Self-assessment tool

This document has been written following the identification of a need within the Research and Education Federation communities for a tool by which to express and monitor compliance with policies and best practices. The self-assessment tool is intended to manage the quality standards self-evaluation process for the entities registered to the eduGAIN inter-federation service. At the time of inception, the following use cases were drivers for the development of a centralised, flexible tool:

- the evaluation of Level of Assurance (LoA) for Identity Providers (IdPs)
- the evaluation of LoA for Service Providers (SPs)
- the assertion of compliance with the Security Incident Response Framework for Federated Identity (Sirtfi)
- the assertion of compliance with the Data Protection Code of Conduct (CoCo)

GEANT project (GN4-2 JRA3 T2.4 Identity Assurance Service) is implementing the tool during 2017.

Software requirements specification

- Draft requirements specification (please comment!): Google doc
- Please comment in the document or send the editors (Hannah Short and Mikael Linden) an email if there is anything specific you would like to discuss.
- Presentation in 22 June 2016: Google slides

Summary

Tool Use Cases
- LoA assessment for IdPs
- Sirtfi compliance for IdPs and SPs
- GEANT Data protection Code of Conduct for SPs EU/EEA
- SP Assurance level (“inverse” of IdP LoA assessment)

Key Requirements (for details, see the requirements specification)
- Responsibility for the tool should be at a federation level. This does not preclude running the tool centrally. This will aid scalability
- The tool should send assessment requests to organisations based on contact information in metadata
- The tool should support multiple question types, yes/no and multiple choice
- Machine readable responses (yes/no/multiple choice) should be supported by secondary, evidence-based free text
- The tool should facilitate peer review; peer assignment should not be determined by the assessee
- Results of assessments should be made available; individual assessee results would be private to the assessee but an aggregated view should be freely available
- Fed Ops should have access to all results of the assessments within their federation
- Access control for an assessment should facilitate private and public sharing
- The tool should support re-assessment and have configurable behaviour in the event that the re-assessment is not done or if it fails