09^{30} — Pime, Bob?, Dave K., Dulco, Kaspars, Tamar, Dobie, Feyza, Nabil, Michael
Ronald O, EricY, < ___ >, Cosmin, Willy, DanC., Marc, Ders, Pawel,
DG, Hordi.

Remote: Vladimir (DG), Shahin, Miroslav, Adeel, Lidija, Heidar

Notes: (Cosmin)

09^{55} EricY: AP Grid PMA meeting.
new vice chair from HPCI (Aida K).

10^{05} Dave K; TAGPMA.
YSEDE 8 July 14–18.

10^{17} Kaspars: S/A status.
- UKeSci CA: still needs to send out CP/CPS. Ready but not jet
distributed.
- LIPCA: not ready jet, time ~ May.
- IRPEN: no new info. next week.
- ph??Grid: pending. Review should be ok.
- NIIF: CP/CPS sent, under review.
- HD Grid: pending in/progress.
- Slovak Grid: done this week?
(ACT). - Armse SFU: no response jet. - needs ping - CP unresponsive.
(ACT). - 11ARGI: no response from CA → needs ping to Boro.
- TR Grid: DONE! ✓
Kaspars willing to go on.

10^{30} Chair election: DG continues.

1⁰ Pawet PLGrid s/a.

③ Ursula to send sma cert hylength in next RAT challenge
there is still a year of leeway, but change < 2016 should be done
also in view of HS Requirements.

14 RA's: auditing is still difficult. Redesign registration-travel form.
proper forms are collected at RA's.
↳ prepare ops procedures for RA's.

personal knowledge is weak.

(#14). Checking signatures would also require checking ID.
for simplicity mission ID, not personal acquaintance.

new CP/CPS? next week / end of May.
Some changes already done operationally.

(ACT). Review: Nabil + David G.

1⁵⁰ Nabil.

#26 verification of purpose? state in cp/cps it's not verified.
colon vs. dash. use 2 dashes.

ready now on website. (May 6th). v1.3 [draft.]

Reviewers: Pawet + David G.

Short updates

UK: discussing handover to Saint for personal only
otherwise upgrade the software from cpm cps to own developed DS reg.

12³⁵ ————
LUNCH

13⁵⁵ Dg / IGTF in 10 years & charter.

Jens contribute to IGTF website. "why"
make the 5 blocks be a selection behind 'for users'; 'for sites'; for RA's.
quick links like overview.

14⁴⁵ New IGTF fed. doc.
15³⁰ on Wiki v.2.0 - v02 DRAFT.

EUGridPMA 31
Dave K / FIM4R

16:10

Groups involved now. SCI / FIM4RKRDP / IGTF / INFRA7-AAI / REFEDS / GEANT.

(ACT) Repositiory of IGTF for B&F on Tuesday TNC.

   SCI : separate notes.
   where does SCI want to go?   } demarcation unclear.

Review conclusions.

   IGTF now broad enough to include everything incl SCI.
   Not sure what SCI wants, since SCI does more.

—

Reconvene
———

THURSDAY 15/5
   (notes: DG.)

09:10 Sans PkP/Scapha :

   a Should we emphasise openness on the website? Do new countries
                     even join (or new groups)?

   ~ (some of slides written before IGTF 10 disc. yesterday).

   shortcuts affect RP's more than authorities.

   we might just say connecting infrastructure.

       all guided & global trust remains with the IGTF.

   the certs we can buy.

   as for wLCG: trust fabric & security was the success. (TNC 2013, Ian Bird).

   → Recommendations for auth2 etc. beyond certs. e.g. also for "RP" business.

10:20 PkP.

   finalised. Should not conflict with v1.0.

   use wiki for changes.

   "24 hrs of inactivity" added to principles. and in sections #2 and #3.

   Done !

11:10 coffee

11:30   DAT : send explicit mail to EG to get it fixed.

   IIPAST & Hands OK.

      test more frequently for failing ones.

   General: challenge end of year.

   Bruce: EG also unresolved for sites in Gizeh. in context of AfROC.

      EG is really needed !

ASREN does try to get more service also in Jordan.

Bruce: CMain DEDS and eI4Africa FP7 supported.
    linked to scientific activity.

———

Heartbleed: amazingly low number of revocations. — for all CA's.
    many were not vulnerable.
    personal not really affected.
    re-issuance was really quick — RP's keeping with IGTF.
    mostly on RP issues.

