IGTF
Interoperable Global Trust Federation
AP | EU | TAG

OIDC Federation for Infrastructures

leveraging the IGTF global infrastructure trust framework with OIDC technology

David Groep

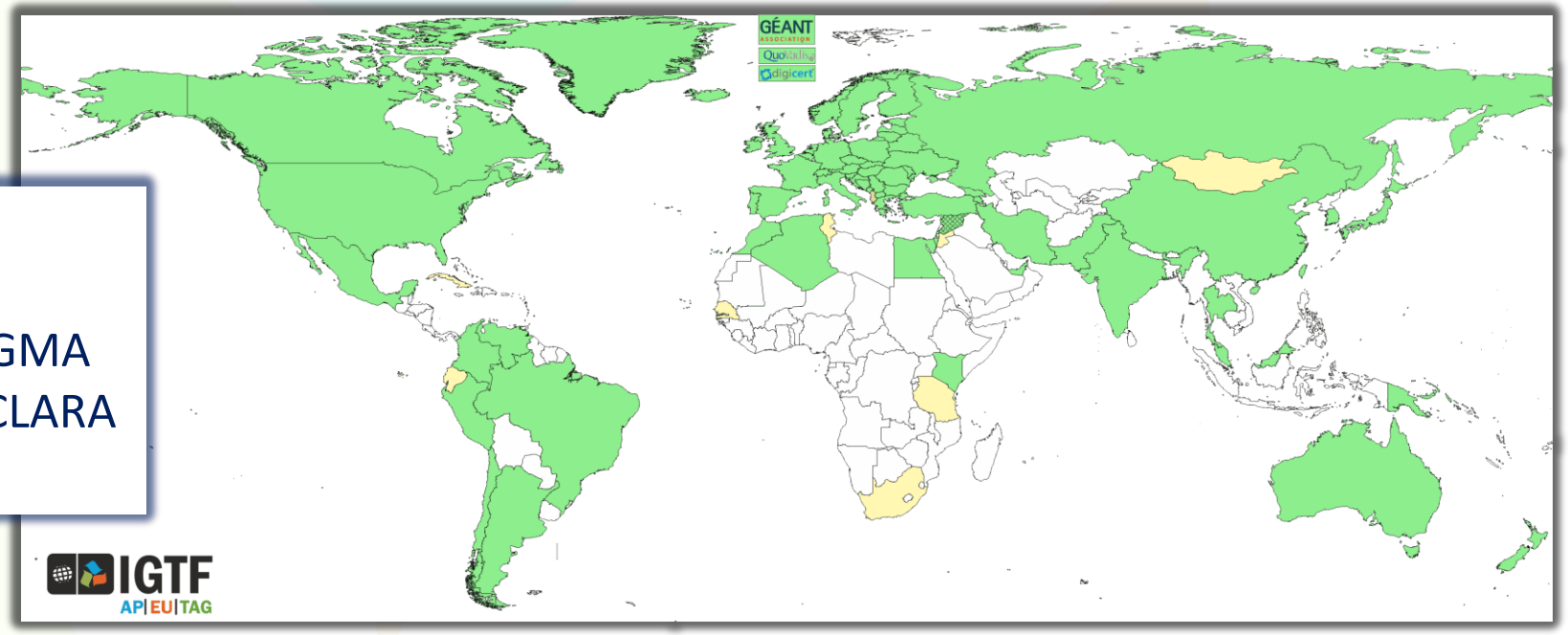
Nikhef

co-supported by the Dutch National e-Infrastructure coordinated by SURF, by EOSC-HUB, and by AARC

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"

EGI	OSG
PRACE	HPCI
GEANT	PRAGMA
WLCG	RedCLARA
XSEDE	. . .



OIDC Fed use cases for research and e-Infrastructures

- EOSC-HUB registration of clients
  goal for EGI and EUDAT is a scalable and *trusted* form of OIDC usage.
  Today < *O*(50) clients; next year maybe *O*(100-1000)?
  cloud-based services (containers, microservices) could push that to millions
- CILogon (and XSEDE) use cases see need for a set of policies and practices that support a 'trust anchor distribution'-like service targeting OIDC OPs and RPs and where RPs that are ‘in the community’ can be identified as such
- ELIXIR (and the Life Sciences) AAI expect growth in # OIDC RPs as AAI extends beyond just ELIXIR and into other biomedical RIs – potentially dynamically created

All of these need a policy framework, on both the (infrastructure) OPs and on the RPs

This is the community that traditionally also relied on the IGTF trust anchor distribution

https://www.eugridpma.org/meetings/2018-01/summary-eugridpma-2018-01-prague.txt

Building conections: Client ID and Client Secret

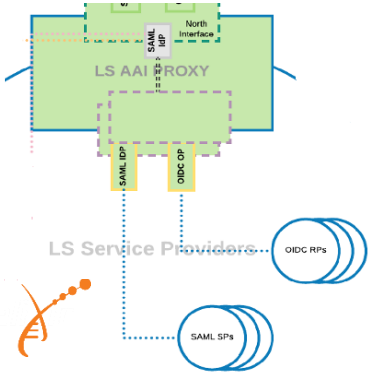
XSEDE
Extreme Science and Engineering Discovery Environment
CILogon

- Planning for Globus migration from X.509 to Globus Auth
- Maintain credential assurance for XSEDE users and systems
- Continue to benefit from IGTF trust community

