sharemd.nikhef.nl

# The Prague 64th EUGridPMA and AARC Policy Meeting Summary - HedgeDoc

40–51 minutes

---

The 64rd EUGridPMA+, AARC Policy and EnCo meeting has just concluded, and I would like to take this opportunity to thank again Jiri Chudoba, FZU, and Daniel Kouril and Jan Chvojka and CESNET for hosting us in Prague.

In this summary, we give an impression of the main discussions, results, and resulting action items. As usual, much is also contained in the slides and ancillary materials that are attached to the agenda pages at and linked therefrom. These notes were created collaboratively by those present, and these contributions are much appreciated! The live version of these notes at https://sharemd.nikhef.nl/s/uejGBwNQN will continue to be augmented (and any omissions fixed)

I hope to see many of you in the other Trust and Identity events: at the EGI Confenrence from June 2nd, at TNC25 in Brighton the week thereafter, and of course at the next EUGridPMA/AARC/IGTF/EnCo+ meeting!

The 65th meeting will be
**October 1 - 3** (lunchtime to lunchtime)
(almost certainly) in Karlsruhe, hosted by Marcus Hardt et al and KIT!

Regards,
DavidG.

---

## IGTF Fabric Updates

The IGTF 'PKIX' trust distribution continues to see evolution, with a gradual move in Europe towards consolidation to the TCS service, now in its 5th generation.

The latest, 1.135, distribution was released on May 2nd, finally making he transition to the Gen 4 GPG package singing key:

- the new packge signing GPG key is 2k RSA: https://dl.igtf.net/distribution/current/GPG-KEY-EUGridPMA-RPM-4
- after the initial release it was updates to remove a regression on SHA-1, which could be resolved transparently.
- DigiCertAssuredIDRootCA-Root only root with SHA1 that will not go away. Very few other SHA1 roots left.

### Fabric updates - eKU cleanup initiated by Google Chrome

Interestingly, chrome (Google) will start to impose requirements on extendedKeyUsage and disallow using server, as described in https://googlechrome.github.io/chromerootprogram/#32-promote-use-of-dedicated-tls-server-authentication-pki-hierarchies. Do we see indirect effects of the DCVOTA discussions here? :)

Have have traditionally seen a lot of (ab)use of server certificates for client purposes, e.g. as attribute signers, or as clients in server-to-server communications. Especially for DCV that has always been an issue (since they are usable for encryption of comms to known andpoints, but are not authentication, and hence should not have been used as such). This has been one of the (two, alongside RPDNC) thinkgs that blocked DCV CAs like LE to be installed in the same trust store used for authentication in most eInfra/IGTF use cases.
This change, once implemented, would allow e.g. LE to be installed alongside the authN trust anchors starting ~ 2027 or so.

At the same time, this will make it impossible for joint-trust server certs to be used for the traditional third-party file transfers based on gssapi-ftp protocol based services that rely on PKIX and server-to-server authentication with server certificates (like GridFTP).
All public joint-trust IGTF CAs will follow. This does not necessarily hold for IGTF-only issuers, but their utility will be limited since both sides need to cooperate. For delegated scenarios (rather than server-based) mutual authentication this issue does not arise. Neither does it affect third-party file transfers that rely on other authentication mechanisms like tokens, nonces, macaroons, &c.
Just to keep in mind: signers for JWTs and other token should have their trust anchor come from OIDF chains, SAML meta-data should have self-signed keys, almost all other purposes: use an automated client ('Robot') certificate: they are purpose made for this use case, especially the 'client robot - email/organisation' profile thereof. E.g. in TCS Gen5: "GÉANT Organization Automated Authentication".

So even though LE will likely never be accredited, by early 2027 it may become safe to install alongside authentication providers.
Meanwhile Google Trust Services (GTS) is already scheduled to adhere to this much earlier as part of the DCVOTA accreditation in TAGPMA. Did the DCVOTA requirements spill over into the Chrome root programme? At least they are very, very much aligned!

## GEANT TCS Gen 5 updates

All authentication and joint-trust services in TCS Gen5 are now available, and working perfectly fine with instant satisfaction:

- TCS5 portal: authentication user certs now also available, only self enrolment++++++++++++++++ ++++++++++++++++++++ sponsor-validated IV+OV S/MIME needs to be done.
- ACME EAB planned for mid-June, alongside S/MIME auto-validation
- for the validation, email or the DNS challenges are required (and from different vantage points on the internet). Intercepting mails on the NREN level to support your institutions is too creative…

### EnCo updates

EnCo, part of GN5-2, has a dedicated Policy and Technology subtask, part of this joint meeting. In this meeting (with at least part of the members present during this session):

- contribute to improve AAI interoperability
- collaborate with AARC TREE
- support AEGIS

## Updates from subsubtasks

- TIIME and FIM4R at Reading: FIM4R is used by EnCo to encourage wider participation and integration of research communities in FIM. Still a vibrant community with lots of attendees (?50 attendees), but the challenge is to get research community members (rather than the AAI techies) to turn up. So it's less about research requirements.
- Hannah took us through the Fim4R v2 paper requirements for review, and did a live poll to see if the requirement had either been met and whether it was still relevant. The results should be collected and put on-line (it is now in a live poll). There was recognition that things were either too difficult (and thus stalled and now no longer important), or they had been done.

