* Final draft * Final draft * Final draft *

REFEDS Identity Federation Baseline Expectations

Abstract:

This document defines a common set of expectations of all participant organisations to establish a baseline of trust in identity federations.

Audience:

This document is intended for those responsible for the operation of Identity Providers, Service Providers, Identity Federations and Identity Interfederation.

Table of Contents

1. Introduction

This document lists the required operational behaviours of Identity Provider, Service Provider and Federation Operators to meet Identity Federation Baseline Expectations (IFBE) for a common trust framework.

Identity Federation Baseline Expectations are met by satisfying the below requirements; how those requirements are met is covered in supporting documentation and subject to continual trust improvements. They are not a fixed target but a long-term commitment to an improving technical and policy landscape, the process being an evolutionary journey rather than a final destination.

These expectations apply to the constructs referred to, for example in SAML, of Identity Providers and Service Providers. They apply regardless of the particular federation

technology or software in use and are commitments of the organisation on whose behalf they are operated.

2. Baseline Expectations of Identity Provider Operators [IPO]

- [IPO1] Your Identity Provider is operated with organizational-level authority
- [IPO2] Your Identity Provider is trusted enough to be used to access your organization's own systems
- [IPO3] You publish contact information for your Identity Provider and respond in a timely fashion to operational issues
- [IPO4] You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response
- [IPO5] You ensure the metadata registered in Federation is complete, accurate and up to date

3. Baseline Expectations of Service Provider Operators [SPO]

- [SPO1] You ensure that controls are in place to protect user privacy in the service
- [SPO2] You do not share information received from Identity Providers with third parties without relevant notification and the information is stored only whilst necessary for operational purposes
- [SPO3] You publish contact information and respond in a timely fashion to operational issues
- [SPO4] You apply security practices to protect user information, safeguard transaction integrity, and ensure timely incident response
- [SPO5] You ensure the metadata registered in Federation is complete, accurate and up to date
- [SPO6] You publish requirements for any user information required to access your service and ensure these requirements are appropriate and respect privacy

4. Baseline Expectations of Federation and Interfederation Operators [FO]

- [FO1] You focus on trustworthiness of Federation as a primary objective and are transparent about such efforts
- [FO2] You publish contact information and respond in a timely fashion to operational issues

- [FO3] You apply security practices to federation operations and ensure timely incident response
- [FO4] You follow good practices to ensure authentic, accurate and interoperable metadata to enable secure and trustworthy federated transactions
- [FO5] You implement and support frameworks that improve trustworthy and scalable use of Federation and promote their adoption by members and other participants
- [FO6] You collaborate with other organisations to promote realization of baseline expectations nationally and internationally