Evolving the EGI trust fabric using distributed responsibility

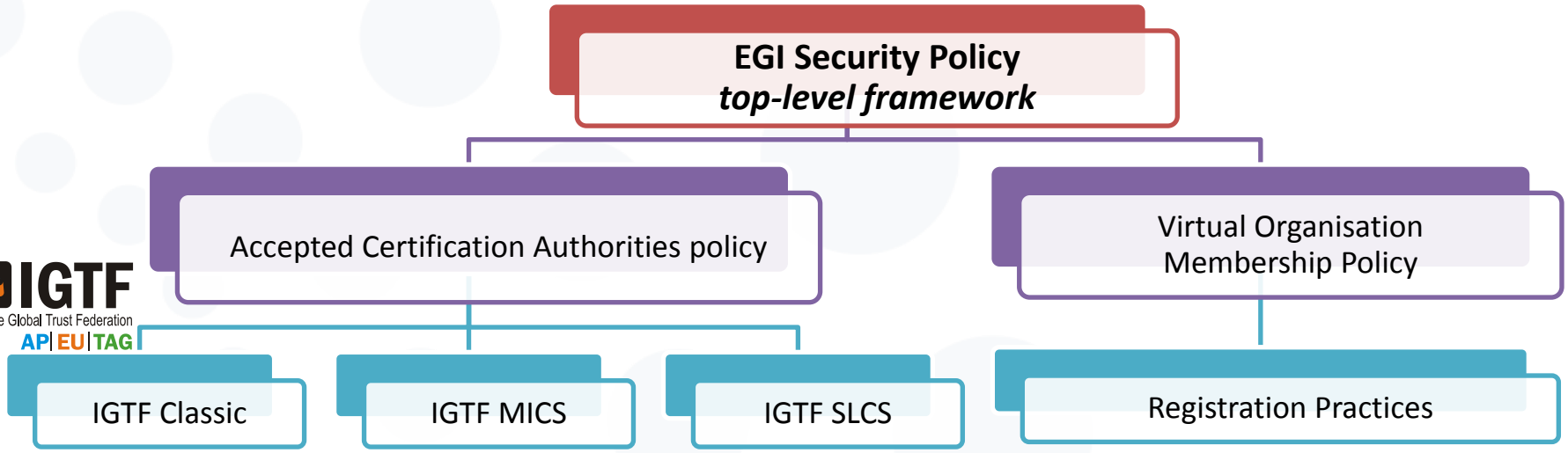
David Groep

EGI IGTF Liaison

orcid.org/0000-0003-1026-6606

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

EGI trust policy space



EGI (based on earlier joint JSPG work) puts user traceability on the IGTF providers

- accepting a set of IGTF assurance profiles: MICS, SLCS, Classic
- with peer-reviewed self-audits and transparency

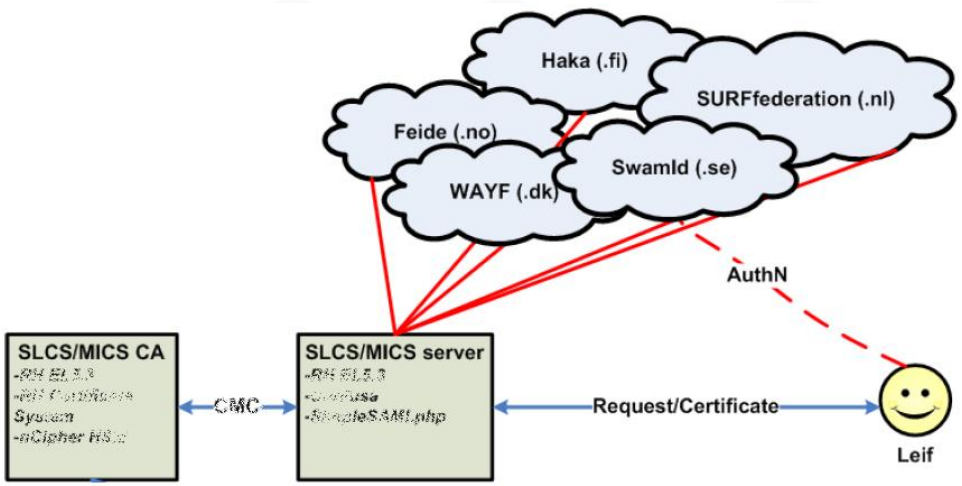
VO registration process is fairly light-weight: no audits, no documented procedures

- but a few VOs are different and do have such processes (mainly wLCG)

