add: Romain Vetting.

Present: Scott Rea, Darell, Walter, Vincent, Roberto, DavidG, JanC, Jana, Pawel, Sergii, Oleg, Hare, Ursula, IanN.

Remote: Miroslav ✓, Christos K., Lidija ✓, Dani ✓, Nuno ✓, John Kewley ✓, Maria Podura ✓, Serge Salamonka, Sens ✓, (+Eric), Adeel

09[50] TAGPMA / Scott + Derek. → see slides No vice chair at the moment.
TAGPMA 26 July 3-5 in San Jose, Costa Rica. (tbc) to get more L/A attendees

10[10] S/A: DZeSC: Ursula send comments after San 26. waiting for Bonnaventure.
RDIG: Eygene gets bit more time, no update
IRAN: only minor things left new SHA-2 in prod.
ArmeSFO: new CP/CPS needed. / waiting for minor things. (really minor).

Junet: remove from membership: "gone".

HIAST: keep suspended.

EUN-EG: they don't react. Ursula to send RATCC to them, then suspend after 30 days.
(there are still CRL's being issued -- maybe via a REBCA track?).
Some users can go to Roberto / INFN-CA.

10[30] Scott Rea / DHCA. - all CA's regulated by nat'l. telecom authority; ~10 M people of which 1.5M emirates.
* transfer scheduled for March 2017 to UAE-hosted data centre.
* issuance based on PKI-based nat'l. ID incl. biometrics.
* two models. now both QV + DV NeBT annotated.
vetting is in-person with the nat'l. ID card + RA. checking the binary pictures inside the card (also for Ankabut users).
now 'very traditional' (and under Quovadis)
* UTF-8 → latin is always a challenge, but there is a standard transliteration.

So: QV ICA is 'just another Trust Anchor' under existing QV CPS using exactly same processes → so this is fine as-is.
Review will focus on the new DV-rooted CA's, which does need much more detail and extensive reading. needs more processing → add 1 to 2 month.

11^45 Ursula / German Grid self-audit & spreadsheet development
new 1.1 has adapted her agenda XLS
-> (ACT) move xls from agenda to wiki pages. + meta-doc.
+ additable elements from assurance profiles may need enhancement
e.g. (28) is a duplicate, etc
S/A: - software re-written in 2015.
- in many cases materially OK, but not documented completely (many B's)
- the 2nd backup is professionally gone and securely shredded -> OK.
- TACAR -> update via Licia
- documented evidence (12) is kind of crucial.
↳ audit of RA's should be in RA agreement ... not "x".
or collect all forms at CA?
↳ send msg to all RA's on audit, just to wake them up

Reviewers: Scott R, Ian N.

12^30 -> 14^00 Lunch

14^00 Ioannis / IGTF-eduGAIN bridge. (AARC)
[Client verify depth 1 ?!]* code on github - additional SSPHP module.
consistency of translation: run a single one in eduGAIN (at GRNET?)
multiple instances in H/A mode. sharing. since it's stateless.
there's an igtf.net subdomain for this
More attributes: are additional attributes defined. (easy to extend).
Ioannis willing to extend
who signs the SAML -> the IdP resigns it as usual.
(* try with TCS G3)
this IdP can now go to eduGAIN via GRNET.
and add REFEDS R&S + Sirtfi planned as well. (based on revocation).

(*) eduGAIN registration via IGTF. for our RP's, i.e. the RI's and EI's (30 up to ~60).
so also gets more members in?
but needs (1) a doc MDRPS, (2) signing infra, (3) legal entity.
Interested: (Scott Koranda,) Scott Rea, DLG, Dave K.
cofunding by AARC2?, dinnertime in FIM4R.

15[10] PRACE (Vincent) – see slides.
[Q: GSI SSH → always or just once?] → depends on local site.
refer to REFEDS MFA + assurance WG profiles
↳ + link explicitly to IGTF→eduGAIN bridge.
users are mainly non-web.

(15[00]–16[15]am)

16[10] answers as usual, see AARC / BPA.
↳ convergence in IdPSP Proxy.
for non-web: OIDC / maybe OAuth together w/ EUDAT + EGI ; SAML ECP doesn't cut it too low adoption. (see GEANT for MS.)

Meeting structure
relative PKI ⟷ FedId is 'kind-of' OK. →

start on Mon. afternoon? 13[00] → ~~UK~~ ~~with Gotiki~~ → discuss w/ Jan for Ljubljana.

Tue 31/1 09[30]. [notes: Walter]
09[30] Maria / CyGrid → now in LinC / UoCyprus.
part of CyGrid (2004 → 2018) up to & incl. InSPIRE
next action → transfer of responsibilities
~~this~~ relation should fit both central CyUni ICT & NREN.
needs to be sorted first.
Review: Pavel, JanChvojka. ✓

09[55] Ugrid / OlegA&Sergii
new SHA-2 CA "G2" (valid until 2037, 4096 RSA). → distribute in 1.81
(AC) and EEC's are now ≥2048 RSA (in V1.5) (≤ OK).
for S/A: see slides. Both logging and availability are OK. Logs are there, just different files.
for D/R → see new session, is OK.
Review: Ursula, Ian N.
based also on new (v 1.5) CP/CPS.

TAIPEI 39 / Florence ④.

Remote vetting.

① Christos' experience w/ german bank on remote vetting. → sufficient for insurance
without the special app uses regular video calls. (special used company)
with a presubmitted form + SMS + flash light.
and then a picture :-)

② in CESNET test (between CA admins) used a card without too
many security features (old CZ card)
but did not work well (and RP's might be too lenient).
needs a challenge. test first?

There are a few banks that do that (known to Christos) Try "M26" bank.in.de.

