pma48 Prague meeting 2020 01 22 ①.

Present: Reimer, David, Sale, Jon C, Sona, Sverf. Maarten.
David f. David C, Jan N, Scott R, Uwe H.

Remote: Cosmin, Lidija, Miroslav, Mischa, Hamah, Nuno, Ronald O,
NimrotAl Sogami, Jens, John Kewley,.

13[30] // Davidf + Jan C - welcome + agenda building.
note takers: Jan.
~~Rbaanth → ...~~ ee.
TCS → wed. en co → the morning.

13[55] // Cosmin. A/A updates.
Austrian Grid → removed in 1.103 → gone.
RDIG → 4 years old now!
suspension process to start. → and inform RP's.
issue formal notice and inform WLCG.
+ time line. send updated cp/cps before Feb 15
or suspend in next distro 104.
MD-Grid: update CP/CPS to match root time period of 21 years.
UKeSc: did the new CP/CPS get sent? ask Jens.

14[15] // RATCC4 → see slides.
to get better improvement write report, sanitized
ACT. categorize., but no naming.
the failed ones merit a test again. after updating.
and on repeat failures may result in going public.
SCCC WG @TechEx → added a crisis mngt. item as well.
to be discussed at TIIME.

14[50] // EISAAC Salone — AP grad PHD see slides.

CNIC + SDG did send mgs on RPKI CC by end of October
(but outside window)

15[00] // Tea

15[15] // David J — TCS GL 5.1.6

Sectigo automatically via Common accredited
IGTF server should be ok since CABF exceeds Classic host
and for personal / Robots the info has TCS CP/CPS anyway
and does not change.

Quick review of Sectigo by Scott & Ruimen
and send redlined name changes for TCS naming in TCS CP/CPS.
sectigo.com/legal.

16[45] // TAGPMA Derek → see slides.

= Thu

09[22] // Maarten + David J - GN4 En Co. Review of PY1 actions and achievements.
+ outreach → FIM4R and a presentations and for ISGC security WS.
+ Review the structure of GN4-3 for information for the T&I activity.
(see list of topics on the Wiki of PY1 activities)

SCI evolution: SCI assessment sheet done in Karlsruhe and use EGI as
an example. put that in the spread sheet and got lots of
2's and 3's. (some). But Uros has most of the effort but
other infra's don't have dedicated effort to contribute.
Uros will upload what is there.

New work on top-level policy work, and abstract trivany specific
policies into a higher level policy + implementation ~~effo~~ measures.
as an evolution of the PDK.
Incl. a structure paper. (publ.) → will be WISE

EUGridPMA 40 Prague.

(EnCo review) (3)

SCCC-SNG: see slides from RATCC4 and the Wiki.
website needs to be updated. → ask Sigita for NISE WP access.
wiki agenda is working, continue with more infra's.
Pgk: encourage others like XSEDE, PRACE, EUDAT, —.
encouragement does work, → see eg how In Common and 'baseline' in 1gt
and they did that with ~1200 hrs within the year
so with the right encouragement can be done.
* SWITCH already does those challenges → invite SWITCH and to contribute
and register on the Wiki. → DavidG.
(RACT).

Assurance Profiles.
- improving REFEDS Wiki pages with guidance → ongoing
and get logo's for the profiles & RAS + coco.
- IANA 6711 done → see doa-profiles page.
- plan one session at TIME unconference, and prep for ISGC.
- Duke joined In Common assurance group.

Next: - trust mark/entity category discussion. Poll outstanding: open!
"are you in favour of signalling a capability to do {SFP, HFP, RPF*}
to help in selecting disc org pages. → user experience.
video conf plans in February.
- - more FAQ (like steps from DimB's shut) to explain what to
do and how.

SIRTFI: - eduGAIN sec involved. no longer a big response handbook
but much more practical procedures. Borrow idea from NLCG
and EGI but needs to be transformed to a distributed environmt.
- take some steps back and take generic perspective by stripping.
Uros + SvenG: develop simple doc, 1-2 pages, which the
operator can put on the wall. Ordering of actions is important.
esp. in timing & sharing.
Comms: security end-points (like federation-level) not well-known.
try a Comms challenge, even using generic contact.

PMA48 - Prague.

SIRTFI : Soute develops a comms mailer/check framework V2. - also usable for generic email lists.

AA ops : Hannah will call in later, AAops for the proxy.
edu TEAMS check → will work with AWS.
with AWS-HSM and use e.g. 2FA for the console
and deploy the priv separation features that are already in AWS
this actually should work.
comments welcome ⇒ either now or dedicated meeting
to get an explanatory version.

PDK → merge with SCI work plan? ✓
discuss at PMA and SPG meetings. → but get concrete.
(ACT) Maarten, DavidG, Dave K.

