EUGridPMA
Status and Current Trends
and some IGTF & AARC topics

December 2019
TAGPMA New Orleans
David Groep, Nikhef & EUGridPMA

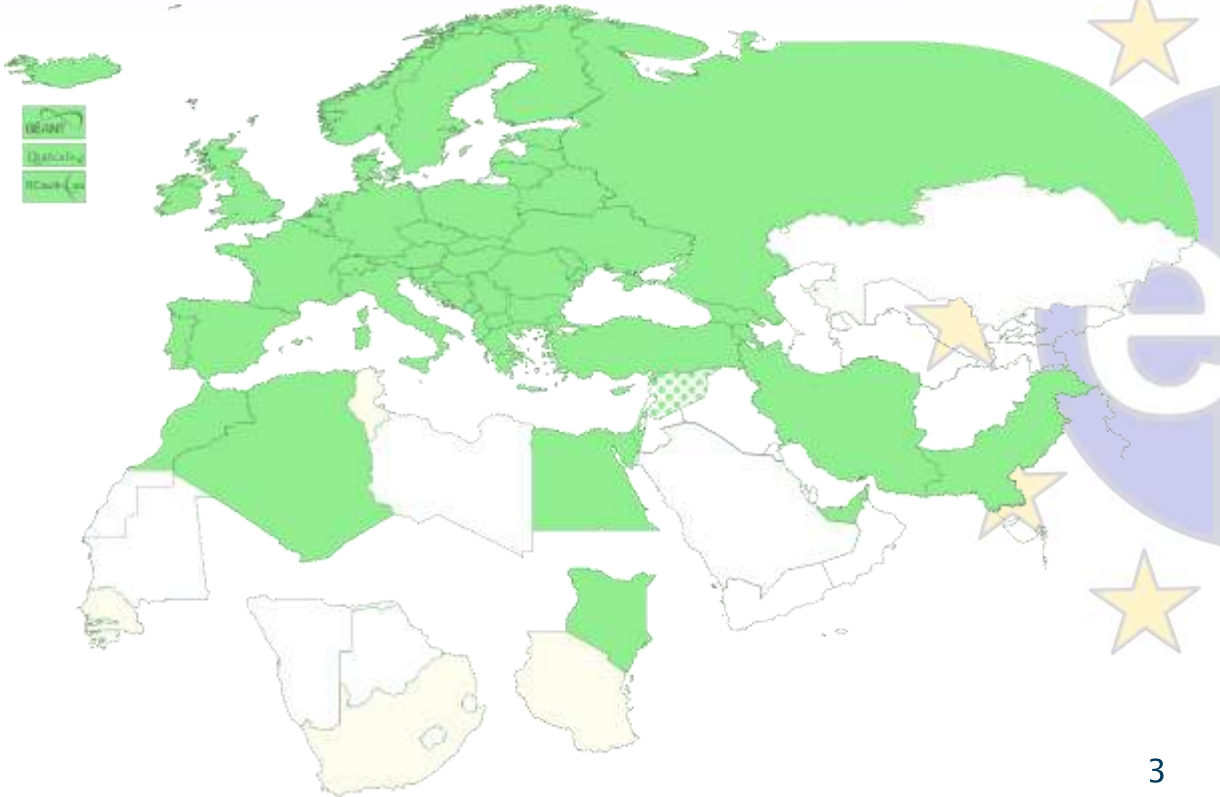
Recent EUGridPMA topics

- PMA membership and evolution of authorities
- Communications Challenges and the ‘WISE SCCC JWG’
- OIDCfed

See also the EUGridPMA47 summary:
https://www.eugridpma.org/meetings/2019-09/

Authority coverage in EMEA

- Europe: AT, CY, CZ, DE, DK, ES, FI, FR, GR, HR, HU, IT, NL, PL, PT, RO, SE, SI, SK, UK; AM, GE, IS, MD, ME, MK, NO, RS, RU, TR, UA and the GEANT TCS
- Middle East: AE, IR, PK
- Africa: DZ, EG, MA, KE
- Multinational: CERN, RCauth.eu, QuoVadis (BM)



