Baseline Expectations for Trust in Federation: Increasing Trust and Interoperability in InCommon

January 10, 2018

Document Repository ID: TI.95.1

DOI: 10.26869/TI.95.1

Persistent URL: http://doi.org/10.26869/TI.95.1

Authors: Tom Barton, Brett Bieber, Ann West, Dean Woodbeck

Publication Date: January 10, 2018

Sponsor: Ann West, Associate Vice President, Trust and Identity, Internet2

Superseded documents: none

Proposed future review date: December 2019

Subject tags: InCommon Federation, Assurance, CTAB, Baseline Expectations, Trust

Table of Contents

A set of common expectations will provide a baseline for trust, collaboration, and ensure value to research and education.

Executive Summary

The InCommon community has adopted the Baseline Expectations for Trust in Federation after a year-long collaborative process. Led by the InCommon Assurance Advisory Committee (now known as the Community Trust and Assurance Board), the community determined that a set of common expectations that all Participants meet would provide a baseline for trust, make collaboration more predictable, and ensure that the InCommon Federation's strategic value to research and education continues to grow.

The InCommon Federation has become an infrastructure that campuses and services rely on for academic collaborations. To be effective, federated logins need to be trusted by service providers, service providers need to be trusted to properly protect personal information they receive, and all parts of the federation system need to operate in a manner that makes it as easy as possible for users to access the services they need. It breaks down when some InCommon Participants don't meet these expectations.

The Baseline Expectations for Trust in Federation are comprised of three brief sets of statements that embody what is required to make federation trustworthy and usable. Each is aimed at the major operational units in the Federation: Identity Provider Operators (IdP), Service Provider Operators (SP), and the Federation Operator. For example, a key expectation of IdPs and SPs is to maintain accurate and complete Federation metadata. The community has also developed a maintenance and implementation plan, including creating procedures and tools to help InCommon Participants meet the expectations.

When InCommon Participants rely on federation, they are partnering with other organizations to do something that they otherwise would do for themselves or forgo altogether.

Background and Strategic Direction

When InCommon Participants rely on federation, they are partnering with other organizations to do something that they otherwise would do for themselves or forgo altogether. Because of this interdependency, they rely on each other to mutually support a level of practice. For example, a fundamental expectation is that Participants provide authoritative and accurate attribute assertions to other Participants. Those receiving an attribute assertion must protect it and respect any privacy constraints placed on it by the source of that information or the community as supported by Federation.

To enable some level of trust to support this interdependency, the InCommon community has identified Baseline Expectations for Trust in Federation, including separate requirements for the operators of Identity Providers, Service Providers and the Federation operator. Each of these stakeholders must at minimum adhere to these Expectations for the systems they support. Over time, the InCommon community will increase the requirements of Baseline Expectations to reflect strategic value to the Participants, and each stakeholder will be expected to support them within a community-specified period of time.

Current Community Support for Operational Trust

Since the creation of the InCommon Federation in 2004, the POP - Participant Operational Practices - has formed the basis for trust. Participants complete a template describing their operational details and publish a web page with that information. This provides a public document that others can use to verify security practices, credentialing processes, and other relevant information.

That approach has become increasingly cumbersome as the InCommon Federation has expanded. The POP takes significant time to complete and is only human readable. A federation approaching 1,000 participants has roughly as many POPs as participants. In addition, these documents exist in various non-standard formats. In short, the POP approach neither scales and nor ensures consistent approaches to practices across the Federation that will need to change over time.

How, then, to address the need for trust among a large number of organizations in a reasonable and scalable way? The answer adopted by the InCommon community in 2017 is Baseline Expectations for Trust in

Federation.[1] When all InCommon Participants adopt these expectations, they will provide a baseline for trust. Participants can expect that all transactions with Federation partners will meet this level of trust. InCommon, as the Federation operator, and the InCommon Community Trust and Advisory Board (CTAB), comprised of community members, will implement a number of processes to support Participants in meeting these expectations. InCommon Operations, for example, will provide each entity with periodic metadata health checks, and the CTAB will guide the development of a community process for interpreting the practices.

