The Karlsruhe 65th EUGridPMA and AARC Policy Meeting Summary

The 65th EUGridPMA+, AARC Policy and EnCo meeting is now over, and I would like to take this opportunity to thank again Marcus Hardt and KIT for hosting us in Karlsruhe, and the participants for contributing to these notes.

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/PiSoDnx2RHSW--qrnWS58g (https://sharemd.nikhef.nl/PiSoDnx2RHSW--qrnWS58g) 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 Internet2 Technology Exchange for FIM4R (on Sunday) and ACAMP (Thursday & Friday), TIIME2026 and the AARC Symposium on Feb 9-13, 2026 in Amsterdam, and ISGC2026 in Taipei.

The 66th meeting will be co-located with TIIME in Amsterdam on the Friday morning the 13th. The 67th meeting will be May 11-13, in a location to be determined.

Regards,
DavidG.

- The Karlsruhe 65th EUGridPMA and AARC Policy Meeting Summary
    - IGTF fabric updates: status of authorities and trust fabric news
        - Authority Update I: IR-GRID CA
        - TCS Gen5 and RCauth.eu updates
    - Developments in the Asia Pacific and the APGridPMA
        - HPCI updates and GakuNin
        - Work in Progress - GakuNin
    - Updates from GEANT and EnCo
    - The policy registration API in AARC - G083
    - Applying policy and sharing templates - a real-world experience
    - TAGPMA Update, ELM, and DCV server certificates
    - TIIME Bus & Nar Conversation
    - Tokens and token lifetime
    - AARC=G100: establishing trust between proxies using OpenID Federation
    - AARC-G052 OAuth2 proxy token introspection
    - AARC-G056 Expressing identity attributes
    - Government eID for identity assurance (and wallets)
        - Relation to the new BPA
        - VCs and Wallets (by Stefan)
    - AARC G084 Security Baseline
    - Identity Federation and eduGAIN in Taiwan
    - AARC Policy Development Kit: prioritisation and open tasks
    - FIM4R evolution and planning
    - OpenID federation - updates by Davide Vaghetti
    - And now for something completely related: GenAI risks and its handling (Liam)

IGTF fabric updates: status of authorities and trust fabric news

- Cosmin Nistor needs to be pinged for nagging people some more (e.g. regarding self assessment of CAs)
- IPv6 CRLs: make a list of issuers that still only have v4 endpoints (even though a fallback exists at the IGTF)

Authority Update I: IR-GRID CA

This presentation did not happen - deferred

TCS Gen5 and RCauth.eu (http://RCauth.eu) updates

This year is 10 year of RCauth! See presentation for details on use, naming, anycast capabilities, and re-use.

- The request to extend to 20y validity is accepted.
- Have MyToken in anycasted mode at some point in the (near) future - Marcus moving ahead slowly – since two years.
- it still makes sense to have other stateful services HA without the need for local 24/7 support (maybe mitigate overly long-lived tokens?)

Developments in the Asia Pacific and the APGridPMA

The APGridPMA coordination is stable, with Eisaku Sakne (NII, chair) and Sai Prasad (eMudhra, vice-chair). The Spring meeting will continue to be co-hosted with ISGC in Taipei, the Autumn meeting with eScience or APAN routine events. (athough there was no IAM workshop at APAN60, there was an APGridPMA meeting, and Eisaku was re-elected as chair for the 2026-2027 period)
ASGCCA is acting as the catch-all for the whole region.
To communicate, APGridPMA is now (also) using Slack, on the apgridpma.slack.com (http://apgridpma.slack.com) web site for intra-membership communications. But since Slack is blocked in .cn, IHEP will not be able to communicate. They are setting up a new CA anyway - they will have to use email (with advice from other APGridPMA members)

HPCI updates and GakuNin

Work in Progress in HPCI comprises: Provisioning a computing environment for end-user, Providing the token-based client software packages, developing container images as well as the GSI middleware.
For Authenticator AL enhancement, Passkeys are being introduced as authenticator to HPCI OpenID provider (with Keycloak), with tuning of authenticator initialization procedures: not too loose, not too strict...
The Shibboleth metadata registration practice was tightened by: shortening X.509 server certificates validity period from CA/B forum; certificates in HPCI federation metadata will be affected because currently, the certificates included in the metadata must be public ones (Publicity of the server certificate ensures its OV). The following issue must also be addressed: how to register metadata including server certificate, in other words, and how we identify and authenticate IdP or SP.

Work in Progress - GakuNin

Medium-scale demonstration experiment starts in FY 2025 (starting October)The detail will be shown in the next meeting O

No updates on Orthros yet - it was introduced in the previous meeting for public services by the JP government, but currently there are no updates on on-line identity proofing.

Updates from GEANT and EnCo

How can we use usefully the time in GN5-2 EnCo after AARC-TREE has concluded, and ensure how to provide continuity for AARC material.

- Compendium
- PDK evolution
- Notice Management registry

This was linked to AEGIS to ensure take-up, but it is a fully closed system that limits participation. But besides that AARC activity did continue without direct funding support, although at a slower pace.

The work is not done - with EnCo funding it raises the priority of things to do, ensuring a heartbeat and FIM4R meetings.
The message from EnCo is that this work is important, and it has ensured continutiy between AARC-2 and AARC-TREE.
For GN5-3 EnCo:

- support of FIM4R
- evolution of the Compendium, since that is not to be static
- simplifying and consultancy for implementation of the BPA
- clarification of Guidelines - which is similar to the role of the WG lists in the IETF (like LAMPS and PKIX are still around and useful)
-

There are two audiences:

- implementators of (proxy) services (NFDI, HIFIS, SRAM, CERN)
- communities that come and use the infra

"Even the 10-commandment AUP is too complex for some users" - do NFDI provides clarification. The audience for AARC guidelines are the impleentors. But how does then the Compendium fit into this, if it is not sufficient? It also helps implementors in communication to their users. CheckIn, NFDI, SRAM are all the same for the users.
But still it can be overwhelming for a user. Also for small-community implementors by the way. E.g. how to get documentation back to the central knowledge base.