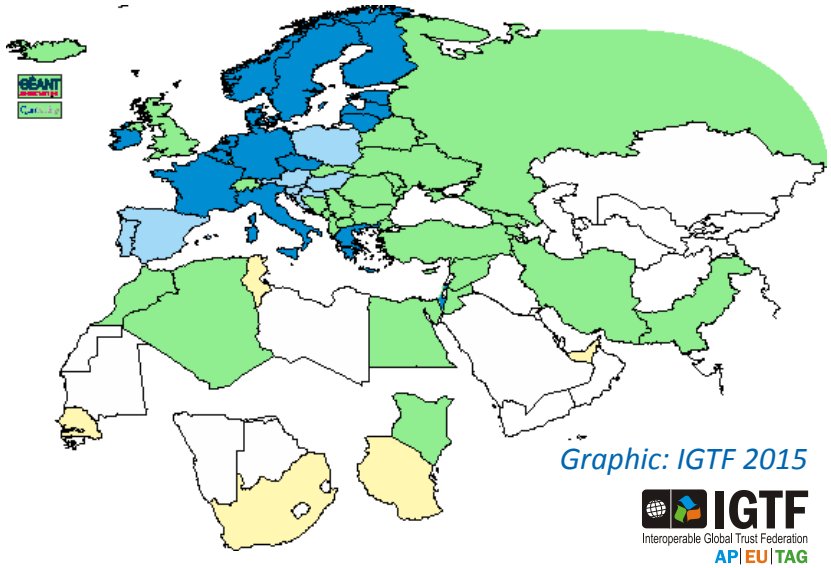
Federated Authentication

Performing reasonable identity vetting of users and providing traceability is non-trivial

- Authorities set of a distributed Registration Authority network
- Or leverage an existing one, based on 'FedAuth' with quality assurance *e.g. through services like DFN-AAI and Trusted Certificate Service TCS*



Graphic from: Jan Meijer, UNINETT



Graphic: IGTF 2015

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

‘Federated Authentication’ for a myriad of services

eduGAIN

okeanos GLOBAL

WELCOME TO OKEANOS GLOBAL!

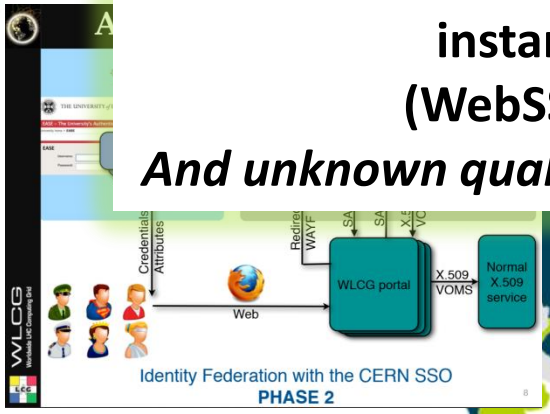
This is GRNET's cloud service, for the GÉANT Research and Academic Community. With ~okeanos global you are one click away from your own Virtual Machines, Networks and Storage.

STATISTICS

Spawned VMs	Active VMs	Spawned Networks
32,426	366	11,254

But SSO single password & federation also means:
instant abuse in case it gets compromised
(WebSSO, imap, smtp, ssh, eduroam, TCS, …)
And unknown qualities of identity in each federation and each IdP ☹

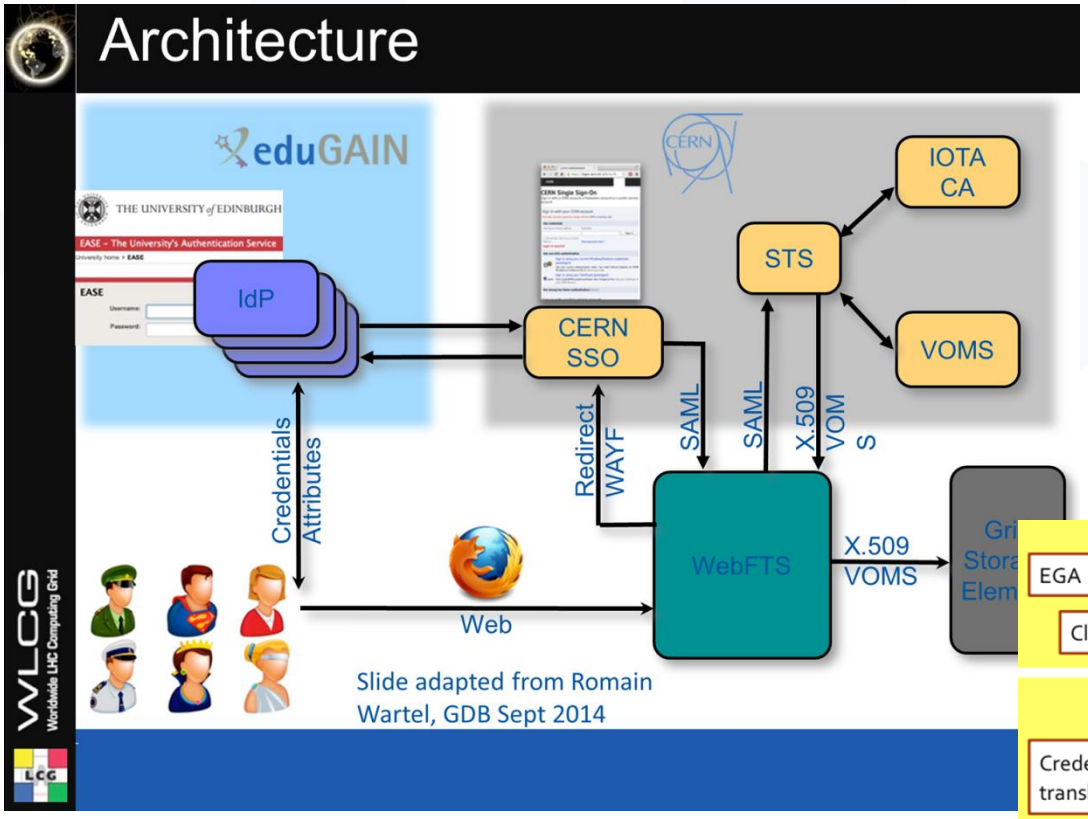
4 ALL’