Membership and other changes

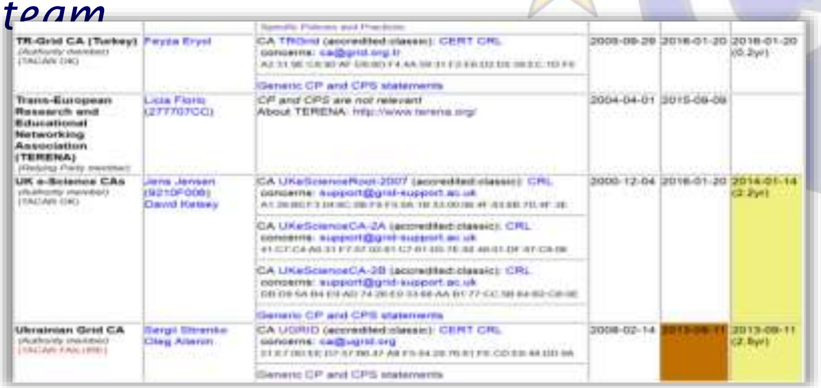
- Responsiveness challenges for some members

  PLEASE take care to renew your trust anchors in time, as well as your CRLs

  EG-EUN now temporarily withdrawn for availability reasons

- Identity providers: both reduction and growth
  - RCauth.eu distributed operations (GRNET, STFC, Nikhef)
    using a shared key (and some smart border-guard-proof distribution)
    governance board + PMA + technical team

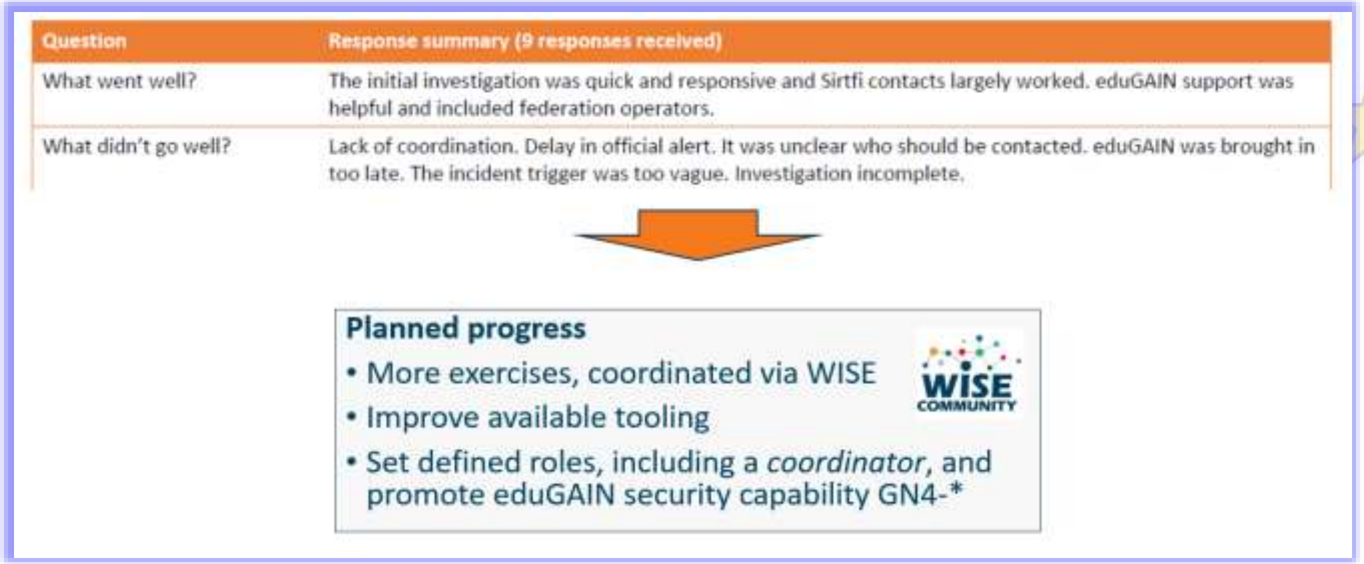
- Self-audit review
  - Cosmin Nistor as review coordinator
  - Self-audits progressing
    on schedule for most CAs



		Specific Policies and Practices			
TR-Grid CA (Turkey) *(Authority member)* (TACAR OK)	Feyza Eryol	CA TRGrid (accredited:classic): CERT CRL concerns: ca@grid.org.tr [illegible] Generic CP and CPS statements	2008-09-29	2016-01-20	2016-01-20 (0.2yr)
Trans-European Research and Educational Networking Association (TERENA) *(Relying Party member)*	Licia Florio (277707CC)	*CP and CPS are not relevant* About TERENA: http://www.terena.org/	2004-04-01	2015-09-09	
UK e-Science CAs *(Authority member)* (TACAR OK)	Jens Jensen (9210F006) David Kelsey	CA UKeScienceRoot-2007 (accredited:classic): CRL concerns: support@grid-support.ac.uk [illegible] CA UKeScienceCA-2A (accredited:classic): CRL concerns: support@grid-support.ac.uk [illegible] CA UKeScienceCA-2B (accredited:classic): CRL concerns: support@grid-support.ac.uk [illegible] Generic CP and CPS statements	2000-12-04	2016-01-20	2014-01-14 (2.2yr)
Ukrainian Grid CA *(Authority member)* (TACAR FAILURE)	Sergii Stirenko Oleg Alienin	CA UGRID (accredited:classic): CERT CRL concerns: ca@ugrid.org [illegible] Generic CP and CPS statements	2008-02-14	2013-09-11	2013-09-11 (2.5yr)