Share documentation on also have users come out of ani-patterns (like the CS3 'solution' used by the ET EMR geosurvey, or Google docs). It ah to be Really Simple in ordr to be usable for users. The infra's need to take care of the users, and AARC TREE should be enabling that kin dof expertise o be shared (the Compendium, for instance, also pointing to solutions providers).

The mid-sized communities (O(100) people) are almost by definition already international, but also national researchers should be convinced that this does not conflict with national directions in T&I (like NFDI is just the evolution also for the direction DFN is going, for instance)

The HIFIS and NDFI infrastructures are communicating that there is infra and that users should start coming and defining 'communities' - but getting them to come and even ask for help and documenation took a long, long time (years).

Accounting is also still an open questions - we did not yet adress it in AARC< but there is an NFDI-Base proposal to start working on this. EOSC will need this, but for the moment it is primarily local (even to the extent of using unix uids). But the data on usage is needed both for CAPM and for pricing and budgetting.

For the time it is indeed local, but you could share identifiers though `eduPersonAnalyticsTag` ?

The AARC TREE WP1 task on 'Federated Authorization' was assigned to SURF (Pieter vdM), but the status is unclear ... for the next few minutes. AARC-G056 has all the attributes inside, but the scope it too broad with too many attibutes. It is coming (has been for the past few years), and it will have entitlements, for WLCG even groups, and authorisation based on assurance, affiliation, and entitlements. For entitlements, these are URNs they are vey long octetStrings and they fill the token size. The GUT is supposed to address this (also with scoped groups?). Mischa and Marcus are aiming to sort out the repetitive information ('urn:geant:dfn.de:ndfi:...', and the base is always the same). The substructuring of information makes it hard for regex matching in e.g. OpenStuk.

For NECTAR, it is still true that any users gets 2 VMs for free, and there is accounting for additional VMs. Getting information thereon is currently ongoing.

For identifying which role is being used for accounting, there can be multiple roles that grant you access to do certain things, but there should be only on 'accounting' role. Would double-counting work for resource accounting (even if it is decidedly forbidden for time registation in EC projects :)

"Accounting and Authorisation are relatives, but they don't live in the same house."

Accounting also has two sides: both the summarizing as well as a PAP whose information can be used by the PDP.

The policy registration API in AARC - G083

The goal of G083 is to reduce the number of click through screens with AUPs and notices on their way to the services - even when they change or are updated.
The communities will host the NPC and the policies will be in the Registry. The registry API was defined in the ArchWG of AARC:

Endpoints according to documentation

- /getpolicies - Json, uri, name and information url
- /addPolicy - uri, name, json doc
- /getApiKey
- /registerService

Modified endpoints

- Landing page (Health check)
- /getpolicy
  Omitted for now
- /getApiKey
- Bearer token instead
  In progress
- /addPolicy - Just a static endpoint with no connection to db

There is now a database back-end, where id and uri are separated (needs carification in the doc).

Open questions:

- ID is provided externally, as it may ome from a different repository
- aut may not be universally availble, but when avaailbale should be persistent. The name is more general
- contacts are an enum

The aggregation should be as high up the chain as possible, to cover asmany services as possible. It however cannot be at the identity layer, because at that point the WISE Baseline AUP purpose binding is not yet vailable. I you push it down at the infra or SP layer then it cannot be spread over more than a few SPs. Hence the link of the NPC to the Community.

Push down VOPersonPolicyAgeement (versioned on id).

Other questions:

- Where is the user information stored? - at the NCP/Community
- How and who knows what information to query for (AU P's)
- Should one query the registry for SP's rather than a specific aup?
- Owner of policy - Who should that be, what information should be stored? – use user identifier or group (like associate with G069-style groups)

** for URL-based names it is relatively easy, since you can check a .well-known (once!) on registering under a URL namespace (so https://wise-community.org/wise-baseline-aup/v1/ (https://wise-community.org/wise-baseline-aup/v1/) is checked with a secret under https://wise-community.org/wise-baseline-aup/v1/.well-known/nr-registry (https://wise-community.org/wise-baseline-aup/v1/.well-known/nr-registry) or so)
** for URNs it is more complex: expert review, or infer from DublinCore for urn:doi: DOIs, or IANA Private MID for urn:oid:

- How to determine if one may add a policy? - open on proven ownership. No addtitional controls at least fo the pilot. As control, ad eduGAIN login and a token/APIkey only to authenticated users.

- Who can register a service and how to validate? - ibidem

On demise of the owner, needs database fix, probably through admin API calls.

Applying policy and sharing templates - a real-world experience

InterTwin recently finished after a 3-year period as an EGI-led EC project. For SRCnet, since August this year (2025) are in a v0.1 state where som mock data can be moved between sites in SRCnet.

InterTwin was a smallish development project, including HPC centres that were not specifically set up for federated AAI and federated access. The environment of Cloud and HPC being mixed added policy needs. Starting of simple with 6 questions in a survey to review alignment with basic capabilities and the EOSC Baseline. The cloud providers were mostly aligned, but the HPC centres were further away policy-wise. The EOSC Security Baseline was not picked up by either.

