be2-consensus

Jump to:

Consensus Process is closed.

The Community Consensus process has closed. This page is preserved for historical records purpose. For the latest on Baseline Expectations 2, visit the Baseline Expectations 2 home page.

Summary

The InCommon Trust and Assurance Board invites the InCommon community to participate in the Community Consensus Process to review the next iteration of Baseline Expectations.

- **What?** Three proposed new Baseline Expectations:
  - 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 published metadata.
- **When?** Participate now! We are evaluating the consensus period as needed while the world responds to the global pandemic.
- **How?** Comment by joining the discussion list. Send email to pubsympa@internet2.edu with the subject: subscribe be-discussion. We need to hear from you about the expected impact of these new expectations in terms of implementation
- **Why?** Details on each proposed expectation are below - but the goal is to improve trust and interoperability.

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.

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.

We now invites the InCommon community to participate in the consensus process to discern the next iteration of Baseline Expectations: Baseline Expectations 2 (BE2).

BE2 adds several security-focused statements. Together, they aim to further improve transactional security, thus trust among services participating in the InCommon Federation. These proposed statements are:

- 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.

Participation and timeline

The Consensus Process for BE2 began on **March 1, 2020**. Due to the global pandemic, we are keeping the Consensus Process open at this time to allow additional time for participation (**deadline August 15, 2020**).

Related content

- Frequently Asked Questions
- Baseline Expectations 2

References

- Baseline Expectations for Trust in Federation
- Community Consensus Process
- REFEDS Multifactor Authentication Profile
- REFEDS Research and Scholarship Entity Category
- REFEDS Security Incident Response Framework (Sirtfi) v1.0
- Baseline Expectation 1 wiki archive

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

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

David Bantz from the University of Alaska, also chair of CTAB, will serve as the discussion moderator. We will share additional clarification material on this wiki.

Who should participate?

We encourage YOU and all community members in the InCommon community to join the discussion.

Proposed Additions to Baseline Expectations 2.0

STATEMENT: 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 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.

MORE: Clarification - Encrypt Entity Service Endpoints

STATEMENT: 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 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.

MORE: Clarification - Entity Complies with Sirtfi v1.0

STATEMENT: 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.

MORE: Clarification - IDP Metadata Must Have an Error URL

Additional Baseline Expectations coming in 2021 and beyond

As the needs of the R&E community evolves, 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:

STATEMENT: 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**.**

When responding to an MFA authentication request conforming with the REFEDS MFA profile, the IdP shall respond with the proper REFEDS MFA Profile assertion signaling whether or not multi-factor authentication occurred. This does not require a participant to enroll any user to use multi-factor authentication. It only requires the IdP to signal whether multi-factor authentication has occurred using the REFEDS MFA profile.

Why is MFA Profile support not included in Baseline Expectations 2?

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.

STATEMENT: 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; 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 Requiring R&S not included in Baseline Expectations 2?

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.

About the Community Consensus Process

The Community Consensus Process 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.

What happens when the Consensus Process concludes?

When the consensus discussion concludes on August 15, CTAB will curate the discussion and if appropriate, officially propose changes to InCommon Baseline Expectations under Baseline Expectations 2.0. The proposal moves to Community Consultation for public review. At the conclusion of the public community consultation, BE 2.0 becomes officially adopted and moves to implementation across the federation.