



EUGridPMA

Status and Current Trends

and some IETF topics

March 2018
APGridPMA ISGC Meeting

David Groep, Nikhef & EUGridPMA

Recent EUGridPMA topics

- PMA membership and reviews
- Infrastructure Policy Alignment & *Snctfi*

Up Next:

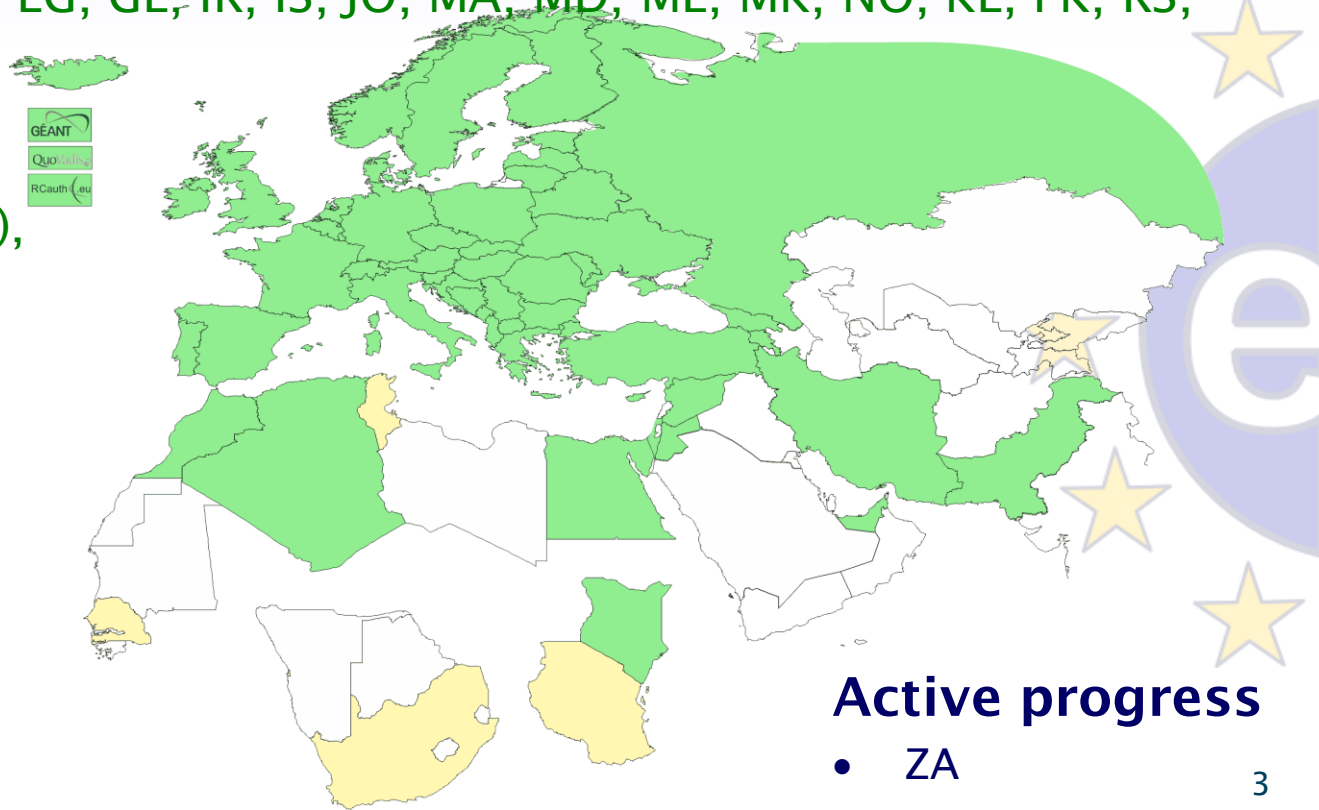
- AAI for research and collaboration
 - Policy and technology Bridging using infrastructure proxies
 - Bridging trust: assurance, security, and uniqueness in RCauth
- OIDC Federation at the IGTF for Research and e-Infrastructures

See also the EUGridPMA42 summary:

<https://www.eugridpma.org/meetings/2018-01/>

Geographical coverage of the EUGridPMA

- 26 of 28 EU member states (all except LU, MT)
- + AE, AM, CH, DZ, EG, GE, IR, IS, JO, MA, MD, ME, MK, NO, KE, PK, RS, RU, SY, TR, UA, CERN (int), TCS (EU), RCauth.eu (EU/NL), QV (BM)



Active progress

- ZA

Membership and other changes

- Responsiveness challenges for some members
PLEASE take care to renew your trust anchors in time, as well as your CRLs
- Identity providers: both reduction and growth
 - Grid-FR now hosted within French government PKI infrastructure
 - RCauth.eu distributed operations (GRNET, STFC, Nikhef)
- Self-audit review
 - Cosmin Nistor as review coordinator
 - Self-audits progressing on schedule for most CAs