Communications Challenges

Based on *Sirtfi* incident role play of AARC in eduGAIN:
testing communications channels identified as high-prio target
Initial model might be along the IGTF RAT CC challenges – can be extended later



Question	Response summary (9 responses received)
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn't go well?	Lack of coordination. Delay in official alert. It was unclear who should be contacted. eduGAIN was brought in too late. The incident trigger was too vague. Investigation incomplete.

Planned progress

- More exercises, coordinated via WISE
- Improve available tooling
- Set defined roles, including a *coordinator*, and promote eduGAIN security capability GN4-*

Proper OpSec needs to be exercized!

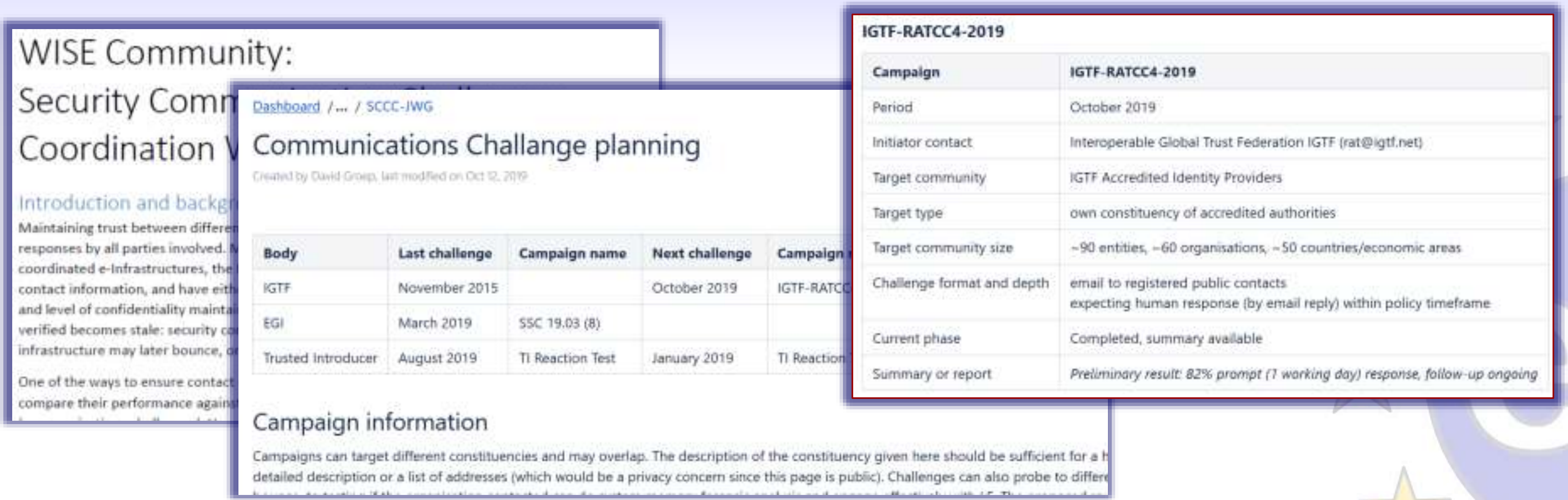
Like the IGTF RAT Communications Challenges, and TF-CSIRT processes, opsec really needs to be exercised often and in-depth to ensure readiness

Logical candidates that could all run the test against IdPs, CAs, SPs, RPs …
… and 'legitimately' claim an interest in their results

- eduGAIN
- IGTF
- GEANT.org
- EOSC-HUB ops, or EGI CSIRT
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, HPCI, …
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, …
- any institution (or person) with access to https://mds.edugain.org/

so soon: all the email in the world will be about Sirtfi Incident Response tests??

WISE SCCC-WG – participate!



