DRAFT

Trust and Identity
CTO Workshop Briefing paper 2023

CTO Workshops 2023 https://wiki.geant.org/display/GWP3/CTO+Workshops+2023

https://events.geant.org/event/1510/

Please add your comments to this document

2023 - CTO workshop briefing paper comments

Authors and Contributors

Casper Dreef (GÉANT), Christoph Graf (SWITCH), Christos Kanellopoulos (GÉANT), Davide Vaghetti (GARR), Klaas Wierenga (GÉANT), Leif Johansson (SUNET), Licia Florio (Nordunet), Maarten Kremers (SURF) Marina Adomeit (SUNET), Michael Schmidt (LRZ), Michelle Williams (GÉANT), Nicole Harris (GÉANT), Niels van Dijk (SURF), Paul Dekkers (SURF), Stefan Winter (RESTENA)

About this document

This document is the briefing paper for the CTO T&I Workshop that will take place in November 2023, with the purpose to discuss the GÉANT's 2025 - 2027 strategy for the T&I area. Based on the input gathered at the workshop, this paper will be updated and an action plan will be prepared to inform the preparation of GN5-2 and other GÉANT projects and initiatives.

Table of Contents

Executive Summary: Where we expect/want to be in 2027

The key principle of this strategy is to ensure that the GÉANT community continues to be the trusted provider for the T&I services in R&E. The Trust and Identity services delivered by GÉANT, in collaboration with National Research and Education Networks (NRENs), are expected to continue working towards an omnipresent Authentication and Authorization Infrastructure (AAI) for the Research and Education community. Mirroring the comprehensive reach of network provision, the AAI will be a cornerstone of the GÉANT programme, ensuring it is accessible to every user within the academic and research sphere in Europe. It will provide a pervasive, secure, interoperable and sustainable Trust Fabric, seamlessly integrated with the technological advancements, that supports and empowers a wide array of scholarly and research activities, fostering collaboration and innovation across Europe and beyond.

eduGAIN will be delivering a global Trust Fabric for Research and Education, continuing to provide the cornerstone for seamless federated access across institutions and acting as the trust mortar for the EUDI Wallets, while also laying a secure foundation for the emerging Data Spaces, ensuring robust and privacy-preserving scholarly and research collaborations.

The expansion of eduroam will continue its growth trajectory and the collaboration with OpenRoaming will provide more access capabilities for eduroam users. The user experience between eduGAIN and eduroam will become more unified (via geteduroam), offering a more seamless and integrated experience.

The GÉANT Core AAI Platform, building upon the eduGAIN Trust Fabric, will be integral to advanced R&E use cases, underpinning critical European initiatives such as the European Open Science Cloud AAI, EuroHPC, and Student Mobility. Key identity services such as InAcademia, MyAcademicID, MyAccessID, and the EOSC AAI Federated AAI will be using the GÉANT Core AAI Platform as their backbone. This integration will ensure a cohesive user experience and streamline access to resources, driving forward the capabilities and the reach of digital identity and access management across Europe's academic and scientific landscapes, while moving complexity from the edges of the ecosystem. The platform will be instrumental in enabling GÉANT and NRENs to deliver a spectrum of value-added services, fostering a more innovative, secure, and collaborative environment within the research and education sectors.

We expect the eduID ecosystem to be witnessing a substantial expansion throughout Europe, marking a new era of interconnectedness for educational identity services. While efforts towards complete

harmonisation will be continuing, there will already be tangible success stories, supported by a harmonised environment that bridges MyAcademicID, MyAccessID and national eduID services.

The EUDI Wallet is anticipated to be widely adopted by European students and researchers, with digital wallet usage becoming commonplace in Europeans' daily transactions. GÉANT, alongside NRENs, will be pivotal in providing the Trust Fabric that ensures the security and authenticity of educational credentials within this framework. Amidst intense competition in the digital wallet space, the trust and reliability offered by GÉANT and NRENs will be crucial.

We must continue exercising awareness regarding the significant threats the Research and Education Trust and Identity space faces from potential replacement by commercial solutions, leading to increased risks of vendor lock-in and misalignment with public values. To mitigate these challenges, it is crucial for GEANT, NRENs and institutions to adopt a proactive and unified approach towards procuring commercial services and diversifying their technologies by using the interoperable trust fabric the GEANT community offers. Furthermore, maintaining an open dialogue with stakeholders, including vendors, and actively participating in standard-setting bodies can help ensure that technological solutions align with the unique values and priorities of the R&E community. Finally by working together and providing our services governed by the, and for the GEANT community, we can safeguard the public values we cherish.

