HellasGrid CA & euGridPMA

EGEE 3rd Parties Advanced Induction Course

January, 2005 - NTUA, Athens

Kanellopoulos Christos
(skanct@physics.auth.gr)
HellasGrid CA Manager

PKI and Grids

Enabling Grids for E-science in Europe

- The primary needs for a grid security infrastructure are:
  - Secure communication (authenticated and perhaps confidential) between the grid elements.
  - Support security across organizational boundaries
  - Single Sign On, including delegation of credentials
- Central concept in the GSI authentication is the Certification Authority and the Certificate

Grid Certificate

Enabling Grids for E-science in Europe

- is encoded in the X.509 certificate format
- Includes 4 primary pieces of information:
  - A subject name
  - The public key
  - The identity of the CA
  - The digital signature of the named CA
- Is nothing more than a "passport".
- Important: The certificate is used only to authenticate (identify) entities on the Grid.

Grid CA

Enabling Grids for E-science in Europe

- The CA is a trusted 3rd party that is used to certify the link between the public key and the subject in the certificate.
- is usually a CA at national level
- Its purpose is to sign certificates for individual who are to access Grid resources, hosts or services
- In order for a Grid CA to be accepted with the current Globus based european infrastructure, it must be first accredited by the euGridPMA

CACG and euGridPMA

Enabling Grids for E-science in Europe

- CACG was established by the FP5 projects DataGrid & CrossGrid and included other project worldwide as a need to facilitate the deployment of international testbeds for Grid computing by having a commonly recognized way to assert identities.
- The group was chartered to:
  - Coordinate the CA infrastructure for CrossGrid and DataGrid.
  - Make recommendation to relying parties within the programs regarding the acceptance of the certificates issued by the participating CAs

euGridPMA

- evolution of CACG to a panEuropean body of Grid CA managers, endorsed by the eIRG (thanks much to the efforts of GRNET).
- 34 members from Europe, North America and Asia

- The PMA is responsible to:
  - Define and issue minimum requirements and best practice documents; these minimum requirements may govern any aspect of the certificate issuance
  - Maintain and revise these documents
  - Accredit authorities in respect to the minimum requirements
  - Be primarily concerned with Grid communities in Europe and their external partners
  - Foster trust relations for authentication purposes within the context of interorganizational resource sharing.

Towards a GlobalGridPMA

Enabling Grids for E-science in Europe

- On June 2004 a new Grid PMA was created in the Asia-Pacific Region (APGridPMA) and was presented at the euGridPMA meeting that took place on September.
- On November 2004 another Grid PMA was created that covers America (TAGPMA). It will be presented in the meeting next week.

Towards a GlobalGridPMA

Enabling Grids for E-science in Europe

- Need to establish trust at the PMA level
- Coordination of the minimum requirements across PMAs
- Need to establish a global PMA.

HellasGrid CA

Enabling Grids for E-science in Europe

- Was created during the 1st quarter 2002
- On May 2002 started the procedure of acceptance by the CACG
- Acceptance on October 2002 after a 5 month review.
- From the beginning the scope was to serve any grid projects within Greece in need for certificates
- Active participation in euGridPMA and GGF CA-Ops WG.