RCauth.eu

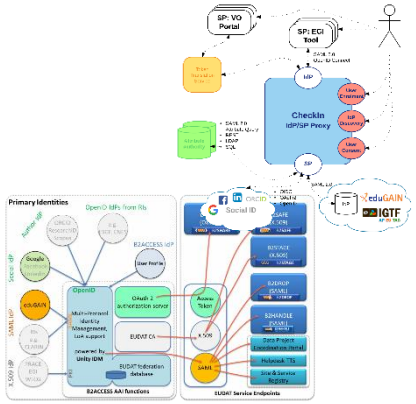
- WaTTS service
- EGI MasterPortal
- MinE Credential Hosting
- *… B2ACCESS, …*

- ELIXIR and LSAAI services
- e-Infra connections



Master Portal

- SSH Proxy CLI
- Prometheus WebDAV portal
- mkProxy service
- …



- EGI CheckIn
- B2ACCESS
- EOSC-HUB AAI

Assurance and trust frameworks

Identity Assurance Profiles for R/E-Infra risk scenarios (https://igtf.net/ap/loa/**)**

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

Policy framework for Relying Parties ('SP-IdPs-Proxies')

- Snctfi - Community Trust Framework in Federated Infras
  https://igtf.net/snctfi

How can we help support RI and e-Infrastructure use cases?

- technology bridges: TCS, RCauth.eu, IGTF-eduGAIN bridge, …
- behind the Infrastructure Proxies for research & collaboration, OIDC gains prominence

thanks to Davide Vaghetti (GARR) whose REFEDS Linz slide content I re-used

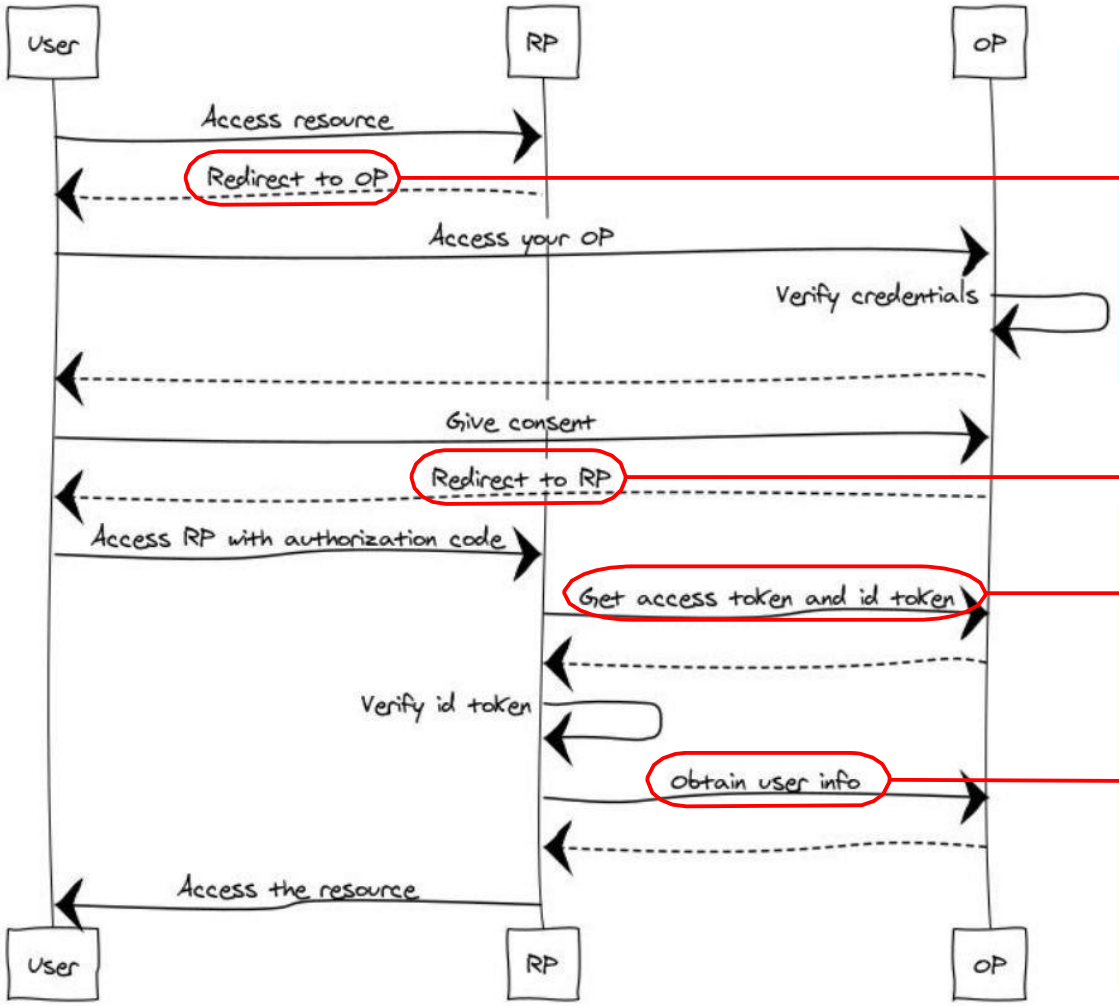
OIDC MECHANICS

OIDC Actors

- The **User** who wants to access a protected resource, either by himself or through an application.
- The **Relying Party** (often called the Client) is the entity that will request and use an access token.
- The **OIDC Provider** (OP) is the entity that will release the access token.