Sustainably operate and evolve the existing T&I services

GÉANT delivers a number of T&I services for the benefit of the R&E community in Europe, and beyond. Those services are: eduroam, eduGAIN, Core AAI Platform (previously known as eduTEAMS) and InAcademia. The service teams are composed by members from the NREN community and where skills are not available, by contractors.

GÉANT will continue to operate and evolve the services within the T&I portfolio. These services need to be delivered with operational excellence to reflect the reputation and importance of T&I services that are nowadays core R&E infrastructure. Special care needs to be directed into securing the sustainability of T&I services in the area of funding, human resources and technology. While the Core AAI Platform and InAcademia already have business models that enable them to use other funding sources, eduroam and eduGAIN are solely relying on the GÉANT project funding. During GN5-1, an analysis about funding the core service delivery of eduroam and eduGAIN services from the GÉANT membership fee is being conducted. The result of this analysis will inform the next steps regarding eduroam and eduGAIN, but also about other services that have a similar horizontal nature.

eduGAIN

The evolution of eduGAIN as a global Trust Fabric and fundamental infrastructure for any advanced T&I service in the R&E sector, will be based on two pillars: improved governance to facilitate decisions and the introduction of a baseline that all eduGAIN participants will need to comply with, in order to increase the trust and interoperability assurances between the eduGAIN entities. The eduGAIN baseline will be built upon REFEDS specifications, which are de-facto standards for the T&I in the R&E sector. The improved governance has been accomplished with the approval of a new eduGAIN Constitution, which includes a new governing body, the eduGAIN Steering Committee, that will be crucial to drive change. Pending implementation of the new eduGAIN Constitution that will commence in 2024, the new eduGAIN Steering Committee shall be in position to make the eduGAIN baseline mandatory, after which it is planned that the eduGAIN service team will work on its implementation. This work will include communication and business development to support eduGAIN members during the transition, and also to adapt eduGAIN tooling and operational processes to support the new baseline.

With the identity landscape changing, new technologies such as OpenID Connect becoming mainstream and the push for a more user-centric identity management which is being implemented via EUDI wallets, it is important to ensure that eduGAIN value is recognised and its position is maintained and strengthened. To date, eduGAIN already offers a global trust anchor root for the R&E worldwide: this can allow eduGAIN in the coming years to facilitate the introduction of new frameworks, but for that to happen eduGAIN needs to expand to a technology neutral, global Trust Fabric that can enable trust via multiple technology profiles. This Trust Fabric with its global trust anchor root and members adhering to the agreed baselines is the foundation for mutual recognition and trusted interaction in cross-sector use cases.

Core AAI Platform

The GÉANT Core AAI Platform is envisioned to be a cornerstone in the landscape of advanced research and education (R&E) by 2027, providing the critical infrastructure for key European initiatives such as the European Open Science Cloud (EOSC) AAI, EuroHPC and programs supporting student mobility across the continent. It will serve as the foundational backbone for a suite of essential identity services, including InAcademia, MyAcademicID, MyAccessID, and the EOSC Federated AAI, enabling the delivery of an omnipresent AAI to the NREN infrastructures, the High Performance Computing area, European Research Infrastructures, and the broader education sector (Figure 1).