  The next FIM4R needs to be set (since TechEx may be devoid of most Europeans). NorduNET technical workshop in September in Copenhagen (September 9-11). Will also have a TCS procurement session. Could be nice for FIM4R as well.

  At least in Feb 9-13 2026 in Amsterdam!
- WISE Community has not met for quite some time, although the interest remains definitely there. As an independent forum, it is a good thing to have, to take things forward. COVID made it harder to build consensus on policy (since it was all remote).

  From AEGIS policy:
- Trust Framework (also AARC TREE D2.1): https://wiki.geant.org/display/AARC/AARC-I082+Trust+framework+for+proxies+and+Snctfi+research+services - this is a work in progress, to be finalised this month and will then be shared with AEGIS. This is the framework that structures the Policy Development Kit version 2
- Security Operational Baseline (you will recognise the document): https://aarc-community.org/guidelines/aarc-g084/ and https://wiki.geant.org/display/AARC/AARC-G084+Security+Operational+Baseline
  This has been used to re-align input from multiple infrastructures and proxies (UK-IRIS, EOSC, and the Site Operations from DPKv1)

  Comments on G084 also more than welcome!
- the 180 days at times seen an an issue
- the EU has one year as a minimum
- NIS2 makes (at least in NL) universities at least important entities

- how could you do Sirtfi if you cannot keep logs for even 180 days?
- The EU “one year” is probably the best outside guideance we have today, which is anyway > 180 days.

  The document was reviewed and some editorial changes made, and endorsed.
- Wallets for education get lots more attention - Adrian Fellman tracking that in EnCo (and Norway, obviously :)
- For TNC25, also ensure you signed up for the side meetings (and 101 if you have not been there before)

  AARC Architecture:
- token lifetime document (MarcusH)
- GUT profile work has stalled a bit due to lack of actual people ~~working~~ organising (note taking, agenda setting, chairing), but there is a lot of demand for it. Please contribute!

## WLCG Trust mechanisms

Which authentication providers should/can WLCG trust? One of the things could be how to extent trust mode easily to clouds.
Google Trust Services is in the process of actually joining (for GCP as a use case) with a joint-trust CA, but are there more/other opportunities, as discussed for example in the HSF discussion on getting AI training data. He was using commercial tools that were not easily able to use CERN’s data stores since CERN did not use joint-trust CAs for their servers.

Now this is of course not “IGTF is going away” even with tokens, but more other options are coming along for server authentication, as discussed above on getting rid of TLSClientAuth eKU in publicly-trusted server certs. Can we clearly define what is actually needed?
The group set up by DavidC was set up to address this broader question. Including review of under which authority (LHC) experiments were using commercial cloud services in the first place (beyond just certificates). And any service where you don’t have to pay for, you know who the product is.

MS: it may be good to separate the various aspects of risk (authentication, digital sovereignty, costs, authority), and have one policy document to which you can refer.
Do we have a document to refer to (e.g. like we have acceptable authentication assurance.).
WLG tends to see itself as an island that does not need to care about the world. This is so for some sites, but there are risks from leaking WLCG to others. But separation is not what we want (or WLCG will lose resources that are joint). But some in WLCG do not seem to care, and have to be put straight periodically. Not only WLCG has this issue, though …

Reopen the question which CAs are trusted? So review Acceptable Authentication Assurance.
This discussion (generally) also comes up with LIGO and OSG in general, due to the different model in the US. See also (one of the 2) discussions in https://bugzilla.nordugrid.org/show_bug.cgi?id=4236

If you wait till 2027, part of the problem goes away.

For now, reinvigorate the WG to give the current reasons? At least the WG should focus on one thing at the time, rather than trying to boil several oceans. The WLCG Token Trust and Tracability WG may have an overlapping mandate.
**Actionable**: So have a document: what are the risks, and what can we do to mitigate the risks. Also for sites supporting more than just WLCG.

CERN at least could do joint-trust TCS, but there are some reasons (Hannah knows?) why this is not yet done throughout.

On the authentication side: we see a pickup of client auth to home IdPs, both with certs today, and -

who knows - later with PassKeys.

On the token issuer side: why trust all these token issuers. Now the EOSC nodes will be bound to G071 (which is the guideline applicable to token issuers) through the EOSC AAI federation requirements. So parts of CERN, even if now WLCG, will get this anyway as a Infrastructure Proxy.

Place to start is with a risk assessment!

And how many sites in the EU/EEA that are part of WLCG will be subjected to NIS2? In NL: the universities are, but not (yet) the Institutes.

## Trust Framework for proxies and Snctfi research services

The Trust framework identifies the smallest set of distinct guidelines (policies, good practices, procedures) necessary to cover trust, security, and operational interaction of proxies in composite-proxy scenarios beyond the community-and-infrastructure proxy doublet of AARC-G045. Some elements may already be in place, such as the attribute authority operations security guidance AARC-G071, others have only been identified as needed but have not yet been described in sufficient detail to formulate policy of good practice. The aim of this paper is to identify the smallest set of distinct guidelines, practices, and procedures needed.

