IGTF
Interoperable Global Trust Federation
AP | EU | TAG

OIDC Federation for Infrastructures

leveraging the IGTF global infrastructure trust framework with OIDC technology

David Groep

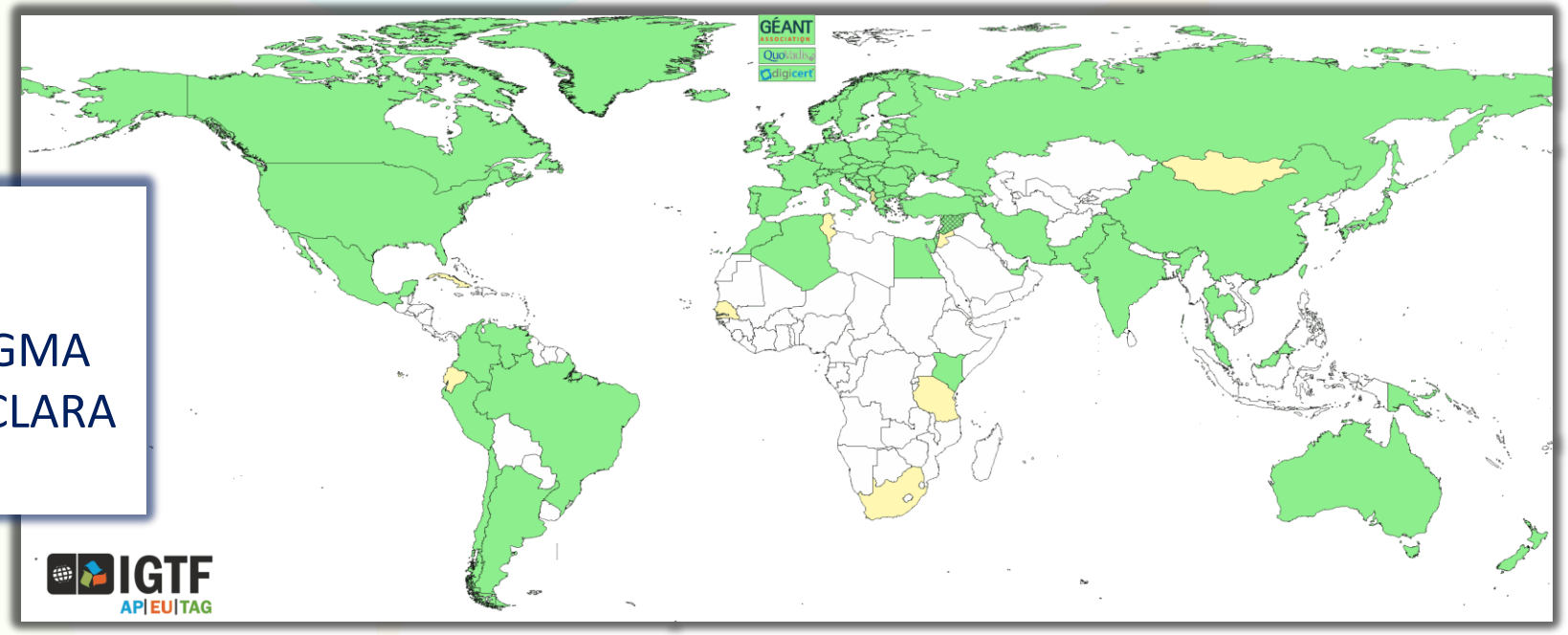
Nikhef

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	. . .



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')

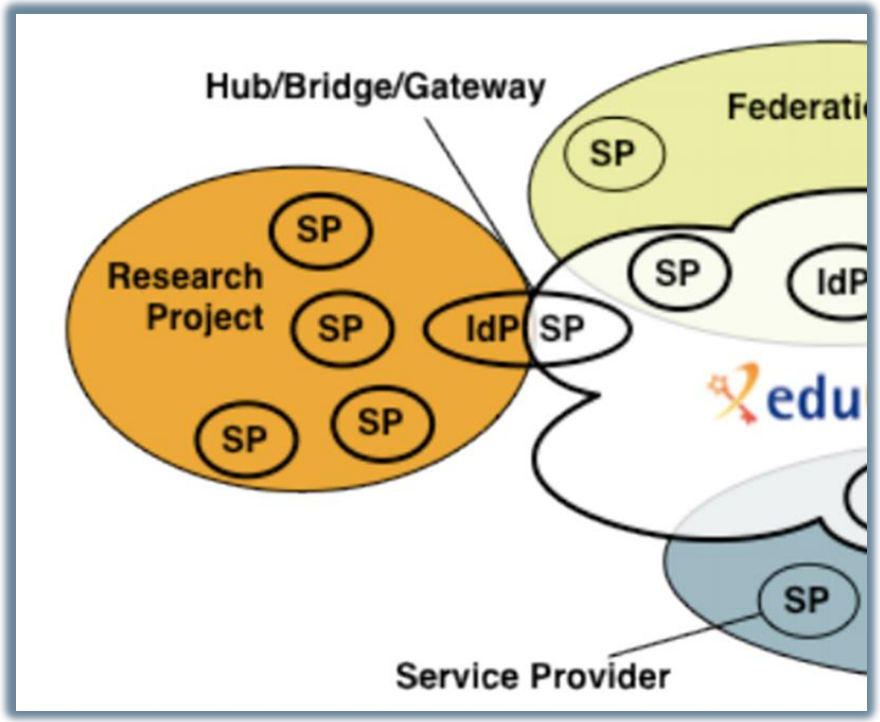
- Snctfi - Community Trust Framework in Federated Infras
  https://igtf.net/snctfi

