SEE-GRID CA CP/CPS Update
&
EGI Catch All CA Service

Christos Kanellopoulos <skanct@grid.auth.gr>
Christos Triantafyllidis <ctria@grid.auth.gr>

GRID & HPC
Operations Center
ARISTOTLE UNIVERSITY OF THESSALONIKI

Brief history...

- May 2004: Start of the SEE-GRID project.
- July 2004: SEE-GRID CA was created
  - "provide catch all PKI services to the wider region of South Eastern Europe in order to facilitate the needs of distributed computing"
  - "pave the way for the countries in the region to establish their own national Public Key Infrastructure and guide them through the IGTF accreditation process"

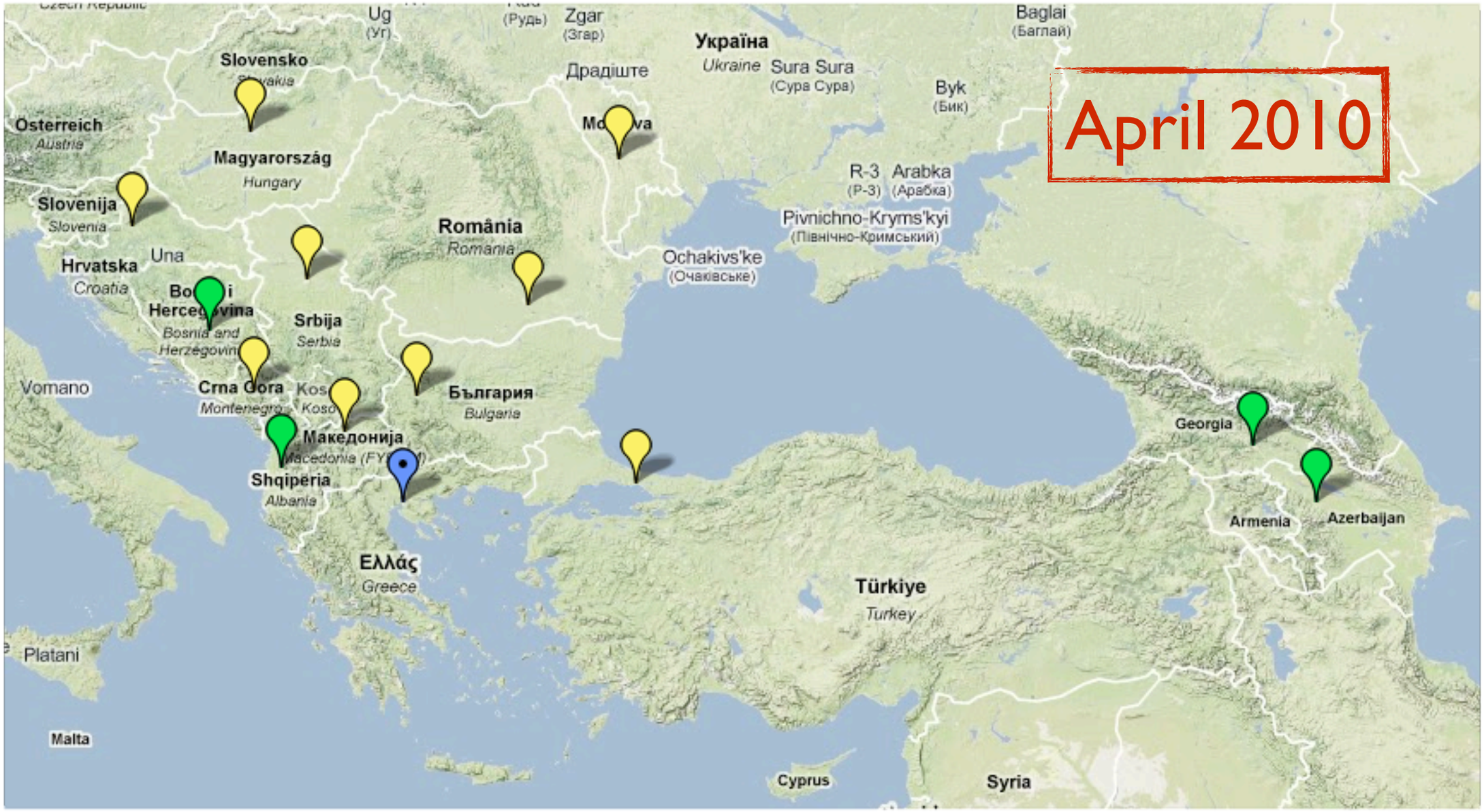
The accreditation...

- September 2004: Accreditation at the 2nd EUGridPMA meeting in Brussels.
- September 2004: Established initial network of Registration Authorities.
    - *RAs in Greece, Albania, Bosnia & Herzegovina, Bulgaria, Croatia, F.Y.R.O.M., Hungary, Moldova, Romania, Serbia & Montenegro, Turkey*

Timeline & Milestones

2004 - 2006	*Operating CA, RA Network, Training, Dissemination*
Nov 2006	*Hungary and Turkey set up their National CA*
Mar 2007	*Bulgaria sets up its own National CA*
Aug 2007	*Croatia and Serbia set up their own National CA; established RA in Montenegro*
Jan 2008	*Romania sets up its own National CA*
Mar 2008	*F.Y.R.O.M. sets up its own National CA*
Sept 2008	*Montenegro sets up is own National CA; established RA in Georgia*
Jun 2009	*Moldova sets up is own National CA*
Dec 2009	*Established RA in Azerbaijan*
May 2010	*Provide Catch All CA Services for EGI*

Current RA Network



Central Registration Authority (1)

Active Registration Authorities (4)

Retired Registration Authorities (8)

EGI Catch All CA Services

- In EGI, SEE-GRID CA will provide catch all CA Services
- In EGEE CNRS has been performing this task
- Goal: Smooth transition of the catch all CA Services from CNRS CA to the SEE-GRID CA.

EGEE Catch ALL CA Service

- CNRS has been operating as the EGEE Catch All CA Service
- The following organizations have been supported by the CNRS CA:
  - Italy: ESA (ESRIN Unit)
  - Senegal: UCAD (CCI Unit)
  - US: MathWorks (Support Unit)
  - Vietnam: VAST (IAMI Unit, IOIT Unit), HUT (IFI Unit)

CP/CPS Update

- The new version of the CP/CPS is available for review at the SEE-GRID-CA web site [1]
- Three type of changes:
    I. Spelling & Wording Corrections
    II. Update of old information
    III. New items
- All changes are tracked on the master document with track changes on [2].
- Changes of type II and III are also tracked in the ChangeLog [3]

[1]: http://www.grid.auth.gr/pki/seegrid-ca/documents/cps/SEE-GRID-CA-CP-CPS-2.0.pdf
[2]: http://www.grid.auth.gr/pki/seegrid-ca/documents/cps/SEE-GRID-CA-CP-CPS-2.0-TC.pdf
[3]: http://www.grid.auth.gr/pki/seegrid-ca/documents/cps/SEE-GRID-CA-CP-CPS-changelog-1.1-2.0.pdf

Change Log

1. The overview text was changed in order to add information regarding the goal of SEE- GRID CA. [1.1]
2. Changed the OID arc of the CP/CPS to: 1.3.6.1.4.1.23877 [1.2]
3. Removed the term “medium security CA” [1.3.1]
4. RAs are appointed by SEE-GRID CA [1.3.2]
5. SEE-GRID CA will provide Catch All CA Services for EGI.eu [1.1, 1.3.3, 3.2.2, 7.1.5]
6. Providers of Computing Infrastructure Services are also considered to be Relying Parties [1.3.4]
7. Apart from research, also educational activities are considered as appropriate use [1.4.1]

Change Log

8. Changed the name of the organization to Grid & HPC Operations Center and the contact information [1.5.1, 1.5.2, 1.5.3, 2.1, 5.1.1, 5.3.1]
9. The CPS is reviewed internally in order to verify its compliance with the IGTF minimum requirements [1.5.4]
10. Added definitions and acronyms [1.6]
11. Certificates issued by the SEE-GRID CA, will be published in a searchable repository after the requester has successfully accepted the terms and conditions written in the CP/CPS [2.3]