In the session, we reviewed the timeline of AARC-I082, and clarified the structure of the policy development kit v2, reclassifying the CoCo part (users) to be part of the collaboration (blue) protection layer.

Authors for subsections have been assigned, and terminology section moved. To complete https://docs.google.com/document/d/1ApYHYVOpfuPnVmahSiJ_CgZsjgkGCuTE/edit ASAP

## Token-based operations

Besides the migrations to tokens that are happening in WLCG, there is a broader movements for other, more diverse VOs, where a single GUT profile is necessary but the development thereof may be too late. But interim solutions for WLCG token evolution should not be incompatible with a future GUT profile. The same set of people should probably work on both token lifetime documents.

In WLCG they see themselves as different and a closed community, so a hidden group of people discussing it ‘is not a problem’. Apparently. Apart from the fact of course that WLCG is not a closed commuity as long as it wants to use resources that are generic e-Infrastructure services. It is even so that not all the experts on *both* sides of the Atlantic are aware or get the information. So the WLCG Authorisation Working Group is left outside this ‘inner’ circle (probably MaartenL is in?).
The ‘finegrained’ capabilities are unlikely to be then used in the end, taking the experience from VOMS as a reference (too finegrained does not make sense). And it does not scale if you have too-fine-grained tokens - this is confirmed by service software developers (like for dCache) and operators like CILogon. Too many tokens should not be used, they all agree.
David Crooks asserts that he is going to lead a security risk assessment, as reconfirmed at the HSF workshop in May 2025. Luna is involved as well.

In ATLAS the idea is that the FTS will get the file-level granularity, but that does not necessarily extend to the storage services which will have a namespace based tokens (posix path structure based). (for write)
The write tokens in ATLAS will be able to write to ALL sites within that path, so the challenge seen there is to prevent a compromised token to be used to write (not delete/update) on other sites, if one (compute) site is compromised. This would normally be addressed with token exchange (with a token issuing having that knowledge that should have been in the PAP of the workload management system, or through call-outs). And it gives you a control point for incident response.
The Atlas workflow management system knows everything, and will feed that to the job (and hence can push appropriate tokens). For reading in ATLAS there is just a single level: read all.

The broadly scoped ‘write this path but across all sites’ works because there is a cleanup consistency mechanism so ATLAS on the consistency check will identify files written that should not have been there.
But this is all a bespoke thing just for ATLAS, not to be used by generic workflow management services (and the implementation is not there yet, should be in 6 months). And the discussion in the closed group, not with the global experts (like in the TokenTrustTracability WG).

For Auger, there is a migration planned, but the target fo the migration (to EGI CheckIn for instance) has a couple of requirements:

- should support a transitionary period from VOMS to tokens
- work with the EGI DIRAC system for workflow mngt
- should work with storage systems that use tokens (and FTS in the future)
- should work with PERUN as the collaboration management system
  and there is a choice both for the provider as well as the token profile to be used.
  For Auger a relatively wide scope for writing would be preferable. And the filesystem scopes based on groups is perfectly fine. EGI/AARC token profile should be good (and the GUT of course).

  More specific discussion on introspection (e.g. for having specific privileged client credentials for security teams to get actual user info for a token (as opposed to pseudonymous sub claim)), refresh flows, and exchange flows ensued. IndigoIAM does not yet support all features, but does support introspection.

  G081 Token Lifetime late draft document: https://docs.google.com/document/d/1U9vvJfWuE8oO7u0FcGVGr3KySvBqwjnkzKO8TKzgoX4
- the EGI CheckIn provision of legacy VOMS may no longer be supported after VOMS left
- for access to data, Auger is using the VOMS servers by Auger itself
- EGI DIRAC can take CheckIn tokens
  https://docs.egi.eu/users/compute/orchestration/workload-manager/
  https://indico.cern.ch/event/1225113/contributions/5417484/attachments/2670491/4629195/Using EGI Check-in tokens - EGIConf23.pdf
  *** check back with Nicolas, and compare with KM3NeT
- the ARC CE token support may be limited to just one token profile - there is probably support for the SciTokens, but EGI has been written as well. There is a common mapping plugin, and there is EGI documentation for it. Generally ARC-CE (and esp. ARC-CE v7) is very flexible in this regard (issuer, subject, groups with regex support). Then it maps to internal identifiers, then local accounts or EGI accounting identifiers.

## APGridPMA and federated developments in the AP region

The status of the APGridPMA itself remains unchanged, with Eisaku Sakane as Chair and Sai Prasad (eMudhra) as the vice chair. Over the years, 11 CAs have retired, with the ASGCCA picking up most of the regional catch-all functions. HPCI was the most recent retraction.

