Operational Requirements for Service Providers

Version 1.0
(04 April 2012)

SP Operational Requirements

Purpose of this document

This document defines identity management and system operation requirements and recommendations for Service Providers joining the HREF Federation.

Throughout this document the interpretation of terms **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT** are defined as:

- **MUST** (or **SHALL**, **REQUIRED**): the definition is an absolute requirement of the specification in order to build and keep trust in the federation.
- **MUST NOT**: the definition is an absolute prohibition of the specification
- **SHOULD** (or **RECOMMENDED**): there may be valid reasons for ignoring the definition, however, the divergence from the specification **MUST** be documented
- **SHOULD NOT** (or **NOT RECOMMENDED**): there may be valid reasons for the particular behaviour to be acceptable, however, the divergence from the specification **MUST** be documented

Identity management

1. The organisation running the Service Provider **MUST** have a Privacy Policy, and its location **MUST** be indicated in the Resource Registry.

Service management

1. The organisation **MUST** develop a role responsible for liaison with the Federation Operator.
2. The organisation operating the Service Provider **MUST** provide end-user support about its service and have its users informed about the availability of the support.

Operational issues

1. Cryptographic keys of the Service Provider **MUST** be at least *1024 bits* long.
    1. Private keys **MUST** be protected.
    2. In case of a key compromise, the Federation Operator **MUST** be notified within *24 hours*.
    3. Use of self-signed certificates with a long expiration time is **RECOMMENDED**.

2. Use of SAML:
    1. The Service Provider **MUST** comply with the *Interoperable SAML 2.0 Web Browser SSO Deployment Profile* (http://saml2int.org)
    2. It is **RECOMMENDED** to support *SAML2 Single Logout Profile* over HTTP Redirect and SOAP Bindings.
3. All SAML endpoints of the Service Provider **SHOULD** be protected by HTTPS.
4. All SAML endpoints of the Service Provider **MUST** be under a DNS domain which is either possessed by the operating organisation, or the organisation **MUST** be commissioned by the owner of the domain (according to WHOIS database) in written form for using its domain in eduID.