HellasGrid Certificates

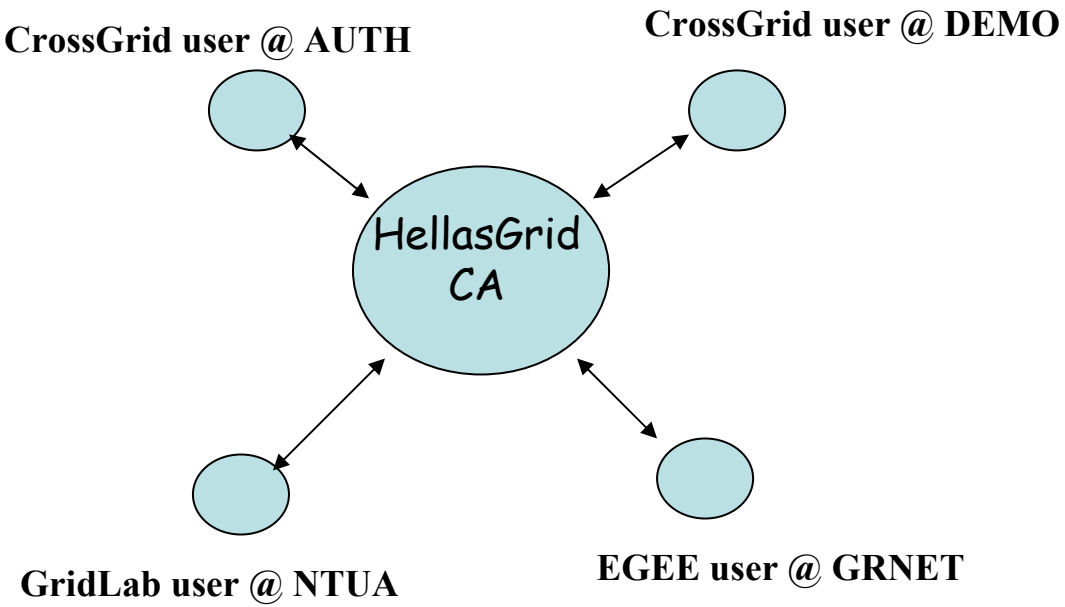
Enabling Grids for E-science in Europe

- Entities involved in the certificate life cycle:
  - –CA: Certification Authority. It's purpose is to sign certificates, revoke certificates, renew certificates, issue crls, operate repository, operate ca web site, maintain and revise the HellasGrid CP/CPS
  - –RA: Authenticate user requests (certificate requests, revocation requests, renewal requests), communicate directly with the user, forward authenticated requests to the CA, keep a log of each action taken.
  - –End entities: certificate, renewal, revocation requests, accept and follow the CP/CPS guidelines

HellasGrid Certificate Issuance

Enabling Grids for E-science in Europe

- Current situation:
  - AUTH provides both CA and the RA for the whole Greece.
    (the users communicate directly with the CA



Certificates for physical person

-The user creates the certificate request on his/her workstation via grid-cert-request

-The user sends the certificate request to hellasgrid-ca@grid.auth.gr

-The CA must receive a fax from the supervisor of the user in which it is be stated that the user is member of the institute.

- The on duty CA Manager will contact the supervisor via phone call to verify the fax.

- The signed certificate is sent to the user who has 7 working days to sent a signed e-mail at hellasgrid-ca@grid.auth.gr stating the acceptance of the CP/CPS

Certificates for servers/service

Enabling Grids for E-science in Europe

- The user creates the certificate request on his/her workstation via grid-cert-request
- The user sends the certificate request at hellasgrid-ca@grid.auth.gr via signed e-mail.
- The signed certificate is sent to the user who has 7 working days to sent a signed e-mail at hellasgrid-ca@grid.auth.gr stating the acceptance of the CP/CPS