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OIDC: OP and RP needs to know about each other



RP redirect the user to the OP's **authorization_endpoint**

OP redirect the user to the RP's **redirect_uri**

RP exchange the code for an access_token at the **token_endpoint** (and authenticate…)

RP requests user claims at the OP's **userinfo_endpoint**

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OpenID Connect – Discovery and Dynamic Client Registration

http://openid.net/specs/openid-connect-discovery-1_0.html

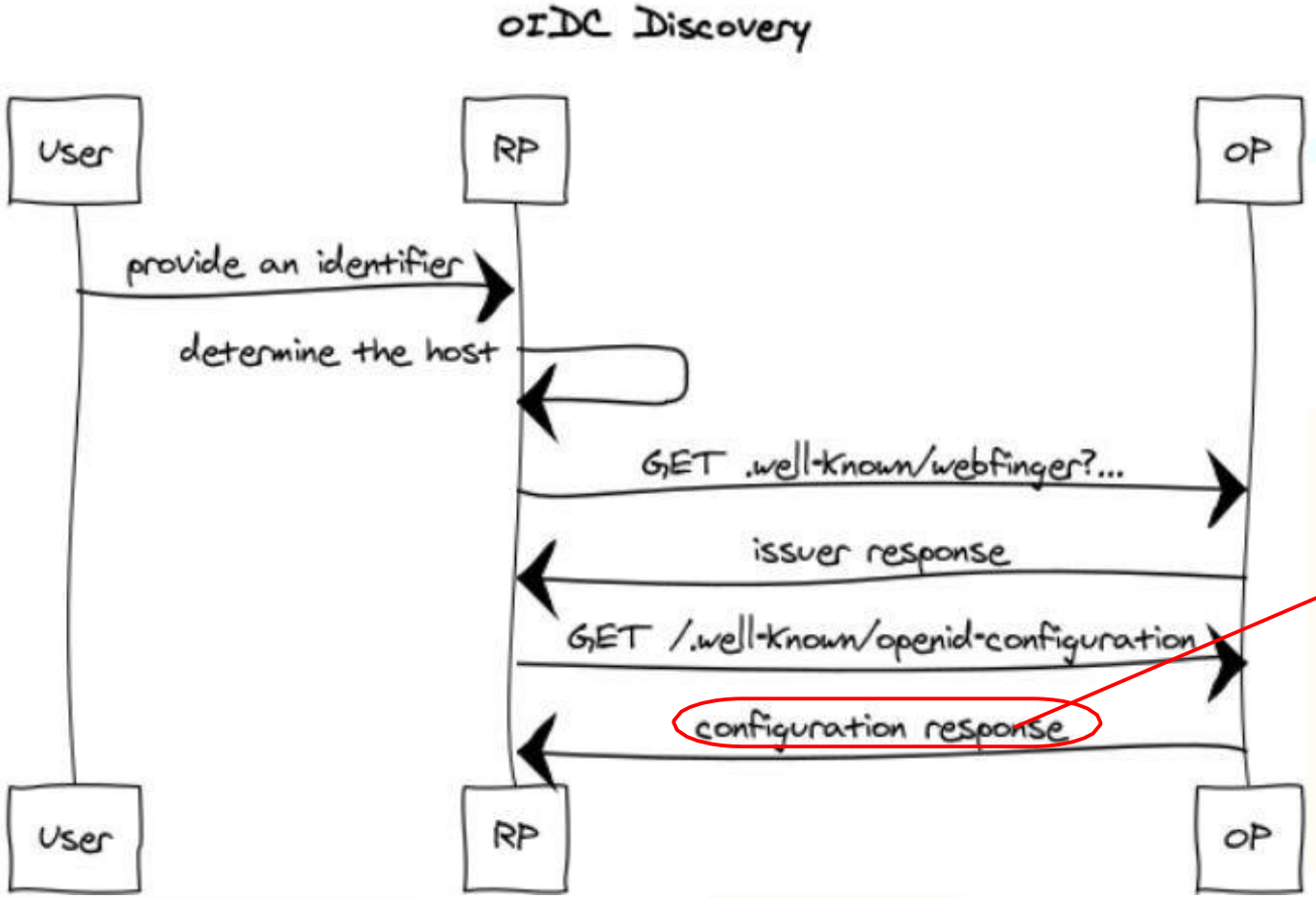
a mechanism for an OpenID Connect Relying Party to discover the End-User's OpenID Provider and obtain information needed to interact with it, including its OAuth 2.0 endpoint locations

http://openid.net/specs/openid-connect-registration-1_0.html

defines how an OpenID Connect Relying Party can dynamically register with the End-User's OpenID Provider, providing information about itself to the OpenID Provider, and obtaining information needed to use it, including the OAuth 2.0 Client ID for this Relying Party

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OpenID Connect Discovery 1.0