Development of the Baseline Expectations

Baseline Expectations for Trust in Federation are the result of a year-long iterative process of assessment and feedback, initiated by the InCommon Assurance Advisory Committee (AAC) (which has since been reconstituted as the Community Trust and Advisory Board or CTAB). Early steps produced a strawman and a gap analysis, with feedback rolled into further updates to the strawman. In the culminating step, an open consultation invited federation-involved people around the world to give their feedback.[2] That step produced some refinement to language but no substantive change to the expectations, providing confidence that they are a reasonable expression of where the community believes that baseline must be at this time.

During the consultation process, the AAC worked to educate the community and seek feedback on the draft,[3] submitting a final document to the InCommon Steering Committee, which approved it in December 2016. Since then, the AAC has worked in coordination with InCommon Operations on timeline for implementation and maintenance processes to ensure ongoing development and support of the Baseline Expectations.

---

[1] See the core Baseline Practices document on the wiki.
[2] Background on the consultation is on the wiki.
[3] See Appendix A for a list.

Implementing the Program

The goal of the program is to enable the community to set expectations for itself, to evolve those expectations for the purposes of increasing trust and interoperability over time, and to enable community-driven communication, transparency, and action when a Participant is not living up to Baseline Expectations for Trust in Federation. There are three primary activities in this InCommon Operations will support the CTAB in the dispute, engagement, and transparency-related processes and provide periodic health checks to Participants on the content of their Federation Metadata.

- Identity Provider Operators, Service Provider Operators, and InCommon Operations are required to meet or exceed the simple statements in the relevant sections of Baseline Expectations for Trust in Federation.
- Going forward, the community at-large represented by the Assurance Advisory Committee (now the Community Trust and Assurance Board or CTAB) will evolve Baseline Expectations for Trust in Federation over time, engage the community on providing clarity around the program and expectations, and resolve complaints from participants about lack of adherence.

Identity and Service Provider Operator Practices

Basically, these statements amount to an “eat your own dog food” expectation. If you don’t, why should others trust you?

Both Identity Provider Operators and Service Provider Operators have these responsibilities:

- Ensure they have applied generally accepted security practices to their entities
- Ensure that all Federation metadata is accurate and complete
- Ensure the required metadata elements are complete: technical, administrative, and security contacts, metadata user information (MDUI), and privacy policy

In addition, Identity Provider Operators must:

- Operate with with organizational-level authority (your organization did this when you signed the InCommon Participation agreement)

- Trust their IdP enough to use it across the organization's own systems

Service Provider Operators also must:

- Reasonably secure information and maintain user privacy
- Not share information with third parties without permission

Community Implementation and Processes

The community at-large, represented by the Community Trust and Assurance Board (CTAB), plays a critical role in ensuring the program is implementable, understandable, and of value. The CTAB sets up community processes for providing guidance, evolving the program, and resolving disputes between community members.

Community Consensus Process for Interpretation - Baseline Expectations for Trust in Federation contain requirements that are expressed at a high level and may need interpretation to determine how they apply to specific operational circumstances.[4] This section describes how the community develops guidance for how to interpret these statements.[5] Results of this process will inform the next iteration of Baseline Expectations for Trust in Federation.

Community Dispute Resolution Process - This process is used to address concerns that may arise about some aspect of an entity's operation from the perspective of meeting Baseline Expectations for Trust in Federation. Dispute resolution proceeds by stages, using an informal and lightweight method at first, and progressing to further formality and rigor only if needed.

[4] See the consultation process on the wiki.
[5] See the implementation and maintenance document on the Baseline Expectations wiki.

InCommon Federation Operator Responsibilities

InCommon Operation Practices

Similar to Identity Provider Operators and Service Provider Operators, InCommon Operations also has a set of responsibilities highlighted in Baseline Expectations for Trust in Federation:

1. Focus on trustworthiness of their Federation as a primary objective
2. Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions
3. Internationally-agreed frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted
4. Work with other Federation Operators to help ensure that each Federation's operational practices suitably promotes the realization of baseline expectations, as above, by all actors in all Federations

Supporting CTAB

In the work concerning the dispute, engagement, and transparency-related processes; Internet2 will provide staff facilitation, publishing, and web support, and related process support for the group.

Providing information on Health of Federation Metadata

Many of the expectations for IdP operators and SP operators involve maintaining accurate and complete Federation metadata. Metadata can be thought of as the trust registry for the Federation. It is the information the enables the trusted and security exchange among participants that makes federation - and access - happen. The expectations specify certain elements that must appear in metadata.

