EUGridPMA
Status and Current Trends
and some IGTF topics

October 2017
APGridPMA Autumn Meeting

David Groep, Nikhef & EUGridPMA

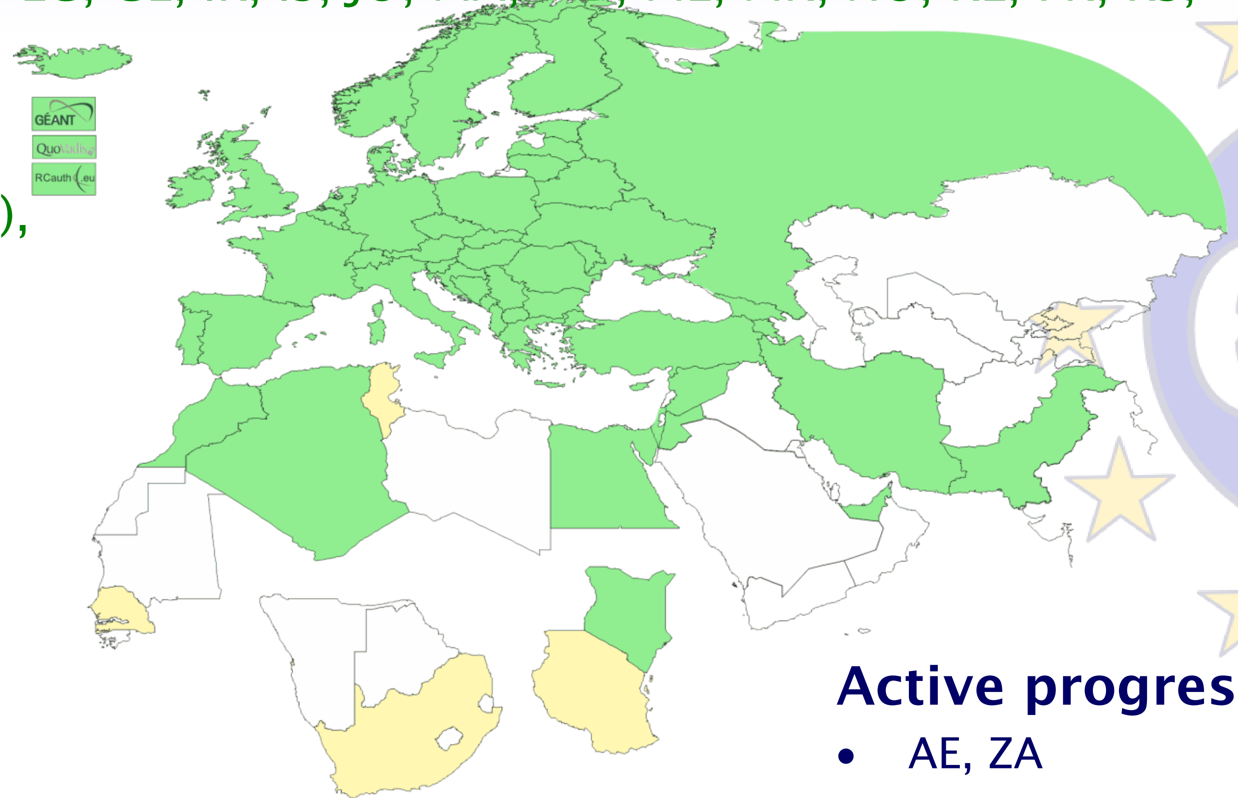
EUGridPMA Topics

- EUGridPMA (membership) status
- AAI developments in the world: FIM4R, Sirtfi, Snctfi, and AARC2
- Meshing authentication: IGTF-to-eduGAIN bridge & RCauth.eu
- New directions: OIDCfed, maintenance of the RA network, and more
- Beyond AuthN: Assurance Assessment Matrix for CO Registries
- IPv6, SHA-1 collisions, and more

See also the EUGridPMA41 summary:
https://www.eugridpma.org/meetings/2017-09/

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)



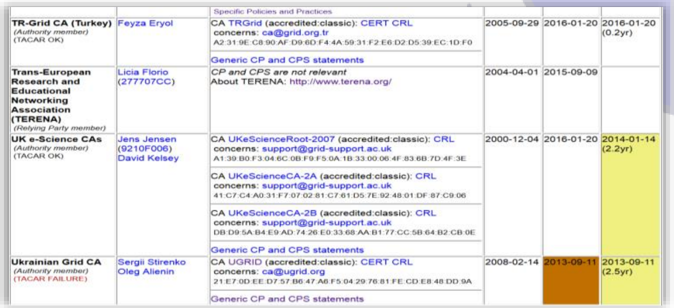
47+4

Active progress

- AE, ZA

Membership and other changes

- Responsiveness challenges for some members
  - JUNET discontinued, HIAST – remains suspended
  - *PLEASE* take care to renew your trust anchors in time,
    as well as your CRLs (applies globally, e.g. for SDG-G2 and CNIC)
- Identity providers: both reduction and growth
  - New CA for e-Infras: RCauth.eu IOTA CA (“for those who cannot use TCS”)
  - New CA for UAE: DarkMatter (phase 2 of 2)
  - Upcoming in UK: Adding a BIRCH CA based
    on “Moonshot” (Assent) and explicit sign-up
- Self-audit review
  - Cosmin Nistor as review coordinator
  - Self-audits progressing
    on schedule for most CAs



		Specific Policies and Practices			
TR-Grid CA (Turkey) *(Authority member)* (TACAR OK)	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:F0 Generic CP and CPS statements	2005-09-29	2016-01-20	2016-01-20 (0.2yr)
Trans-European Research and Educational Networking Association (TERENA) *(Relying Party member)*	Licia Florio (277707CC)	*CP and CPS are not relevant* About TERENA: http://www.terena.org/	2004-04-01	2015-09-09	
UK e-Science CAs *(Authority member)* (TACAR OK)	Jens Jensen (9210F006) David Kelsey	CA UKeScienceRoot-2007 (accredited:classic): CRL concerns: support@grid-support.ac.uk A1:39:B0:F3:04:6C:0B:F9:F5:0A:1B:33:00:06:4F:83:6B:7D:4F:3E 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:92:48:01: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:B2:CB:0E Generic CP and CPS statements	2000-12-04	2016-01-20	2014-01-14 (2.2yr)
Ukrainian Grid CA *(Authority member)* (TACAR FAILURE)	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 Generic CP and CPS statements	2008-02-14	2013-09-11	2013-09-11 (2.5yr)