Questionnaire with six policy-related questions to all Intertwin cloud and HPC centres

Changes to the PDK contained:

- TLP: Remove references to central instances that dont necessarily exist evereywhere (EGI CSIRTS...)
- AUP: Needed additions for HPC centres
- Service Operations: Pulled in clauses for HPC centres

HPC Still does passports and ssh-keys

- Very hard to move HPC to federated identities

Overall result:

- Questionable how useful is it to create policies for a 3year project. It's just not enough time to influence any centres policy.

SRCNet (data transfer, storage and processing for SKA) Context

- Much bigger project (9 Nodes (countries))
- Current status: initial services running
  AuthN
- Existing users onboarded through creating accounts with ska email and username
- Few enough users that participation in meetings is enough
- Plan to use 34 party software to check passports and then create accounts
  AuthZ
- User accounts created and maintained by SKAO

- (username/password)
  Templates used
- IRIS
- Infrastructure Policy
- AUP
- Service Providers
- Incident Response
- Nothing covering processing of personal data, no data protection
- There will only be science data in 0.1
- IAM has a privacy policy

What we did and how it worked

- Copy IRIS policies
- Adjust for global rather than UK federation
- Agree approvals process and risk ownership within SKA (actually: SRCnet)
  - Least senior person capable of owning the risk
  - Approval by representative from each individual node
- Complexity by the difference in nodes
  - Some are 3 people and have no lawyers/people with policy experience/don't have a signing process
  - Some are STFC and SURF (at the time) plus other orgs in their country
  - Technical documents so approval in the appropriate team

How did we go forward

- Agreement from here to deliver new work in the next 3 months (3 months before 0.1)
- Decision to time-limit the policies so that future work is required before implementation in 0.2
- Agreement to resolve comments on the policies as soon as they appear
- Agreement to use all ofthe templates (including user facing policies) despite added bloat

What went wrong Saturday 5{" of October onwards

- Surprise rewrite and reformat of all security policy
- Not policies anymore
  - "Operating Level Agreements"
  - Don't need agreement, alignment or enforcement
- Exact details lost to time
  - Looked a lot like corporate security policies with Ctl+C Ctl+V from ISO 27001
  - Parts of policies where they don't belong
- Only 3 documents, no infrastructure policy
  - Approvals and Maintenance in all policies
  - Responsibilities for management, service providers and users in policies for those groups
  - Exceptions and sanctions section moved to service providers policy
  - Security Officer references removed

How it was fixed

- Security policy removed as a requirement for 0.1

- Find someone new to act as a middle ground
- Awaited installment of SKAO security officer
- Policy writing through inclusion
    - Show what is being done in other federations
    - Invite to relevant conferences
    - Introduce to more senior colleagues

How does the policy framework look now?

- Still OLAs
- Content of the policies back into a workable state
- Some artifacts of change still included
    - Password length
      https://confluence.skatelescope.org/pages/viewpage.action?pageId=274527742 (https://confluence.skatelescope.org/pages/viewpage.action?pageId=274527742)
      No work has been done since January

Learnings

- Policy development in agile frameworks needs to be done carefully or not at all
- Each step is fast but that doesn't mean you can rush the process
- Most time taken soclialising and getting approval
- Get direct involvement from federation/project leadership
- They need to feel like they own the policies
- Need shared understanding on how the work will actually be done
- Comments on policies are for conversation
- There is a point from which changing the policies is destructive

TAGPMA Update, ELM, and DCV server certificates

Derek joined from Pittsburg remotely. The chair and co-har are still the same (Derek and Ale), but the secretary and webmaster role are vacant for now.
The membership of TAGPMA is shrinking, with some CAs retiring (NCSA, SDSC), and DigitCert has not shown up recently either. These might be suspended if there are no updates. This should be chekced with the RPs (WLCG, EGI). The best souce would be DigiCert itself, but they do not quite answer.
WLCG & EGI: are users affected by DigiCert being withdrawn?

Having membership in more than one PMA (for eMudhra) is not common, but with each one being just oen ofmany members in a PMA (and the PMAs are independent but are a federation) the impact would be small anyway. And we do hae RPs being members of more than one PMA (WLCG).
It is unlikely to be a governance issue, so no reason to block.
And eMudhra is getting an American customer, with REUNA using eMudhra as an issuing back-end :)

Google trust services DCVOTA adoption under way
Alexandro has reviewed GTS and completed it positively. Mine will do the 2nd one. The GTS CPS is much more a live document, also incorporating changes for the IGTF use cases to facilitate accreditation.

@Derek: please provide the technical data for the distribution.

- some may be at https://pki.goog/repository/ (https://pki.goog/repository/) (TLS CPS version, July 2025)
- Is the 4th profile in the IGTF distribution
- Derek will act also as th Trusted Introducer from the Americas
- The RPs WLCG and EGI will accept this as part of the standard acceptable authntication authorities (alongside Classic, MICS, SLCS). Also since DCVOTA has all the controls on keyUsage and namespace in place.

REUNA Update

- REUNA CA replacing its infrastructure with cloud-based infrastructure provided by eMudhra.
- REUNA (Classic) CA CP/CPS updated to reflect updated certificate parameters and new CA service implementation.
- Comprehensive review conducted July-September, with several rounds of updates made to the CP/CPS as needed.
- Final comment round under way among TAGPMA voting members (deadline September 30, 2025).
- TAGPMA Vote to follow pending results of comment round inquiries.

Grid Canada CA update

- Current Grid Canada CA certificate updated (to be distributed in IGTF distribution 1.133) to extend validity to July 12, 2027.
- Grid Canada CA CP/CPS update review restarted in September 2025.

NSF Cybersecurity Summit 19-23 October, and SC in StLouis Nov 16-20 - those are the places to catch Derek!

