Contribution ID: **41** Type: **not specified**

Can R&E federations trust Research Infrastructures?

Tuesday, 7 March 2017 14:00 (20 minutes)

Research Infrastructures increasingly use national and global "Research and Education" (R&E) authentication federations to provide access to their services. Collaborators log on using their home organization credentials, the Research Infrastructure (RI) enriches it with community information, and access decisions are made on its combined assertions. Studies in the AARC project have shown that research communities connect to the R&E federation using an 'SP-IdP proxy' design pattern: a single logical component makes the RI appear as a single entity towards the R&E federations. The RI can also augment the 'R&E identity' of their users with membership information. Thus the RI shields itself from heterogeneity in the global R&E federations and it eases service deployment by 'hiding' all services behind a single proxy identity provider (IdP) that itself needs to be registered only once in R&E federations. The AARC Blueprint Architecture identifies this model as a recommendation for engaging research collaborations with R&E federations.

The use of a proxy in itself poses policy challenges: services 'internal' to the community see only a single IdP that they have to trust ultimately. Generic service providers that span multiple research communities will have to trust many of these proxies – there are over a hundred multi-national RIs in the world but many multi-purpose e-Infrastructures as well. And towards the R&E federations, the SP-IdP proxy hides all of the research services: home organisations and R&E federations see just a single service provider, even if the services behind it are provided in hundreds of different administrative domains.

Building on the Security for Collaboration among Infrastructures (SCI) framework, the "Security Networked-Community Trust-framework for Federated Identity" (Snctfi) proposes a policy framework that allows determination of the 'quality' of such SP-IdP proxies and the research services behind them. For example, a SP-IdP-proxy for EGI – proxying for all its compute and storage services – would be able to express to the R&E federation space that is has an internally-consistent policy set, that it can make collective statements about all its constituent services and resource providers, and that it will abide by best practices in the R&E community, such as adherence to the Data Protection Code of Conduct (DPCoCo), REFEDS Research and Scholarship (R&S) entity category, Sirtfi – the security incident response trust framework that is in itself a development from the SCI structure.

By addressing the structure of the security policy set that binds services 'hiding' behind the SP-IdP proxy, Scntfi allows comparison between proxies, assign trust marks for meeting requirements, and it allows a scalable way to negotiate and filter based on such policies. It eases authentication and attribute release by R&E federations as well as service providers (by easier enrolment in federations and because R&E IdPs may be more willing to release attributes if the proxy can convincingly assert DPCoCo and R&S), but also aids assessment by generic e-Infrastructures providers that know the RI proxy meets their trust requirements.

We will describe the requirements on the Scntfi framework and show how it applies to research and generic e-Infrastructures.

Primary author: Dr KELSEY, David (STFC-RAL)

Co-author: Dr GROEP, David (Nikhef)

Presenter: Dr KELSEY, David (STFC-RAL)

Session Classification: Network, Security, Infrastructure & Operations I

Track Classification: Networking, Security, Infrastructure & Operations