Change Log

12. There will be no access controls for the CA certificate, the latest CRL and all versions of the CP and CPS, under which SEE-GRID CA has issued End Entity certificates [2.4]

13. SEE-GRID CA will support also Robot certificates [3.1.1, 3.1.5, 3.2.3, 4.1.2, 7.1.4, 7.1.5]

14. SEE-GRID CA checks that organization requiring certificate services for their users are affiliated with GRNET or EGI.eu and that there is person acting as liaison between the two [3.2.2]

Change Log

15. Digital processing entities must have a valid DNS name and the requesters must use their personal certificates in order authenticate themselves at the SEE-GRID CA portal or digitally signing the e-mail before submitting their certificate request. [3.2.3]

16. The telephone number of the subscriber is not verified. [3.2.4]

17. Adherence to the IGTF minimum requirements is the criterium for interoperation. [3.2.6]

18. Requests can be submitted either via the web portal or via digitally signed e-mail [3.3.1, 3.4, 4.4.1, 4.7.3, 4.9.3]

Change Log

19. At least once every five years or in case the request for re-key a personal certificate is due to revocation or expiration of the existing certificate or compromise of the private key, the user must present himself/herself in from of an RA in order to have his/her ID vetted [3.3.1, 4.7.3]

20. All users who have enrolled to the SEE-GRID CA can submit a certificate request. [4.1.1] 21. Reworked enrollment process and responsibilities [4.1.2] 22. Identity vetting must take place at least every 5 years. [4.2.1]

21. Each certificate request is assigned a unique hash string instead of a 10 digit number. [4.2.1]

Change Log

24. Removed the sentence stating the the subject must submit the certificate request within 2 working days after the id vetting has taken place. The requesters first submit their certificate request and then they have their identity vetted. [4.2.2]

25. SEE-GRID CA publishes only those certificates , whose requesters have accepted the terms and conditions outlined int the CP/CPS [4.4.2]

26. The on-line repository with the end entity certificates will be accessible only via a search web form. [4.4.2]

Change Log

27. Certificates can be used also in other kind of Computing Infrastructures [4.5.1, 4.5.2]

28. Subscribers must generate a new key pair for each certificate they request to be signed by the SEE-GRID CA. [4.7.1]

29. SEE-GRID CA does not modify signed End Entity certificates. [4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7]

30. Changed word “subscriber” with “owner” [4.9.2]

Change Log

31. The CA equipment is located in the Data Center of the Grid & HPC Operations Center and thus it uses the Power Generators, UPS, and Cooling System of the Data Center. [5.1.3]

32. Off-line media might be magnetic tape cartridges, floppies and CD-ROM" [5.1.6, 5.1.7]

33. GRNET is the Greek NGI [5.3.1]

34. Along with the old CA certificate, also the old CA private key must remain available. [5.6]

35. Added "No stipulation" instead of empty text. [5.7.2, 5.7.3, 5.7.4, 7.2.2, 9.2.1, 9.2.2, 9.2.3, 9.3.1, 9.3.2, 9.3.3]

Change Log

36. Changed “person, service or server” with “End Entity”. [6.1.5]
37. Removed Netscape Cert Type from the Certificate Extensions [7.1.2]
38. Removed non-repudiation from the key usage of the EE certificates [7.1.2]
39. Added Hash Function, RSA Encryption and Signature Algorithm [7.1.3]
40. Allow the following name space for EE Certificates: /DC=EU/DC=EGI/C=Country/ O=Institute/OU=[Hosts|People|Robots]/ CN=SUBJECT NAME [7.1.4, 7.1.5]

Change Log

41. Added description for the name constraints on the OrganizationalUnit field [7.1.5]

42. All EE certificates will include the OID 1.2.840.113612.5.2.2.1 [7.1.6]

43. SEE-GRID CA will issue only CRLs in version 2 format. [7.2.1]

44. Added subscriber's work phone number in the information that is not deemed as private . [9.4.3]

45. SEE-GRID CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation. [9.7]

Change Log

46. Removed the following statement: "SEE-GRID CA is run on a best effort basis and does not give any guarantees about the service security or suitability" [9.8]

47. Corrected the "Laws of Greece" to the "Greek Law" [9.14]

Thank You! Any Questions?