Baseline Expectations for InCommon Execs

January 10, 2018

Baseline Expectations for InCommon Execs

The InCommon community has adopted a set of Baseline Expectations, which introduce minimum expectations for federation participants. This will touch every InCommon participant and will almost certainly mean making changes in your metadata.[1]

You will find background information and resources on the web and wiki.[2] This summary offers a quick overview so you can determine what your organization needs to do to meet the expectations. We encourage you to discuss this with your InCommon site admins.

[1] Metadata is the InCommon trust registry. Each organization maintains the metadata for its identity provider(s) and/or service provider(s). The metadata makes interoperability possible.

[2] Web: www.incommon.org/federation/baseline. Wiki: https://spaces.internet2.edu/x/sALxBg

Updated and Complete Metadata

Expectation: Updated and Complete Metadata (everyone)		
Metadata Item	**Why is this important?**	**Who Does This?**
Display Name	Provides the commonly used name for your organization or service	Your site admin adds, then reviews and updates regularly, via the Federation Manager portal.
Technical administrative, security contacts	Provides other federation participants (and users) with key contacts for troubleshooting	Your site admin adds, then reviews and updates regularly, via the Federation Manager portal.
Privacy Statement URL	Provides other federation participants a way to review your privacy policy	Your site admin adds, then reviews and updates regularly, via the Federation Manager portal.
Logo URL	Helps a user quickly find his/her home organization, and also alerts them in a graphical way which service they are accessing	Your site admin adds, then reviews and updates regularly, via the Federation Manager portal.
Error URL (IdPs, not yet required)	Provides a landing web page at the user's home organization for the user who has problems authenticating, so the user isn't left at a dead end. The SP can point a user to this URL when there is an issue.	Your site admin adds, then reviews and updates regularly, via the Federation Manager portal.

Other Expectations for Identity Providers

Other Expectations for Identity Providers (Those deploying identity providers in the federation include virtually all college and university participants plus many research organizations.)		
Item	**What does this mean?**	**Who Does This?**
IdP is operated with organizational-level authority	Responsibility for operating the institution's IdP is assigned appropriately, usually to the central IT organization	Your organization did this upon signing the Participation Agreement.
Your IdP is trusted enough to be used across your organization's own systems	The quality of the IdP operation is equivalent to the quality of any other authentication service that is used to login to important systems, such as HR, course management, or grants administration systems.	Self-attested - you agree that you comply with this simply by publishing an IdP in InCommon metadata.
You apply generally accepted security practices to your IdP	User accounts are points of potential compromise, so reasonable security protections and security incident response measures should apply.	One key indicator is whether your IdP is running the latest version of federating software.

Other Expectations for Service Providers

Other Expectations for Service Providers (those with commercial, collaboration, or other services available for federated access)		
Item	**What does this mean?**	**Who Does This?**
Controls are in place to reasonably secure information and maintain user privacy	These express the expectation that an SP system that collects user data will protect it in alignment with how the organization determines protections for other systems that store or process personal information.	Self-attested - you agree that you comply with this simply by publishing an SP in InCommon metadata.
Information received from IdPs is not shared with third parties without permission and is stored only when necessary for the SP's purpose		Self-attested
You apply generally accepted security practices to your SP		One key indicator is whether your SP is running the latest version of federating software.
Unless governed by an applicable contract, attributes required to obtain service are appropriate and made known publicly	The SP only asks for data that is essential for providing the service, and makes known which attributes are being requested.	Self-attested