wLCG FIM4R pilot

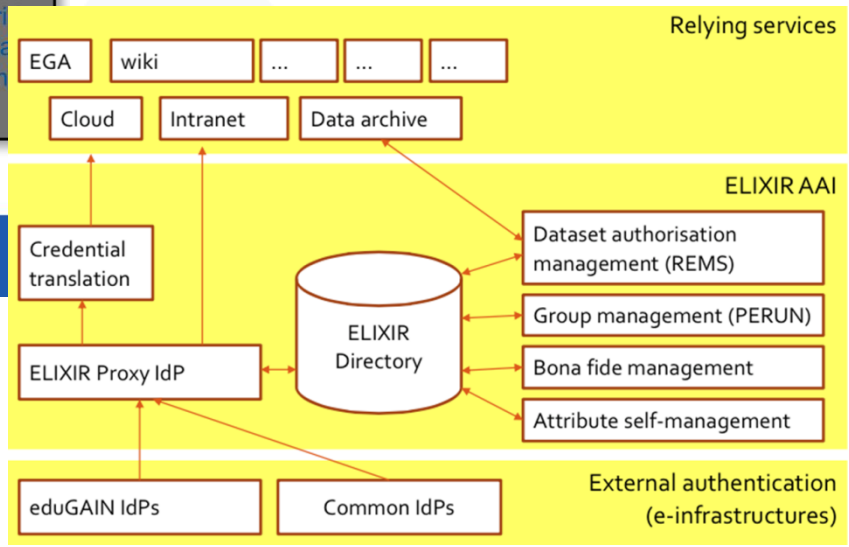
background: eduGAIN connected federations as of November 2014 – Brooke Schofield, TERENA

Federated use of the eInfra



WebFTS 'FIM4R' in wLCG
Romain Wartel

ELIXIR reference architecture
Mikael Linden et al.



Why the move to FedAuth

Cross-national federated access progressed tremendously

- eduGAIN: more federations, with technical interop across countries
- Increased awareness of research & scholarship use cases
- 'the will to make it happen': demonstrated by SirTFi, AARC, VOPaaS, …

A great promise for easier collaboration

- Move to authenticators 'closer' to the user understanding – mainly home organization credentials
- Ability to 'hide' end-user PKIX technology – and offer simpler authentication for web-based services through 'OpenID Connect' and 'SAML'

And there are bridges – since for non-Web, command-line and brokerage 'SAML2Int WebSSO' does not work

- STS, CILogon, TCS, SSH-to-MyProxy tokens, Moonshot, …

Issues hindering the adoption of FedAuth

Although many production federations are pretty good, and quite a few IdPs have good processes …

- public documentation, self-assessment and peer-review are missing
- it's **not consistent** across IdPs

and processes are not designed for collaboration use cases

- re-use of identifiers is common (also an issue for social IdPs)
- the identity providers provide no identity … or it's non-consistent
- identifiers generated are specific to each SP

and may not provide traceability needed for valuable resources

- some allow users to change their own data (including e.g. their email address and all contact data), or do not collaborate in case of issues

