Implementing Baseline Expectations in InCommon Metadata

Version 1.1 (Revised November 10, 2017)

This document translates the Baseline Expectations described in [TI.34.1] into an initial set of requirements for InCommon metadata.

Proposed Metadata Requirements

Below, each statement from Baseline Expectations is expressed as one or more requirements for an entity's metadata, grouped by the role of the federated entity.

Identity Providers

Baseline Expectation	Metadata Requirements	Other Requirements
"The IdP is operated with organizational-level authority"	N/A	Federation Manager Application: - Review web UI for consistency with Baseline Expectations (terminology, grouping/layout of controls, etc.) - Add references to Baseline Expectations with links to appropriate documentation
"The IdP is trusted enough to be used to access the organization's own systems"	N/A	Federation Manager Application: - Review web UI for consistency with Baseline Expectations (terminology, grouping/layout of controls, etc.) - Add references to Baseline Expectations with links to appropriate documentation
"Generally-accepted security practices are applied to the IdP"	REQUIRED: - SSL certificates on endpoints are in place	SSL certificates are subject to quality testing performed by InCommon operations or a service provider on its behalf. Results of these scans may be saved by and acted upon by InCommon operations at its discretion.
"Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL"	REQUIRED: - Entity includes at least one "technical" contact with a valid email address - Entity includes at least one "administrative" contact with a valid email address - Entity includes at least one "security" contact with a valid email address - Entity includes a valid DisplayName - Entity includes a valid HTTPS Logo URL - Entity includes a valid PrivacyStatementURL RECOMMENDED: - IDPSSODescriptor includes a valid errorURL attribute	Logo and privacy policy URL subject to the following test conditions: REQUIRED: - Results in a '200' based on an HTTP GET

Service Providers

Expectation	Metadata Requirements	Other Requirements
“Controls are in place to reasonably secure information and maintain user privacy”	N/A	Federation Manager Application: • Review web UI for consistency with Baseline Expectations (terminology, grouping/layout of controls, etc.) • Add references to Baseline Expectations with links to appropriate documentation
“Information received from IdPs is not shared with third parties without permission and is stored only when necessary for SP’s purpose”	N/A	Federation Manager Application: • Review web UI for consistency with Baseline Expectations (terminology, grouping/layout of controls, etc.) • Add references to Baseline Expectations with links to appropriate documentation
“Generally-accepted security practices are applied to the SP”	RECOMMENDED: • SSL certificates on endpoints are in place	SSL certificates are subject to quality testing performed by InCommon operations or a service provider on its behalf. Results of these scans may be saved by and acted upon by InCommon operations at its discretion.
“Federation metadata is accurate, complete, and includes site technical, admin, and security contacts, MDUI information, and privacy policy URL”	REQUIRED: • Entity includes at least one "technical" contact with a valid email address • Entity includes at least one "administrative" contact with a valid email address • Entity includes at least one "security" contact with a valid email address • Entity includes a valid DisplayName • Entity includes a valid HTTPS Logo URL • Entity includes a valid PrivacyStatementURL RECOMMENDED: • SP endpoints do not use unencrypted http	Logo and privacy URL subject to the following test conditions: REQUIRED: • Results in a ‘200’ based on an HTTP GET
“Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly”	N/A	Federation Manager Application: • Review web UI for consistency with Baseline Expectations (terminology, grouping/layout of controls, etc.) • Add references to Baseline Expectations with links to appropriate documentation

Federation Operators

Expectation	Metadata Requirement	Other Requirements
“Focus on trustworthiness of their Federation as a primary objective and be transparent about such efforts”	N/A	

“Generally-accepted security practices are applied to the Federation’s operational systems”	N/A	
“Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions”	(The following requirements apply to the federation operator’s metadata processes, but not to the metadata itself.) REQUIRED: • Federation metadata is reviewed for accuracy, completeness, and compatibility with the current InCommon metadata specification RECOMMENDED: • Contact email addresses are checked for deliverability at least annually • URLs in metadata are checked at least monthly • SSL certificates on entity endpoints are checked at least monthly	
“Frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted”	N/A	
“Work with relevant Federation Operators to promote realization of baseline expectations”	N/A	Share InCommon practices and metadata specification with other federations and federation operators

