InCommon Federation: Improvements and Roadmap

Tom Barton, Shannon Roddy, Nick Roy, Dave Shafer, Ann West
What’s There to Talk About?

• A Lot!
• Overview of Progress on Baseline Expectations
• What’s happening with Federation Operations?
• What’s next?
This is what InCommon is about...
Role of the Community Trust & Assurance Board

CTAB embodies the InCommon community’s leadership of programs that increase trust in federation

Focus this year: **Baseline Expectations!**

And what is that? ...
InCommon Baseline Expectations: Federation Operators

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
InCommon Baseline Expectations: Identity Providers

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
InCommon Baseline Expectations: Service Providers

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**
### Processes that Make Baseline Expectations Happen

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Give specific, actionable info to the right people at the right time</td>
<td>Metadata Health Check</td>
</tr>
<tr>
<td>Formal, transparent resolution of concerns about federation entities</td>
<td>Community Dispute Resolution</td>
</tr>
<tr>
<td>Enhance Baseline Expectations</td>
<td>Community Consensus</td>
</tr>
</tbody>
</table>

And loads of webinars, messages, presentations, direct contacts
Baseline Expectations Progress towards December 14th Deadline
Continuing to Build Trust

- Get InCommon community through initial phase December 14
  - Need help? Weekly office hours. Tools that show your status. FAQs.

- Regular cadence of community re-assessment and adoption
  - SIRTFI?
  - R&S support by academic IdPs?
  - errorURL metadata requirement?

- International impact
  - BE for IdPs adopted as conformance criteria for REFEDS Assurance Framework
  - Promote uptake of similar programs by other R&E Federations
InCommon Operations

• Works to support business processes for all areas of InCommon
• Maintains shared trust models in cooperation with the community and other federation operators
• Must ensure that best practices are in place to maintain trust in InCommon services
• Establishing a continuous improvement trajectory is a core objective
Process Improvements Since mid-2017

- Multiple-custody level 2 technical support service desk and incident handling
- Increased frequency of releases for the Federation Manager in support of initiatives:
  - Baseline Expectations
  - SIRTFI
- Federation manager roadmap ([https://spaces.at.internet2.edu/x/_omTBg](https://spaces.at.internet2.edu/x/_omTBg))
- Rolled out monthly notices to site administrators and execs in support of Baseline Expectations program
- Hiring in key areas
  - Project Management
  - Service Management
  - Security
  - DevOps
  - Engineering
Next Steps

- Deliver a production per-entity metadata service and new metadata signing key (MDQ) using Amazon Web Services and DevOps approaches
- Deploying changes to the Federation Manager to allow easier self-assertion of entity attributes (R&S for IdPs, for example), as well as automating many parts of metadata approval
- Developing requirements for a true test federation service to allow interoperability testing for participants and prospective participants
- Integrating with Internet2’s collaboration platform, which uses COmanage and Grouper
- Identifying additional areas for automation, reporting, and dashboarding including security, metadata standards, SLA measurements, etc.
Further Out In Time

- InCommon working groups and staff looking at:
  - Support for recommendations of Attributes for Collaboration, Streamlining SP Onboarding, Deployment Profile Working Groups
  - New Working Group: Identity Provider(s) As-A-Service
  - OpenID Connect Federation
  - Examining IdP and SP proxies as a way to enable software which does not meet requirements for multilateral federation to coexist in the federation
  - Adoption of advanced discovery requirements set forth in, e.g. RA21
  - Gap closure with needs identified in the Federated Identity Management for Research (FIM4R) v2 paper
DevOps: Since TechEX17...

- Refactored and Dockerized application
- Implemented continuous integration using Docker and Jenkins on Amazon ECS
- Moved from fixed to rolling releases

Metadata Pipeline

1. Federation Manager
2. Metadata Signing
3. Metadata Distribution

- Developed prototype per-entity signing process using Docker with Amazon ECS and CloudHSM
- Developed prototype per-entity Metadata Query (MDQ) service using Amazon CloudFront and Lambda@Edge serverless functions
DevOps: Federation Manager Deployment Frequency

Mean Time Between Deployments (Weeks)

- 2016: 52 weeks
- 2017: 7 weeks
- 2018: 3 weeks
DevOps: What’s next?

- Implement continuous delivery using Kubernetes
- Develop internal and external-facing APIs
- Deploy production automated signing service
- Deploy production per-entity Metadata Query (MDQ) service
DevOps: One Codebase, Many Deploys

Metadata Pipelines

production
Federation Manager → Metadata Signing → Metadata Distribution

test
Federation Manager → Metadata Signing → Metadata Distribution

development
Federation Manager → Metadata Signing → Metadata Distribution

my-feature-branch
Federation Manager → Metadata Signing → Metadata Distribution
DevOps: Want to know more?

- Come to the session this afternoon:
  1:40–3:30 p.m.
  Pacifica Ballroom 2/3

- Drop me a note:
  dshafer@internet2.edu
  @DavidSShafer
InCommon Baseline Expectations: Federation Operators

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.