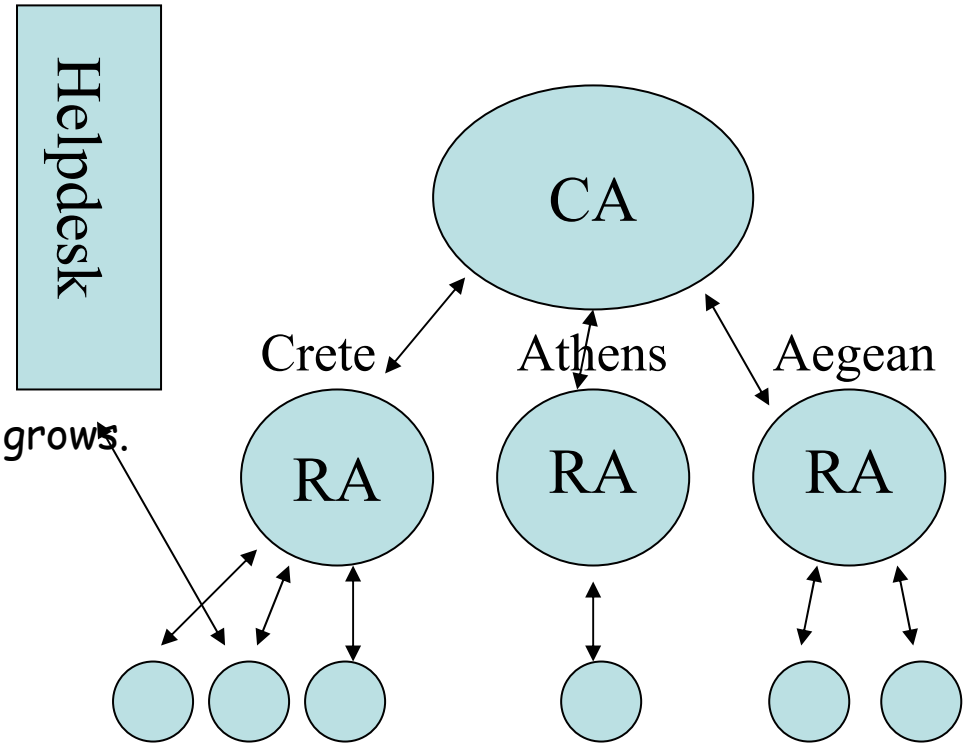
HellasGrid Certificate Issuance

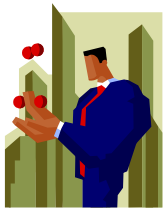
Enabling Grids for E-science in Europe

- The service is operational for 3 years
- … But there are drawbacks:
  - A lot of bureaucracy is involved
  - Does not scale!

Distributed RA scheme

- Create distributed RAs that will serve all the locations
- At least 1 area of:
  - Crete
  - Patra
  - Aegean
  - Athens
  - Ioannina
  - Thessaloniki
- 1 RA at each Institute as user base grows.





RA

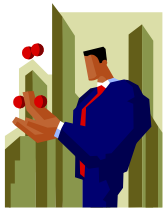
Subscriber

CA Portal

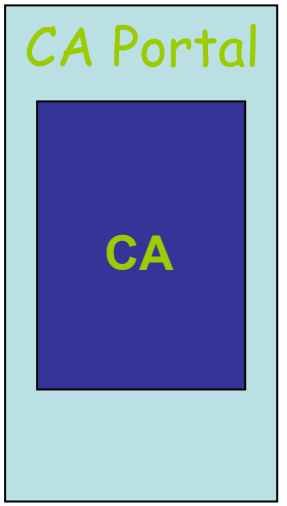
CA

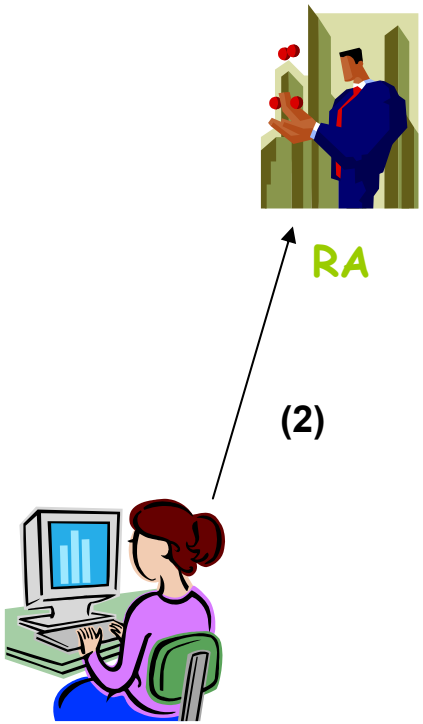
The players…

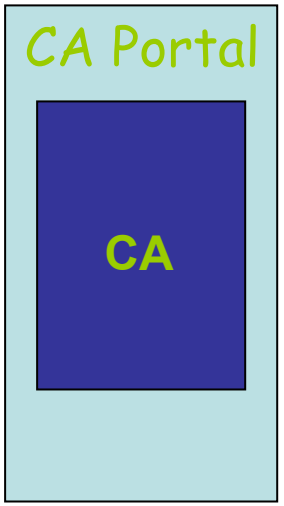
1. User generates a key pair. Private key must be 1024 or 2048 bits long and protected by strong pass phrase (>= 12 chars..)



