Contribution ID: **16** Type: **Oral Presentation**

Sitting under a broad-leaved AARC-TREE – making authentication and authorization for research collaboration even better

Friday, March 29, 2024 11:30 AM (20 minutes)

The authentication and authorisation infrastructures (AAIs) for research worldwide have for years now based their architectures in the "AARC Blueprint Architecture" and the suite of accompanying guidelines. Developed by the "Authentication and Authorisation for Research Collaboration" (AARC) community, and fostered by the accompanying "engagement group for infrastructures" (AEGIS), the model has been a key ingredient of the European Open Science Cloud, many national research AAIs, and research and e-infrastructures in Europe, the Americas, and the Asia-Pacific region. However, with the increased scope and complexity of novel federated identity models, come new challenges. The single 'AAI proxy' model of the initial AARC blueprint – which combined identity sources, community collaboration management, authorisation controls, and service provider connections - has already evolved to include both 'infrastructure proxies' to provide coherency on the service provider side, as well as 'community proxies' focussing on membership management.

Yet the challenges keep coming at an ever-increasing pace, both in terms of complexity as well as in the range of communities that can benefit from this coherent 'AARC approach' to federated access management. The new AARC-TREE project, the short label name for "AARC Technical Revision to Enhance Effectiveness", will define common strategies for the development and deployment of AAIs in the large-scale Research Infrastructures where single proxies do not suffice.

For example, there are multiple technical federation models (such as OpenID Connect Federation besides SAML) and a multitude of identity sources (academic, governmental, and self-sovereign) that need to co-exist and be linked together. And global interoperability between infrastructures must be strengthened to avoid fragmentation and unnecessary duplication.

At the same time, we see that collaborations and thematic research domains struggle to keep up when just provided with guidelines and architecture, and this gets more urgent as collaborative AAIs extend beyond research to education, high-performance computing, and mid-sized communities.

In this contribution, we will reflect on the AARC Blueprint Architecture for AAI and identify its critical areas that need improvement, look forward to addressing more AAI interoperability requirements and service gaps for more research infrastructures, and to enhancements of the AARC BPA to support more effectively research infrastructures by further expanding authorisation aspects and enabling new use-cases. The upcoming project combines both technical and architectural measures as well as trust and identity policies to define and validate new technical and policy guidelines for the AARC BPA. We will describe the project objectives, the outline of the upcoming architectural and trust policy guidelines, and – most importantly – how one can contribute to this open and deliberately globally inclusive process. By employing existing structures (such as REFEDS, FIM4R, IGTF, and WISE), via a compendium process, and through broad global representation in AEGIS as a direction-setting body, the project strives to expand the number of research communities that can implement the AARC BPA and the AARC guidelines.

Primary author: GROEP, David (Nikhef and Maastricht University)

Co-authors: KELSEY, David (STFC-RAL); Dr KANELLOPOULOS, Christos (GÉANT); KREMERS, Maarten (SURF); FLORIO, Licia (NorduNET); LIAMPOTIS, Nicolas (GRNET)

Presenter: GROEP, David (Nikhef and Maastricht University)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations