InCommon

Baseline Expectations for Trust in Federation

Version 2

Final; November 3, 2020

Repository ID: TI.34.2
Authors: Members of the InCommon Community Trust and Assurance Board
Sponsor: InCommon Community Trust and Assurance Board (CTAB)
Superseded documents: TI.34.1 http://doi.org/10.26869/TI.34.1
Proposed future review date: November 2021
Subject tags: InCommon, federation, assurance, trust, framework

Introduction

As the strategic value of Research and Education Trust Federations ever increases, from time to time it is important to reflect on, then assess and distill what forms the basis for sufficient trust amongst all participants. On that foundation, we can identify gaps and agree to changes that need to be implemented by various Federation actors in order to sustain and grow that trust.

What trust do we, as participants, need to have in the Federation? When we rely on the Federation, we are relying on other organizations to do something for us that we would otherwise do for ourselves or forgo altogether. The unique value proposition of the Federation makes possible the integration of resources, services, and users across the globe into the myriad ways that the R&E mission is undertaken.

This document describes the expectations for each of the three types of Federation actors: Identity Provider, Service Provider, and Federation Operator. Together, they express the Baseline Expectations for Trust in Federation.

Version 2 of this document continues the mission to further trust in the federation by clarifying a few security and supportability requirements.

In these statements, the terms “Identity Provider,” “IdP,” “Service Provider,” and “SP” refer to the operational entities that act in the federation and not to the organizations that operate them.

InCommon Federation Baseline Expectations

Baseline Expectations of Identity Providers

1. The IdP is operated with organizational-level authority.
2. The IdP is trusted enough to be used to access the organization’s own systems.
3. Generally-accepted security practices are applied to the IdP

    3.1. The IdP complies with the requirements of the REFEDS Security Incident Response Trust Framework for Federated Identity v1.0 **[Sirtfi]**.

    3.2. All IdP service endpoints are secured with current and trustworthy transport layer encryption.

4. The IdP’s published metadata is accurate and complete, including site contact information (at least one each technical, administrative, and security contacts) and Login and Discovery User Interface (MDUI) information (display name, logo URL, privacy policy URL).

5. The IdP's published metadata includes a current errorURL **[Metadata]**.

Baseline Expectations of Service Providers

1. Controls are in place to reasonably secure information and maintain user privacy.
2. Information received from IdPs is not shared with third parties without permission and is stored only when necessary for SP's purpose.
3. Generally-accepted security practices are applied to the SP
    3.1. The SP complies with the requirements of the REFEDS Security Incident Response Trust Framework for Federated Identity v1.0. **[SIRTFI]**.
    3.2. All SP service endpoints are secured with current and trustworthy transport layer encryption.
4. The SP's published metadata is accurate and complete, including site contact information (at least one each technical, administrative, and security contacts) and Login and Discovery User Interface (MDUI) information (display name, logo URL, privacy policy URL).
5. Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly.

Baseline Expectations of Federation Operators

1. Focus on the trustworthiness of their Federation as a primary objective and be transparent about such efforts.
2. Generally-accepted security practices are applied to the Federation's operational systems.
3. The Federation supports the Security Incident Response Trust Framework for Federated Identity **[SIRTFI]**.
4. Good practices are followed to ensure the accuracy and authenticity of metadata to enable secure and trustworthy federated transactions.
5. Frameworks that improve the trustworthy use of the Federation, such as entity categories, are implemented and adoption by Members is promoted.
6. Work with relevant Federation Operators to promote the realization of baseline expectations.

Implementation Considerations

It is equally important to consider how these baseline expectations are to be operationalized: why, and how, should anyone believe that these expectations are met in almost all federated transactions? Is it important to know, fairly promptly, when any of those expectations no longer hold, or is it enough to know that the process by which partners become active in Federation ensures that those expectations are valid? What keeps them on track? This is addressed in companion documents **[BEPractice]** to be referenced here upon their acceptance by the InCommon Federation.

Appendices

Appendix A: References

[SIRTFI] REFEDS Security Incident Response Trust Framework for Federated Identity. https://refeds.org/sirtfi.

[BEPractice] Baseline Expectations Implementation Guide. http://doi.org/10.26869/TI.137.1.

[Metadata] SAML 2.0 Metadata Guide. https://www.oasis-open.org/committees/download.php/51890/SAML%20MD%20simplified%20overview.pdf

https://www.oasis-open.org/committees/download.php/56786/sstc-saml-metadata-errata-2.0-wd-05-diff.pdf

https://kantarainitiative.github.io/SAMLprofiles/saml2int.html (see [SDP-MD12])

Appendix B: Change Log for this Document

Changes in version 2, TI.34.2

- **Renaming AAC to CTAB** - The Attribute Assurance Committee (AAC) has been renamed Community Trust and Assurance Board (CTAB). All prior references to AAC have been changed to CTAB.
- **Formatting Baseline Expectations Statements** - Updated numbering to the Baseline Expectations Statements to make referencing each statement easier across all documents.
- **Introduction** - revised phrasing to improve readability
- **Paragraph 1.3** - IdP needs to conform to SIRTFI framework; reiterates IdP requirement to encrypt endpoints
- **Paragraph 1.5** - IdP must register errorURL.
- **Paragraph 2.3** - SP must conform to the SIRTFI framework; all SP endpoints must be encrypted.
- **Paragraph 3.3** - Federation Operator must support SIRTFI.