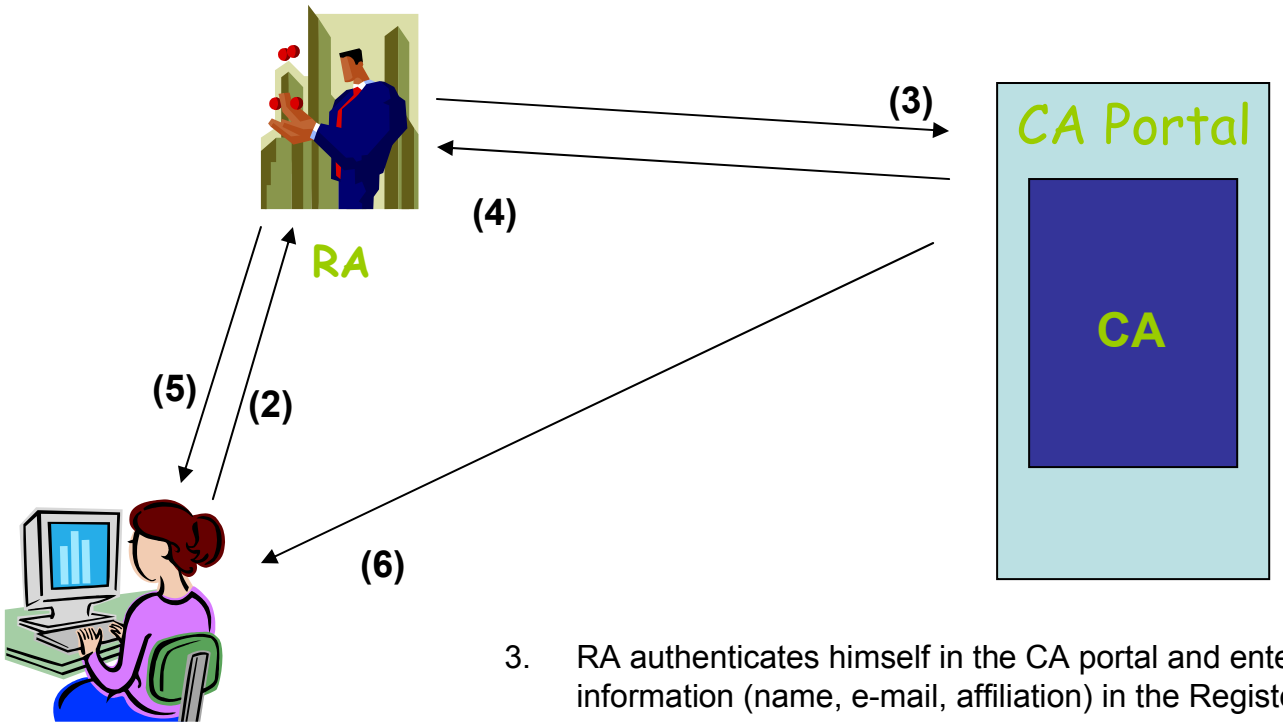
RA



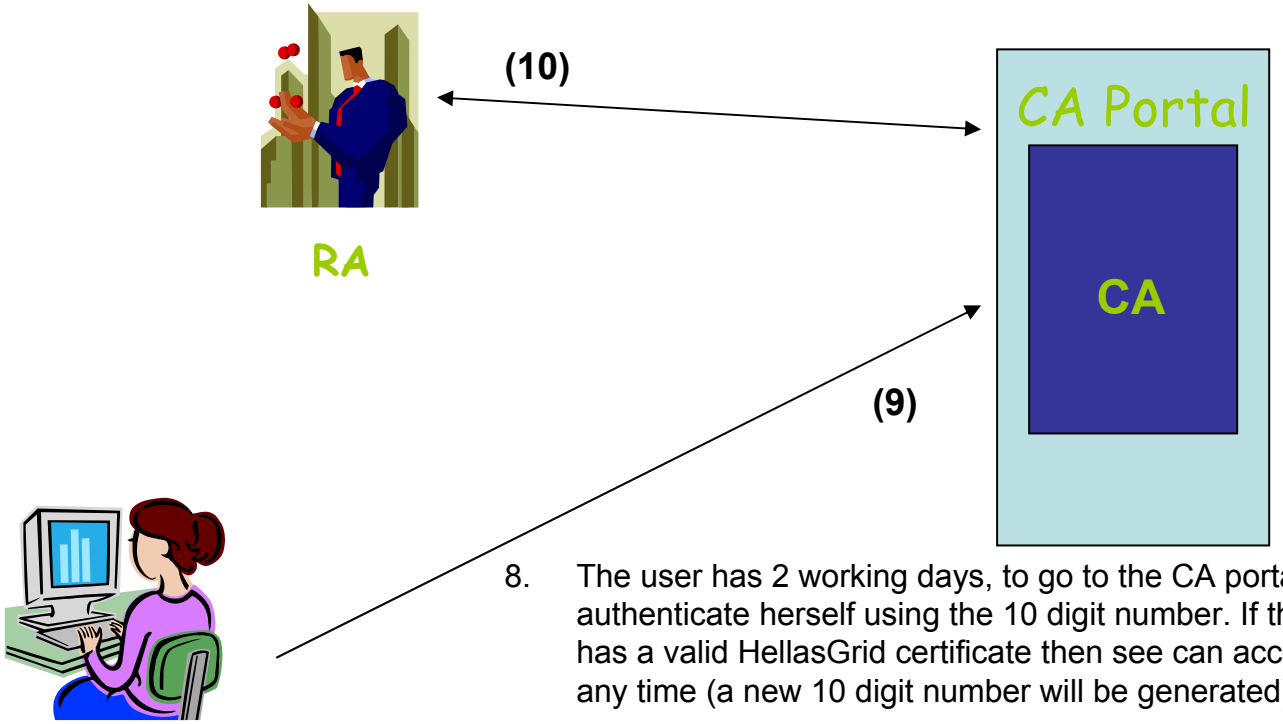




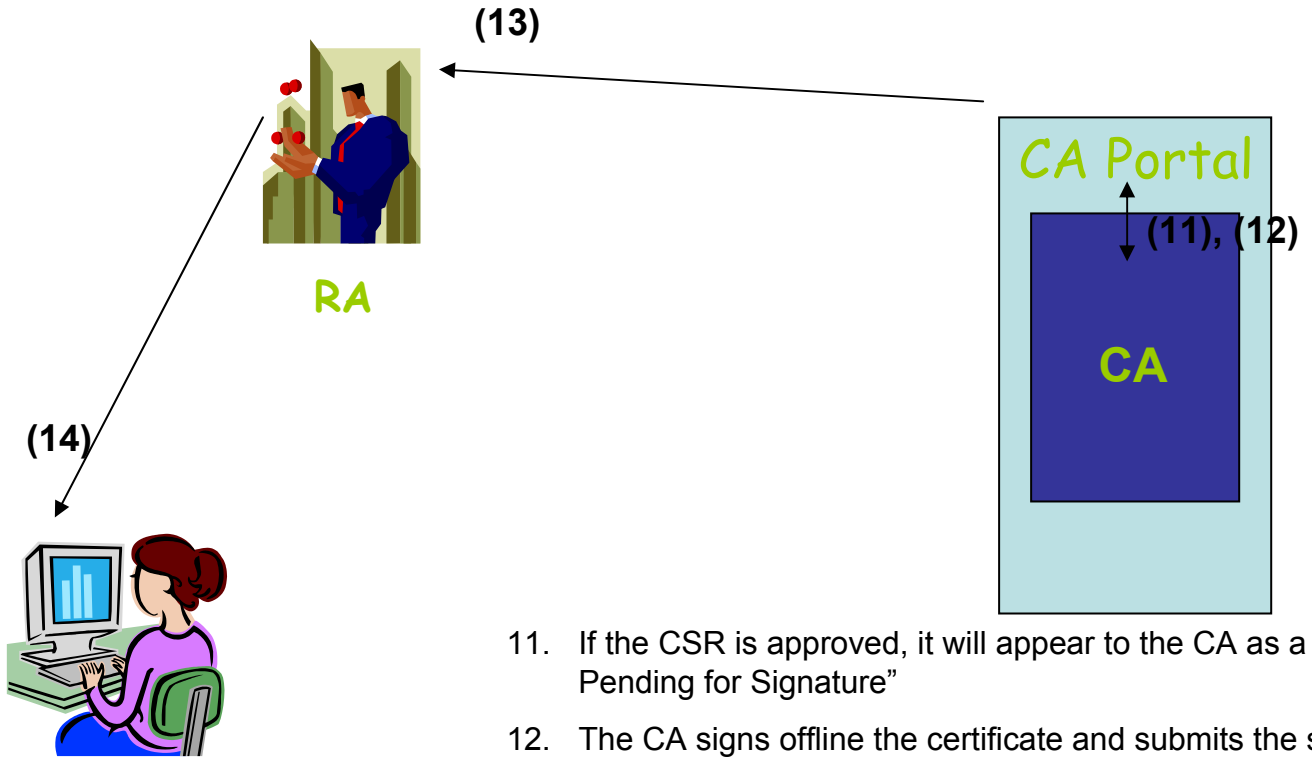
2 . If user hasn't identified herself to the RA within the last 3 years, she must appear personally and present her photo ID or passport along with formal papers which state her affiliation.



