OIDC Federation for Infrastructures

EUGridPMA 42
Prague, CZ

David Groep
davidg@nikhef.nl

“establish common policies and guidelines that enable interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers”

- technology-agnostic assurance profiles (see IANA registry)
- with specific renderings – PKIX, Attribute Authorities, …

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

- technology bridges: TCS, RCauth.eu, IGTF-eduGAIN bridge, …
- native SAML R&E federation most effective through REFEDS now
- behind the bridges for research & collaboration, OIDC prominence!

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**
  we will be doing that today!
- verify compatibility of IGTF Assurance Profile framework
  for ‘technology-agnosticity’ with OpenID Providers (proxies) and RPs
- test a OIDCFed scenario
  e.g. starting with use cases: WLCG, RCauth.eu, … ELIXIR, EGI CheckIn
- assess structure and needed meta-data in a ‘trust anchor service’,
  - how to address RPDNC
  - links it with dynamic client registration through ‘.well-known’
- liaise with OIDC Fed efforts in AARC and GN*-*, and Roland Hedberg

Client ID and Client Secret

RCauth.eu

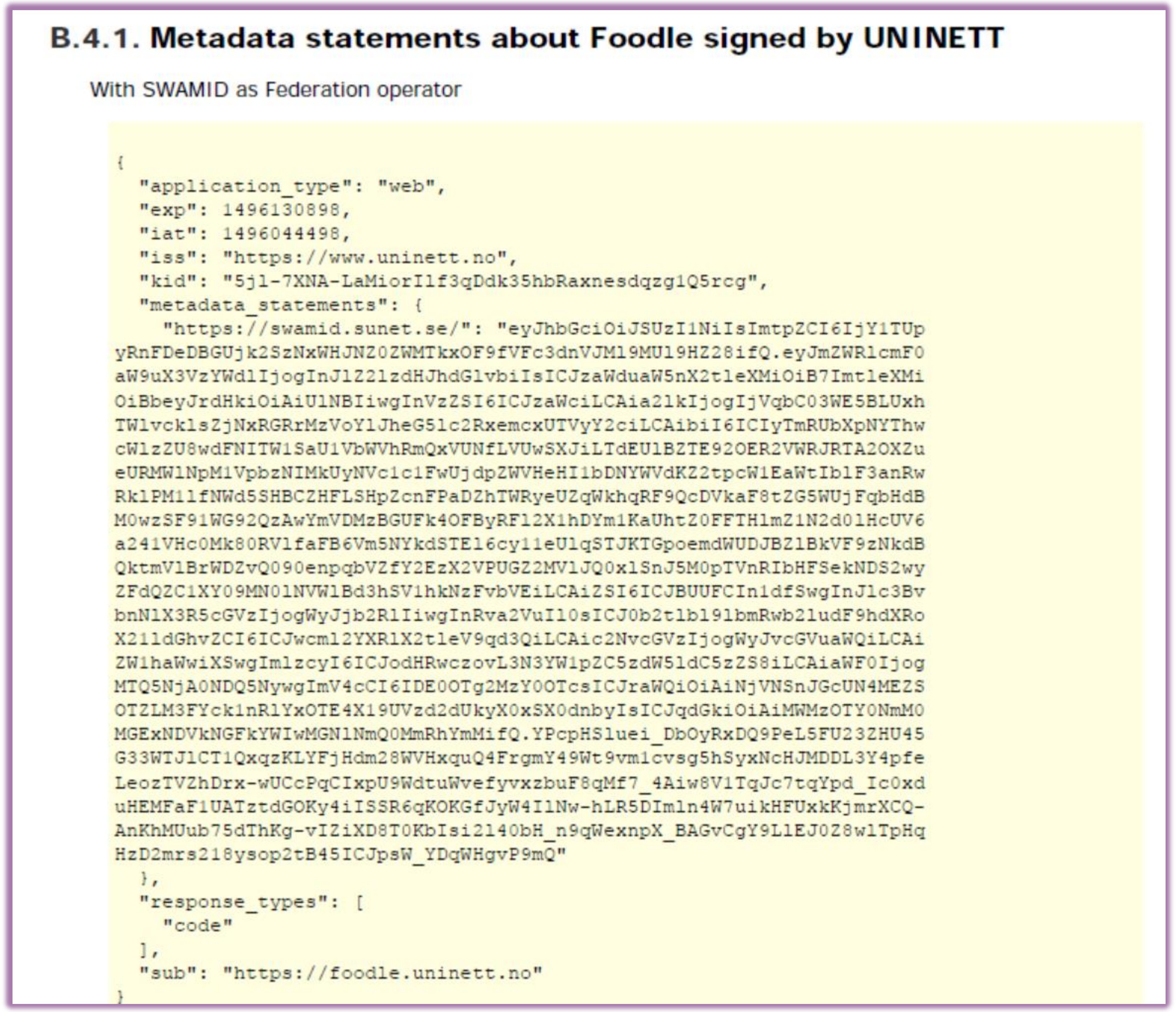
- WaTTS service
- EGI MasterPortal
- MinE Credential Hosting
- *… B2ACCESS, …*

Master Portal

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

OIDC Fed

- See spec by Roland Hedberg

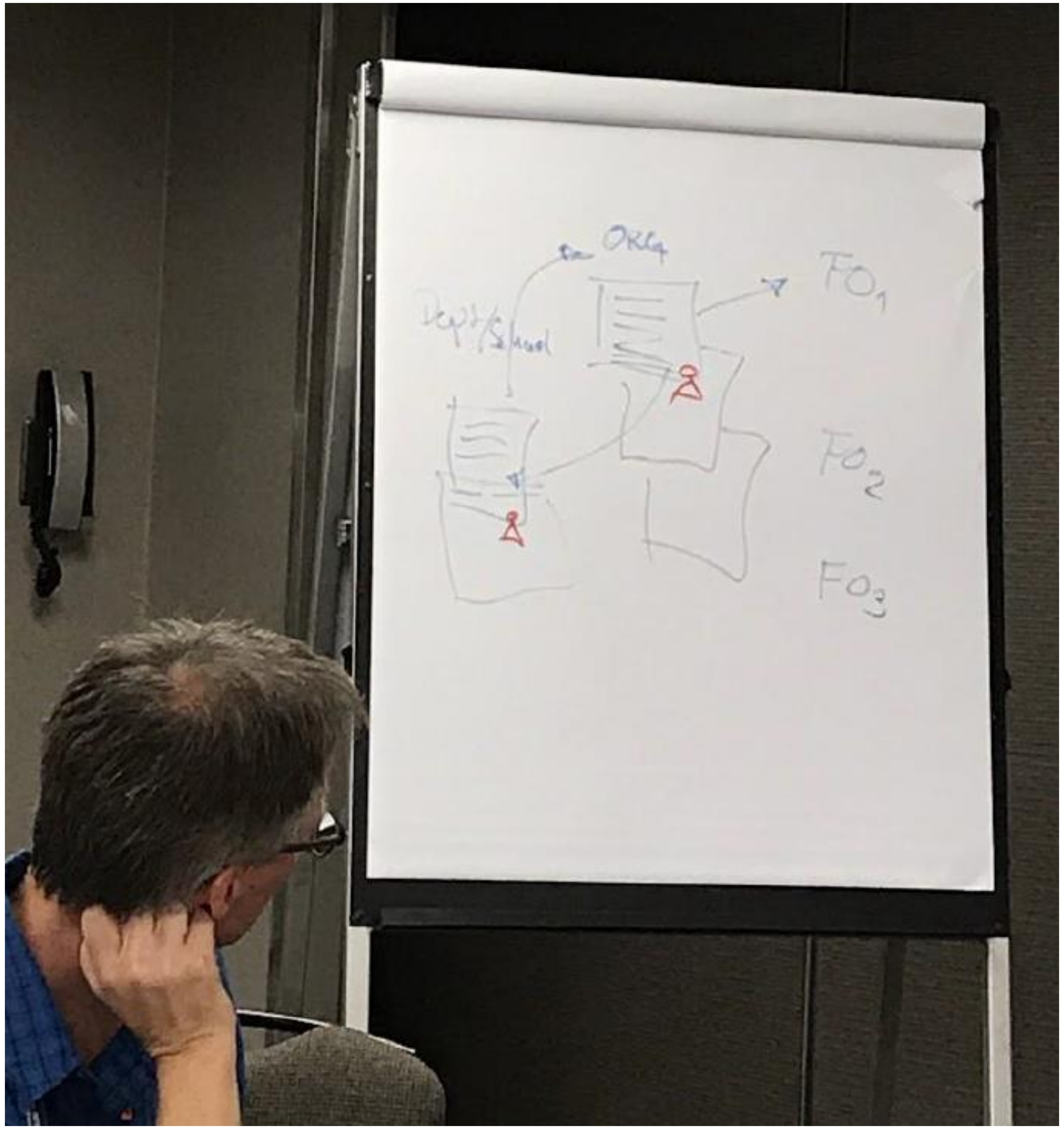


B.4.1. Metadata statements about Foodle signed by UNINETT

With SWAMID as Federation operator

```
{
  "application_type": "web",
  "exp": 1496130898,
  "iat": 1496044498,
  "iss": "https://www.uninett.no",
  "kid": "5jl-7XNA-LaMiorIlf3qDdk35hbRaxnesdqzg1Q5rcg",
  "metadata_statements": {
    "https://swamid.sunet.se/": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjY1TUp
yRnFDeDBGUjk2SzNxWHJNZ0ZWMTkxOF9fVFc3dnVJMl9MUl9HZ28ifQ.eyJmZWRlcmF0
aW9uX3VzYWdlIjogInJlZ2lzdHJhdGlvbiIsICJzaWduaW5nX2tleXMiOiB7ImtleXMi
OiBbeyJrdHkiOiAiUlNBIiwgInVzZSI6ICJzaWciLCAia2lkIjogIjVqbC03WE5BLUxh
TWlvcklsZjNxRGRrMzVoYlJheG5lc2RxemcxUTVyY2ciLCAibiI6ICIyTmRUbXpNYThw
cWlzZU8wdFNITW1SaU1VbWVhRmQxVUNfLVUwSXJiLTdEUlBZTE92OER2VWRJRTA2OXZu
eURMWlNpM1VpbzNIMkUyNVc1c1FwUjdpZWVHeHI1bDNYWVdKZ2tpcW1EaWtIblF3anRw
RklPM1lfNWd5SHBCZHFLSHpZcnFPaDZhTWRyeUZqWkhqRF9QcDVkaF8tZG5WUjFqbHdB
M0wzSF91WG92QzAwYmVDMzBGUFk4OFByRFl2X1hDYm1KaUhtZ0FFTHlmZ1N2d01HcUV6
a241VHc0Mk80RVlfaFB6Vm5NYkdSTEl6cy11eUlqSTJKTGpoemdWUDJBZlBkVF9zNkdB
QktmVlBrWDZvQ090enpqbVZfY2EzX2VPUGZ2MVlJQ0x1SnJ5M0pTVnRIbHFSekNDS2wy
ZFdQZC1XY09MN01NVW1Bd3hSV1hkNzFvbVEiLCAiZSI6ICJBUUFCIn1dfSwgInJlc3Bv
bnNlX3R5cGVzIjogWyJjb2RlIiwgInRva2VuIl0sICJ0b2tlbl9lbmRwb2ludF9hdXRo
X21ldGhvZCI6ICJwcml2YXRlX2tleV9qd3QiLCAic2NvcGVzIjogWyJvcGVuaWQiLCAi
