2018.01.22 FEDGROUPMTG42 (1)

Present: Ingrid, Melanie, Dana, Sam, Darrell S, Marc, Scott, Dave L, Bouchra Samia, Ian N
Remote: Miroslav, Vladimir, Christos, Roberto C, Mischa S*, Davide Vaghetti, Marcus H,
Reimer, Licia, Michal P, Nicolas L

PEARC - July 22-27

9^{10} Welcome. Agenda: - future meeting planning → timing & funding?
List of deliverables still needs to be done.
discuss again.
@comms egagement.
- next time: input of QC on keys and crypto → RAT discussion.
appropriate for IGTF.

Minutes: Dave L.

9^{25} Eric Yen/APGridPMA: see slides
10^{05} Dave L/ TAGPMA update: see slides. CILogon has sent around another, it ought to be accredited by now:
Grid Community forum set up with steering group and on github.

14^{10} OIDC Fed/ Darrell:
relation SAML2 ⇔ OIDC Fed for general taher case of by GN* - *. The role of intl. federations will need a generic trust framework for that. The model will be similar - trusted by all. Apart from trust, everything is different; from tech to metadata federation. Some of that is native to the OIDC discovery & dyn client registration.
In OIDC there is an explicit metadata exchange method.
Trust req. most imp.
—

14^{50} Davide V / GEANT & AARC: (see slides)
"effective connection of RPs" in AARC
- In OIDC world there is
(each of fed spec. 1.0 revs) →
now: how to sign/create the chain of signing keys effectively & responsive.
↳ online signing service. (both discovery and client asset PKI).

Add to agenda
- documents needed?
- Sirtfi - RP binding.

EUGridPMA42.

②

DavidV/ there can be parallel federations – no model imposed by standard.
very open – no NREN approval needed.
- options are also meshed. bridge for federations.
- resemble SAML hierarchies with one trust anchor and all aggregated metadata
with one federation key to rule them all.
but it can be 'stopped' at any level, abc@Org.
both MD statements and signing keys can be by reference (URI's)

15[33] / Michal P: ELIXIR & LSAAI.
there are for now just a couple of clients. As it extends beyond ELIXIR
(cloud) service providers will be using OIDC – and there are many, esp
for all of LS. Trusted registration is needed.
And do it soon, before LSAAI kicks off. (RSN, Q1/Q2 2018, so soon!)
Level of trust by IGTF will be Org + Snctfi qualified.
RI specific stuff ("able to handle human data") will anyway be
inside the ESFRI's.
Snctfi & SCI would be good enough.
=
new now: RP's take an active role in federation (in ELIXIR it's user initiated).
interact with orgs.
The general model by DavideV needs ~~scale testing~~. Scalability tests.
- trust is more the bilateral enforcement of technology. but processes & procedures
or the individuals.
- change management. → rapid cycling of keys through refs URI's.
target ~15 min. , so you need HA/redundancy.
[- but you can trust pre-registered URL's (and you trust pre-configured https:--)]

16[22] JimB/ CILogon & SCI tokens. (see slides)
- analogy to trust anchor distribution. (IGTF signed distribution).
- policy and practices needed for XSEDE
- compare CILogon (OAuth) to SciToken (OAuth2) OAuth2. + scope access token.

SimB// Client registration: the RP should be in the 'community' (RCE) within the, say, RCS category.

↳ dynamic client reg in federation context → espn.

↳ Lo translate. "tags" into (overlapping) federations. Could be "different federation" (so there will be a set of IGTF federations! :-))

the 'can obtain (& mesh) federations.

need not be under a single root. → flattening is possible.,

adding to JSON is more complex (also DavideV).

=a single root is not needed

decide decision to RP (consortium)? fed per "owner" of the, say, RCS.

"one who owns a policy set runs a federation"?

-and with many entities. → decide via orgs.

↳ complexity? meta-data authorities proliferation.

and you then need aggregation of type of EGI, WLCG, &c.

↳ scalability earlier led to eduGAIN central.

→ scalability needs → O(100). @IGTF will be easier

actual OP's: <100 RPs: >>100k, but O(100) orgs.