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

Snctfi: aiding Infrastructures achieve policy coherency

- ✓ allow SPIdP Proxies to assert ‘qualities’, categories, based on assessable trust
- ✓ Develop recommendations for an Infrastructure’s coherent policy set




Sctfi v1.0 AARC

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsara)

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Derived from SCI, the framework on *Security for Collaboration among Infrastructures*
- Complements Sirtfi with requirements on internal consistent policy sets for Infrastructures
- Aids Infrastructures to assert *existing* categories to IdPs REFEDS R&S, Sirtfi, DPCoCo, …

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

https://igtf.net/snctfi

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

IGTF OIDC Federation Task Force

The IGTF task force for OIDC Federation will

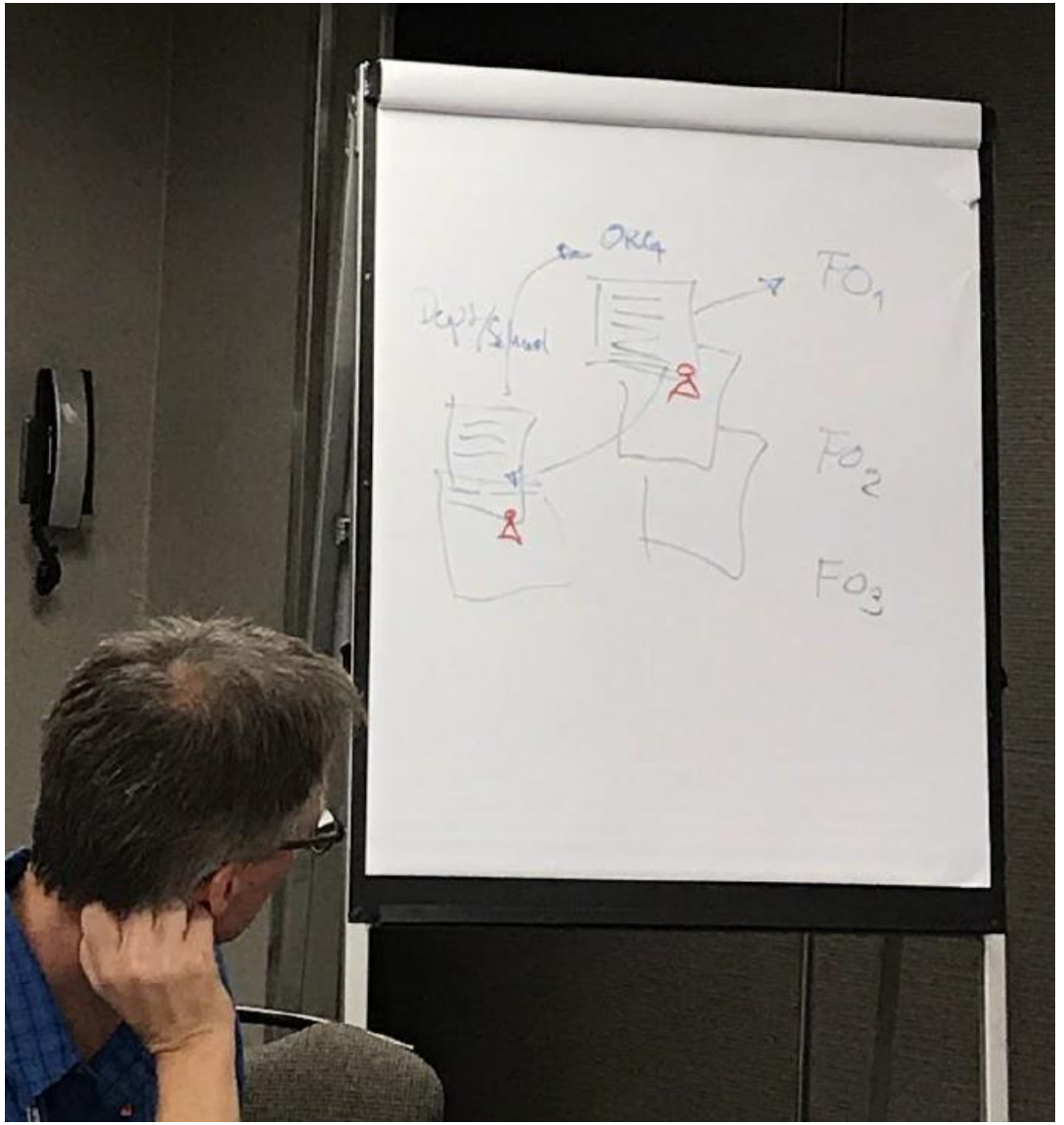
- identify specific objectives – *I2 TechEx*
- scope needs and requirements for R/E infrastructure OIDC Fed – *Prague EUGridPMA 42*
- verify compatibility of IGTF Assurance Profile framework
  for 'technology-agnosticity' with OpenID Providers (proxies) and RPs
- **test an OIDCFed scenario**
  e.g. starting 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

