InCommon Service Provider Onboarding   - Final Report

DRAFT v1, April 2018

Table of Contents

1. Introduction

A summary of the working group's mission is as follows:

"The Streamlining SP Onboarding Working Group will **identify and document standards** for Service Provider operation within the InCommon Federation using the CIC Cloud Services Cookbook as a starting point. Having **standards available that help SPs onboard** will add to the value proposition for SPs in the InCommon Federation and reduce variance in configuration and increase interoperability."

With that mission, the working group set out to gather and review existing standards that are documented for both Service Providers (SP) and Identity Provider Organizations (IDPO); starting with the 'CIC Cloud Services Cookbook'.   Drawing on several dozen different standards and criteria, the working group then set out to narrow these standards down to a set of criteria that we felt were most applicable to the SP onboarding process. Specifically selecting those criteria, that if followed and applied correctly, would streamline the SP onboarding process while providing the SP with optimal levels of interoperability and security. Lastly, to narrow the criteria down further, we grouped them into two categories: minimum and recommended. 'Minimum' criteria defined as those criteria that should be met by all SPs regardless of their setup. 'Recommended' criteria being those criteria that would be strongly encouraged, but depending on various factors, not always necessary.

In conjunction with identifying and documenting these core set of SP standards, the working group also set out to help clarify what the value adds were for meeting these standards with respect to becoming an InCommon member and leveraging the InCommon federation.

To see the complete list of criteria, please see 'InCommon Service Provider Onboarding - Criteria Document'.

2. Using the Criteria as the Foundation for a Questionnaire

The 'InCommon Service Provider Onboarding - Criteria Document' provides a foundation, built on a set of consistent standards, for Service Providers (SP) in InCommon to follow. A set of standards that would apply equally to vendor (commercial), education, and research SPs (for more details on the variety of SPs that exist across these three categories, please see Targeted Service Providers).

However in many cases, a standalone criteria document may provide too steep of a learning curve for new or inexperienced SPs to follow. For example, SPs that are interested in joining InCommon but need pointers on where to start and what standards they need to get started with. Or SPs that need help understanding the terminology that make up the criteria or need technical assistance with implementing the criteria. Therefore, as a complement to the criteria

document, a self-assessment (questionnaire) style approach was developed. An approach that would "walk" the SP through standards adoption and the overall onboarding process into InCommon; providing the opportunity to self-assess against the criteria while also interweaving helper material, online references, and appropriate guidance every step of the way.

With the end result being, the centralization of a core set of standards and best practices that are more readable, easier to follow, and accessible to a much wider experience spectrum of InCommon Service Providers. And for those Service Providers that are more experienced and have already designed and deployed their applications, the self-assessment questionnaire will give them the opportunity to reassess their current setup against the latest set of SP criteria and best practices.

3. InCommon Service Provider Onboarding - Questionnaire

This questionnaire style approach allows onboarding SPs to self-assess; using a series of yes/no questions that present guidance, recommendations, and criteria depending on the answers given. With each question representing a particular standard or criteria sourced from the 'InCommon Service Provider Onboarding - Criteria Document'.

For a **preview** of the questions in the questionnaire, you can reference the Questionnaire Outline in the Appendix of this document. For the **complete** experience, the actual Questionnaire can be found (and filled out) here: InCommon SP Onboarding - Questionnaire.

Additionally, the questionnaire is able to provide appropriate context and helper material to each question being asked; allowing the SP to understand what the question is asking and make an informed decision on how to best answer the question. Taking this further, if the SP decides to answer a question a certain way that would imply they are not meeting a specific criteria item, then the questionnaire provides the associated risks along with recommended next steps. At which point, the SP has the information they need to make the proper decision on whether to proceed, given the associated risks, or not.

By the end of the questionnaire, the SP should should understand the onboarding criteria, the fundamental concepts behind the criteria, the steps required to meet the criteria, and be able to find references to applicable online resources if further information or assistance is needed.

4. Summary

With the InCommon criteria document and the questionnaire, Service Providers have resources they can follow that will guide them through standard adoption and help streamline their onboarding process into the InCommon Federation. While at the same time, providing clarity for how standard adoption, combined with membership in InCommon, can lead to improved interoperability with other SPs and more streamlined integrations with Identity Provider Organizations within InCommon.

Appendix A. Questionnaire Outline

A. Establishing Trust
    a. Is your organization a member of the InCommon Federation?
    b. Has your organization registered your service's metadata with the InCommon federation?
    c. Has your organization defined a process for keeping your metadata up to date?
    d. Does your application consume, refresh, and verify the signature on InCommon metadata routinely?

B. Technical Interoperability
    a. Does your application implement SAML2 using the recommended software?
    b. Have you generated your SAML (X.509) certificate using the InCommon security and trust requirements?
    c. Will your application be authenticating users via more than one Identity Provider, either within a single institution or within a Federation?

C. Identifiers and Attributes
    a. Does your application support a relevant portion of the InCommon Attribute Set?
    b. Is your application able to support user identification using at least one of the eduPerson or SAML V2.0 Subject identifiers?
    c. Please specify those minimum attributes that your application requires from its user community?

D. Authorization
    a. Will your application be using authorization to allow or restrict access?
    b. How will your application be authorizing its user population?

E. User Experience
    a. Checklist
        i. Login Experience - Is the login page accessible and easy to find? What's the experience if a user logs in but is not authorized?
        ii. Logout Experience - Does your application support a proper logout? Is the logout page accessible and easy to find?
        iii. User Information - How are the user attributes (UserID, display name, email) exposed, presented, or shared within your application?
        iv. Error Messaging - Are error messages user friendly? (What happened, why it happened, what the user might do to remedy the situation)

Appendix B. Targeted Service Providers

The targeted audience for the 'InCommon Service Provider Onboarding - Criteria Document' and the 'InCommon Service Provider Onboarding - Questionnaire' material include the following class of Service Providers:

1. You are a vendor (commercial or third party), education, or research Service Provider and fall into one of the following categories:
   a. Have not yet joined InCommon but are interested; and need more information on the value adds for joining InCommon and need assistance with meeting the necessary standards and criteria for becoming a operational InCommon member
   b. Have recently joined InCommon and need assistance and/or a jumpstart for getting started and becoming operational
   c. Have been a member of InCommon for quite some time, however need to self-assess and determine whether you are meeting the necessary standards and maximizing the potential of your InCommon partnership

Note: Those SPs that fill out and submit the questionnaire, the questionnaire results could serve as an SP "profile". Which could then be shared with Identity Provider Organizations during engagements, to head of additional questioning and further help streamline integration efforts.

Appendix C. Opportunities to Surface the Questionnaire

With the 'InCommon SP Onboarding - Criteria Document' and the 'InCommon SP Onboarding - Questionnaire', what may be the opportune times to surface this material?

1. During a home institution's RFP (request for proposal) process, the Service Provider (vendor) would be directed to the questionnaire and their response used as part of the institution's vendor evaluation
2. The questionnaire would be encouraged for Service Providers to follow as part of joining InCommon
3. For existing InCommon Service Provider members, site administrators or executives would be encouraged to self-assess and review the criteria on a periodic basis
4. This material could be surfaced on a 'New InCommon Member' landing page

Appendix D. InCommon Service Provider Onboarding - Questionnaire

Quick reference to the InCommon Service Provider Onboarding - Questionnaire

Appendix E. InCommon Service Provider Onboarding - Criteria Document

Quick reference to the InCommon Service Provider Onboarding - Criteria Document