

OIDC Federation for Infrastructures



Nikhef

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!

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
- liaise with OIDC Fed efforts in AARC and GN^{*}-^{*}, and Roland Hedberg



Master Portal

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

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

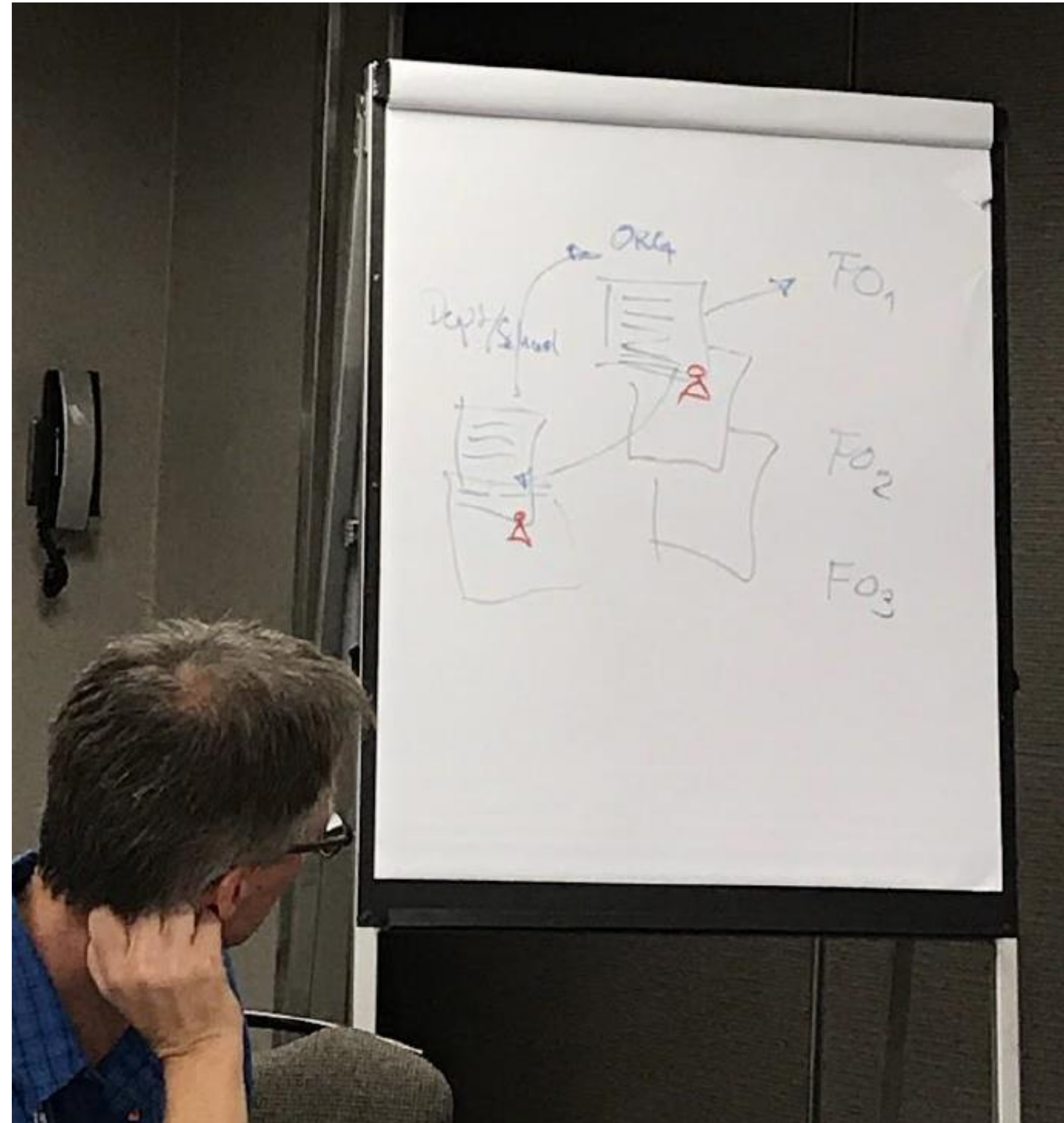
- See spec by Roland Hedberg

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": "5j1-7XNA-LaMior1lf3qDdk35hbRaxnesdqzgiQ5rcg",
  "metadata_statements": {
    "https://swamid.sunet.se/": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjY1TUUp
yRnFDeDBGUjk2S2ZxWHJN20ZWMkxOF9fVFc3dnVJM19MU19HZ228ifQ.eyJmZWRLcmFO
aW9uX3VzYWdlIjogInJlZ2lzdHJhdG1vbiIsICJzaWduaW5nX2tleXMiOiB7ImtleXMi
OiBbeyJrdHkiOiAiU1NBIiwgInVzZSI6ICJzaWciLCIAa2lkIjogIjVqbC03WE5BLUxh
TWlvcclsZjNjRGRrMzVoY1JheG5lc2RxeMxcUTVvY2ciLCIAibiI6ICIyImRUBXpNYThw
cWlz2U8wdFNITW1SaU1VbWVhRmQxVUNfLVUwSXJiLTdEU1B2TE92OER2VWRJRTA2OXZu
eURMW1NpM1VpbzNIMkUyNvc1ciFwUjdpZWVHeHI1bDNyYVdKZ2tpcW1EaWtIb1F3anRw
RklPM1fNwd5SSHBCZHFLSHpZcnFPaDZhTWRYeUZqWkhqRF9QcDVkaF8t2G5WUjFqbHdB
M0wzSF91WG92QzAwYmVDMzBGUfK4OFByRF12X1hdYm1KaUhtZ0FFTH1mZ1N2d01HcUV6
a241VHc0Mk80RV1faFB6Vm5NYkdSTE16cy11eUlqSTJKTGpoemdWUDJBZ1BkVF9zNkdB
QktmV1BrWDZvQ090enpqbVZfy2EzX2VPUGZ2MV1JQ0xlSnJ5M0pTVnRiBHFSEkNDS2wy
ZFdQZC1XY09MN01NVW1Bd3hSV1hkNzFvbVEiLCIAiZSI6ICJBUUFCInlndfSwgInJlc3Bv
bnNlX3R5cGVzIjogWyJjb2RlIiwgInRva2VuI10sICJ0b2t1b191bmRwb21udF9hdXR0
