Clarification - Encrypt Entity Service Endpoints

Statement - All entity (IdP and SP) service endpoints must be secured with current and supported transport layer encryption.

What is it?

When registering an entity (IdP or SP) in InCommon, all connection endpoints of that entity must be an HTTPS URL. Further, the transport layer security protocol and associated ciphers used must be supported and trustworthy versions.

For an IdP, a “connection endpoint” includes the locations for the ArtiffactResolutionService, the SingleSignOnService, the SingleLogoutService, and the AttributeService

For an SP, a “connection endpoint” includes the locations for the AssertionConsumerService and the SingleLogoutService

Who does this requirement apply to?

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

How do I meet this requirement?

To meet this requirement, all endpoints of an entity must maintain a grade of A or better according to the test criteria defined in the SSL Labs SSL Server Rating Guide.

Qualys SSL Lab Server Test 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 must apply mitigating measures within 90 days.

Periodic Scanning - The InCommon Federation will implement automated, periodic testing to verify that all registered endpoints meet the “current and trustworthy” criteria. Endpoints in a registered IdP or SP must be accessible from a public location on the Internet in order to facilitate testing.

Related content

- Clarification - Entity Complies with Sirtfi v1.0
- Clarification - IDP Metadata Must Have an Error URL
- Clarification - Encrypt Entity Service Endpoints