Contribution ID: **12** Type: **Full presentation: short (15 mins.)**

Making Identity Assurance and Authentication Strength Work for Federated Infrastructures

Tuesday, 3 November 2020 09:45 (15 minutes)

In both higher Research and Education (R&E) as well as in research-/ e-infrastructures (in short: infrastructures), federated access and single sign-on by way of national federations (operated in most cases by NRENs) are used as a means to provide users access to a variety of services. Whereas in national federations institutional accounts (e.g. provided by a university) are typically used to access services, many infrastructures also accept other sources of identity: provided by 'community identity providers', social identity providers, or governmental IDs. Hence, the quality of a user identity, for example in regard to identity proofing, enrollment and authentication, may differ - which has an impact on the service providers risk perception and thus their authorization decision.

In order to communicate qualitative information on both identity vetting and on the strength of the authentication tokens used between the identity providers and service providers, assurance information is used - with the strength being expressed by different Levels of Assurance (LoA) or 'assurance profiles'combining the various elements in community-specific ways. While in the commercial sector assurance frameworks such as NIST 800-63-3 or Kantara IAF have been established, these are often considered as too heavy with strict requirements, and not appropriate for the risks encountered in the R&E community. This is why in the R&E space a more lightweight solution is necessary.

The REFEDS Assurance Suite comprises orthogonal components on identity assurance (the REFEDS Assurance Framework RAF) and authentication assurance (Single Factor Authentication profile, Multi Factor Authentication Profile) and provides profiles for low and high risk use cases. The Suite is applicable in many scenarios, like identity interfederations (cross-national collaborations) or for exchanging assurance information between identity providers and Infrastructure Proxies (according to AARC Blueprint Architecture). This presentation serves as a guidance on how the assurance values can be assessed and introduced into existing AAI scenarios.

This 15 minutes talk starts with a short overview of existing assurance frameworks such as NIST 800-63 and Kantara and the standards introduced in the R&E sector. We will discuss their relationships and dependencies and how they relate to the management of risks. Following that, use cases of the REFEDS Assurance Suite will be presented to show how the REFEDS specifications can be used to exchange identity and authentication assurance in cross-collaborative scenarios. The focus of this talk lies in providing basic recommendations to facilitate the adoption of exchanging assurance information. The recommendations will provide information about both the identity side, i.e. based on employed processes, what can be said about the quality of the identity assurance, and on the services side, i.e. based on the provided services and use cases, what is the required or expected identity assurance.

Primary authors: Mrs ZIEGLER, Jule Anna; GROEP, David (NIKHEF); STEVANOVIC, Uros (KIT-G); KELSEY, David (STFC); NEILSON, Ian (STFC); KREMERS, Maarten (SURFnet)

Presenter: Mrs ZIEGLER, Jule Anna

Session Classification: How to make your service more secure?