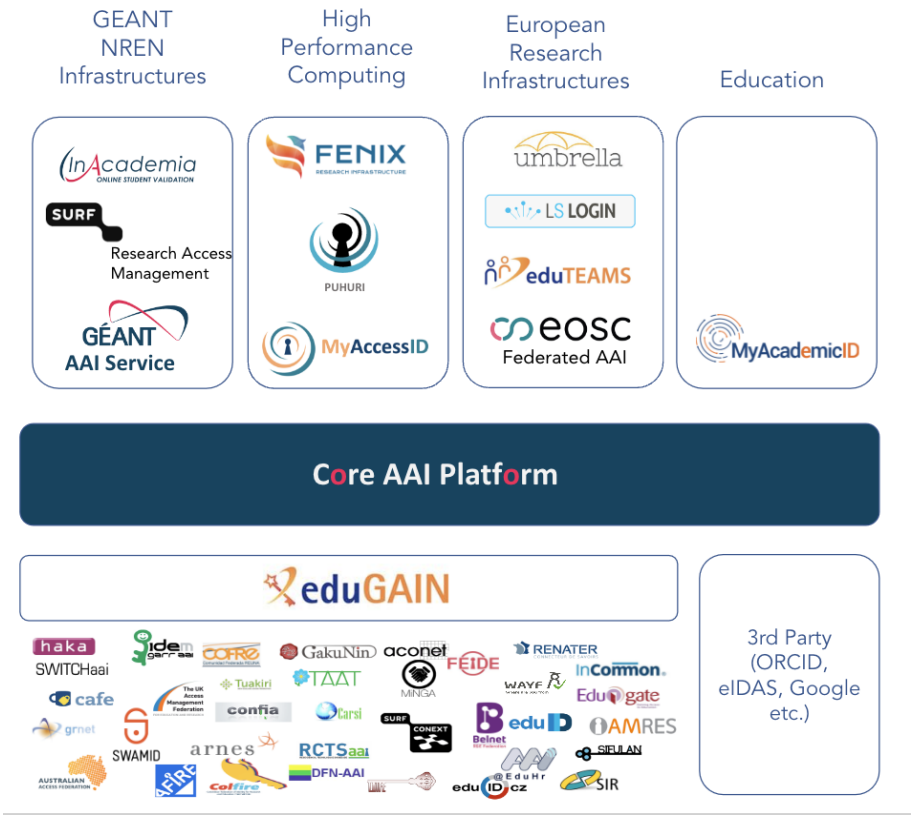

Figure 1. Overview of eduGAIN and Core AAI Platform

On the backend, the Core AAI Platform will offer a robust control plane, significantly enhancing the efficiency of service delivery, both for existing services and for facilitating the roll-out of new ones. By implementing an API-first approach, the platform will ensure a high level of integration capability, allowing NRENs to weave these services seamlessly into their existing ecosystems. This approach not only enhances the current offerings but also paves the way for the addition of richer functionalities that NRENs can extend to their user bases via their own channels. For instance, NREN Federations will be able to support OpenID Connect relying parties, provide identities to high value services that require for medium and high-level proofing—essential for trust in digital interactions—, deliver flexible second-factor authentication mechanisms that can be deployed as needed, depending on the security

requirements of the service or the data being accessed and deliver advanced community and group management management capabilities.

The Core AAI Platform will not leave any NREN behind. For those without the capacity or desire to maintain their own technical systems, the platform will offer a comprehensive UI layer equipped with "sane defaults." This means that these NRENs can outsource the technical heavy lifting to the Core AAI Platform while still delivering advanced capabilities. This inclusive feature ensures that even NRENs with limited resources can provide their constituents with access to state-of-the-art identity and access management tools.

This evolution of the GÉANT Core AAI Platform represents a stride toward a more integrated, secure, and user-centric digital infrastructure for the European R&E community. As the needs of this community grow increasingly complex, the platform's role in simplifying, securing, and scaling service delivery becomes ever more critical, cementing GÉANT's position as a leader in digital identity services for R&E on a global scale.

The strategic design of the Core AAI platform, with its clear delineation from the AAI services layered above, is set to provide a dual evolution path, ensuring that each can progress in its domain without impeding the other. This separation enables AAI services to innovate and grow independently, fostering the development of distinct business models and service offerings that still rest on a robust and enduring technological base. Such a foundational separation is poised to maximise both agility and stability within GÉANT’s service ecosystem, supporting a diverse and dynamic environment for R&E advancements, with the end goal of providing a converged user experience.

InAcademia

The InAcademia Service will continue to deliver and innovate the privacy preserving, pay-per-validation interface towards commercial services. Operating in steady state, its focus will remain on outreach, as well as developing features for alternative onboarding methods that intend to increase uptake; this is in the context of the continued desire to build alternative sources of revenue for T&I. The integration with the GEANT Core AAI Platform will continue towards its completion, opening the door for use of new capabilities (such as the EUDI Wallet) and synergies with services, such as MyAcademicID, to deliver more a holistic approach towards an evolving ecosystem of services that requires student validation capabilities.

MyAcademicID

MyAcademicID's planned expansion to focus on University Alliances, alongside its continued support for the Erasmus Without Paper programme, represents a strategic evolution within the European educational landscape. As eduID deployments become more prevalent across NRENs and a gradual shift towards an eduID-centric ecosystem is anticipated, MyAcademicID will foster a closer relationship with these initiatives and provide a key integration layer, delivering advanced capabilities required by scholarly services.