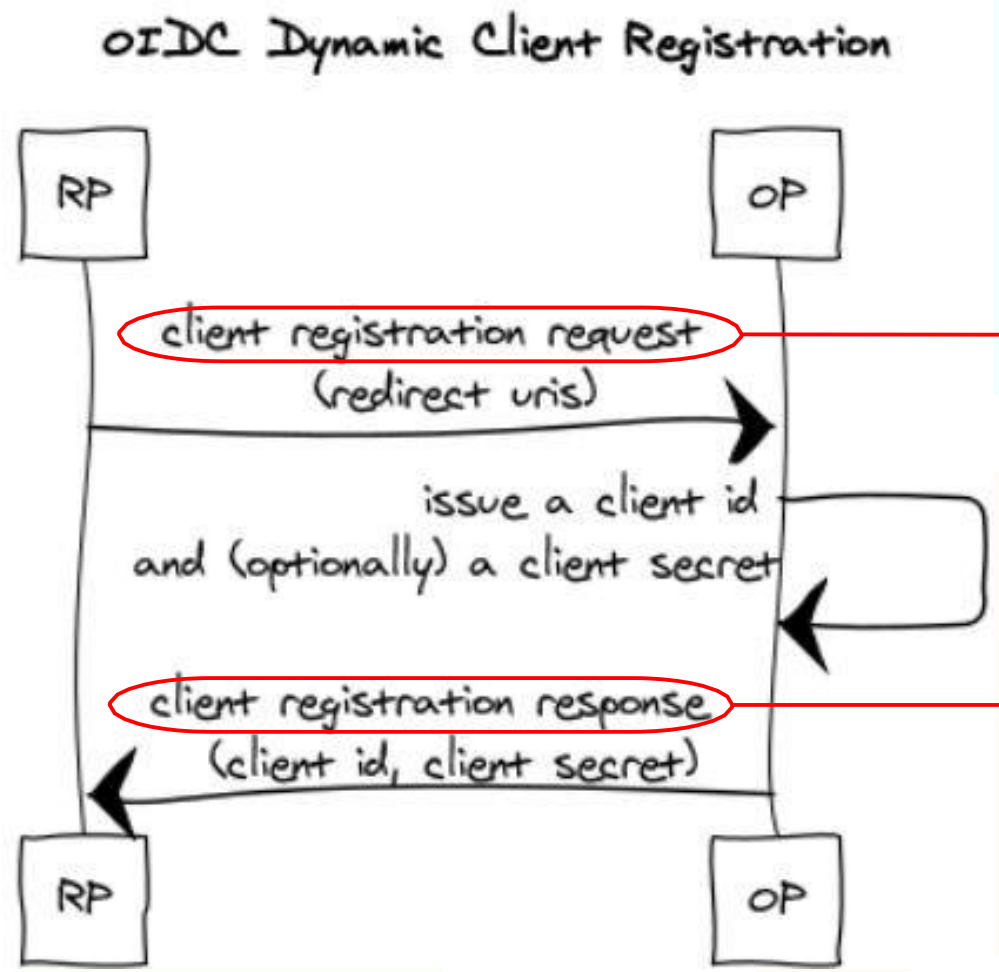


The **RP** receives and consumes the **OP** metadata (provider configuration).

No trust information is provided.

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

OpenID Connect Dynamic Client Registration



The **OP** receives a client registration request from the **RP**.

No trust information is provided.

The **OP** sends a client registration response to the **RP**.

No trust information is provided.

slide content thanks to Davide Vaghetti, GARR, for GN4-2-JRA3-T3.1.A

Slides on general OIDC Fed work: Roland Hedberg, Ioannis Kakavas, Maarten Kremers