AAI in a wider context

IGTF traditionally well-linked to research and e-Infrastructures

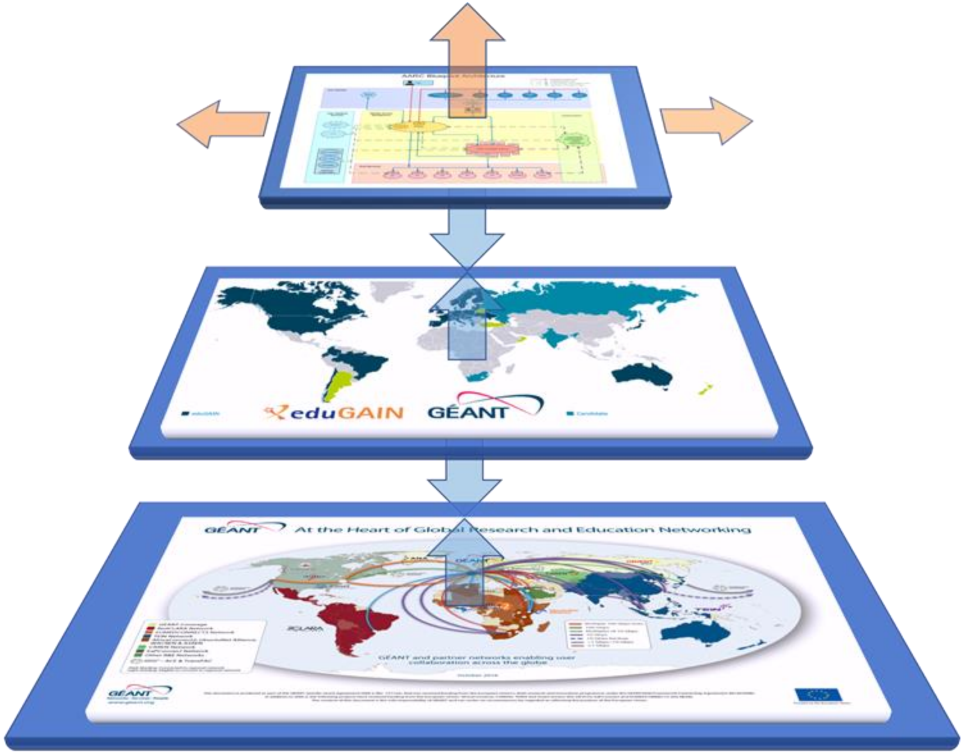
- *support for research use cases*
- *user-centric authentication based on a ‘bottom-up’ approach*

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 baseline LoA)*
- *help communities express ‘common’ qualities through Snctfi*

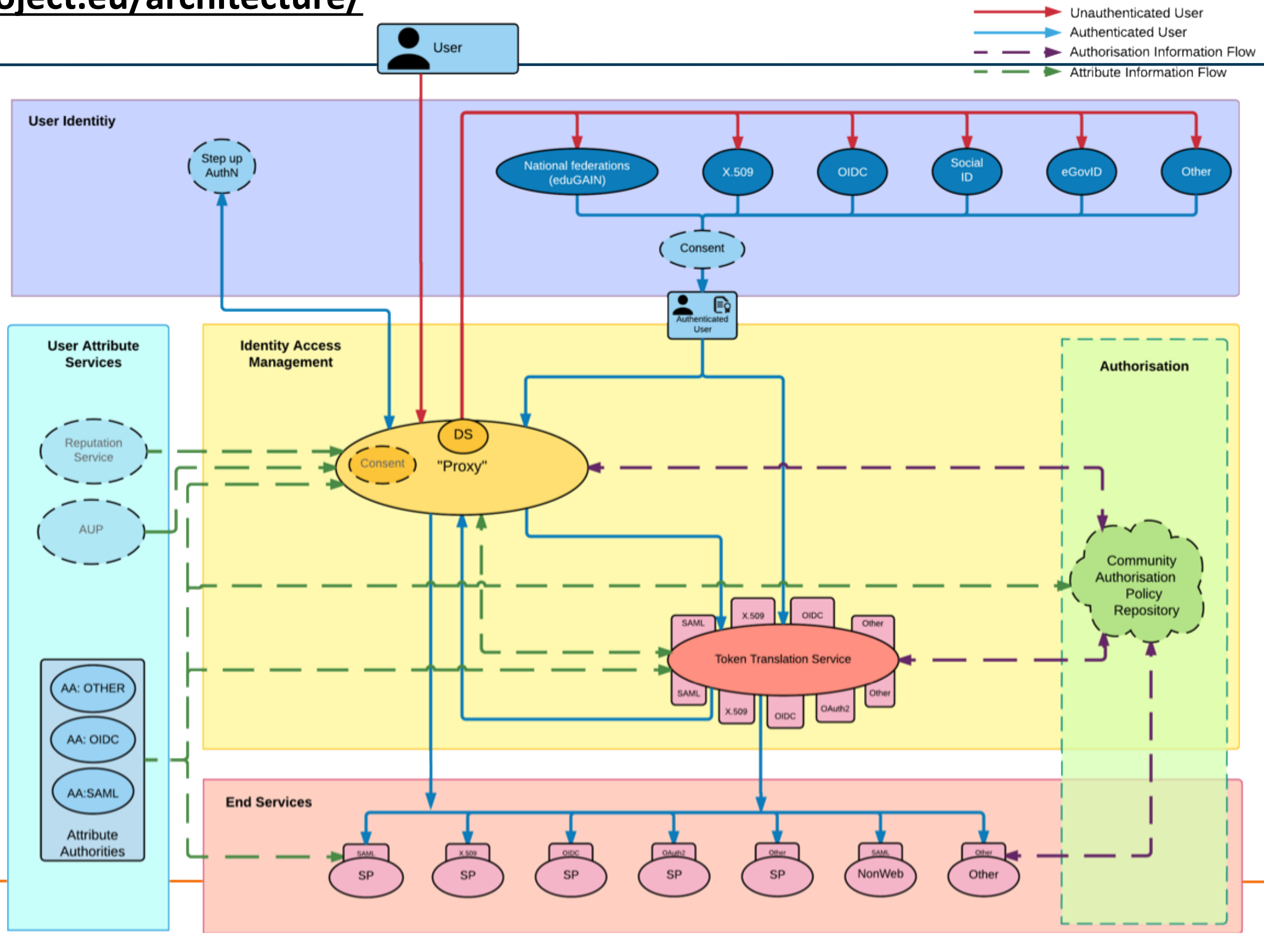
AARC Blueprint Architecture - Enabling an ecosystem of solution on top of eduGAIN

- A Blueprint **Architecture** for authentication and authorization
  - A set of **architectural and policy building blocks** on top of eduGAIN
- **eduGAIN** and the Identity Federations
  - **A solid foundation** for federated access in Research and Education



