Participants:
local: Jan Jona Chwastek, David G., Scott R, Mare V, Dusan R,
Dave K, Ian N, Jens

remote: Miroslav, Vladimir, Christos, Cosmin, Dan Chiojha,
Feyza, Bozidar Proevski, Nuno (HK), John Kewley

—

Jelentes: - policy, - tech, - relationships | move focus (gradually) to include
more RP's etc. → | more (R/I) infrastructures
| -> keep practically working mode
| for tech and policy!

Steering group: Dave K., Scott, (extra meetings).
· for planning.

Re-elected Chair: David G.: move along the planned dev's in
relation to federation & "AARC"

—

Cosmin: IGSA Review.

ArmesFo: OK ✓

AustrianGrid: no change - no reaction.
(ACT) David G to send final warning to Willy as chair
(AI) . otherwise the AustrianGrid CA will be suspended.

RDIG: restarting, needs a new self-audit.
- delete from list from now.
- schedule for new s/a.

DZeSc: David G: OK
Ursula still pending.

CyGrid: ~~merging~~ CyNET taking over.
ask CyNet to update CP/CPS and do new self-audit

GridKA: no respons.

UGrid. ~~waiting~~ for new CP/CPS. uploaded - reviewers waiting for S/A sheet

UKeSc: re-accreditation. for Pathfinder CA.
others have not been done yet! → sha-1 for some
intermediate CA's

—

14:00 Scott R/ blockchain. [see slides]
- permissioned blockchain is the one relevant for IGTF?
- for the medical case: also privacy can be addressed (not shown here).
- ~~keep~~ use 'derived credentials' to prevent leakage.

Internal use cases:
* publish (under control of the PMI) the traceability requirement.
usually private, unless the majority agreed that a condition has occurred.
* because of cracking the algo in the future, if it is now public. Hash only??

permissioned BC: - use it on RA's as ~~recta~~ strengthening processes through publishing the hash?

- "accountability of accounting systems". as a use case?
  - ↳ start + end of submission as a transaction, which means that the accounting data is actually accurate.
  - ↳ prevent re-publishing of records.
- time stamping? The ledger is the ultimate time source.

Tea 15^10 - 15^40.

15^40 Scott/Dark Matter [see presentation]

new CA hosted in UAE now, (next to the QV IRA's that are already accredited)
hosting in Abu Dhabi, with D/R site in Dubai
UAE global root generated last week on-prem.
the IGTF specific private ones after WebTrust Audit next week

EJBCA updates in RA module to do key management as well (e.g. key escrow where the CA does not want to get the keys).

now going through WebTrust audits (all 3: network systems; BR; EV).

Anhabit still there, new classic ca dedicated to them.

= publicly trusted (QV) ones can be issued to Middle East (only, for contract).
= private trust (IGTF DM) one is a single ICA for servers and people.

Auditors changed from EY → KPMG
(EY was also the QV auditor).

new CP/CPS extends policy to end-entities. → changes to sections 3, 4, 6 with more details.

(almost new :-)?
Reviewers: DKG, Feyza, Jens. (2/3) target: few weeks.
Keyed review to the IGTF one, not all diff :-)

fix links (ACT).

16^20 Busan/AEGIS

---

new CP/CPS foreseen - too many changes needed!
so review the next version :-).

- RA audits → there are only 2 people, so trivial to do → will do.
- privacy law aim is to be in sync with EU GDPR for adequate protection

complete review requested! Reviewers: DavidG, and ask Emir. (ACT).

16^35 announcements. Meeting lunch (1400 →) to lunch all. Both Hon or The start.
16^50 (Scott: Hon, Darrell: Tue)

Eric Yen - new chair in Oct planned during upcoming WLCG meetings.

APGridPMA - 11 prod. CA's, next focus on selfaudit of all CA's.

[see slides] - IPv6 still only @ 50%, WE

- web server upgrades almost done now (from Ulf's mail)
- MICS spreadsheet based on LoA + Tech Guidance.
- Remote vetting → to be documented on wiki
- APAN for colocating and trainings.

APGridPMA: Oct 15th - one day before HEPiX!

