Operational Requirements for Identity Providers

Version 1.0
(04 April 2012)

IdP Operational Requirements

Purpose of this document

This document defines identity management and system operation requirements and recommendations for Identity 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 operating the Identity Provider **MUST** document its privacy policy and make it available to its users.
2. The organisation **MUST** define the sources, the maintenance procedures and approximate quality of the data about its users, and supply this documentation to the Federation.
3. Uniqueness of the usernames **MUST** be guaranteed.
4. One individual **SHOULD NOT** have more than one user accounts.
5. Role accounts (such as 'director', 'secretary') **SHOULD NOT** be used.
6. Use of attributes:
    1. Attribute implementations **MUST** follow the Attribute Specification.
    2. The Identity Provider **MUST** implement the following attributes:
        - eduPersonTargetedID
        - eduPersonScopedAffiliation
        - schacHomeOrganizationType
        - eduPersonPrincipalName
    3. The Identity Provider **SHOULD** implement the following attributes:
        - displayName
        - mail
        - eduPersonEntitlement

    4. The IdP **MUST** ensure that eduPersonTargetedID and eduPersonPrincipalName are not re-assignable.
7. Limitation of test accounts:
    1. all test accounts **MUST** be identified and documented along with the individual who is responsible for the test account
    2. real transactions **MUST NOT** be initiated by test accounts
    3. test accounts **SHOULD** be distinguished with appropriate homeOrganizationType value.
8. User credentials (i.e. passwords) **MUST NOT** be transmitted over public network in unencrypted form.
9. If initial user passwords are distributed, it **SHOULD** be done through non-electronic form
10. Changes in the users' affiliation to the institution **MUST** be populated to the IdP database within *7 days*
    1. If the authoritative source of user information is an external database (i.e. student information system), then the above timeframe starts from the time of the change in the primary system.
    2. Students may use 'alum' affiliation after leaving the organisation. Values 'student' or 'member' **MUST NOT** be used afterwards.
    3. For faculty members and employees, affiliation values 'staff', 'employee', 'faculty' and 'member' **MUST** be revoked.

Service management

1. The organisation **MUST** develop a role responsible for liaison with the Federation Operator.
2. The organisation operating the Identity Provider **MUST** provide end-user support for its affiliated users and have them informed about the availability of the support.
3. The organisation **MUST** provide the following data to the Federation Operator as anonymous daily statistics about the Identity Provider usage:
    - number of unique users;
    - number of transactions initiated to each federation service;
    - total number of logins.

Operational issues

1. Any transaction including personal data **MUST** be logged and log files **SHALL** be kept for at least *30 days*.
    1. The log files above **MUST** be treated in accordance with the applicable data protection laws.
2. Cryptographic keys of the Identity Provider **MUST** be at least *2048 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**.
3. Use of SAML:
    1. The Identity Provider **MUST** comply with the *Interoperable SAML 2.0 Web Browser SSO Deployment Profile* (http://saml2int.org)
    2. It is **RECOMMENDED** to support *SAML2 Web Browser SSO Profile* over HTTP Artifact Binding.
    3. It is **RECOMMENDED** to support *SAML2 Single Logout Profile* over HTTP Redirect and SOAP Bindings.
4. All SAML endpoints of the Identity Provider **SHALL** be protected by HTTPS.
5. All SAML endpoints of the Identity Provider **MUST** be under a DNS domain which is possessed by the operating organisation.
6. All scopes used by the Identity Provider **MUST** be under a DNS domain which is possessed by the operating organisation.