		Specific Policies and Practices			
TR-Grid CA (Turkey) <i>(Authority member)</i> <i>(TACAR OK)</i>	Feyza Eryol	CA TRGrid (accredited:classic): CERT CRL concerns: ca@grid.org.tr A2:31:9E:C8:90:AF:D9:6D:F4:4A:59:31:F2:E6:D2:D5:39:EC:1D:FD	2005-09-29	2016-01-20	2016-01-20 (0.2yr)
Trans-European Research and Educational Networking Association (TERENA) <i>(Relying Party member)</i>	Licia Florio (277707CC)	<i>CP and CPS are not relevant</i> About TERENA: http://www.terena.org/	2004-04-01	2015-09-09	
UK e-Science CAs <i>(Authority member)</i> <i>(TACAR OK)</i>	Jens Jensen (9210F006) David Kelsey	CA UKeScienceRoot-2007 (accredited:classic): CRL concerns: support@grid-support.ac.uk A1:39:80:F3:04:6C:0B:F9:F5:0A:1B:33:00:06:4F:83:6B:7D:4F:3E	2000-12-04	2016-01-20	2014-01-14 (2.2yr)
		CA UKeScienceCA-2A (accredited:classic): CRL concerns: support@grid-support.ac.uk 41:C7:C4:A0:31:F7:07:02:81:C7:61:D5:7E:92:4B:01:DF:87:C9:06			
		CA UKeScienceCA-2B (accredited:classic): CRL concerns: support@grid-support.ac.uk DB:D9:5A:B4:E9:AD:74:26:E0:33:68:AA:B1:77:CC:5B:64:82:C8:0E			
Ukrainian Grid CA <i>(Authority member)</i> <i>(TACAR FAILURE)</i>	Sergii Stirenko Oleg Alienin	CA UGRID (accredited:classic): CERT CRL concerns: ca@ugrid.org 21:E7:0D:EE:D7:57:B6:47:A6:F5:04:29:76:81:FE:CD:E8:48:DD:9A	2008-02-14	2013-09-11	2013-09-11 (2.5yr)
		Generic CP and CPS statements			

Upcoming events

**EUGridPMA 43,
Karlsruhe**

May 23 – 25, 2018

I2GS, TAGPMA

May 6-10 (incl 10th!), San Diego, CA, USA

TNC18 and REFEDS

June 10, 11-14, Trondheim, NO

PEARC18

July 22-26, Pittsburg, PA, USA

TechEx

Oct 15-18, Orlando, FL, USA



AAI in a wider context

IGTF traditionally well-linked to research and e-Infrastructures

- *support for research use cases*
- *user-centric authentication based on a 'bottom-up' approach*

In Europe, the AARC project supports evolution of 'traditional' R&E federations towards this research and collaboration use

- *common Blueprint Architecture promoting **SP-IdP Proxies***
- *harmonised **policy supporting production use** of federations (Sirtfi and "R&S", non-reassigned identifiers and assurance)*
- *help communities express 'common' qualities through **Snctfi***
- *allow newer technologies (**OIDC**) on the Infrastructure side*

Assurance and trust frameworks

Identity Assurance Profiles for Infrastructure risk scenarios

<https://igtf.net/ap/loa/>

- BIRCH - good quality (federated) identity,
DOGWOOD - identifier-only with traceability (*R&S+Sirtfi+a few bits*)
- RFC 6711 Registry: <https://iana.org/assignments/loa-profiles>
- technology-specific ‘trust anchor’ distribution services

Supporting research and e-Infrastructure use cases

- technology bridges: *TCS, RCauth.eu, IGTF-eduGAIN bridge, ...*
- behind Infrastructure Proxies OIDC gains prominence: *OIDC Fed for RP pilot*

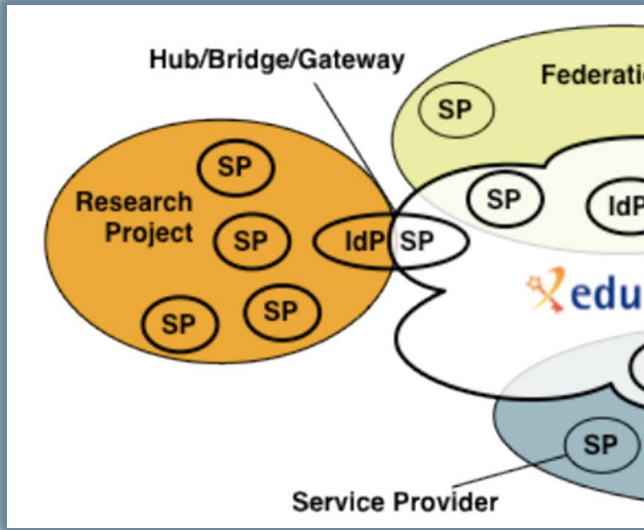
Policy framework for Relying Parties (‘SP-IdPs-Proxies’)

- Snctfi - Community Trust Framework in Federated Infrass
<https://igtf.net/snctfi>
- Policy Development Kit



Snctfi: aiding Infrastructures achieve policy coherency

- ✓ allow SP-IdP-Proxies to assert 'qualities', based on assessable trust
- ✓ Develop **recommendations for an Infrastructure's coherent policy set**



Graphics inset: Ann Harding and Lukas Hammerle, GEANT and SWITCH

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Complements Sirtfi with requirements on internal consistent policy sets for Infrastructures
- Aids Infrastructures assert *existing* categories R&S, Sirtfi, CoCo
- Support communities and infrastructures with a *policy kit* and *Acceptable Use Policy* alignment



Trust for global e-Science infrastructures

“establish common policies and guidelines that enable interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and relying parties”