17:00 Niclas / EGI&AARC & B2ACCESS: see slides

*Integrated presentation EOSC-HUB/AAI, describe both systems.

goal "scalable" & "trusted" from OIDC Fed.

now: here O(50-100), in near year O(100-1000).

then cloud services with many services per user. → oops. O(1M+).

current client reg doesn't do revocation or maintenance of clients.

↳ monitoring needed. → OIDC endpoints are public, and can be tested.

PRACE.

EOSC// - in EGI, clients need to comply with policies (EGI Sec Policies) via OpsTeam.
- in ELIXIR it's self-asserted.
also this needs to be checked.
peer reviewed self audits → hierarchical model, by org.
also an Eg. RCauth "feel" new and improved.

Marcus/NaTTS+ "OIDC-Agent": (see slides) → Use cases!
'oidc-Agent' just like ssh-agent.
potentially (#users * #devices) → O(1M+) clients.
Very appealing to XSEDE as well (Jim B).
one level of indirection by client-introduced clients (but that's out of scope of fed spec).
policy should be tackled, because clients are also (implicitly) services and can act as such. → limit to Access Tokens, could solve this.
IdP tick box if they are not techn capable of running a service.

17[60] End of day 1

2018.01.23 // 2

09[15] Remote people: Cosmin, Vladimir, Miroslav, Roberto, Miriam Pilkhyan

09[20] Cosmin // (ACT)
* AustrianGrid – no response. → email does not work.
will be suspended by next distribution. by end of Feb.
* RDIG still pending. Ask self-audit next week in Geneva. (ACT)
* German Grid: will be updated tomorrow
* UGrid: DONE (Distributed Rec todo)

09[22] Bouchra // MaGrid Updates: (see slides).
We RP's are now all located in Rabat – hard on travel, and many users are PhD candidates that leave too soon to be an effective RP.
Considering TCS for MaGrid use cases as well, but need eduGAIN connect first which is not yet there.
Nor SARIL issuance can work, but for O(100), but not thousands.
CESNET runs own portal using api, but that is more work.
- eduPKI → eduRoam only.

09561 Comms's RP's

relevance: OIDC is a value proposition. →

publicize: PEPR newsletter; BLOGS.

as OIDC Fed becomes more concrete → propaganda.; "It needs trust and policies"

invite folk from EOSC-HUB who are funded to do this.

scope should help: there was no alternative for RI/EI

and it's pinedria in orgs that will be the challenge for eduGAIN/REFEDS.

Targeted meeting for propaganda., and hijack PRACE sessions.

with a concrete pilot to show.

How does that attracts new RP members: they can influence the direction.

RP's can use it to exchange ideas and also learn from each other

(also sharing Snctfi and policy bits).

Who likes to join: Life sciences (but we see the IT proponents)

(ash)

REFEDS/SKA. → part of WP 6.1. } needs other demonstrator operational.

LIGO/Virgo → for OIDC

Get the message across that IGTF is taking things up (and not going away).

① → - for the tech demo OIDC: Mischa + Jouke + SimB (~ 0.5-1 FTE?).

- for propaganda: EOSC-HUB + PRACE effort, and invite these communities in there.

④ → * WISE community: dedicate time to Snctfi & OIDC & policy bit for SCI session.

(ACT). talk in plenary about the IGTF OIDC fed.

- for propaganda: Sara Coelho - describing this to her also helps to clarify the ideas themselves.

③ → also involve GEANT folk & Laura!

- talk at I2GS & TNC in an PRACE session.

- GEANT Connect magazine feature or article?

Invite also TAGPMA. (SimB). + Derek.

OIDC Fed might attracht funding also for Latin America (and Rest of APP)?

(ACT) - talk at APGridPMA.

- PRACE InfoShare, - poster @ ISCG.

other communities: natl. projects (like Daphne in the UK)?
based on response from (AARC) surveys (like on AUP?). | Jens, Ian Kerr, Mariam P., [illegible]

10[57] // Coffee // 11[26] Snctfi. [Remote: + Uros, Nuno, Roberto, Hannah, Jens, Reimer, Miroslav, Vladimir,

Snctfi: offshoot of SCIv1, published Apr 2017 and now in TNC17 proceedings
trust in RP's is getting more important for OIDC Fed, for O(100) it can be assessed, but not O(1M+) services.
so assess communities, not services.

Snctfi implicitly requires Sirtfi.

