InCommon Service Provider Onboarding - Criteria Document

DRAFT v1, April 2018

Document Title: InCommon Service Provider Onboarding - Criteria Document
Document Repository ID: TI.97.1
DOI: 10.26869/TI.97.1
Persistent URL: http://doi.org/10.26869/TI.97.1
Authors: InCommon Streamlining SP Onboarding Working Group
Publication Date: April 2018
Sponsor: InCommon TAC

Table of Contents

Streamlining SP Onboarding - Criteria Document

A. Establishing Trust

Minimum Criteria:

1. DO register your Service Provider's metadata with the InCommon federation
2. DO define a process for keeping your Service Provider's metadata up to date
3. DO configure your Service Provider to verify the signature on metadata

Recommended Criteria:

1. DO consume and refresh the InCommon metadata at least daily

B. Technical Interoperability

Minimum Criteria:

1. DO use SAML software which fulfills all of the MUSTs in the Kantara SAML v2.0 Implementation Profile for Federation Interoperability
2. DO follow the InCommon security and trust requirements for your SAML certificate(s)

Recommended Criteria:

1. DO implement SAML2 using the InCommon recommended software (all of which meets the requirements of the Kantara SAML v2.0 Implementation Profile for Federation Interoperability)

C. Identifiers and Attributes

Minimum Criteria:

1. DO support the InCommon Attribute Set
2. DO support a varied set of user identifiers
3. DO commit to a stable user identifier (i.e will not be reassigned and has minimal risk of changing) that is only assigned to a single individual (i.e. has the necessary scope to ensure uniqueness and is not shared across multiple individuals)

Recommended Criteria:

1. DO support the InCommon recommendations for user identifier standards (i.e. the eduPerson and the SAML V2.0 Subject Identifier Attributes Profile Version standards)
2. DON'T mistake eduPersonPrincipalName for a valid email address
3. DON'T assume email address can be treated as a unique user identifier (and cannot be released as a unique identifier) without prearrangement with the Identity Provider.

D. Authorization

Recommended Criteria:

1. DON'T assume successful authentication means the user is authorized for the service
2. DO decide on a consistent approach for authorizing user access to your application (for example the eduPerson standard and in particular the eduPersonEntitlement or eduPersonScopedAffiliation attributes)
3. DO be clear about where the allow/deny decision logic is evaluated

E. User Experience

Recommended Criteria:

1. DO provide a consistent user experience for how user information (i.e. attributes) are presented and shared within the application

References

InCommon - Policies (and Practices)
“The documents listed below comprise the policies and practices under which the InCommon Federation and Participants operate.”
https://www.incommon.org/policies.html

InCommon Federation - Participant Operational Practices
Includes questions SPs should be asking themselves along with common terminology
"The purpose of the questions above is to establish a base level of common understanding by making this information available for other Participants to evaluate.
https://www.incommon.org/docs/policies/incommonpop_20080208.pdf

InCommon - Participation Agreement
The criteria entities must meet in order to be a participant in InCommon

InCommon Federation Software Guidelines:
https://www.incommon.org/federation/softguide.html
InCommon Federation Attribute Overview:
https://www.incommon.org/federation/attributes.html
Link to full agreement: https://internet2.app.box.com/v/InCommon-Participation-Agreemt

Federation Participants - Recommended Practices
“In this document the InCommon Federation presents recommendations for federation participants regarding many aspects of federation practice.
https://spaces.internet2.edu/display/InCFederation/Recommended+Practices

Federation Basics
What it means, using high level concepts
https://www.incommon.org/federation/basics.html

CIC Cloud Services Cookbook
“The CIC IdM Working Group launched a project to produce a collection of guidelines that set out best practices and requirements that could be recommended to candidate SaaS vendors.”
https://carmenwiki.osu.edu/display/CICIDM/Cloud+Services+Cookbook+Project

REFEDS Extension of the Cloud Services Cookbook
"As part of the 2016 Workplan (see REF16-3C), the REFEDS community aims to extend the Cookbook so it covers a more global scope."
https://wiki.refeds.org/display/FBP/Cloud+Services+Cookbook

Baseline Expectations - Working Group
“The intent is to improve interoperability among InCommon Participants and ensure that the Federation has a common level of trust by establishing expectations that all Participants agree to meet”
https://spaces.internet2.edu/display/BE/Baseline+Expectations+for+Trust+in+Federation

InCommon Deployment Profile - Working Group
"Develop a Deployment Profile that describes REQUIRED and RECOMMENDED practices for IDPs and SPs operating in the Higher Education and Research community."
https://spaces.internet2.edu/display/DPWG/Deployment+Profile+Working+Group+Home

InCommon Attribute Overview
https://spaces.internet2.edu/display/InCFederation/Supported+Attribute+Summary

SCHAC
"The need of interoperability among different components and the need of exchanging information outside institutional and sometime outside national boundaries have increased awareness of the role that attributes play."
https://wiki.refeds.org/display/STAN/SCHAC

inetOrgPerson
"We define a new object class called inetOrgPerson for use in LDAP and X.500 directory services that extends the X.521 standard organizationalPerson class to meet these needs."
https://www.ipa.go.jp/security/rfc/RFC2798EN.html

SAML2 Int Spec
“This specification standardizes two new SAML Attributes to identify security subjects, as a replacement for long-standing inconsistent practice with the <saml:NameID> and <saml:Attribute> constructs”
https://www.oasis-open.org/committees/download.php/61575/saml-subject-id-attr-v1.0-wd03.pdf