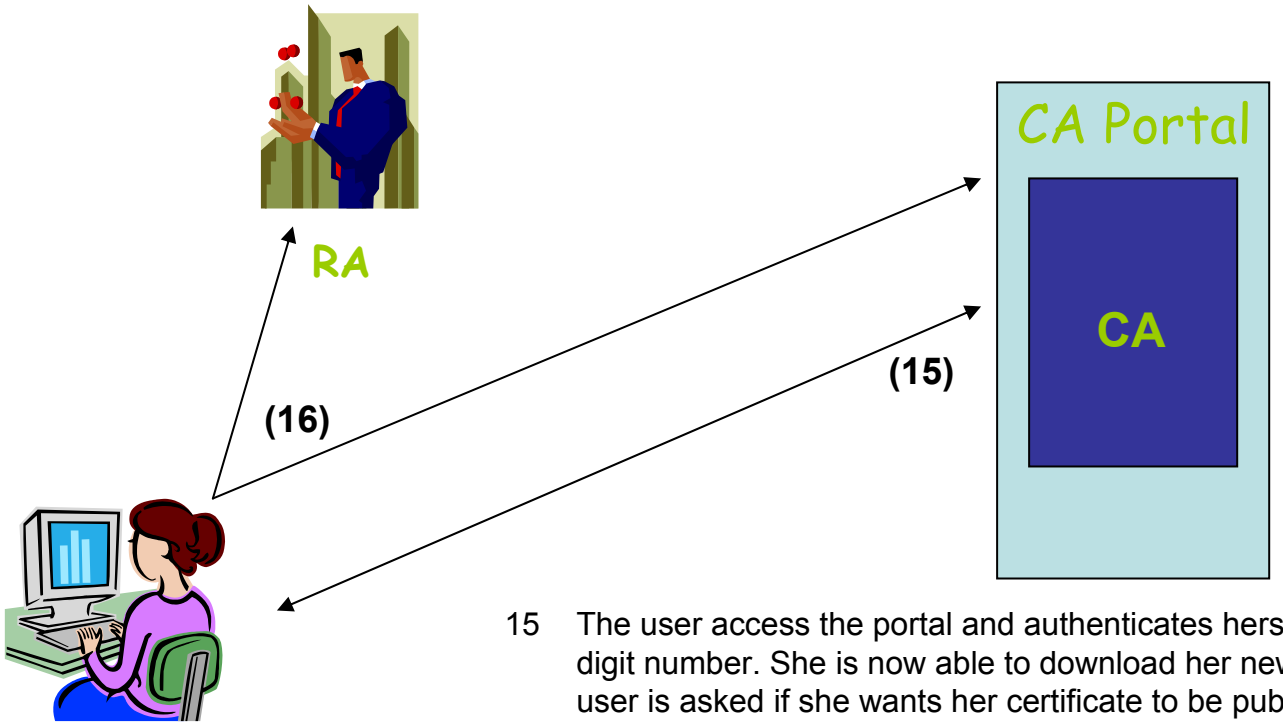
3. RA authenticates himself in the CA portal and enters the user information (name, e-mail, affiliation) in the Register Form
4. the portal generates a 10 digit number and the first 5 digits are shown to the RA.
5. The RA prints the 5 digit number and gives it to the user.
6. The rest 5 digits are sent to the registered e-mail address.
7. An SHA1 hash of the 10 digit number is kept in the database along with the user information



