EGI Catch All CA Update

Christos Kanellopoulos <skanct@admin.grnet.gr>

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*

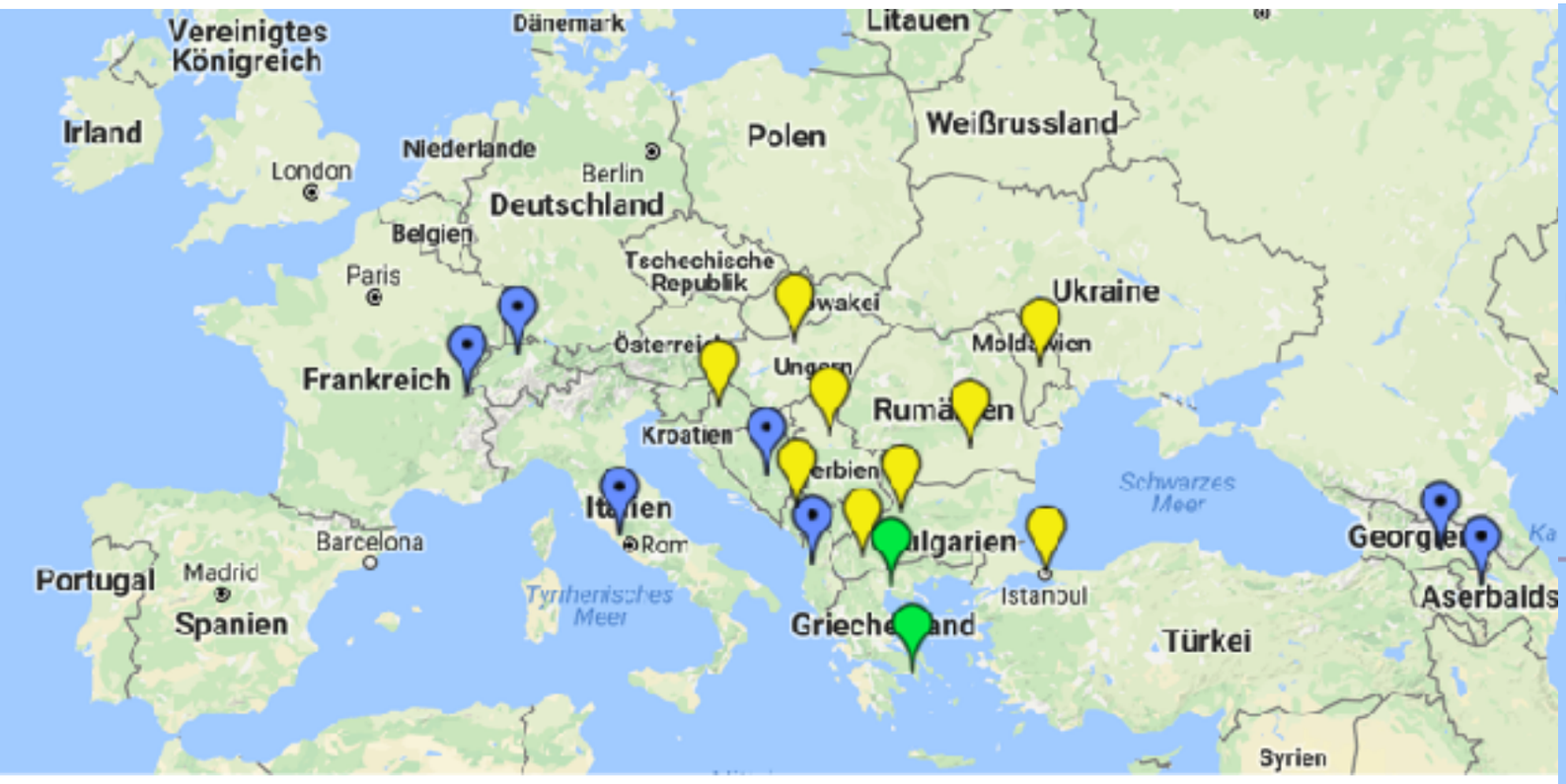
Timeline & Milestones

May 2010	*Provide Catch All CA Services for EGI*
Oct 2010	*Established RA in Senegal*
Dec 2010	*Established RA at SixSq in Switzerland*
Sept 2013	*Established RAs in South Africa and Nigeria*
Nov 2014	*Rollout of new CA certificate*
Jan 2014	*Established RA in Tanzania*
May 2015	*Established RA at University of Bern in Switzerland*
Nov 2015	*Established RA at Terradue Srl in Italy*

Current RA Network & Status

- Active Registration Authorities (12)
- Retired Registration Authorities (9)
- EGI Catch All CA

Current RA Network & Status



Active Registration Authorities (12)

Retired Registration Authorities (9)