TIIME Bus & Nar Conversation

Using eduID as a national account linking discussion in the (NFDI) node - and you can link more than one community AAI to my EduID. Where “my”/“you” is the end-user. The community AAI and eduIDs need a trust relationship.

The Community AAIs are OPs to the eduIDs.

But there would be a MyAccessID in the middle for everyone :(even for national users. It “would” be replaced by OIDF once available, but *how* that would help and avoid the mandatory MyAccessID is/was not yet clear.

Would be good to have the picture in a scenario with at least two national nodes that *both* have a national eduID - and then how does the common identifier for the user work out? The eduID would be generating the identifier, but then how to share that one across nodes?

Wallets will have ti easier to share identifiers, but just OIDF *will* ease trust between eduID and communities, and between nodes, but not necessarily the common identifier?

Discussions continue …

Tokens and token lifetime

AARC-G081 recommendations on life times by Marcus et al.

The scope is just about tokens getting lost or stolen, and whatshould (or will) happen then - so not about crypographi strength or QC. Properties are binding, rotation, rovocation, and the signature.

- https://aarc-community.org/guidelines/aarc-g081/ (https://aarc-community.org/guidelines/aarc-g081/)

The guidance is intended to be general and apply to any: people setting up an new OP, and get with 'sane' defaults. Ifthere are some edge infrastructures that need excessively long lifetimes (outside the scope of the guideline) then there is an escape clause and still claim 'reasonable' life times.

- Access Tokens that can be verified offline: 1 hour, 15min, 6 hours (linked to incident response times) since they cannot be revoked at all
- Access Tokens that must be verified online: 1 hour, 15 min, 25hrs
- Refresh Tokens are designed to live longer than Access Tokens - different for public clients and confidential clients. Where the public clients are discouraged, and the max refresh token lifetime for public clients is limited to 30 days. A binding between the client and the user can be used to mitigate part of this to compensate for stealing refresh tokens. Binding the (software) public client to the user is a way out - but an ongoing debate.

These should also the defaults for setting up a new OP.
The intent of using refresh tokens, and having them live long enough, is clear.

This now goes back to AEGIS (Monday 13th of October) for approval.

AARC=G100: establishing trust between proxies using OpenID Federation

The idea was to hve an informational document to 'profile' OpenID Federation, and this document should describe the federation model – in a document shorter than the OIDF spec itself (it is now 35 pages):

- https://docs.google.com/document/d/1i-SblN6e5Uaw7iJQUBRXZzyf-RTae38nq7mR-6nyFlE (https://docs.google.com/document/d/1i-SblN6e5Uaw7iJQUBRXZzyf-RTae38nq7mR-6nyFlE)

Two trust models:

- G100.1 basic trust model is just OIDF
- G100.2 trust mark based federation: The filtering uses Trust Marks on the federation level to only get relations between only selected entities. And it adds metadata policies.

Comments on G100 can still be sent until October 10th – and it will be sent to AEGIS on October 13th in time for the November 10 AEGIS meeting.

At least EGI and EOSC are interested in implementing this guideline – but of course GARR actually has a working federation 😄

AARC-G052 OAuth2 proxy token introspection

The use case is a token from infra A ends up at OP of Infra B, and there is some trust between infra A and B. How to deal with validation of the token if you don't know about the other infra.

The OP software does not need to be changed at all with TIP. This is already used in production (although the exact party is not known). The EOSC AAI relies heavily on token introspection.

This guideline is in AEGIS final call.

AARC-G056 Expressing identity attributes

This addresses the attribute profiles and what can you expect from you OP. Most OPs implement this (apart from the CERN OP - this is what the GUT would try to solve), as it implements G069 entitlements.

There are binding for SAML, OIDC, SCIM, LDAP, and for OIDC in which scopes the claim will be provided.

This document also defines the name mapping between attributes, claims, and assertions.

Government eID for identity assurance (and wallets)

Assurance evaluation work for AARC-I085

- https://wiki.geant.org/spaces/AARC/pages/1176567841/AARC-I085+eID+assurance+model+suitability+assessment (https://wiki.geant.org/spaces/AARC/pages/1176567841/AARC-I085+eID+assurance+model+suitability+assessment)
- https://docs.google.com/document/d/1s124B0DwCDGlgchTEAQy_NOHgYmuC8f7xs2O_l65j-M (https://docs.google.com/document/d/1s124B0DwCDGlgchTEAQy_NOHgYmuC8f7xs2O_l65j-M)

There are some challenges to integrate Wallets in the AARC BPA, with the hope/assption that the upcoming upcoming Walter ecosystem will help leverage govt eID assurance. The current eIDAS1 system is not helping, but eIDAS2+ may change that. This leads to the ongoing work:

- what to review and take into account when using the new ecosystem
- sections 6 and 7 are (very!) new today
- these actually fulfil the AEGIS need for guidance (and M2.2)

While technical systems are available, the uptake varies a lot between countries and sectors (as per the table made by Signicat). For example in the Netherlands, penetration of eID is very high, but scoped *only* to government and healthcare. But nowhere else. Whereas in the Nordics the bankID system is used throughout, in many sectors, and much more adoption by end-users.

ANd those are sill national. The eIDAS1 dashboard shows interconnects, but it is also obviou that not all memberstates are connected. And even if a technical interconnect exists, there are many cases where the connection is asymmetric. So even though there is trust and a tech infrastructure, it is not actually usable for the research communities (or even R&E in general).

The EUID Wallet Ecosystem is much more complex - the EUDI Wallet Instance (the purple box) is just avery small part with many other components. And policies: e.g. governments that might want to limit use, or trust, for certain services or sectors. And the model may not fit the multi-lateral model currently underpinning R&E federation and also the AARC BPA.

