Present: DaveL, Fabian, JanN, Lidija, DaveG, Miroslav D
   JanC, PeterU, Hamrah*, Daniele, EricY, Casmin
   JanC, Elisab*, Nano, Mirov, JohnU,
   218, 244, 140, 110

Casmin, SIA review
   * LIP CA reviewed and now OK (DaveL).
   * VENET: no response yet. → new method.

New process:
   * The MEUP CTP has a complete success with a single joint meeting. After Liège was happy, change of system was needed.
   * Need very nice experience. 2 hrs. After the SIA changed machine and there were some new resolved, few issues.
   * Keep clock of old machine, see deactivation needed.
   * MICE spec destruction for new material.
   * Megabyte for EEC's = new 2048 bit. From now on, pending confirmation.

* North sticking with the new process.

  - Polish Grid CA also worked with multiple meetings to be performed by Pavel and Tejaa later.

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

For the urgent ones (including HPRAL): start all in parallel and hoping enough reach.
   VENET, TSG, PANDA, B2GC, GridPL, Letters/NIIF, LNF.

Grid PL: need to update the CSR process to get rid of sludge? Self-avoid first?
   * CSR generation tools by CESNET using SnooScript.
   * SHF-1 root migration. Already done. :)
   * Prepare → find by dom. 2023.
Audit ref: assurance level + RH tech quickhunch

(190) Fix access to twiki for RH and.

RE auth anycast -> anycast is easy! :)

COFFEE

STM-1 Self-Signed Roots

RH may have an RH support contract or CERN

it's not a CARB thing.

STM2 migration for IGF. 1911 EEC's are show-2, but should we pressure the roots.

steps: - ask RH first?

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

- what happens if you add our roots to pki-lab.

See tickets from OSG and OIN. Add and Maarten L.

Contact STM-1 CEO's? Davinci to contact all.
- also check intermediate's (John U)

BUNCH

CP/BE 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 tosun world (i.e. ≤ 2026).

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

  "SS" style services first, exclusively w/ tokens, transport first.

  David C + Alistair Dehurte / PRL T1
  + Maarten L.
TCs/Inc short notice?

only affects TCs/Inc -> orb different root.

* send new CP/CPS
* general truth is OK!

Delhi

Membership: xSEDE ended, Delhi now representing ACCESS.

UTF-8 -> encoding can be specified.

Software still does not work w/ non-ascii. OSSL <-> Ramagalli contains.

Use BR/OV only, and rational representation. Should be fine, even better. Can do it (still).

EV is out of scope, luckily.

TAGPM meeting!

Not BPA 2022 -> Bloomington.
TechEx / PMR / TAGPM in Denver.
Panel on Tuesday afternoon "IPAM" sessions.

Trusted (IGT) lists of token issues, based on self-assessment.

- PPR15 8071
  + assurance
  and then list of endpoints + metadata (closest, policywise?)

+ Delhi, Dave, ...

alternative digital OICf feed is fine.

use SSON w/ some metadata. - okay w/ OICf feed!

\[ \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \]

for TAG -> incl. DigiCert also for new intermediates.
ENGINEERING CERN TUESDAY

Presid: Adeel, David, Don, C, Liddams, Nilsband D,
Jan M., Eisahn, Dorelan, Dave, Ke, Del, David,
Hamish, Alistair, Devanware, Minra, Jan C., Licca, Manuel, Tom D,
Monten-L., Schott

Eisahn/PP

* 136GCDN still coding an catch-at
* 10 active members

* 31st PMP in week of March 19, 2013 (186C)

* OAuth-SSHD ➔ a SEC agent? for Farm storage + compute

  to be licensed with OpenNebula

* HPCF will collaborate with CTP to transfer files from PIC to HPCF

  now using GridFTP and FTS2.

  @PIC, client auth is with TC664 cert. (which is name-unique)
  auth N of FTS is client/kebab

  Galen Nin ➔ nahl. foundation

  to address assurance issues for research, a reg on "proxies" has
  been established "Orthros"

  ➔ also linked to gridID, ORCID, etc

  link to MARC BDP? BEGIS?

  (Assurance 1912 sought)

  ✔ LINK Eisahn and Christen on BEGIS membership

  (Indigo DAM v2 is not there yet)
Splitting trust... in a token landscape.

Strong trust - timeline for tokens defined per community
- DNS needs to make more rapid progress than got IECG
- separate trust stores - at the same time as DRM migration?
- GDPR is going away at some point, but some ERC systems still use it. In the US, there is no longer needed.
- Global online, off web DAV.

Not all communities move at the same pace.

- Do not invest too much in "token systems" model and ALD
- look also to taskforce on tokens to look for examples when there are current issues.
- transport and token trust are degraded in tokens and then DAV if fine for transport.
- Tokens then need to be trusted.
- access to storage should move to tokenized tokens
- standardized SAML to proprietary object store protocols.
- plugin approach in ZFPL, FTS, and Racio to translate
- our SUT to their own system (e.g. on IECG systems in US).


- HTD GOFA taxonomy.
- using self-assessment and peer reviews.
- "IECG as a whole then need to be 'happy' with the
- issuer, with IGT's clarity that for the RPs.
- minimum levels for issuer can be multiple, it's about the
- procedures.
- single list, with metadata in JSON (OAIfed spec).

- Need a RFC7989 guidelines on how to get in.
- is efficient and quick and clear.
- "few weeks".
inserting token issue w/ new manual copy-paste.

which to configure on HTCondor CE + one line in a
common script? 

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

---

DS/8021: intro discussion

Hannah:  Integrating IDM integrated with CERN SSO. Now using
CERN accounts.

CERN SSO → IDM → token + LDP → R.P.

experiment a HE in-person F2F

deploy issues on OpenShift. This is shared. for non-
look into separation.