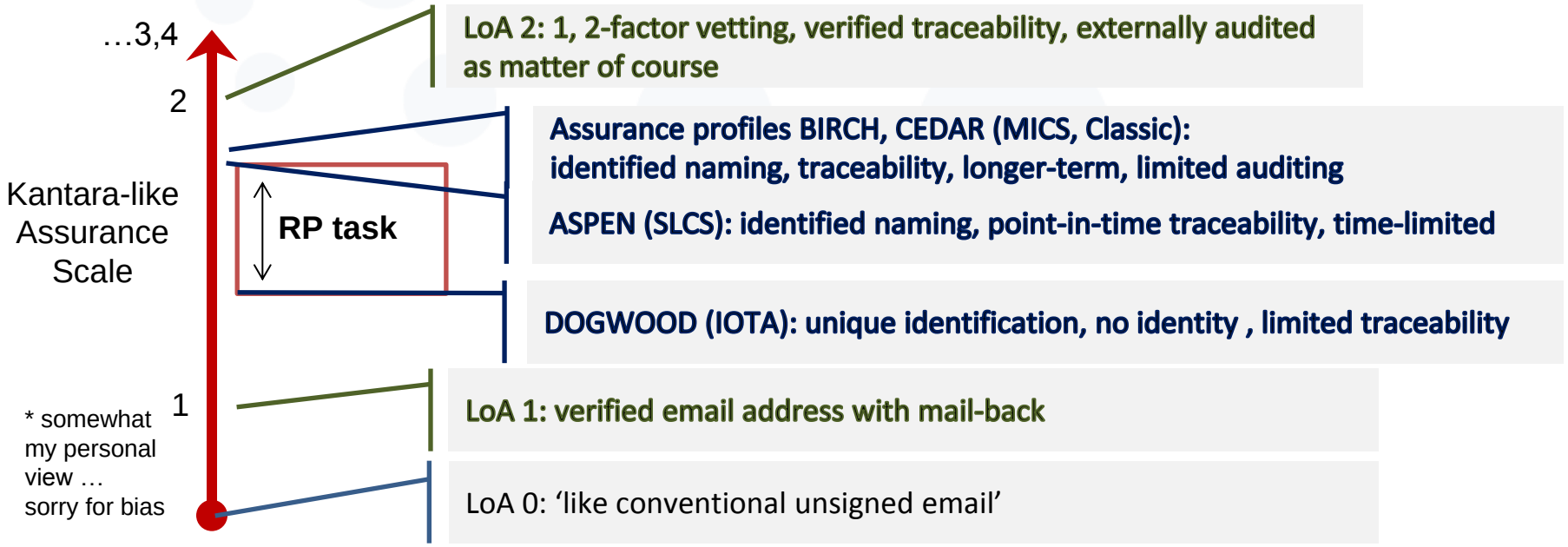
Assurance profiles as charted by the IGTF

So many production federations and IdPs are pretty good, but …

- they are all different, and the lowest common denominator is quite low

… so IGTF for 'conventional' assurances requires **additional per-user controls**

… and the ('uniqueified') AP 'DOGWOOD' (IOTA) leaves an assurance gap



Redistributing responsibilities with IOTA

Who can absorb the responsibilities, if not the identity providers?

Requirements:

- End-to-end traceability must remain the same
- Changing or documenting federation and IdP processes is a 'lengthy' process – but adding some requirements does work (e.g. SiRTFi on incident response)

… so who can absorb the responsibility?

- The resource centres – and go back to 1995 with per-site vetting ☹
- The Infrastructure or funding agencies, through a rigorous registration process – PRACE 'home sites', or XSEDE registration + NSF granting
- EGI UMP – that's what's happening partially in the LToS service
- Or the communities?

Moving the bar towards differentiated assurance

http://igtf.net/ap/iota *(part of http://igtf.net/ap/loa)*

- IOTA AP assurance level 'DOGWOOD' *is* different, and remainder of the elements ***must*** be taken up by somebody else – the VO or the sites
- Only thing you get is an opaque ID
- Consider questions about
  - Real names and pseudonyms
  - Enrolling users in a community
  - Keeping audit records
  - Auditability and tracing
  - Incident response

Identity elements

- identifier management
- re-binding and revocation
- binding to entities
- traceability of entities
- emergency communications

- regular communications
- 'rich' attribute assertions
- correlating identifiers
- access control