WISE Community:
Security Comm
Coordination V

Introduction and backg

Maintaining trust between differe
responses by all parties involved. M
coordinated e-Infrastructures, the
contact information, and have eith
and level of confidentiality mainta
verified becomes stale: security co
infrastructure may later bounce, o

One of the ways to ensure contact
compare their performance agains

Dashboard / ... / SCCC-JWG

Communications Challange planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign
IGTF	November 2015		October 2019	IGTF-RATCC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe

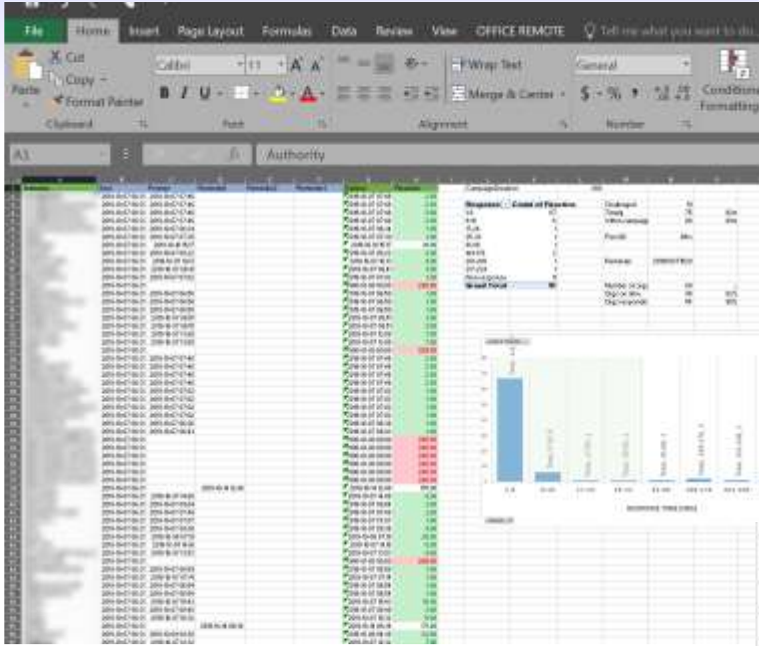
IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	*Preliminary result: 82% prompt (1 working day) response, follow-up ongoing*

WISE, SIGISM, REFEDS, TI joint working group
see wise-community.org and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

IGTF RATCC4 Results



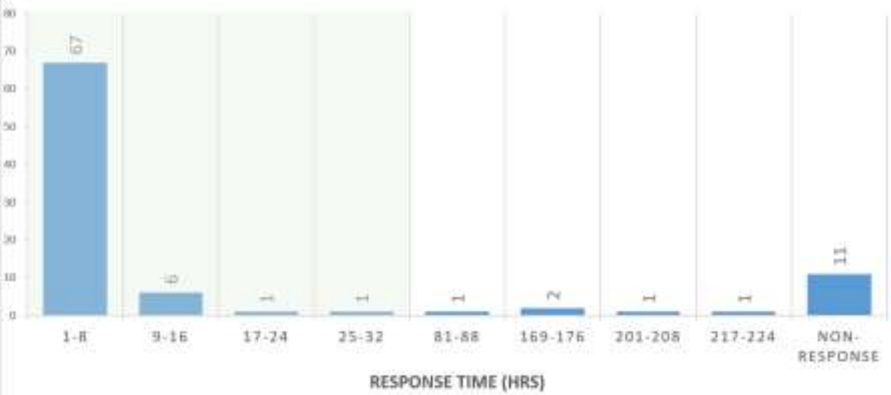
In total there are 91 trust anchors (root, intermediate, and issuing authorities) currently in the accredited bundle,

managed by 60 organisations.

Of the 60 organisations, 49 responded within one working day (82%), representing (incidentally) also 82% of the trust anchors.

Within a few days more, 3 additional ones came in, and 4 more responded after a reminder.

In total, 90% of the organisations responded to the challenge, representing 88% of the trust anchors.



