Processes to Maintain Baseline Expectations by InCommon and its Members

December 13, 2018

Repository ID: TI.105.2

Authors:

Tom Barton https://orcid.org/0000-0003-1878-3448

and the InCommon Community Trust and Assurance Board (CTAB)

Sponsor: InCommon Community Trust and Assurance Board (CTAB)

Superseded documents: TI.105.1

Proposed future review date: TBD

Subject tags: InCommon, federation, assurance, trust, framework

I. Introduction

In recognition of the importance of the on-going and gradually increasing level of trustworthiness needed in federation transactions, InCommon Participants have established Baseline Expectations as one means to define what they expect of each other, and of InCommon Operations. As a baseline, federation members must meet or exceed this level of trustworthiness. The processes defined below are the means by which InCommon and InCommon Participants can hold each other accountable for meeting these expectations, and to establish rough consensus on how these expectations should be observed in specific operational circumstances.

The processes defined below fall into several categories. Some are mostly automated processes undertaken by InCommon that are designed to help Participants keep their federation metadata aligned with Baseline Expectations. Another defines how the Participant community can establish their consensus on how Baseline Expectations should be observed in specific operational circumstances, e.g., whether security practice XYZ meets the expectation that “Generally-accepted security practices are applied” to an IdP or SP. There is also a process by which a specific Participant’s practice can be assessed against Baseline Expectations and any needed mitigation agreed by peers.

These processes all aim to help Participants understand when and how they deviate from meeting Baseline Expectations and provide help to get them back on track. But in the worst case, when a federation entity is not meeting expectations and no remedial course of action is available, the entity is altered or removed from federation metadata as recommended by the InCommon Community Trust and Assurance Board (CTAB) upon approval being given by the InCommon Steering Committee under authority given it by the Participation Agreement (PA) and in accord with InCommon's Federation Operating Policies and Practices (FOPP).

The overall result of operating these processes is that all InCommon entities meet Baseline Expectations - not 100% perfectly 100% of the time, but variances are diligently identified and corrected in a reasonable period of time.

2. Community Consensus Process for Interpreting Baseline Expectations and Acceptable Operations

Baseline Expectations contain requirements that are expressed at a high level and may need interpretation to determine how they apply to specific operational circumstances. For information on how the community develops guidance for interpreting these statements,

> *Please refer to http://doi.org/10.26869/TI.107.1.*

3. Community Dispute Resolution Process

> *Please refer to http://doi.org/10.26869/TI.118.1 for the most up-to-date version of this process.*

4. On-Going Federation Operational Processes

As a Federation Operator adhering to Baseline Expectations, InCommon implements several processes to ensure that Participants' federation metadata is accurate. These help address the Baseline Expectation of Identity Providers (IdPs) and of Service Providers (SPs) that "Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL", and also partially fulfill the Baseline Expectations of "Focus on trustworthiness of their Federation as a primary objective and be transparent about such efforts", and "Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions". For more information on this process, see Appendix A.

Process to Notify InCommon Community of Intent to Alter Participant Metadata

This process is followed when InCommon is required to remove or alter Participants' metadata as the last step in two of the processes described in this document, as noted below. Changes to metadata necessitated by response to a security incident are handled through the InCommon Security Incident Handling Framework.

InCommon will use this process under the following circumstances as a last attempt to notify a Participant organization of an identity provider or service provider that does not meet Baseline Expectations and that the entity will be altered or removed from InCommon metadata:

1. InCommon metadata checking, as described in Appendix A, has failed to elicit a required correction by the Participant to its entity metadata.
2. The InCommon Steering Committee, upon accepting the recommendation of the CTAB, given after unsuccessfully exhausting all avenues of collaborative resolution of a Baseline Expectations concern raised by a federation member, authorizes InCommon to take this step towards altering federation metadata to remove or alter the identified entity.

Process

1. InCommon updates the CTAB's public docket (in circumstance #2) or creates a public docket entry (in circumstance #1) describing why this entity has arrived at this process, e.g., non-responsive to Error URL being corrected.
2. The VP or AVP for Trust & Identity personally notifies the Executive Contact at the Participant to notify them of the status of their identity or service provider under concern.
3. The public docket is published along with Participant contact information to give other parties the opportunity to contact the Participant in hopes of precipitating a reasonable resolution of the matter, and functions as *Last Call* to the concerned Participant before their entity's metadata is removed or altered.
4. If the issue has not been addressed within 30 days of publication, the entity will be removed or altered as authorized.

InCommon will ensure that appropriate controls are in place to mitigate the possibility of an unauthorized reinstatement of an entity altered or removed by this process.