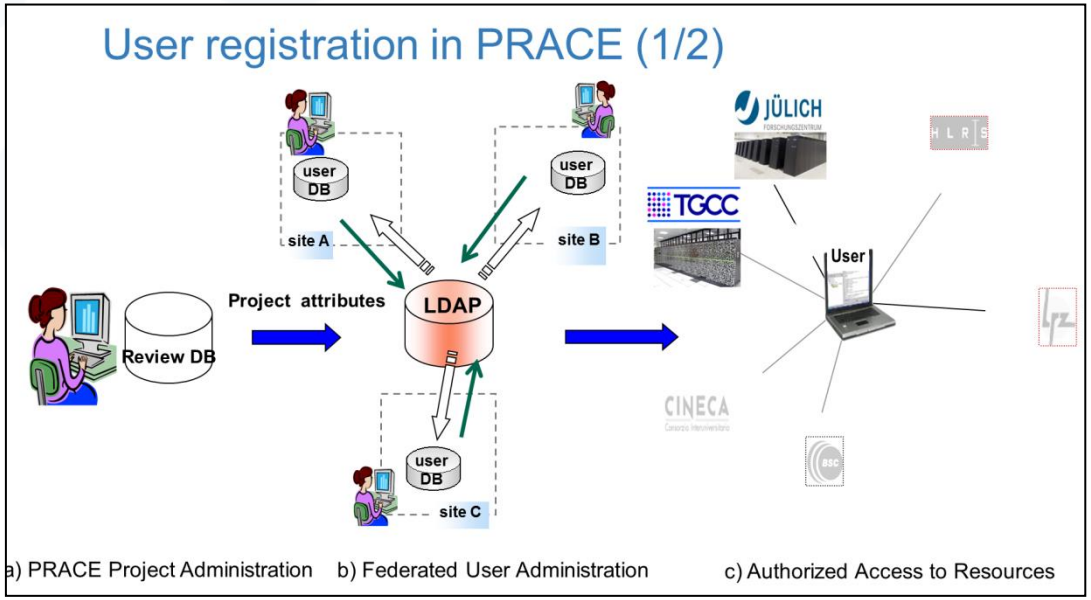
Specific Delegated Responsibilities

Need for proper traceability does not go away, so …

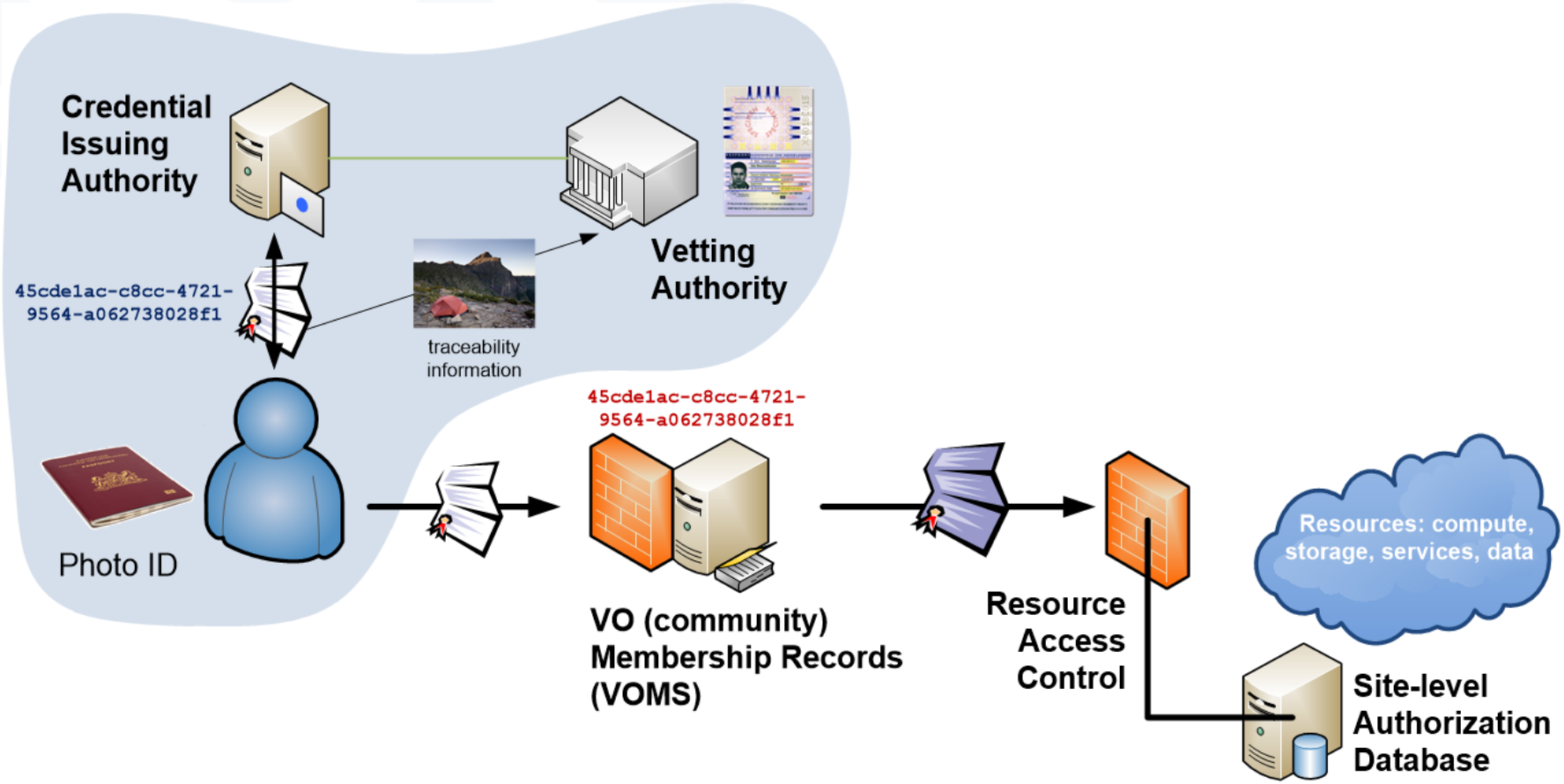
- who holds that information need not only be a traditional CA
- but can be another entity with similarly **rigorous processes**

