PMA45 CERN GVA. Jan 2019 21 jan. (1)

Present: Paolo, Davidf, Maarten, Mirat, DaveK, IanN, Eisaku, Ingrid, SamC, ScottR, Hannah.

Remote: Miroslav, Pawel, Vladimir D, Nuno, Uros [AndersW, SK,] Jens

13[06] Intro with MaartenL

13[30] Eisaku/APGridPMA update.

- some auditing delayed because review sheets not available yet -> fixed.
- remote ID vetting now approved by PMA -> HPCI about to roll-out.
- NAREGI-CP: supported ciphers b/c make up TLS 1.3

FedID in AP region via APAN IAM - joining to eduGAIN, with push @APAN47 in Korea in Feb 2019

Number of orgs from mainland China in eduGAIN? Scalability.

13[53] Cosmin/SA status:

Austria	-> about to ~~do~~ closed down.,	close S/A. ✓
Russia	-> no feedback yet, wait for Evgene.	pend
MD-Grid	-> also needs a new root	pend
MAGrid	-> no reaction, wait for implementation.	pend.
CESNET	-> needs DLG to do something.	
BG.	-> Ian is ok, pending DLG	
UKeSc	-> needs Jens to update CP/CPS.	
RoSA	-> OK!	✓ success.

others: issues w/ Egypt (3 wks) and serious for BYGRID.

1403 TCSG4

LoRa and "constraint" envs needs ECC, and that has to be up to the root. "25519" ⇕ depends on end-user devices

+ Quantum.

++ for ACME

* TCS lessons learnt presentation by SamC -> as input!

TCSG4 ~~Investor~~ seven OVals not active yet in WG's.

extra: more profiles, incl. one with multicast/anycast.

there are of course other proposals, ~~but~~ not in R/E Infra.

Outlook: latest 2019 version requires separate certs for signing and encryption!

15[00] Coffee.

15[25] Maarten / GN4-3. [see slides]

will be open for participation. Make sure collaboration keeps working also outside GN4-3.

open model - and "Europe" can be flexible to some extent.

16[20] Jens - RC auth. en [see slides]

check the integrity of the randomness does not need to be secure.

TCS vs Pathfinder

16[50] Derek / TAGPMA.

[see slides]

==

TUE 22 JAN

09[15] SCI - Uros, Davela // see attached sheet. ~~there~~ are changes in v2 that have been reflected herein.

review of sheet → see "V&-US".

averaging and weighting does not really make sense. Some may be critical and all have to be there, others are ~~too~~ open for interpretation (like PHD's B.C.D model).

10[35] Coffee.

11[01] IanN / Assurance. [see slides]

the boxytted profiles each are (should be) distinct to address a (research) use case. there may be overlap, but the differences are significant for a use case. Mapping & consolidation is inherent property.

11[00] IanN // Assurance: - common vocabulary based on requirements / use cases?
- ensure we demonstrate that each profile has a unique niche.
- no duplicates
- REFEDS influenced by feasibility (e.g. Student/Freshness)
. common language? → beyond NIRC

Session @ THE →
(define the conclusions first.)
IGTF NOO RP driven and capabilities openly discussed and engaged.

12[10] Security in FIM // Hannah. -- relationships between entities impacts global "trust"
(- announce next update of info " in template.)
- organise list of trust groups by type: org or personal, each with its own use case. personal trust may result in orgs loosing contact with peers.

14[10] AARC NA3/ DLS //.
⇒ FIM4R support: EOSCH + GN4 + RI's
#6 - SCI assessment → IGTF for peer review - self-assessment.
- AUP → ISGC Taipei w/ Von + BobC.
label "CC-BY.".
- DPR → close to the RI's re distribution.
in GN4-3 WP5.3 : service universal compliance. Maybe NPB with PIF teams may have a DPR task/activity.
(ACT?) ⇒ need a discussion place + mailing list. specific for research infra.
in practice it's Ulros, so maybe just EnCo / WP5.4.
⇒ - PDL list → WISE SCI WG.

Missing: common umbrella and vision → help personal overlap.
ensure coordination → continuity of trust in people.
help for communities in designing their AAI's? → GN4 + EOSCH
needs 1-on-1 consultancy, and more than a flowchart.
Otherwise people find keycloack.

PMB 45

instead of anchoring it in a particular project (with inherent bias), should be 'neutral': WISE WG or even better maybe FIM4R WG?
or: RDA-FIM4R-TG ? → new communities!

16[10] // Hannah - AAOps // see doc → SCI ++.
→ 16[50]
16[55] Sens // Soapbox on complexity.
17[30] [Closing]

Wed

09[15] Assurance.
- 13 profiles from Uniform. IGTF, REFEDS, eIDAS.
define/list why each profile is there inspired by specific distinct use cases. That's better than dictating why the exist.
so we made X because (N-X) did not do it.

REFEDS has the split with ACCR // S.M.O.A.
see slides

BYOCA → VEGI RP will notify EGI ops. that BY-Grid is going out.
then terminate BYOCA. ✓

11[00] SCI comparison with ISO standards? → NISE Wiki SCI
just like federation was not part of IDEM; SCI works for loosely coupled federation whereas eduGAIN is single-org.
- "access of SCI in interfederation" as per EnDOR.
NISE doc → also what is not in SCI
both content and methodology → Dave + Uros.

[PHM5 in Abingdon → NA3 final meeting. on Monday 18th ≥1400 L.]

assessment also in EOSCHUB, with "services" being the "assets" for FATSM. (Done it in March).

put in: privacy considerations in the multi-proxy environment. (D32). (strict minimisation is -not- always true!).

start with two documents, with the assessment being an AARC-I x doc.

then have the AARC/WISE I* doc @ Mal.

Policy hit → extend to SCI? At WISE and discuss in Abingdon.

=

Can eduTEAMS itself claim Sirtfi, even if the upstream is not?
with traceability/contact in place.

but if upstream idp was compromised, how would that incident be communicated to all affected SPs and to eduTEAMS.
so what about a compromised authenticator? eT does not have that.

"could" be acceptable if the SPs are already linked, and it is NOT even in eduGAIN as a whole. But it is white washing non-compl. IdP's.
it would be worrysome if the IdP upstream really is "bad"
not in the spirit even if it literally does not require info on authN compr.
/ Sirtfi + registry ?! that would solve it.
email of users must be checked for untrusted IdP's (challenge-resp.)
on the edge, but preferably not. Further controls on IdP level needed.

chain has to be representative of the statement
but outsourced SdI's under contract is fine because of the contract.

if there is technical reason to not have sdtfi, the SirtFit registry will work.
or get explicit statement and white list.
and edu TEAMS to keep that record of agreements.