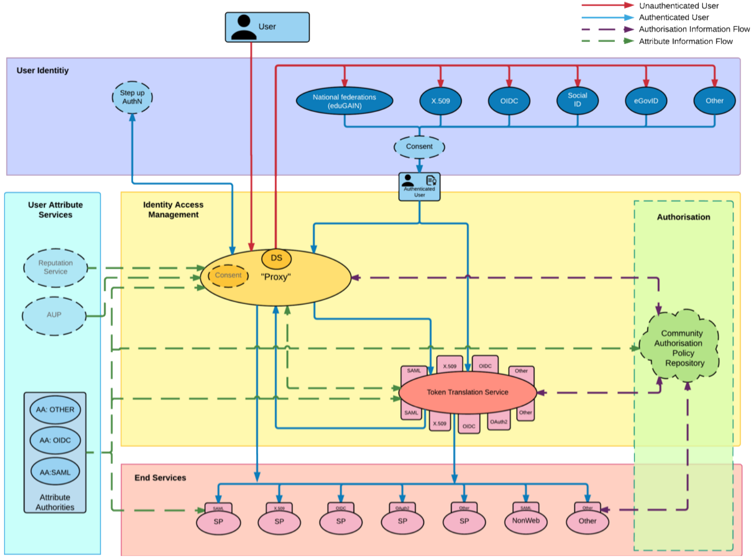
AARC Blueprint Architecture

https://aarc-project.eu/architecture/



AARC Blueprint Architecture

https://aarc-project.eu/architecture/

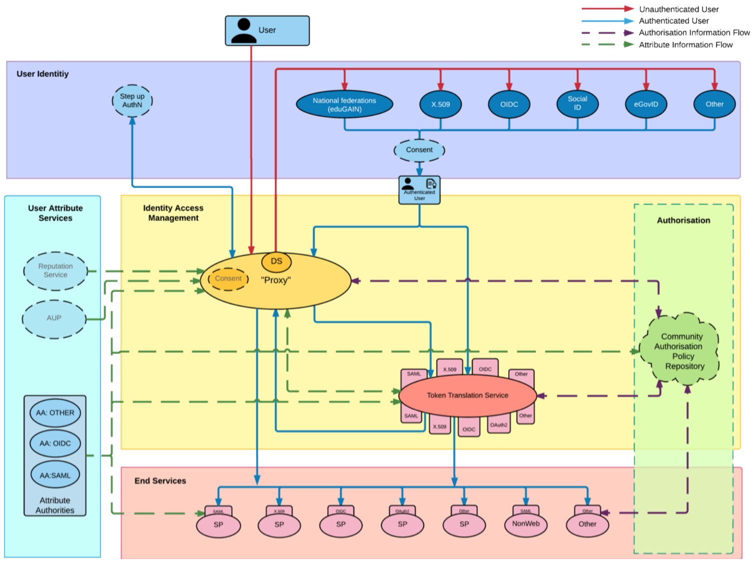


Guidelines and support documents

- Best practices for managing authorisation
- Expressing group membership and role information
- Scalable attribute aggregation
- Implementation of token TTS
- Credential delegation
- Non-web access
- Social media IdPs
- Use cases for account linking
- Use cases for LoA elevation via step-up authentication

AARC Blueprint Architecture

https://aarc-project.eu/policies/



Policy recommendations & frameworks

- Security Incident Response Trust Framework for Federated Identity – Sirtfi
- Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – Snctfi
- Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases
- Differentiated LoA recommendations for policy and practices of identity and attribute providers
- Recommendations and template policies for the processing of personal data by participants in the pan-European AAI

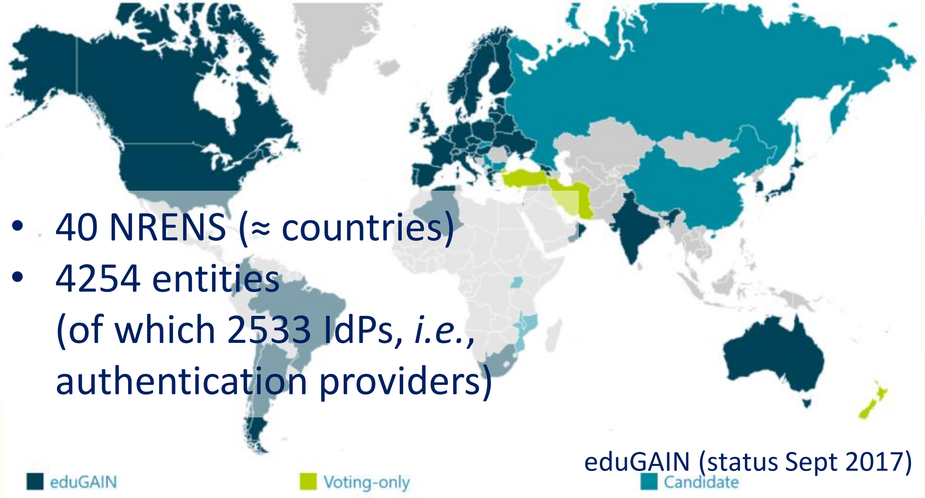
What the IGTF can do (for authN services)

- Inspired and aligned with community and e-Infrastructure needs
- Differentiated assurance with both a solid and transparent level
- Assessment model via peer-reviewed self-assessment
- Promotion of alignment within Infrastructures – maintenance of **Snctfi**

And our ‘conventional’ capabilities of providing a quality authentication source:

- *User-centric* authentication – independent of user’s home organization
- Ability to transfer registrations across authorities and countries
  (with the Registration Practice Statement)
- guidance on trust and trustworthy operations for AuthN and Attributes

eduGAIN … and Infrastructure Proxies



- 40 NRENS (≈ countries)
- 4254 entities (of which 2533 IdPs, *i.e.*, authentication providers)

eduGAIN (status Sept 2017)

- organisation-centric, and with much national autonomy in policy & practice
- where it reaches the users *and* a ‘link’ is made, provides great ease of use
- in most organisations, research is not the primary use case (yet) for the ‘IdP’

