME/.globus/usercert.pem
  ```
- To get the encrypted private key:
  ```bash
  openssl pkcs12 -in YourCert.p12 -nocerts -out $HOME/.globus/userkey.pem
  ```

You must set the mode on your userkey.pem file to read/write only by the owner, otherwise *grid-proxy-init* will not use it.

- chmod go-rw $HOME/.globus/userkey.pem
Grid Proxy

- Once your user certificate is in place, you need to create a grid proxy which is used for accessing the Grid.
- In Globus, you can do this using `grid-proxy-init`.
- A proxy is like a temporary ticket to use the Grid, default in the above case being 12 hours.
- Once this is done, you should be able to run “grid jobs”
  - `globus-job-run site-name /bin/hostname`
The working of GSI can be better understood if we consider the following “actors”:

- The user laptop (used for requesting and importing the user certificate)
- The user client machine (which requests the grid services)
- The Grid site (usually the head node of a cluster that provides the grid service)
- The Certificate Authority (CA that issues the user certificate)
- The VO admin (for adding authorized access to grid sites)
1. Import CA certificate chain
2. Request user certificate (include sponsor and VO information). Public key generated by browser included.
3. CA confirms with the sponsor (with a phone call!).
4. Issues a user certificate (assigns a subject name to the user)
5. User imports the issued certificate (The browser holds the private key and confirms the authenticity of the cert)
6. The .p12 file is copied to the client machine

Continued..
7. User requests the VO admin access to required grid servers/services.

8. VO admin adds the subject of the user certificate to the *gridmap-file* of each of the required head nodes (ex. Using VOMS).


10. User requests a head node of a grid site for some service. Ex. `globus-run`.

Continued..
8. VO admin adds the subject of the user certificate to the gridmap-file.

10. User requests a head node of a grid site for some service. Ex. _globus-run_

The proxy generated in the previous step is forwarded to the grid site.

11. The grid site verifies the identity of the user by matching the subject of the proxy received with the request with the entry in its gridmap-file.

12. If authenticated, the requested service is performed.

13. User gets the response from the grid site.
Steps 1 thru 7 talk about acquiring a Grid user certificate
- This is a one-time affair;
- Certificates, once obtained, are usually renewed once every year

Step 8 enables authorization of a user to access a set of grid sites

Step 9 creates a temporary ticket for the user to perform grid operations

Step 10-13 are repeated for every job a user executes on the grid
A *gridmap* file at each site maps the grid id of a user to a local id

- The grid id of the user is his/her subject in the grid user certificate
- The local id is site-specific;
- multiple grid ids can be mapped to a single local id
  - Usually a local id exists for each VO participating in that grid effort
- The local ids are then used to implement site specific policies
  - Priorities etc.
The gridmap-file is maintained by the site administrator.

Each entry maps a Grid DN (distinguished name of the user; subject name) to local user names.

```
# Distinguished Name Local username
#

"/DC=org/DC=doegrids/OU=People/CN=Laukik Chitnis 712960" ivdgl
"/DC=org/DC=doegrids/OU=People/CN=Richard Cavanaugh 710220" grid3
"/DC=org/DC=doegrids/OU=People/CN=JangUk In 712961" ivdgl
"/DC=org/DC=doegrids/OU=People/CN=Jorge Rodriguez 690211" osg
```
OSG Authentication: Grid3 Style

VOMS server @ iGOC
VOMS server @ LLab
VOMS server @ OLab

Mapping of user's grid credentials (DN) to local site group account

DN mappings
gridmap-file

Merci
This slide is adapted from Jorge Rodriguez's presentation on "Building, Monitoring and Maintaining a Grid"
Authentication Test

- Submit a simple job to a remote site; check if the remote gatekeeper “knows” you – has your Grid identity authorized to run jobs:
  - $globusrun -a -r <sitename>/jobmanager-fork
    - GRAM Authentication test successful
- Look for the “test successful” message. This means you are “authorized” to use the <sitename> “resource”.
- If this still fails, there is a problem with your Grid certificate or your entry in the gridmap-file on that remote site.