Transitioning the Community to InCommon Baseline Expectations for Trust in Federation

Document Repository ID: TI.113.1
Persistent URL: http://doi.org/10.26869/TI.113.1
Authors: InCommon Operations and
InCommon Community Trust and Assurance Board
Publication Date: October 2018
Sponsor: Internet2 Trust and Identity Executive Management

October 8, 2018

This document describes InCommon Federation Operations' plan, in collaboration with the InCommon Community Trust and Assurance Board, to transition participants to meeting the metadata elements of Baseline Expectations of Trust in Federation (BE).

Executive Summary

In January 2018, the InCommon community adopted the Baseline Expectations for Trust in Federation, a set of common expectations that all participants must meet. The goals of the change are to 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. BE replaced the previous trust-through-transparency approach ("publish your practices for your partner to review") with a set of requirements that will evolve over time. This momentous change occurred on June 15, 2018, when the new InCommon Participation Agreement went into effect, reflecting the new trust requirements.

The next step was determining the final adherence targets, risks to adoption, and transition plan to ensure the new policy was effective across the Federation. To ensure smooth and timely adoption of these Baseline Expectations, InCommon Operations conducted extensive outreach, contacting those organizations that had not met BE to understand the challenges with implementing the metadata requirements---the only requirement included in BE that the community can measure. Using information and ideas gleaned from this fact finding, InCommon

Operations and the Community Trust and Assurance Board (CTAB) developed a Transition Plan to complete adoption by December 14, 2018.

This plan concludes with using the recently approved Community Dispute Resolution Process to address matters that may arise from organizations unable to meet Baseline Expectations by the December deadline. It is worth noting that the final stage of the Dispute Resolution Process may include the removal of entity descriptors from the InCommon metadata which, if needed, would require an InCommon Steering Committee vote.

Background: What is Baseline Expectations?

In January 2018, the InCommon community adopted the Baseline Expectations for Trust in Federation, a set of common expectations that all participants meet, to 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 (ref: Baseline Expectations for Trust in Federation: Increasing Trust and Interoperability in InCommon). BE replaced the previous trust-through-transparency approach ("publish your practices for your partner to review") with a set of requirements that will evolve over time. This change momentous change occurred on June 15, 2018 when the new InCommon Participation Agreement, that reflected the new trust requirement, went into effect.

Adoption of Baseline Expectations

Providing complete information (or metadata) is the only aspect that the community can measure of the current BE specification. When we say an organization "meets BE," it means that it has provided contact aliases, logo URL, and privacy policy URL for each of its registered systems.

As of October 3, 2018, 70% of InCommon participating organizations have met the metadata requirements of Baseline Expectations. The following table provides additional statistics:

	Total Count	Count of meets BE	% of Completion
Participant Organizations	756	532	70%
Identity Providers	522	395	76%

Service Providers[1]	4,379	2,247	51%
All Entities (IdP + SP)	4,901	2,642	54%

Baseline Expectations for Trust in Federation relies on establishing and conducting related processes to promote increasing levels of trust. **While the Federation Operator will strive for 100% adherence, organizations will likely have local considerations and needs that may require them to maintain systems that do not meet BE. The Federation will be considered transitioned when 90% of the Service Providers and 95% of the Identity Providers have complete metadata as defined by BE.** Any production service that interacts with another organization's systems however must adhere to BE.

To reach this level of adoption in a timely fashion, InCommon Operations and CTAB identified the need for a Transition Plan to both incent participants to adopt and help them do so by providing education, shared best practices, and tools. To begin, we identified the risks and then conducted extensive outreach to understand barriers to adoption.

The Baseline Expectations Transition Plan

Risks Considered in the Transition Plan

InCommon Operations and CTAB considered several risks when planning for the adherence targets and process for getting all participants to meet BE:

Stakeholder Confidence in the Program: The need for BE was surfaced by research service providers who had grown wary of federating with identity providers that didn't have complete and accurate metadata. We risk losing the research community support for InCommon if we don't place a high priority on IdPs meeting BE.

Outdated/Inactive Entities: The Federation has been operational for over 14 years, and may include systems registered in the metadata that have no one supporting them. It's likely these will be removed due to lack of action and communication, after due process. However, if these systems are still in use, the Federation Operator will need to be vigilant at the time of removal for a quick rollback of changes, if needed.

[1] A few organizations have large numbers of SP's that have not met BE. Working closely with these organizations should substantially improve the adherence rate in the coming weeks.

Logo and Privacy URL: It may take time for participants to engage organizational stakeholders about the use of logos and privacy policies. The CTAB is promoting options in both of these areas that should not require significant delays or lengthy local negotiations.

InCommon Communication: The Federation's ability to connect with all participants, especially the sponsored partners, is limited. While these (typically) corporate organizations are participants in their own right, they tend to respond better to identity provider requests because of the customer relationship.

Delegated Site Admin Communication: There are service providers in the Federation that are operated by departments outside central IT. Evidence indicates that central IT site admins are, at times, having difficulty connecting with these delegated service provider operators.

Order of Focus: Not all systems registered in the InCommon metadata pose the same risk to others. For instance, several campuses have registered their own locally-scoped services that are not available to other participants' use. These should be addressed last in whatever process we identify. The process should consider the risk of various classes of registered systems and address them in turn from the highest to the lowest.

