Baseline Expectations for Trust in Federation

Final v1, September 2016

Repository ID: TI.34.1
Authors: Tom Barton and members of the InCommon AAC
Sponsor: InCommon Assurance Advisory Committee (AAC)
Superseded documents: (none)
Proposed future review date: December 2018
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 by all participants. On that foundation we can understand gaps and agree to changes that may need to be implemented by various Federation actors in order to sustain that trust.

What trust do we need to have in Federation? When we rely on Federation, we are partnering with other organizations to do something for us that we would otherwise do for ourselves or forgo altogether. And mostly the latter: Federation makes possible the integration of resources, services, and users across the globe into the myriad ways that the R&E mission is undertaken.

Below are three short lists of expectations expressed at a high level, one for each of three types of Federation actor: an Identity Provider, a Service Provider, and a Federation Operator. Different specific situations may have higher or lower risk and hence greater or lesser expectations, but the following are expectations that should be true of all, or almost all, transactions with Federation partners. They express the baseline for trust in federation.

This formulation of the baseline expectations is the result of a year-long iterative process of assessment and feedback, shepherded by InCommon's Assurance Advisory Committee. Early steps produced a strawman that formed the basis for gap analysis with the views of subsequent audiences whose feedback was rolled into further updates to the strawman. The culminating step in the process took the form of an open "consultation," in which federation-involved people around the world were invited to give their feedback to the last strawman. That step produced some refinement to language but no substantive change to the baseline. So there is reason for confidence that this formulation is a reasonable expression of where the community believes that baseline to lie, at this time.

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.

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
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

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
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and 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 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. Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions
4. Frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted
5. Work with relevant Federation Operators to promote realization of baseline expectations

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 to be referenced here upon their acceptance by the InCommon Federation.