EUGridPMA+ 56 CERN 4-6 oct 2022.

Present: Dave K*, Maarten*, Jan N*, Lidija, David G*, Miroslav D
Jens C, Adeel UR, Hannah*, David C, Eric Y, Cosmin
Ian C, Eisaku*, Nuno, Mirvat AS, John K,

218.244.140.110

Cosmin. S/A review

- * LIP CA reviewed and now ok (David G).
- * KENET no response yet. → new method.

New process:

- ✓ The MREN CA was a complete success with a single joint meeting. Also Lidija was happy, change of system was needed.

Was very nice experience. 2 hrs. After the S/A changed machine and there were some, now resolved, perl issues.

keep disk of old machine.: secure destruction needed.
MILSPEC destruction for key material.
key length for EEC's ~~is~~ should now 2048 bit. from now on.

pending confirmation.

(*) Worth sticking with the new process (*).

- Polish Grid CA ~~also~~ worked with multiple meetings

to be confirmed by Pawel and Feyza later.

(*) Formal declaration of conformance at next plenary meeting or mailing list. (2-week).

For the urgent ones (including MARGI): start all in parallel. and hoping enough react.

KENET, TSU GRENA, BYGCA, GridPK, KIFU/NIIF.

GridPK: * need to update the CSR process to get rid of keygen? self-audit first?

- * CSR generation tools by CESNET using JavaScript.
- * SHA-1 root migration. already done! :)
- * prepare → final by Jan. 2023.

#2

Audit ref: assurance level + PKI tech guidelines

ACT Fix access to twiki for PL grid.

—

RC auth anycast → anycast is easy! :)

═

COFFEE

═

SHA-1 Self-signed Roots

RAL may have an RH support contract. or CERN

it's not a CA/BF thing.

SHA-2 migration for IGTF. All EEC's are sha-2, but should we pressure the roots.

steps: - ask RH first?

- just do re-issuance if you can! → send doc.

- what happens if you add our roots to p11-kit.

See tickets from OSG and ATLAS. And ask Maarten L.

ACT Contact SHA-1 CA's? DavidG. to contact all.

- also check intermediate's (John K)

═

LUNCH.

═

CA/BF Joint Trust issues:

* We do not have influence over all software, so suggestion on #10 has only limited effect. Generic open source projects would not follow. Would need evaluation.

* This is an issue only until token world (i.e. ≤ 2026).

* Is there a place to start using the new paradigm. e.g. in storage acesse only looking at transport-only trust.

↳ "S3" style services first., exclusively w/ tokens + transport trust.

⇒ David C + Alistair Dewhurst. / RAL T1

+Maarten L.

S/MIME - TCS/InC short notice?

only affects TCS/InC → only different root.

* send new CP/CPS.
* general thrust is OK!

=

Derek. Membership: XSEDE ended, Derek now representing ACCESS.

UTF-8 → rendering can be ASCIIfied.

software still does not work w/ non-ascii

OSSL ⇔ BouncyCastle.
continues.

use BR /OV only, and national representation. Should be fine, even Sectigo can do it (still).

EV is out of scope, luckily.

TAGPMA meetings!

WOTBAN&AZ 2022 → Bloomington.
TechEx / FIM4R / TAGPMA in Denver.
panel on Tuesday afternoon "IAM" sessions.

Trusted (IGTF) lists of token issuer. ; based on self-assessment.
- AAOPS G071
+ assurance.

and then list of end-points + metadata (digest, policy urls?)

++ Derek, Dave, ...

alternative [illegible] OIDCfed is there.

use JSON w/ some metadata. - align w/ OIDCfed. !

REC?

SHA-1 for TAG → incl. DigiCert also for new intermediates.

16^{42} end

EUGridPMA 56 · CERN TUESDAY.

Present: Adeel, DavidC, Jan C, Lidija, MiroslavD, IanN*, Eisaku*, Maarten*, Davide*, Jule*, DavidG*, Hannah*, Alistair Dewhurst*, Mirvat, Ian C, LiciaF, MarioL, TomD, MaartenL., JohnK

#4.

Eisaku / AP.

- ASGCCA still acting as catch-all
- 10 active members.
- 31st APGridPMA in week of March 19, 2023. (ISGC)

- OAuth-SSHd ⟷ OIDC agent? ✓ for GFarm storage + compute.
  ↳ based on keycloak.
  ↳ usability improvements now use oidc-agent from KIT ✓ (+Putty!)
- HPCI will collaborate with CTA to transfer files from PIC to HPCI now using GridFTP and FTS3.

