Implementation Guidance and Best Practices for Baseline Expectations 2

candidate-draft, September 2020

Repository ID: TI.137.1
Authors: Members of the InCommon Community Trust and Assurance Board
Sponsor: InCommon Community Trust and Assurance Board (CTAB)
Superseded documents: N/A
Proposed future review date: November 2021
Subject tags: InCommon, federation, assurance, trust, framework

Content

Introduction

This document provides implementation guidance for InCommon Participants and the Federation Operator when updating systems to adhere to the statements introduced in the 2nd edition of the InCommon Federation Baseline Expectations for Trust in Federation (Baseline Expectations 2, BE2) **[BE2]**. Specifically, this document clarifies the implementation requirements for the new statements introduced in Baseline Expectations 2. It also recommends best practices and implementation strategies where appropriate.

To differentiate between required actions and recommended practices, this document uses keywords defined in **[RFC2119]** to indicate requirement levels. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **[RFC2119] [RFC8174]** when, and only when, they appear in all capitals, as shown here.

The terms “Identity Provider,” “IdP,” “Service Provider,” and “SP” refer to the operational entities registered in the federation. Where the document refers to the organizations operating these entities, the terms “IdP Operator” and “SP Operator” are used. Alternatively, “Participant” may be used to generically refer to an organization who has registered an IdP or SP in the InCommon Federation.

Baseline Expectations 2 Implementation Guidance and Best Practice

1. All entity (IdP and SP) service endpoints must be secured with current and trustworthy transport layer encryption.

1.1 What does current and trustworthy mean?

When an InCommon Participant (Participant) registers an entity (IdP or SP) in the InCommon Federation, all connection endpoints specified in that entity’s SAML metadata MUST be properly encrypted using sufficiently strong transport layer encryption protocol and cipher, i.e., every connection endpoint URL MUST be an HTTPS URL. The transport layer security protocol and associated encryption ciphers used MUST be supported by its maker and is of a version generally deemed trustworthy in the industry.

For an IdP, a “connection endpoint” includes the locations listed within the ArtifactResolutionService, the SingleSignOnService, the SingleLogoutService, and the AttributeService.

For an SP, a “connection endpoint” includes the locations (URLs) listed within the AssertionConsumerService and the SingleLogoutService

1.2 Who does this requirement apply to?

This requirement applies to all entities (identity providers and service providers) registered with the InCommon Federation.

1.3 How do I meet this requirement?

[BE2-P01]

An IdP or SP meets the requirements of this statement when every connection endpoint URL in its registered SAML metadata, entered via Federation Manager is an https:// URL.

By entering an https:// URL, the participant certifies that the endpoint is properly encrypted.

To verify adherence, IdP and SP operators SHALL use the Qualys SSL Lab Server Test **[SSLTest]** to check for gaps in implementation[1]. An overall rating of A or better is considered meeting the requirements of the InCommon Baseline Expectations. If the test score is less than an A, the IdP or SP Operator SHALL apply mitigating measures within 90 days.

The InCommon Federation will implement automated, periodic testing to verify that all registered endpoints meet the “current and trustworthy” criteria.

1.4 Implementation Guidance for IdP and SP operators

[BE2-P02]

Make endpoints accessible from the internet

Each endpoint registered in an IdP or SP SAML metadata SHALL be accessible from the Internet so that the InCommon Federation Operator may periodically inspect registered endpoints using automated testing tools (such as the Qualys SSL Lab Server Test) to verify each endpoint meets BE2 requirements.

If the InCommon Federation Operator is unable to inspect an endpoint because it is not accessible from a public location on the internet, it will notify the Participant. The Participant SHALL remediate within 90 days of notification.

---

[1] The Open Web Application Security Project’s (OWASP) Transport Layer Protection Cheat Sheet and the TLS Cipher String Cheat Sheet **[OWASP]** offer detailed criteria for encryption security evaluation.

[BE2-P03]

Re-test periodically

As technology evolves rapidly in this area, it is important that deployers test and update their security implementations to mitigate the risk of data loss and system compromise, as well as to provide greater awareness and transparency. The deployer SHOULD retest at least every 90 days.

1.5 Implementation Guidance for Federation Operator

[BE2-F01]

Modify Federation Manager to require https URL for all IdP and SP

InCommon SHALL update Federation Manager to require all connection endpoints (IdP and SP) to begin with https:// before Baseline Expectations 2 takes effect.

