Invitation to Participate in Baseline Expectations v2's Community Consensus Process

Overview

The InCommon Community Trust and Assurance Board (CTAB) invites the InCommon community members to participate in the Community Consensus Process to review the next iteration of Baseline Expectations. The consensus process takes place from March 1, 2020 through April 15, 2020.

Introduction

The InCommon community adopted a set of "baseline expectations" for entities in the InCommon Federation in 2018. The Community Trust and Assurance Board (CTAB) worked with participating organizations and InCommon operations to inform, assist, and monitor all participating entities to comply with these expectations. **[Baseline]**

Meeting BE required commitment to the community and significant work by participating organizations - and you stepped up! As of today, ***all 5451 entities in InCommon meet these expectations for complete metadata*** including listing technical, administrative, and security contacts, user interface elements, and links to a privacy policy statement.

Representatives of member organizations have formulated requirements to further greater assurance and security of federation entities. CTAB surveyed the community in 2019 to assess readiness to adopt several potential additional Baseline Expectations; analysis of that survey was presented in IAM Online and at TechEx in December 2019.

Community Trust and Assurance Board (CTAB) now invites the InCommon community to participate in the consensus process to discern the next iteration of Baseline Expectations: Baseline Expectations v2 (BE 2)

BE 2 focuses on raising the bar around security. The proposed additions in BE 2 include these three proposed components:

- All service endpoints must be protected with current and trusted encryption (TLS).
- All entities must conform with the REFEDS Security Incident Response Framework v1.0 when handling security incidents involving federation participants.
- All Identity providers must include a valid errorURL in its published metadata.

Consensus Process Participation and Timeline

The Community Consensus Process **[Consensus]** outlines repeatable steps CTAB uses to facilitate community discussion and consensus in support of Baseline Expectations for Trust in Federation. It ensures that:

- consensus discussions include participation by those having a substantive position, proposal, or stake in the matter under discussion.
- discussions balance the level of participation with the diversity of participation, *i.e.*, don't let one or two voices drown out others.
- the outcome is representative and well-thought-out.

CTAB facilitates or moderates each discussion to ensure the above.

Participation and timeline for Consensus Process for BE 2

The Consensus Process for BE 2 will take place from **March 1, 2020 through April 15, 2020**.

To participate, sign up for the BE2 consensus process discussion mailing list at *be-consensus@internet2.edu*.

David Bantz from the University of Alaska, also chair of CTAB, will serve as the discussion moderator. We will share additional clarification material as appropriate on the Baseline Expectations wiki **[BE2FAQ]**.

Who should participate?

We encourage YOU and all community members in the InCommon community to join the discussion.
[alternate contact]

What happens when the Consensus Process concludes?

When the consensus discussion concludes on April 15, CTAB will curate the discussion and if warranted, officially propose changes to InCommon Baseline Expectations under Baseline Expectations v2. The proposal moves to Community Consultation for public review. At the conclusion of the public community consultation, BE 2 becomes officially adopted and moves to implementation across the federation.

Proposed Additions to Baseline Expectations v2

All Identity Providers (IdP) and Service Providers (SP) service endpoints must be secured with current and community-trusted transport layer encryption.

When registering an entity (IdP or SP) in InCommon, all connection endpoints of that entity must be an https URL. The applied transport layer security protocol and associated cipher must be current and trusted by the community.

Popular security testing software such as the Qualys SSL Lab Server test **[SSLLab]** offers a convenient way to test your server against these criteria and identify weaknesses. If using the Qualys SSL Lab Server test, an overall rating of A or better is considered meeting the requirements of the InCommon Baseline Expectations.

All entities (IdP and SP) meet the requirements of the Sirtfi v1.0 trust framework when handling security incidents involving federation participants

The Sirtfi trust framework v1.0 **[Sirtfi]** enables standardized and timely security incident response coordination among federation participants. When signaling and responding to security incidents within the federation, entity operators shall adhere to the process defined in the Sirtfi framework.

All IdP metadata must include an errorURL; if the condition is appropriate, SPs should use the IdP-supplied errorURL to direct the user to proper support.

IdP entity metadata must include a valid `errorURL` in its IDPSSODescriptor element.

An `errorURL` specifies a location to direct a user for problem resolution and additional support in the event a user encounters problems accessing a service. In SAML metadata for an IdP, `errorURL` is an XML attribute applied to the IDPSSODescriptor element.

When a service provider is unable to process an authentication assertion from an IdP, it may display within its error message a link to this URL to direct the user back to the IdP for additional assistance.