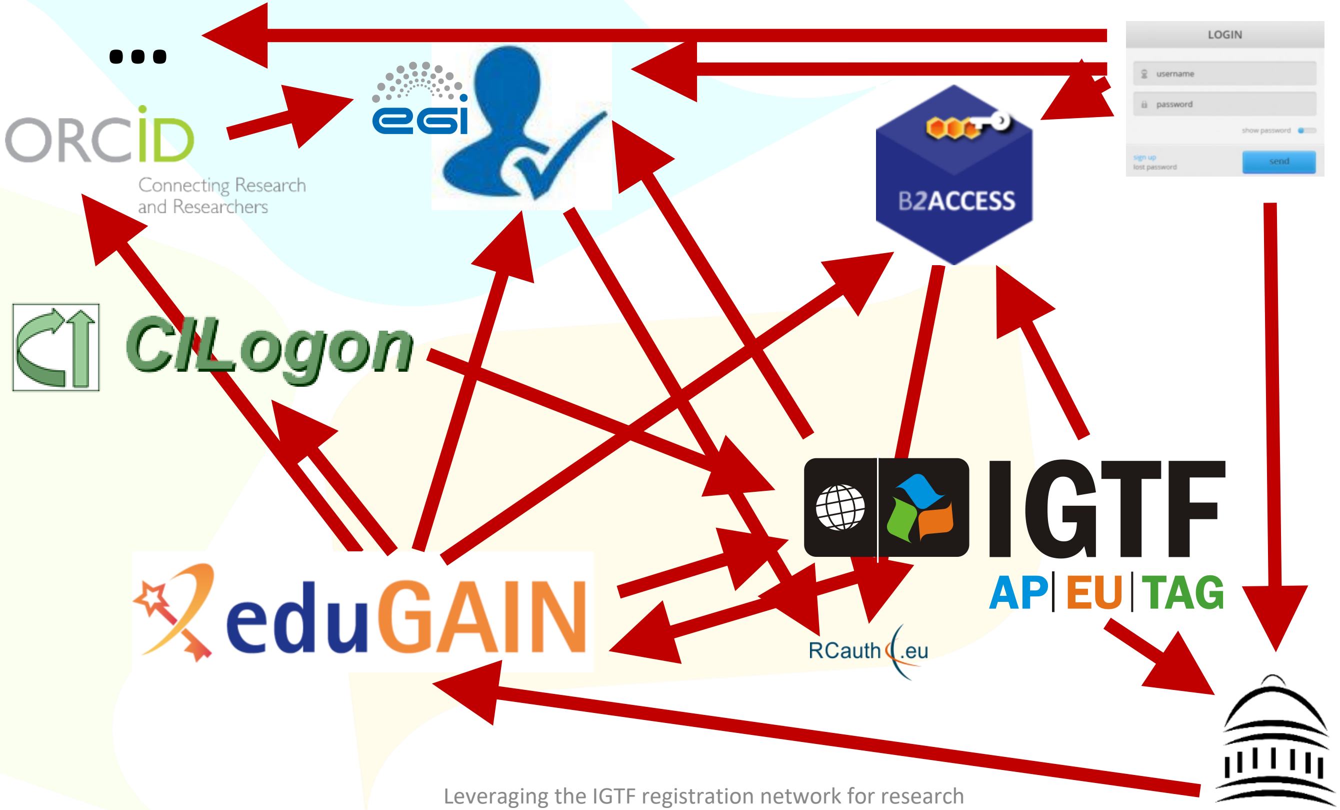
B2ACCESS

CILogon

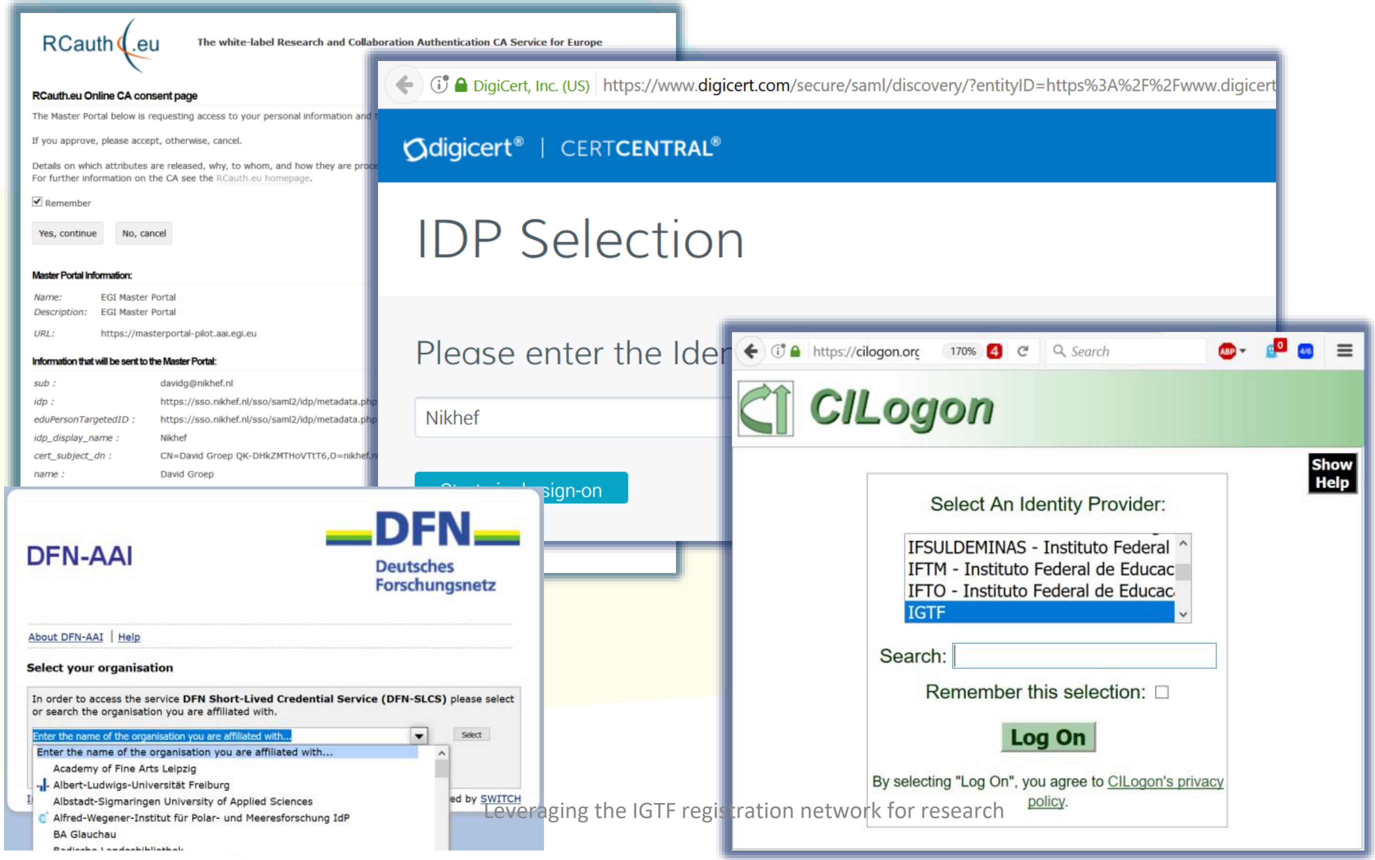
ORCID
Connecting Research and Researchers

- EGI CheckIn
- B2ACCESS
- CILogon
- ORCID
- …

Turtles all the way down … and up!



TCS – CILogon – DFN SLCS – RCauth.eu



RCauth.eu

The white-label Research and Collaboration Authentication CA Service for Europe

RCauth.eu Online CA consent page

The Master Portal below is requesting access to your personal information and t

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are proce
For further information on the CA see the RCauth.eu homepage.

☑ Remember

Yes, continue | No, cancel

Master Portal Information:

Name:	EGI Master Portal
Description:	EGI Master Portal
URL:	https://masterportal-pilot.aai.egi.eu

Information that will be sent to the Master Portal:

sub :	davidg@nikhef.nl
idp :	https://sso.nikhef.nl/sso/saml2/idp/metadata.php
eduPersonTargetedID :	https://sso.nikhef.nl/sso/saml2/idp/metadata.php
idp_display_name :	Nikhef
cert_subject_dn :	CN=David Groep QK-DHkZMTHoVTtT6,O=nikhef.nl
name :	David Groep

DigiCert, Inc. (US) https://www.digicert.com/secure/saml/discovery/?entityID=https%3A%2F%2Fwww.digicert

digicert® | CERTCENTRAL®

IDP Selection

Please enter the Ider

Nikhef

sign-on

DFN-AAI

DFN Deutsches Forschungsnetz

About DFN-AAI | Help

Select your organisation

In order to access the service **DFN Short-Lived Credential Service (DFN-SLCS)** please select or search the organisation you are affiliated with.