RP's more important (see before), like in EOSC-HUB. Vision of EOSC-HUB is to be a hub with very many services and communities; including thematic services.

Policy development kit also important for EOSC-HUB, ~~also~~ besides AARC.

EGI-SPG has an expansive set. Work items of EOSC-HUB.
- alignment of AUP's
- GDPR guide lines
- VM management in clouds, for 'hierachical' service offerings (VAR's).
  beyond VM's to containers, both end-users and micro services, or a low-level job, or offering services from containers.

"PDK": from NA2 AARC: focus on Research Communities for federation
as a basis use ~~feature~~ SCI & Snctfi for each of the components
management of docs: stay where they are for most but allow branding with logo's.
Templating approach (? track with GitHub? :-)) { attribution to projects will be fine by coverletter

morph SCIv3 into the policy development kit. → WISE community workshop.
group by themes of EGI SPG page.
priority: start with community policies and the AUP
also feeds the training needs for NA2.

PMAG

PDK// How much commonality is there in the policies? AUPs can give a hint.

in many cases its minor changes, but some are very different! (7).

-Helmholtz Federation. as sacrificial lamb. - they need it ahead now

-EOSC-HUB needs to have a framework to merge EGI and EUDAT

EUDAT also needs to devise the policy anyway.

-for, eg., BBMRI a layered AUP would work

-for EGI all statements are required.

an RI should be able to say "we are compliant to SCI v2 and meet ÷ —"

and meet a baseline profile.

* elements can be OK, to be also a basis for a risk-based model

* small communities might just take policies as-is!

For services: for the review - structure of the kit (SCI based + grouping based on EGI)

- community centric Snctfi policies

AUP, comm sec. pols (2x)

data protection: we need CoCo v2 results (would that work?)

application-level data protection is out of scope, but a user-issue!

for "us" stick to low-risk attributes.

PDK: → clearly define scope to infra-ops. → does incur risk. /opsec

Model

SPG: Documents wiki

Goloc: AARC Policy shortcoming: google doc Workflow

(the goloc is a rough assembly of ideas & refs for now)

- more abstract categories. →

- for adoption: you need community to do a risk assessment and then decide on which policies you need, and what to tweak.

- flowchart model for risk assessment by communities to help pick the right policy set

- look at stuff TF-DPR (Andrew C) did for an example.

- WISE Risk Assessment Working group. RAN-WG.

reporting (72 hr data breach) would that work between services!

PM42. (8)

join WISE for getting risk going.

12:30/Lunch//16:00

16:00 Sam V / AUP Policy: (see Wiki page on AARC Wiki).

AUP clauses matching with EGI as a basis, ⇒ EGI/EUDAT/ELIXIR are similar.
with the PRACE one being different.
comparing with the BBMRI one to see an extreme
and the ELIXIR one has some community-specic elements.
mapping shows elements that are unique.

- Where does the user see the AUP.
  - ↳ in PRACE the home site takes the role of 'community' for AUP tickling.
    the "peaceful" in PRACE would probably already have been covered by the project review
    so is a duplicate, but lowers risks for sites...
- scale of analysis: lowest common denom. then build on it by hierarchy.
  - ↳ come build identical words for the minimum ↳ to allow X-ET use
  - ↳ categories on top of that
    - ↳↳ have a guide to usage of the template.
    - ↳↳ have a baseline that "should not be changed" and then allow to extend
      (but not degrade :) the items or add items.

But the baseline will then be harmonized.

getting adoption with infra's also via WISE. to get XSEDE (and OSG?)
for Europe: 1dh via BBMRI NBS, then EGI (end of Mar after WISE).

Site AUP's are usually overly complex because they (have to) allow private use.
(Helmholz does not have one yet).

Before WISE: - joint discussion AARC - EOSC at all meetings.
- strawman AUP (maybe based on EGI). with EUDAT/PRACE involvement.
start with structure. ↳ Ralph

@WISE SCI NG - involve more people.
March - formalize V1
in time for AARC2 review.

AUP/IanN: Uros→training pretam. plans, but people don't know what they want.
(14:51)

- Incident Response
- Assurance Profiles.

Scott/ NIST800-63v3: (see slides)

63D is not an afterthought, but was not ready in time for incl. in 63C

- Why is federated assurance different?? real-world alignment because of flexibility and interpretation prudence.
- flexibility may lead to confusion - but disc. on "real" front-end number single scale, which was discussed but failed.
- Analysis to be conducted with OIDC and SAML 2 federations, like e.g. and eIDAS.