And now for something completely different …

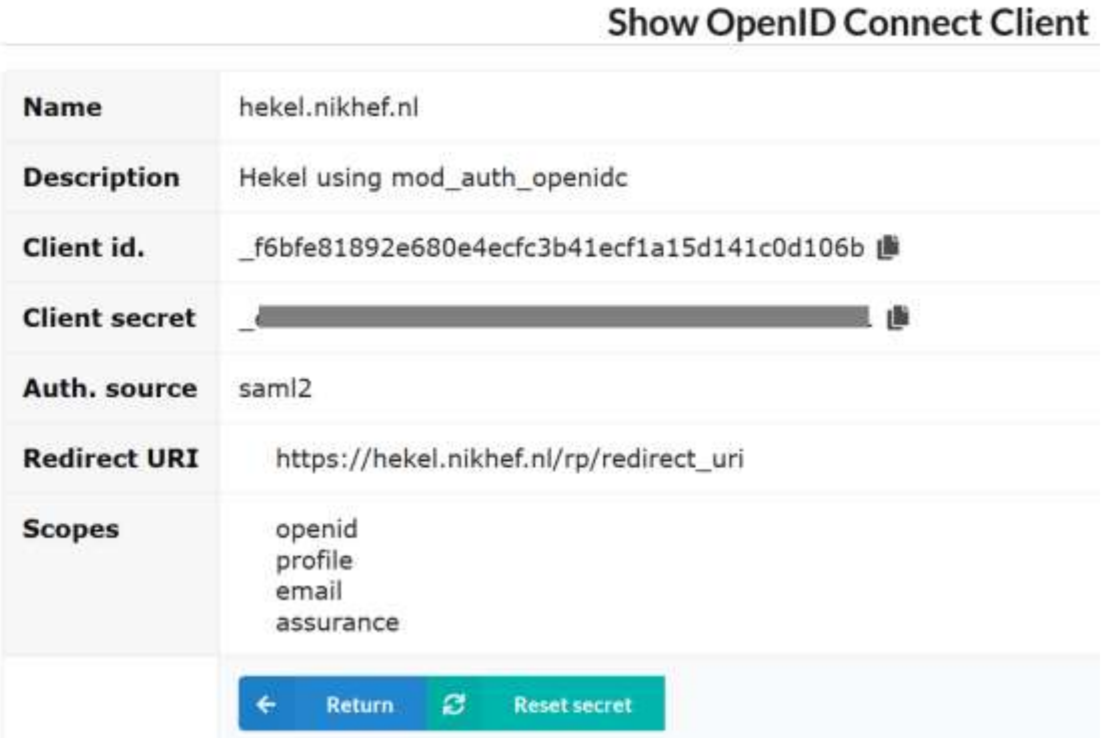
OIDCFED.IGTF.NET

OIDC Federation use cases for communities

Why did we embark on OIDC Fed for global e-Science?

- 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

And registering clients does not scale…



Show OpenID Connect Client

Name	hekel.nikhef.nl
Description	Hekel using mod_auth_openidc
Client id.	_f6bfe81892e680e4ecfc3b41ecf1a15d141c0d106b
Client secret	_[redacted]
Auth. source	saml2
Redirect URI	https://hekel.nikhef.nl/rp/redirect_uri
Scopes	openid profile email assurance

configuration of a (test) client on the Nikhef institutional OP sso.nikhef.nl

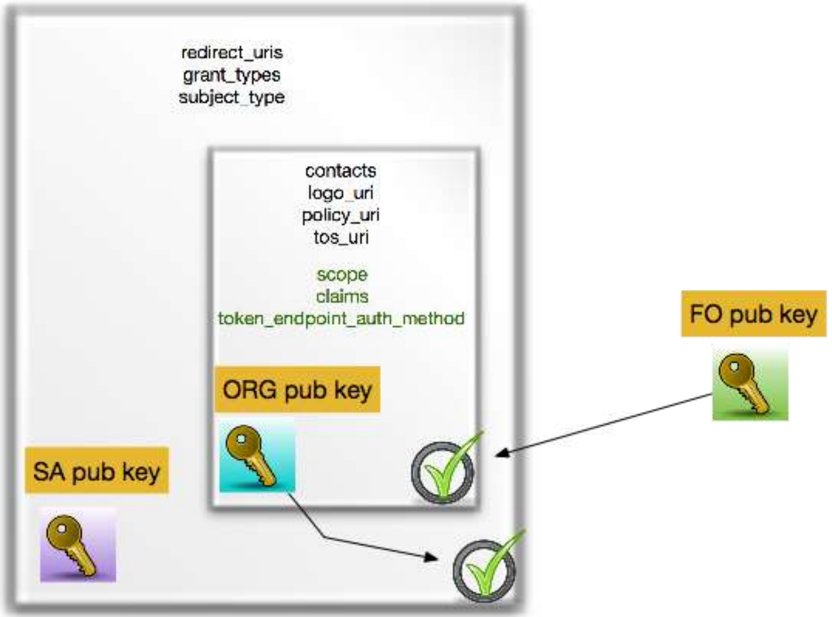
OIDC Fed ‘policy’