Enter the name of the organisation you are affiliated with... | Select

- Enter the name of the organisation you are affiliated with...
- Academy of Fine Arts Leipzig
- Albert-Ludwigs-Universität Freiburg
- Albstadt-Sigmaringen University of Applied Sciences
- Alfred-Wegener-Institut für Polar- und Meeresforschung IdP
- BA Glauchau

ed by SWITCH

https://cilogon.org 170%

CILogon

Show Help

Select An Identity Provider:

- IFSULDEMINAS - Instituto Federal
- IFTM - Instituto Federal de Educac
- IFTO - Instituto Federal de Educac
- IGTF

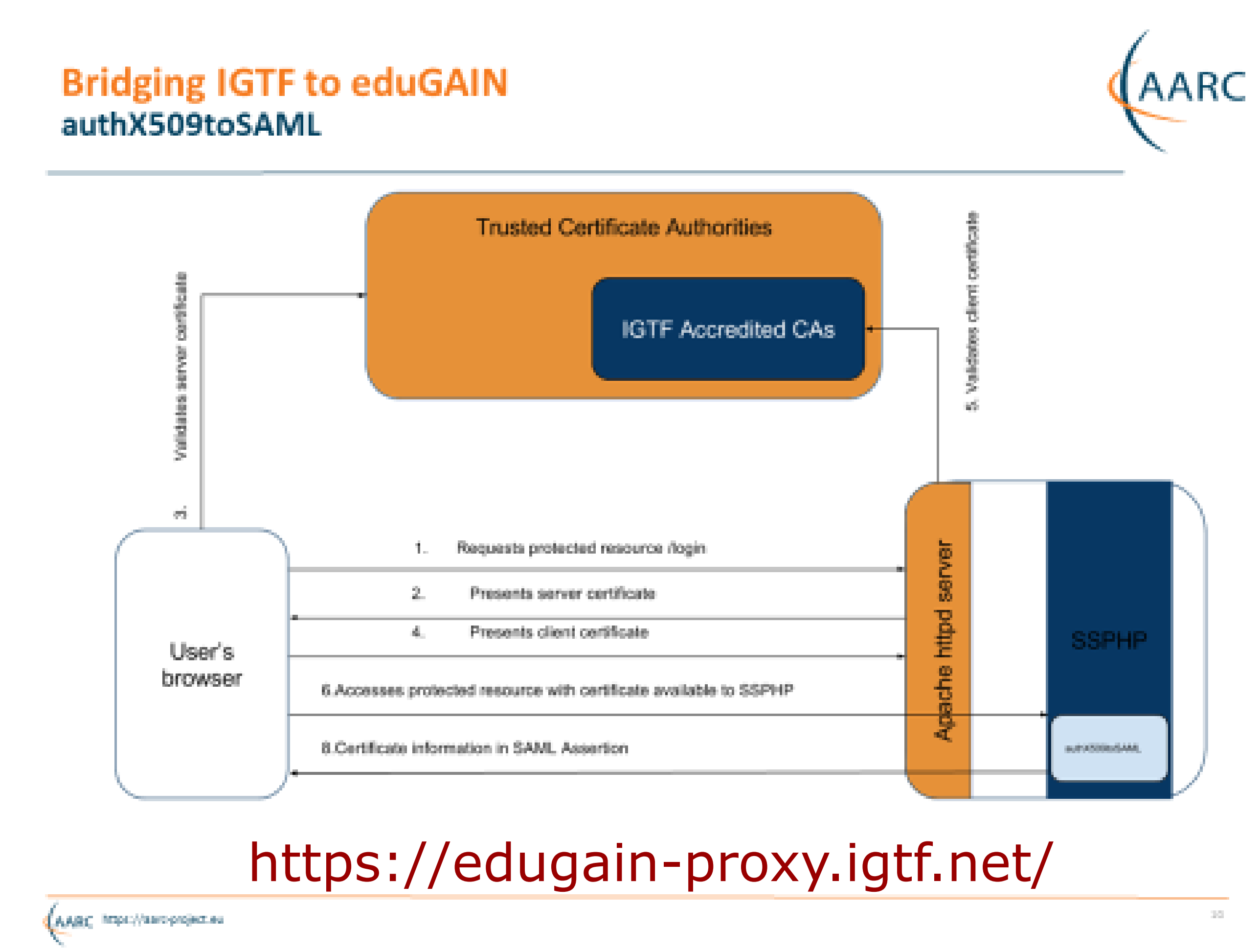
Search:

Remember this selection: □

Log On

By selecting "Log On", you agree to CILogon's privacy policy.

IGTF t



Bridging IGTF to eduGAIN

authX509toSAML

AARC
Trusted Certificate Authorities
IGTF Accredited CAs
3. Validates server certificate
5. Validates client certificate
User's browser
Apache httpd server
SSPHP
authX509toSAML
1. Requests protected resource /login
2. Presents server certificate
4. Presents client certificate
6.Accesses protected resource with certificate available to SSPHP
8.Certificate information in SAML Assertion
AARC https://aarc-project.eu

https://edugain-proxy.igtf.net/

10 October 2017

Work by Ioannis Kakavas and Nicolas Liampotis (GRNET) for the AARC project

Guidance we have and use

Assurance Profile – now being registered with IANA RFC6711

- https://www.igtf.net/ap/

Assessment support

- http://wiki.eugridpma.org/Main/AssuranceAssessment

'Back-office' template practices

- https://www.eugridpma.org/documentation/rps/

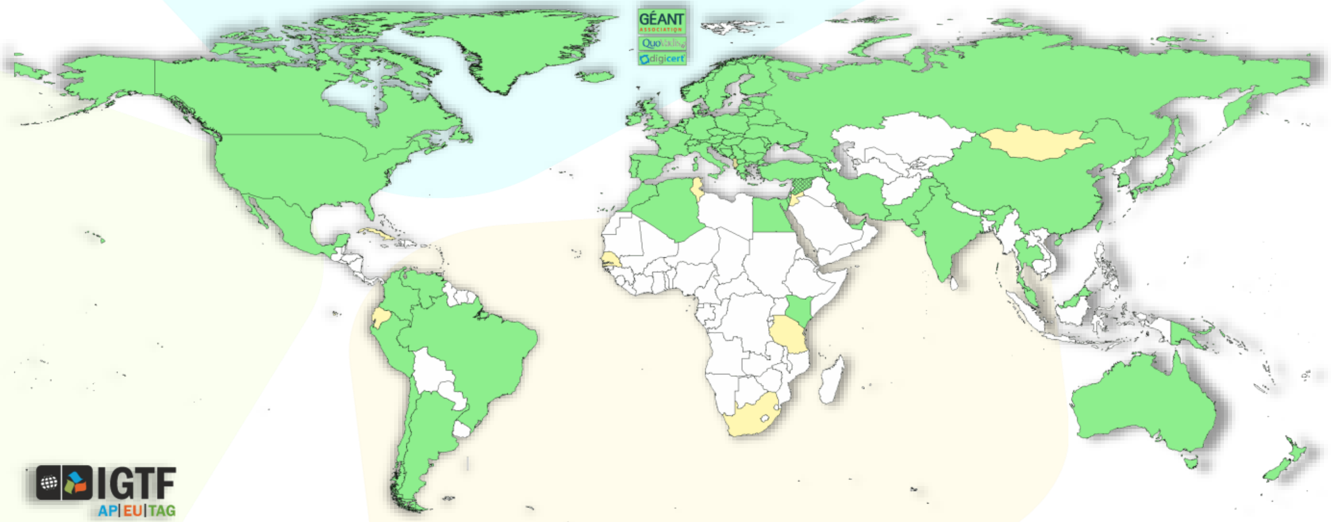
Registration Networks

Although the process is labour-intensive and relatively slow, for some user categories the prevalent ‘user-held’ credential is the only one that ‘works’:

- non-academic users (SMEs, industrial R&S)
- users in a place without an eduGAIN federation
- users in a place that does not do unique ID
- users in an organization that does not release attributes
- users in an organization that does not provide assurance
- …

Are we the ‘high-quality IdP of last resort’?