- APGridPMA accepted the Elm assurance profile and the DCVOTA profile at its last meeting. This means they are now globally accepted (EUGridPMA did it in January 2025).
- There is an APAN IAM working group, for the support of buildup of SAML2 and other federation services in the region joining with eduGAIN and based on the REFEDS profiles.

  Next meetings:
- 35th APGridPMA in HK colocated wih APAN60 (July 28-1 Aug)
- 36th in Taipei with ISGC2026

## GakuNin and Orthros

Key Components in New GakuNin Trust Framework

GakuNin IAL/AAL
• Stipulation Of IAL and AAL: By having IdP and SP refer to it, unified and efficient discussions can be made possible, and by each institution complying with it, the trust of GakuNin as a Whole can be guaranteed. https://meatwiki.nii.ac.iD/confluence/x/JOSfBO

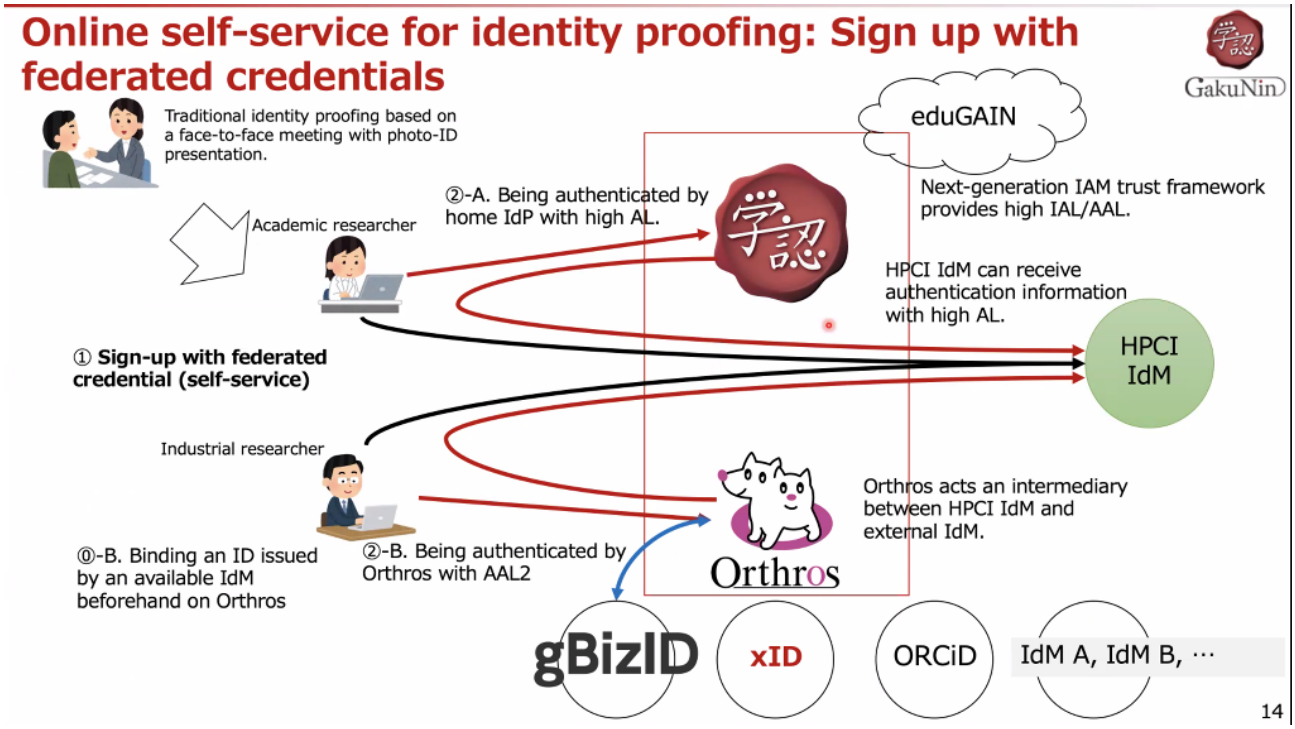
Authenticator Registry
• Evaluation Of authenticators based on GakuNin AAL: Evaluating authenticators, publishing the results, and encouraging universities and research institutes to promote multi-factor authentication at their IdPs. https://leve12.gakunin.jp/

Authentication Proxy Service “Orthros”
• AL matching, credential bridging, fundamental attribute coordination: By mediating requests from SP and linking with Idp, it is possible to guarantee IAL and AAI-.

IdP Hosting Service
• Addressing issues Of IdP building and operation: Reduce the burden on universities and research institutions in building and operating IdPs, and allow all institutions to operate IdPs by choosing from a variety of operating formats that suit their institution.

Advanced Group Management
• Support for high and complex authorization control: In addition to basic attributes, group management can be based on attributes that general IdPs do not handle, making SP authorization management more efficient.

Additional details on Orthros are contained in the presentation:




The MyNumber Card also carries the username via the xID service, but does not contain the link to the organisation that the user is coming from. So a proof of enrolment is needed, preferably using an on-line procedure that is the equivalent of the offline combination of photoID and proof of enrolment.

How would the online/offline procedure work? It may rely on either the home IdP association, or potentially a verifable credential issued by the same.

### Future Plans for GakuNin and Orthros

- GakuNin:
- We will make a report about the result of the medium-scale demonstration experiment FY2024.
- HPCI
- We will consider an online procedure with composite identity documents.
- We will design a new IdM and IdP architecture for HPCI.

## The Wallet Ecosystem and eID assurance

The ambition it ro review suitability of eID (and Wallets) for *research* use cases. The reason being that home organisations consistently failed to provide such details, so maybe govt eID would work better?

Niels van Dijk and Martin Kuba will share some ‘interesting’ background - which may conclude that, considering usability as well, eID is not currently in a state where it can be used.

Where should we be deploying wallets?
The EU realised eIDAS v1 was something of a failure in adoption, and eIDAS version 2 was introduced based on a ‘wallet’ for citizens, to be provided by the member states by 2026, including basic information including an identifier, given and surnames, and some other forms of credentials. The ‘other’ things could be drivers licenses, id cards, but also educational diplomas. And it should be usable in other sectors, not only citizen to government. And some large service providers (outside of govt) also were set to MUST accept these (like large social platforms).
But the EU needed a couple of things at the same time. One is legislation, since many of the existing laws state specific (physical) representations of documents like drivers licenses and passports. A lot of implementing acts by the Commission have been promulgated since.

“member states should setup and register providers and consumers of identities”, “what are the technical capabilities of the wallets” (with an architectural reference framework ‘ARF’). The result for the latter was OIDFederation, but it was based on memberstate consensus. Which takes a *long* time, going from ~27 protocols down to a few, and then to two protocols.
The reference implementation (the Reference Wallet) was then procured commercially by the Commission, based on the ARF, followed by four Large Scale Pilots to engage with this future ecosystem. Like DC4EU for the educational space & EHIC cards. Payment, banking, travel were others.

But the reference implementation was late (+1yr) and this has cascading impact on all the pilots, so they mostly did their own thing to at least get the pilots to work. And now there are all different (and whether they have fulfilled the requirements of the contract with the LS pilots and the EC).

But there are now a couple of OpenID specs in implementers drafts for many of the cases, but these are still all moving targets. Before the end of summer 2025 there *should* be a stable standard, but now with the pressure for legislative implementation being so high, so now governments are changing the standards to reduce national implementation, which has severely impacted the cross-national use cases, esp. for education.
Added to that the mandatory registration of all the entities involved, and the lack of a pan-European registation scheme from day 1, so now you have register in each and every country, based on each state’s national law. Which are All Different in terms of the regitration requirements and process. It will have 5+ years to even think about resolving it. So in the short term is does not scale at all due to this, due to having 27+ different requirements and profiles.

With that, it makes it impossible to use eIDs from wallets in the research and AARC BPA ecosystem.
The registration would have to be per country, but the legal issues to get access to relevant information will take ages.
There is also no agreement on what the PID will *actually* contain for each country, and whether

there is enough information to make identity verification possible. Only 3 of the 16 are mandatory: givenName, surname, and date of birth. And those are insufficient to get uniqueness, so it's useless for an identifier. And they can change over time.
The national identifier is not part of the set, and in some countries (like NL, where it's the BSN) will not be allowed to be processed.

So, what *can* we use, based on the ARF, in the AARC BPA context?

- Key use cases: Identity, Improve LOA, Credential Transportation, and Credential Aggregation
- Potential bonus: Transparency (the user is always involved), Discovery, GDPR, and reduce or eliminate SPOFs (since the wallets are very distributed, so only during updates you need the authentic source)

Features we *can* get from wallets, not being government eID, are more likely. Including Trusted Wallet (everything is signed always), Trusted Credentials, Expiration & Revocation (which is well organised in the wallet ecosystem), Transparency, Usable credentials, Interoperable Credentials, Discovery, and a scalable Trust Framework and scalable RP registration.

The EUDI is interesting, but of course research is global, and having something that only works in the EU27 is not going to be of much help. Education and research has to cater for much more, also for identity assurance levels. And (many) countries in the world will not have a wallet ecosystem at all.

Now eduGAIN in its current (SAMLish) form is not going to ever be scalable or usable for wallets. The move to OpenID Federation will help, since many of the wallet ecosystems look suspiciously like OIDConnect. But we will have to deal with RP registration ourselves anyway. That is a policy that we (R&E) have to write down. OIDFederation profile for eduGAIN is being worked on the GN5-*. The REFEDS RAF assurance framework will work for the Verifiable Credential for the wallet. From an assurance perspective this is nice, since RAF can thus be re-used without changes!

*"REFEDS Assurance Framework can be re-used for the Wallet VCs"*

Using the EUDI Wallet (certified wallets) has a few advantages, if we would be able to get our credential issuers registered, which is far from guaranteed. But there is more: the usability is limited, focussing on passports and drivers licenses, which is where the low-hanging fruit and requirements are for member state government. So getting new credential types when everyone is busy doing other stuff.
The scalability for e.g. eduID is horrendous, since you have to register in each member state. And you get interoperability issues if member states require changes that are incompatible.