OIDC FEDERATION

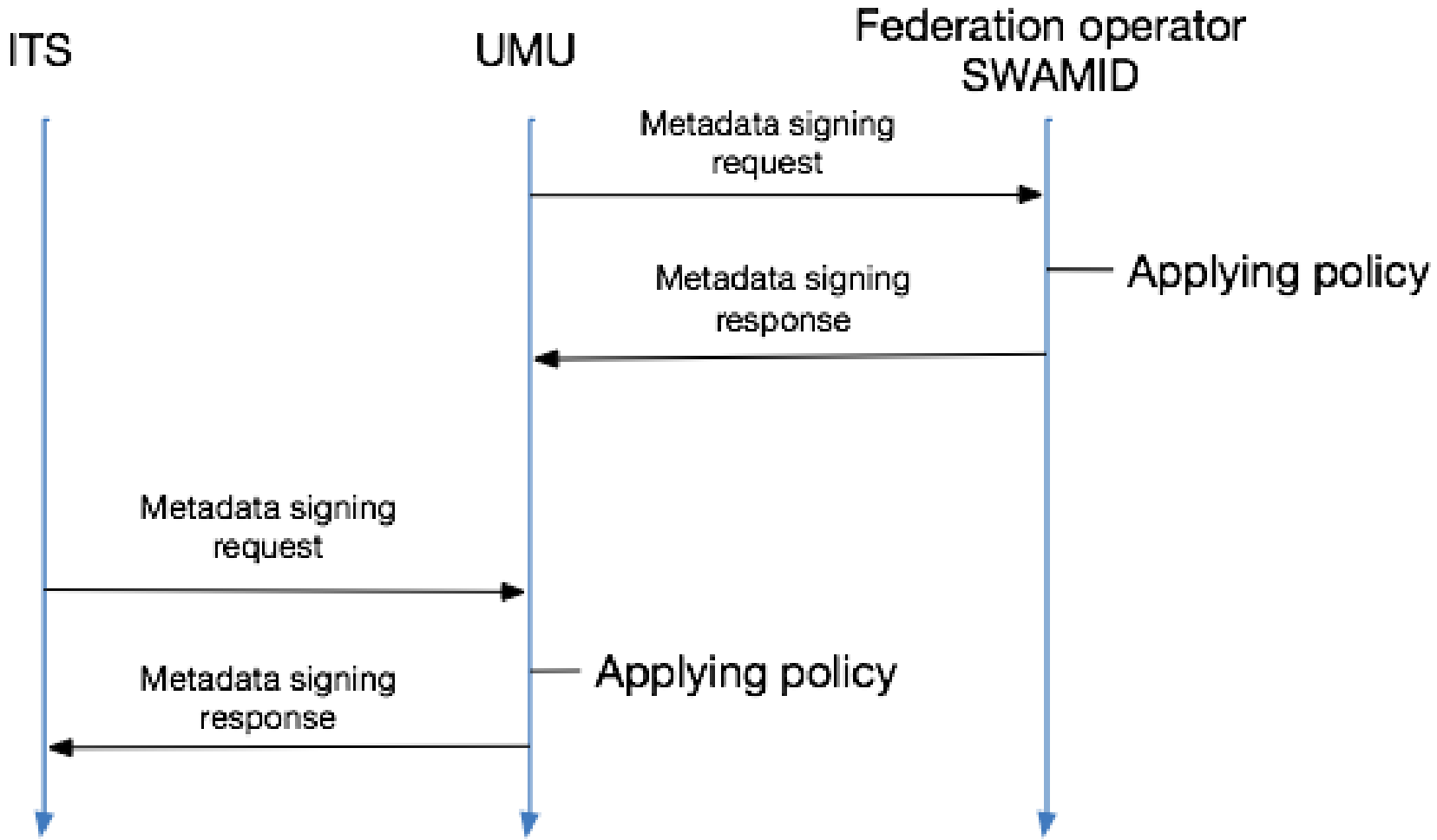
OIDC Identity Federations – *The Specification*
Governing principals

- Allow dynamic discovery and registration without losing trust
- Enforcement of federation and organisation policies
- Allow delegation of entity registration
- Metadata transport and origin independent
- Self-contained metadata

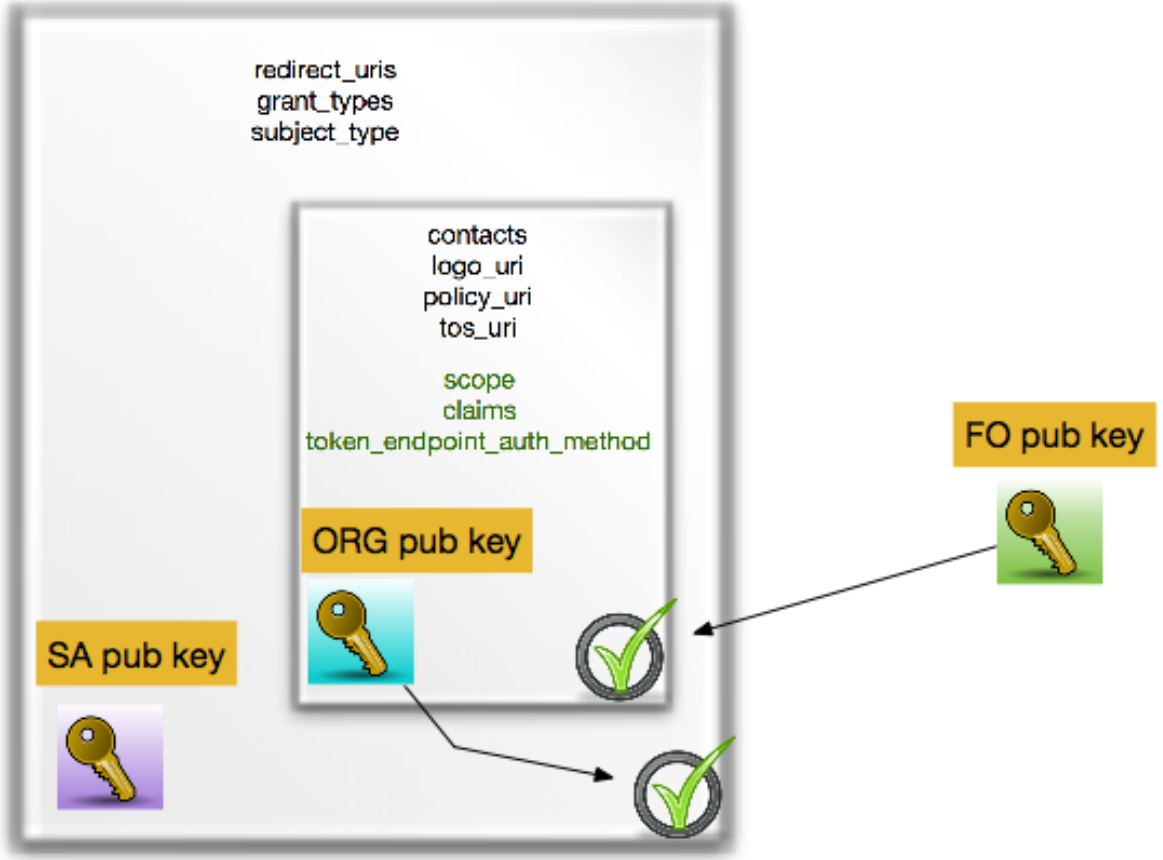
OIDC Identity Federations – *The Specification*
Building blocks