For making final, over-all decisions you need to consider all vector elements it's still early days for understanding.

REFEDS brought out "identifier", and "association freshness".
sociologically, 2-3 is optimal number of choices. 4 is too much, 1 too simple.

Too many profiles now? many in RFC 6711 levels registry.
REFEDS adds 2, AARC BPA adds 2 texts, would have 4 in IANA.

What risk inspires which level? → risk levels are (expected to be) in there
(15:43) looking to -53 should have been there.

16:10 // Assur. Assess Matrix (DG) // review now in v0.3.

RFC §4.2.4 non verified information. - one way technically to express
| which elements are verified if not all is verified.
| but unverified info may be useful (display name, eduPerson or so)

not addressed by IGTF AP's. (yet).

- Links to idea for per-attribute assurance (and provenance). c.f. Sens-T

in PKIX embed policy object then need to assess :((
in the Community membership policy, also did not address -- implicit assumption that that data is 'correct'. But in many cases much data are self-service editable. But RP's expect verified.
· in RFC3647 3.2.4 → needs statement in PP's. !

17[03]// Karlsruhe meeting May '18 23-25 May lunch-lunch.

Mel 24/03[20] Marc → new PKI is now there. CNRS wanted to terminate and now moved to ministry. New GridFR CA as actually 4: Root + 3x ICA.
classic PP; based on "openxpki PKI" operated by the ministry.
Enrolment and it are still the same, with same RA structure.
signing machines are all at the ministry. Only service portals @ Renater.
now: with robots.
TCS "was not the chosen solution" (because of operational model FG & TCS@FR).
only technical changes (3x ICA and backing software) + HSM.
- same namespace.
- reverse proxy in front of online CA. (also for IPv6)

OK Approved + distr.
in next release end of Feb!

—

Dave// RCauth.eu.
because of CRL signing needs option #1
also used by others, but typically in A-P standy. HA.
#1 chosen as OK.
- partner leaving requires notice long enough to cycle keys of ICA.
(local backup via HSM will remain possible) → key destruction impossible
⇒ Leaving must be defined in CP/CPS.
⇒ define transfer process in advance.
legal entity: consortium with 4 legal entities
for embargo purposes: may be declined to non-affected country?
revocation is a risk → but no partners are at risk at the moment.
⇒ "contract" between ops members → Moll

regular updates to IGTF

1[02]

EUGridPMA 42 2018.01.24.

11:00 Coffee

11:30 Germany Ingrid. Selfaudit Gridka-CA.

- IPv6 will be done early Feb '18
- SHA-1 for a root is still fine.
- CP/CPS has been at the same since 2014 →
  new CP/CPS in Karlsruhe meeting.
  ↳ send to reviewers IanN & ScottR.

CAA req. from UniBonn. use eg. "grid-ca.de",
but its not required to honour CAA by GridPP CA.

11:40 / Suns' Soapbox. "sharing experiences"

we had CAOPS, ... also about software for CA's like OpenCA mods &c
for new stuff (like IOT) introduce EC keys. or interesting linking
to network management system (CERN).

can you think of "CA as a service"? copying happens anyway...
like plugging in IdP in Pathfinder (Assent) CA.
↳ assert SAML2 attributes for Dirkfy or Birch in the result
from the moonshot exchange.

why trust this Birch CA → audit, or trust based on 3rd party or
other assertions. Or a legal letter from the org.
who signs the compliance statements? Legal or a clueful person (admin).
(using reforms.-)

should their provisioning code can be shared?
many CA's do similar things like RCauth, Pathfinder, &c
but MyProxy with moonshot does not work with pathfinder CA.

practice of sharing "elements" (code, snippets). → we need a sharing forum.

(TCS docs as example - don't need to be signed by legal.)
how to communicate? more meetings is not an option...
don't loose the expertise on CAOPS list (iron-IGTF people).
send mail to CAOPS. → links to existing repositories

- who to volunteer to kickstart CAOPS again?
  maybe others on the caops list?
  not that many tokens.
- on redmine add links to github repo's.
✓ - people with code should publish
/ - and add link to it on redmine.
—