

EUGridPMA+ 67 Ljubljana meeting

Next meeting, EUgridPMA68+, again co-located with EnCo, IGTF, and AARC Community, will be in Abingdon (Cosensers House) from Tuesday Feb 2 till Thu Feb 4, 2027.

Thanks to STFC/RAL and Liam Atherton for hosting us!

IGTF fabric updates

Status of authorities and trust fabric news

DavidG presents 😊

End of dual-hash announced in March 2026

Dropped legacy hashes in August release (1.145)

Despite a migration period of 15+ years, there was still software that resolved SSSLeavy MD5 hashes of the CA name.

Temp re-instated dual hash, but this needs to be fixed downstream.

See Maarten Litmaath's nice overview (<https://twiki.cern.ch/twiki/bin/view/LCG/MajorIssuesWithMW>) which in item 2 links to a merged PR for voms-api-java (<https://github.com/italiangrid/voms-api-java/pull/100>) but ~~but~~ ~~AFAICT not yet released~~ and released in voms-api-java v3.4.0 (<https://github.com/italiangrid/voms-api-java/releases/tag/v3.4.0>). Other users of the canl-java probably need to do the same.

Also, things that RPs think work, but which are in fact side effects - with security implications.

AI era: CPR based on AI-supported reading of CPS docs, resulting in large-scale revocations

SHA1 hashed roots deprecation

Self-signed root updates from SHA-1 to SHA-2 family: recently fixed 5

4 CAs to go

- DFN GridGermany is progressing, only awaiting OCSP validation and HSM import (see Reimer's talk)
- ASGC still needs to confirm migration plan, keeping in mind that it is the catch-all for the Asia Pacific region. The cert has to replace anyway before Oct 4 2027 (when the current one expires)
- ROSA (Romania) and SEE-GRID pending. There may be no SEE end-entities left (to be checked with Nicolas/GRNET)

GEANT TCS Gen6 updates

including the option to work with PQC experiments and the new (S/MIME) hierarchies!

22 years of TCS, currently going for gen6

Uses cases mainly institutional driven, with (small) research case for IGTF certs.

6th gen TCS keeps the same features and qualities as previous versions

reconsolidated the tcs cps and all technical addendums, materially the same as the 5th gen tcs with the same hierarchy

1 certtype for email

5 for authentication

available from <https://www.eugridpma.org/review/#tcs6> (<https://www.eugridpma.org/review/#tcs6>)

CA Update DFN

Reimer

Update on the DFN CAs - in the IGTF distribution since ~2005 running the GridGermany CA at DFN CERT in its own data centre. On the same infrastructure a public WebPKI trust also ran, but that has been deprecated and is fading out. Still an ETSI audit was done last month, but that was probably the last one.

The 'Grid' PKI is still there, with 20 organisations using it, and since 2005 issues 30k certs, with 800 still valid - of which half are Server certificates.

Since a while the Root is also the issuing CA, relatively old with 2048-bit RSA and (for now) still a SHA-1 signature algo. DFN is about to re-write the policies for a while now, but that work has been delayed a bit. The actual text is now almost there, and that new text will describe a new hierarchy with a new Root and intermediates, based on 4096-bit RSA and a SHA-2 based self-signed root.

Meanwhile, the current issuing (and Root) CA may be replaced as well with a SHA-2 based signature and the same key - with a new serial - but the OCSP responder takes a bit more time if the new cert is inserted there. (the client are sending the CA over to the OCSP responder - they should be sending the keyID? - it could just be a software problem in the OCSP responder) The DFN admin team is working on this case.

By Tuesday, the OCSP issue was resolved. The new SHA-2 family DFN GridGermany CA is now in final testing and can be released next week.

CA Update Elliptic UK

Donald Chung - see also the slides

The UKeScience 2B is going to run out in October (31st) 2027, as well as the old Root from 2008, in order to get an orderly transition a new CA hierarchy was launched.

But: the new hierarchy was using ECDSA, but there was still old software out there that could not handle EC keys (canl-java). So for the moment the UKCA can redirect (based on DN) to the old hierarchy on issuance. The old one still uses RSA.

This keeps almost all of the processing chain intact (CErtWizard, CertSorcerer, &c). In this was - with a bypass list - this can be accommodated. Even 'all users' can be added in bulk.