Assurance requirements:

- Identity Requirements, Unique, non-shared individual accounts, Persistent, non-reassigned identifiers, Identity proofing, Affiliation assertion, Strong authentication / Multi-factor authentication (MFA), Support for different assurance levels, Timely updating of identity, Requirements for outsourcing assurance
- Technical scalability: Adoption, Policy scalability, Machine-readable transparency, User perception, Fit for purpose

Now we want to outsource *our* assurance requirements to a govt partner. Like we see the issues in eduGAIN with the diversity of federations (which is there mitigated by the AARC BPA proxy model):

Requirements for outsourcing assurance

- Technical scalability: Only when the technical exchange of identities is based on open standards, and profiles have been defined to guarantee interoperability, identities may be used at scale, The cost for implementing and maintaining multiple standards and profiles is very high.
- Adoption level: The level Of adoption Of a certain identity scheme is defined in multiple Ways, The ability to adopt a certain system be limited by policy or cost, If an identity scheme is effectively a nice product, technical tooling may not be available to implement the identity solution, and developers might not be familiar with the implementation of the identity.
- Policy scalability: The identities of the user population of the research community have to live in authentic sources, which must be part of trust frameworks the research community can actually use. As research communities are often pan-European or even global, this may mean having to deal with trust frameworks with very different legal and policy requirements, as these are typically bound to all kinds Of local regulations. This may heavily influence the ability to use a certain identity resource.
- Machine-readable: Identity proofing steps, required attributes, levels of assurance, what evidence is required, etc., should be documented and made public. Also clear policies about who is responsible for what [Ziegler]. It is however impossible to (manually) read and evaluate all policies. Therefore the aforementioned processes should be not just transparency expressed but also in a machine readable format, allowing for automated even real-time evaluation and processing,
- User perception: Researchers have a certain perception Of Which identity they will Want to use to conduct their engagements with the research communities. Often, that perception Of What is acceptable and usable is based on local and cultural practices. This may lead to very different preferences across communities or countries.
- Fit for purpose: The identity sources should at least in part align with the primary business of the research communities. Using sources like e.g. the end-user oriented identity systems provided by Big Tech, may look very appealing because of scale and usability. However the very different business drivers of these parties pose a significant risk to the long term usability of such identities as policy and technical specification may change at any time in accordance with Big tech business drivers. [For example: FACEBOOK]

If e.g. the EUDI wallet ecosystem would require to register services in each member sate, that would be a blocking factor for our ecosystem, as it will never scale (and too many issues with jurisdictions).

The machine reasable work work with OIDF, as there the trust framework supports machine readable/actional assessment.

There are also cultural differences: is it accepted to use government ID for work? Itis standard in the Nordics, but quite strange to the Dutch :)
Same for the business drivers for identity and authentication sources. So is the ecosystem “Fit for Purpose”?

The assessment of eIDAS and assurnace coming from both aspects of these requirements.

Relation to the new BPA

Wallter may be *a* solution to the assurance problems (and where are dragons). But it does not

mean that it is the only possible solution. There are a few more solutions. And there are infra's like EISCAT where the users just do not have an IdP.
We are not going to directly assess Walters at this point in time. The mitigation for any challenges is not part of this document, and for some challenges there are no mitigations. It is too early, or solutions (like zero-knowledge proofs) are not part of the ecosystem yet. Also adoption may be and even remain aproblem.

"The Right Document at the Right Time"

VCs and Wallets (by Stefan)

From a more high-level overview on government eID for identity assurance and **wallets** (Stefan Liström, Sunet)

What should be included in the GN5-2 Wallet sub task to address AARC and FIM4R use cases?

Ongoing wallet work
First Large Scale Pilots (LSPs)
• DC4EU, EWC, Potential and NOBID, April 2023 - July 2025.
• DC4EU worked on the use cases for educational credentials e.g.
diploma and micro-credentials.
Second iteration of LSPs
• "WE BUILD" and "Aptitude", from August 2025 till August 2027.
• Focusing on both natural person wallet and business wallet.
and there is the Géant 5-2 project (and others).

Who is in charge of the identity used to identify yourself? Is that the "identity provider" in the traditional R&E federations, or the user, like in the Wallet ecosystem.

The GN52 EnCo Wallet task is investigative, exploring the landscape of Higher Ed and Research, including NREN invovlement, and see how that interacts or could interact with the Wallet ecosystem:

1. Current state of the Digital Identity Wallets
   – Regulation, national adoption & NREN involvement
2. Digital identity wallet terminology
   – Use of terms about the same thing in different specifications
   (and look at attribute name divergence between e.g. wallets and OIDC)
3. The role of identity federations in the wallet eco-system
   – Can OpenID federation be used both by eduGAIN and wallets?
4. Interoperability for Identity Wallets and Credentials
   – What do we need to do to interoperate between NRENs

These topics will evolve: making this a community effort, align terminology (and define an ontology) for wallets and credentials in R&E, cross-boundar use of identities and the underlying trust infrastructures, and interoperability - specifically also outside Euope.

Follow us or maybe even help us!

