49th EUGridPMA Virtual May 2020

Present: (26) + Mirvat, Tan K + Eisaku
+ Dennis vd.

13^47 · Eric
→ 13^50 ✓ see slides.

14^00 - different emirates had different travel rules. DT was national security exception.
incident: one of staff of the DC's tested positive → for 3 days stand down to figure it out and be tested before coming back on site.
Day before lockdown: OCSP/CRL preparation.
OR split A + B team.
holding up fine!

Adrian: ~~make~~ ~~[illegible]~~ ~~bad~~ delayed.

Anders: got excemption to update CRL. 2 user, 2 robots, 2 voms + 3 hosts.

Cosmin: only partial lockdown, can keep going.

DutchGrid: not locked down + natl. crit. infra. :)
+ changes to CP/CPS
CERN: mostly ok, access would have been possible if needed
UK: design. key worker, access could have been done if needed
ARNES: designated natl. critical service. :)
LIP: could go if needed (CRL based, users can wait). rest pointed to TCS.

14^15 Mihael: SisuID + remote vetting
focus: ID proofing.
↓ 14^35 nationality → ambiguous.

(2)

* like gov azure level authentication does similar things with 'scanning' photo ID and photo

* account linking remains a separate risk.
  may be some heuristic.

* in NL this + linking with social secno gives substantial.
  the linking using BSN also worked for banks.

* the app will become the 2nd Factor for the SIDN OIDC provider.

* for CERN: multi-factor reset has the same need.

  how much of this is data management done by SIDN that we should have to do, e.g. in GN4+?
  the system is open source, but the photo matching is done by a commercial provider.

* SURFnet is doing similar things with ReadID in the TOI Incubator?

* SidnID will soon be reading NFC. Next the phone could take a video to do liveliness check

* Business model: ELIXIR is actually investing.
  even if using commercials: Signicat, Innovalor
  or develop for R&E

  not only NREN's need also RI + eInfra to join otherwise you get national differences that are nonsensical for remote working.

d
11/57

15[05] / Sens. Remote Signing. → see presentation for consideration.
software staring?

for existing online CDS it's easier, just like good
pre existing BC/DR planning.

Threats: loss HSMs that have remote heads. for encrypt.
and a copy of the DB backup can be in a more
accessible place and sync back later.
now what is the spend per subscriber?

Remote voting now.
UAE already.
UK + NL + BI
interest in Latin america.

16[00]

16[05] Derek. TFGPMA. de Blicles.

16[30] Cosmin. RDIG → system needs to do something new.
MD-Grid → Valentin working.
UKesc → OK now! ✓

Thursday.

13^{37}. TCSG4 (dalled)

ECC: openssl probably works, most recent java works.

Argury Misch, Uros

↓

$\underline{14}^{05}$ RCauth

presentation of final setup in the autumn.

↓

14^{19}

Maarten. T&I EnCo.

It's hard to pick up AARC Stuff and then figure out what to do is complex. (e.g. software to use).

AARC inaction is too much just a shim and does not tell what was actually done.

"subscribe to updates" button on the AARC site

(Hannah) . * software or service?

* doing it right is nontrivial.

* "but how you get keycloak"

✓ show specific guidance for configurators/with examples in XML/json

+ decision tree ⇒ Hannah.

14^{43} break → 15^{00}

PMA49

15:02 David C, JanN / CMMP* + PDK.

the current [illegible] level in the [illegible] seems [illegible]. Chris explains it was Sirtfi-based and what is needed in that context only, so only defined an index.
so it was not aimed at EOSC & e [illegible] infrastructures.

CMMP: towards one, but for mid + large comm's
for small comms, the contact is the PI
↳ and write that in the granting letter
↓
scoping, clarified in the preamble.

(doc editing) see link in presentation.
↳ contributors under WISE → all folk + Maarten + David
send to WISE list.
add guidance, since there are no details any more inside it

Friday 13:30
13:34 // Dave Kelsey SCI → broadened to all future plans following from the April WISE meeting
☺ SCI V2 does not actually mention federation ("eduGAIN" style)
prioritize SCI groups, with community thing first.
actual feedback (like from SLATE) is very useful.
[Chris + Tom.]
Will Sirtfi v2 be incorporated into SCI v3 (but timeline is not defined yet, and make SCI v3 just refer to Sirtfi v2..
+ focussed tasks now on updating first.