- Trusted 3rd party
- Chain of verifiable claims
- Compounded metadata

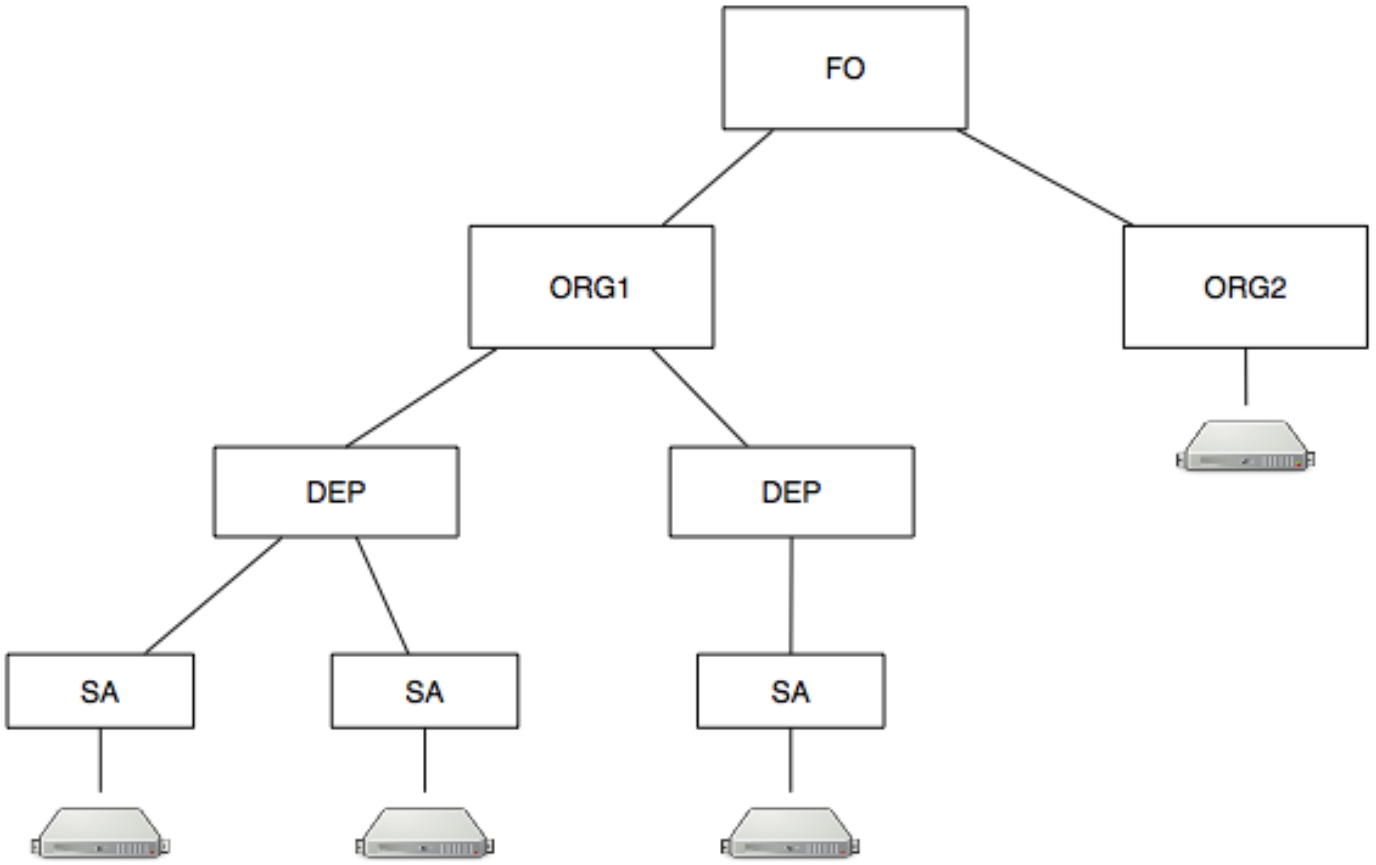
OIDC Identity Federations – *The Specification*
Metadata construction



OIDC Identity Federations – *The Specification*
Compounded metadata statement



OIDC Identity Federations – *The Specification* Depth



OIDC Identity Federations – *Implementations & Tools*
Reference Implementation in Python

- https://github.com/OpenIDC/fedoidc
- Federation aware OpenID Connect Provider
- Federation aware Relying Party
- Support for Federation Operator related functionality

OIDC RP FEDERATION PILOT

IGTF "RP oriented" OIDC Fed can leverage existing framework

- connect RPs from infrastructures that are IGTF members (EGI, HPCI, OSG, WLCG, GEANT, PRAGMA, PRACE, XSEDE, …) *and new IGTF RP members can join of course!*
- Accreditation process and membership guidelines in place
- OPs in the federation (RI/EI IdP-SP-Proxies) use IGTF APs and *Snctfi* framework where needed
- RPs in the federation become the responsibility of their member representatives
- regional ('national') RP groups via their existing authority member

for RP trust (more than today) re-use Sirtfi, WISE, and trust groups

Scoping and model discussions

ACAMP session nodes (see Wiki)