- Géant wiki: https://wiki.geant.org/spaces/G52W5/pages/958103668/Subtask+-+Wallets (https://wiki.geant.org/spaces/G52W5/pages/958103668/Subtask+-+Wallets)
- Join our community: https://lists.geant.org/sympa/info/wallet-community (https://lists.geant.org/sympa/info/wallet-community)
- Let us know if you have feedback on the wiki information or want to contribute: steli@sunet.se (mailto:steli@sunet.se)

Demos:

- Issuer - https://demo-issuer.wwwallet.org (https://demo-issuer.wwwallet.org)
- Wallet - https://demo.wwwallet.org (https://demo.wwwallet.org)
- Verifier - https://demo-verifier.wwwallet.org (https://demo-verifier.wwwallet.org)

How would e.g. students use these wallets in daily life? This is part of WEBUILD, but not in the GN project. Collaboration with users would be nice, but GN does not reach the end-user. But NRENs are interested in the education sector :)

Outside of Europe:

- In the US and Canada there is a lot of work, although the technology is a bit different - so interoperability and trust will be a bit challenges.
- In Japan there is issuing of microcredentials.
  This is a good time to align directions. The overall concepts are similar, but technology may be very different.

ELIXIR built a demo (already some time ago) to give access to a Finnish researchers for resourcs at the NIH, using verifiable credentials.
At least now we need up-front relationships to establish trust beween parties, and the ecosystem can be much more dynamic as technical trst and infrastructures does not need to exist upfront, but can be created on demand. This aids usability and makes many more use cases possible, esp. across boarders and outside of Europe.

The EUDI Wallet ecosystem is very nation-state driven, which can results in mation-state level blocks to prevent research collaboration across borders and regions. This may be a good reason to have our own governance model - and have models by community/infrastructure.

There should be a decentralised trust ecosystem underpinning this, so that the technology dos not create a risk dependency on specific parties (like GEANT suffered from with eduGAIN).

AARC-G100 decision on trust is with the end RPs.

Feedback on outsourcing criteria for AARC-I085 “eID Assurance” is much appreciated (and appreciated with a certain rapidity)

AARC G084 Security Baseline

Live editing of the document at

- https://sharemd.nikhef.nl/6PnNbLYOQH2bDHTiqi6mwA (https://sharemd.nikhef.nl/6PnNbLYOQH2bDHTiqi6mwA)

The document was consolidated and implementation details (the last paragraphs on designating a responsible persons) has been removed.

The Annotated Baseline (https://wiki.eoscfuture.eu/pages/viewpage.action?spaceKey=EOSCF&title=EOSC+Security+Operational+Annotated+Baseline#EOSCSecurityOperationalAnnotatedBaseline-collaborative-responseCanyouelaborateonwhatismeantbyitem9anditsincidentresponserequirements? (https://wiki.eoscfuture.eu/pages/viewpage.action?spaceKey=EOSCF&title=EOSC+Security+Operational+Annotated+Baseline#EOSCSecurityOperationalAnnotatedBaseline-collaborative-responseCanyouelaborateonwhatismeantbyitem9anditsincidentresponserequirements?)) will be ported to the AARC Wiki and become part of the PDF documentation.

Identity Federation and eduGAIN in Taiwan

WIth plns since 2018, now starting to link the TWAF Access Federation to eduGAIN, following the latest APAN meeting in Japan. It serves not only the HEP and APP experiments, but all of the scientific computing in TW with ASGC being the national scientific computing core facility - with support from the national science council.

A new stream of users was more web-based than the existing user base, which was fine with CLI access to facilities. JupyterLab and web-based notebooks are the preferred interface of the new, broader, user base.

The Taiwan Access Federation provides a framework and support infrastructure to facilitate trusted communications and collaboration within and between research and education institutions in Taiwan and overseas.

- Support data & resource sharing and collaboration infrastructure for R&E communities
- Shaping the enhanced NSTCCore/ASGC Authentication & Authorization Infrastructure
- Trust building and e-infrastructure efficiency are the cornerstone for the TWAF

This TWAF will be linked to the eduGAIN interfederation.
It will have 31+1 institutions, with 67 universty project PIs and 134 PIs from Academia Sinica, with in total 689 users.
TWAF will also support the library use cases - including ORCID login and cross-library resource access.

The SP use case is resource roaming and scavenging in a federated resource acces model - with account mapping between SPs.

The target to join eduGAIN is now by the end of October (slightly deferred). It will be based on PyFF (replcing Jagger which has been EoLed) - and moving out from the testbed to a dedicated infrastructure. It will be in a prototyping phase for 6-12 months hereafter, during which testing & verification, user community engagement, gap identification, and formulating operation plan will happen.

The initial federtion with be SAML-based, with plans for OIDC later. The Production Phase, with a business model and sustainability built in, is foreseen for Q4 2026.

Issues and Challenges

- Extra responsibility and cost at IdPs and SPs
- Privacy - what (personal) information will be shared by the federation
- Federation Operation: Single Point of Failure - high availability; Accounting; and Pricing

Choices:

- Prepare for OIDC at some point, not delaying the federation which must be SAML for now
- Hub-n-spoke would make transition to new technologies esier, but then has a higher FedOps cost (and who would pay that - even if the cost for SP/RP and IdP/OP is lower)
- joining now for free, but that will lower the capacity at FedOps to do all that work (not much staff foreseen now...)
- full mesh: they are now SAML IdPs and SPs, unfederated, and moving to H&S or Feide model would not quite work.
-

And join ISGC March 15-20, 2026 ()!

Low hanging fruits

- Filesender (filesender.org (http://filesender.org))
- EduROAM guest service (eva.eduroam.TLD)
- ORCID.org (http://ORCID.org)
- Sync and Share (nextcloud)
- Erasmus without papers (european student exchange)
- SurfSpot (https://www.surfspot.nl/ (https://www.surfspot.nl/) - discounted software for students based on uni site licensing &c)
- InAcademia (Student verification for studen discount) (paid for by industry) - https://inacademia.org/ (https://inacademia.org/)
  Furhter recommendations
- Make sure the REFEDS personalised attribute bundle will be release
- Entity Categories: R&S, Personalised, Sirtfi, (no DPCoCo in TW), and RAF Assurance
- Maybe also REFEDS Assurance Framework (RAF: https://refeds.org/assurance (https://refeds.org/assurance))

AARC Policy Development Kit: prioritisation and open tasks

Based on https://aarc-community.org/guidelines/aarc-i082/ (https://aarc-community.org/guidelines/aarc-i082/), the PDK stucture and policy wrk for the next 2-3 monhs will include:

What is Collaboration ***Membership Management***
This was highly contentiuous, trying to get consensus on what a Collaboration was. There is a UK-IRIS document on that.