Security Assessment, Signing Security, Cloud Security (MDQ service & HSM, FM), Security Frameworks, SIRTFI
Baseline Expectations for Trust in Federation

Trust fabric - Minimum level of trust & standards
Baseline Expectations of Identity Providers

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
Shibboleth IdPv2 - End of Life 2016

List of Shibboleth IdPs Registered by InCommon

This page includes a complete list of Shibboleth IdPs registered by InCommon, grouped by Shibboleth software version.

List of IdPs in InCommon by version: https://spaces.at.internet2.edu/x/0IIQBq
IdP Security - SSL/TLS Ciphers

We scanned the Internet! (Not really)

• A limited analysis of ciphers in use at IdPs is cause for some concern
• If you haven’t looked at what ciphers your IdP (or load balancers) are offering on these services, it’s worth a look. Remember, your user’s passwords, and services you depend on, depend on IdP security!
• Services like ssllabs are useful
  – BUT, DON’T FORGET THE “BACKCHANNEL” !!
  – ssllabs will only scan port 443
  – The backchannel often uses the SAML signing key, more later
• Weak or vulnerable ciphers, export level crypto
IdP Security - SSL/TLS Ciphers

Information about your IdP is already in the wild!

443-https-heartbleed-full_ipv4

Summary
This dataset is composed of TCP SYN scan on port 443 against the public IPv4 addr the Heartbleed attack. Details on our Heartbleed check can be found at https://jalada/

Latest Scan
Our latest scan was run at 2018-09-12 00:56:09. The data from this scan is available
Recommendations

- TIER
- Follow up-to-date best practice guides for cipher selection
- Patch your IdP software for security issues (Shibboleth, etc.)
- Search for your IdP (and SPs) in public domain sources
  - (shodan, censys, etc.)
- Have your security team involved
- Scan your IdP (nmap, ssllabs) and inspect cipher lists/software versions

- User credentials are traveling these paths!
ROBOT Attack

- December 2017, Hanno Böck, Juraj Somorovsky, and Craig Young publish a paper describing vulnerabilities in RSA decryption and signing operations.
- The attack has roots back to 1998. Crypto is hard to “get right”.
- [https://robotattack.org/](https://robotattack.org/)
- This was mostly seen as a non-event in the Shibboleth world.

Until...
ROBOT Attack

Attack would allow signing of arbitrary data with the SAML signing key.

If you are not using the “back channel” Attribute Resolution endpoints, it should probably be disabled to reduce attack surface.
SAML/XML Canonicalization Vulns.

- A number of SAML/XML signature libraries and SPs have flaws in the way they process SAML/XML signatures.
- Many commercial Service Providers have implemented SAML SSO in custom applications, or they use vulnerable or old libraries, or simply use them in unsafe ways.
- These have been/are services that are used by many Higher Eds.
- For any one Identity Provider to test all of their Service Providers independently is a significant task. For every Identity Provider to test all of their Service Providers is immense duplicated effort.
- We haven’t found the right model quite yet for coordinating this sort of effort. The coordination can’t happen in the public due to the nature of the vulnerability, but keeping it closed has proven unwieldy and difficult to manage.
  - New collaboration platform may help address some of this
Federated Incident Response

Feb 2018, Federated Incident Response exercise

- Test incident involved CERN, INFN, Nikhef, LIGO, SWITCHAII, InCommon, IDEM, SurfConext
- Full report published on the GEANT wiki: https://wiki.geant.org/x/A4LWBQ
- Incident Response in an inter-federated environment presents many challenges.
  
  - Stay tuned… Repeat exercise coming soon!
InCommon Security Incident Handling

- In the interest of transparency, past incidents and the incident handling framework are documented & published

- [https://spaces.at.internet2.edu/display/InCFederation/Incident+Handling (https://goo.gl/PqjmT6)](https://spaces.at.internet2.edu/display/InCFederation/Incident+Handling)

- On call rotation

  +1 734 352 7045 (PREFERRED)
  [security@incommon.org](mailto:security@incommon.org)
InCommon Baseline Expectations: Federation Operator Score Card

✓ Trustworthiness and transparency
✓ Generally-accepted security practices
✓ Accuracy and authenticity of metadata
✓ Frameworks that improve trustworthy use of Federation
✓ Work with relevant Federation Operators
Like What You Heard?
Annual Advisory Group Membership Drive...

InCommon Steering Committee - Policy body of InCommon Federation and related services

Technical Advisory Committee - Requirements gathering for InCommon Federation. Advisory to Steering

Community Trust and Assurance Board - Steward of Baseline Expectations and its evolution. Advisory to Steering
Get Collaboration Ready!

InCommon Attributes for Collaboration and Federation Working Group
Tuesday 12:10-1:40

Why Should Enterprise IdP Operators Care About Federation & Research?
Tuesday 1:40-3:30
Questions?