ZW1haWwiXSwgImlzcyI6ICJodHRwczovL3N3YW1pZC5zdW5ldC5zZS8iLCAiaWF0Ijog
MTQ5NjA0NDQ5NywgImV4cCI6IDE0OTg2MzY0OTcsICJraWQiOiAiNjVNSnJGcUN4MEZS
OTZLM3FYck1nRlYxOTE4X19VVzd2dUkyX0xSX0dnbyIsICJqdGkiOiAiMWMzOTY0NmM0
MGExNDVkNGFkYWIwMGNlNmQ0MmRhYmMifQ.YPcpHSluei_DbOyRxDQ9PeL5FU23ZHU45
G33WTJlCT1QxqzKLYFjHdm28WVHxquQ4FrgmY49Wt9vm1cvsg5hSyxNcHJMDDL3Y4pfe
LeozTVZhDrx-wUCcPqCIxpU9WdtuWvefyvxzbuF8qMf7_4Aiw8V1TqJc7tqYpd_Ic0xd
uHEMFaF1UATztdGOKy4iISSR6qKOKGfJyW4IlNw-hLR5DImln4W7uikHFUxkKjmrXCQ-
AnKhMUub75dThKg-vIZiXD8T0KbIsi2l40bH_n9qWexnpX_BAGvCgY9LlEJ0Z8wlTpHq
HzD2mrs218ysop2tB45ICJpsW_YDqWHgvP9mQ"
  },
  "response_types": [
    "code"
  ],
  "sub": "https://foodle.uninett.no"
}
```

- scoped to the RP + Proxy case is not very complex, actually



OIDC Fed ‘policy’

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

Information sharing

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)

Keeping in touch

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

Needs and Requirements

- ELIXIR & Life Sciences AAI (Michal Prochazka)
- CILogon developments (Jim Basney)
- behind EGI Check-In (Nicolas Liampotis)
- Recommendations in AARC and GN*-* (Davide Vaghetti)
- WaTTS (Marcus Hardt)

followed by a discussion on

- *what tools we can use on the IGTF side (scripts, URL triggers) ,*
- *what tools on the client side for auto-populating RPs (periodic cron jobs, scripts)*

Let’s do it!

Nikhef

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606