But since the transition cannot yet complete, it requires longer function of the 2B and 2006 root CAs. For that to happen, the validity period should be extended - this will be done in the requested update of the IGTF distribution shortly.

The CP/CPS will be updates accordingly. (2008 Root and 2B are already in SHA-2 variant)

There is an open ticket (129) on CANL-java to address the issue - which is a string comparison issue on matching the algorithm name:

<https://github.com/eu-emi/canl-java/issues/129> (<https://github.com/eu-emi/canl-java/issues/129>)

WLCG may take some time to change ... CANL Java does not seem to be very actively developed, which may be very old by now. And that does not even begin to take into account roll-out delays. CANL-Java usually comes also with other software like dCache. Also STORM (the .it storage) is affected, as well as VOMS.

Independently, also XRoot also does not have ECDSA support. There may be issues in the GCT toolkit (grid-proxy-init) as well - that needs to be reported and then fixed.

Note that also DZScience is using ECDSA!

Now if RPs have problems even with a simple change from RSA to ECDSA, what will happen when a PQC hits? Or SHA-3 (which is already there!)?

The issues are often Java, and probably mostly BouncyCastle - as well as issues with CANL-Java which is outside of control. So there is a Java-BouncyCastle issue (the move to deprecate Java was not yet endorsed)

The issue is that the distributed system is almost an experimental system - too many moving parts and not all can be tested. Like ECDSA was not tested.

So for our RPs:

- ECDSA SHALL be supported by (proposed) May 30st 2027?
 - algorithms agility (SHA-3, PQC) SHALL be supported by December 2027?
 - full deprecation of SSLeay MD5-based CERT_DIR hashes by May 30th 2027?
- Petr has shared some of these ideas (not timelines) with WLCG earlier, but then WLCG showed no interest since they were not pushed:
- <https://twiki.cern.ch/twiki/bin/view/LCG/MajorIssuesWithMW> (<https://twiki.cern.ch/twiki/bin/view/LCG/>)

Should be checked with Maarten Litmaath as well. Maybe after DC27, but early in the Shutdown otherwise people don't want to touch it again.

Testing could be done e.g. with EGI using the OPS monitoring, and get client certs from TCS since TCS is a full dual-algorithm hierarchy (ECC+RSA). But as an independent test, otherwise it would affect measurement of site A/R. But it should be a comprehensive test - which is fine for the EGI ops tests (but not the CA release software tests).

Future developments

Short-lived SSH certificates from a new CA 3A hierarchy

- but what about the fact that a common user name is in the certificate. The UK-IRIS DIRAC - but will they use the same username everywhere?
- look carefully at scope of the SSH certificates

ACME support: being planned

WISE SCI evolution

David Kelsey (UKRI-STFC), Liam Atherton (STFC UKRI)

Created back in 2015 as a joint SIG-ISM and SCI activity: WISE Informatoin Security of e-Infrastructures. This worked particularly well in connecting with the US, by co-locating with NSF, and linking to TrustedCI and the HPC activities in the States.

Early-on it has ocmunity-wide meetings, but also it has working groups on specific activities (training, risk management, threat intel). But the SCI (initially IGTF) activity was a founding activity and that has been there throughout. This provides the trust framework for federate dinfrastructures that was sitting above the detailed wording of policies. This made sense since specific wording cannot be quite agreed across different groups.

AARC-2 produced polict templates, and WISE would maintain it. Sirtfi did that for incident response, and was taken up also by REFEDS.

But the COVID lockdowns prevented the last true-WISE meeting in London, and the joint SIG-ISM/ WISE remote VCs did not make much progress. Specifically, the work on the GDPR accounting policies did not quite progress since consensus could not be reached over VC due to interpretation difficulties.

And with AARC-TREE starting and developing PDKv2, the use case for WISE SCI specific meetings kind-of went away, sinc that was all done in AARC.

Now WISE needs to be picked up again as an activity as SCI. And Liam is willing to work on this :~)!

SCIv2 has some clear deficiencies:

- no federation (but way of trusting infrastructures)
- lack of acknowledgement of assurance levels
- proxies (and agentic work?)

A new vesion of the SCI top-level document is valuable.

