53rd EUGridPMA and IGTF meeting

Tuesday, 28 September, 2021 13:30

Dear IGTF, EnCo, EOSC ISM, EUGridPMA and AARC community members!

Thanks to all those that joined the on-line sessions of the 53rd EUGridPMA+ joint meeting. As we are hopefully moving closer to an in-person trust building environment in January, people participated in this hopefully last fully virtual event, spread over all time zones and from all our regional PMAs. Plus a large attendance form the AARC, GEANT Enabling Communities, EOSC ISM, SURF, and IRIS communities. Thanks for joining!

In this summary, I'll try to give an impression of the main discussions and results. As usual, much is also contained in the slides and ancillary materials and documents that are attached to the agenda at https://eugridpma.org/agenda/53 or linked therefrom. In this summary:

- APGridPMA and TAGPMA updates
- WISE SCI v2 'how-to' guide development
- Security Baseline for EOSC - PDK adoption and evolution
- AARC PDK policy – evolution for the EOSC and beyond
- RCauth.eu updates
- Enabling Communities: progress and next steps
- Trustworthy tokens
- Evolution of CAs for WLCG Ops
- Beyond the Normal State Of Operations - Jens' Soapbox
- Assurance
    - Demo: assurance with eduBADGES, eduID and ReadID (by Peter Havekes)
    - Assurance Evolution (by Jule)
- KENET CA update
- Operational matters
- Attendance

The next 54th EUGridPMA+ meeting is scheduled for Tuesday January 25 (09.30 CET) till Thursday the 27th mid-day, and will be **in-person** in **Garching near Munich, kindly hosted by Jule Ziegler at LRZ**. As a backup, virtual participation will of course still be possible, although must of the trust building and innovation happens more naturally and productively in a face-to-face setting.

Hope to see you soon!

Best, DavidG.

Agenda and Next Meeting

The next meeting will be in-person in Garching! From Tuesday 25th January 09.30 till Thursday 27th at ~ 13.30.
"How to trust trustworthy token issuers" was added as a topic to the agenda

APGridPMA updates

There are fewer CAs operational, with some of the regions falling back to the catch-all at ASGC - but at the same time in some countries communities are getting better linked through APAN to eduGAIN, offering new possibilities is that area - and there is an IAM WG at APAN with support for SAML2 and federated authentication services. Also GakuNin at the NII as a trust framework is being linked to both the IGTF assurance framework and REFEDS - connecting to eduGAIN. The GakiNin trust framework is (unconfirmed) also including opsec policies and practices.
Also in the AP region there is a move from IAM to move to tokens by the user communities and infrastructures.
Next APGridPMA meeting in at ISGC2022 at 20-25 March (2022).

TAGPMA updates

NERSC has now been withdrawn in favour of InCommon CA services. Also ANSP has plans to re-engineer their infra on the longer term. Jim Basney is having lots of CILogon CA migration to a new infrastructure (to AWS EAST), although it is taking longer than initially anticipated. Digicert's status of actually issuing IGTF compliant certs is unclear.
There is again a WoTBAN&AZ workshop on October 18th 10AM-2PM EDT (UTC-0400)!
See https://sciauth.org/workshop/ for the programme and call for contributions.
At least on the US WLCG side (Mine) are looking for migration scenarios that allow for a working migration.
The ARC-CE will accept _a_ token, likely not multiple types - they have (ARC-CE) been involved in some of the Token CE Hackathons for interop.

WISE SCI v2 'how-to' guide development

How to check your maturity against the SCI v2 framework? Based on the experience from the current infras and prepare for a potential SCIv3. And take in the input from AARC PDK evolution. The current state is in the slides (https://indico.nikhef.nl/event/3280/#5-wise-sci-v2-how-to-guide-dev). The "Security Plan" is a pretty difficult item to describe - since a 'plan' is rather abstract.

