Operationalizing Baseline Expectations Working Group - Summary Report

Introduction

The implementation of Baseline Expectations (BEs) by the InCommon Identity Federation marked a milestone in the creation of trust and assurance within the federation. For the first time, organizations within InCommon were able and expected to self-assert trustworthy operational practices for their federated entities, both identity providers (IdPs) and Service Providers (SPs). Nonetheless, assertions of this sort, however accurate and well-meaning when they are made, are prone to become stale via a number of mechanisms:

- Practices that are trustworthy at one time become deprecated as technology progresses. For example, ciphers that are considered secure today may be considered insecure next year.
- Organizations evolve and shift their practices over time. For example, work that was done on premises may be outsourced in order to save costs.
- Institutional knowledge as to how particular practices match the assertion or even that such assertions have been made may be lost due to personnel turnover.

Consequently, the InCommon Federation Community Trust and Assurance Board (CTAB) has recognized that InCommon has an interest in monitoring the degree to which the self-assertion of BEs drift over time and in aiding organizations in maintaining the accuracy of their assertions. However, the methodologies and apparatus for querying organizations and measuring assertions has to be developed *in toto*. As a result, CTAB created the Operationalizing Baseline Expectations Working Group (OBEWG) to consult with InCommon's Operations in developing guidelines and general methodologies for monitoring BE assertions for InCommon participants. This document and an accompanying spreadsheet summarize the working group's findings.

Participation

The following people (in no particular order), all members of CTAB and/or of the InCommon Operations team participated in the OBEWG:

- David Bantz
- Albert Wu
- Tom Barton
- Johnny Lasker
- Warren Anderson
- Kyle Lewis
- Richard Frovarp

- Harsh P Biscuitwala
- Andy Morgan
- Derek Eiler

Methodology

The OBEWG met biweekly for several months. The discussion of the group can be broadly divided into three categories. The first was establishing guiding principles which inform what it means to operationalize BEs. The bulk of the remainder of this document is devoted to describing these principles. The second was a discussion of the assertions of the BEs in the context of these principles, with attention to how each assertion might be tested, what the expected result of the test would be, the frequency of testing, etc. The OBEWG's conclusions on operationalizing each of the BEs can be found in the spreadsheet here. Finally, implementation details of operationalizing BEs were discussed briefly, however, ultimately it was felt that InCommon Operations staff would be in the best position to determine how the procedures described in the spreadsheet are to be implemented.

Principles

During the initial meetings of the OBEWG, the bulk of the discussion was devoted to identifying key principles related to operationalizing BEs. These principles would then guide the specific tests of BE assertions used to operationalize BEs.

Communication

A central feature of the day-to-day work of operationalizing BEs will be the ability for InCommon operations staff to communicate with representatives of InCommon participants about BEs. Toward this end, it will be important for InCommon to have current contact information for participant representatives such as the InCommon Executive for the participant and their Site Administrator, which is currently not always the case. A substantial part of operationalizing BEs will involve mechanisms to gather and maintain this contact information.

Authority to Assert

It was recognized early that Baseline expectations assertions require a wide range of knowledge and authority to assert. For example, the *IdP is operated with organizational-level authority (IdP1)* requires that organizational-level authority to assert. This is the level of authority that, for example, the InCommon Executive for the Participant, who has signing authority for the Participation Agreement has. On the other hand, the *IdP's published metadata includes a current errorURL (IdP5)* is an assertion that participant Site Administrators are more likely to be able to make with certainty. Operationalization of BEs, therefore, should be a process which involves both of these roles for a participating organization.

Timeliness

The OBEWG recognizes a tension between keeping assertions current and having a process that is manageable for both InCommon Operations staff and for participating organizations. For this reason, it was determined that monitoring of assertions should follow an annual or semi-annual cadence. Staggering of monitoring for different expectations may be an option in avoiding a yearly “crunch” of assertions.

Simplicity

The OBEWG acknowledges that adding ongoing monitoring of assertions in BEs places an additional burden on both InCommon participants and InCommon staff. As such, to the degree possible, simplifying assertion to minimize burdens should be a primary goal of operationalizing BEs. As an example, since the InCommon Federation Manager software already exists as a platform to allow InCommon participants to interoperate with the InCommon federation, extensions to that platform that allow reports of assertion checks to be communicated to participants and that allow participants to re-assert their entities would be preferable to building new infrastructure. Likewise, for cases where testing of assertions would prove difficult or impossible, a simple email communication reasserting that a participant’s entities are still in compliance with BEs may be all that is required.

Cooperation

There was a strong emphasis on creating a cooperative atmosphere between participants and the InCommon federation within the OBEWG. By creating strong communications between participants and InCommon staff throughout this process, the OBEWG believe that most BE assertion lapses can be handled by simply informing participants. Because some assertions require technical work from participants, sufficient time to address lapses of those assertions should be given, and an acknowledgement of the lapse and statement of intent would be sufficient as a first response. In some cases, further information or help in mitigating lapses might be required, and InCommon Operations staff should be able and willing to provide guidance to participants. Only after repeated attempts to communicate issues and help resolve them would the dispute resolution process be invoked.

Conclusion

The community recognizes that operationalizing BEs represents a significant expansion in both the InCommon Federations role as a federation operator and in the responsibilities of participants. This, in turn, requires careful consideration of what it means to operationalize BEs and of how to implement the required changes. However, it is our belief that the result is a commensurate expansion of trust and assurance within the federation that benefits all parties.