Some communities have an existing registration system that is very robust

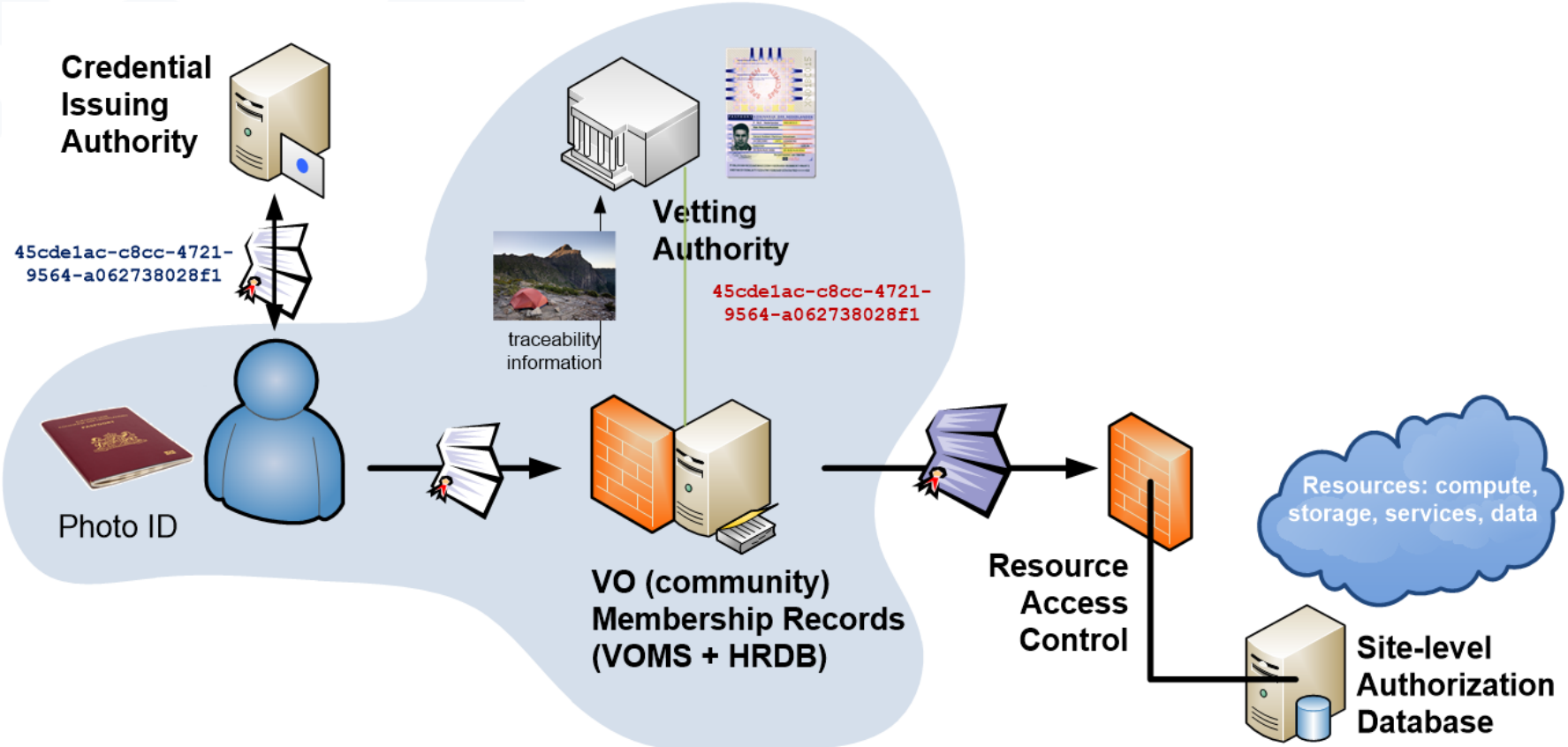
- PRACE – in-person links at the home sites
- XSEDE – NSF grant approval process
- wLCG –CERN Users Office and HR Database