Timeframe: This is our first time rolling out a change of this magnitude and required response. Setting a target that's too aggressive may create a longer list for CTAB to review and force their hand to publish more on their docket than what's "reasonable." We need to provide enough time for migration and not too much time to start eroding our trust from key stakeholders. Furthermore, we want to set an expectation ongoing of consistent change management.

Developing the Plan: Community-Needs Discovery

Between late June and late August, InCommon contacted participants that had not met Baseline Expectations to understand why. We wanted to learn about the challenges to developing a reasonable and actionable transition plan that mitigated the risks mentioned above in a timely and community-friendly manner.

We sent targeted email messages to InCommon Site Administrators and InCommon Executives asking:

- How soon do you think your IdPs and SPs will meet the metadata expectations?
- What are your impediments to meeting the metadata expectations?
- What can InCommon do to help your process of meeting the metadata expectations?
- Would you like to speak with us about any of this?

The messages were staged over time for different sub-communities:

- **6/21/2018:** First message to the 223 organizations with IdPs that did not meet all metadata expectations.
- **7/5/2018:** First message to 30 hand-picked service providers that did not meet all metadata expectations.
- **7/10/2018:** Second message to the 178 organizations that still had IdPs that did not meet all metadata expectations.
- **8/2/2018:** First message to an additional 119 organizations with SPs that did not meet all metadata expectations.

The solicitations resulted in 39 email exchanges and 8 video conference interviews. In addition, we noted a significant number of metadata updates occurring within the first few days after emails were sent. This demonstrated that many organizations did the work to meet the metadata expectations without further interaction.

Themes and Observations from the Discovery

Several themes and observations became apparent during the interactions.

- The response rate to the emails was approximately 11%. In some cases, non-response was due to missing or incorrect contact addresses, for both Site Administrators and Executives --- underscoring the need for BE!
- Even when the addresses were correct, the person may not be engaged because they may:
    - Have left the organization.
    - Not be paying attention.
    - Not have background in identity federation to understand the importance.
    - Not believe they're authorized to act on behalf of their organization for the issue.
    - Be busy. Federation is not the contact person's only priority.
- Some contacts shared a concern that resolving the metadata expectations may affect the operation of their production systems. Education is needed to reassure these participants that nothing they change with regard to Baseline Expectations will break any systems or services.
- Upon receiving an email, a number of participants updated metadata to meet BE without responding to the message. The biggest unknown is set of participants that neither responded and nor took action to meet BE (just over 200).

- Nine organizations have 50+ entities not meeting BE, representing more than half of the total number of SPs not meeting BE. Seven of these organizations have expressed a desire for a tool that could assist with mass metadata updates.

Defining Key Transition Plan Actions

Informed by the data, the InCommon staff and CTAB identified December 14, 2018, as the deadline for meeting Baseline Expectations. We developed the following plan and set of activities to complete the transition:

1. Communicate and Educate

Timeframe: September/October 2018
Related Artifact: Baseline Expectations Communications Schedule

To continue raising awareness, we are expanding community communication to emphasize the importance of timing and necessary actions, including:

- Webinars, emails, and newsletter articles directed at both executive and administrative levels articulating the importance of the metadata expectations.
- Documentation describing how the metadata will be used and the benefits of meeting the expectations.
- Educational materials outlining the details for updating metadata as well as any potential impact of changing the metadata.
- Publicized “office” hours with technical staff answering questions and helping participants meet the expectations.

In addition, InCommon will continue to provide monthly health check reports as well as the “Lists of Entities in InCommon Metadata Aligned With Requirements of Baseline Expectations”.

2. Develop Process for Extensions

Timeframe: November 2018

As with most programs, there should be reasonable consideration for adherence extensions. The InCommon community will devise and publish a process for requesting extension for meeting BE.

3. Adherence Deadline

Time: December 14, 2018

Starting December 14, the InCommon staff will identify organizations that have not met Baseline Expectations and work with CTAB to begin the Community DIspute Resolution Process.

4. Community Dispute Resolution Process

Timeframe: January 2019

In January 2019, organizations with entity descriptors that have not met the metadata expectation or been granted an extension will be forwarded to the Community Dispute Resolution Process. Dispute resolution proceeds in escalating stages, starting with an informal and lightweight method, and progressing to further formality and rigor only when needed. *The result may include the removal of entity descriptors from the InCommon metadata, which will require an InCommon Steering Committee vote.*

The processes for maintaining the Baseline Expectations, including the Community Dispute Resolution Process, is located at The Baseline Expectations for Trust in Federation site.

Conclusion

The InCommon Baseline Expectations for Trust in Federation requires a tremendous effort for the community and for InCommon Operations. As of early October, 70% of the organizations do meet the new requirements, which is good news. After considering the risks and discovering adoption challenges, InCommon Operations and CTAB developed a transition plan to conduct further outreach and education and, likely as important, set a deadline for adherence. Those not meeting BE after December 14, 2018, will be submitted to the new Community Dispute Resolution Process. This effort represents a significant legal, technical, policy and process evolution on the part of the community and InCommon Operations and sets a foundation for increasing trust, security, and value over time.