IGTF “RP oriented” OIDC Fed can leverage existing framework

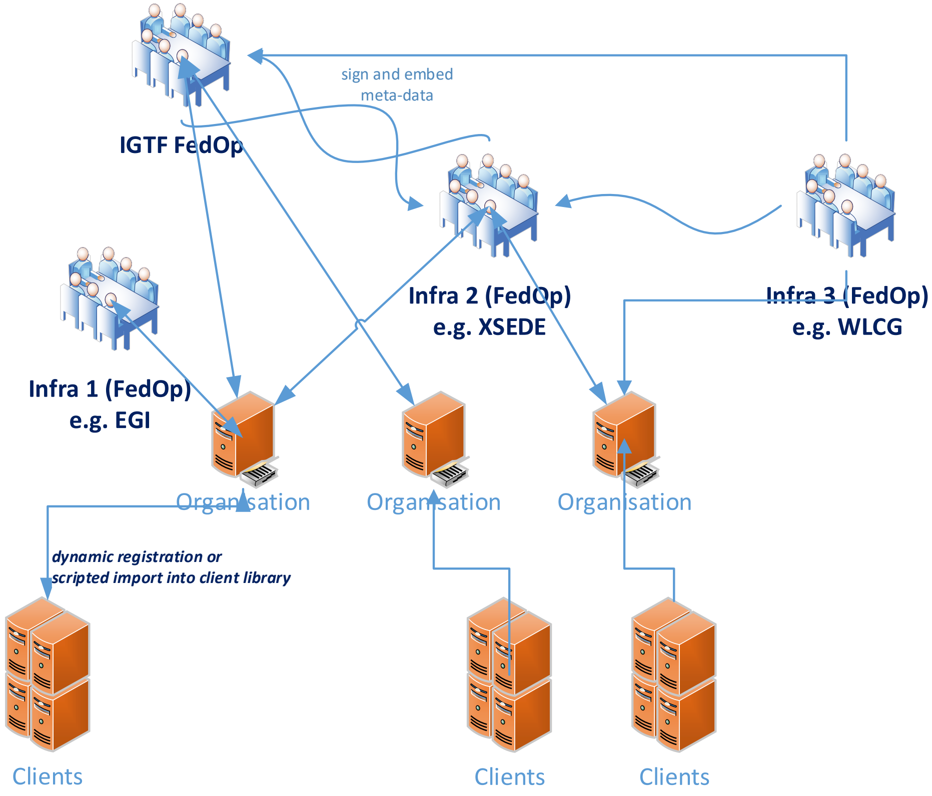
- connect RPs from infrastructures that are IGTF members
  (EGI, HPCI, OSG, WLCG, GEANT, PRAGMA, PRACE, XSEDE, …)
  and new IGTF RP members can join of course!
- Accreditation process and membership guidelines in place
- OPs in the federation (RI/EI IdP-SP-Proxies) use IGTF APs
  and Snctfi framework 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

OIDCfed is basically signing a tree of entities with extensions

we kind-of know building trees and meshed of signed entities work – is this ‘just recast it JSON’ ?

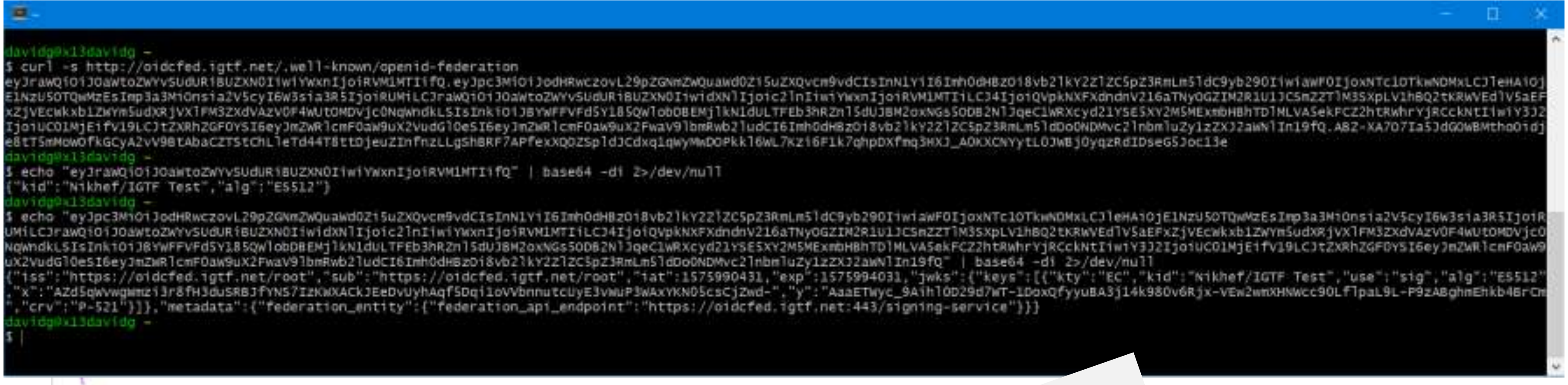


Or can we do without a single one to rule them all?