  @PIC, client auth is with TCS G4 cert. (which is name-unique) authN of FTS is client/robot

GakuNin → natl. federation.

to address assurance issues for research, a WG on "proxies" has been established "Orthros" → also linked to GovtID, ORCID, &c

link to AARC BPA? AEGIS? ↳ account linking!

(Assurance IAL2 sought)

(AI) LINK Eisaku and Christos on AEGIS membership.

(Indigo IAM v2 is not ~~there~~ yet)

DavidC Splitting trust ... in a token landscape.

sharing trust. → time line for tokens differs per community.

DUNE wants to make more rapid progress than just WLCG.

---

separate trust stores. → at the same time as JWT migration?

GridFTP is going away at some point, but some HPC systems still use it? In the US, this is no longer needed. Globus online ~~off~~ web DAV.

not all communities move at the same pace.

(*) not invest too much in "older systems" model and GSI

back also to taskforce on tokens to look for examples where there are current issues.

transport and token trust are separated in tokens.

and then DCV is fine. for transport.

Tokens then need to be trusted.

access to storage should move to standardized tokens. to translate IAM to proprietary object store providers.

plugin approach in GFAL, FTS, and Rucio to translate our JWT to their own system (e.g. on HPC systems in US).

TrustList. Maarten: do better job on running proper AA's.

that G071 + assurance.
using self-assessment and peer review.

"WLCG as a whole then needs to be 'happy' with the issuer, with IGTF doing that for the RPs".

assurance levels per issuer can be multiple, it's about the procedures.

single list, with metadata. in JSON (OIDC fed spec).

(*) need a EUGridPMA guideline on how to get in.
↳ efficient and quick, and clear.

"few weeks".

inserting token issuer url's : now manual copy-paste.

✓"how to configure an HT condor CE → one line in a config file"

common software? JSON → automate, also the selection.

+ tool to select from it. (python trickery?)

DS // S071 : intro slides.

Hannah: Indigo IAM integrated with CERN SSO. Now using CERN accounts.

CERN SSO → IAM ⟶ token + LoA → RP.

experiment ↗ HR in-person F2F

deploy issuers on OpenShift. ~~S~~this is shared. for now.

look into separation.

Andrea C went through it and it looked OK.

Tom D : also IAM in UK-IRIS.

more federated identity use in IRIS.

otherwise similar to Hannah.

Hannah: SIMPLE where possible.

make a spreadsheet (like SCI).

review by peers to learn from each other as well.

but complete quickly.

trustworthy ness is about the AP, not the upstream IdP's.

G071 / IRIS. (see Google sheet)

- AN-1 has broader scope: G026 | G069 as well. actually broader than issuer.

- Bug in G071 AN1.3 "for sbb & attr."

==

Trust list for issuers:

- single list, since.
- no sep. by assurance, since we have amr + acs.
- based on G071, since
  - SSON, inspired by OIDCfed.

EOSC AAI federation based on SAML for now. But OIDC provider trust needed for cross-provider access.

New AARC guideline on remote token introspection.
"go verify the token at the issuer".

mechanism now being defined, separate doc on trust issues.

members of the federation are the proxies, not the clients.

{ - SSON issuers
{ - SSON web keys. } → to be fetched by all AARC proxies.

allow proxies to see a common trustneeds.

The IGTF list could add "trust marks" ⇒ and Entity Categories.

(*) and aggregate all these lists, from EOSC and elsewhere.

for now, adding G071 may add more hurdles than EOSC.

add trust marks (EC's) as labels in metadata.

-filter based on <policy-url's in the SSON list.

subset of OIDCfed:

- security_contact
- policy-url.

- use github PR's to add to the list, with a review process? Should be relative simple.

Christos

JSON (and SAML) should be generated from submitted metadata.

(a bit like PEER?) or in pyFF.

we can define the JSON format regardless ~~fo~~ of the ECs and trust marks.

IGTF to "eat" the EOSC AAI fed level. and filter tags.

other regions can do the same, and then have a grass-roots OIDC fed.

(ACT) On JSON format: AppInt to announce to IGTF.

Also the EOSC AAI fed trustmarks need to be curated. but this has not been discussed yet.

* no curation process defined yet, (only automatic, for SAML only).

(either adding, or removing it) → no governance yet.

a lot should also be happening on the national level. with local hubs (like SRAM in NL) so that it can be distributed.

* Initial reaction.