EGI Catch All CA

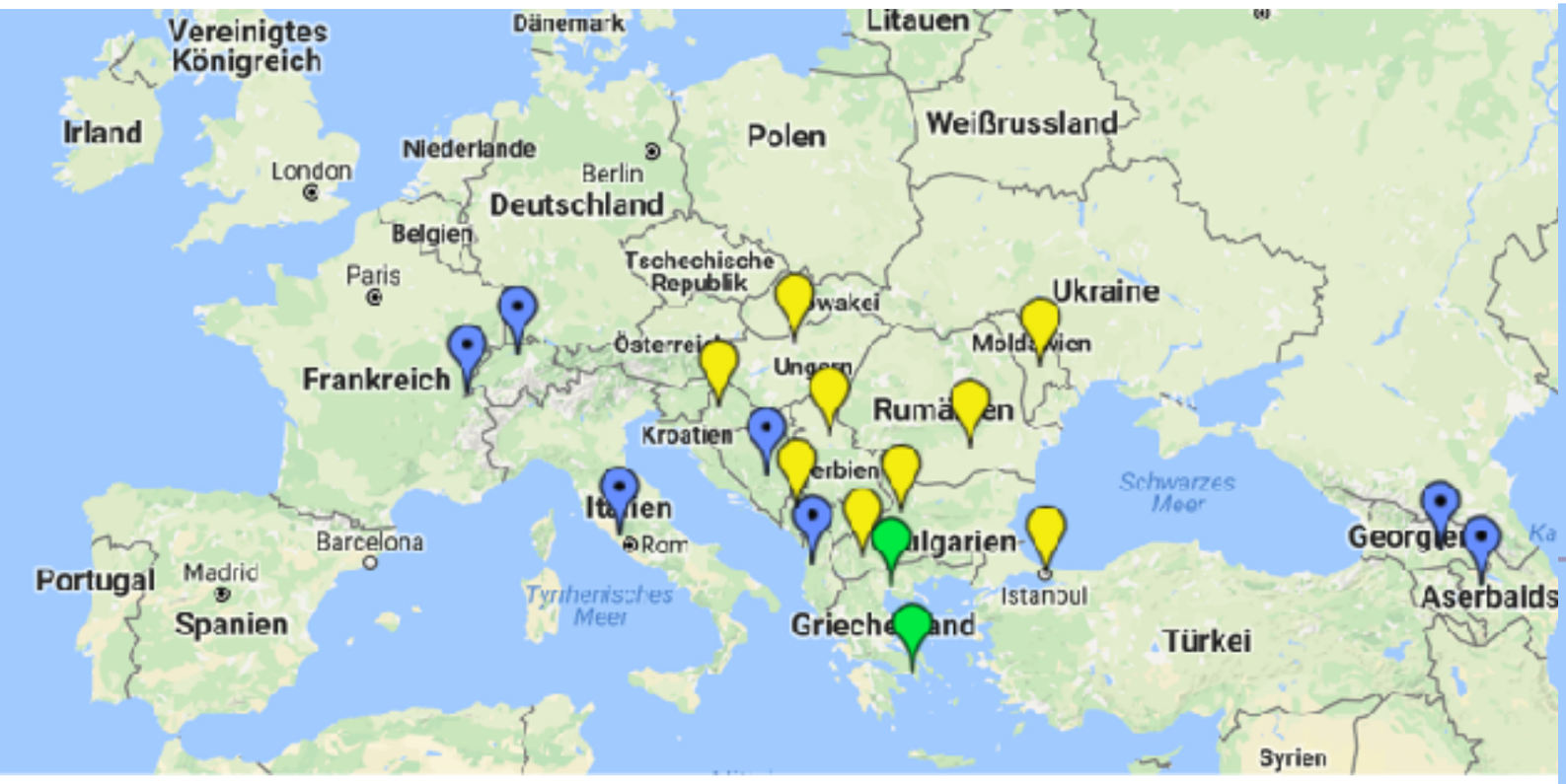
Active Certificates

People: 45

Hosts: 127

Robots: 9

Current RA Network & Status



Active Registration Authorities (12)

Retired Registration Authorities (9)

EGI Catch All CA

Active Certificates

People: 45

Hosts: 127

Robots: 9

SRCE (HR): 2

MTA SZTAKI (HU): 1

Current Processes

User Certificates

- User generates a new certificate request
- User sends the CSR to the RA
- The RA performs the identity vetting process
- The RA sends a signed e-mail with the CSR to the CA
- The CA issues the certificate and sends it to the User and the RA

Current Processes

Host/Robot Certificates

- User generates a new certificate request
- User sends the CSR to the RA
- The RA approves the certificate request
- The RA sends a signed e-mail with the CSR to the CA
- The CA issues the certificate and sends it to the User and the RA

Experiences

- Requests for expanding certificate coverage can consume a lot of time
- Time for setting up a new RAs ranges from a few weeks to ~ 1year
- The manual process for certificate requests is error prone and time consuming
- Certificate and CRL issuing requires manual intervention by the CA operators and is time consuming

In the meantime…

- Hellenic Academic and Research Institutions Certification Authority (HARICA)
- 2 ROOT CAs, 27 Intermediate CAs
- Certifications: ETSI TS 101 456, ETSI TS 102 042, CA/B Forum BR
- Pre-installed in browsers and OS (Mozilla Firefox, Microsoft Windows, Apple (iOS, OSX), Linux/Android.
- Qualified certificates for Greek public services