Andrew C went through it and it looked OK.

Tom D: also IDM in UIE-IRIS.

more federated identity use in IRIS.

otherwise similar to Hannah.

Hannah: SIMPLE when possible.

make a spreadsheet (like SEI).

review by peers to learn from each other as well.

but complete quickly.

specifically run is about the R.P. not the upstream IdP's.
9071/1218. (see google sheet)
  - RAN-1 has broader scope: GO26/GO28 as well.
    actually broader than issuers.
    - Buy into GO24 RAN-1.3 "for 66 & attr."

Trust list for issuers:
  - single list, since.
  - no sep. by assuranc since we have amr+acs.
  - based on GO24, since.
  - SSO, inspired by O1DCfed.

EOSC HRII federation based on SAML for now. But O1DC provides trust needed for cross-provider access.

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

Mechanism now being defined, dynamic doc on trust issuers.
  members of the federation are the proxies, not the clients.

- SSO issuers
- SSO web-logins — to be fetched by all IEEEC proxies.

allow proxies to see a common trust needs.

The IETF list could add "trust marks" and Entity Categories.
  and aggregate all these lists, from EOSC and elsewhere.
  for now, adding GO71 may add more hurdles than EOSC.

add trust marks (EC’s) as labels in metadata.
  filter based on policy-urls’s in the SSON list.

Subset of O1DC feed:
  - security-contact
  - policy-url.
  - use github PR’s to add to the list, with a review process? Should be relatively simple.
SSON (and SAML) should be generated from submitted metadata.
(a bit like PEER?) or in pyFF.

we can define the SSON format regardless of the Ecs and trust marks.
IETF to "eat" the EOSC MAINTIRED level, and filter tags.
other regions can do the same, and then have a
grass-roots OGC-fed.
On SSON format: Appoint to announce to IETF.

Also the EOSC MAINTIRED 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) \rightarrow no governance yet.

A lot should also be happening on the national level, with
local hubs (like SRRM in NL) so that it can be distributed.
* Initial concern.
EnCo

Hooten K. (see slide). EnCo as linking pin, bringing support to a range of OASIS and Federation/edugain ecosystem.
- edugain Security Handbook
- FindR on Sunday Dec. 4th.

GNS: 1 Jan 2023 → 31 Dec 2024 (2yr).

Topics: trust policies for tolm issues; process for listings;
OIDC fed.
Sctfi and proxies: formalize obit to foster trust for InCommon?
AppInt.

Needs a concrete use case for all of them.

My Academic ID proxies also for Erooms in scope?
Register via websites that all are behind one proxy.

Erooms is wanted since they feel they lose control w/ a proxy...

"Sctfi v2 in GNS to get this better trusted."

"Trust Mark!"

For GNS → 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
OIDC fed based on list of issues.

End of GNS is near, in San. Marine will be backed well.
EnCo and ISG will security workshop.
Submission of talks before Oct 8th.
"What did EnCo GNS achieve?"

A holistic view of enabling eC. collaboration through networking & federation.
"EnCo v2 talk."

+
Is this trust work actually tangible?
- write down
- link to REFIS
  / acceptable + operational output.

scalability of trust, Donhor, WLCG (4 anchors) vs. EOSC.
EOSC will have > 150 providers, then procedures and
transparency are needed.
WLCG has lots of breadcrumbs [from Leif].

+ engagement: EuroHPC!
  - non-web
  - O1DC-agent / Marcus H.

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

Next RC: 1400 CET Nov. 2nd EnCo

COFFEE

Assurance & FIM4R.

"Middle Thing" = working process (based on RAPID discussion).
Add intro slide/paper beforehand.

Tagging assurance: even if you implement RAPF @ the IdP, there
is too much novelty to do for rich-average IdP's.
One cannot track RAF adoption, once it's assertion-based.
If tickets is probably too limited to measure this, once it
does not list attributes.

Driving adoption: NIH in the US requires it, DFN also starts
introducing it. Now moving to RAF in Germany.
RAPF via CERN account linking + homeIdP? Needs quite some work!
FIM4R Agenda. last call also to FIM4R-list. (STD has already
gone out),
WISE: in-person meetings are much more useful to get real work done.

US participation has dropped a bit. Move to Trusted CI? WISE 19 UP would be useful for them.

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

ISGC Security day:
- Emby OpSec & federation better!
  + Australian proxy op + GalenNin proxy!
  + program early, based on Denver topics
    and from February 7 MYR in Europe then.

OpSec + Federation:
- bring communities closer together.
- it’s more than just info sharing
- joint exercises using a federation scenario,
  (like the Kessler exercise in Taipei)
- Romania’s CSC/Sec challenge in federation context.
  but must in the middle facing true federation models.
  bridging the chasm that currently still faces GN4-+
  Discuss scenario at GN43 - NPS all hands!

No SCF updates now long-term convergence on SCF v3
how best to organise is for the WISE workshop.

Lunch
Sno's Soupbox // Sven had suggested a table, but that now IS a Soupbox!

Upgrading to SHA2 - but how paranoid?
The offline machine now spawns an HTM w/ a push mechanism, can esc R1 ac.ile.
User costs are slowly falling, but costs went up.
2B exists in two variants, but the Root is SHA-2 only for now.

ACT
Remove 2B from WhSc. Root namespaced/signing policy.

But for a broken SHA-1, if it's broken then you can just create
arbitrary content -> only effective resolution is on the RP
side in their software.

ACT
Option 4: Certified an SHA-2. -> could be withdrawn.

TCS impat? nulle. -> changing!

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

ST2-256

And use `-skipca`.

Next meeting:

- Fri 14R: Wed 15 afternoon → Thu 16 th