- Most useful asset is our RA network!



ASSURANCE ASSESSMENT SUPPORT

IOTA in the EGI context

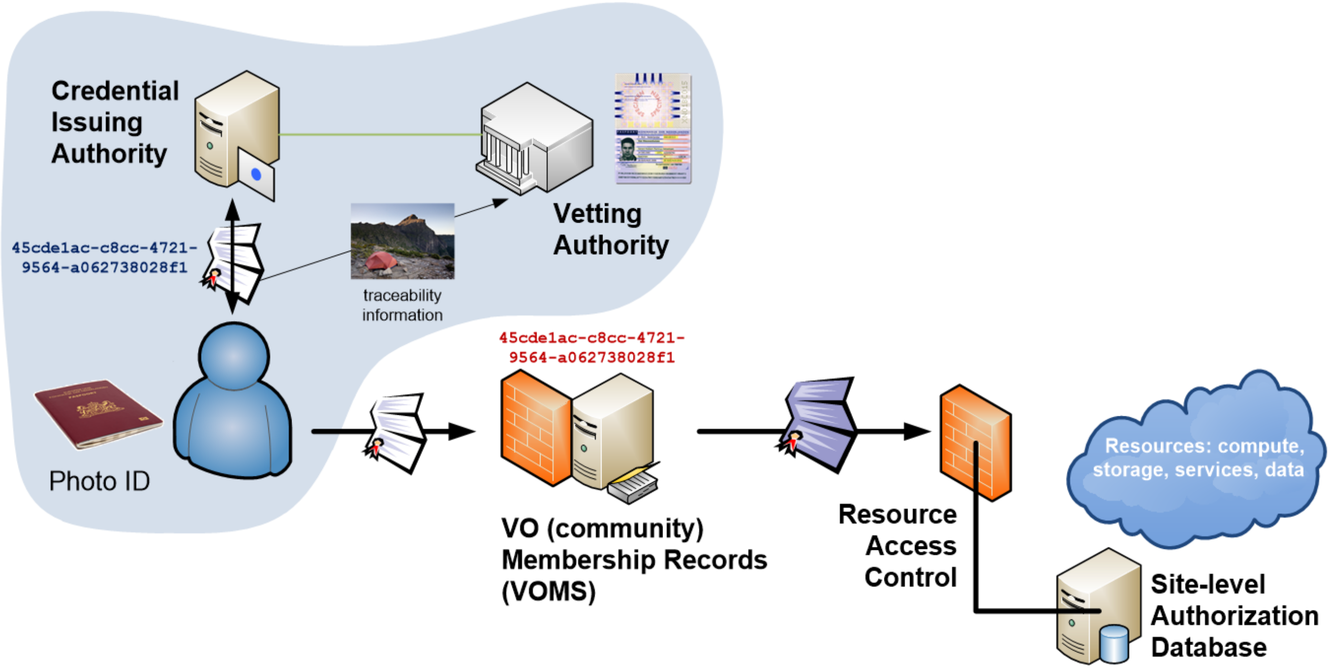
EGI – by design - supports loose and flexible user collaboration

- 300+ communities
- Many established ‘bottom-up’ with fairly light-weight processes
- Membership management policy* is deliberately light-weight
- Most VO managers rely on naming in credentials to enroll colleagues

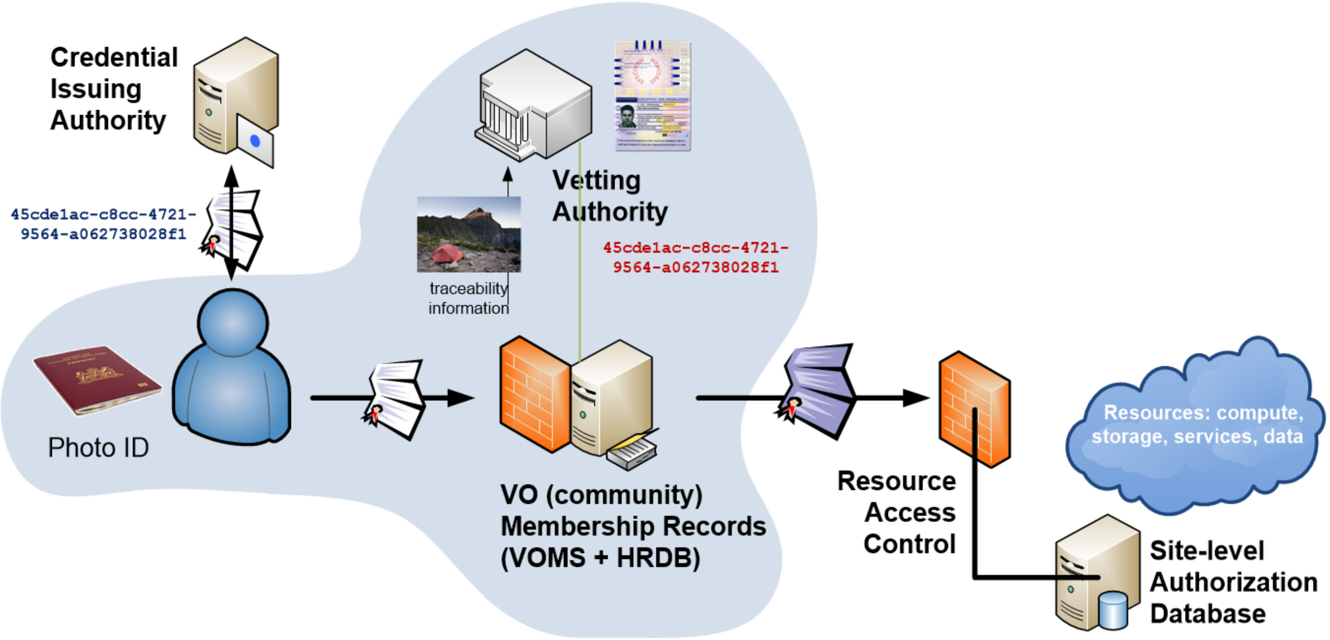
Only a few VOs are ‘special’

- LHC VOs: enrolment is based on the users’ entry in a special (CERN-managed) HR database, based on a separate face-to-face vetting process and eligibility checks, including government photo ID + institutional attestations
- Only properly registered and active people can be listed in VOMS