- do not over-complicate the initial set-up
- retain dynamics in the system by leveraging existing trust
- stick to OIDC core attributes makes life easier
- discovery – leave this for the RPs, but make our data available
- allow overlapping federations and be complementary (COIs)

Don’t boil the ocean

- scope to the expected $\mathcal{O}(100)$ organisations
- leverage existing trust and current operational mechanisms

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

IGTF OIDC Federation Task Force

The IGTF task force for OIDC Federation will

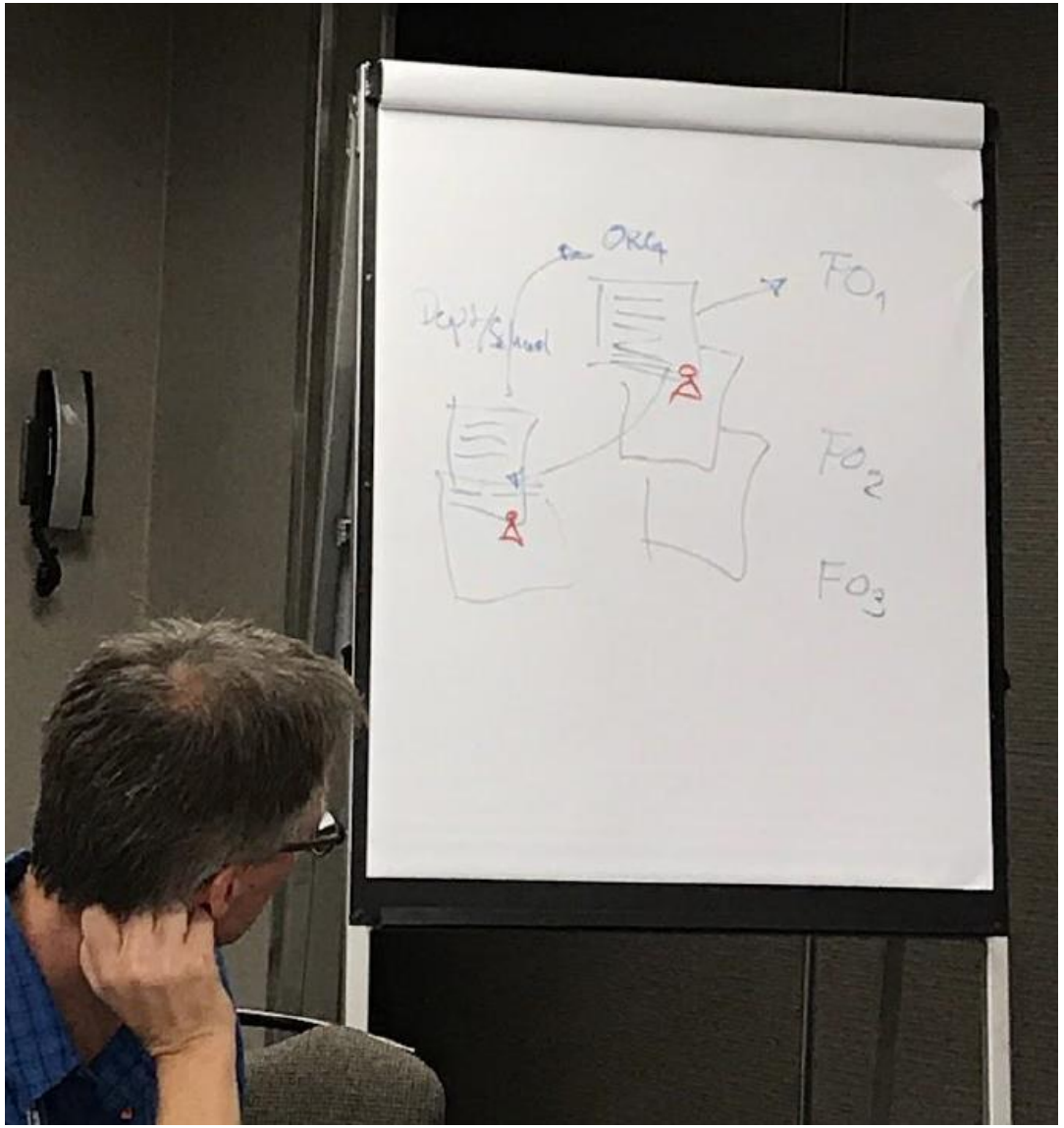
- identify specific objectives – *I2 TechEx*
- scope needs and requirements for R/E infrastructure OIDC Fed – *Prague EUGridPMA 42*
- verify compatibility of IGTF Assurance Profile framework
  for ‘technology-agnosticity’ with OpenID Providers (proxies) and RPs
- **test an OIDCFed scenario**
  e.g. starting with use cases: WLCG, RCauth.eu, ELIXIR/LS, EGI CheckIn, …
- assess structure and needed meta-data in a ‘trust anchor service’,
  - how to address RPDNC
  - links it with (dynamic) client registration
- liaise with OIDC Fed efforts in AARC and GN*-*, and Roland Hedberg

