InCommon Baseline Expectations: Designing How to Transition the Community

Repository ID: TI.120.1

Persistent URL: http://doi.org/10.26869/TI.120.1

Authors: Ann West, https://orcid.org/0000-0001-5484-6827

Sponsor: Internet2 Trust and Identity executive management

Note from December 2018:, This document is a description of the first phase of the project to transition the community to support Baseline Expectations for Trust in Federation. A summary of Phase 2 and resulting project approach can be found here: http://doi.org/10.26869/TI.113.1

June 1, 2018

InCommon Baseline Expectations: Designing How to Transition the Community

This document describes how the InCommon Federation Operator will work with CTAB to achieve the meeting of BE by the community scoped to the completion of InCommon metadata elements of Baseline Expectations of Trust in Federation. Not included in this process is the adherence of other BE components, which are under the jurisdiction of CTAB.

Target

Baseline Expectations for Trust in Federation relies on establishing and conducting related processes to support increasing levels of trust. Organizations will have local considerations and needs that may require them to maintain systems that do not meet BE. While the Federation Operator will strive for 100% adherence, 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.

Risks in Designing a Transition Plan

It's highly likely that specific members of the InCommon Community were expecting that the federation will meet BE on June 15, 2018 which given the magnitude of the change, is not feasible. There are several risks that the team must consider when planning for the adherence targets and process for getting all to meet BE:

Stakeholder Confidence in the Program: The need for BE was surfaced by research service providers tired of federating with identity providers that didn't have complete and accurate metadata. We risk losing the research SP support of 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Outdated/Inactive Entities: The Federation has been operational for over 14 years, and there are likely systems registered in the metadata that have no one supporting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 roll back of changes, if needed.

Logo and Privacy URL: Two components, the logo and privacy notice, may take time for the participants to engage organizational stakeholders about their use. The CTAB is promoting options for organizations to use that they believe don't require significant activity.

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 an identity provider, as opposed to federation, 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 not located in IT.

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 participants and address them in turn from the highest to the lowest.

Timeframe: This is our first time rolling out a change to the participants of this magnitude and required response. We are unsure how long this will take and what the local issues are with meeting BE. 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." It could also make InCommon look "insensitive and out of touch" with local constraints. 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.

Contact Priority in Order of Risk/Opportunity

To address order of focus, stakeholder confidence, and communication risks above, below is the priority order of audiences to be engaged with transition-related activities.

1. **Organizations with Governance and Advisory Representatives guiding Trust and Identity.** While these organizations and their lack of adherence do not introduce more risk for transactional trust, they introduce governance and program integrity issues by not meeting BE.
2. **InCommon Level 1 Higher Education Institutions (Research-focused)**
3. **Organizations with IdPs running Shibboleth v.2 with missing baseline elements in metadata.** While running outdated versions of the software is not currently a specified BE issue, it is expected that CTAB will remedy this quickly. We can let orgs know about this likely next step.
4. **Research and Scholarship Identity and Service Providers**

5. **Other Identity Providers.** Identity Providers introduce the most risk into the federation because they perform the identification and authentication and house an attribute source for the federated relationship.
6. **Research organizations offering InCommon-wide Services**
7. **Sponsored Partners (Corporate and Non-profit) offering InCommon-wide service providers.**
8. **Sponsored Partners and others offering bilateral services.** A number of companies create customer-specific federated instances. These pose risk only to that one customer.
9. **Organization-scoped Systems** that are available only to the organization's users and not to another participant.

Plan Overview

While BE goes into effect on June 15, 2018 with the end of the 90-day legal notice, we will need to give the community a transition period to meet it. The first phase of the transition focuses on information gathering to inform the final dates of implementation and it places heavy emphasis on getting identity providers and organizations with governance representatives meeting Baseline Expectations. The second phase provides the hard-date incentives and finality of enforcement.

Phase 1: Impact of BE, Transition Plan Development and Transparency of Those Meeting BE

The first 3-month phase includes:

- Aligning expectations around the June 15, 2018 effective date. The first step is to communication to participants about intentions for phase 1 and 2 and that there will be a final effective date to drive discussion.
- Engaging organizations not meeting BE and determining issues with adherence. The outcome of this activity should be an anonymized report of local obstacles for IdPs and SPs that can be published to educate participants on their partners' issues.
- Developing an informed transition plan. This plan should include support needed and strategy for providing the support, methodology for communicating the need for a local delay and related plan for adherence, and final dates for enforcement.

