

# 1 Draft REFEDS Identity Federation 2 Baseline Expectations

3

## 4 Abstract:

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

7

## 8 Audience:

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

11

## 12 Table of Contents

13

14	<b>1. Introduction</b>	1
15	<b>2. Baseline Expectations of Identity Provider Operators [IdP]</b>	2
16	<b>3. Baseline Expectations of Service Provider Operators [SP]</b>	2
17	<b>4. Baseline Expectations of Federation and Interfederation Operators [FO]</b>	2
18	<b>5. References</b>	3

## 19 1. Introduction

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

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

28 In these statements, the terms “Identity Provider,” “IdP,” “Service Provider,” and “SP” refer to  
29 their usage within the SAML Browser SSO profile [SAML2prof] as operational entities that  
30 act in the federation and not to the organizations that operate them.

## 31 2. Baseline Expectations of Identity Provider 32 Operators [IdP]

33

- 34 • [IdP1] Your Identity Provider is operated with organizational-level authority
- 35 • [IdP2] Your Identity Provider is trusted enough to be used to access your  
36 organization's own systems
- 37 • [IdP3] Your Identity Provider must have contact information published allowing timely  
38 response to operational issues
- 39 • [IdP4] You apply security practices to protect user information, safeguard transaction  
40 integrity, and ensure timely incident response
- 41 • [IdP5] You ensure the metadata registered in Federation is complete, accurate and  
42 up to date
- 43 • [IdP6] You support applicable and necessary automated release mechanisms of user  
44 information

## 45 3. Baseline Expectations of Service Provider 46 Operators [SP]

- 47 • [SP1] You ensure that controls are in place to protect user privacy in the service
- 48 • [SP2] You do not share information received from Identity Providers with third parties  
49 without relevant notification and the information is stored only whilst necessary for  
50 operational purposes
- 51 • [SP3] Your Service must have contact information published allowing timely  
52 response to operational issues
- 53 • [SP4] You apply security practices to protect user information, safeguard transaction  
54 integrity, and ensure timely incident response
- 55 • [SP5] You ensure the metadata registered in Federation is complete, accurate and  
56 up to date
- 57 • [SP6] You publish requirements for any user information required to access service;  
58 ensure these requirements are appropriate and respects user privacy (unless  
59 governed by an applicable contract)

## 60 4. Baseline Expectations of Federation and 61 Interfederation Operators [FO]

- 62 • [FO1] You focus on trustworthiness of Federation as a primary objective and be  
63 transparent about such efforts
- 64 • [FO2] Your Federation must have contact information published allowing timely  
65 response to operational issues
- 66 • [FO3] You apply security practices to federation operations and ensure timely  
67 incident response
- 68 • [FO4] You follow good practices to ensure authentic, accurate and interoperable  
69 metadata to enable secure and trustworthy federated transactions

- 70 • [FO5] You implement and support frameworks that improve trustworthy and scalable
- 71 use of Federation and promote their adoption by members and other participants
- 72 • [FO6] You collaborate with other organisations to promote realization of baseline
- 73 expectations nationally and internationally

## 74 5. References

- 75 • [IFBE] REFEDS Identity Federation Baseline Expectations, {Link TBD}
- 76 • [SAML2prof] OASIS Standard, Profiles for the OASIS Security Assertion Markup
- 77 Language (SAML) V2.0, March 2005. <http://docs.oasis->
- 78 [open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)
- 79