BIL guidance on doc fraud applies now also to employers & landlords.
(show link).
but bank did not check watermarks, but some of the details were
certainly visible. process took 5-10 sec. though.

for our RA training, designate just one RA / CA
→ use whitelisting of document types, and describe in CP/CPS.
→ existing out-of-band relationship.
→ contact external sponsor (based on public sources)
→ see also Wiki

EIDAS ↔ eduGAIN bridge to do electronic remote vetting based on govID.
(today that does not work everywhere: no readers, or no access because
of privacy - like in NL).
EIDAS now in a deployment phase and attention is elsewhere
pilot postponed, intention still there
model of EIDAS would favour a per-memberstate eID-scheme approach.

RA training in RA's "RPS" and include it in accreditation. and include it
in the audits of the RA. (incl. training). No need to attend meetings, though.

Remote-vetting RA's can be close to the CA operation.

11^30 Jens / UK eSc. update
Pathfinder interconnect piggyed in UK. (Moonshot → relation to GEANT statement)
also Assent is still lacking some policy coordination.
2A repurposing needs a cool-down period (& new name class)

| and still features lacking there Pathfinder may help & expand beyond UK later

* revalidation (and Δ of 1 release) of package name.
* CP/CPS needed. → full review.
* hierarchy + key can stay the same
Reviewers: David G, <call on list for +1 reviewers>

—

Jens: RCauth for EUDAT in jointly managed CA. → joint w/ EGI, GEANT, etc)
wildcard for multi VO VOboxes (VO-specific named used)

For SHA-1: updating just the intermediates at least gets rid of the warnings.

IPv6: available @ RAL, but not at CA yet.
use Cloud Flare.

TACAR has to be updated, change him subordinate should be possible easily by PGP mail.

[back at ~15^00]

IPv6 CNRS: CA will be retired and replaced by govt CA (which might be IPv6)
CyGrid: ping → CF
DZeSc: " "
DigiCert: ping, needs all CDN providers to move. Ask Clint again.
TAGPMA / CC: discussed on list.
IRAN GRID: ping. CF status unknown (EAR)
MaGrid: ping, CF
PSNC: main web server admin. will get pinged by Pawel
RDIG, Rosa: ping CF
UGrid: working on it right now

See Jim Basney's guide to CF
Following the WLCG timeline: IPv6 by Apr 1st 2017.
add ref to MB document.

16^10 OGF/Jens Jensen.

Whole range in WG status. most active are OCCI and NSI (GLUE, DFDL)
+ cloudplugfest.org and other 'plugfests'
ISO/IEC status means OGF can attend like a country (but not vote).
- a doi for GFD documents? it is free open access publishing already.

On CAOPS

keep also external input, which is valuable!
co-organise with other events (like TIIME) and engage more
e-infrastructures - not yet explored.
for security still open. (IDEL, VOMS-PROC, CAOPS).

concrete goals help, but attending F2F may be difficult due to funding.
which event is a challenge (e.g. hardly anyone @ PMA goes to TIIME).
for networking NSI this actually worked. - needs help from organisers
that have enough rooms.

either? restart with more, new people (and thus new goals as well).
or absorb into IGTF? but then we loose the publication and ext. input.

@ infra meetings like DI4R?

evaluate on new meetings on CAOPS mailing list.
e.g. at AARC plugfest (but overlaps w/ EUGridPMA).

(ACT). Jens to send to caops-wg list on strategy. Others to chime in!

16^45 Soapbox / Jens. 'Devine Strategy / Tragedy"

The Question about Innovation: which ones survive?
some stay at the publication level and a project, but no lasting result...
"elegant solutions, working ones or both"
Cloud hosts: transient, moving to IoT on lightweight devices? Provisioning?
use CAOPS as a feedback mechanism - case studies? (incl. inc. response)

[(ACT) ⇒ session on blockchains and how PKI should properly support BC? [Jens, Scott R]
identification of endpoints + permissions management infrastructure..
"distributed ledger" & append-only.]

(+) 'When making things better, there's always the risk you're making it worse".
(+) VM's are just like physical.

09[30] APGridPMA / Eric Yen   colocation usually with APAN e.g. APAN44 in Beijing

- endorsement of new APs based on Assurance has been done in Aug 2016
- for video calling → join on Wiki? no new my hysteria seen yet.
- closer involvement of RP's, as well as with natl. Identity federations.

09[35] Snctfi, – RP coordination in a federated world.

* based on SCI, as published RS's, to foster trust amongst EGI, PRACE, XSEDE & WLCG and Snctfi

relevant for both IdPs, but also e.g. like PRACE.

just like SCI v2 while

doc. Snctfi can go to IGTF as a document home (like for SCI)

(since fimLR does not have one)

- as to binding the SPs in the infra: the "contract" (TermB) is actually this policy set maybe supported by an MoU or OLA (like EGI).
- R&S does put requirements on scope and (some) behaviour of the SP.
- federations are all still very different and even R&S adoption is national.
  ↳ R&S does need heuristics.

- consider version binding for Snctfi (v1) and R&S (v1.4).
- use the FIM considerations from UNISci Cloud as the answer to the Question: "OS1: do you have a security model".

(+) - structure of Snctfi also makes sense for PRACE: will bring to Security Forum to discuss.

Sirctf1

Define the word 'Infrastructure' to be the community of users and SP's alongside the set of examples of communities

(inline editing). review capitalisation of "infrastructures" where applicable. as per meaning in glossary.

-describe the proxy trust relationships at (top) level of document.

Roadmap: goodfinal draft for FIM4R/TIIME (Feb '23)
suggest changes before, via the phone conf.

version 0.2 in GoogleDocs. "** VYTo/". including comments therein.

12[30] closing