For the trust framework, the EU has chosen a Trust List approach. You already need 6 list just to get the basics working - one for each logical entity. This has all the problems we know from SAML meta-data :( Including multi-day propagation delays.

And still it will not work beyond the EU …

But can we use it as an assurance step-up with minimal data? "Has an EUDI identity". It gives a warm and fuzzy feeling of trust on top of an existing identity for some cases. But is that enough value for the research use cases involved, like those with sensitive data?
Still the challenges for scalability with RP registration, trust framework, and interoprability remain.

Or use wallets for our own purposes, irrespective of the EUDI? For example for aggregation and composition of collaboration attributes, rather then having the proxy re-write everything, but just collating?
But then on the receiving end you may lack the link to the trust framework (in SAML it assumes you have pre-established trust, the wallet ecosystem may have non verified verifiable credentials, piggybacking on the govt. framework??)

The EU promised a pan-European registration scheme at some point in the future, so we could also

just wait.

Meanwhile, SURF has been experimenting with community credentil types (for the UHarderwijk) since the model is very well suited to transport credentials and attributs from various research communities across.

Or do we just dominate the world, by getting rid of all the proxies, replacing the whole access protocol translation blob with a wallet. And if users are used to handling their wallet anyway … maybe as a browser-based wallet [even EUDI does no longer requires the wallet to be on a mobile device, it can now we also elsewhere]. Then they can select the (browser-based) wallet based on the activity they are undertaking.

So what we need for assurance in a trusted ecosystem?

- A trusted Wallet: Wallet (unit) attestation
- Trusted Credentials: Trusted Issuers, Trusted verifiers/RPs, **Use RAF and use SIRTFI**
- Expiration & Revocation
- Transparency
- Usable & Interoperable credentials: build on eduPerson, SCHAC and voPerson
- Discovery
- Challenging is the scalability: Trust Framework (Centralized vs Decentralized), Trust lists (EUDI) vs OID Federation, Leverage EUDI? and National Feds and eduGAIN?
- and will this ultimately change Token Translation?

The scalability beyond government is going to be a challenge. SURF already has 2000 services to be registered. A country the size of NL probably has 100 thousands on entities to be registred. But imagine a second-hand webshop where there are millions of parties that need to engage with the wallet …

**So what will be in M2.2? Re-scope, since we now have new knowledge!**

Revocation has its special properties as well. Because every verifier needs to, upon receiving your driver's license credential, needs to check against the revocation registry if this specific driver's license is still valid. So the driver's license credential itself is still valid because it's just adjacent with a signature. That will still be valid.
But the driver's license, the verifier at that point will have to check is the credential itself still valid By the way, it will probably also have to check if the issuing party is still valid. It might also be for a driver's license that's a little bit unlikely but for an educational credential, it could be that the institution no longer exists or something like that. So that's another check they would have to do.

The revocation repository is operated by the issuing source. And that one needs to be checked.

The UK is taking the same specfications (almost) as the EU wallet stuff, even if the trust is going to be different, there could be interop. The other EEA countries follow the EU, and even CH is trying …

If there is an eduWallet, will a user alway have two wallets, one from the govt and one for education. And it would require duplication of a lot of things, but then having medical records next to the IKEA Family card with different trust levels is a bit strange (or would IKEA need to go through all the government hoops?)
Revocation is also a challenge if you stuff everything in your government wallet, and then the govt revokes your wallet, you would loose everything. And do you trust your government enough? And why? The govt will then hold too much power over you.

For the M2.2 report:

- what are the challenges in a non-existing ecosystem?
- what is the impact of changing implementing acts, like per-country registration
- timing is a most important part, and how fast do the member states converge (so not in November 2026, but may in 2030, 2035?) It took 10+ years for eduGAIN as well!

## government eID schemes (Martin)

*(see also https://indico.nikhef.nl/event/6378/contributions/25615/attachments/)*

eID vs. eduGAIN: same technology, different properties

- eduGAIN as inter-federation of Research & Education federations of students, teachers, researchers, employees of universities, libraries, hospitals, but *levels of assurance are seldom reported*
- eduGAIN does provide eduPersonScopedAffiliation attribute describing type of affiliation, but not citizen identity like date of birth or id card number
- then eID is the inter-federation of national state digital identity schemes, so time extent you get citizens levels of assurance clearly defined and reported provides citizen identity BUT does not provide affiliations to any organizations or researcher status

  And even the identifier is targeted to the country
- a user cannot be correlated to the same user accessing services in other countries
- ‘my identifier is’
- test.swedenconnect.se: CZ/SE/b95bf3b4-132a-4823-85ce-2aa3a3077df2
- eidas.services-publics.lu: CZ/LU/5522cf9a-5cd6-4a95-b536-eOa1b918d4a2
- EU Login: CZ/EU/997c4f07-769d-400a-be74-5fe4e87f579d

  You cannot as a country connect to your own node, because the eIDAS wayf is not allowed to show your own country - there should be a selection page before that ‘use your national ID’ OR ‘use eIDAS’. So Swedes cannot use eIDAS login to MyAccessID. Sigh.