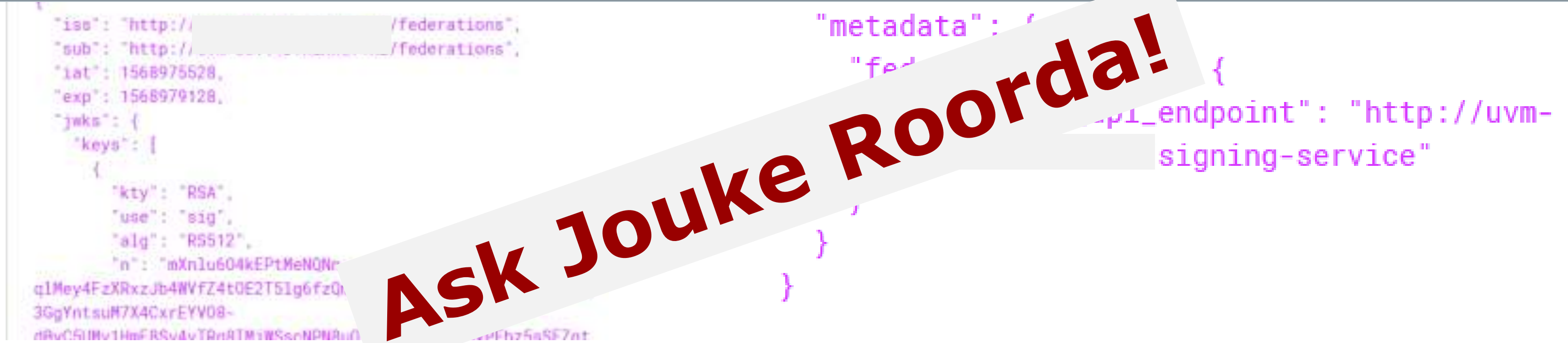


- today the RIs and EIs trust the IGTF trust anchors and *may (but do rarely)* add their own
- Can the 'federation' be the community and import a commonly trusted set?
- Can the IGTF allow devolved registration *provided* that the trusted organisations implement the same policy controls *Snctfi* and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