X211dGhvZCI6ICJwcm12YXR1X2tleV9qd3QiLCIAic2NvcGVzIjogWyJvcGVuaWQiLCIAi
ZWihaWwiXSwgImlzcyciOiB7ImtpZCI6IjY1TUUpZC5zdW51dC5zZS8iLCIAiaWF0Ijog
MTQ5NjA0NDQ5NywgImV4cCI6IDE0OTg2MzY0OTcsICJraWQiOiAiNjVNSnJGcUN4MEZS
OTZLM3FYcklnR1YxOTE4X19UVzd2dUkyX0xSX0dnbyIsICJqdGkiOiAiMWMzOTY0NmM0
MGEzNDVhNGFkYWIwMGN1NmQ0MmRhYmMiFQ.YPcpHSluei_DbOyRxDQ9PeL5FU23ZHU45
G33WTJ1CT1QxqzKLYFjHdm28WVHxquQ4FrgmY49Wt9vniCvsg5hSxNcHJMDDL3Y4pfe
LeozTVZhDrx-wUccPqCIxpU9WdtuWvefyvxzbuF8qMf7_4Aiw8V1TqJc7tcqYpd_Ic0xd
uHEMFaF1UATztdGOKy4iISSR6qKOKGfJyW411Nw-hLR5DImln4W7uikHFUxkKjmrXCQ-
AnKhMUub75dThKg-vIZiXD8T0KbIsi2140bH_n9qWexnpX_BAGvCgY9L1EJ0Z8w1TpHq
HzD2mrs218ysop2tB45ICJpsW_YDqWHgvP9mQ"
  },
  "response_types": [
    "code"
  ],
  "sub": "https://foodle.uninett.no"
}
```

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



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

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

- 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)*

Keeping in touch

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

And also

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

Let's do it!

req : 50 Hz
plen : 2.80 μ s
offs : nA

pos : 0
macro d.f. : %
2100ns : %
backgrnd : %

slit
trigger 2

me	filename.ext	bursts [k]	dump [M]	Q ptr [k]	Q ATR [k]	Q ETR	H3 ptr [k]
55	12c dice, 479	48.7	7.3	89.9	80		
19	emp/9a.480	147					

Nikhaf

David Groep

davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>