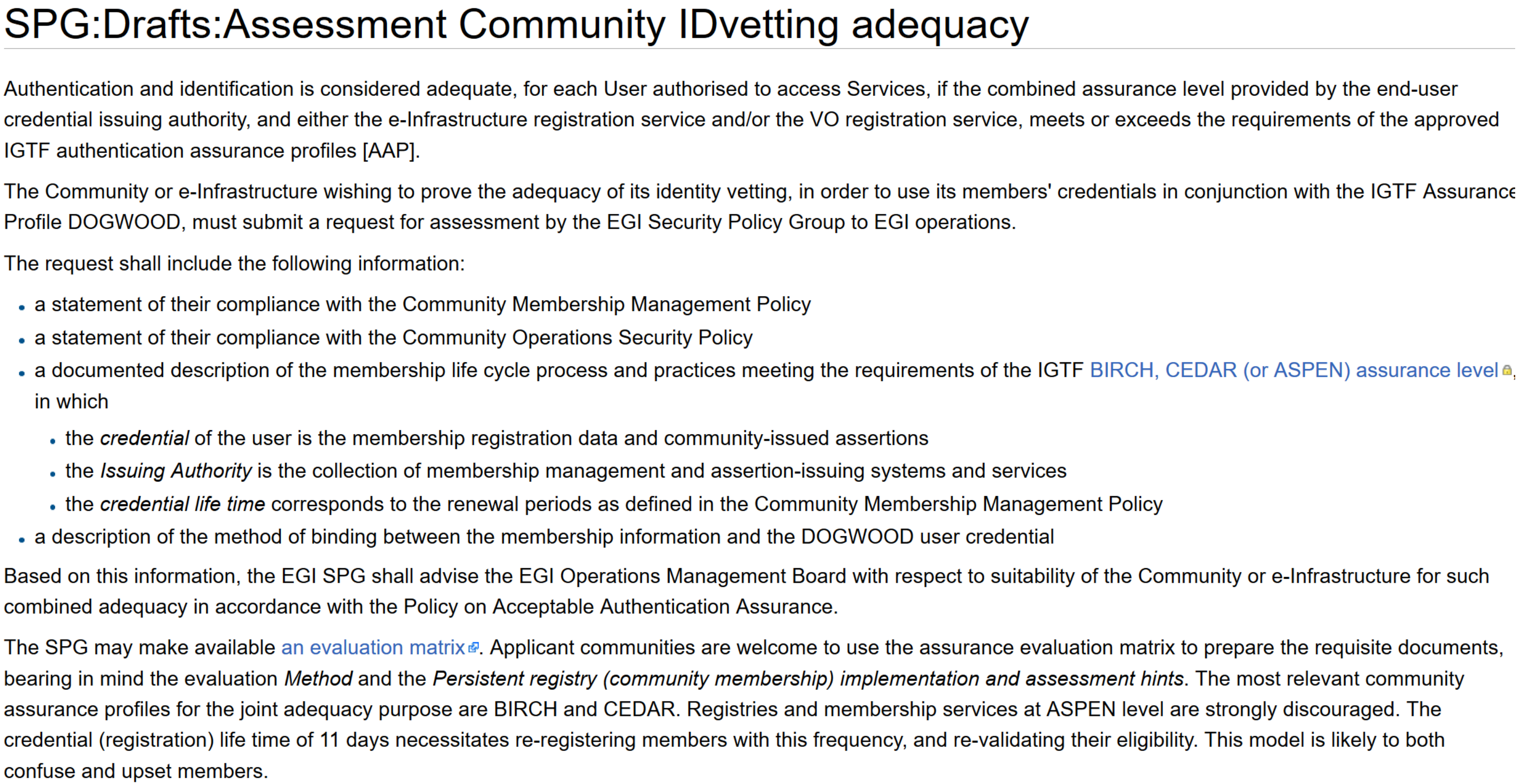
Distributed Responsibilities I: Trusted Third Party


Credential Issuing Authority
Vetting Authority
45cde1ac-c8cc-4721-9564-a062738028f1
traceability information
Photo ID
45cde1ac-c8cc-4721-9564-a062738028f1
VO (community) Membership Records (VOMS)
Resource Access Control
Resources: compute, storage, services, data
Site-level Authorization Database

Distributed Responsibilities II: Collaborative Assurance & Traceability


Credential Issuing Authority
45cde1ac-c8cc-4721-9564-a062738028f1
Vetting Authority
45cde1ac-c8cc-4721-9564-a062738028f1
traceability information
Photo ID
VO (community) Membership Records (VOMS + HRDB)
Resource Access Control
Resources: compute, storage, services, data
Site-level Authorization Database

Developing an assessment framework



SPG:Drafts:Assessment Community IDvetting adequacy

Authentication and identification is considered adequate, for each User authorised to access Services, if the combined assurance level provided by the end-user credential issuing authority, and either the e-Infrastructure registration service and/or the VO registration service, meets or exceeds the requirements of the approved IGTF authentication assurance profiles [AAP].

The Community or e-Infrastructure wishing to prove the adequacy of its identity vetting, in order to use its members' credentials in conjunction with the IGTF Assurance Profile DOGWOOD, must submit a request for assessment by the EGI Security Policy Group to EGI operations.

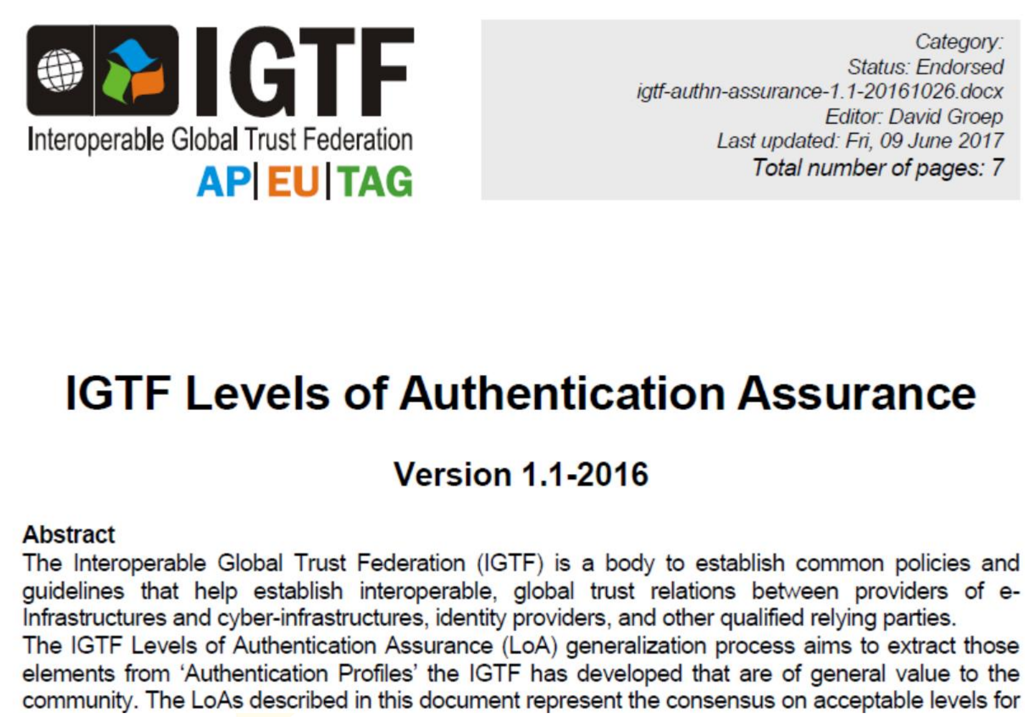
The request shall include the following information:

- a statement of their compliance with the Community Membership Management Policy
- a statement of their compliance with the Community Operations Security Policy
- a documented description of the membership life cycle process and practices meeting the requirements of the IGTF BIRCH, CEDAR (or ASPEN) assurance level, in which
  - the *credential* of the user is the membership registration data and community-issued assertions
  - the *Issuing Authority* is the collection of membership management and assertion-issuing systems and services
  - the *credential life time* corresponds to the renewal periods as defined in the Community Membership Management Policy
- a description of the method of binding between the membership information and the DOGWOOD user credential

Based on this information, the EGI SPG shall advise the EGI Operations Management Board with respect to suitability of the Community or e-Infrastructure for such combined adequacy in accordance with the Policy on Acceptable Authentication Assurance.