- re-establish links with the US colleagues (and TrustedCI)? Adam Slagell is keen to re-engage. Likely Derek Simmel as well. Might be useful for ACCESS-CI as well. And maybe also to GENESIS?
- SCI document is clearly out of date
- import experience on eployment of the AARC PDKv2
- it is still widely liked!
- in GA4GH: there are many (MS, AWS) that are in themselves maybe federated, but they do not trust each other. They were pointed to SCIv2 as a framework y Steveb Newhouse, where it was potentially applicable (but they never had found it)

But how to restart it? Process proposal to get to the right audience:

- as a side-meeting of another meeting? that would exclude either the US people or the rest of the world

- GEANT Security Days (but that would exclude researchers as it is NREN institutional) - but that is mostly for outreach
- the overlap with IdM people is limited.
- the EOSC Federation is an obvious new community - but getting to them is maybe via the Security WG (if the right people can get on it) - and the Symposium/Winter School
- co-locate with ISGC will get AP people and Europeans, but not many US people
- EOSC is a good way to reach out, even if there are no researchers there. But that may not be necessary, since they rely on the infrastructures to get there.

Concretely:

- send out an initial mail for a VC call to establish where to meet and to actually restart? Liam has the mail written out already ... (Action: Liam)
 - then try and find a date that makes sense
- needs a refresh of the list membership first. DaveK will do that (Action: DaveK)
- include link to GEANT (Casper) from the start? (Action: Casper)
- to keep things going, add a WISE (and PDK & Policy) to the standing EnCo VC agenda - and Liam is organising those monthly anyway. By moving between morning (for .au participation) and afternoon (for .us) it can work. Invitation do need to go to a wide community than now to make it known to the WISE/SCI community. (Action: Liam)

AARC PDK implementations and evolution

presented by Liam

As presented (https://indico.nikhef.nl/event/8167/contributions/31721/attachments/11639/18186/WLCG_OTF_-_Trust_Framework.pdf (<https://indico.nikhef.nl/event/8167/contributions/31721/attachments/11639/18186/WLCG%20OTF%20-%20Trust%20Framework.pdf>)) at the WLCG Open Technical Forum OTF this is equally applicable to EGI (as this is basically setting the stage for the Joint Policy Working Group JPWG).

The solid black lines are an (almost) 1-to-1 copy of the policy doc, whereas dotted lines are taking elements/concepts from the old document and adding them (or merging them) into one of the new documents.

The other target is to reduce the number of references to other policies, so that there are no symlinks and the document(s) become more readable (akin to what was done in RAF v2).

Created jointpolicy.org (<http://jointpolicy.org>) (and the jpwg.org/joint-policy.org (<http://jpwg.org/joint-policy.org>) domains) for ease of use.

Updates from the APGridPMA, HPCI, and NII

Speaker: Eisaku Sakane (National Institute of Informatics)

- Twice-yearly meetings of the PMA meeting in person: at ISGC Taipei and at eScience or APAN events in autumn.
- Proper self-audit reporting on a yearly basis
- ASGCCA acts as a catch-all for the region
- at the moment 6 authority members: ASGC, IGCA, IHEP, KEK, KISTI, eMudhra; and HPCI as an RP member
- comms also via Slack (apgridpma.slack.com (<http://apgridpma.slack.com>)) but not yet active

IHEP now has a SHA-2 family based Root with a new trust anchor.

Last one to be done is ASGCCA:

- new CPS of ASGCCA has been received
- the new trust anchor (SHA-2) to be issued VerySoonNow™
- detailed schedule is for Eric Yen to share. Eisaku-san will follow up.

There are several regional collaborations on trust and identity, in particular with the IAM Working Group at APAN. The IAM-WG session was held at APAN 62 in the Auckland NZ meeting. Now Eisaku-san is also the chair of the IAM WG there, so that co-locating APGridPMA and IAM-WG meetings makes perfect sense (going to be an APGridPMA+ meeting).

Future meeting:

- APAN63 in Singapore March 1-4 2027 (conflicting with TIIME in Karlsruhe)
- 38th APGridPMA colocated with ISGC in March 2027
- 39th APGridPMA colocated with APAN64 *also* in Taipei
- and APAN65 in February 2026 in Seoul.