In tandem, the alignment between MyAcademicID and InAcademia is expected to offer a seamless user experience, greatly enhancing the European student mobility framework. This synergy is further reinforced by the Core AAI Platform's upcoming support for the EUDI Wallet, empowering MyAcademicID to manage and issue Verified Credentials firmly rooted in the eduGAIN Trust Fabric. The incorporation of the EUDI Wallet into MyAcademicID will not only offer a first hand immersion into new service access paradigms but will also significantly shape the educational sector's adoption of this emerging technology.

Moreover, MyAcademicID's capability to issue Verified Credentials will provide a bridge for Higher Education Institutions (HEIs) that are not immediately ready to update their software stack to accommodate new technologies. This feature will ensure these institutions can still participate in the EUDI Wallet ecosystem, maintaining inclusivity and facilitating a smoother transition period as they upgrade their systems. This dual approach underscores MyAcademicID's potential to act as both a facilitator and a guide in the unfolding narrative of educational technology integration within Europe.

MyAccessID

MyAccessID is swiftly establishing itself as an indispensable identity layer within the High Performance Computing ecosystem. Its essential role has been further solidified by the EuroHPC Joint Undertaking's recent tender call, which stipulates that the EuroHPC Federated Platform must utilise MyAccessID. This is a considerable leap forward, however to fully realise the ambition of creating an omnipresent AAI for the research and education sectors, continued efforts and developments are necessary.

MyAccessID spearheads a number of innovations that are being introduced in the AARC Blueprint Architecture and which are first implemented by the Core AAI platform. Support for compensating

identity vetting controls and 2FA capabilities are already underway, while support for a new paradigm of terminal access via SSH, critical for a large number of scientific use cases, is already in pilot. The MyAccessID model, strategically designed to integrate Infrastructure Service Domains rather than individual services, offers a scalable and robust framework that is conducive to the sustained expansion of service use cases. Towards this direction, MyAccessID will take advantage of the new control plane that will be provided by the Core AAI platform and enable the NRENs to be able to integrate MyAccessID in their own service portfolio and provide the same capabilities to their national research infrastructures.

EOSC AAI

GÉANT, in collaboration with National Research and Education Networks (NRENs), remains pivotal in the development and provision of AAI services, integral to the delivery of EOSC. EOSC will continue to leverage the existing AAI provided by NRENs and GÉANT, optimising resources and avoiding redundancy by capitalising on these established structures rather than developing parallel systems. By 2027. EOSC will focus on contributing to the standardisation process and providing unique requirements and use cases. This approach will enable the EOSC to focus on its strengths, offering valuable insights to inform standards within the R&E sector.

eduTEAMS

eduTEAMS has been a trailblazer in implementing advanced Authentication and Authorization Infrastructure (AAI) services tailored for Research Infrastructures, following the AARC Blueprint Architecture. It operates with two distinct business models: eduTEAMS Shared and eduTEAMS Dedicated. As new identity layers from services like MyAcademicID and MyAccessID come into play, eduTEAMS is set to pivot towards a model where these services provide the identity layer. Consequently, eduTEAMS will concentrate on enhancing its community, collaboration, and group management features.

This strategic shift is anticipated to simplify the eduTEAMS service portfolio, effectively reducing its complexity. By streamlining its offerings, eduTEAMS aims to deliver a more focused and efficient suite of tools that cater to the evolving needs of research communities, emphasising the facilitation of collaboration within and across various research groups and projects.

eduroam

The adoption of eduroam continues to grow, and we continue to partner with the industry on standardisation (eg. in the Wi-Fi Alliance) and roaming activities. We see the service has served as a blueprint for the industry, like WBA's OpenRoaming. OpenRoaming serves as a neutral host between service providers and identity providers in the world, not just in the educational sector. As eduroam is a member of WBA, we can offer OpenRoaming services to our community and continue to make eduroam a part of OpenRoaming for those interested in its capabilities. With the status quo of deployed equipment and software it is still challenging to use the technologies involved for all users and institutions, therefore it is not expected that OpenRoaming will replace eduroam, but it will benefit eduroam users with additional coverage and give organisations additional options to provide guest-access where it is applied. The onboarding of users is an important topic for the adoption of eduroam. Initiatives like OpenRoaming, Hotspot 2.0 ask for different ways of onboarding, requiring specific tools. This makes this work even more necessary and therefore it remains a key activity in the eduroam task, with geteduroam and similar tools relying on eduGAIN as the trust anchor for their operations.

