AMD 43 Karlsruhe (1)

Present: Scott R, Melanie, Ingrid, Walter, Hannah, Dave K, Ian N, Uros, David G, Valentin, Emir, Reimer, Marc, Nabil.

Remote: Eric Yen, Cosmin, Jan C, Lidija, Miroslav, Feyza, Nuno, MistaSalle

ext. items: - January meeting in UAE?
- new CESNET CA4 → friday morning.

13[20] / APGridPMA: usually colocated with other meetings — see slides
increased interest in OIDC and PARE

6-10 Aug @ APAN in Auckland.
31 mar - 5 apr 2019 in Taipei @ ISGC (Sun or Monday).

next IGTF AHM in Taipei (mar 2019).

13[39] Cosmin / SA status:
- GridKP: Ian's question still pending.
- RDIG: Dave to follow-up. (OCT).
- Austrian Grid: will wind down within ~ year or so.
to define dates for termination. last was 1 year.

new ones this meeting

13[49] / Valentin, RENAM self audit
- current CA root expires april 2019.
- country 'small enough' for always F2F.
- RA also only validates domains owned by user's org. (almost always .md).
- new CA available online (ftp is in presentation).
and the CA root is SHA256 signed now.

audits review: Feyza, Cosmin.

14[10] / OIDC. intro.

Mischa - even in OIDC fed GN4 working group things are still in flux and training still needed.

- mobile clients (seen as prime use case initially) are not as simple as initially thought → may get out of scope.

- SNSPHID → see github for example, based on acr's for enrolment. and how to get the client ID → looks a bit like an EntityID

AIDA3 - Karlsruhe

OIDC

- out of band profile being worked on by Roland.

- For us: how to get client served.

the 'between infra' use case ~~xxx~~ is needed to support cross-federation. but services will move quickly so some stuff is needed

SPFE will be replaced likely, but will take looooong time?

the urgent stuff is the simpler one with a proxy.

The NLCG ~~claims~~ AuthZ work is more about claims, not trust.
the standardization of claims is not about the semantics. and will likely not be x-community.

Andrea's IAM model for using tokens in OAuth/OIDC will be used a lot likely.

distinguish the optional bits is useful.

The trust is independent, but you have to be careful who to trust (e.g. a phone cannot be trusted, ~~xxxx~~ so linked to the user).
unless in combination w/ trusted exec env + signed apps.

Hannah + INDIGO IAM → expand a bit? complementary to static efforts
↳ and it would need to be implemented in IAM. Next meeting.
alongside CheckIn.

and use WATTS as a test client. doing dyn. reg. now with IAM, but now needs to know which IdP's to support?
the "which IdP's" you could get from the federation.

(DEMO). use MP(OAuth) and CILogon as OP → and then use a web page for us as an example.

policy: templates for OP (and RP) policy docs like RFC3647.
pressure on OP's (proxies) since otherwise their users will not get services of RP's.
for RP's, pressure comes from GDPR and need for attr. release.

- identify minimal set of policies.
- express in policy-uri's in metadata.

PMA43

15:45 / Derek. TAGPMA. → See slides
"It's not an OSG implosion, just a redirection of funding".
"just streamlining and more agile".

also see Brian's presentations
- but: DOE labs can _also_ go to InCommon. confirmed by SimB!

Scott: need is for private (not public trust) certs.
LE long term sustainability model is to have higher assurance banking to pay for the DCV orgs.
so the checking will require LE to be in the community - directly in competition with their sustainability model. ⇒ b/the AuthN bit

DG: their technical profile violates their CSP extent.

Derek: they are also not likely to show here.

(The position paper was internal (and has 'interesting' way of assessing risk).

! - DOGWOOD + community for clients works because of dual signature ("VOMS")
with an attr. statement from the community.
for hosts "in the community" you would need a proxy as a credential on the server end.

[DG: reiterates the already-known risks] validation, BGP hijacking, inability to link key to entity unless you essentially do a full CA again!

TIGPMA working group needs a clear mandate → Derek.

real question: do you want to put everyone at risk for the idea of one.
⇒ InCommon is much cheaper!

and the RA infra (which they can keep anyway) is the expensive bit.

and 'opensciencegrid.org' (URN machine) is free!

TCS: useful focus will be high assurance, so EV / EVCS DC. → DCME

Germany: locally LE blocked by default, opened maybe on demand "nightmare on Elm street". : no traceability.

and you only need 30s of rerouting.

- if we do to agree to a profile, what about accreditation?
For the no-revenue stream of LE?

17:00

other means to assess trust. And why would LE be different from other DCV?
and prevent a split of trust world --

09[15] Andreas H / KIT welcome.

09[29] PDU@SCI (Hannah). Scope 10 now mainly Research communities but the idea is to extend it more also into e-Infrastructures.

answers a question posed to PARC by the communities.

acceptable assurance: pick G021.
flavours based on RIR? or are examples? like some REG options.

limited # levels → and consultancy:

try interviews first then abstract a flowchart from it.
- targetted guidance GOLD on the LSAAI
- try that also for the HDF
from these 2 abstract the pertinent questions?

even the PDU was not read by the prospective communities — not the right people, or they consider it too long.

But: you need endorsement at higher level of mngt.

and adoption of policy is not enough, you need associated procedures as well → role for e-Infra's?

and now EOSC(Hub) will also have to be successful for smaller communities.