13:55 Sirs // Soaph. → groups discussion, interoperation and new communities and committees.
is coverage complete and distinct?
do we lack elements? are they in "the right place"?

it looks like an impressive number of committees, but only few bodies. Is that actually a useful impression.

—

activities scattled across elipses, so how to find out what is going on, and when?

(x) looking for the gaps!

more people may ~~only~~ also spread ideas, i.e. positive

—

in IGTF there is lack of comms for private information (like SLES + PGP).
~~but~~ in the last 20 years has not really been needed beyond the mini-RAT.
↓ and unused stuff decays.

14:30 [Break]

14:45 IAAOps//David J

3.7//2. information about stuff you as an AA + have, you should log, and the comm identifier of a upstream if you only have that
endservices need the proxy to keep the logs.
extent of logging in eduGAIN unclear.
but they have the data anyway!
point-in-time history is important for I/R.!
does the DB keep the change logs as well?
GDPR does not play a blocking role here, and its legit interest all the way,
For I/R you need to know ~~who~~ it was.
it may be in the database, but it need to retain history.
It's anyway Sirtfi!

GOLD

What does "being audited" means? The RP's are left with the risk but have no recourse or commensurate response.
[3.6 8] it audit as more than just "SCI.

"into agreement" applies to both. and make clear it does not imply a specific business relationship.

agreement may already have been set up.

For XSEDE LDAP: ability to reconstruct reliably the assertion is enough :)

and what about failed requests.

if you're a transparent proxy, you're not an AA and thus out of scope!

and Sirtfi is mandatory · much of this.

[3.g] maybe worded too strongly, but the contract is with the comm, not the RP.

Sirtfi? ~~pro~~-active notification not yet included.

does GEANT see all the SP's as "owned by the community" maybe?
~~this is not generally the case!~~
in which case they're with cold until Sirtfi v2
the community has the contract.
Uros: maybe "SHOULD" release, and if not RP's or SP's can just block them.

But maybe Christos may be afraid of the reverse, e.g a few people on EduTeams Shared, and then that PI asking for the DR/BC plan?
ask Christos!

(49) May 2020 (8)

* on web urls — ok, many comm. docs not have one.

* on comm policies: implicitly isn't already fine, wording unclear.

* and really discourage project names, but not forbid.
remember xenon.biggrid.nl :((

but also reverse: geant.org.... :)

=

3.2§3: christos does not like RP's/SP's. :)
client auth:
rules out public clients &c.

on "physical": reword to make even clearer that we're
after a secure hosting. Can be done, either
in contracts (like FEDramp, gov cloud)
or even with very good controls all switched on
in AWS.

HSMs: "highly reccommended". And are cheap in public cloud
like AWS.

=

lifetime: linked to lack of revocation / renewal.
and needs of incident response.

higher level "current best practices".

co-editors: Uros, Maarten, Dave K, David G.

16[02] Jule // Assurance and risk mgmt paper for ISGC.

~~N~~complication from too many controls (SP800-53 has far too many).
Can use cases be grouped, for instance, just like what TrustedCI did for risk?

use case driven. → if unsure, pick medium :).

Communities and RP's ~~want~~ "simple / concrete" guidance.
see recommendations, based on groupings.

many use cases are "medium" since we work in the framework that we have, and make the use cases like contractors fit in by making them go through the process

"VO portal policy" for (lower) assurance use cases, and "step up" to get to higher critical use cases. } (use case ~~as right~~!)

so assurance is not constant. And with the new proxies we have the tools to do that.

And for collaborative tools as examples, they can have lower?

Or "medium is too expensive" from OSG.
↳ this is a risk assessment, but then with a local in focus and not considering federation partners.
minimal 6-points from NNA 3.1 "Mikael" baseline as min?
Ability to suspend/block is better with high-value credentials but we cannot "measure" exactly, unless you can valuate.

16[30] next: 7-g ~~sept~~.