I2GS 2017 v01

Building Trust for Research and Collaboration

bridging technology and policy divides

Nikhef

David Groep

I2GS 2017

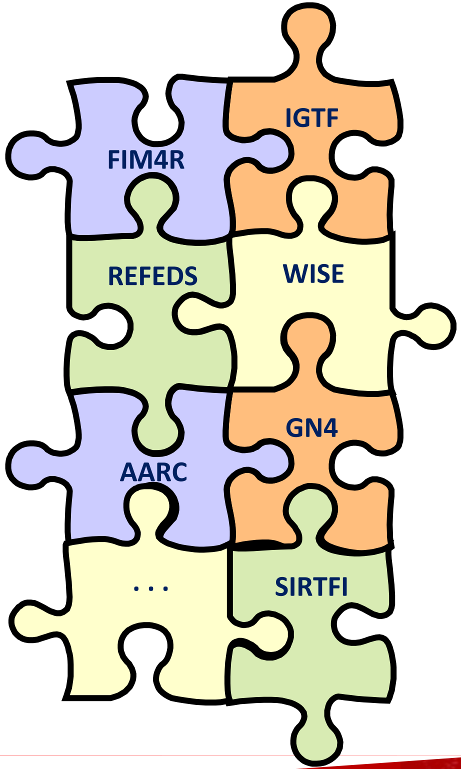
Image by Cristian Bortes, May 2011, CC-BY - https://flic.kr/p/9Uvwng

Putting the Policy Puzzle Together

- research and collaboration across *highly distributed communities with bottom-up collaboration needs*

- ongoing global efforts towards a common goal

- Interoperation with global impact



David Groep
Nikhef
Amsterdam
PDP & Grid

IGTF – *Interoperable Global Trust Federation*
supporting distributed IT infrastructures for research

- IGTF, started in 2000 as the EU DataGrid CA Coordination Group, brings together
  - e-Infrastructure resource providers, user communities and identity authorities

  to agree on

  - global, shared minimum requirements and assurance levels
  - inspired and coordinated by the needs of relying parties

- Trust is technology-agnostic
  - focus on global, coordinated identity across communities and across service providers for *cooperative services*
  - define 'best practices' for assurance levels, attribute authority operations, credential management, auditing and reviewing