Continue to innovate in the T&I area

The Trust and Identity area is in continuous expansion in all sectors; work is under way to align and standardise protocols across sectors in order to to improve security, transition the architecture to a more user-centric model and to lower the overall cost of development and deployment.

GÉANT community is engaging in innovations at different layers:

- Within the GÉANT services to ensure they keep evolving;
- Within the GÉANT project by supporting incubator tasks to allow for more agility in exploring new, potentially disruptive, topics. The Incubator is complemented by the TIM (Trust and Identity Mentorship) programme which was developed as an instrument for NRENs to give the opportunity for young talents to work in the T&I area;
- By participating in key international activities in standardisation and software development, such as IdentityPython (it provides common funding and governance for key federation and identity technologies), WiFi alliance, WBA, IETF, W3C etc;

- By participating in activities of strategic importance, which are elaborated in the last paragraph of this document.

The activities around the distributed identity and the EUDI wallets have been significant during the last year. These developments are creating a new model for how digital identities will be issued and used by researchers and students. It is becoming clear that the wallet paradigm is pushed from government and industry as the solution to interact with services so it is important that we establish this interaction with our environment. While some members of our community actively participate in projects related to EUDI wallets and education use cases, we need to complement and establish this work within the GÉANT activities and build our strategy to that end. The landscape around EUDI wallets is still very much in development (both in legislation and standardisation area), and perhaps at this point of time we cannot say with certainty which kind of activities will need to happen post 2025, however it is clear that we will need to engage with this and to that end plan the effort. Some of this effort will go into adapting our software stack to be able to work with digital identity wallets (issuer, verifier, trust fabric), but activities such as evolving the idea around the education wallet might be very relevant as well. Crucial for the success will be to forge strategic partnerships within and outside of the academic community.

There are many wallet related activities happening outside the GÉANT project and several GÉANT members including GÉANT are involved in,e.g. the EUDI Large Scale Pilots. We have a significant presence and knowledge of our community to help inform decisions and take the lead from what the rest of the academic world is doing, and also from what the EC explicitly needs our community to do. However tactical coordination to achieve this will be crucial, and in that respect GÉANT will play a key role.

Academia, research and education are not islands but are very much dependent on and affected by what is happening outside the sector. In the field of R&E trust and identity we have been “blessed” by being in a leadership position for so long, however we must not forget that other sectors of society are also working in the same field.

Support GÉANT community to expand the coverage and quality of their T&I services

The increased demand for identity services puts an additional pressure on GÉANT and the NRENs. Service providers and communities expect a quick response to their needs regarding the use of federated identities. It is recognised that more effort is needed to better promote T&I services, and the work should be done within the NRENs constituency, GÉANT community and towards the relevant stakeholders and communities. This should at the same time enable to disseminate the work done within the NRENs and to make sure that the community needs are well articulated for federations to be ready to respond and to roll out new features.

Examples where coordination with federations was key to successfully support the requirements for user's digital identity are the European Student Identifier requirement for the Erasmus+ programme and the identity assurance requirements for access to the EuroHPC resources. GÉANT needs to be an instrument of connecting and translating the T&I business demand from different areas into the requirements for R&E federated identity. Without such a vehicle to instigate CTOs and IT Managers at institutions to understand why active support for high-quality IdPs and attribute release is important, other strategic initiatives risk failure at the ground level. In order to scale we may also need to build partnerships with other actors to provide integration and first-line support for T&I services.

It is evident that proper resourcing of the T&I expertise and technical capabilities remains to be an issue for many organisations - from the academic and research institutions and infrastructures all the way to the federation operators. This is evident in cases of slow adoption of new frameworks and gathering requirements, but also from the footprint of federated identities in the educational institutions, where we can observe in a number of countries a significant gap. The GÉANT community needs to address these issues by constantly investing in building competences and capabilities, but also by providing alternative solutions such as eduIDs.

Continue to play a strategic role in the T&I area in the R&E

The GÉANT community has been playing a strategic role for years in delivering, innovating and enabling community collaboration in the T&I area. The Trust and Identity have expanded during the years to address the growing need for strategic engagement required by the GÉANT community.