FIM4R: meeting at TIIME.,
blogs on fim4r.org. + case study! (Hannah).

at TechEx 19/ACAMP: some like LIGO/ScottK are giving up on R&S
and do their own, → too slow takeup. maybe RID as a global
attribute store.
should FIM4R should reflect on this? and avoid the non working bits.
so where are we now?
OIDC fed for Snctfi → see slides on OIDC fed.

Outreach: AARC leaflets @ ISGC guerilla.
spread at coffee &c to get new communities in
and talk over coffee.
~~and~~ talk to APGridPMA meeting, but there gouged no access :(
(ACT) are there FIM4R leaflets?

PHAID Prague. 2020 0123. (5)

11:30// Sale-assurance.

presentation for ISGC and in paper. Structure today.

(AC) re-use diagram from AARC-IDSD. publish IDSD to Zenodo.

Paper: pick a few use cases, with examples to show how the profiles work and what could qualify

it's the SP that needs the assurance. pick a medium ~~to~~ soft one?
and a low for 'canned' application. (social ID + a proxy)

only the biomeds (may) need higher assurance: ← AARC wiki
but hardly any RP has done a full risk assessment.
for the medium case use NLCG.
for lower via canned applications maybe DeNRIR + VO portal/policy.
take inspiration from the FIM4R case studies → is assurance defined there?

include ~~AUP~~ acceptance in the input. And need for 2FA (also cost).
although for banks ~~de~~regulatory pressures pushes for MFA.
for MFA → step-up as a service (like SURF, or eduTEAMS)

Freshness. → ~~processes~~. processes needed. The biomed use case for
ethical constraints / access to datasets pushes for 1-day, which
is overkill for others where 31 days is fine.
* ACAMP/TIME discussion slot? *

provenance of assurance in a multi-proxy environment.

[12:37 lunch]
14:04//

14[th] // RCauth - Sens. Mische.

Roadmap reported to EOSCh - but got stuck on key distribution.
pending exchange to GRNET now that HSM is in place.
database sync, in long term VPC over a lambda, but initially
do a VPN
needs completion by end of Quarter (so end of March)
Governance is now fine
Q2 2020 will see monitoring and alerting.
Self-audit certification by Q3 2020 to report results.
then investigate usability of ~~the~~ the front-end portals.

can proceed with distribution - following the agreed plan.
means of communications are in place (including keybase.io
distributed vaf/ can be done with simple HA without source ip binding
~~since the Shib is~~
only a back-channel would be complicated.
HA for Checkin is active-active using memcached for SSPHP & Shib.
-

14[36] // Mannat - AAOps to NCLG (see slides). see PMA site and AARC-G048.
On VOs ok? ok, as long as all controls then meet the security
requirements of the most sensitive services.
#2 is there to protect against scenarios
(like putting in RBAC on AWS accounts, and make
sure that untrustworthy services are not colocated with
secure ones).
Common attack scenarios like hypervisor exploit from
guest., or compromise of the mngt of the platform.

(7) for the token lifetime, this should apply to the access token.
since the refresh tokens are ~~re~~ revokable. (and bound to
the scope).

PMA48 (7)

AAOPS/Hannah for OIDC SWT's signing key either from OIDCfed but for non well-known endpoint & + (preferably EV). TLS.

this should be documented in an FAQ for AAOPS.

15[15] // Uros, Dave - SCIv2. assessment.

push through WISE to other eInfrastructures.

(? and involve eduTEAMS in WISESCI assessment work as well (e.g via Video))

but then eduTEAMS is just the proxy...

new 'infrastructures', such as CS3 for EOSC, or the EOSC supporting projects like Synergy or Pillar.

visibility of assessments? ± recall the SCI WG and have a call.

to define common direction for 2020+

*how to make SCI authoritave for fostering cooperation? WISE

*most use is actually to the infra itself based on their own assessing.

with support ~~from~~ from the WISE community.

SCI WG → evolution of PDK actually fine here?

⇒ Dave K to revamp SCI before the WISE April meeting.

15[30] // TED.

Roberto leaves PMA by Sun 31st 2021. ☹

16[03] // Dave, Ian - Top-level policy comparison, - did we loose elements?

EOSCH alignment, but when exposed to UKIRIS comment came back that too much was taken out of the original EGEE/SSPG version -- it was too content less.

* the "additional policies" list is considered too exhaustive and long.

and -- they all have to exist.

split to implementation measures, but the (top-level) policy ought to be stand-alone readable. And a lookup-list like the EGI evidence-focussed wiki as a way of finding the impl. measures

PDK evolution (IRIS) // Ian, Dave U -

Boot strapping a new infrastructure.
need AUP, Privacy Policy, and the top-level policy.
then on to community management
but the top-level policy needs to be able to stand alone for a while.
this means it should keep some stuff in the top-level even if it's duplicated later.
Eg. also for EOSC you need some req. on users, or communities.
but the sections on network and physical security are too specific instead.