Changes to Metadata Requirement Levels

Implementing metadata requirements for Baseline Expectations would change current requirements as follows:

Entity Type(s)	Requirement	Current Level	Baseline Level
IdP, SP	Entity includes a valid DisplayName	REQUIRED	REQUIRED
IdP, SP	Entity includes at least one "technical" contact with a valid email address (contact may be a person, group or list - group or list recommended)	REQUIRED	REQUIRED
IdP, SP	Entity includes at least one "administrative" contact with a valid email address (contact may be a person, group or list - group or list recommended)	OPTIONAL (SPs), REQUIRED (IdPs)	**REQUIRED**
IdP, SP	Entity includes at least one "security" contact with a valid email address (contact may be a person, group or list - group or list recommended)	OPTIONAL	**REQUIRED**
IdP, SP	Entity includes a valid HTTPS Logo URL	OPTIONAL	**REQUIRED**
IdP, SP	Entity includes a valid PrivacyStatementURL	OPTIONAL	**REQUIRED**

IdP	SSL certificates on endpoints are in place	REQUIRED	**REQUIRED**
SP	SSL certificates on endpoints are in place	OPTIONAL	**RECOMMENDED**
IdP	IDPSSODescriptor includes a valid errorURL attribute	OPTIONAL	**RECOMMENDED**
SP	SP endpoints do not use unencrypted http	OPTIONAL	**RECOMMENDED**

Metadata Validation Mechanisms

Metadata requirements are currently validated using a variety of manual processes and features in the Federation Manager. As we implement the requirements for Baseline Expectations, metadata validation will make greater use of input validation rules in the Federation Manager, automated static analysis of the metadata aggregate, email delivery checks, and HTTP/HTTPS probes. A variety of reports (delivered by email or available online) will inform participants about the health of the federation in aggregate, and by organization and entity.

Entity Type(s)	Requirement	Current Mechanism(s)	Future Mechanism(s)
IdP, SP	Entity includes a valid DisplayName	FM	MD health check, FM input validation
IdP, SP	Entity includes at least one "technical" contact with a valid email address (contact may be a person, group or list - group or list recommended)	FM	MD health check, FM input validation, Email deliverability check
IdP, SP	Entity includes at least one "administrative" contact with a valid email address (contact may be a person, group or list - group or list recommended)	Manual (IdPs), None (Others)	MD health check, FM input validation, Email deliverability check
IdP, SP	Entity includes at least one "security" contact with a valid email address (contact may be a person, group or list - group or list recommended)	Manual (SIRTFI entities), None (Others)	MD health check, FM input validation, Email deliverability check
IdP, SP	Entity includes a valid HTTPS Logo URL	Manual (IdPs), None (Others)	MD health check, FM input validation
IdP, SP	Entity includes a valid PrivacyStatementURL	Manual	MD health check, FM input validation, HTTP check
IdP	SSL certificates on endpoints are in place	Manual	FM input validation, SSL certificates are subject to quality testing performed by InCommon operations or a service provider on its behalf. Results of these scans may be saved by and acted upon by InCommon operations at its discretion.
SP	SSL certificates on endpoints are in place	None	SSL certificates are subject to quality testing performed by InCommon operations or a service provider on its behalf. Results of these scans may be saved by and acted upon by InCommon operations at its discretion.
IdP	IDPSSODescriptor includes a valid errorURL attribute	Manual (IdPs), None (Others)	MD health check, FM input validation, HTTP check
SP	SP endpoints do not use unencrypted http	None	MD health check, FM input validation

Next Steps

Create a draft InCommon Metadata Specification v1.0.0 which incorporates these requirements arising from Baseline Expectations, as well as other current and near-term planned metadata requirements.

Abbreviations

- Identity Provider (IdP)
- Service Provider (SP)
- Metadata (MD)
- Federation Manager application (FM)

References

- [TI.34.1] Baseline Expectations for Trust in Federation, https://spaces.at.internet2.edu/display/BE/Baseline+Expectations+for+Trust+in+Federation?preview=/116458160/116458162/TI.34.1-BaselineExpectations-v1-2016-09-7.pdf
- REFEDS Security Contact Metadata Extension Schema