8. The user has 2 working days, to go to the CA portal and authenticate herself using the 10 digit number. If the user already has a valid HellasGrid certificate then see can access the portal at any time (a new 10 digit number will be generated)
9. The user submits her CSR using the form provided. A SHA1 hash will be generated the moment the user submits the form and it will be sent via e-mail to the corresponding RA and the CA, while it will also be saved in the database.
10. The CSR request will appear in the “Pending Section” of the RA that initially identified/authenticated the user. It is up to the RA to check if the CSR should be approved.



11. If the CSR is approved, it will appear to the CA as a “Certificate Pending for Signature”
12. The CA signs offline the certificate and submits the signed certificate in the portal.
13. The RA Manager is notified about the new certificate via e-mail.
14. The RA Manager informs the user via e-mail that her certificate is ready to be downloaded from the CA portal.



15 The user access the portal and authenticates herself using the 10 digit number. She is now able to download her new certificate. The user is asked if she wants her certificate to be published in the public directory.

16 Within 5 working days the user must send a signed e-mail to the RA Manager and the CA Manager stating that she adheres to the CP/CPS under which her certificate was signed.

Host/Service Cert Request

Enabling Grids for E-science in Europe

- The requestor must already have a valid HellasGrid CA certificate before requesting a server or service certificate;
- The submission of the certificate request can be done either via a web interface or via e-mail.

Host/Service Cert Request

Enabling Grids for E-science in Europe

- **Case 1: Web interface**
  - The user will have first to import her certificate in the browser in order to be authenticated "automatically" by the CA portal;
  - upon successful authentication the user will be able to submit the certificate request via a web based form;
  -The corresponding RA checks the users affiliation, the DNS name in the csr and the naming scheme.

Host/Service Cert Request

Enabling Grids for E-science in Europe

- **Case 2: Email submission**
  - The user will send an e-mail signed by her certificate to seegrid-ra@grid.auth.gr with the certificate requests attached.
  - The certificate request will be forwarded to the appropriate RA
  - The corresponding RA checks the users affiliation, the DNS name in the csr and the naming scheme.

Host/Service Cert Request

Enabling Grids for E-science in Europe

- If the RA approves the request, the certificate will be signed by the CA, uploaded in the portal and the RA is notified;
- The RA notifies the user about her new certificate(s).
- The user accesses the portal and downloads her certificate(s) (need to import her certificate in the browser first in order to be authenticated)
- Within 5 working days the user must send a signed e-mail to the RA Manager and the CA Manager stating that she will adhere to the CP/CPS under which her certificate was signed.

MyProxy Service

Enabling Grids for E-science in Europe

- Normal life time for a grid-proxy is 12h. This not suitable for running long time jobs.
- This behavior can be overridden using the flag -valid (NOT secure as Grid proxies are stored in /tmp)

MyProxy Service

Enabling Grids for E-science in Europe

- The MyProxy service is an Online Credential Store
- The proxy certificates are stored in a remote system and can be retrieved whenever and wherever one needs them. No need to manage private and public certificates on User Interfaces.

MyProxy Service

Enabling Grids for E-science in Europe

- Since November 2004 AUTH has been operating a myproxy service located at myproxy.grid.auth.gr
- The service is hosted on a stand alone server which is monitored 24/7 with HIDS and NIDS

Authorization Services

Enabling Grids for E-science in Europe

- AUTH will provide VO services for the HellasGrid/EGEE-SEE region based on VOMS
- The first server will be operational by the end of January 2005.
- The service is hosted on a stand alone server which is monitored 24/7 with HIDS and NIDS

VOMS Features

Enabling Grids for E-science in Europe

- Single login using voms-proxy-init only at the beginning of the session (was grid-proxy-init)
- Expiration time: the authorization information is only valid for a limited period of time as the proxy certificate itself
- Backward compatibility: the extra VO related information is in the user's proxy certificate, which can be still used with non VOMS-aware services
- Multiple VOs: the user may "log-in" into multiple VOs and create an aggregate proxy certificate, which enables her to access resources in any of them

The End.

Questions?