213.244.140.110 // 6430 7736 500 // 4483 4483 // EU Grid PMA 57 (1)

Present: ~~Adeel~~ Elisabetta, DaveK, Derek, DavidC, TomD, Hannah, LiamA, Maarten, JohnK, JohnL, ~~Ethan~~, IanN, Paolo Tedesco, Elna Seyer

Remote: Adeel, CasperD, Miroslav, Mischa Salle, Nicole Harris, Cosmin Nistor, Heros..., Erik Yen, Lidija, NicolasL,

Intro.

Self/audit Cosmin

Otag 45

TSU GRENA: prod and hint at suspension. (ACT) DavidG.

not even with new process. did they respond :(.

NIIF/HU is also non-responsive, ask (via GCC) and DavidG. (ACT).

Bygs → needs suspension after mail. (ACT).

KENET: worked a few month back OK. Now silent.

Cosmin to send mail from non-STFC address.

✓ GridPK: OK! ✓

MREN: OK ✓

Polish Grid: OK ✓

Ask Kostas to retire SEE-GRID.

Cosmin to mail: AndesW, IRAN-GRID, Algeria, Armenia.

(ACT) Add comment field to membership (private) table.

NGIs worried about lack of assessments.

APGridPMA // Eisabetta Sothane. (see slides).
10 [20]

RCauth // Nicolas L, (see slides).

STFC to join fully in Q3 2023; with new network service systems.

Interest from CTP, Project MinE, UK,

Lack of uptake on the CAM model hampers it as well.

need for papers in journal as well as whitepaper doc.

John K // Ulleße. Catch-all use.

- soon SHA-256 Roots, and update RPDNC for the ICA's.
- new hierarchy will come later. (not now)

Since the Ulleße CA does not need to comply with BR CPDF as its private trust only:

- TAGPMA is fine with it, totally. Will mention on the call (Derek) "we should not start issuing for the whole world". It is unusual.
- FNAL might get Sectigo to work still.

- Fix CPS for Ulleße CA may not even be needed.
- Some FNAL people would need to get a Ulleße personal cert.
- It will be an intermediate solution - and the exception should be documented. Limited to specific communities.

✓ WLCG is fine with it ✓

- The Ulleße now also works with edugAIN supported remote vetting.

= Only from FNAL

SHA-1 VMWare + ELG are now known.

- DigiCert not very responsive.
- GridCanada + CI Logon in 1.110 ok.
- release when requested.
- OSG / Fermi would try to 'join' "BEGIN LIMITED CRT" joint magic.
- strongly encourage to move.

SMIME : OK as presented, incl. TCS.

AARC: machine-readable AUP for comparison?

HIFIS: some communities set up their own hidden proxies behind the proxy to prevent having to write privacy notices!

to don't ask but help?!

* common policies that are provided rather than ask for it.
: like the cookie law? opting consent.

* outreach. +training.

Browsers?

---

* User Centric: combined assurance based on community policies

---

Uni IdP's don't do all of the assurance, and hence don't ever do assurance (Scott Hunter).

---

also cross-sector with students in companies.
(also 'sectors')

Link to ORCID? collecting identity? (ORCID is 18+ only!)

---

* Ease of Use: fewest possible #hubs

"Testimonial' style compendium, with an editorial team. Good common practice.

together in a compendium with an analysis and how this works together.

repository (GitHub?) with documents & contributed solutions.

what Persuade use by example. show the examples!

FIM4R → issue: should seems to move to back-end.

here look more towards community thing.

"web-engagement".

TAGPMA / Desch:

⊕ Tomofumi will respond RISN on the SHA-1 issue.

- QV marketing is confusing on DigiCert acquisition.

- Token-based WS @ SCI tokens panel @ TechEx22.

16[30] = WLCG ~~token~~ Trust Evolution (+ Maarten L).

- recently ~~all~~ restarted based on impetus by FNAL.
- UkeScCA can now supported FNAL in the short term (specific case).
- how to address the cloud user cases is still open.
  - splitting out trust sources.
  - changes to software might / will be needed. [1]
- OSG keeps returning to the same discussion again in the GDB.
- ATLAS would like to use Google (which leads to mngt pressure to make progress in the Evolution WG.

[1] Can software (storage foremost) ~~be~~ be adapted?

- dCache
- HTCondor } ? are likely to work already.

⊛ but needs to stay aligned with non-WLCG communities.

Short-term: CMS will try to introduce a local CA within the expt framework only. (but TECH ONLY! not chain impact)

FTS can initiate transfers.

OSG risk assessment on Let's Enc: not 'formal', but useful!

~~xxx~~ "There is more to trust in cloud services than just certificates" ~~xxx~~

- which bypasses all registration procedures! ad-hoc in expt!

changes in the expt model and TCO ↔ link to ATLAS Gonzalo + David S.