Assessment Chart A and B differ, but which one is the 'better' option is quite dependent on the question, based on the FAQ guidance. Which one is actually better depends on the feedback form actual experience. This needs volunteers (welcome: contact Ian and the WISE SCI WG! For the moment only UK-IRIS is working on this with an actual person assigned) And CS3MESH4EOSC, as a true federation with independent infras, might be extremely suitable for SCI as a template; alongside of course the EOSC Exchange providers.

For the SCIv2 how-to guidance: decided to publish 'here and now' - and of course also inform the WISE SCI WG to announce that it's ready (and can be improved later in a subsequent version). The WISE publication process is not yet formally defined, but could take inspiration from the REFEDS process (although that is rather heavyweight). And separate normative and informative documents (with the 4-week periods for normative documents, and the others more lightweight).
Rest of the process discussion will be included in the PDK evolution discussion (along with the relative roles of WISE and AEGIS in adoption of normative frameworks)

Security Baseline for EOSC

The EOSC is more loosely coupled.
#5 is the 'core of the EOSC model': but the people who know what #5 means, are anyway more likely to be knowledgeable :) The controls are a bit 'weak', but this is a hook for follow-up after an incident to address participation in the EOSC - and as a reputational backstop.
Adding it to the FAQ can help (with the **** incident and EC*), but any list risks being taken as a limitative one.
Encouraging risk assessment is essential to get awareness and compliance.

Many of the items extend Sirtfi, but it goes a bit beyond that. This FAQ should be specific to the Baseline, as Sirtfi already has a (non-technical) FAQ (this EOSC doc should have a standalone FAQ). And this one does make Sirtfi items more specific.

on #6 - distinguish between information gained as a result of service access, vs. the (out of scope) information contained within the service. This item in the FAQ is challenging to word unambiguously.
Also confidential might be operational data like software versions - or even use aggregaes (commercial in confidence).
The intent of #6 is wider than just personal data.

The "named persons" should be designated, but not necessarily disclosed or registered with EOSC. A role is not sufficient. Because roles maybe unoccupied, but a person can be found. In the end the boss goes to jail anyway in the end. But at some point this also needs to be 'tested'. "Someone should own the process of monitoring this baseline, and that's the person you want named here". So it's a *process* contact point, like in ITSM processes
The Trusted CI framework also addresses this issue by emphasizing the need for sufficient staff effort.

The generic contact points come out of Sirtfi anyway.

Discussion on the evolution of the document should be possible as well - through the EOSC onboarding process we would be the natural spot, i.e. during the (AAI) onboarding.

PDK evolution:
Having reviewed the document, this is sufficiently different from the 'conventional' one to warrant adoption into the PDK on its own. Other PDK thoughts:

- the PDK needs a 'lijmwijzer' (the "Bison Sealant Advisor") to find the most appropriate and comfortable one.
- for the Baseline AUP we did *not* want anyone to change it. This Security Baseline is different, as it can be used as a template and can be changed.

AARC PDK policy – evolution for the EOSC and beyond

The WISE SCI working group has been working on HowTo guidance for the assessment and encouraging the infrastructures to actually do their self-study. This has experienced slower uptake than anticipated, and meanwhile the US SLATE project has noticed that the current version does not fully take federation into account - which does call for an SCI version 3 which incorporates that aspect more explicitly.

The policy templates from the PDK help implementing the SCI policies - most of them being templates, apart from the AUP that really ought to be adopted as-is without modification for interoperability reasons. Yet unlike the AUP, new templates may well contain optional components, or 'parallel' templates like we identified in the Service Operations policy (tightly coupled) vs. the EOSC Baseline Security Operational Policy (loose distributed system).