GakuNin updates

Medium-scale demonstrators will start in FY2026 (i.e. soon) with Orthos as a proxy service to provide a federated ID for non-academic users as well, and with account linking possibilities (external IDs).

Orthos has Passkey support built in, as well as an eKYC method (to be implemented in FY2026). Already there is a group management feature for universities, local government, and companies that find it difficult to participate in GakuNin otherwise.

HPCI JP

New developments in provisioning of end-users environments, using token-based access via client software packages. Provided via HomeBrew and as a container image (published in October 2026).

Assurance level enhancements are progressing via Passkeys as an authenticator (KeyCloak as OpenID provider), and a user self-enrolment authenticator initialisation procedure with recovery codes.

For the link to the federation, and Shib metadata registration practice statement is now available. replacing its public (WebPKI) X.509 cert in meta-data with a self-signed private cert.

New model of integration of HPCI identity sources leveraging the federation build on the Home IdP and HPCI as an attribute authority source. In the flows shown (e.g. on slide 11) the user can go to HPCI and identity proofing can proceed with home IdP credentials and then the access protocol translation and attribute services follow the AARC BPA model. The HPCI A3 is then the infrastructure (or site-local?) proxy ("Attribute Services, Authorization, and Access Protocol Translation") in the AARC BPA 2025.

Here Orthos sit on top for Home IdP linking (slide #13), and then the infra proxy combines A3 as well as the HPCI IdM system (HPCI ID equivalent in EuroHPC is MyAccessID) - but the A3 is very different, taken on a different role, and that is using the "MAP Core Middleware" product developed at NII. The HPCI services are then linked to that proxy. The HPCI IdM is then the PIP (Policy Information Point), and the PAP and PDP behind the proxy (slide #14). Implementation uses KeyCloak for the proxy part here. PAP and PDP still open, PIP is the local "MAP" development for the membership structure database (with "M" for Membership).

All to be implemented in FY2027, and then in FY2028 build the new system in HPCI and start production operation!

The conceptual picture presented should be inspirational for other deployments (in AEGIS, e.g. in .nl) and how to effectively connect (national) resources to the federation infrastructure.

Tuesday, 20 October

EGI and WLCG Policy Evolution - introduction

Dave Kelsey

The Joint in the JPWG was WLCG and EGEE - and historically started as a JSPG policy group (although jspg.org (<http://jspg.org>) has been lost) as part of EU DataGrid. The start of EGEE (2004) also started the policy activities in the security WP (Ake Edlund) and WLCG and EGEE decided to develop policy together. In 2010 the policies were revised and aligned with EGI and the EGI Foundation.

The total list of security policies was grown over the years, and there are many policies that are all interlinked. This created referential complexity that makes the EGI/WLCG policy suite less penetrable.

The AARC PDK v2 addresses this by managing audience specificity and simplifying the policies.

The EGI and WLCG policies will now be revised according to this model, as endorsed by the WLCG Open Technical Forum (the policies will go to the WLCG Management Board). The EGI policies are actually further along, as these got updated along the way. Both WLCG and EGI agree that the activity should lead to identical policy (including wording) unless there is a *really, really* good reason. It is anyway the same group of people.

The common document repository in the end was the EGI DocDB, since WLCG stopped using EDMS, and hence WLCG can only refer to the EGI DocDB (and formatted as in an EGI document template since there is no common WLCG doc template known). In this new incarnation from the JPWG there will be the same text, but different cover pages (one for EGI and one for WLCG). This would need a template for WLCG first (and Luna is looking at that). This will be sorted out in the JPWG workshop at CERN (Dec 1-3, 2026).

As for the approval process:

- for EGI, this goes - after consultation with the sites - goes to the OMB. It used to go to the EGI Executive Board, but this may now be overkill for the security policies.
- for WLCG it will be the Management Board, after discussion in e.g. the OTF, since there should be no open issues left by the time it gets to the WLCG MB.

So now we review the policies that have already evolved in EGI but are still in the old rendition in WLCG, but also to re-align quickly, especially for those that are obviously out of date (predating GDPR for instance). And: what are the new risks related to e.g. the token transition.

How to priority and re-map has been presented by Liam in the Monday slot of this meeting.