This policy in the PDK is not yet there, but there is a draft of a short Membership Management policy draft, made at a short meeting between Hannah and DaveK on a new version:

- https://drive.google.com/drive/folders/1Dl1_9TcPA2OX9CsurYmZqWgKwKGPCQCL (https://drive.google.com/drive/folders/1Dl1_9TcPA2OX9CsurYmZqWgKwKGPCQCL)

The UK-IRIS version (at https://www.iris.ac.uk/wp-content/uploads/2023/05/IRIS_Community_Security_Policy.pdf (https://www.iris.ac.uk/wp-content/uploads/2023/05/IRIS_Community_Security_Policy.pdf)) puts more (12 point) requirements on the community, but already much simpler than the PDKv1 version, which had all fo the life cycle management included as well (which might be useful for annocated vresions and guidance, but also lots of stuff on governance).

For the PDK

- put on a wki with the pillar structure
- governance: these are the question ‘you’ need the answer. This is not a policy template, but more a series of questions and guidance.
- There shall not be a top-leve policy, but the text from I082
- at least fixup the membershipmanagement policy in the next 8 week
- create the PDKv2 on the AARC wiki
- discus and present at ACAMP in Denver, present at FIM4R
- dedicated meeting on this document (hopefully in Amsterdam/Utrecht?) Dave will talk to Hannah.
-

FIM4R evolution and planning

There will be a half-day meeting of FIM4R in Denver at TechEx (on the Sunday afternoon) and a full=day Monday on February 9th in Amsterdam colocated with TIIME2026 (https://indico.nikhef.nl/e/tiime2026 (https://indico.nikhef.nl/e/tiime2026)).

Agenda items for Denver could be:

- previou experiences from the communities
    - LiamA (or TomD) on a random topic on infrastructure
    - updates from the AAF
    - updates from internet2 if they have updaes
- Hannah will want to present the Compendium
- PDK v2
- Optional Eisaku
- Ask TomB for a (generic) update from the US communities (MaKr: it think it was a Internet2 person)
- Middlesize communities: asking Warren and/or Scott or Benn (SCG)
- What have we learned at the end of the day, where's the interaction
    - What is the role of middlethings for communities
    - Can express communities what they want and how do make sure they will if they can't
    - How do we reach out to the communities? As the big one have solved it (somehow) and small ones either use small tools, don't know us or use services (but how do we proxy these)
    - Have we reached out to all the audience we described in the fim4r papers? Did they (and we) followup
    - Vendor lock-in: do communities care? (all kind of lock-ins) - national orthematic?
    - analysis of the FIM4Rv2 requirements - what is needed fo v3?
    - Print out v2 and Cut out all the statements from v2 and ask the audience whether it's solved, failed miserably, no longer relevant, or still open.
- For the Amsterdam meeting:
    - get a preview from SURFaccess (Edwin vd Bospoort, Marlies) on UX design and the reltion between visibility into but not control over resaerhc collaboration from home orgs (and vv?)
    -

OpenID federation - updates by Davide Vaghetti

The eduGAIN OIDF Pilot has now started (after a 2-year incubation period). While today R&E federations are based on SAML, this will at some point change since SAML is no longer evolving, and most of the rest (industry, cloud) is moving to OAuth2 and OIDC 1.0.

But OIDC itself is missing a trust layer to build federation, and triggered the specification on the OpenID Federation, with Roland Hedbreg starting that work in the R&E space. The OIDF spec, while targeted at OIDC, is in priniple open to any protocol. Such as the EUID Wallets.
The eduGAIN Service and the T&I Incubator run a PoC to develop tools to build OID Federations for R&E.

With OIDF you get, as a recap:

- A Trust Framework for Federations: Defines a way to establish and manage trust between organizations.
- Hierarchical Trust Model: Trust flows through chains of signed JSON Web Token (like PKI).
- Signed Metadata Distribution: All critical configuration data (endpoints, keys, capabilities, policies) is published as signed JSON metadata statements that are fetched and validated from federation’s entities.

The specification defines

- Entity Statement: A signed JWT that contains the information needed for an Entity to participate in federation(s), including metadata about itself and policies that apply to other Entities that it is authoritative for.
- Trust Anchor: An Entity that represents a trusted third party.
- Intermediate Authority: An Entity that issues an Entity Statement appearing somewhere in between those issued by the Trust Anchor and the subject of a Trust Chain.
- Leaf Entity: An Entity with no Subordinate Entities. Leaf Entities typically play a protocol role, such as an OpenID Connect Relying Party or OpenID Provider.
- Trust Chain: A sequence of Entity Statements that represents a chain starting at a Leaf Entity and ending in a Trust Anchor.
- Trust Mark (new in the spec): Statement of conformance to a well-scoped set of trust and/or interoperability requirements as determined by an accreditation authority.
- Resolver: An endpoint that provides Resolved Metadata and Trust Marks to another Entity.

But the full protocolmay be a bit heavy for end-entities, esp. trust chain resolution (as in slide #8), with the authority hints and the dynamic retrieval and chain building.