Which policies are the most urgent / most useful to tackle? Even the baseline is at times seen to be lacking items regarding liability (of the user towards the provider). Focus on a specific document one at a time may actually be more beneficial than working on all of them at once.
Considerations on the future:

- there is a role for both the AARC Community and AEGIS (in approving it), but all collaborating under the auspices of WISE. AEGIS is too closed for that and has a tighter focus.
- there is an unmaintained Moodle course (hosted by GEANT)
- the templates are now in google docs, which is less than ideal, even if it does allow easy download in many formats.
- lots of work has happened but all slightly diverged from the main PDK and not yet brought back into the fold
- the challenge for WISE is to re-engage better with the US efforts after staff changes in the US.
- concrete work can be done in the CS3MESH4EOSC context: the project did not 'know' about the PDK till now but where policies are needed
- start with the documents (with feedback from Ralph) on service operations, and one other one (top level maybe?)
- ELIXIR also recently added a new policy (on joining?) that was recently released under an open license, a topic not addressed in the PDK
- The role of the top-level policy is slightly different, usually triggering a thought process by the infrastructure to consider responsibility, assignment of roles and responsibilities.
- The EOSC baseline in effect becomes like a top-level for the EOSC connected service providers

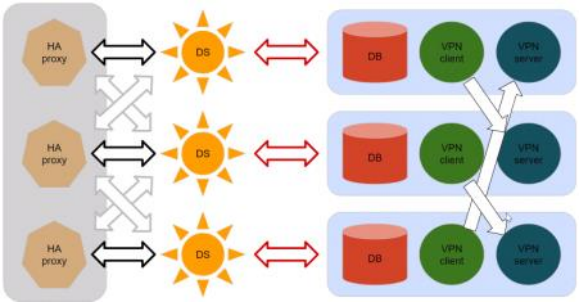
The actual wordsmithing and heavy-lifting - if it does not happen automatically in any WISE WG - can benefit from the input of the broader AARC Policy Community, where some effort can be available.
For some reason the Sirtfi WG does work better over zoom, probably because Tom Barton does a lot of work in-between meetings (and maybe manages better to encourage others to do likewise).

Proposal is to start with the evolution of the service operations policy (security baseline), and then proceed to the top-level policy. The centre for this work would be the WISE Wiki, with a push every 2 weeks in a shortish videocall (in the later European afternoon to get US participation). Hannah will initiate this on the WISE SCI WG mailing list.

Hannah will also talk about this at the upcoming WISE meeting on 26-27 October 2021.

RCauth.eu updates

The next iteration will move towards signing by 'your closest' issuing instance. It took a bit longer to get the technical issues straightened out based on the current VPN layer:



but the technical implementation is rather complex - besides the procurement and unfortunate pandemic issues. And synchronisation between sites takes time (since major upgrades relies on few skilled people, and sending private material needs care and attention).
But having set this up, the various 'failure modes' can be mitigated. Several components can be 'lost', and the scenarios for recovery will be different.

Meanwhile, the operational experience and documentation (some of this on github at https://github.com/rcauth-eu) can be re-used by any CA that wants a 'cheap' on-line CA that meets the technical accreditation requirements - e.g. for currently-offline CAs that want to go online. And it can be for non-auth purposes like digital signatures which could also be done by strong the short-term certs and making those available alongside the signed doc and a timestamp server. There are more user stories, like multiple-assurance CAs, R&S 2.0 + RAF, and multiple profiles. or RCauth as an OIDCre provider.

Enabling Communities: progress and next steps

As an addition to the slides shown by Maarten: the Assurance paper has been accepted for publication after positive review. And the Sirtfi group is making good progress on a 'version 2' of the document, taking in the feedback from the survey that was sent out over summer. Registration for the SIG-ISM and WISE is now open.
At the 2/3 mark for GN43, the preparations for GN5 have started - planned to commence January 2023 - with preparation sessions in the run-up to writing down the plans. Meanwhile this is the time to review the ongoing activities in T&I EnCo - with input from those not directly involved contributing to the work plan very welcome as well. The URL is https://edu.nl/ctxxg:

- Assurance is a bigger challenge, and is there more we can do there? It is becoming part of 'R&S2'
- How does the move to tokens affect other communities? Can we help those to transition, esp. for the smaller communities?
- Both Shib and SSPHP now have a fully compliant OIDC OP implementation - also useful for proxies
- Climate modelling community gets not that much attention - they are at OpenID v1, and some PKIX, but they are not that engaged. [JJ]
- One of the lessons UK-IRIS is learning is merging both very well organized communities like those at the LHC, and at the same time lots and lots of small groups in astrophysics, and communities organized around facilities like Diamond. They could all need a different ways of engagement. And things like tokens pop up everywhere.
- Can those be engaged in the IGTF (and EnCo) process as a relying party? They show up a bit at FIM4R, but not in the 'techno-policy' side.