5. Reinstatement

An entity that was removed or altered per the above process can be reinstated to InCommon metadata as follows.

1. If the entity was altered or removed by the processes defined in Appendix A, then
    a. Either the Participant's Technical or Executive Contact or a Site Administrator may make a request to InCommon to reinstate the entity to its federation metadata. The request must contain a copy of the entity metadata proposed to be reinstated.
    b. InCommon staff will determine whether or not the entity metadata submitted with the request meets the criteria of the processes defined in Appendix A and reinstates the metadata if it does. Either way, this outcome will be reported on the Baseline Expectations Website.
2. If the entity was altered or removed upon the recommendation of the CTAB as the final outcome of the Community Dispute Resolution Process, then
    a. The Participant's Executive Contact must make a request to InCommon to reinstate the entity to its metadata. The request must contain a description of the mitigation that was implemented to address the concern that led to its entity being altered or removed.
    b. InCommon will refer the request to the CTAB, who will review the mitigation and determine whether or not it results in the entity meeting Baseline Expectations.
    c. The CTAB will communicate its decision to InCommon staff, who will reinstate if that is the CTAB's recommendation. Either way, this outcome will be reported on the Baseline Expectations Website.

6. Publication of the Operation of These Maintenance Processes

A Baseline Expectations website makes all Baseline Expectations related information publicly available. The following materials shall be published:

- The Baseline Expectations themselves. This is the page linked in the FOPP and PA rather than inserting Baseline Expectations-specific wording into those agreements. It is referred to appropriately from the incommon.org website.
- Summary of the Baseline Expectations maintenance processes (this document) incorporating links to related Baseline Expectations website pages.
- Metrics on the "Maintain Accuracy of Contact Info, MDUI, Error and Privacy URLs in Metadata" process in Appendix A, such as date of completion of last cycle, date of next cycle, stats on # updated addresses/cycle, # entities moved to "Process to Notify InCommon Community of Intent to Remove Entities from Metadata"/cycle.
- Metrics on the "Process to Notify InCommon Community of Intent to Alter Participant Metadata", such as when which entities were put on notice, ultimate disposition of those, date of next cycle.
- Proposed and final statements of acceptable or unacceptable operations arising from the "Community Consensus Process for Interpreting Baseline Expectations and Acceptable Operations" process, with dates.
- Suggestions for future changes to the Baseline Expectations themselves.

- Publically viewable activity of the “Community Dispute Resolution Process”, including summary of the dispute/concern, dates of entry into Second and Third Stages, resolution and either date of remediation or date of recommendation to the Steering Committee to alter or remove the entity from federation metadata, Steering Committee decision and date.

Appendices

Appendix A: Maintain Accuracy of Contact Info, MDUI, Error and Privacy URLs in Metadata

Following is a progression of steps taken to validate currency of each entity’s contact info, MDUI information, Error and Privacy URLs in federation metadata. Steps 3 onwards are only taken if preceding ones do not conclude satisfactorily. Groups of entities may be put on different cycles to manage the effort required.

1. Send email to each email contact with an embedded code so that replying to the email will automatically update an associated database, eg, as commonly supported by listserv software. Do this every 6 months.
2. Monitor MDUI information, Error and Privacy URLs for an acceptable response and if any fail continuously for 2 weeks, re-notify the associated contacts.
3. Run a report on the database after the notification or reply has expired (2 weeks) and send a follow up to non-respondents.
4. Run another report after 2 weeks and send a follow up to Executive Contact or a senior IT manager (which is not kept in metadata) of non-respondent Participants.
5. Send 2nd notice to Executive Contact or senior IT manager if no answer after 2 weeks.
6. Phone call to Executive Contact or senior IT manager. Repeat 3 tries over 2 weeks if necessary.
7. Use Process to Notify InCommon Community of Intent to Alter Participant Metadata.
    a. Notices due to unverified contact information or unacceptable MDUI information, Error or Privacy URLs should state clearly that (1) InCommon is using this means as a last resort to contact someone at Participant to resolve the issue, which is the desired outcome, (2) if no contact can be made after 1 month, InCommon will have no choice but to remove or alter Participant’s $Entity metadata on $Date, and (3) the specific basis in the FOPP or PA for that action, if no contact is made.

Appendix B: Change Log for this Document

Version	**Date**	**Change**
Version 2, TI.105.2	Published Dec. 2018	Dispute Resolution and Consensus Process descriptions were moved to their own documents; minor editorial changes.
Version 1, TI.105.1 http://doi.org/10.26869/TI.105.1	Published Sept. 2017	Initial version