Federated Identity Management Considerations

This list of questions was compiled to provide a starting point for identifying requirements for FIM at a new infrastructure. What considerations should be made during the design if an infrastructure intends to use federation via eduGAIN as its primary access mode?

User Groups

- Do all R&E users belong to an eduGAIN enabled home organisation?
- Are there any users outside the R&E Community? E.g. citizen scientists.

User Data

- Which attributes will be required from home organisations?
- Which additional attributes, if any, will be required from the users directly?
- Which additional attributes, if any, will be required by the infrastructure/community? (e.g. group memberships or entitlements, cf. also section “Authorisation” below)
- What user data will be stored centrally within the infrastructure?
- For how long will user data be stored?
- How will a user be able to request a change to or deletion of their user data?
- How will an individual be identified?
- How will multiple accounts belonging to an individual, either consecutively or in parallel, be associated?
- How will variation in user data from multiple home organisations be resolved?
- How will assurance of the accuracy of user attributes be established, for the authentication token overall and on a per-attribute basis?
- Will each identity provider populate a global, non-reassignable unique ID?
- Will all user data remain within the organisational domain of the collaborative organisation? (or are external services (PAAS/IAAS) used?)

Participant Policies

- Will a common policy set be defined for all participating organisations; e.g. security response, data protection?
- Is there an acceptable use policy for end users?
- Which takes precedence if a participant policy for this infrastructure contradicts a local policy of a home organisation?
- How will participating organisations assert compliance with relevant policies?
- How will end users assert compliance with relevant policies?

Security

- How will the risk profile of the services accessed via the infrastructure, including external services, be established?
- Is the security capability of each participating organisation sufficient to cover the risk profile of the services?
- Is the security capability of each participating organisation known and documented?
- Is adequate proactive and reactive software defence employed at each participant organisation? How is this defined?
- How will traceability of user actions be established?
- Will shared accounts be granted access to the infrastructure?
- Can we ensure that participants proactively contribute to incident response?
- Are participating organisations Sirtfi compliant? https://refeds.org/sirtfi

Trust

- Do we have sufficient assurance that the identity belongs to the asserted person?
- How will participating organisations' membership be established?
- Are face-to-face passport checks or other forms of identity proof required?
- Can existing identity proofing at participating organisations be reused?
- Does identity vetting need to be controlled centrally, by the infrastructure?
- Do all participating organisations agree to abide by confidentiality protocols during incident response and general communication?

- Is there an established network of trust groups to provide coverage of all the participants?
- Are there individuals identified at participating organisations to assist with trust and security?

Authorisation

- Will an authorisation system be used to define user roles within the infrastructure? Would such an authorisation system be externalised?
- Will there be any automatic mapping between attributes and user roles?
- Will a blacklist of authorisation be implemented?
- How will membership be expressed?
- Are multiple authorisation roles needed?
- Is there a relation between authentication assurance and authorisation roles? How is that expressed?

Contributors: Niels van Dijk (SURFnet), Mikael Linden (CSC), Mark Jones (UTHealth), Michal Prochazka (CESNET), Lukas Haemmerle (SWITCH), Hannah Short (CERN), Romain Wartel (CERN), Wolfgang Pempe (DFN)