The SPG may make available an evaluation matrix. Applicant communities are welcome to use the assurance evaluation matrix to prepare the requisite documents, bearing in mind the evaluation *Method* and the *Persistent registry (community membership) implementation and assessment hints*. The most relevant community assurance profiles for the joint adequacy purpose are BIRCH and CEDAR. Registries and membership services at ASPEN level are strongly discouraged. The credential (registration) life time of 11 days necessitates re-registering members with this frequency, and re-validating their eligibility. This model is likely to both confuse and upset members.

The need for guidance



IGTF
Interoperable Global Trust Federation
AP|EU|TAG

Category:
Status: Endorsed
igtf-authn-assurance-1.1-20161026.docx
Editor: David Groep
Last updated: Fri, 09 June 2017
***Total number of pages:** 7*

IGTF Levels of Authentication Assurance

Version 1.1-2016

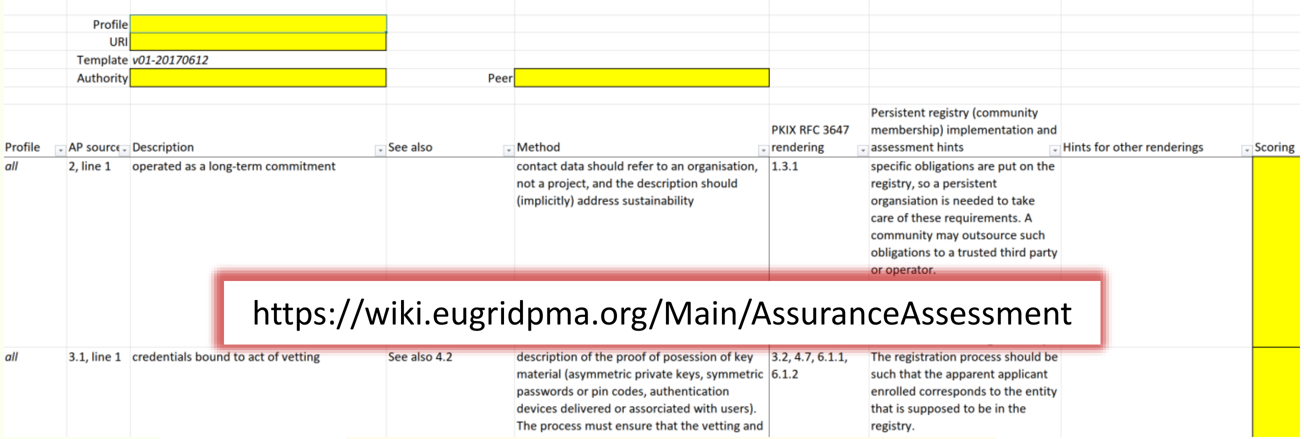
Abstract

The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.

The IGTF Levels of Authentication Assurance (LoA) generalization process aims to extract those elements from 'Authentication Profiles' the IGTF has developed that are of general value to the community. The LoAs described in this document represent the consensus on acceptable levels for

Assessment Matrix

- Mapping for PKIX/RFC3647 is trivial
- How to apply out BIRCH/CEDAR guidance to community registries?



Profile			
URI			
Template	*v01-20170612*		
Authority		Peer	

Profile	AP source	Description	See also	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints for other renderings	Scoring
all	2, line 1	operated as a long-term commitment		contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organsiation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator.		
all	3.1, line 1	credentials bound to act of vetting	See also 4.2	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or associated with users). The process must ensure that the vetting and	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry.		

https://wiki.eugridpma.org/Main/AssuranceAssessment

- Relevant for COmanage & VOMS communities, but maybe wider?

NEW TECHNOLOGIES, SAME TRUST

Changes from within and without

Diversification of technology

- PKIX works technology-wise, but new users not accustomed to it
- SAML R&E federations move quite slowly because of installed-base
- New communities and infrastructures like
  Oauth2 & OIDC because of industry support

and the end-of-service announcement for the Globus Toolkit stirred the community in some countries and regions as well

On Trust

‘the key factor the IGTF has is not PKIX itself, but the global trust fabric supporting research and e-Infrastructures’

- We should retain full PKIX support for many years to come *the Infrastructures will not move away quickly, and EGI, OSG, XSEDE, WLCG, have committed to support GSI and tools*
- Using the IGTF as a ‘research federation’ registration vehicle in eduGAIN (SAML) is likely not cost-effective – we better push for research support in eduGAIN via existing groups
- There is no OIDC federation, but a large need for OAuth in the Infrastructures – and here we can and should play a role!

OIDC Federation Task Force

The IGTF *decides* to set up a task force to push OIDC Federation next to its current trust anchor distribution. This group will

- further identify objectives
- scope the needs and requirements for Infrastructure OIDC Fed
- verify compatibility of the IGTF Assurance Profile framework for technology-agnosticity with OpenID providers
- test a OIDCFed scenario
  e.g. starting with the WLCG use case as a concrete implementation
- assess the structure and needed meta-data in the trust anchor distribution, how to address RPDNC, and how it links with dynamic client registration through '.well-known'
- liaise with other OIDC Fed efforts and Roland Hedberg

Joining OIDC Fed

- Group wiki page

  https://wiki.eugridpma.org/Main/OIDCFed

- Mailing list

  oidcfed@igtf.net

- Current members

  JimB, Jens, DavidG, DaveK, Derek, Eric Yen, Sang-Un, Scott Rea, and Roland Hedberg

FAITS DIVERS: IPV6!

IPv6 status

- New continuous v6 CRL monitor
  http://cvmfs-6.ndgf.org/ipv6/overview.php

- 43 CAs offer working v6 CRL (it’s not going up any more ☹)
  - but: also 1-2 CAs that give AAAA record but the GET fails …
  - Still many endpoints support only legacy IP
  - the ClouldFlare cache solution is trivial, so please either …
  - dl.igtf.net *can* act as v6 source-of-last-resort for RPs that need it

For more details,
see https://www.eugridpma.org/meetings/,
but meanwhile:

UPCOMING MEETINGS

Upcoming events

EUGridPMA 42, Prague January 22 – 24, 2018