  The conclusion: *current* eID is not usable, not even for assurance stepup, reviewing the slides for the reasons.

  So what about the wallets? In GA4GH a possible VerifiableCredential (VC) might be possible where the VC is part of the semantically connected graph, using an onthology relationship. In genomics they are highly concerned about data access, and access should e.g. be ‘non profit cancer research and a bona-fide researcher’.

  The Selective Disclosure “SD-JWT” is a bit like a X509 certificate: attributes and a key. It has hashes of data, with the disclosues conveyed outside of the SDJWT. So you have a subset of disclosures, but they can all be checked based on the SD-JWT based on the hashes of each disclosure.
  It’s currently an RFC draft.

  Summary
- eID Network is far from full mesh
- eID cannot be accepted by research organizations in some countries
- MyAccessID provides eID connection, but does not provide the original data
- EU Digital Identity Wallet will provide semantic data model with selective disclosure

  So we are not there (yet) for research :(

Other notes:
The 'self sovereign' background is possibly still there, but the other core principles will be squashed by government intervention and control. What is still there is that the verifier will be using OIDC to the wallet, so the government SHOULD not restrict it, but of course they do it anyway because of the registation in the ecosystem as RPs. So that kills off the interoperability and standard compliance. And in NL they even restrict which claims an RP is allowed to receive. So that is definitely NOT self-sovereign. So there is intervention and blockage all over the place, including the registration process by itself.
**So then we will need a second wallet which is not under EU/EU-MS control. R&E will thus need a parallel ecosystem: eduID/eduWallet is thus needed.**

Actual use of government eID in MyAccessID is extremely low, less than 1%, since you almost only use it for taxes and so (or you COVID certificate), and maybe that is going to change with the wallet ecosystem if it is actually used beyond government/healthcare services.

The lack of the identifier may even be deliberate to not have tracking. Today the implementing act restricts it to name + DoB, which is not unique.

So what happened to the digital passports that were 'imminent' as claimed by the EU (the project lead of the ARF for wallets) at the TIIME Copenhagen meeting in spring 2024. So what happened? Oh well …

What may work in NL for edu wallets: there is a national enrolment service for students (studieLink), which *is* allowed to process national ID numbers. Now as they enrol there, we can mint an eduID for every student in the Netherlands, and then create a delegated credential of the social security number (e.g. a SHA hash thereof) from which you can recover the identity wallet if you loose the (mobile) device with all your diplomas &c in your wallet. You need that stable identifier for account recovery. Also in 10 years.

Besides using a mobile device wallet, there is also work on a WWWallet, with an encrypted blob on a device to which access is controlled by means of passkey or other strong authenticator. The WWWallet can just implement all the required protocols, but it is using the browser APIs to interact with the encyrpted blob. And that blob you can replicate and put in a secure place - since it's encrypted anyway, and you can use the passkey to get in. SURF is investigating this model, allowing use in the far future, also employing file syncing.
You can have multiple authenticators to the same encrypted blob, so that gives you some resilience against loss of device.

For some government cases, they want even split key material and store part of a govt HSM, which is then controlled by the government. It has to on-line and a govt that is coorperative with the user.

So: the ecosystem is far for complete. Today, and in 2026!

## Trust and Identity in GEANT 5+

*Casper's slides are at* https://indico.nikhef.nl/event/6378/contributions/24890/attachments/

The GEANT5-2 project has a continuous Enabling Communities task that supports work in a wide array of forums that enable communities to work together on trust and identity ("WP5", and within it task 6), in a new or preferably disruptive way.

Roadmaps for the 4 services: https://wiki.geant.org/display/G52W5/Trust+and+Identity+Services+Roadmaps

- the Monday at TNC25 has the Mobility Day, also part of T&I eduroam™
- The T&I incubator has been broadened to also allow for new improvements on existing services (stll in sprints).
- Call for ideas for the Incubator can be submitted to https://edu.nl/78te4

- And there is the Mentorship programme 'Tim', to give students the opportunity to work on one of the Incubator sprints as part of their study or thesis. That is also a good way to promote NRENs in the labour market (Pro-M and Cynet got good staff out of this programme): https://community.geant.org/trust-and-identity-mentorship/

  Enabling Communities has three subtasks: Outreach, Wallets, and Policy & Technology. And now T&I has a dedicated comms specialist from Sikt!

  EnCo also supports the TIIME unconference, next year in February 2026 at Nikhef (Science Park) in Amsterdam, NL, jointly with the AARC Symposium, FIM4R and an eduID day. https://tiime-unconference.eu/ and https://indico.nikhef.nl/e/ewti2026

  **A cross-cutting activity on Wallets, OIDC and OIDF**

  A task force across projects and activities to bring this together, with input from eduGAIN, Incubator, AARC TREE, EnCo Wallets, Policy and T&I Comms.

  There are so many known unknowns (as shown by Niels in his presentation) on the EUDI and the relation with R&E, so that R&E can and should probably set its own agenda. We need it on time and with the right scope.