and this works now: oidcfed.igtf.net



```
davidg@x13davidg ~
$ curl -s http://oidcfed.igtf.net/.well-known/openid-federation
eyJraWQiOiJOaWtoZWYvSUdURiBUZXN0IiwiYWxnIjoiRVM1MTIifQ.eyJpc3MiOiJodHRwczovL29pZGNmZWQuaWd0Zi5uZXQvcm9vdCIsInN1YiI6Imh0dHBzOi8vb2lkY2ZlZC5pZ3RmLm5ldC9yb290IiwiaWF0IjoxNTc1OTkwNDMxLCJleHAiOj
E1NzU5OTQwMzEsImp3a3MiOnsia2V5cyI6W3sia3R5IjoiRUMiLCJraWQiOiJOaWtoZWYvSUdURiBUZXN0IiwidXNlIjoic2lnIiwiYWxnIjoiRVM1MTIiLCJ4IjoiQVpkNXFXdndnV216aTNyOGZIM2R1U1JCSmZZTlM3SXpLV1hBQ2tKRWVEdlV5aEF
xZjVEcWkxb1ZWYm5udXRjVXlFM3ZXdVAzV0F4WUtOMDVjc0NqWndkLSIsInkiOiJBYWFFVFd5Y185QWlobDBEMjlkN1dULTFEb3hRZnl5dUJBM2oxNGs5ODB2NlJqeC1WRXcyd21YSE5XY2M5MExmbHBhTDlMLVA5ekFCZ2htRWhrYjRCckNtIiwiY3J2
IjoiUC01MjEifV19LCJtZXRhZGF0YSI6eyJmZWRlcmF0aW9uX2VudGl0eSI6eyJmZWRlcmF0aW9uX2FwaV9lbmRwb2ludCI6Imh0dHBzOi8vb2lkY2ZlZC5pZ3RmLm5ldDo0NDMvc2lnbmluZy1zZXJ2aWNlIn19fQ.ABZ-XA7O7Ia5JdGOWBMthoOidj
e8tT5mMowOfkGCyA2vV9BtAbaCZTStChLleTd44T8ttDjeuZInfnzLLgShBRF7APfexXQDZSpldJCdxq1qwyMwDOPkk16WL7Kzi6F1k7qhpDXfmq3HXJ_AOKXCNYytLOJWBjOyqzRdIDseG5Joc13e
davidg@x13davidg ~
$ echo "eyJraWQiOiJOaWtoZWYvSUdURiBUZXN0IiwiYWxnIjoiRVM1MTIifQ" | base64 -di 2>/dev/null
{"kid":"Nikhef/IGTF Test","alg":"ES512"}
davidg@x13davidg ~
$ echo "eyJpc3MiOiJodHRwczovL29pZGNmZWQuaWd0Zi5uZXQvcm9vdCIsInN1YiI6Imh0dHBzOi8vb2lkY2ZlZC5pZ3RmLm5ldC9yb290IiwiaWF0IjoxNTc1OTkwNDMxLCJleHAiOjE1NzU5OTQwMzEsImp3a3MiOnsia2V5cyI6W3sia3R5IjoiR
UMiLCJraWQiOiJOaWtoZWYvSUdURiBUZXN0IiwidXNlIjoic2lnIiwiYWxnIjoiRVM1MTIiLCJ4IjoiQVpkNXFXdndnV216aTNyOGZIM2R1U1JCSmZZTlM3SXpLV1hBQ2tKRWVEdlV5aEFxZjVEcWkxb1ZWYm5udXRjVXlFM3ZXdVAzV0F4WUtOMDVjc0
NqWndkLSIsInkiOiJBYWFFVFd5Y185QWlobDBEMjlkN1dULTFEb3hRZnl5dUJBM2oxNGs5ODB2NlJqeC1WRXcyd21YSE5XY2M5MExmbHBhTDlMLVA5ekFCZ2htRWhrYjRCckNtIiwiY3J2IjoiUC01MjEifV19LCJtZXRhZGF0YSI6eyJmZWRlcmF0aW9
uX2VudGl0eSI6eyJmZWRlcmF0aW9uX2FwaV9lbmRwb2ludCI6Imh0dHBzOi8vb2lkY2ZlZC5pZ3RmLm5ldDo0NDMvc2lnbmluZy1zZXJ2aWNlIn19fQ" | base64 -di 2>/dev/null
{"iss":"https://oidcfed.igtf.net/root","sub":"https://oidcfed.igtf.net/root","iat":1575990431,"exp":1575994031,"jwks":{"keys":[{"kty":"EC","kid":"Nikhef/IGTF Test","use":"sig","alg":"ES512"
,"x":"AZd5qWvwgWmzi3r8fH3duSRBJfYNS7IzKWXACkJEeDvUyhAqf5Dqi1oVVbnnutcUyE3vWuP3WAxYKN05csCjZwd-","y":"AaaETWyc_9Aihl0D29d7WT-1DoxQfyyuBA3j14k980v6Rjx-VEw2wmXHNWcc90LflpaL9L-P9zABghmEhkb4BrCm
","crv":"P-521"}]},"metadata":{"federation_entity":{"federation_api_endpoint":"https://oidcfed.igtf.net:443/signing-service"}}}
davidg@x13davidg ~
$ |
```



```
{
  "iss": "http://[redacted]/federations",
  "sub": "http://[redacted]/federations",
  "iat": 1568975528,
  "exp": 1568979128,
  "jwks": {
    "keys": [
      {
        "kty": "RSA",
        "use": "sig",
        "alg": "RS512",
        "n": "mXnlu604kEPtMeNQNr
q1Mey4FzXRxzJb4WVfZ4tOE2T51g6fzQ
3GgYntsuM7X4CxrEYV08-
d8vC5UMy1HmFBSv4vTRq8IMiWSscNPN8u0                 zPFbz5aSF7qt
```

```
"metadata": {
  "fe                          {
                    api_endpoint": "http://uvm-
[redacted]signing-service"
    }
  }
}
```

Ask Jouke Roorda!

Next meetings

EUGridPMA 48	Prague, CZ	22-24	January 2020
APGridPMA 2020	Taipei, TW		March 9, 2020
EUGridPMA 49			May 2020
IGTF All Hands (& EUGridPMA50?)	Pittsburg, PA, USA		September 2020