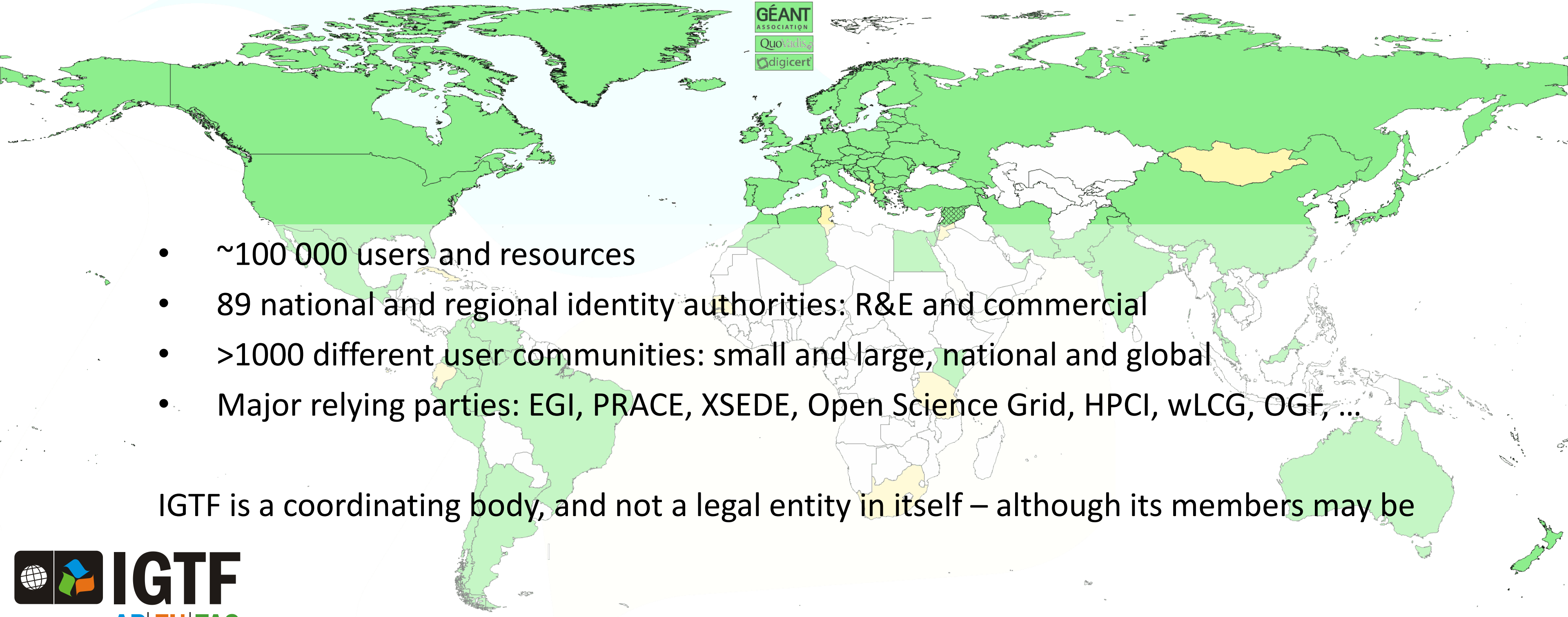
Relying Parties as a Key Stakeholder

Service providers ('relying parties') absorb almost all of the residual risk – as they host and manage resources under threat

- Sources of 'subject authority' should **align with RP interests** to be useful
- RP must have policy controls to **compose sources of authority**
- RP must be **equipped with effective controls** to mitigate risks

source: NorthWood LAN party 7 - http://www.linuxno.de/

Coverage: users and providers



- ~100 000 users and resources
- 89 national and regional identity authorities: R&E and commercial
- >1000 different user communities: small and large, national and global
- Major relying parties: EGI, PRACE, XSEDE, Open Science Grid, HPCI, wLCG, OGF, …

IGTF is a coordinating body, and not a legal entity in itself – although its members may be

IGTF
AP | EU | TAG

Premise is *end-user (researcher)* oriented **https://www.igtf.net/**

Minimum Requirements & Peer Review

- Federation imposes *minimum requirements* on identity provider participants
  - Reflect operational and security needs of resource providers
  - Differentiated LoA support
    - classic user-based subscriber services: serve all users
    - identity services leveraging federations with ID vetting
    - Identifier-Only Trust Assurance
      – *if relying party has other ways to vet its users, leveraging identifier uniqueness and incident response*
  - **Research-inspired verification process**: self-audits, peer-review, transparent open policies and processes
  - ‘meet or exceed’ required minimum standards

‘BIRCH’ , ‘Capuccino’

‘DOGWOOD’ , ‘Baseline’

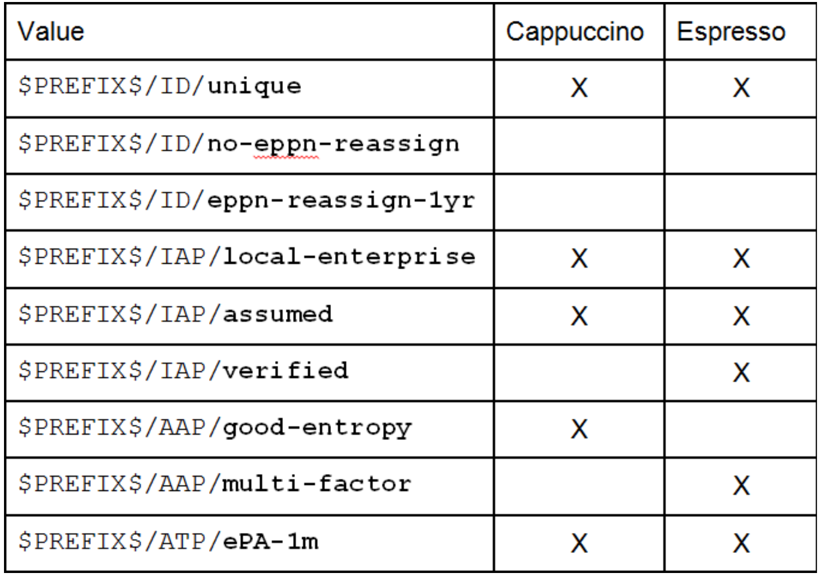
Differentiated Assurance Profile – in eduGAIN, REFEDS, and beyond

Specific definitive guidance to IdPs and federations

- **Uniqueness** at least ePUID or ePTID/NameID extra: ePPN non-reassigned or 1-year-hiatus
- **ID proofing**: 'local enterprise', 'assumed' (Kantara LoA2, IGTF BIRCH, eIDAS low), or 'verified (LoA3, eIDAS substantial)
- **Authenticator**: follow REFEDS MFA 'good-entropy' or 'multi-factor'
- **Freshness**: ePA/ePSA reflect departure within 30 days