Distributed Responsibilities I: Trusted Third Party



Distributed Responsibilities II: Collaborative Assurance & Traceability



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

*) https://documents.egi.eu/document/79

Software support for DiffLoA

What is needed it for the infrastructures (resource centres) to differentiate between 'light-weight VOs' and 'heavily-managed VOs'

- Preferably on a per-VO basis
- Allowing IdPs with a lower assurance profile to be used for heavily-managed VOs'
- Whilst ensuring light-weight VOs can continue to enjoy airiness since they're combined with higher-assurance IdPs (CAs)

```
# Example VO-CA-AP-file, please adapt according to requirements

# First the VOMS entries
/pvier          "/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth",\
                file:TERENAeSciencePersonalCA.info, file:TERENAeSciencePersonalCA-2.info, \
                file:TERENAeSciencePersonalCA-3.info
/dteam          file:policy-igtf-mics.info,file:policy-igtf-classic.info
```

Software capabilities today

'For site-controlled redistribution to work, **all** software in the infrastructure faces with redistributed responsibility **must** support it'

Key components

- Argus Authorization System
- Site access control suite for C 'LCMAPS'
- … embedded ACL systems in (storage) software

For some it's there (like LCMAPS on next slide), for others its 'fairly trivial' to implement (Argus), but all needs to be deployed and used as well

- way to feed CA policy information to Argus decision engine is needed
  i.e., a "PIP" in AUthZ lingo speak, or it will not scale, but this is planned
- For service-specific authorization systems an inventory is needed

LCMAPS example implementation

```
# Example VO-CA-AP-file, please adapt according to requirements

# First the VOMS entries
/pvier      "/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth",\
            file:TERENAeSciencePersonalCA.info, \
            file:TERENAeSciencePersonalCA-3.info
/dteam      file:policy-igtf-mics.info,file:policy-igtf-classic.info
```

- For each VO (FQAN), list the set of acceptable CAs and (IGTF) Assurance Profiles
- Relying parties can easily add their own bundles (in info files)
- Under control of the resource centres – who have to take the risks

For Argus

- Read “CA” and “Profile” information in a Policy Information Point
- The decision in the Argus policy is then a simple “AND” of VO+CA/AP

A Generic (CERN or EGI) IOTA CA

But this software is not there quite yet

- Needs at least Argus (and a PIP)
- Deployment
- Ubiquitous adoption

Meanwhile, we do want to experiment with FedAuth in production

- Solution: implement the VO requirements in the IOTA CA, making it a special IOTA CA scoped to VOs that do their own tracing
- Accept that special CA in the infra with specific policy controls
- Which wLCG in this case can safely do
  - because it satisfies the requirements
  - and the policy (also EGI's) already allows for exceptions
  - And it's deployed only as needed – so now only for wLCG

*'Twee geloven op één kussen, daar slaapt de duivel tussen'**

** old Dutch saying: two religions sleeping on one cushion? The Devil sleeps in between!*

Can you combine two policies within the same infrastructure?

- Can been done if new policy does not negatively affect the other one
- Which in this case is OK, since the specific new CERN IOTA CA
  - In itself implements all the policy requirements of a traditional CA by insisting on LHC membership
  - the same requirement that already governs the Classic CERN CA