In addition, special emphasis will be placed on engaging governance and HE IdPs.

Messages to be included in Organizational Engagements

This is primarily a fact-finding, education as well as a warning phase. We want to remain positive, listen and help, stress the benefits, and make it clear we're using their feedback to develop a final plan. However, we also want to provide a clear understanding of final enforcement. Below is rough list of questions of what should be conveyed/tracked/asked:

- (Is the contact information that we have accurate? Whom did you end up talking/communicating with? Is there an AI for SM to follow up on something?)
- Once the contact is identified:

- Do you know what BE is? Have you seen the messages?
  - If not, how can we help you get connected in?
  - (May have to provide a short explanation and set of links for them)
- We've noticed that your org's metadata doesn't **meet** (don't use comply or a security term) BE.
  - It looks like you have X IdPs and/or X Sps that don't meet BE. They are (....)
  - Are there questions we can answer for you?
  - Are there things that InCommon or the Community Trust and Assurance Board can provide to help you? If yes, what are they?
- What is your timeframe for meeting BE?
- (If applicable): We also noticed you run a very old version of the Shibboleth IdP as published here. We believe the Community Trust and Assurance Board will shortly determine that maintaining current federating software will be in scope for the third IdP BE "Generally-accepted security practices are applied to the IdP."
  - What is your timeframe for upgrading?
  - What kind of further help/training do you need to help with your upgrade?
    - Do you know there's release of Shibboleth IdP with easy installation and a UI available?
- Do you federate with other InCommon partners?
  - It would really help if you could contact them and make sure they are working on it and remain good InCommon Federation partners. Let us know if you need anything.
  - BTW, we will start publishing a list of organizations that do and don't meet BE to help you starting in July and August. We'll announce the BE enforcement date in early September too.

Phase 1 Timeframe: June 4 - September 7

June 4 - 15

- Set up contact process
  - Identify 2 individuals called BEEs (Baseline Expectation Engagers) to contact organizations. (Done)
  - Develop list of governance and IdPs to push. Develop list of SPs to investigate/push. (Done)
  - Develop tracking/logging mechanism and process for contacts.
    - The organizations will likely change nightly, so the contact list will need to have a diff shared with the BEEs so they don't contact an org that has updated their metadata. (Done)
  - Develop script/talking points for contacts. (Done)
  - **June 15, 2018** – Email participants. Baseline Expectations go into effect. Remind Participants that Federation Manager now warns against submitting metadata that do not meet expectations. Notify community of phased plan and that *we will announce enforcement dates in September* once we better understand adoption

challenges. Include dates when we will begin publishing orgs that meet and don't meet BE. (Done)

June 18 - August 10

- Continue monthly health checks and report outs to the community. (underway)
- Contact organizations. (underway)
- Develop report from compiled list of local concerns from contacts. (first draft complete)
- Develop informed transition plan.
- **July 27, 2018** - Publish List of Orgs that Meet BE.

August 13 - 24

- Vet transition plan.
    - Given the volume of communication about BE, it is expected that we can shorten this review time to two weeks.
- Publish report of local concerns to aid in educating the community about adoption issues and provide rationale for transition plan.
- Continue monthly health checks and report outs to the community.

August 27 - September 7

- **August 27, 2018** - Publish List of Orgs that Do Not Meet BE to aid in transition.
- Develop Phase 2 of the transition plan and related dates to reflect local constraints.
- Review with InCommon's Community Trust and Assurance Board and inform the Steering Committee

Phase 2: Formal Transition Plan Developed and Implemented

Phase 2 focuses on implementing the transition plan developed in Phase 1. A final analysis will be conducted and used to develop deadlines for the community and accompanying impacts and related processes for those organizations that don't.

Note from December 2018: This document is a description of the first phase of the project to transition the community to support BE. A summary of Phase 2 and resulting project approach can be found here: http://doi.org/10.26869/TI.113.1