All: organisational-level authority, also used locally for 'real work', good security practices

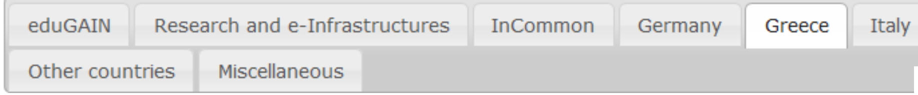
Logical grouping and profiles for the Infrastructures



Value	Cappuccino	Espresso
`$PREFIX$/ID/unique`	X	X
`$PREFIX$/ID/no-eppn-reassign`		
`$PREFIX$/ID/eppn-reassign-1yr`		
`$PREFIX$/IAP/local-enterprise`	X	X
`$PREFIX$/IAP/assumed`	X	X
`$PREFIX$/IAP/verified`		X
`$PREFIX$/AAP/good-entropy`	X	
`$PREFIX$/AAP/multi-factor`		X
`$PREFIX$/ATP/ePA-1m`	X	X

… and simplicity for all

https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework



Fed Security Operational Procedures

'A Very Timely Activity'

Incident response capabilities at IdPs and SPs: Sirtfi v1 brings these to light

Beyond v1: establish proper channels, expectations, and the operational capability

Establish 'homogeneous' Incident Response Procedure

- with central operational capability
- and information sharing

IAM Online Europe

IAM Online Europe webinars are broug

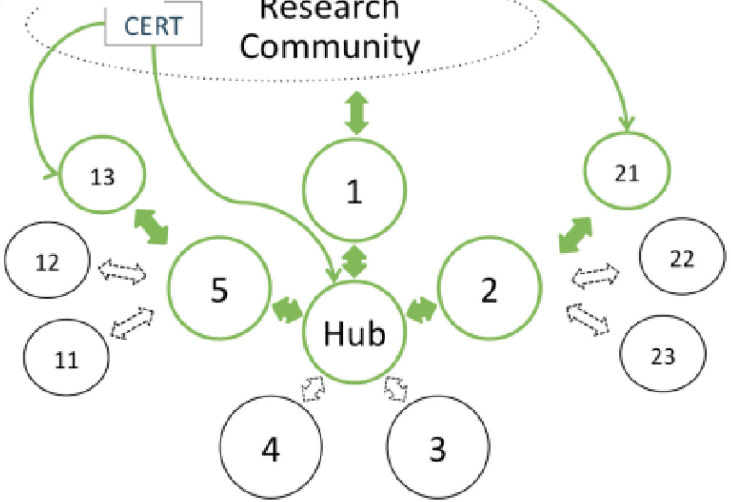
iamonlineEU 001 Sirtfi

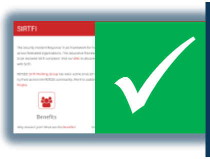
IamOnline

38 views • 4 days ago

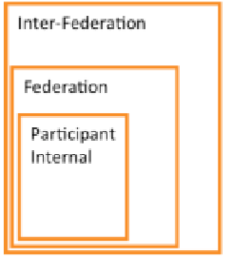
31-12-2016

Deliverable DNA3.2: DNA3.2 - Security Incident Response Procedure

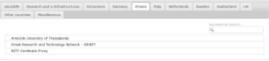




Mar 17th	**137 entities (+23) that support Sirtfi**
Apr 23rd	**160 entities (+23)**