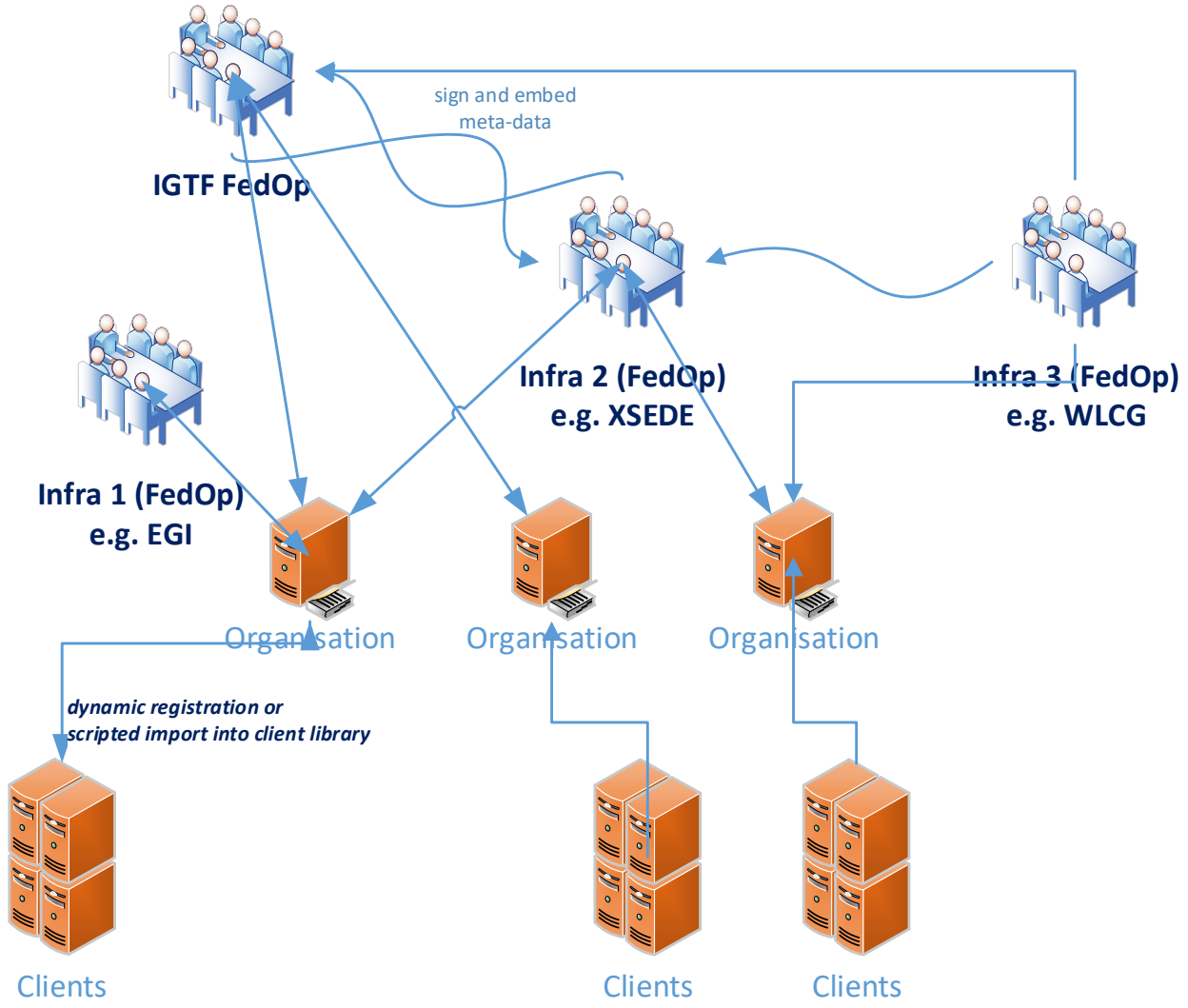
- Based on the spec by Roland Hedberg

- 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!

- oidcre@lists.refeds.org (REFEDS)
- TIIME, TNC, TechEx, …

Questions?

BUILDING A GLOBAL TRUST FABRIC