The TNC Trieste call for proposals is not yet open. The expectation is that is opens soon (October 12th), and closes Nov 30th for single presentations. Should we plan a workshop/BoF of FIM4R/EnCo/assurance alongside TNC. There should be

one (if it's not being organized already). The challenge would be to get the communities there.
We might push in a number of single papers to warrant a session - assurance is the obvious candidate, with both Jule's published paper, and the FIM4R assurance work. And someone from the REFEDS R&S/RAF 2 workgroup community on adding assurance attributes to the core set.
Trustworthiness of tokens (e.g. from the IGTF community based on WoTAZBan) should be added here.

Trustworthy tokens

How do 'we' (relying parties) establish trust in the 'new' token issuers? Is that also best done with profiles and accreditation, e.g. through the IGTF, and is then the AA OPS guidance sufficient?
The issues regarding identity assurance and vetting do not go away, and the AAOPS guidance _is_ technology agnostic. With the active move to tokens by some communities, it is getting urgent to establish this trust.
Defining a trustworthy identity management service is of value to the community. We preferably do not want rogue services entering the ecosystem. Is it the IAM/proxy instances that we should be reviewing and accrediting?
Since nobody else is looking at the policy side of things, with lots of work on the technical side (where trust is important, but specific to the technical implementation).

As an operator of a token issuer, the operator should check against the AAOPS guidance and then present that through a peer-review self-assessment and only after approval it would be included in a 'list of trusted end-points'. Each of the token issuers would need to be in a 'list'. In general, people _do_ think having security policies in place is useful (even if they do not necessarily like it). But that's just one way of looking at it, and it might depend on the community.
And there are tooling limitations for now - so how did that work in the early IGTF days?
The token model is more community focussed and less 'user-centric', which was one of the reasons we needed coordination early on where authN/AuthZ was separated. The token issuer it more blurred, where e.g. proxies are both sources and OPs, and sometimes just carrying somebody else's attributes. This does fit the AAOPS checklist options, where you need to verify the instance, not (only) the software.

And **now** is the right time given that it's moving close to production. And AAOPS can help, but then how to we do the peer review. The strength of the original CA coordination group was that the peer review also helped by having CAs with similar issues talking to eachother. So they learn also from eachother. So should the proxy operators present to each other (e.g. in an IGTF context) so that they are both trusted reviewers and learn from each other.
There is an IAM users workshop - maybe that's a good place to discuss this as well? Just before the November GDB. Tom Dack already had ideas to add a policy slot there. We need a speaker for that slot… Hannah volunteers for the first assessment - and give the talk if at all possible.

Add a slot there to discuss policy on deployment, operational trust, how to get identity in? As a short 'awareness' slot in such a meeting, and at the NSF Cybersecurity Summit at the token workshop. And TNC next summer to broaden out!

It may be a good incentive to put 'ad hoc' communities onto trusted existing issuers. So not set up your own, but then use of, say, CheckIn, eduTEAMS, an managed IAM, &c. And a network of token issuers that's trusted.

The personal identity proofing stuff and its provenance is passed through.

Evolution of CAs for WLCG Ops

It's about host (and not user) certs, and the scope is all kinds of cloud-provisioning CAs (so not only LE but also the other automated DCV CAs that come with cloud provisioning 'by default' for web-only DCV).
And any configuration of trust is at the site level, and - at that layer - is not a WLCG specific decision but has wider impact related to other communities.
The traceability discussion - especially in the context of composed services and layering - needs to be kept in mind when selecting trust anchor beyond their proper scope.
The CAA records at the site level in effect have not been considered (in "don't have to get approval" for instance).
The name changes for public web CAs are beyond our control (for TCS, but also any other publicly trusted CA). For some, that might end up with the NULL subject name (LE now has CN only)?