https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf



Trust is technology agnostic

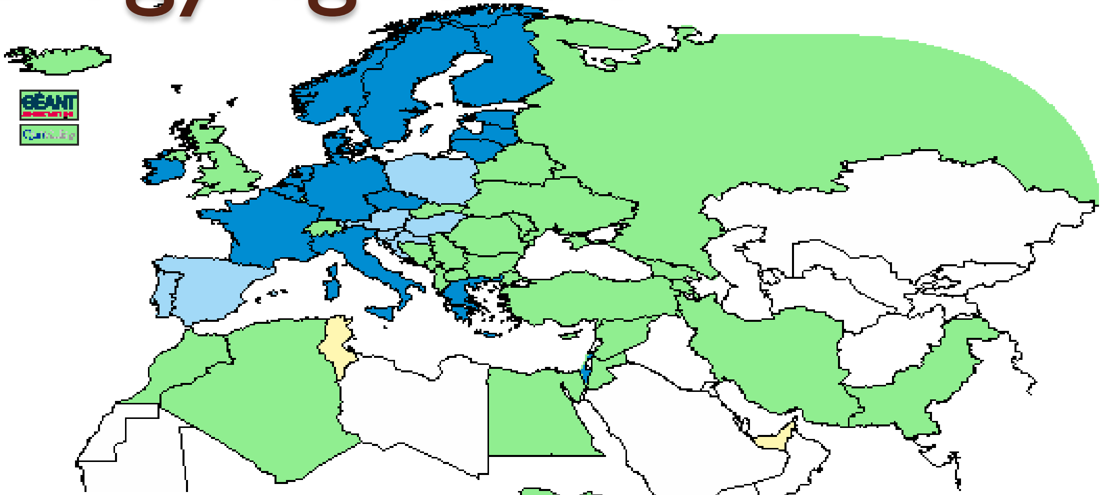
SAML to PKIX

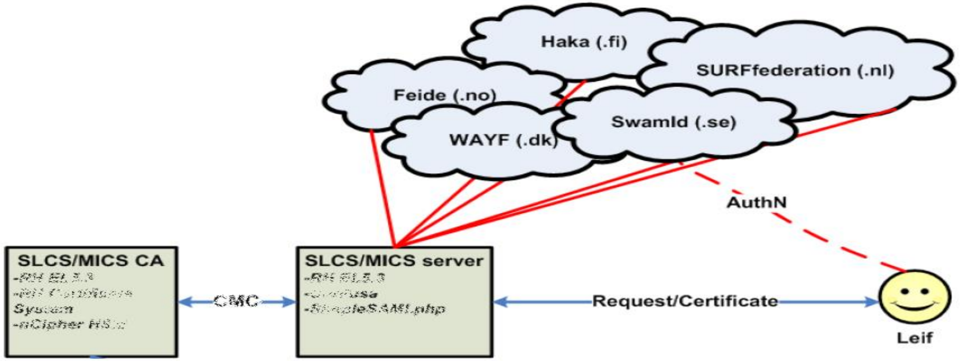
GEANT TCS

DFN AAI SLCS

CILogon

RCauth.eu





PKIX to SAML

IGTF Certificate Proxy @ GRNET

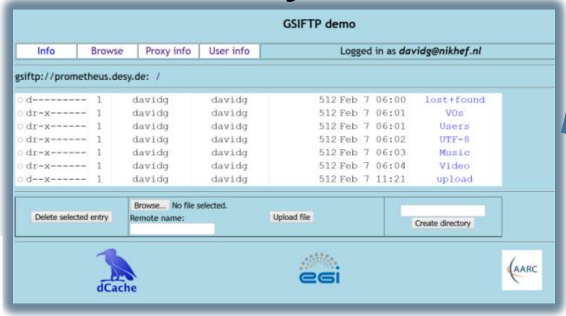
SLCS/MICS graphic: Jan Meijer, UNINETT

Seamless (eduGAIN) Access via the CILogon-like TTS Pilot: aims

- **Ability to serve a large pan-European user base without national restrictions**
  - without having to rely on specific national participation exclusively for this service
  - serving the needs of cross-national user communities that have a large but sparsely distributed user base
- **Use existing resources and e-Infrastructure services**
  - without the needs for security model changes at the resource centre or national level
- **Allow integration of this system in science gateways and portals with minimal effort**
  - only light-weight industry-standard protocols, limit security expertise (and exposure)
- **Permit the use of the *VOMS* community membership service**
  - attributes for group and role management in attribute certificates
  - also for portals and science gateways access the e-Infrastructure
- **Concentrate service elements that require significant operational expertise**
  - not burden research communities with the need to care for security-sensitive service components
  - keep a secure credential management model
  - coordinate compliance and accreditation – and help meet EU privacy stuff in just one place to ease adoption
- *Optional elements: ability to obtain CLI tokens (via web flow or ssh); implicit AuthZ*

