29th EUGridPMA. mo 9 Sept.

Remote. Vladimir Dimitrov., Miroslav.,

Local: Cosmin, Alexandru, DG, Oleksandr, Oleg, VincentR, Jean-François, Maspars, Willy, Roberto, Dusan, Paolo, Nuño, Hardi, Bri, Eric, Robert (NCSA), Jean Christophe Read (BELNET).

Cosmin: logistics.

09[45]. Robot cone.

09[50] Eric Yen: AP update. - HPCI CP is Japan taking over from NAREGI & AIST.

-

10[15]. TAGPMA update: LGTF all hands! Approved MICS change!

10[05]. Self-audit status (Maspars). new status by Maspars

pk IrisGrid → should go to San Masa.

Emir → should be hit over the head.

(ACT) ArmeSFo → needs new reviewers. → DaveK (Sara).

CyGrid. → DONE! (new CP/CPS published)

(ACT) MARGI → needs new contact on website, PMA link OK. list new name: DG.

(✓) NIIF → review, Dusan. + Nuño

Belnet → migrating to PCS delayed, self-audit by end-of-Sept.

Maspars continues till Abingdon.

(ACT). move to confidential Wiki. (new)

11[05] Dusan / AEGIS. SA.

- 7 RA's (Lix Belgrade) < Dusan does have a backup operator. → add to list.
- SHA-2 via OpenSSL script editing.

or move to OpenCP? if this does not work.

(✓). Peer: Willy

11[20] Paolo <see slides>
OCSP.

11[40] - 12[20] IOTA AP (Dowd G). presentation.

[12[30] - 15[10] lunch :-)]

15[10] PRACE (Vinient).
also in PRACE/DEISA the bioinf. can load through a portal. Did need additional traceability which was non trivial.
- not much XSEDE cross use.
~~- pseudonyms are ok for PRACE since binding is retained.~~
- security req. "e.g. ISO 27001". or other indicating the level.

Auditing. also SARONGS?
without upstream PRACE can hardly accept it.
would make it more like 'experimental AP'.

① IOTA AP should not require anything which is not in classic or MICS/SICS

'eduGAIN' and IOTA useful for specific projects and portals.
(not for general case)
eduGAIN would help for traceability.

DavdL: GDB headed, no guidance yet.
quantification of risk associated with auditability upstream IdP's.

conversely: edugain-CP not exist yet.
SARONGS: ~~BLAMS~~ has audit rights on upstream IdP's

for RP ⓐ - audit need.
ⓑ - Incident Response → Questionnaire (in ppts)
Changes by PRACE incorporated in Wiki!

Tue. (3).

programme

(9. Georgia: RobertoC and. ~~Dave~~ ~~David G.~~ Jens reviewers.

09[30] Hardi: HITSA/EEnet.

TAAT: 6 IdP's @TCS eScP level, incl. all 3 big universities done ✓

end of BalticGrid 21 SEPT 2015. → to TCS (expected).

university SSO pages are high assurance because of natl. ID card. ✓

—

SHA-2. EGI OMB request to 1 dec.

WLCG should be 'happy' once EGI is ready (since OSG was OK already).

users can still request SHA-1 even after

default will be SHA-1 till Dec 1st.

at least for larger CA's

after that, at least some should try - but beware of support load.

all dependent dates move +2 mo..

Request to delay also affects TAG/AP.

AP likely OK., from TAG DigiCert & Grid Canada are most important for EGI.

OCSP: start encouraging → more timely, matches emerging suspension in EGI.

- good for testing CERN MS

- VOMS server really should check. → early!

EMI CAL really should remain & support OCSP (and SHA-3)

through EGI CSIRT.

29th ⊕. Hanck / Nick cuts for end-users; Paolo: SSO@CERN. | renewal of CA cert. guidance. ④.
RAT (Ursula).
? testing possibilities?
RP Q. type of Q and concerns.
DNSSEC? (no).

11 30 Ursula / RAT

List of nonresp.

APAC: leaving already this year.

CNRS: operators will be kicked by Jean-François.
new address by Jean-François in new CP/CPS.

✓ EG: rechallenge, no people but w/ CRL.

✓ HAST: CRL expiration will stop CR,
but are they still functioning. Derek concerned.
Chair Rechallenge, give alternative contact possibility.
(RAT). Chair to check.

✓ IGCA: Eric will check in F2F in Beijing ✓
rechallenge.

✓ IHEP: got new manager. : rechallenge.

✓ IRAN: personal email works, rechallenge.

JUNet: Mazyad very irresponsive! (BAD) } ⊕ have to show up in Abingdon
⊕ otherwise: out!
⊛ selfaudit? - present improvement plan
+ comm
in-person required. ⊕

✓ NCHC: no valid certs, rechallenge.

NECTEC: check in Beijing.

✓ UniAndes: rechallenge, they are active ok.