- **REFEDS:** It is the global initiative that brings together R&E Identity Federations to articulate the requirements of R&E in the ever-growing space of access and identity management. REFEDS is providing frameworks for standardising T&I across the Academic and Research Federations. In addition, REFEDS works with other organisations, on behalf of its participants, in order to influence the direction of initiatives that are key to the Federations. REFEDS is supported by GEANT and the contributions of its members.
- **AARC & AEGIS**: Authentication and Authorization for Research and Collaboration (AARC) community is a collective of experts and stakeholders from the research and education sector, focused on developing and promoting a harmonised approach to authentication and authorization. The community works to implement the AARC Blueprint Architecture, creating a framework that enables seamless access to online resources and services across different institutions and borders. The AARC Engagement Group for Infrastructures (AEGIS) is the governing body of the AARC community. It brings together representatives from research and e-infrastructures, operators of AAI services and the AARC team to bridge communication gaps and make the most of common synergies. AEGIS enhances the wider and more effective uptake of AARC guidelines and recommendations by infrastructures in their federated access solutions, so that they can focus on providing other support for research activities. A new AARC Project for which the GÉANT community has secured the funding will start in 2024. In over two years it will deliver an updated AARC Blueprint alongside a set of recommendations for a common long-term strategy for AAI services from infrastructures.
- **FIM4R**: Federated Identity Management for Research is a collection of research communities and infrastructures with a shared interest in enabling Federated Identity Management for their research cyber infrastructures. In order to achieve this, FIM4R develops requirements bearing on technical architecture, federated identity management, and operational policies needed to achieve a harmonious integration between research cyber infrastructures and R&E Federations.

- **Student mobility**: GÉANT and NRENs need to continue playing a key role in the Student Mobility space. The collaboration with the EC and the National Agencies on the support for the Erasmus+ programme will continue. In addition, we are expanding our focus also to the emerging space the University Alliances. The University Alliances is a flagship initiative under the European strategy for universities, , launched by the European Commission. The ambition of this initiative is to expand to 60 European Universities Alliances involving more than 500 higher education institutions by 2024.
- **EuroHPC:** Represents a pivotal initiative for Europe, aiming to bolster its technological independence and global competitiveness through the development of a robust high-performance computing ecosystem. Already, MyAccessID is recognised as the mechanism for authenticating users in the EuroHPC Federated Platform. GÉANT and the NREN community need to remain closely engaged and deliver the AAI that meets the evolving requirements of the EuroHPC stakeholders.
- **EOSC:** It is a cornerstone initiative for the European scientific community, aiming to unify research data and resources across disciplines and borders. As a federated ecosystem, EOSC will continue leveraging the strong, secure, and interoperable AAI infrastructure provided by GÉANT, ensuring that researchers can access resources efficiently and securely, thus fostering a more integrated and accessible European research landscape.
- **Data Spaces:** Data Spaces are a key architectural component within the European strategy for data, designed to facilitate secure and seamless sharing and interoperability of data across different sectors and borders. They are envisioned to allow businesses, governments, and researchers to collaborate and innovate on a scale previously unattainable, harnessing the power of big data and AI while respecting EU values and regulations such as data privacy. GÉANT and the NRENs need to ensure their presence in the design and implementation of Data Space that is relevant to the research and education space, ensuring that we can meet emerging requirements and that our T&I services play a key role across sectors.
- **SeamlessAccess Initiative**: designed to help foster a more streamlined online access experience, while maintaining an environment that protects personal data and privacy. Seamless Access bridges the user experience gap, improving the usability of existing federations and federated services. The service is delivered through a coalition of Internet2, GÉANT, NISO and STM, where GÉANT provides operational and product management capabilities. The SeamlessAccess Initiative will be focusing on improving the adaptability of the service within the local federation context and in delivering the first class discovery support for the EUDI Wallet.

- **EUDI wallets:** GÉANT aims to fortify eduGAIN as the R&E Trust Fabric and develop a federation framework for digital wallets leveraging OpenID Connect, striving to set a global standard for digital wallet interfaces in research. While national initiatives will guide educational use, the unregulated, global nature of research necessitates universally deployable digital wallets. The strategic relationships we build should include global research collaborations, infrastructures, dataspaces, public and private organisations and NGOs that in some way interface with the global research system in a user-facing way. Building such a strategic partnership is hard. GÉANT should start small, start with the relationships we have and build iteratively.
- **Standardisation Bodies**: Engagement with key standardisation bodies such as IETF and W3C is crucial for GÉANT as it enables influence on the development of global standards, ensures interoperability and the adoption of cutting-edge technologies, and maintains technical excellence. This involvement strengthens GÉANT's leadership position, advocates for the needs of the research and education community, fosters beneficial collaborations, and provides insights that support innovation within the sector.