To participate in developing community consensus for BE 2, sign up for the BE2.0 consensus process discussion mailing list at

`be-consensus@internet2.edu`!

To sign up:

- Send a message to `pubsympa@internet2.edu` from the address you want to subscribe to the list.
- In the subject line of your message, type in: `subscribe be-consensus Firstname Name` (replace Firstname and Name with your own first name and name).
- Leave the message body blank.

Appendix A: Additional Baseline Expectations coming in 2021 and beyond

As the needs of the R&E community evolve, so will Baseline Expectations. We anticipate some expectations will require a longer transition period to adoption. To help everyone get prepared early, these are additional Expectations that are likely to be introduced in future iterations of InCommon Baseline Expectations:

All entities (IdP and SP) shall support the REFEDS MFA Profile.

When requesting an IdP to perform multi-factor authentication during a sign-in event, an SP shall submit the SAML authentication request conforming with the REFEDS MFA Profile **[MFA].**

When responding to an MFA authentication request conforming with the REFEDS MFA profile, the IdP shall respond with the proper REFEDS MFA Profile assertion on successful authentication. [*not requring MFA roll-out to users, but abillity to signal use*]

Why is this not included in the 2020 edition of Baseline Expectations?

Some IdP and SP software used by participants is unable to process authentication context, so could not meet this expectation. CTAB and others hope to find one or more “work-arounds” that would enable these IdPs and SPs to address this lack.

All IDPs shall support the REFEDS Research & Scholarship (R&S) Entity Category.

An IdP registered in the InCommon Federation shall support the REFEDS Research and Scholarship (R&S) Entity Category **[R&S]**; it shall release to qualifying SPs user attributes defined

in the REFEDS R&S attribute bundle for individuals who participate in research collaboration in the R&E community.

Why is this not included in the 2020 edition of Baseline Expectations?

Some IdP and SP software used by participants does not support the entity category attribute. CTAB and others hope to find one or more “work-arounds” that would enable these IdPs and SPs to address this lack.

Appendix B: References

[Baseline] InCommon Baseline Expectations for Trust in Federation; https://incommon.org/federation/baseline/

[BE2FAQ] Clarification to Proposed Baseline Expectation 2.0 Statements; https://spaces.at.internet2.edu/display/BE/be2-faq

[Consensus] Community Consensus Process for Interpreting Baseline Expectations; https://incommon.org/federation/community-consensus/

[MFA] REFEDS Multifactor Authentication Profile; https://refeds.org/profile/mfa

[R&S] REFEDS Research and Scholarship Entity Category; https://refeds.org/category/research-and-scholarship

[Sirtfi] REFEDS Security Incident Response Framework (Sirtfi) v1.0; https://refeds.org/sirtfi

[SSLLab] SSL Server Test Powered by Qualys SSL Lab https://www.ssllabs.com/ssltest

Appendix: Actual Email text

To All InCommon Participants,

InCommon invites all InCommon community members to participate in the Community Consensus Process to review the next iteration of Baseline Expectations: Baseline Expectations 2. The consensus process takes place from March 1, 2020 through April 15, 2020.

Baseline Expectations 2 adds several security-focused statements. Together, they aim to further improve transactional security and trust across the InCommon Federation.

We invite you to provide your input during the Community Consensus Process from March 1 to April 15, 2020. Please consider these proposed requirements' contribution to increased

assurance and interoperability within InCommon as well as impact of implementation within your organization when commenting.

To learn more about the proposed additions in Baseline Expectations 2, visit https://spaces.at.internet2.edu/display/be/

Visit the Community Consensus Process web page to learn how the Community Trust and Assurance Board identifies and finalizes the next set of requirements: https://www.incommon.org/federation/community-consensus/

To participate in the discussion and provide feedback, subscribe to the Baseline Expectations Consensus discussion list:

1. Send email to `pubsympa@internet2.edu` from the address you want to subscribe to the list.
2. Enter the subject line of your message like: `subscribe be-consensus` *`myGivenName mySurName`*

Once reviewed, finalized, and approved by the InCommon Steering Committee, these requirements will become mandatory for all participants.

Thank you for your enthusiasm and interest in making the community work together more trustworthy by implementing the Baseline Expectations for Trust in Federation over the last 2 years! As of today, ***all 5451 entities in InCommon meet these expectations for complete metadata***. We look forward to hearing your thoughts about the new requirements and working together to increase trust across InCommon.

Best regards,

David Bantz
University of Alaska
Chair, InCommon Community Trust and Assurance Board

Ann West
Associate Vice President for Trust and Identity, Internet2