- Compatibility with eIDAS
- 3 Data Centers with DR capabilities
- HSM (FIPS 140-2 Level 3 certified)

In the meantime…

- eduGAIN is actively working on the expansion of the academic federations across the globe
- New policy/operational framework increase the trustworthiness of the Identity Federations/IdPs
  - Code of Conduct
  - Research & Scholarship Entity Category
  - SIRTFY
- EGI is actively enabling federated access to services (very soon they will join eduGAIN)
  - Still certificates are needed for various workflows

Next steps…

- Migration of the EGI Catch All CA from offline to an online configuration
- Initial set up using Safenet 5110 eToken (FIPS 140-2 level 3 certified)
- Online CA machine located in the main DC
  - Physical access to the DC only by authorised personnel using access cards
  - Physical access to the online CA service only the CA operators
  - Network access to the online CA only from the RA portal

Next steps…

- Transition from the e-mail based process to a web based certificate request process
  - Initial phase re-use the existing web portal (HARICA)
  - adaptation to the requirements/workflows of the EGI Catch All CA
- Support for authentication to Federated Identity Management Systems (FIMS) (in parallel to the existing RA network)
  - Support for IdPs that support SIRTFY and R&S or equivalent (e.g. EGI AAI)

Next steps…

- Hardware infrastructure already in place
- CP/CPS update Oct 2016
- RA portal ready by Nov 2016

grnet
Networking Research and Education

Thank you for your attention!

Questions?