OIDC Fed pilots

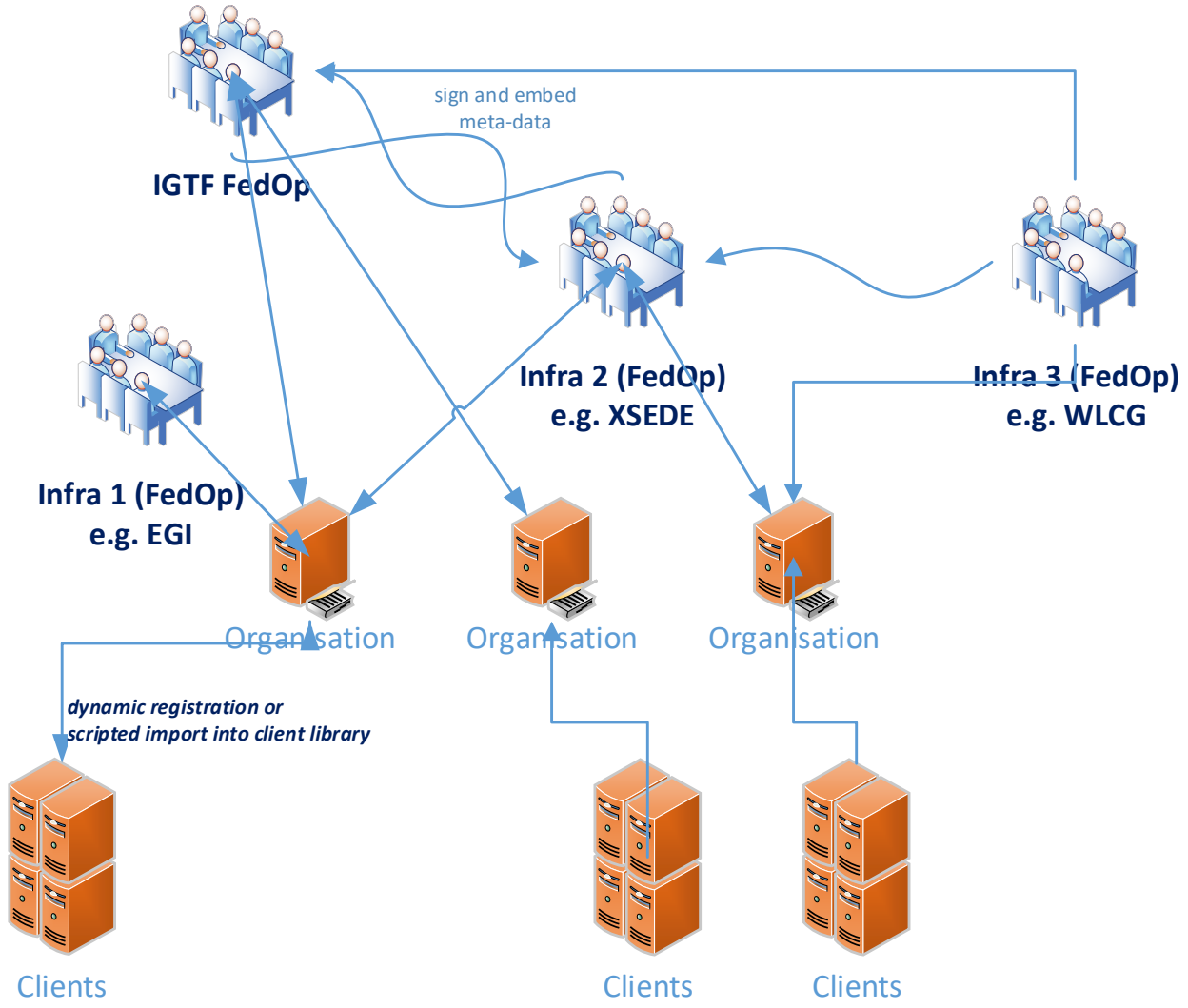
- Based on the spec by Roland Hedberg

- scoped to the RP + Proxy
  case is not very complex, actually
  Infrastructures can use trusty shortcuts that would be too costly at the general R&E scale

- leverage *existing policy and trust* framework
- ‘pilot’ RPs and proxies will be using scripting and glue to get integration with existing services, based on assessed trust framework
- we *can* leverage existing trust



Can we do without a single one to rule them all?



- today the RIs and EIs trust the IGTF trust anchors and *may (but do rarely)* add their own
- Can the 'federation' be the community and import a commonly trusted set?
- Can the IGTF allow devolved registration *provided* that the trusted organisations implement the same policy controls *Snctfi* and the proper *Assurance Profiles*?

For the benefit of Research Infras …

- IGTF membership process and *Snctfi* jointly give you the trust of Infra SPs (RPs)
- use peer-reviewed (self-)assessment as foundation of the ‘scientific process’ of trust
- technical details on how the IGTF FedOp will sign and distribute meta-data statements – subject to discussion at TIIME, AARC, and IGTF meetings
- new communities and (proxy) operators can join IGTF any time
  - there is no fee or something like that
  - but we request participation in the peer-review and assessment process …

Information sharing

Keeping in touch

- http://wiki.eugridpma.org/Main/OIDCFed
- oidcfed@igtf.net (https://igtf.net/mailman/oidcfed)

but don’t forget everyone else!

- REFEDS, GEANT
- TIIME, TNC, TechEx, …

Questions?

BUILDING A GLOBAL TRUST FABRIC

components of this work have been co-supported by:
the Dutch National e-Infrastructure coordinated by SURF,
EOSC-HUB – EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777536
AARC (2) – which has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2)