FIM4R Position Paper

On the Desired Evolution of EOSC Authentication and Authorisation Infrastructures

Authored by: the FIM4R Community

The European Open Science Cloud (EOSC) will soon enter the next phase of integration and consolidation with the establishment of a common service portal listing underpinning services that enable distributed resources in the areas of computation, data, open access, and above-the-net collaboration services. The existing e-Infrastructures that are anticipated to be part of the EOSC each provide their own capabilities in terms of trust and identity management, integrity protection and risk management, as well as capabilities to support business continuity and disaster recovery in case of security incidents. There are also specific trust, collaboration management, and security services that are jointly managed by multiple e-Infrastructures for the benefit of (but in many cases not exclusively) the European research and collaboration community as a whole. These include for instance the glue between the EOSC AAI suite of services that each implement the AARC Blueprint Architecture (AARC BPA), i.e. the AAI services such as those from both national and pan-European Infrastructures as well as components such as credential translation bridge services.

The Federated Identity Management for Research (FIM4R) community at a recent full-day workshop in Vienna and at the TIIME conference later the same week (17-20 Feb 2020) discussed its views on the evolution of the EOSC AAI and the conclusions are documented here[1]. These have been distributed to the whole FIM4R community, including those who were not in Vienna, with individuals given a two week comment period after which all input was incorporated. This paper is an agreed statement on behalf of the whole community.

We believe that the successful EOSC AAI landscape will be composed of multiple, interoperable Authentication and Authorisation Infrastructures (AAIs) protecting clusters of services. The following recommendations are intended to enable this desired outcome.

The EOSC AAI Framework Should Integrate with Existing Services

The level of maturity varies significantly between Research Communities, with some already operating production AAIs and others more likely to seek an AAI service offered through EOSC. All these AAIs must interoperate within EOSC and provide researchers with an intuitive, “low-friction” user experience. Many researchers are accustomed to existing authentication flows, through web interfaces branded by their own Research Community - FIM4R does not

[1] Please note: the majority of FIM4R Research Communities represent funded bodies that operate production infrastructure, at the same time we recognise the large level of diversity among the long tail of science and have attempted to keep it in mind when writing this document.

believe that Researchers should change this flow to authenticate via “Login with EOSC” or equivalent. Rather, EOSC services should be transparently integrated behind Research Community proxies.

EOSC Should Incorporate Existing Services

Some Research Communities may also wish to offer services to other Research Communities through EOSC; such a process should be made as intuitive as possible without users visibly leaving the environment of their own Research Community.

Harmonise AAI Services within EOSC

Any EOSC AAI service offerings should leverage existing products and services (i.e. not reinvent the wheel), and be made available in a modular way such that individual components can be plugged in to existing AAIs if relevant. As stated in FIM4Rv2, *“The diversity of the research communities should be reflected in the AAI offerings; we do not see a single solution as a sustainable future.”* AAI services, solutions and products offered by EOSC should be available for Research Communities to select **on demand**, Research Communities should not be expected to adopt a specific tool and undergo a costly migration to a new system to benefit from EOSC. At the same time, Research Communities must be prepared to adopt interoperability guidelines in line with the AARC BPA. These guidelines already include relevant standardisation of protocols and user identity and access schemas for use in EOSC. Such guidelines should be agreed and adopted following consensus between multiple Research Communities and Infrastructures operating production AAIs. Establishing trust between AAIs (and with the services behind them) is essential; certain best practices in operational security (e.g. Sirtfi) and the ability to support federation frameworks (such as the REFEDS Assurance Framework) should be mandated. We see the AEGIS community as an appropriate body for agreeing such guidelines.

The EOSC AAI Framework Should Prioritise User Experience

Researcher experience must be prioritised, such as: minimising the number of required authentications (Single-sign-on), limiting the number of Acceptable Use Policies and consent workflows to which a user is exposed, ensuring sufficient attribute release between proxies for valid authentication. In light of the high variability of computing background per research domain, researchers must not be expected to navigate complex technical processes to enable their access. A scalable, legal, solution should be found to enable the flow of personal data required for authentication and authorisation in alignment with the EU’s General Data Protection Regulation (GDPR).

EOSC Should Provide Operational Support

Experience with Federated Identity in FIM4R indicates the need for a strong operational support capability that coordinates with Research Community infrastructure operators to resolve user authentication and authorisation issues - EOSC should take this into account.

Links and References

[AARC Blueprint Architecture] https://aarc-community.org/architecture/
[REFEDS] https://refeds.org
[AEGIS] https://aarc-community.org/about/aegis/
[FIM4R] https://fim4r.org
[FIM4Rv2] https://doi.org/10.5281/zenodo.1296031
[TIIME] https://tiimeworkshop.eu
[Sirtfi] https://refeds.org/sirtfi
[REFEDS Assurance Framework] https://refeds.org/assurance