As a Federation Operator adhering to Baseline Expectations for Trust in Federation, InCommon will implement health checks of metadata and distribute the results to the individual Participants. This will help ensure each Participant's federation metadata is complete and accurate.

InCommon Participation Agreement and FOPP Changes

Adoption of the Baseline Expectations for Trust in Federation will require changes to the InCommon Federation Operating Policies and Practices (FOPP)[6] and InCommon Participation Agreement.[7]

The changes to the FOPP and Participation Agreement include removing the POP requirement, inserting language about adhering to Baseline Expectations for Trust in Federation, and updating the dispute resolution process. It also includes changing the name of the InCommon Assurance Advisory Committee to the InCommon Community Trust and Assurance Board (CTAB).[8]

Given this significant requirement change of publishing practices to meeting or exceeding Baseline Expectations for Trust in Federation, InCommon Operations anticipates this will require a 90-day notice of the Participation Agreement prior to taking effect.

[6] https://incommon.org/docs/policies/incommonpop_20080208.html
[7] https://internet2.box.com/InCommon-Participatin-Agreemt
[8] The AAC was originally constituted to support the InCommon Assurance Program, but the group is generally interested in federation trust. The name change reflects a broader mission and the addition of Baseline Expectations to its purview.

Timeline for Adoption and Implementation

The Baseline Expectations for Trust in Federation and the Implementation and Maintenance Plan were developed by the AAC, submitted to the community for a consultation period, revised, and then approved by the InCommon Steering Committee.

During 2018, communications and outreach will focus on adoption and implementation.[9]

- Early 2018 - broad communication and review of changes to the InCommon Participation Agreement
- First half of 2018
  - Create Health Check tools to provide participants with information specific to the metadata of their entities
  - Begin community consensus process for interpreting Baseline Expectations for Trust in Federation
  - Begin operationalizing community-led dispute resolution process
- Throughout 2018
  - Develop documentation and support materials to explain the Baseline Expectations for Trust in Federation and processes to the community
  - Webinars and sessions at appropriate meetings
  - Regular communications about the program

[9] This wiki page has a detailed view of the timeline.

Conclusion

The InCommon Participant community includes roughly 950 organizations that have deployed 500 Identity Providers and more than 4,000 services in the Federation. The community is also connected through GÉANT's eduGAIN to international services and collaborators. While these numbers point to a growing trust infrastructure, the scale presents clear risks.

Over time, increasing a Participant's value will be directly tied to evolving their practices as well as those of the Federation Operator to meet new requirements. This requires consistent change management across the Federation (and ultimately its partners around the world). It also requires a way for Participants to have input into this evolution, InCommon Operations to support it with tools and processes in place, and a scalable way for the community to manage this change with their partners.

Baseline Expectations for Trust in Federation defines a first round of the practices and establishes the first communication and definition (and transparency) processes to manage ongoing change.

Appendix A – Community Outreach

1. Consultation on Baseline Expectations for Trust in Federation opens - July 6, 2016
2. Community webinar: Baseline Expectations for Trust in Federation, July 6, 2016
3. Community webinar: Baseline Expectations – Last Call for Comments, Aug. 3, 2016
4. Final Baseline Expectations document released - September 30, 2016
5. Community webinar: Baseline Expectations and their Implementation, Oct 5, 2016
6. Community webinar: Baseline Expectations Implementation - June 7, 2017
7. Consultation opens: Baseline Expectations Implementation and Maintenance Plan - June 22, 2017
8. IAM Online webinar: Baseline Expectations Implementation and Maintenance - July 19, 2017
9. Community webinar: Refocusing Community Guidance of InCommon's Trust Programs: Baseline and Bronze - Oct 4, 2017

Conference Sessions and BOFs

1. 2016 Internet2 Technology Exchange, September 2016
   Strengthening Community Trust: New InCommon Baseline Practices (program session)
   http://meetings.internet2.edu/2016-technology-exchange/detail/10004396/

2. 2016 Internet2 Global Summit, May 2016
   InCommon Baseline Practices BoF https://meetings.internet2.edu/2016-global-summit/detail/10004161/

3. 2015 Internet2 Technology Exchange, October 2015
   POP Killers Anonymous (Advance CAMP Unconference Session led by Jacob Farmer)
   https://docs.google.com/document/d/1dYYS74HABG0mnpqa5fnSB6t70kjknQw8viiyIZYm7wQ/edit