Initial fix for UK-IRIS will be soon, and can inspire updates to PDK.

Tomorrow: agenda

next meeting: Garching May 13-15 noon-noon.

Utrecht/Amsterdam Sept 7-9 noon/noon (ofwel H220 ofwel Surf 3.4)

17'14 // end.

09[20] // Agenda building.

09[30] // Dave L - policy guidance for RP's. (and EGI in particular).

① [see notes on CoCu HDJ → abstract based on risk assessment of the services at the RP's services.

"don't do harm" → top-level policy for the federation.

top level policy should also add policy on a per-service target.

but try & prevent SPG to become the court of arbitration.

but the SPG can make advise to management, who then makes the decision.

now start writing :)

② DP Coco → meeting with Dutch AP happened on Jan 20th. discussion is also around the monitoring body. More at TIIME.

- For EGI federation, rebrand the WLCG privacy policy

About 'good quality' and 2FA? not all social ID is good, and you don't quite know if the user had 2FA enabled and used with free and anonymous SIM cards &, google actually is just non-reassignment. Back that only for @gmail.com identifiers.

10[15] // Hannah - OAuth trust. - [see slides]

many communities moving to others, and that needs signing. Today via the well-known end-point.

&

If you got the signing keys from well-known https, then either the URL must be really verified through either ORCID, or use EV or so. Or passed via other authenticated means. The URL must be good, and verified for glyph collusion and phishing and such

OAuth trust

| in a delegated scenario - see QQ52 token exchange from AARC. | discuss on AppInt.

Here you need an expert group to suggest 'best practice' for federation.
and IGTF can bring this

you want automated services almost P2P, but you have reliance on assurance. And that is what LE/DCV does not give you.
you need to add identity on top.

IGTF can bring that capability. different policies may apply.
policy statement and marks in the metadata.

The MDSS can assert policy URI's like trust marks. and incrementally add them - so RP's can filter on these.
The minimum would be a good well-known end point and key sanity. (baseline) + sec. contact
- Then add AAOps, Membership policy compliance &c comes later.
So kind of a mix of TACAR and meta-data marks.

IGTF will sign collection of orgs for AA's token issuers

will initially be a handful, one per VO or so

Put in oidcfed.igtf.net, put these in the mdss including a uniquename and the uri for the end-point for the key.
in the same kind of format even if manually curated - and at least it is not ad-hoc.
With a script to extract the data and install locally. from cron
* initially just distribute trust anchors without policy qualifiers.

model foresees ~O(100) OP's and ~O(50k) RP's, so it is larger than just WLCG.
in the end also direct link to end-resources like cloud & HPC's, even if WLCG now only uses it for the payload.

for the RP's, one would also conceivably fully trust that it's the right URL. If jwks-keys are a uri, it does rely on DNS being OK. but if DNS is broken, one would need (fingerprints) of the signing keys inside the signed federation metadata.

without OIDCfed, everything hangs off DNS, esp. if allowing DCV-only. it can be scraped and scripted, but one needs OIDCFed-like or out of band,

Checking policy OIDS to ensure OV/EV on the https url cert. use same mechanism browsers use (require the "O" attribute +publictrust).

so-a known uri could be fine if combined with "O" ~~++~~ either
(public or IGTF trust)
- or embed (fingerprint) of (org-level) in OIDCfed metadata.

but maybe start at least with a list, ~~eventifi~~ from trusted source, even if it contains just url's (that then could be DCV-only).

the risk is that personal data are released to unauthenticated RP's, if the AA accepts DCV-only. For CERN, that might be an OC-11 violation. for users that then authenticate at the RP: in the end it's a risk assessment.

start with the oidcfed.igtf.net service and add afew AA's (OP's) and RP's as they emerge.

11:33 // Jens' Soapbox Soap<>box

Story of time and false dichotomies.

history of languages standing with COBOL up to 90 for 40 years
many things are equally applicable to skills, or protocols.

"90+ % of the financial transactions involve COBOL code in the US"

*should you break compatibility or adapt to "latest thinking"?
Perl & C emphasis stability, python & ruby adapt to 'latest fad'.

so for the IoT? vast range of interoperability, latency in roll-out updates,
and -- complexity has to go somewhere.

so is SAML vs OIDC also a false dichotomy?
or X.509 vs tokens, similarly a dichotomy... you still need auth!.

so what about the next 40 years, when we are all in a nursing home?