    OpenSSL info release process will now likely improve.

Should the IGTF or the CA's have some operational capability.
to run tests?

Ⓐ. Quiet consensus that CA's are willing to work operationally,
    in these cases.

Ⓚ. Test applications and services are good to be shared.
    with people also in the OpSec world, we can share tools.

    subscriber and cert contact may be different.

    CA's sometimes react faster.

    EGI CSIRT tools may have to disregard CRL.... for test.

    IGTF may still scan ---.   e.g. EUDAT never scanned.

    there was no IGTF/PMA message. should there have been a
    (template to forward to) subscribers.

Ⓣ. - would have been useful → RAT.
    keep some info private to PMA members. (from others)

Ⓢ. not the general list.
                    Ⓥ. use wiki for access control

Ⓐ .

———

Bruce : Sub-Saharan Africa.

     quite good support for an African PMA after a bootstrap period.
     with a defined deadline.
     and use TAG model on a "branch" with separated but coordinated.
     chair. and meetings.
     time zones work out.

     more video, may be in two full rooms with a link between
     them.
     dead lines (also for catch-all) are needed or things drag on forever.
       Roberto has been dangerous : -)

     distribute operations, but in long run a central issuing CA for e.g. Ubuntunet.
     but with "VCS like" backend issuing box.

     produce overview month 13 note on future direction incl.
       timeline to African chapter and PMA.

    ————

SAGrid CP/CPS Review.

   (?)   - current key on line → will need to generate a new one off-line. (✓)
   (?)   - C = RSA ?   → /DC=za/ DC=sanren /+
   (✓)   - 1024 → 2048 . + SHA -2.
   (16)   Virtual F2F - via SANREN video. - recorded.
      SANREN has database of all contacts who can sign off and
      validate the copies.
      they can vouch for the RA's.
      then like Brazil and Turkey doing equivalent of Notaries-public.

   (✓)   should be ok.   😊.
    ————

- auditing: audit system in same system controls environment.

(?) - hypermounting: os machine off-line all the time ?
     timing is ok.   ⤷ move machine to be really off line.
                    - not as a VM.   (ok)

     cost: RPi + HSM. < $100,-   → for now off-line. signing.   test distro
                                                        "brain." bash

Ronald O. UUNET.

(✓) move "offline' CD from VM to offline planned. &.
looks a lot like the SPGrid CD.
'service' certs still there.—

RFC 2527 → 3647.
 This is not clear on the website, old template.

- Use the new SPGrid as a new template (RFC3647 ++).
- template should be empty of real content (so no GRRR :-).

(9) Reviewers: Willy, Marc.

Self audit guidelines are a good checklist. add to web page.
 Collect and add to igtf.net members.

———

Jan Chvojka / CESNET.

(5) 'unsure' → is actually excellent!
papers w/ident info on archived.

Review: Dave U + David G.

———

16:00   Shahin / IRGrid. Self-audit.
Root challenge issue solved (forward auto final).
0 = D (Advise)   3 = A (good)
RFC 3647 change already done.   all guide OK. :-)
Plan for June-August incl. SHA-2 ~ end of June.
~~Review~~
Reviewers: Emir + Kaspars.

———

16:15   TSU / Memur.
  GRENA.
(?)   C/L naming → DC?   move to DC., maybe drop the L.
(✓)   1024 → 2048 for EEC.   + SHA-2 CP.
ID- copies returned? <> private info 'not retained' c.f. #34.
  in .LV low changed and now record the number if OK.
   or last few digits. | process:
            | - reviewers should see new CP/CPS
- USB maybe easier than CD-ROM?   and be happy
- acceptance will be removed. | - 2 weeks → then OK!

MICS profile.

  – generalisation: – remove CA bits
                    – make it an LoA document coming out at
                      IGTF
                    – as a consensus of RPs.
                    – as req. on IdP's and Fed.

  complementary to SCI stuff.

  present at the BoF at TNC. (10min).

  take to TAGPMA.

  complements the lower IOTA level.

_____

  Pru → Wiki.
_____

  Online CA: on wiki, please review.
       need: TAGPMA.

_____

16⁵⁵ Panel: Poznan.

  dinner 19³⁰ Noah, next to town hall.

_____

(ACT:)
  – igtf web site spreadsheets.
            include review/design hints in spread sheet for CA off line.
  – convert PKP to word doc. & publish