InCommon SHOULD generate reports of entities (and associated contact information) currently not meeting this requirement to facilitate outreach and mitigation.

[BE2-F02]

Implement automated, event-triggered SSL testing

InCommon SHALL develop an automated, event-driven mechanism to periodically inspect registered endpoints to detect implementation deficiencies. Such inspection SHALL be performed using Qualys SSL Lab's SSL Server Test API.

The Federation Operator SHALL test each registered entity at least every 365 days. It SHOULD test when a significant change event occurs (e.g., changes in the entity's metadata, SSL Lab changing the grading criteria, etc.)

The results from the inspection SHALL be made available to the entity organization's InCommon Executive (Exec) and Site Administrators (SA). The SA SHALL be alerted via warnings in Federation Manager as well as email notification. The Exec MAY be alerted via a self-service dashboard, or alternatively email alerts. InCommon SHALL work with the Participant's SA to remediate the defect. If the Participant does not remediate the defect within 90 days of initial notice, the Federation Operator SHALL escalate the matter via the Community Dispute Resolution Process to establish a mutually agreeable remediation plan and timeframe.

While this testing is not required at the beginning of Baseline Expectations 2 implementation, InCommon SHOULD prioritize the testing implementation so that it can begin such testing as early as possible in order to support continued Participant adherence to this requirement.

2. Every entity (IdP and SP) complies with the requirements of the SIRTFI v1.0 trust framework.

2.1 What is SIRTFI?

The SIRTFI trust framework enables coordinated response to security incidents in a federated context that does not depend on a centralized authority or governance structure to assign roles and responsibilities for doing so. It does so through a set of self-asserted capabilities and roles associated with an IdP or SP organization's federated entities.

2.2 Who does this apply to?

This requirement applies to all entities (IdPs and SPs) registered with the InCommon Federation. As SIRTFI is designed to enable coordination of security incident response across federated organizations, these requirements only apply when the entity is involved in a federated SSO event in the InCommon Federation.

2.3 How do I meet this requirement?

[BE2-P04]

To meet this requirement, the operator of the IdP or SP implements the practices specified in the Security Incident Response Trust Framework for Federated Identityv1.0 **[SIRTFI]**. See the SIRTFI FAQ **[SIRTFIFAQ]** for additional details: https://refeds.org/sirtfi/sirtfi-faqs.

To signal their conformance, the Site Administrator (SA) or Delegated Administrator (DA) MUST check the "Complies with SIRTFI" checkbox for each entity in the InCommon Federation. The SA or DA also MUST make sure that the Security Contact registered in the metadata can function as the incident contact described in the Sirtfi framework (section 2.2 Incident Response).

2.4 Implementation Guidance for Federation Operator

[BE2-F03]

Modify Federation Manager to require Sirtfi for all entities

InCommon SHALL update Federation Manager to require all newly registered entities (IdP and SP) to check the "Complies with SIRTFI" checkbox effective when InCommon transitions to Baseline Expectations 2.

InCommon SHALL update Federation Manager to warn the Site Administrator of any existing entities that have not checked the "Complies with SIRTFI" checkbox. It SHALL further update Federation Manager by BE2's adherence deadline to perform the following:

- require all entities to check the “Complies with SIRTFI” checkbox;
- introduce language in Federation Manager to inform the SA of the obligations they are accepting by checking the box, as well as follow up instructions should the SA have questions;
- introduce a mechanism to notify the InCommon Exec when the SA accepts the SIRTFI requirements.[2]

InCommon SHALL generate reports of entities (and associated contact information) currently not meeting this requirement to facilitate outreach and mitigation.

3 Identity Provider must include an errorURL in its metadata.

3.1 What is an error URL?

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 identity provider (IdP), `errorURL` is an XML attribute applied to the IDPSSODescriptor element.

When a service provider (SP) 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.

3.2 Who does this requirement apply to?

This requirement applies to all identity providers registered with the InCommon Federation.

3.3 How do I (the IdP operator) meet this requirement?

[BE2-P05]

An IdP’s metadata MUST include the `errorURL` attribute on its <md:IDPSSODescriptor> element. The content of the `errorURL` attribute MUST be an HTTPS URL resolving to an HTML page.