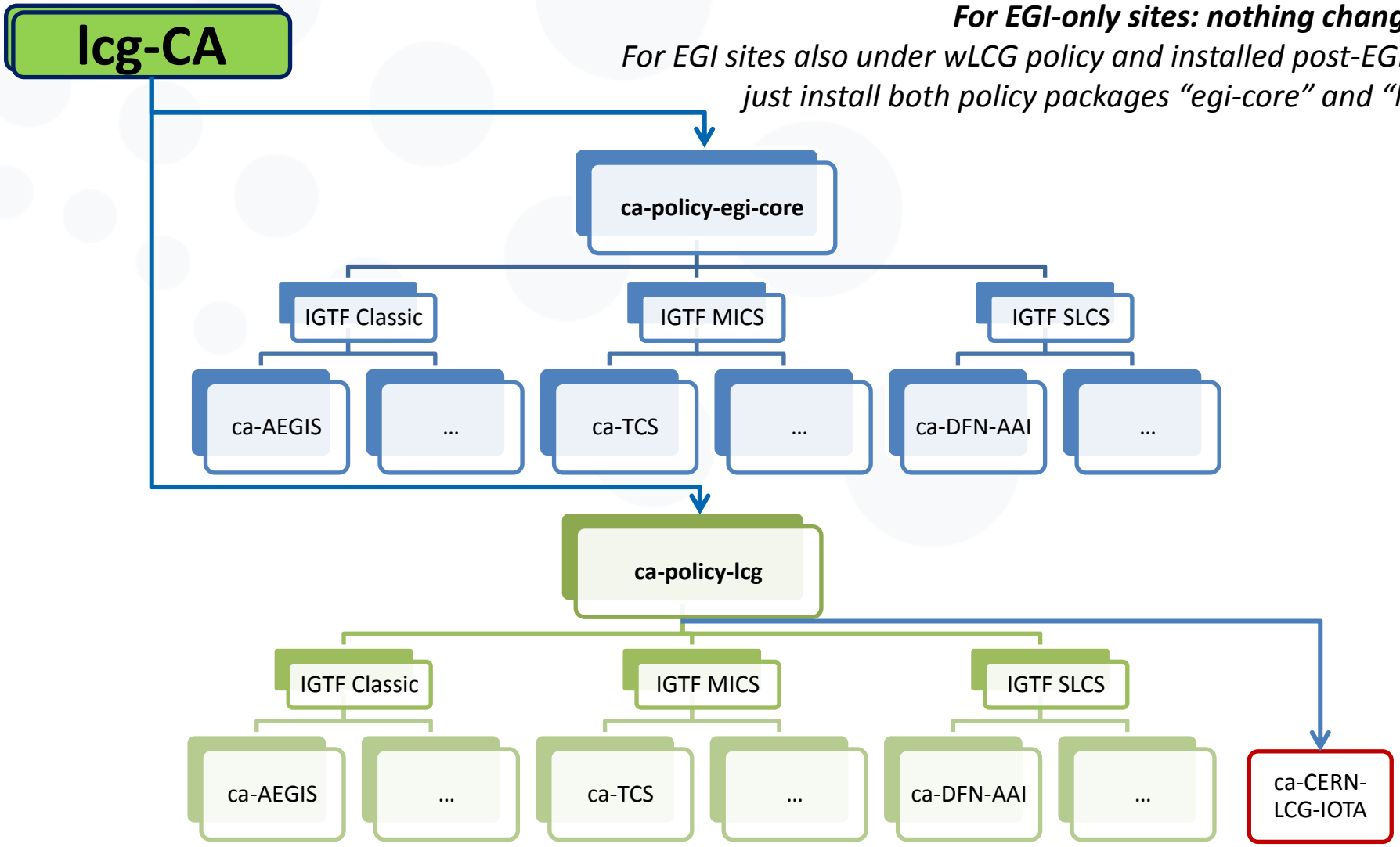
- But note that is **does not generally hold** for arbitrary IOTA CAs
- Have to wait for "VO+CA-authZ" before adding e.g. InCommon Basic

- Technically it is a relatively easy change

Dependencies in policy installation

For EGI-only sites: nothing changes!

For EGI sites also under wLCG policy and installed post-EGEE: just install both policy packages "egi-core" and "lcg"



Changes to the trust fabric

- EGI sites continue installing the egi-core
  whilst preparing for a future of differentiated assurance
- wLCG sites (also the EGI ones) also install the wlcg policy
- Net result is that the EGI+wLCG sites add one CA:
  the special, circumscribed, CERN LHC IOTA CA
- This does not compromise the integrity of the trust fabric at any site, since the VO (actually CERN) takes care of traceability through additional policy constraints

"WLCG-CERN-IOTA-statement-MB-20151028"

http://www.nikhef.nl/grid/tmp/WLCG-CERN-IOTA-statement-MB-20151028.pdf

Document on the Agenda Page

- Read it: it contains **specific safeguards** that are essential
- This **does *not*** open a door to arbitrary IOTA CAs: this cannot be done since we want to support loose collaborations – until we get VO+CA decision support in all middleware
  - foreseen in Argus&there in LCMAPS, needs bit more development
  - should also be deployed and honoured at all EGI sites
- But **does** open the way to innovative use of FedAuth and many new use cases – including support for federated research and scholarship!

- **For EGI-only sites: nothing changes** … yet
- For EGI+wLCG sites: install the "ca-policy-lcg" package in addition to "ca-policy-egi-core" when so requested
- **Both packages** are contained in **both** yum/apt repositories
  - so it does not matter whether you use the EGI or LCG repository

Thank you for your attention.

Questions?

… and join the AARC session on Thursday!

www.egi.eu