"What is trusted" - and how does that work across the supplychain.

Always comes back to risk assessment.

the last risk assessment was in ~2004 (D2.5).

on every interface ask the ~5 risk questions.
"who is talking, how authenticated, valid how long, revokable, integrity/ident)

⊛ User and Resource trust are both evolving and both have equally complex!!!

09:15 Maarten / GN5-1 : WP5 T6 EnCo is still there and strong in the
- new Framework Programme.
- InAcademia has its own task now.

* MyAccessID accesses to LUMI HPC. Persistent identifier. * !

better alignment of eduGAIN CSIRT and WP6 in GN5.

On assurance → [since Sule left]

* combined assurance explanation + models
* step-up via eIDAS (as prep for AARC TREE?)

Sirtfi v2: should not adoption be tracked by eduGAIN

by means of the eduGAIN CSIRT comms challenges, mock incidents, and exercises.

At some point eduGAIN steering requires it!

OIDCfed als being tackled in AppInt now for interop, in arch.

Workplan 2023

[edu.nl / dq3d3]

* PDK - pathways to policy suites?
  - not all are the same, but many stand with aup / tac / privnotice.
  - not all are a BPA proxy.
  - top-level policy is "hard", makes people think about what their infra is (like for UK IRIS).
- joiner-mover-leaver process guidance / examples for AA's.

Policy with respect to retirees (@CERN and elsewhere).

- they loose link to org, and even security training would not help much.
- biggest source of phishing and helpdesk calls on expired passwords.
- email forward should be enough.
- leaving them fully active is dangerous!!

PTA57 (6)

AAOPS reviews

WLCG - some things are fixed, but communities don't care that much and won't do it.

"iss" should be able to be set to a persistent unique name, like https://cms.cern/

↳ but need to be checked w/ IAM devs.

eduTeams (Christos) "EduTEAMS Steered"

* the platform is (in a hosted service) itself the controller, and "the community" is just a (processor) customer.

* This is actually common, although in SRAM the controller is the "home org" of the community (and not only SURF).

AN-1 community gets own sub-namespace. in sub.

* on the "issuer": entity ID of the interfaces.
OIDC "https://proxy.eduteams.org"
so is fully dedicated to the AA purpose.

AAR-1: this is actually defined by the AA operator as this is the data controller responsibility

AAR-2: unclear.

AAR-3/6: is actually on the community (more like guidance)

AAS-3: lifetime of REFRESH tokens. in eTS = 1 week, but is that the 1/2 hr one.

Pressure is for longer (6mo, 1yr).

WLCG Refresh: 1 day → 30 day max, recomm: 10 days.

also operational impact, and workflow interop.

we need guidance around this.

KMS.2. OIDC has short-lived keys. SAML is more complex but with hierarchical encryption and tmpfs, this is COMPLIANT! (✓)

Best practice guidance needed.

! Beware of GitLab secrets, as they may not be that secret...!

AR2-1a 18 month backlog of traces.

TomD // UK IRIS AAOPS w/ Angela Correa-Beltran.

OE-1 on-site. Overall sthing: in the RAL data centre

OE-3: for MFA, if you get REFEDS MFA in ACC, then also accept it.
Current communities only "kindly asked", but no real request; yet.

KM-1: only OIDC, rolled over via well-known endpoint.

KM-4: was quite a large list, now being controlled.

KM-5: currently just on dask.

compare to Christos' elaborate setup. Or Jens' HSMs.

NET-1: segmentation ongoing.

all still behind just JANET.

AR2.1c → do removals get logged? Unknown.
→ account linking changed?

> Main item: long storage <

Next? PMA 58: monday 22 + tue 23rd May
SURF Amsterdam VLC1/VLC2.

OIDC Fed - OIDC fed for SSPHP in Incubator (Mihály).
- python library to be plugged to SATOSA.
- GARR has OIDC fed on Shib.

so there can be interop tests. (in Q4 2023) also in ~~eduTEAMS~~ implementation.
- but for the moment eID Wallets is higher prio
- less resources for Federation.

For IAM: dev. effort changed after Andrea left. Maintaing and migration to keycloak was too much.
so working only on new features, and no longer migration to keycloak planned for now.

CheckIn: there is a keycloak plugin (v13), but has to be synched to latest keycloak version.

*cross signing or with some 'hubs' (for X-continental trust)

OIDC

in OIDC you should also expose the end services.
advertising RP's behind the proxy is already possible.

For the trust issues, experiment first?

esp. with path construction. Work in AARC ongoing

See also AARC AppInt doc, but that is quite theoretical.

Try with the Incubator? unlikely.