For the eduGAIN implementation, there are three *prnciples*:

- Principle 1:
  The eduGAIN federation has one defined mechanism to establish trust among all the participants.

  - Requirement: Trust Chains is the basic technical trust of the federation.

- Principle 2:
  eduGAIN is a federation of federations, end organisations cannot join eduGAIN directly.

  - Requirement: All Immediate Subordinate Entities to the eduGAIN Trust Anchor MUST have the federation_entity entity type, such as Intermediate Authorities and Trust Mark Issuers.

- Principle 3:
  eduGAIN is a federation of federations and it builds on the layer of local trust already provided by the federation.

  - Requirement: An Immediate Subordinate Entity to the eduGAIN Trust Anchor MUST be a Trust Anchor for its subordinates and be operated by a federation operator. MUST provide a Metadata Registration Practice Statement (MDRPS). The MDRPS must contain metadata policies, including a description of trust chain constraints for subordinates.
  - the federations may allow intermediate authorities, as long as they put a requirement on those to *also* have an MDRPS. And no too mny levels, please!

- Principle 5:
  All the eduGAIN entities MUST be discoverable and their trust resolvable to the eduGAIN Trust Anchor.

    - Requirement: eduGAIN and Intermediate Authorities subordinate to the eduGAIN TA MUST provide a resolve endpoint.

- Principle 6:
  End entities that have eduGAIN as Trust Anchor must be validated against the eduGAIN OpenID Federation Profile. Additional validation is required to support other profiles, specifications and trust frameworks.

    - Requirement: Trust Marks convey trust information about the eduGAIN OpenID Federation profile and other profiles, specifications and trust frameworks.

These all went into the eduGAIN OpenID Federation Pilot, which has now (Oct 2025) started! A lot of groundwork has been done, with

- an overall comprehension of the OpenID Federation (OIDF) specification.
- working knowledge of OpenID Connect (OIDC) Providers and Relying Parties.
- working knowledge of the current eduGAIN SAML Technological Profile.

Use Cases - part 2
Validate entities to be "exported" to eduGAIN at the provided eduGAIN Trust Mark Issuer validator. Retrieve the issued eduGAIN Trust Mark and refer to it in the entities' statements. Repeat use cases - part 1 with Trust Marks.

The hard work: profiling the OIDF for R&E and alignment with the current constraints and security considerations (linked to the pilot since it is the same set of people)

Participation requests
Requests for participation should be sent by the eduGAIN delegate or deputy to support@edugain.org (mailto:support@edugain.org) With the followtng content:
• eduGAIN Participant name.
• The Entity Identifier of the Federation Trust Anchor.
• The Federation Trust Anchor public key in PEM format can be communicated in one of the following way: ...

To join the effort:

- Every other Monday 14:00 PM CET/CEST (full meeting schedule on the wiki page)
- Meeting Notes (rolling): https://docs.google.com/document/d/1eiigmnxUF6mmueaedCq6fSKeSOKtyoscw5EZ0THEOBM (https://docs.google.com/document/d/1eiigmnxUF6mmueaedCq6fSKeSOKtyoscw5EZ0THEOBM)
- Participants mailing list: https://lists.geant.org/svmpa/info/edugain-oidf-pilot (https://lists.geant.org/svmpa/info/edugain-oidf-pilot)
- GitHub: https://github.com/GEANT/edugain-oidf-pilot (https://github.com/GEANT/edugain-oidf-pilot)

For RPs to join OIDF there is simple Offa module (a bit like mod_shib/mod_authz) that is simple to add. The python stuff is not regularly maintained. There is no SaToSa module for OIDF parties. But there is a Rust implementation! (Gabriel did the Go version).

Support in Shib is also coming RSN.

For tranition scenarios: SAML will be around for a long long time, but maybe for eduGAIN you could have a single OIDFed infrastructure that you use to generate SAML MD distributions based on info in the OIDF ecosystem (as proposed by Niels van Dijk).

And now for something completely related: GenAI risks and its handling (Liam)

see also slides

No GenAI risk work done being made available by STFC, but also not by UKRI, DSIT, or the Government.
GenAI providers offer heavily biased risk analysis, and “UKRI states that only web-based Enterprise CoPilot should be used”. The GenAI in Project Management SIG created and use cases collected. These people have paid Enterprise CoPilot licences, but the Org is mostly not project managers.

What are we **not** doing:

- Telling people “no”
- Assessing how useful GenAI is in reality
- Enforcing the useless UKRI Policy
    - You have to use the web portal version of enterprise CoPilot
    - UKRI will not pay of enterprise CoPilot
    - Dept doesn’t have the money to pay for people to have enterprise CoPilot
    - 30 Project Managers across UKRI have a paid version
    - UKRI as a whole is 7736 people
    - The paid version is $30 a month
    - $232,080 per month for all of UKRI (E171,980 or€197,523)
    - UKRI themselves use an assortment of tools

In the suvey, of the 19 that repsonded “other”, about 9 of these used AI for writing scripts (the other 10 were “do not use AI”)

Even if you buy the Enterprise version of GitHub CoPilot, it iactually uses a mix of OpenAI, CoPilot, and Claude, so your input data leaks anyway to non-enterprise pltforms!

Risk Assessment Template can be shared (will be on the agnda).

Present online: Any Nguyen (AAF), Miroslv Dobrucky (IISAS), Amineh Akhavan (LRZ), Amin Mahnamfar (KIT), Stefan Liström, Niels van Dijk, Davide Vaghetti.
Present in Karlsruhe: Marcus Hardt, Gabriel, Peter, Patrick, Adrian, DaveK, MaartenK, DavidG, Eisaku, EricY, Liam Atherton