be2-guide-encrypt-endpoints

This article is a part of a document curated under the Internet2 Trust and Identity Document Stewardship program. It has been reformatted for web display and may contain additional annotation. Download the official text from the Internet2 Trust and Identity Document Repository at: http://doi.org/10.26869/TI.137.1.

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

TL;DR

- For every registered IdP and SP, perform SSL server test against each server hosting the connection endpoints (SingleSignOn, SingleLogout, AttributeService, ArtifactResolutionService); Each server should receive a SSLLab Server Test score of A or better.
- If necessary, devise remediation plans to bring server score to A or better.
- Perform on-going, periodic testing to make sure the servers hosting connection endpoints continue to maintain A or better.

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?

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 meet this requirement, all endpoints of an entity SHALL receive a grade of A or better according to the test criteria defined in the SSL Labs SSL Server Rating Guide **[SSLRatingGuide]**. Qualys SSL Lab Server Test **[SSLTest]** is a reference implementation of this guide, and is suitable to use to test an entity against the Rating Guide's criteria. 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.

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.

1.4 Implementation Guidance for IdP and SP operators

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.

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

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.

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.

<< Back to Introduction | Continue to Entity Complies with SIRTFI >>