Present: EIscha, IanN, Hannah, Maarten K, Sale, DavidS, DaveK.
Video: DanC, EricY, Adeel, MiroslavD, DavidC, Mirvat AS, TomDach, LidijaM.

EnCo

MaartenK: <see slides> EnCo as linking pin, bringing support to a range of eScience and federation / eduGAIN ecosystem.

- eduGAIN Security Handbook.

- FIM4R on Sunday Dec. 4th.

GN5: 1 jan 2023 → 31 dec 2024 (2yr).

topics: trust policies for token issuers: process for listings.

OIDC fed.

Snctfi and proxies: formalise abit to foster trust for InCommon?

AppInt.

needs a concrete use case for all of them.

MyAcademic ID proxies also for Erasmus in scope? register via websites that all are behind one proxy.

incommon is hesitant since they feel they loose control w/a proxy...

↳ Snctfi v2 in GN5 to get this better trusted.
| "Trust Mark"!

For GN5 → CERN will keep collaborators even if not directly funded.

(Marcus & Mische may help) Hannah will remain involved but is pressed for time of course.

SCCC is marginal

OIDCfed based on list of issuers.

* End of GN4-3 is near, in San Marino will be back as well.

* EnCo and ISGC - security workshop.
- submission of talks before Oct 31st.
"What did EnCo GN4 achieve?"

(*) * "A holistic view of enabling eSc. collab through networking & federation".

* +Snctfi v2 talk

Is this trust work actually tangible?

⑥ - write down
- link to AEGIS.

} actionable + operational output.

scalability of trust, Dunbar, WLCG (4 authors) vs. EOSC.

EOSC will have >> 150 parties, then procedures and transparency are needed.

WLCG has lots of breadcrumbs [from Leif].

⑦ engagement: EuroHPC!

- non-web.
- OIDC-agent. / MarcusH.

|| FIM4R: requirements in all the new communities, and use this as input to EnCo. And then be more concrete.

Next VC: 1400 CET Nov. 2nd EnCo.

COFFEE

Assurance & FIM4R.

"Middle Thing" → working process (based on ACAMP discussion).

Add intro slide/paper beforehand.

Flagging assurance: even if you implement RAF @the IdP, there is too much reading to do for risk-averse IdP's.

One cannot track RAF adoption, since it's assertion-based.

f-ticks is probably too limited to measure this, since it does not list attributes.

Driving adoption: NIH in the US requires it. DFN also starts introducing it. Now moving to RAF in Germany.

RAF via CERN account linking + home IdP? Needs quite some work!

FIM4R Agenda: last call also to FIM4R-list. (StD has already gone out).

Dave K. WISE: in-person meetings are much more useful to get real work done.

US participation has dropped a bit. Move to Trusted-CI? WISE AUP would be useful for them.

Now that ACCESS has started: better funded effort?
could be in Bloomington @ NSFCSS.
How to engage better w/ the Americans.

ISGC Security day:

- linking OpSec & federation better!

+ Australian proxy op + GakuNin proxy!

* programme early, based on Denver topics, and from February FIM4R in Europe then.

OpSec + Federation:

- bring communities closer together.
- it's more than just info sharing
- joint exercises using a federation scenario, (like the Alessandra exercise in Taipei).
- Romain's CSC/Sec challenge in Federation context.

but meet in the middle focusing true federation model.

bridging the chasm that currently still faces GN4-*

(*) Discuss scenario at GN43-WP5 all hands!

No SCI updates now. long term convergence on SCI v3

how best to organise is for the WISE workshop.

Lunch

Scho's Soapbox // Sens had suggested a talk, but that now is a soapbox!

++SS = SK!

Upgrading to SHA2 - but how paranoid?

the off-line machine now spawned an HSM w/a push

mechanism, ca1 esc.rl.ac.uk.
user certs are slowly falling, but hosts went up!

2B - exists in two variants. but the Root is SHA-1 only for now.

ACT Remove 2A from UKeSc. Root namespaces / signing policy.

| but for a broken SHA-1, if its broken then you can just create arbitrary content → only effective resolution is on the RP side in their software.

the risks for SHA-1 are not on the CA side.

For VOMS servers: add --skipissuer.

Quantum is too early. SHA-3 too fresh. EC should be throughout.

ACT. Org Cert first are SHA-1. → could be withdrawn.

TCS impact? n UK. → charging!

Option #2 seems good. Post QC has even issues for main contender.

SHA-256 ✓

And use `--skipca`.

==

|| Next meeting. { IGTF + Feb 13 afternoon → Wed 15 morn.
FIM4R Wed 15 afternoon → Thu 16th