Flow for RCauth-like scenarios

Community Science Portal

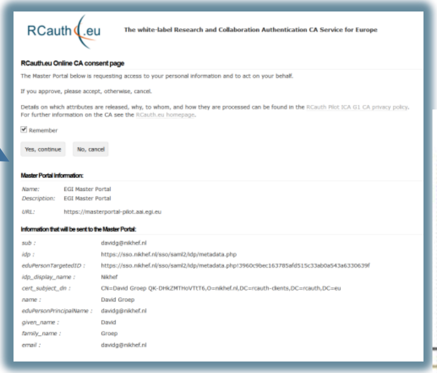


GSIFTP demo

Logged in as *davidg@nikhef.nl*

gsiftp://prometheus.desy.de: /

```
d---------  1  davidg  davidg  512 Feb 7 06:00  lost+found
dr-x------  1  davidg  davidg  512 Feb 7 06:01  VOs
dr-x------  1  davidg  davidg  512 Feb 7 06:01  Users
dr-x------  1  davidg  davidg  512 Feb 7 06:02  UTF-8
dr-x------  1  davidg  davidg  512 Feb 7 06:03  Music
dr-x------  1  davidg  davidg  512 Feb 7 06:04  Video
d--x------  1  davidg  davidg  512 Feb 7 11:21  upload
```



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 to act on your behalf.

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are processed can be found in the RCauth Pilot ICA G1 CA privacy policy. For further information on the CA see the RCauth.eu homepage.

☑ Remember

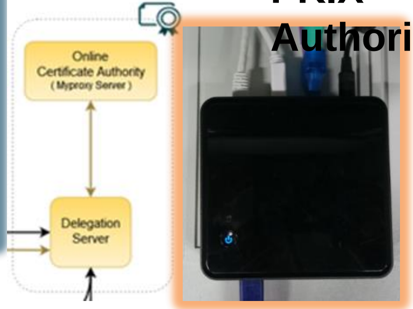
Master Portal information:

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

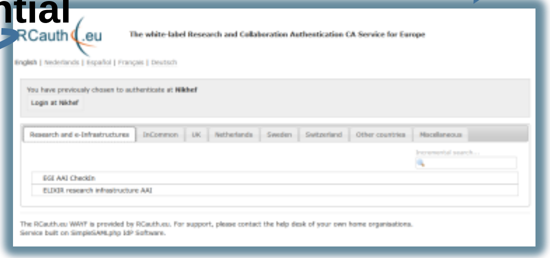
Information that will be sent to the Master Portal:

sub :	davidg@nikhef.nl
idp :	https://sso.nikhef.nl/sso/saml2/idp/metadata.php
eduPersonTargetedID :	https://sso.nikhef.nl/sso/saml2/idp/metadata.php!3960c9bec163785afd515c33ab0a543a6330639f
idp_display_name :	Nikhef
cert_subject_dn :	CN=David Groep QK-DHkZMTHoVTtT6,O=nikhef.nl,DC=rcauth-clients,DC=rcauth,DC=eu
name :	David Groep
eduPersonPrincipalName :	davidg@nikhef.nl
given_name :	David
family_name :	Groep
email :	davidg@nikhef.nl

Accredited PKIX Authority



Infrastructure Master Portal Credential Store

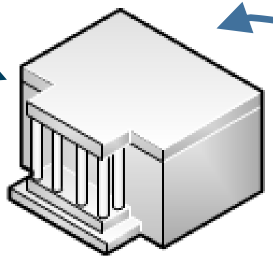


RCauth.eu The white-label Research and Collaboration Authentication CA Service for Europe

You have previously chosen to authenticate at **Nikhef**

- EGI AAI CheckIn
- ELIXIR research infrastructure AAI

The RCauth.eu WAYF is provided by RCauth.eu. For support, please contact the help desk of your own home organisations.
Service built on SimpleSAMLphp IdP Software.



REFEDS R&S
Sirtfi Trust

Policy Filtering WAYF / eduGAIN

User Home Org
or Infrastructure IdP

Built on CILogon and MyProxy!
www.cilogon.org

CILogon

see also https://rcdemo.nikhef.

The Reverse: the IGTF-to-eduGAIN bridge

“the ultimate assured-identity IdP of last resort”

- authenticate with any IGTF accredited client cert
- known to the (SAML2int, R&E) eduGAIN community via GRnet
- with assurance information in ePAss (and 2FA set in ACCR)
- asserts REFEDS R&S and Sirtfi (based on IGTF qualification)

will appear as https://edugain-proxy.igtf.net/

R&S + Sirtfi tags should enable many research SPs to trust you

work by Ioannis Kakavas (GRNET) and Christos Kanellopoulos –
see github for implementation of SimpleSAMLphp module

Thank you

Any Questions?

davidg@nikhef.nl

AARC

http://aarc-project.eu/

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).