T3.1B User-centric identity federation

Description

- Develop user-centric identity federation: user-managed access.
- Engage with federations on the principle of user-managed access, not only technically, but also reflecting the principle that the user is the resource owner and should therefore be in control of their own “data”.
- Develop pilots based on eduKEEP- and eduID-like approaches, currently at TRL 6–8 in various national developments, to enhance to scale for international interoperability.

Information

https://www.geant.org/Innovation/Research_programmes/Pages/eduKEEP.aspx

Deliverables

Best Practice for User Centric Federated Identity

Summary

The current practice for identity federation in research and education is to manage identity with an organisation-centric approach, where users are assigned an identity as part of their enrolment process in organisations. This identity attached to the organisation can then be used to access services in a federation or inter-federation. This deliverable looks at identity in a wider context and outlines how to combine user-managed or user-centric identities with organisational identity. In this scenario organisations are no longer the sole providers of identity in a research and education context, but the advantages of classic identity federation are preserved, especially in terms of vetting, trusted sources of attributes, and privacy.

This change in architectural approach aims to address challenges for lifelong R&E identity and stemming from an increased mobility of users between institutions that have been observed over more than 10 years of R&E identity federation operations in production. Focusing on those use cases where a user-managed rather than organisation-managed R&E identity is an improvement over current practices, assessments are provided of the demand for this sort of approach and the readiness level of federations to adopt it, and example architectures and best practices outlined for delivering user-managed, lifelong R&E federated identity and the related policy and governance.

A user-managed R&E identity model can especially improve the current user experience and user management practices over the organisation-centric approach for use cases related to mobility between institutions, multiple affiliation and lifelong learning. Account linking enables the user to have access to all relevant affiliations at a given time, and the existence of an educational identity independent of individual organisations enables lifelong learning, while providing a closer trust relationship with the sector than fully commercial or social identity providers.

Currently two NRENs, SWITCH (Switzerland) and SUNET (Sweden), are taking the lead and already implementing this new approach, although based on different architectures. GARR (Italy) is planning to roll out its own version of this model, incorporating national eGOV-ID identities. These three architectures are compared and analysed in the document.

Finally, a set of practices are identified to guide potential adopters who are considering moving from an organisation-centric approach to user-centric R&E identity management. Policy, governance, data protection, technology, security and interoperability principles are covered.

The work presented in this deliverable, including practical examples of NRENs that are adopting this approach and the additional knowledge gathered, aims to encourage more federations to consider the shift from purely organisational identities to lifelong individual R&E identities which enable users to manage their relevant affiliations more flexibly.