Federation Interoperability Working Group Home

Working Group Agenda/Notes

⚠️ Notes for this Working Group were live-scribed here

Working Group Chair: Walter Hoehn, University of Memphis

Working Group Flywheel: Nick Roy, Internet2

Email List: fed-interop-wg@incommon.org . To subscribe this list, email sympa@incommon.org with the subject line **subscribe fed-interop-wg**

Update: June 6, 2016:

The implementation profile this group created in the fall/spring has been transitioned to the Kantara Federation Interoperability Working Group.

The new home for this work on Github can be found here:

https://github.com/KantaraInitiative/SAMLprofiles/tree/master/edit/fedinterop

A rendered version of the profile can be found here:

https://kantarainitiative.github.io/SAMLprofiles/fedinterop.html

We encourage all who are interested to participate in, or at least monitor the ongoing push toward publishing the profile as a Kantara recommendation. Information about the Kantara FI-WG can be found at: https://kantarainitiative.org/groups/federation-interoperability-work-group/

Update: March 3, 2016:

The group has delivered its final report to the InCommon TAC, available here:

Final Report - Federation Interoperability Working Group 1

A PDF of the SAML Implementation Profile generated by the work of this group is available here:

SAML V2.0 Implementation Profile for Federation Interoperability 20160418.pdf

Access to the repository that contains the asciidoc source for the spec is documented here: Accessing GitLab Repository

Update: February 17, 2016:

The group has concluded the comment period, with no comments external to the group's membership. Finalization of the document and report to the TAC will be prepared shortly.

Update: January 26, 2016:

The group has concluded drafting of the interoperability profile:

http://walterhoehn.com/dl/SAML-Impl-Profile/rendered/main.html

This has been shared on the InCommon Participants, Shibboleth Developers, and REFEDS lists, **for a public comment period lasting through February 15, 2016.** Comments are welcomed at: fed-interop-wg@incommon.org.

Update: October 29, 2015:

The working group is well on its way to having a draft ready for public review. Although not fully "feature complete," and still undergoing heavy revision, much of the "SAML v2.0 Implementation Profile for Federation Interoperability" is in place, and can be seen here:

http://walterhoehn.com/dl/SAML-Impl-Profile/rendered/main.html

This document is updated every 5 minutes from changes pushed to its source control repository by group members, so it's always current.

If you're interested, please take some time to examine the document and provide feedback either by joining and commenting on the mailing list (see subscription info above) or by contacting the flywheel, Nick Roy, at nroy (at) internet2 dot edu.

Problem Statement

When InCommon was created 10+ years ago, it was an explicit goal to keep the bar for membership and operational participation as low as possible. This helped to grow the Federation to its current size. However, this has also hindered interoperation. Members cannot make any real assumptions about policy, practices, and the supported functionality at other member sites when attempting to interoperate. Both IDPs and SPs suffer from this problem. Areas that are affected include:

1. The functionality provided by a SAML implementation (whether open source or commercial)
2. The sites' policies and architectural choices integrated with their SAML implementation of choice
3. The way that a site configures the overall package to operate within InCommon

This Working Group is charged with developing both minimal and best practice statements in order to improve the "interoperate by default" situation.

Stakeholders/Influencers/Influences

Different audiences can impact different aspects of this problem:

1. Companies/software developers who build this software need a list of the required functionality. This should build on existing SAML standards, specifications, InCommon standards/recommendations, and REFEDS/eduGAIN standards/recommendations.
2. Deployers will need a list of functions that they will need to configure/enable in their chosen SAML software, as well as architectural patterns (best practices or guidelines) for integration with services offered in the context of the federation.
3. Campuses will need a list of policy issues/questions and operational practices that promote "interoperate by default" that they will need to address before configuring their SAML software (eg support for R&S, etc). A separate group will develop trustmark related recommendations which will address policies related to IDM practice.

This Working Group will need to develop lists for all three audiences.

Charter

The Federation Interoperability Working Group will:

1. Develop a list of minimal requirements for implementers of SAML software, in order to minimally interoperate within InCommon with a minimum of IDP Admin involvement.
2. Develop a list of minimal requirements for deployers configuring SAML software, and seeking a baseline of interoperability with other InCommon entities.
3. Develop a list of policy issues that promote "interoperate by default" that participants should address as part of the process of deploying an IDP. (are there comparable policy questions for SPs?)
4. Develop a list of Operational Practices that promote "interoperate by default" that deployers should adopt (e.g. responsibilities for user support and incident response, patterns for integrating with existing services or designing new services to work well in the context of federation).
5. Identify which of these requirements could be "tested" if InCommon (or the Internet2 Industry Program) were to deploy a testing framework.

This Working Group is charged with developing the "WHAT" of interoperation in several different areas. Follow on efforts will be charged with developing specific technical recommendations for "HOW" sites can accomplish the WHAT.

This group is encouraged to think in terms of "levels" of compliance in each area (e.g. baseline, better, best).

This group is encouraged to coordinate, as appropriate, with other Federations and via REFEDS.

The group might want to have separate subgroups working on implementation vs deploy requirements.

Note: The InCommon Priorities item also mentions developing a replacement for the POP. The TAC has asked the AAC to approve and begin work on the TrustMark WG Charter that they developed, and to send the resulting report back to the TAC. The TAC will then develop a cover memo and assemble a package of documents to complete the Steering 2015 item.

Membership

Membership in the Working Group is open to all interested parties. Members join the Working Group by subscribing to the mailing list, participating in the phone calls, and otherwise actively engaging in the work of the group.

Version Control Repository

Details for accessing the working group's version control repository are here.

Work Products

1. Sept 2015
    a. An initial list of baseline requirements that a SAML software implementation must meet
    b. An initial list of baseline requirements that deployers of SAML software must meet
2. Dec 2015
    a. A complete, fully specified set of baseline requirements that a SAML software implementation must meet
    b. A complete, fully specified set of baseline requirements that deployers of SAML software must meet
    c. A List of which items can be "tested"
3. ??
    a. A list of "better" requirements that a SAML software implementation must meet
    b. A list of "better" requirements that deployers of SAML software must meet.
    c. Make the encryption certificate in SP metadata optional
    d. Test IdPs for metadata refresh and tag the ones that don't with hide-from-discovery

Related Resources

1. The saml2int Deployment Profile.
2. A list of proposed Changes to saml2int.
3. A Draft IdP Deployment Checklist.
4. A Draft InCommon SAML Implementation Profile
5. Kantara eGovernment Implementation Profile
6. Net+ Guidance for Services
7. CIC Cloud Services Cookbook
8. Kantara Federation Interoperability Working Group - Disposition of Comments on SAML v2.0 Implementation Profile for Federation Interoperability
9. Good Federation Citizenship - IAM Online
10. The Federation Lab SAML Test Suite (git)
11. OASIS SAML2 Wiki
12. Scott's list of OASIS specifications (see below)

    - http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
    - https://wiki.oasis-open.org/security/IdpDiscoSvcProtonProfile
    - https://wiki.oasis-open.org/security/SAML2MetadataIOP
    - https://wiki.oasis-open.org/security/SAML2MetadataAttr
    - https://wiki.oasis-open.org/security/RequestInitProtProf
    - https://wiki.oasis-open.org/security/SAML2MetadataAlgSupport
    - https://wiki.oasis-open.org/security/SAML2MetadataUI
    - https://wiki.oasis-open.org/security/SAML2MetadataDRI
    - https://wiki.oasis-open.org/security/ASLO
    - https://wiki.oasis-open.org/security/SAML2EnhancedClientProfile

See Also

InCommon Working Groups Home