2023 InCommon Technical Advisory Committee Accomplishments

Repository ID: TI.172.1
Persistent URL: http://doi.org/10.26869/TI.172.1

Publication Date: December 1, 2023
Sponsor: InCommon Technical Advisory Committee

Introduction

The theme for this year's InCommon Technical Advisory Committee's work was "future-proofing the federation." We began using these themes a couple of years ago to both help guide our work plan and keep us focused during the year. As such, the thread of future-proofing was very clear in everything we did this year.

In the past, our work plan has been extensive, and we feel that we've done a little work in a lot of areas. This year, we wanted to dive deeper into some specific areas. We chose to approach this year's work plan by dividing the year in half.

The first half of the year was devoted to three overlapping topics: subject identifier adoption plans, SAML 2.0 deployment profile adoption plans, and ReFeds entity category adoption. All of these improve the flexibility and scalability of the federation, making it more valuable now and in the future.

The second half of our year still had progress from the areas started in the first half. We also added some other items that were by that point also ready for our attention: addressing the participation of proxies in the federation and the long-standing need for federation testing.

We also tracked several emerging technologies this year, the most significant of which was browser changes coming about from Fed CM. The progress of Fed CM and how it impacts the future of the federation is obviously an important concern to InCommon and its participants.

The following sections discuss our specific progress in all of these areas -- both what we accomplished and what we hope to see done in the future.

Work Items for 2023

Deploy Access Entity Category & SAML Deployment Profile

A work group was created this year to bring more focus to developing this work. A significant amount of work was completed regarding access entity categories. The group generated a 20-page draft Deployment Guidance for Access Entity Categories document.

This document was presented at TechEx/CAMP 2023 and feedback from the community was solicited.

The draft covers a summary explanation of the REFEDS Access Entity Categories, deployment guidance for both Identity and Service Providers as well as some basic recommendations for the Federation Operator. The bulk of the document includes recommendations for using and deploying specific required attributes for the entity categories including subject-id and pairwise-id. These two attributes are new to the community and the TAC wants to promote proper consideration of these attributes to organizations and push the community away from eduPersonPrincipalName and eduPersonTargetedID to SAML V2.0 Subject Identifier Attributes **[SubjectId]**, otherwise known as subject-id and pairwise-id.

SP Middlethings - Next Step (Federation Proxies)

In early 2022, the InCommon Technical Advisory Committee (TAC) considered a collection of opportunities and threats related to identity federation in research and education for deeper study. Of these, the topic of federation proxies (FPs) rose to the top for the initial study, as they provide great benefits but also have potential challenges, primarily when used for the benefit of service providers (SPs). An *ad hoc* group of community members was convened to study the issue. The group's work in 2022 is described in "Framing a Discussion to Foster SP Middlething Deployments" **[SPMiddlething]**, which was followed by a community discussion at the Internet2 Technology Exchange in December of that year.

In 2023, the group produced its final report to the TAC and the InCommon Steering Group, "Formalizing the Role of Federation Proxies within the InCommon Federation" **[FedProxyFormal]**. The report provided a summary of what the group had learned, as well as a short list of proposed actions. These actions included modifications to the InCommon Federation's governing policies, enhancements of its documentation related to FPs, and consideration of potential adjustments to its cost recovery model.

The TAC is creating a follow-on group to address the proposed actions in 2024.

Federation Testing 2.5

At the end of 2022, the Federation Testing workgroup chose to concentrate future efforts on black box test case development—evaluating an identity provider's or a service provider's ability to interact with fellow federation services according to current good

identity federation practice. Separately, the InCommon Community Trust Assurance Board (CTAB) published a summary report on operationalizing Baseline Expectations in May 2023.

Starting in the latter half of 2023, the Federation Testing workgroup reconvened to compile federation (and inter-federation) standards and practices into a single reference work or index while also reviewing the current state of testing resources. The workgroup identified several gaps while conducting this analysis. Most extant testing resources are operated by identity federations only for member identity providers. Few testing tools are generally accessible, and only one resource—a reference Shibboleth IdP deployment—supports service providers. Service providers have very different skill sets and operational focuses compared to identity providers. They cannot reasonably deploy their own feature-complete reference IdPs for verification and validation purposes while also developing and operating their services. Additionally, the global research and education community does not have consensus on what constitutes good identity federation practice. Opinionated guidance and complete, working reference implementations do not exist. These gaps affect identity federation scaling by impeding the communication and execution of meaningful, cross-organizational changes to federation operations and the global research and education identity trust fabric.

The Federation Testing workgroup sees two immediate needs arising from this analysis. First, the InCommon Federation needs a "Federation Readiness Check" IdP to facilitate service provider onboarding, ideally available to the general public. Second, the InCommon Federation needs a clear definition of current good identity federation practice beyond the minimum expressed by Baseline Expectations. These needs will drive the next iteration of the workgroup in the 2024 TAC Work Plan.

Browser Technology Changes

Judith Bush reported on the work being done by the community and then by the REFEDS Browser Changes working group. A "Hackathon" that was more of a Summit was held in Mountain View, CA with representation from InCommon and InCommon members as well as the global community, establishing a relationship with representatives from Mozilla Firefox and Google Chrome.

Initial enthusiasm gave way to some frustration as the direction of the FedCM work consistently prioritized the needs for IdPs that relied on third party cookies. A spring Internet Identity Workshop side meeting proposed a model that was barely adequate, but still supported a SP initiated flow where intermediaries could be discovered and consent granted. Later additions required establishing IdP status with the browser, which means

that federation proxies or IdP proxies have to be introduced to the browser before any cross-site SP that depends on the proxy can redirect the user to that proxy.

Continued engagement with the FedCM community group, drafting a working group charter, and attending other W3C meetings has put a time demand on community members. The state of the work was presented at TechEx. The sense of the community was that we must continue to engage, not in that we believe the current direction will support the ecosystem we currently have, but so that we can identify a next generation solution. The FedCM solution seems unlikely to ever support the complexities of the interactions needed to support research and collaboration needs. Back channel interoperations and other trusted credential exchanges may be needed. The FedCM API may be part of some front channel exchanges, but cannot itself support community needs.

References

[SubjectId] SAML V2.0 Subject Identifier Attributes Profile Version 1.0, https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.pdf

[SPMiddlething] Framing a Discussion to Foster SP Middlething Deployments, http://doi.org/10.26869/TI.168.1

[FedProxyFormal] Formalizing the Role of Federation Proxies within the InCommon Federation, http://doi.org/10.26869/TI.169.1