EnCo: wallets infoshare

Speaker: Casper Dreef (GÉANT Association)

Please connect to

<https://geant.zoom.us/j/63625234173?pwd=N481K1tBKugah63zrYrmDPXOqvJsAB.1> ([https://](https://geant.zoom.us/j/63625234173?pwd=N481K1tBKugah63zrYrmDPXOqvJsAB.1)

geant.zoom.us/j/63625234173?pwd=N481K1tBKugah63zrYrmDPXOqvJsAB.1)

a transcript and recording will also be made available after the webinar completes.

EOSC National Node Example: Dutch National Node

Speaker: Maarten Kremers (SURF)

Please refer to the slides as well - and specifically also read the "Organising Research and a Commons".

Notes:

- The security posture of EOSC, and how that works downwards into the EOSC Nodes, is still very much unclear, with requirements not necessarily propagated to all places where they are relevant.

GEANT EnCo updates

Speaker: Liam Atherton (STFC UKRI)

- WISE meetings adjacent to the EnCo meetings
- WISE SCI now part of EnCo as well
- GN53: unclear how the budget cuts affect EnCo, the GPPC has some proposals on its table, and they (and the PMO) are changing their mind on a daily basis. The 'final' decision will be made at a GPPC meeting Friday next week. The only thing that can now be said is that we have to take likely budget cuts (40% or so).
 - the outreach part may be moved entirely under T0 and be combined with Marcomms (and also the interaction with WP3).
 - the cuts do not necessarily come from the Commission, but the cuts are a result of the GPPC choices. And GN53 being at the end of the 7 year budget of Horizon Europe, and now the money is kind-of gone.
 - how the new FP10 framework will work out if obviously not yet clear with the budget still under discussion.

- Casper is tracking this.
- Do all the work until summer 2027, i.e. nuder GN52

Introduction to EuroHPC (Federation Platform) activities

Speaker: Dejan

EuroHPC has moved more towards federation, with the EFP taking the 'project' as a basis and now allowing PIs to add members to a project that then do get auto-provisioned.

Other questions, e.g. regarding Sirtfi, multiple MFA, REFEDS MFA, vulnerability management, and policy/access remain open.

Updates for the trust fabric

First order review of the (ECC) issues reported in

- https://bugzilla.mozilla.org/show_bug.cgi?id=2083709 (https://bugzilla.mozilla.org/show_bug.cgi?id=2083709)
 - https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/0R3XLJL6FuE/m/0XofdebrAAAJ?utm_medium=email&utm_source=footer (https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/0R3XLJL6FuE/m/0XofdebrAAAJ?utm_medium=email&utm_source=footer)
 - <https://blog.mozilla.org/security/2026/10/20/protecting-firefox-users-following-the-compromise-of-emudhra-intermediate-certificates/> (<https://blog.mozilla.org/security/2026/10/20/protecting-firefox-users-following-the-compromise-of-emudhra-intermediate-certificates/>)
- and for the IGTF included trust roots and intermediates, these are Gen2, Gen4 and Gen 5, as well as emSign Root TLS CA - G1 for InCommon CA 4. So there is No Issue for InCommon (or for any production certs).

When software properly processes CRLs there is no risk anyway, and there is no effective use of the affected issuers anyway.

This was already coordinated completely by eMudhra anyway, and the ECC ICAs were not put in production anyway, no certs issues, ICAs revoked - all is fine.

The concern by Mozilla is just their lack of trust in software support being able to deal with revocation of ICAs and CRLs; hence their OneCRL actions.

Summary: AI/LLM tokens are changing the industry (and the perception).

Update from the Americas

Speaker: Derek Simmel (Pittsburgh Supercomputing Center)

Quick review of InCommon CertiNext dependencies

- the GTS Cas cannot do prefix naming. In due course that is no longer required once (and only once) TLSClientAuth is dropped for all these CAs that are potentially issuing "/CN=" -only naming. Since Chrome deferred the deadline, this point has now moved to ~ end 2027.
- Once there are no possible name collisions again among public CAs that issue directly into an FQDN CN space, the requirement coming from the Federation Document is no longer pertinent to Server SSL certs
- all DigiCert roots and ICA shall be dropped - DigiCert has not re-engaged and there are no valid subscribers left - will be dropped in 1.147

ISGC Security workshop and promotion

Maarten Kremers

To spread the word about ISGC, the conference relies (too) heavily on the PC members to communicate. While Maarten can contact GEANT and the EOSC community, what are obvious channels?