For WLCG, there will be a recommendation to its management board to set up a Resource Trust Evolution task force (and list) by David Crooks, with representatives from WLCG stakeholders (https://twiki.cern.ch/twiki/bin/view/LCG/ResourceTrustEvolution). The needs need to be clearly identified. David Crooks and Maarten Litmaath are leading the WLCG effort.
Participation from the IGTF community is obviously welcome. Significant part of WLCG will be on multi-community resources, with more providers becoming multi community. So the WLCG workgroup is a good place to have the active discussion and participating broadly there, although the output cannot as such be an direct IGTF output - although synergies are actively sought.

The issue often encountered is in storage where data transfers also go to and from web browsers, so public trust is needed (and only a limited number of issuers like TCS and InCommon are both IGTF and web browser trusted).
And there is an AuthZ issue - "why trust a commercial cloud endpoint that tries to suck in (sensitive) data?" So is there a resource registering service (like GOCDB) that now needs dynamic registration. And who is 'responsible' for that service, e.g. when you're sending sensitive data. And there's a mix of commercial and trusted services. And how does suspension and traceability work then (and revocation)?
It might be good to have also reps with sensitive data on the working group list.

So … sign up via the web page at https://twiki.cern.ch/twiki/bin/view/LCG/ResourceTrustEvolution

Beyond the Normal State Of Operations - Jens' Soapbox

The space of a CA is very large to cover all of these dimensions, so things will break. Can we lessen the impact of a break, or make them break less often?
E.g. for secrets, where the 'middle case' is the best one, and both extremes (no secret, or shared secret) are both bad:

Now, some people are worse at keeping secrets than others - like managers or their PAs. Or tech staff who take things home … and loose it or leave it around. And a simplistic 2-out-of-3 breaks because one can brute force the third piece - and you want a simple scheme so you don't need a cluster to do the math.
And more complex schemes (like SSSS) do not really help, since pieces are hardly ever used, and the keepers loose their pieces, or the pins that protect them. And people leave slowly, and the redundancy is slowly lost. And revocation in e.g. SSSS requires a new full rekeying.
But is the RCauth.eu distributed model with key sharing is actually a solution to the problem? The key has three active copies, shared with a secure protocol. And the key is 'safe' in the sense that you don't have to give parts of the key to managers since the redundancy is at the site level. As long as you trust the (people at the) site, and the access to the activated key is temporary (and the rest is in an HSM). Yet: how can it fail? You need to rebuild from the other two sites (if you indeed destroyed the non-HSM-based key). Getting the OTP distributed takes a lot of time …
Quantum Key Distribution solves that, but can 'normal' crypto do something similar in replenish the OTP material? The OTPs exchanges used different trade-offs, and in some cases there is not enough pre-existing pad left. And you need to keep the OTP secure all the time. What's the other option? Reconstitute from the two other sites using XORing material (exported keys or a non-HSM-locked copy). Or start with more sites (with N>3) and focus on service availability instead (in case the HSM were to die, which is a rare event) by allowing for the rare failures).

Can such an RCauth sharing *model* be used for other kinds of stuff? A 'guard each other's secrets' scheme where you share with friends rather than managers. And your friends use their secure infrastructure to protect your secrets.
For preventing failure modes, the UK eScience CA uses robust software that does not change all the time (bash+perl), since other software like python etc. break to often backward-compatibility. Even people are at times overly 'helpful' (by

design…) and a security risk.

But in general, there is not enough *forward* planning to recover from risks, and if it were there, it is not shared enough within the community. This knowledge is scare and valuable! For example, the PMA Wiki hardly sees any use - and the last was by John Kewley … well over a year ago. There is lots of experience between us, but we don't sharing this at the technical level (although we do discuss models), but there are gaps that we did not cover!

