Baseline Expectations Implementation

IAM Online, July 19, 2017

Brett Bieber, University of Nebraska-Lincoln and Chair, InCommon Assurance Advisory Committee

Tom Barton, University of Chicago and Internet2
How did we get here?
InCommon Assurance Program, Bronze/Silver Profiles

Why not Bronze or Silver?
1 Silver (did not renew), 5 Bronze (no equivalent in NIST 800-63-3)

POP Killers Anonymous! (Participant Operational Practices)

How can federation members be accepted as “trustworthy”?

Can assurance of consistent practices across Participants increase value for all?
What’s the solution?
Identity Provider (IdP) Baseline Expectations

1. The IdP is operated with organizational-level authority
2. The IdP is trusted enough to be used to access the organization’s own systems
3. Generally-accepted security practices are applied to the IdP
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL
1. Controls are in place to reasonably secure information and maintain user privacy.
2. Information received from IdPs is not shared with third parties without permission and is stored only when necessary for SP’s purpose.
3. Generally-accepted security practices are applied to the SP.
4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL.
5. Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly.
Fed Operations Baseline Expectations

1. Focus on trustworthiness of their Federation as a primary objective and be transparent about such efforts
2. Generally-accepted security practices are applied to the Federation’s operational systems
3. Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions
4. Frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted
5. Work with relevant Federation Operators to promote realization of baseline expectations
What have we done?
Phase 1
Conception and Initiation
2015—2016

Conception and Initiation
Five (un)conference sessions
Four webinars
Community Consultation Period

Finalization
AAC vote, approval and recommendation to InCommon Steering
InCommon Steering Committee vote & approval
Phase 2

Implementation Plan
Development and Finalization
2017—2018

Draft Community Consensus
Identify Automatic Monitoring Processes
Draft Community Dispute Resolution Process
Draft Process to Reinstate Entities Altered or Removed
Draft changes to Participation Agreement (PA) and Federation Operating Practices and Procedures (FOPP)
Phase 3
Implementation and Operationalization 2018 —

Review period for change to Participation Agreement

InCommon Operations begins automated monitoring

Community Dispute Resolution Process Available

Community Consensus Process Available
A closer look
InCommon automated monitoring

Routinely check metadata and notify members of issues

Complete and functioning contact info
Elements supporting good federated user experience
Progressively escalate notifications as needed
  Automation
  Executive contact
  Publication
Unilateral correction in non-responsive cases
Community dispute resolution process

Clear process, roles & responsibilities for resolving a Baseline issue affecting a member

1. A concerned member brings a Baseline Expectations issue to attention of another member, or asks InCommon to do so.
2. If needed, AAC + Community Review Board assesses and accepts resolution plan.
3. If needed, AAC recommends unilateral correction to InCommon Steering.
Community consensus process

Develop community guidance on Baseline Expectations

A member unsure of how Baseline applies to some aspect of their environment raises the question in a public venue.

AAC facilitates discussion and articulates the outcome:
- Publish Baseline guidance
- Record prospective change to future rev of Baseline
- Recommend another course
Changes to PA and FOPP

Replace ~10 year old Baseline-like terms in PA
Remove *Participant Operating Practices* requirement from PA
Add InCommon’s Baseline operational processes to FOPP
Connect with PA’s Dispute Resolution Procedures

Make Baseline an integral part of the InCommon Federation
How will this work?

A few big steps and some little steps!
Big Step 1

*Improve reliability and value of the federation by cleaning up metadata*

- Complete and accurate contact information
- Elements supporting good federated user experience
- InCommon monitoring to show Participants what’s missing in their metadata and help them to correct it
Big Steps 2+

Mature the federation by establishing process for broad stepwise change

One step at a time!
Select next target to focus on from proposals arising through community consensus process
  Impact, feasibility
  This is a governance activity
Campaign to address selected target
Iterate
Individual members are alerted to an issue
  Community Dispute Resolution Process
  InCommon automated monitoring
If the issue isn’t resolved in a reasonable time frame, recommendation for unilateral correction is brought to InCommon Steering
All proceedings are published
Reinstatement when the issue is finally resolved
What’s left to do?
Implementation Plan

Transition implementation plan into a proper project plan

Work with InCommon Operations

Amend Participant Agreement (PA) & Federation Operating Policies and Practices (FOPP)

Communicate widely with participants

Begin rollout of automated processes
  Initially to work intensively with participants whose metadata needs a tune-up
Where are we headed?
Next Steps & the Future AAC

Seed community consensus process

Recruit new AAC memberships and adjust charter

Prepare AAC to review dockets

If the idea of helping InCommon to mature and increase its value appeals to you, please consider serving on the AAC, or on a Review Board when asked.
Evaluate Today’s IAM Online

https://www.surveymonkey.com/r/IAMOnline-July2017
Internet2 2017 Technology Exchange

October 15-19, 2017
San Francisco, California

Note the Trust and Identity Track runs through Noon Thursday, October 19

https://meetings.internet2.edu/2017-technology-exchange/