Baseline Expectations for Trust in Federation

Host: Chris Spadanuda, University of Wisconsin-Milwaukee and chair of InCommon Assurance Advisory Committee (AAC)

Presenting: Tom Barton, University of Chicago and Internet2

Welcome

- Welcome to today's InCommon Assurance Call on the topic of Baseline Expectations for Trust in Federation

- The InCommon Assurance Advisory Committee appreciates your comments and feedback during and after this call.

What's led us to today's topic?

- InCommon, together with R&E Federations internationally, is the foundation on which a global access management infrastructure is being built for the R&E sector

- It must be trustworthy

- Enough that transactions having real risk can confidently be conducted over this infrastructure

InCommon trust factors

Plus

InCommon people take trust seriously

Assurance Advisory Committee of community members focused on trust

Technical Advisory Committee of community members that take security seriously

Government-grade assurance frameworks are available

Delta

Participant Operating Practices statements lack consistency

InCommon governance has favored inclusiveness over strict observance of participant commitments

Limited federation-wide standards, advisory only

Bronze and Silver have limited uptake

So here we are: Reality Check

- What trust do we need to have in Federation?

- When we rely on Federation, we are partnering with other organizations to do something for us

- What are the most important expectations of how those partners behave?

Baseline Expectations

- Main actors in Federation are IdPs, SPs, and Federation Operators

- Short, simple, high level statements of how each of them should behave to merit our trust in them, and hence trust in the federation they comprise

- Here they are, and we'd like your feedback: Are they about right?

- "Consultation" page for gathering feedback (July 6 - Aug. 10, 2016)

  https://spaces.internet2.edu/display/InCAssurance/Baseline+Expectations+for+Trust+in+Federation

Baseline Expectations of Identity Providers

1. The IdP is trustworthy enough to access the institution's own enterprise systems

2. The IdP is operated with institutional-level authority

3. The IdP is treated as an enterprise system by institution-level security operations

4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

Baseline Expectations of Service Providers

1. Controls are in place to reasonably secure information and maintain user privacy

2. Information received from IdPs is stored only when necessary for SP's purpose

3. Security incident response plan covers SP operations

4. Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL

5. Attributes required to obtain service are appropriate and published

Baseline Expectations of Federation Operators

1. Focus on trustworthiness of their Federation as a primary objective

2. Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions

3. Internationally-agreed frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted

4. Work with other Federation Operators to help ensure that each Federation's operational practices suitably promotes the realization of baseline expectations, as above, by all actors in all Federations

Questions

1. Are these the right sets of expectations? Missing anything key? Expressed at the right level?

    - IdP
    - SP
    - Fed Ops

2. What barriers might you face in meeting these expectations in your circumstances?

    - IdP
    - SP

3. How long might it take your org to comply?

4. Is self-attestation of compliance enough? Peer attestation(s)? Internal Auditor?

Reminders

- Please register your thoughts in the table on the wiki.
- Consultation on Baseline Expectations for Trust in Federations is open July 6 - Aug. 10, 2016
  - https://spaces.internet2.edu/display/InCAssurance/Baseline +Expectations+for+Trust+in+Federation
- Help with wiki access, if needed:
  - https://spaces.internet2.edu/display/IWS/Getting+access+to+the +Internet2+federated+wiki

Thank You!

Tom Barton
Senior Director, Architecture, Integration and Security
Chief Information Security Officer
tbarton@uchicago.edu

InCommon Assurance Community
assurance@incommon.org