To get the sharing working, should we not be writing more papers for conferences, sinc ethey give us concrete and firm deadlines (and thus get things done). It worked for the Assurance stuff … and TNC, ISGC, NSF CSS, &c are there for us. And a paper with many authors in this case is actually good, with more people contributing.
We have more technologies now than we had before. AppInt has a chat channel - would such a channel for IGTF operations and operators be useful nowadays? RCauth has a (private) channel as well. So a PMA channel on KeyBase, even if it's a subgroup. A Keybase channel to 'keep communication going' and keeping in touch might be a good complement (or alternative for some) for long meetings. For example a working group channel on sharing and managing secrets? The people are the most important element (and having a bit of funding to work on progressing e.g. RCauth). You have to keep the momentum up.

As an attempt, Jens will setup a Keybase group (open to all IGTF) to work on the paper on key sharing and the RCauth experience - usable for sharing keys in any kind of authority having secrets 'you care about'. There is stuff there worth sharing.

Assurance

Demo: assurance with eduBADGES, eduID and ReadID (by Peter Havekes)

eduID is a guest identity provider for the Dutch ID federation "SURFconext" - connected on request to a specific service provider (without much assurance). The new eduBadges service adds 'microcredentials', but they have to live much longer than any specific account, and thus eduID - a persistent identifier but not assurance - is a natural choice for authentication. But lacking vetting data, the eduBadges are linked twice: both to your institutional credential as well as your eduID.
But that fails with non-local students that could not do a higher assurance identity validation. This triggers the need for a remote identity vetting. The PoC aims to implement that, based on InnoValor's ReadID app and NFC. The service is currently in the PoC stage, do the tech works, legal and contracts still to do!
The technical part is now the easy bit. And this now looks almost too good to be true :)

The workflow is reminiscent of the step-up workflow, adding information to eduID - and you only do that only 'once' in your life, which creates a persistent step-up of the eduID account to which it is linked.
The most difficult part if holding the NFC chip still! And from the T&I Incubator, there will some issues with Apple devices.

The number of countries pushing out NFS is pretty high - it's not only standard but also actively promoted. And ReadID is being used by many governments as well (NL, UK, …).

Assurance Evolution (by Jule)

The assurance paper is now almost done - the ISGC paper has been accepted for publication (as-is). The preprint is on Zenodo (https://doi.org/10.5281/zenodo.4916048). Should we do a whitepaper on the need by specific research infrastructures on how assurance is used there. That study, alongside the paper, can then be used to push federations and IdPs (or eduTEAMS) to make the use cases more clear.
With the backing of FIM4R, we could also promote the use of available technologies (like the ReadID from above) to make the assurance step-up more available and easier to accomplish.

The FIM4R Assurance Workshop Hannah organised was very useful, but it remains difficult to get concrete use cases out

of the community. Ralph has the PRACE AAI infrastructure where the registration process is currently distributed, and each site for now requires very specific local information and this information is not currently used (and thus the work duplicated). At the moment the other sites do not have sufficient information to make that adequacy decision - and maybe even the REFEDS RAF does not yet spell it out in sufficient detail either. The 'loose' definition of vetting is at times seen as a risk for sites that are more tightly controlled (also on attributes that may not be considered relevant on all sites, like nationality vs. country of residence vs. country of active affiliation). Similar considerations are far from unique for PRACE and also pop up in other infrastructures.
The 'strength' of the attribute values comes into play, and 'really seen an identity card' is at times really required.
But then, is the 'origin' site willing to share sufficient data with its peers, even if the information is well collected? That release is generally based on consent of the user - and as long as the attribute (values) can be filtered. it comes down to trust *within* the infrastructure …

This is supposed to be covered by the REFEDS RAF framework, but that may not be obvious since many of the practices are hidden in referenced (indirect) documents whose references are listed in the RAF itself (like Kantara, eIDAS, IGTF, &c). So this information - when available - can be used already today. Jule will contact the (local) PRACE reps as well.