A Participant’s Site Administrator accomplishes this by entering the appropriate errorURL when registering the entity using Federation Manager.

[2] Federation Operator should evaluate the frequency of notification to Execs so to not to flood the Exec with unnecessary notices.

3.4 Implementation Guidance for Identity Providers

The HTML page referenced by the `errorURL` MUST be suitable for referral by SPs when it requires the IdP's assistance to help the user troubleshoot an error.

The `errorURL` MUST be reachable from public locations on the Internet.

The `errorURL` MUST be an https:// URL.

The page SHALL contain the appropriate language/instruction, either directly or via a pointer to a help desk, to help a user resolve access issues, for example:

- The SP did not receive one or more attributes or values it requires for basic identification and/or personalization purposes. This typically applies to unique identifiers, name, and email address attributes that are common to federated interactions.
- The user is not authorized to access the SP. This may be caused by an inadequate assurance level (when expressed independently of authentication), entitlements, affiliation, or missing attribute or value. An SP denying a user access due to local authorization control measures SHOULD NOT direct the user back to the IdP via the errorURL over since the IdP would have no control or be able to help the user.
- The SP received an invalid/inappropriate authentication context, for example, an SP requires MFA, but the assertion sent by the IdP does not contain the appropriate MFA authentication context.
- Other errors - an SP has encountered an error and has evidence that the condition could be remedied by the end-user or IdP organization with relatively minimal further involvement by the SP.

The IdP operator SHOULD consider implementing the Enhanced errorURL format described in the SAML Metadata Deployment Profile for errorURL Version 1.0 **[ErrURL].**

3.5 Implementation Best Practices for Service Providers

Baseline Expectations 2 does not have specific requirements for Service Providers regarding the use of `errorURL`. We offer the following best practices for SP's to help maximize the value of using this mechanism and to better overall user experience. These "optional" best practices may become required elements in future editions of Baseline Expectations.

[BE2-P06]

Best practices for service providers: when should I invoke the IdP's errorURL?

It is appropriate to refer a user to this error in the following conditions:

- The authentication assertion does not contain the required/requested user attributes for the SP to identify the user and/or grant access.
- The authentication assertion does not meet the required authentication method (such as MFA) the SP has previously negotiated with the IdP operator.

Prior to directing the user to the `errorURL`, the SP should make sufficient effort to help the user understand the nature of the error to help facilitate the support request submission.

It is NOT appropriate for an SP to direct the user to the IdP's error URL if the error is caused by failures within the SP's application and/or infrastructure. In the cases of local error, the SP should direct the user to the appropriate application support desk.

To signal more precisely the nature of the error, SP operator SHOULD support the Enhanced errorURL format described in the SAML Metadata Deployment Profile for errorURL Version 1.0 **[ErrURL]**.

3.6 Implementation Guidance for Federation Operator

[BE2-F04]

Modify Federation Manager to require errorURL for all IdP

InCommon SHALL update Federation Manager to require all newly registered IdP to supply a valid errorURL effective when InCommon transitions to BE2.

InCommon SHALL update Federation Manager to warn the Site Administrator of any existing IdP missing a valid errorURL. It SHOULD further update Federation Manager at a later date (adherence deadline) to require ALL IdPs to contain a valid errorURL.

InCommon SHALL generate reports of entities (and associated contact information) currently not meeting this requirement to facilitate outreach and mitigation.

Reference

[BE2] Baseline Expectations for Trust in Federation, Version 2 (draft location), https://drive.google.com/open?id=1Ubwc4RoqEO6HtbN6t9dpGvY2eiD5zcs3Zw5gh9xHMsk

[SIRTFI] REFEDS Security Incident Response Framework v1.0, https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

[SIRTFIFAQ] Sirtfi Frequently Asked Questions, https://refeds.org/sirtfi/sirtfi-faqs.

[ErrURL] SAML Metadata Deployment Profile for errorURL Version 1.0, https://refeds.org/specifications/saml-v2-0-metadata-deployment-profile-for-errorurl-version-1-0

[OWASP] (OWASP) Transport Layer Protection Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html and the TLS Cipher String Cheatsheet, https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html.

[SSLTest] Qualys SSL Lab Server Test, https://www.ssllabs.com/ssltest

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels, https://tools.ietf.org/html/rfc2119

[RFC8174] Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, https://tools.ietf.org/html/rfc8174