Membership

(RAT) (Jovi in Kyiv) Fayza + UGrid.

Attendance reset for. BG.ACAD + SlovakGrid + pkIDAs for videos at 2 day.

in Abingdon: JUNet, BYgrid, Algeria, Morokko, MARGI, MREN.

encourage: CyGrid, IRAN, S.Gnet.
+ all blue.

⊛. UKeSc. selfaudit in Abingdon.
Pawel } selfaudit
Emir

GridFR → new CA manager will replace SF and do the SIA.
moves to security dept. next Monday.

[lunch] dinner "Harbour" 19:30 @ Ramada. ~19:45 Strada Pia to Amzei 10-22.

18:30 Jens: HSM, PUCP for CA's, IGTF 'future' in 10y.

HSM mainly for compliance and performance.
but there is vendor lock and changing hardware
- and locks you to certain OS versions for driver compatibility.
- and loose ability to upgrade → might as well be an off line software
- HSM's are 'evil' c.f. API's

cf. James' π-HSM+Aladdin.
- they import currency like HEBCA. (2 different HSM vendors)

human operators don't really check. (2B ca had identity based ACL).

what do we actually need? from the HSM.
other options: shared HSM? signing 'service' shared by many CA's.
↳ single point of failure.

Requirements on alternative systems:
* 'secure' (what does FIPS 140-2 L3 protect against?)
↳ rationale of risks.
go through the risk and determine relevance and impact.
there are already many CA's that just use OS API and sign anything based on (uid/passwd) pair.
CA key compromise is still very cumbersome and tedious
either highly secured stand alone system, OR
* simple systems in a safe?
Come up with criteria? Jens, DG;

Use case: quick revocation 24/7 and immediate CRL issuance.
(less protection needed?)

Jens: Key protection for 'important' keys. (6)

protection of backup and archival. at end of life cycle

key distribution is error prone (people loose their share-bit).

people are a large part of the problem.

→ trust very few people, and separate responsibilities.

may loose even offline backups.

replacement is still hard.

if there's more than one manager you need credential change process.

"LUKS"

but nobody does n/m multiperson control. (in room now).

better double for rare tasks like backup recovery?

but why more than usual operations?

for IGTF AH. meeting?

From TAGPMA. - private discussion:

Vision: tech-agnostic interoperable trust.

Where Jim B agreed that 'more CA's is better'.

=

Why re-evaluate the risks e.g. based on cost.

—

(*) non-FIPS / non-HSM model risks → La Plata.

16:20 Dowell.

May 13-14 Tartu or 27-28 if EGI takes 12-16.

Sep 9-10 Belgrade.

AAOps → Steve T still needs to try (has read)

discuss @ IGTF AH., ask Steve T to make list of discrepancies.

Link to SP Code of Conduct and REFEDS reference Fed. Agreement.

easy in H&S, nontrivial in F/H (no solution yet)

29th EGP (2)

For CredRepo Guideline.

(AC) * present. in La Plata.

* find willing volunteer (maybe in EU)

then to EGI to include in process. (ask Tiziana)

Wed 16/9.

09:30 TechNed. topics

- new guidance. Wiki updated ✓
- testing in production mode.

Production testing: ~~group~~

- testing group does not scale (may work for CERN)
- point users to local CA for support.
- most CA's set up to offer best-effort support to subscribers for ~~end~~ use w/ services.

✓

① IOTA + VO: no s/w support yet for making (VO+IOTA) combined requirement (e.g. VO-P only with classic, but VO-B is good enough to do IOTA as well)

↳ needs new s/w!

KIT output will be lower assurance.

Questionnaires linked to agenda.

* credential repos: interest in EE. → also many non-grid apps. (NFC tokens, mobile SIM card.

bit like CILogon w/ fed. front end. like mobile. AAE fed auth to repo.

SHARING might do it.

(X) → very few others currently planned.

② can we re-use NFC contactless (Credit) cards? Currently mostly low-value transactions.

Better protection in EE with mobile/SIM storage. Maybe revocable @ SIM

Cred Repo's: (8).

(*) - ask NCI's / EGI if, given HyProxy and like s/w, they would be willing to consider running a CR?

- which countries can use NFC / SIM technologies?

- where TCS is available: what other solutions outside web/email used to store creds.

(c.f. Redatec B's online ca: did not work w/ TCS policy).

(*) differentiate between signing (and authentication. {certenConfirm}

(Adobe?)

(ACT) for next TCS?

for which purposes do users mostly use their TCS personal certs.

(ACT) └ get statistics for TCS. → ask Team.

have CRepo auth linked to federation.

—

Test Suite.

- generate structure.
- send samples

—

AH meeting. for video, Δt = 3-4 hrs.

- HSM / non FIPS models, resilience
- vision beyond x509.
- recovery PODAB
- IOTA
- cred repo guidance.
- test suite.
- name: "interoperable", "global", "trust".
  but keep brand name, maybe as tagline.