And it does make sense to attach PRACE to the FIM4R whitepaper process (and PRACE 6IP ends mid-2022, and the future beyond that is not yet clear, but after PRACE it may also be relevant for EuroHPC). Both Jule and also Mario Reale can pursue this (since Mario is involved with PRACE's request to set up the AAI in a GEANT context).

For the FIM4R assurance work - establish a separate meeting for the editorial team (and join the REFEDS Assurance calls)

KENET CA update

The CA remained small for a while, and much work was done to also set up a local federated infrastructure with compute and storage resources. That got more awareness from users regarding computing, and this in turn will fuel demand for federated identity - and the CA as well. That will need new hardware (the current setup was from 2016 using then-available hardware), now will be setup with up-to-date hardware. And have a strengthened team to support the CA (and ensure continuity in ROBAB cases). This should also get more people to perform operational tasks as well as self-audits and presentations. The COVID situation has also adversely affected the organisational readiness and planning. Integrating the CA with the other KENET services is now planned to progress apace - now that it concretely enhanced the quality of service it provides to researchers alongside the compute, storage, and web conference services). And it can integrate well with the federated user authentication.

Future plans could include integration of 'eduGAIN' services with the CA with federated authN.

The upgrade will include some changes to the CP/CPS - the online repo has the new version. https://ca.kenet.or.ke
Nuno to have a look at the new one for the peer review (and Ronald for Nuno's LIP CA)

Operational matters

- self-audits updates: TRGRID update has been circulated and the CA is now awaiting confirmation that it's OK. By the end of the meeting this will be confirmed and OK. RDIG CA is now OK and done!
- MDGrid will be suspended - lack of domain name grid.md and no active subscribers in v1.113 (Oct 4th)
- LIP CA self audit: steadily dropping number of subscribers, since RAs are closing down as subscribers migrate to TCS. Naming issues with DigiCert TCS, and also took a long time with Sectigo TCS and CABF rules (and the 64 character and EV rules). The future of the LIP CA is as a backup for LIP itself - until June 2023 when it's a year before the root expires (in 2024). If the TCS issues do not stay away, it will remain and be extended.
  Ronald Osure will be peer reviewer
- KENET presented the CA updates and assessment, with Nuno the designated peer reviewer
- Changes in the TCS CA naming could happen as CABF is revising its guidance, and the back-end (Sectigo) changes practices for self-protection (e.g. replacing locality with ST since ST in some cases has an ISO backed document for checking). ACME for IGTF OV is still pending - many operational issues defer this on the priority list again and again.
  DFN is onboarding many German orgs as well - and 70 of these orgs got stuck in OV validation for several reasons

(mostly issues with chamber of commerce entries and/or long names). "ESO" is the current example - surprisingly they don't accept names from international treaty orgs that are short. But then also Sectigo is under the same useless pressure from folk like Ryan Sleevi (i.e. Google) who think agility is more important than security and trust - as shown in https://connect.geant.org/2020/07/15/the-tough-world-of-internet-certificates.
But the CABF mess remains also with any new provider - but e.g. storage access requires both public and IGTF trust. Maybe, maybe, the GEANT position paper sent to the EU on independence on trust anchors (https://www.geant.org/Resources/Documents/CAB_GEANT_Statement-GPiesiewicz.pdf) can help -- maybe in a decade from now? …

Attendance

We thank the following people for the extended attendance and stamina for sitting through the virtual meeting: Baptiste Grenier, Bill Yau, Cosmin Nistor, David Crooks, David Groep, David Kelsey, Derek Simmel, Eisaku Sakane, Eric Yen, Eric Yen, Hannah Short, Ian Collier, Ian Neilson, Jens Jensen, Jezreel Nyange, Jule Ziegler, Lidija Milosavljevic, Maarten Kremers, Miroslav Dobrucky, Mirvat Aljogami, Nuno Dias, Reimer Karlsen-Masur, Ronald Osure, Saruni, and Uros Stevanovic, Mischa Salle, Peter Havekes, Ralph Niederberger.