---

eg[40] JensS/AAAI [see slides]

Rlamth was IOTA, not MICS.

- aim is ~5 IdP's (today: only STFC still) in WP3.2's workplan. (till end of June)
- CA has public repo + a moonshot authn service. (simpler than SARoNGS).
- VOMS is optional and now out of scope.
- public info includes links to AUP, etc

- delete: retains randomised ID, remove rest?!

- lost traceability → for BIRCH short lived certs.
  or IdP's should retain sufficient info.
  there is a specific doc for this.
  as part of Assent contract; bind within a COI
  as Assent does not do LoA at all.
  why not bind to entire CP/CPS just like TCS? → needs a lawyer.
  signup is manual anyway. → ask SISC.

'right to be forgotten' is conditional → retain some data.
~~same~~ here automated → ~3 yr. still ok? seems fine.

long term aim: replace classic. (and a new HSM).

Accreditation: needs full document set.

in UKAMF there's also guest IdP's etc. → here the CA will do explicit sign-up and vetting of IdP's, so only trusted orgs will get in.

Reviewers: @christos, DavidG.

Target end of June is rather ambitious. → as possible

PMA40

10^{15}

DavidG/Transliteration

- the Ш → sh (instead of Š → S) does not work for Serbian. given the historical context of that particular transliteration.
- OK for new model
- for multilingual attributes. use "en" first (and don't concat values) check again for RCauth wayf.

11.30

DavidG / RCauth governance.

- RCauth distr. OK.
- needs obser. of org control.
- MoU's with orgs (with disengagement option). w/ responsibilities.
- same key, slice up serial space (encode BASE64 as name).
- FZJ → STFC.
- key distribution ceremony (record).

12^{10} Jens / DR

[slides online]

- very long passphrases? → 1/3 should still be long. use a barcode scanner with USB HID? :-)
- many of this we need for RCauth distribution → work on that in EOSCHub context.
- and for new UKeSc. Root.

14^{00} Trusted CS updates

(ACT) . upload PKP v2 to public

- check AARC def. for improvement in §Intro. / TTS.
- fixed sections Intro, Naming, Site, Rep + add Sirtfi.

(15^{30}). see Wiki

16^{00} TAGPMA/Derek.

- end of RNP AL natural as a result of consolidation.
- LACGrid → needs to be fixed by mid-June!
- REARC?

16^{20} – 16^{50} finished T/CS

17^{00} Next meeting: Sept 2017: 25 – 27th lunch-lunch (14^{00} – 12^{00}) Manchester!

09^40 Soapbox/Dens "Security Policy" →
in the context of backups of roots & balancing disaster recovery vs. security.
"policy should say what you want to achieve", "rest is implementation".
—
assurance convey beforehand and/or convey with credential.
c.f. the REFED AP work & 4 dimensions.
Istanbul Soapbox:-

(Uniqueness we always assumed)

10^00 Dina / EUN joined

Source of authority is moving around and being distributed.
even more, as in the AARC BPA
and signatures are being lost as data are forwarded and translated. →
this is basically provenance as we know it from research.
For AARC2: add this? "duty of care" in managing this data. → "admissible electronic evidence."
- But do all the RP's understand how to consume/interpret it.
and just accept IGTF blessing.
but in practice, trust will be between SP Proxy and the RP's will be ultimate.
People & interface is important: 4 options is too many, ∅ kills empowerment, ≤3

10^30 EUN/EGgrid/Dina → s/audit — updated contacts needed
└Hussein — OID update

extra: The certificates all created as per user requests and documented.
F2F in all cases. → academic users only.
for each user there's a paper file. centrally.
community is very small → via SME's, just 4 entities.
EG only 4-5 faculties in need of credentials.

Reviewers: Dušan, DavidG.

* old versions → fixed CRL.
* IPv6
* SHA-1 → fix for gen

11^30 IGTF as a federation → advantage for FOG & eduGAIN.SG access.
Interest DIMB + Jordan S. + DG.
operational capability distribut.
also for IGTF eduGAIN bridge,
fix RNS +Stetif for NL and DE :-)

CAOPS during next PMA in Manchester.

Roundtable: