09^15 RoundTable update

09^24 ASGC/Eric. Decommissioning NECTEC end of Oct 2016 (ACT).

IPv6 support comming in AP.

wLCG needs this --> add to agenda, DPK do talk.

10^03 Derek/TAG PMA update. Derek will take over from Scott again.

10^20 Scott R/ Dark Matter AE

- currently with QV as a subordinate of QA3.
- in final state different trustanchors for public trusts and IGTF.
- own roots by Q1/Q2 2017.

Own infra in acceptance test mode & isolated right now. --> expect 6wks +

using ejbca and 20^+ HSM's @L3 FIPS 140.

↳ intended for IoT in Dubai as smart city.

- web site 4 wks +
- operational in UAE expected nov. 2016.

Why IGTF → Ankabut

→ global retail community (with PubTrust by 2017)

- in the future eIDAS assurance is scheduled?

most work in cooperation w/ UAE govt; UAE govt owns the roots.

- intention is to serve beyond GCC (apart from contries to whom export restricted)

- Robots are open question, depends on eg Ankabut.

Review: Christos added to Jens, Feyza, Dandolf.

11^00 [coffee]

11^30 Cosmin/ S/A review.

- ArmeSFo: machine sent S/A doc but no CPS. only on Friday:

CP/S in place since May.

- IRAN grid: incorporate Miroslav's comments first.
- AustrianGrid: either new CP/S by Jan. or start decommissioning?
- RDIG : no news.
- DZeSc: pending review

Grid FR: self-audit report in January on EU2 CA
(project to move to ministry CA is in slow progress.)

Cy, ES, German grid/KIT, BY
attendance: QV, MD.

—

11[30] Jim: 3-year host certs instead of 13 mo. request like LIGO. for multi-year science run.
In CAB: 39 mo OV/DV. and 27 mo for EV.
for people 1 year is fine. for hosts: - easy alignment
- training remembered.

But in CAB/PT: association to domain is stronger, in classic sysadmin is now enough to get a cert and the sysadm life cycle maybe 1-year is enough.

permitted to use longer certs 3yr. IF it complies with validation requirements of BR. so domain ownership (whois and/or 5 addresses).

- up to 39 mo. if validated with domain validation.
- up to 13 mo if validated through RA check of services ownership.

RPs: they think it's all ok (wlcg, egi, xsede, [ligo] ok).

14[05] Christos: EGI Catch-All S/A.
[see presentation] moving to online use on ISO01 atchen.
→ migrate to new CP/CPS oct 2016. → Reviewers.
* for the new CA → explicit allowance of each IdP, which will be checked to see if an local CA exists.
Registration to EGI SSO may be required.
* RA process in the federated IdP's? currently will yield IOTA will need two different intermediate CA's.
onboarding will be by individual IdPs. today LoA can thus be added by contract

[Lehmsters] Scope will be those who cannot use TCS, but use an equivalent process.

* new ECI catchall is not the eIDAS service ! at least not yet.

+ push CP/CPS down on IdPs by agreement for HICS.

Reviewers: (CP/CPS + ancillary docs.) Jan N, Ronald O

14[45] Sim B/ Generalized LoA.

* also MFA is 'self-asserted' in InCommon. There are no audit/checks beyond standard 'in good standing'. Which is never checked: nobody has ever been kicked-out of the federation in InCommon.

* auditors don't work - peer review does, and being transparent.

Whatever we do to do checks, don't call it audit to prevent US Orgs to stall.

"self testing", "review", "self assessment"...

"assessment and peer review".

Given IC failure. try reverse:

push BIRCH to REFEDS. → may work for e Research IdP's, even if the uni's don't.

This mimicks the TCS pushing down in the CAS by contract.

15[40] Ueleg / IPv6 →

- 2 are 'bad' w/ AAAA but not working. → should be fixed
- end of 2016 for all Grid PMA.
- use CloudFlare w/v6 for free → see SimB's presentation from Pittsburg meeting

timetable → end of year, either directly or via CF.

review by Dan.

(TCS conditional)

16[00] Scott / Scapbox + SHR2.

B2ACCESS needs to keep state. → and keep its own traceability.

wording on dogwood in 3.2 was confusing.

B2ACCESS has to be the "O".

SAML assertion in the EEC → was used to bypass REFEDS and join AuthN+2.

maybe: per-IdP extensions that are included when requested by authenticated specific IdP. (do IETF could get it's own OID included).

others would ignore. (non-critical

on OIDCfedSC: if this were to happen, people would not object.

SHA-1: RP's would need to drop SHA-1 algo for subordinates.
see doc → (seems complicated and needs analysis).

•

{ ~~If~~ when SHA-1 is broken → S/W will and must drop support.
✓ eI's will drop SHA-1 if broken...
{ in which case risk does not exist! :-)

UUedSC → upgrade plan is ok. ✓

VideoVetting → compensatory controls description.
missing? of high enough definition → also by secure channel!
for reapplication might need less comp controls?

* training of RA's on remote vetting for each CA.

For 3-yr host certs → not ~~use~~ assert TLSWebClient?

<u>Wednesday</u>

09'5 Eisaku / MICS checklist
checks on IdP for MICS IdP profile → akin to ~~Sirtfi~~ Sirtfi checks & assessment test.
way we verify trust can have many options. → try different methods.
do internal checks based on heuristics, e.g like done in the TCS event.
share pdf to list.

Ned

09:55 Eisaku / remote vetting:

Q → compensatory controls

F2F process has never rigorously defined by PMA → CP/CPS + RA proc

last report option (but keeping in mind notary publics are 'useless').

consider a points system to rate the compensatory controls.

eg. phone oob = +25, HDuid = +50, &c. } → as evidence for PMA during assessment.

check request if from the user

test and also check negatives.

checks during the in person for passport has never been required on

listing req. on RA's.

should be managing risk and define the 'acceptable' level: and in-person has been varying as well, and both NLCS & EGI are fine with this.

checking w/issuing authority in person is needed at LoA 3+

CP/CPS should pick → try with some CP's and do it!

allow for this to be proposed to the PAA, and if the PMA then endorses it, it can be done on current BIRCH/CEDAR RP's.

today, remote users may just be made an RA. :-)

→ See new Wiki text! ↳ and video + not. pubic is already ok!

RPs all want this :-)

11:00 Shahin / DR.

3/2 or 5/3 → only for D/R, not normal operations. . chance depends on staff turnover.

because of personal changes.

the 2-year period is because of media aging. → paper might also be an option.

11:45 DG/LoA circulate be last Tom's comment.

11[55] Scott / Business purposes of CA's.

biggest risk is in RA processes.

helping the CSP credentialling process should we devote more effort in defining the RA process. So, while not overdoing it, there should be a base of confidence. → RPS.

RPS may be too detailed? But there should not be nothing.

- easy to onboard but have provable process.

IGTF has no expl. guidelines on RA designation.

- document onboarding process → new guidelines

would be good → collect examples from around CA's with intent to inform and educate our community.

↳ esp. import for large, generic providers. (DCert, QV, HPCI, CILogon+, EGI catch all)

(ACT) . create on private wiki area to submit examples.

12[15] Dens / CAOPS.

- fixed many typo's in GFD225 → check ups and publish via Andre. Is hard.

→ - new version of GFD-169 for mics. → pick up.

- very few meetings, but lots of overlap w/ EGTF → more co-locating w/ IGTF.

- guru can travel to ISO as "OGF" being equivalent to a country (without vote)

Ljubljana ~~March~~ May 8-10 2017.