- We need to influence direction within our scope
- REFEDS information exchange should in included
- regular calls to ensure coordination between the different groups: infoshares and periodic meetings
- is this purely European thing? Most of the wallet work seems to be in Europe, but there are some national activities globally. The wiki (https://wiki.geant.org/display/G52W5/Subtask+-+Wallets) has an extensive list. But it's hard to get information on who in the NRENs is working on this. 'Not only Europe is struggling'.
- What would be the impact of waiting too long? Do we then just get Apple and Google to dominate this space? Europe lacks the central authority for setting the interop profile.

  So we need awareness-building, as we are not in the coordination/alignment phase yet.
  And we should not just wait for 2.5 years so by the end of GN52 we are still waiting on government legislation.

  So we will proceed with
- instate periodic update/sync meetings
- inform the Comms specialist to share that we are working on this and that the NRENs SHOULD join and share their state as well
- define what is actionable (and than act)

  For the global tech interop, that will probably be IETF through RFCs. As for the policy and profiling elements … would that not end up at the ICAO, since it would be a reflection of physical passports that they already standardise.

## OpenID Federation Policy Expression

OID Federation are here to stay: they provide a lot of benefits can have a more flexible, scalable trust apologies, more transparent trust by having Everything expressed the same metadata, metadata policies
And it's a trust infrastructure that also supports the wallets, and there are already a lot of activities around it, ongoing efforts in, for example, the eduGAIN pilot.

- Benefits : Build flexible and scalable trust topologies, more transparent trust, unique trust

infrastructure that can support SAML, OIDC and Wallets

- Ongoing efforts
- eduGAIN pilot: https://github.com/GEANT/edugain-openidfed
- REFEDS Profile for R&E WG: https://docs.google.com/document/d/1zUB6Yk4NCC98cUVIBlSNUiDEnrdKBA_OCw46LLCldN4
- OID-Fed architecture for digital wallets: https://openid.net/specs/openid-federation-wallet-1_0.html
- Interop event: https://openid.net/the-openid-federation-interoperability-event
- Gaps: Discovery , Onboarding of entities
- Tooling : Specification and profiling for R&E

A helpful point for policy expression are the Trust Marks, signed JWTs that codify properties by a Trust Issuer.

Policy Expression

- Policies as Trust Marks: Signal conformance to sets of criteria determined by an accreditation authority,and Filtering during discovery or as requirement for onboarding
- Trust Mark Owner vs Trust Mark Issuer: Enables delegation of issuance, Owners do not need to be part of the federation, while Issuers do, the Issuers need to be acknowledged at the Trust Anchor, and Self-issued Trust Marks also supported
- Policies as profiles: Signaling behaviour as part of transactions, and reflect the Claims and scopes in OIDC & OAuth2

**Challenges**

- OID-Fed introduces new entities (TAs, IAS)
- The role of proxies

Can one express the issuer of the trust marks using an organisation ID in the trust mark?

- Yes, in the meta-data there is an organisation name extension (defined in section 5.2.2 of the OIDF spec) that could be used for this.

Can there be multiple signers to a trust mark?

- Peer reviewed self assessment would show up as a list of independent but related trust marks with the same identifier.

Would these trust marks and expression be rolled out in an eduGAIN OIDF rendering relatively soon?

- Not yet clear, but the roadmap is being defined by the eduGAIN steering group. Since eduGAIN is global, it needs global engagement as well, but it may help to put OIDF for eduGAIN higher on the steering group agenda.
  Davide Vaghetti should know, and he is anyway aware of AARC/OIDF work.
- At least don't profile the trust mark and expression options away in the MVP … they are useful for auth federations (like EOSC) to keep some of the elements on trust. This can be raised again at the eduGAIN Town Hall in TNC25 will also have this discussion.
- In the eduGAIN Pilot: IDEM/GARR, SURF (with either SRAM or Conext), and approx. three others. Probably SUNET is in. Others are keen, like FEIDE/Sikt, but they are not yet in (but are ready to join any time), and a mix of H&S and full mesh, and small and large federations, is good to have in the pilot. Davide will know who is engaged in the proces now.

What use cases are enabled by OIDF? And what does that mean for the AARC PDK?

- OID Federation makes it easier to join federations and have the federation be more dynamic. For example the SRAM case in the Netherlands the “Research Cloud” platform is a resaercher-built workflow system, and adding the tools that are spun up in there should be connected to the federation, and OIDF will enable that use case. This is the ephemeral services use case that is a strong OIDF driver.

## Logistics

Present: Daniel Kouril, Jan Chvojka, Peter Bolha, DavidG, Dave Kelsey, Casper Dreef, Liam Atherton, Adrian Fellman, Petr Vokac, Arnout Terpstra, Maarten Kremers, Martin Kuba
Remote: Miroslav Dobrucky, Mischa Sallé, Nicolas Liampotis, Diana Gudu, Niels van Dijk, Marcus Hardt, Eisaku Sakane, Matt Viljoen

The next 65th meeting will be
**October 1 - 3** (lunchtime to lunchtime)
Location is tentatively Karlsruhe South Campus