Some channels (like the VO management channels on the VO portal) exist but are not the appropriate ones.

While for the security workshop the need is for local engagement (given we would promote a

train-the-trainer approach), that does not necessarily help for the ISGC conference proper, where the mix of systems, policy, and applications is a key element of the value of the conference.

Discussion about engaging socials, and how to get a 'viral' vibe to ISGC...

Wednesday, 21 October

Random notices

- the eMudhra G3 ECC root is now being pulled as well (30k certs affected), as per https://bugzilla.mozilla.org/show_bug.cgi?id=2083709 (https://bugzilla.mozilla.org/show_bug.cgi?id=2083709) and <https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/0R3XLJL6FuE/m/VAgSvefvAAAj> (<https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/0R3XLJL6FuE/m/VAgSvefvAAAj>).
- There may be an issue for OS-provided trust stores as used for validating token issuers' well-known endpoints. RP sites may need to update their trust stores (available for Ubuntu and Debian now) if the RP software is not processing revocation information.
- the PHP issues CVE-2026-109618 and CVE-2026-109619 are distracting to the meeting as well. The Chair apologizes (but set `session.upload_progress.enabled = Off` as soon as possible and restart anyway)

Policy Evolution - trusted lists and trusted issuers

On token issuers, AARC-G071, and peer reviewed self-assessment for AAOPS, and transport vs issuer trust

Speaker: Dr David Kelsey (UKRI-STFC)

When 'we' move to tokens, the communities have to work out how to get 'their' list of trusted issuers. The IC people noted that they are now 'trusting' a lot of things, and are considering why they are trusting? What about identity vetting of users? What about ...?

This is a topic that the IGT could take upon itself. For the CAs this worked since these were 'national' capabilities and not tied to a particular community or collaboration. So there the trust was independent.

Mischa can put a lot of questions to the group, and this was discussed in the last TTT meeting (see notes there <https://indico.cern.ch/event/1730175/> (<https://indico.cern.ch/event/1730175/>)):

- the TTT got rough consensus on having a separate trust list for token issuers, rather than having to rely on the entire OS trust list.
 - then 'we' have control
 - it can weed out CAs that are less trusted/less well known
 - move beyond decision on a case-by-case basis (like we did for the AWS CA For CILogon)
- Do 'we' think that we need such a trust list: a subset of the system CAs.
 - then we need to distribute

This would not be an assessment on a per-token-issuer basis. Only the issuer URL is then used (to get the .well-known endpoint) and then used to obtain the key used to sign the JWTs.

In the end we rely on WebPKI to get the signing keys (and the trusted URL), and that trust may need a bit more than just webPKI.

Things have improved in DCV land as well, e.g. multi-point observability for public CA cert issuance.

- it will be a small (sub)set of CAs anyway. It is like accepting the set of permissible VOMS servers in the past for AC-based access.

Note that this would not resolve then trust in the out-of-band distribution of URLs, and that comes to the sites because the sites just fall for these messages. So it hinges just on the write access to a wiki. It is very easy to spoof.

- this could also be a role for IGTF, but then what should be done, and what is the assurance level? Who should be distributing that list?

- this does not move beyond the current dual-use of CAs (until eKU TLSClientAuth in public trust goes away in ~2028)

So maybe there should be just policy guidance, and then monitored out of band?

- a small list of trusted CAs in place does not prevent others to set up a token issuers, form a different URL, but using the same trusted CA, then convince sites to configure that CRL.
- the entire security now hinge on the protection of the source of the URL list, which would now is likely just a wiki. So the ecosystem security hinges on individual credential security for write access to such a wiki.
 - so use a properly signed RPM or JSON with that list?
- then do a (9)peer-reviewed) self-assessment based on AARC-G071/AAOPS, and then give out trust marks for that?
- while or the CERN experiments it might work due to the User Office registration, but do the other communities similarly meet tracability needs?
- OI DFed will/may take that problem away a bit?

At the moment there are more questions than answers:

- how to distribute the trusted token issuer endpoint URLs
- why would sites trust a list that comes from WLCG/the experiments anyway?
- which software do we trust
- how would other communities that WLCG share trusted issuers? Are these issuers shared on a common endpoint/AA Operator?
- what about the EOSC Nodes? There the tokens should be portable and use introspection across domains.