EOSCHub → new action on AAI solutions as part of "talk to communities"

⇒ addding 15-20 communities. (use cases, size, kind of data).
but now focus is on technical issues, yet results may inspire new discussion on e.g. assurance.

survey will be sent early June, with discussion in June on role of AAI for communities.

questions are very explicit to elicit clear answers. (on authn, registration, &c).

these communities → results also to PARC (SIRTFI).
can they be contacted again?

in the diverse EOSC ecosystem, services may be community-based so their policies may (and will) not be those of the generic e-infra's.
You cannot impose 'external' policies in that case.

FIM4R policy-aware people can join the policy team

start with a policy checklist. to determine what is needed in a community.

↳ then add procedures as a questionnaire.

PHA43 Karlsruhe.

(5)

PDK)

CTSC has a checklist on risk assessment, and "compulsory for large communities"
but not assurance usually.

(A) for small communities: develop a 'story' to show how policies help as many grid controls.

make sure the licensing is done right to ach sources.

(B) for EOSC hub now is the right time to talk to communities

→ add to questionnaire to ask contact point for communities.
and ask FIM4R.

— other policy elements added → see slides

10[15]

Break

11[14] PMP – see slides on agenda page and real-time editing
- add preamble.

– the citation requirement is confusing and also questioned in general (see ...de request to re-use).
so should/could be in a more specific agreement if needed.

– every service has to have a privacy policy, and [the community]
should maintain a registry (no more than 2 clicks away).
like for the LMMI.

15[15] SRCE S/A Emir: see slides — done update.

GDPR → legitimate interest for keeping records
but performance of contract to get the name in the first place.

example use of Legacy Dutchgrid CA – re-use balancing test.

simpler version fine, but need to keep 14 points

look also at DPCoCo

16[45] AAOps/Hannah

– "AP" term is in AARC BPA.
– inline edits in gdoc cern.ch/go/~~....~~ 6P6p

17[15]

PMA43 Karlsruhe + Jens remote.

09[15] Nabil NaGrid. [see slides]

B2→ BC/DR ? → passphrase sep from key!
↳ related to key distribution, Jens.

business separation between NaGrid and TCS @ Raiffeisen: community arrangement.

Ⓐ Reviewers: Walter de Jong, Ingrid S.

passphrase should be separate from encrypted key split! Even across personal safes. at home. is better.

"separate from the private key"

or use the comming of CA's as an archival service. ("manual blockchain")

09[2] SanC/ CESNET CA4. see slides.

- ~~[illegible]~~
- see trustee was useless as the key always had to be in the HSM slot for nShield HSM.
- EC is fine → equivalent length. (256 ECC bits). works in TCS.
- is it good to mention GDPR in the CP/CPS? notice should work. linked from the form and on the web. active act and log the action.

in EIDAS: you have to accept all if you accept one, but accepting one is not required. But you cannot discriminate.

→ only required for interaction with govt.
but you have to by one from a TSP (Trust Service Provider).

authN in ID card is there by default, but signatures are a paid add-on.

but if it's easier to do the QC certs, then it's fine.
and they meet ≥ Kantara LoA2.

ID check in combination with reg form. which has affiliation.

plan: - CA4 in 1 September release

Ⓐ. - review of CP/CPS before: Emir + DavidG.

PHP43 Karlsruhe.

10[19] / Sens RCauth.eu key distribution.
link to document
-option: buy (not)HSMs and use ejbca to sgnc the package.

-having different keys is expressible to users and distro.

-additional options: same HSMs.
-but etoken is too slow.

- new PGP party for key exchange over video?

- option 1 is voted out, 1b means relying, so /could/ be done.

- private key transport for bank purposes (BonC). split and sent in 3 pieces by 3 different methods.
should be sufficient for us. live video stream interactive.

have maybe 2 methods should work. with existing key.

should be fine. esp. if you split and then encrypt the part.

3 separate inputs and get on a video call to reconstruct.

- or use LUKS containers of arbitrary size?

option 2 accepted.

[10[52] Coffee] [audit of CA room & more] ✓

11[21] DCV (certbd) with Sens.

- cost of good alternatives is trivial, and now accesible for DoE Labs.
- in the end the choice is with the RP's, but then you don't want a split world.
- join [redacted] mailing list! on.
- CT logs, means you have to check on connection. to positively check org endorsement. Filtering for our community.
- CRL checking is done universally and done in our community.
- beware of changes in software needed. 'developer bias' on rollout.

11[43] Sens' Soapbox. IoT + ECC with check of integrity of microcontroller.
Sens' project proposal in Barcelona.
(and ECC is still secure) Tomcat/DogTag exp. server in container setup and then dried.

"Why is everything so complicated" esp. CA + tomcat in Docker container

software storing: change your requirements, not your software!
and community is important → ejbCA is most used!

primeKey virtual appliances (and even have eTokn as PKCS#11 provider). Easy to move.

(+) more work needed. → see need it simpler ... and shared!

and docker makes things complicated. Not a magic bullet.

collaborate of new CT like soft nova? Not urgently needed now, but maybe later if useful.

—

Next meetings:

+ September 24-26 tentatively in Geneva.

+ Jan 2019. Abu Dhabi runs the risk of low attendance.
so discuss more.
other option is France (Marseille, Grenoble, Paris or Lyon or Rennes).
maybe 21-23 Jan 2019

—

12.14 Closure.