And then still also the LHC experiments are still using VOMS proxies (and many other communities are still happily using VOMS, and the VOMS server, C-based, is still supported as well). All RP software also is still happily using VOMS, and many communities are also still VOMS-happy :)

- also the EGI Communities will like to have a body to assess/distribute trusted information
- the same holds for communities that are actually global - which is the IGTF role
- the AA operators will be relatively small in number

In summary?

There is a role for the IGTF on peer reviewed self assessment of the (limited number) of trusted issuing operators

- already a set of issuers, including the ones from WLCG, NFDI, and also the GEANT Core AAI , SRAM, went through the self-assessment based on AARC-G071.
- this will be the token issuing *operator* trust mark
- the check against AAOPS is not too complex (Bas was fine with it). It can be done without having your own token issuer practice statement, and just refer back to the AAOPS guidelines directly.
- this is what the IGTF is already doing
- an operator will then have one or more URLs for token issuers
- the URLs can then be signed by any (trusted) CAs (as per the previous discussion, maybe - the list is then the list of all CAs used by all 'assessed' token issuers ...)
- the IGTF to maintain a list of peerreviewed trusted operators?
- relation to AEGIS: AEGIS validates the interfaces for interoperability (in software/services). The IGTF can do the policy peer review process and publishing of the list of operators.

It does mean that AA operators will need to partake in this process. Some mild external push would be helpful (it is far less complex than ISO27k), but it does mean that 'the members want it'. And the acceptance of your tokens is another good pressure point.

So if WLCG is going to use (Euro)HPC sites (and they will have to!) then having more points to convince the EPF that WLCG is trustworthy and using AAOPS for that is one (part of the) puzzle that can help gain access? Almost all new capacity for WLCG and the like will be in (Euro)HPC centres.

How to get the token issuers to the meetings to present/share?

- resource providers can insist on the trust marks, but then there are too many resources in WLCG, so WLCG may not care about resources dropping out.
- work with EPF to requirement AAOPS? Then WLCG could go to the national share, so that will be at the HES to decide. So the request (e.g. when running ARC CEs) should come from the hosting sites, not EuroHPC FP. There the pressure from end-users like WLCG would maybe trump other requirements?

Som of these items may need to cycle back to the WLCG TTT.

AAOPS AARC-G071 review

Can we get a clearer version of AARC-G071 that is easier to process and use as a basis for self-assessment.

- work on simpler version (check-listable) of G071 is needed
- check whether the content is still up to date
- then the peer review can be lighter
- start re-writing in Abingdon, but prepare beforehand - and get access to STFC colleagues

FIM4R evolution

DaveK

Writing a version-3 of the FIM4R paper was put forward (previously already) since v2 is rather old and got input from 40 individual communities. Since, communities have moved to using service providers for this, so it is unlikely that these would come back to write an update for federation, since there are federation providers now. For smaller communities: these are largely under the radar, and are unlikely to engage anyway.

Despite the good plan in February, there has not been much progress since the Amsterdam FIM4R meeting. Can we get to some progress before the Karlsruhe meeting?

- FIM4E (while FIM4L is not very active) - since they should be writing requirements, and FIM4E has Licia involved

What should be in AARC-FOREST to address these issues?

- OpenID Federation
 - Wallets
- that does not mesh well with FIM4E

What about doing the analysis on the FIM4R v2 paper requirements, and go through the 40 requirements there and check whether they have been met? And maybe, in the process, also identify any gaps in there.

But there is a significant lack of people (even if money is there ...).

For Karlsruhe, we can fill the agenda, but not enough cycles to write a new paper.

PS:

Hopefully profiling the Wallets will be not significantly different between research use cases and R&E in general (but will likely be different from other societal use cases).

Present

On-site: Jan Jona Javorsek, Dave Kelsey, Maarten Kremers, Donald Chung, Jan Chvojka, Liam Atherton, Peter Bolha, David Groep, Casper Dreef, Eisaku Sakane, Dejan Lesjak

Remote: Adeel ur-Rehman, Jens Jensen, Mischa Salle, Petr Vokac, Miroslav Dobrucky, Reimer Karlsen-Masur, Derek Simmel, Scott Rea.