2021 InCommon Technical Advisory Committee Accomplishments

Repository ID: TI.164.1
Persistent URL: https://doi.org/10.26869/TI.164.1
Publication Date: February 10, 2022
Sponsor: InCommon Technical Advisory Committee

Introduction

The InCommon Technical Advisory Committee moved several large items forward in 2021 and laid the groundwork for future efforts. These included, among other things, planning a roadmap to adopt the SAML 2.0 deployment profile, plans for a federation testing working group, and collaboration with Seamless Access. The TAC also had a successful engagement with the Educause Higher Education Information Security Council to make important federation-related updates to the HECVAT. The committee also created recommendations to InCommon for the future of InCommon's IdP discovery service which will be wrapped up and sent forward in 2022. The following sections provide details on each area of focus from the TAC's 2021 accomplishments.

Adopt SAML Deployment Profile

In 2018, the InCommon Deployment Profile working group completed a rewrite of SAML2int, the SAML 2.0 interoperability deployment profile. This profile was approved by InCommon and ratified by Kantara in 2019. In 2021, a subgroup of the InCommon TAC developed a roadmap for InCommon and its members adopting relevant requirements from the profile. The subgroup consisted of Judith Bush (OCLC), Mark Rank (Cirrus Identity), Albert Wu (Internet2), and Keith Wessel (University of Illinois at Urbana-Champaign).

This was a multi-month effort that began with identifying which profile items were relevant to InCommon and its members. Items were then grouped into those which were already in practice, could be deployed in the short-term, and could be deployed in the long term. The group also identified which items were testable as well as which could be enforced.

The roadmap was published on the InCommon wiki. The group intends this page to be a reference for the community to track the adoption of the profile over time and know what's happening next and when. TAC and InCommon will need to address specifically when and how each item on teh roadmap will be put into place.

The group did not address topics around subject identifiers (see below) or SAML logout. Those proved to be complex items that deserved separate attention.

Subject Identifier

In 2018, OASIS published the SAML 2.0 subject identifier attributes profile, a companion work to the SAML 2.0 interoperability deployment profile. This profile introduces new SAML identifiers. The TAC recognized that migrating the community to new subject identifiers would be a large, multi-year effort and that addressing some smaller items in the deployment profile first would give a more immediate return. Albert Wu (Internet2) with assistance from the TAC produced some internal documents to help explain the value to the community of migrating to these new identifiers as well as a high-level roadmap for the migration. The early steps of the migration are reflected in the SAML2int roadmap referenced above. Additional communications and execution of these plans will be left to the TAC in future years.

Federation Testing

Problem statement: The InCommon community has been asking for an easier, more tangible way to validate that services planning to integrate with the Federation will interoperate seamlessly. In particular, a federation test environment has long been a frequently requested feature.

InCommon is looking to this working group to produce a set of prioritized, actionable requirements for a federation test environment. This would include describing the user stories for the user of a test federation and drafting the requirements.

The TAC believes having a test Federation that would demonstrate integration issues before having services and identity providers going live would make federating easier and more predictable.

Initial outreach at CAMP and ACAMP and over mailing lists has not turned up any people willing to work on the project outside of the TAC. Some creative outreach and new working group patterns may be needed for this project.

SeamlessAccess

SeamlessAccess is a freely available IdP discovery service, designed using the information found in NISO's "Recommended Practices for Improved Access to Institutionally-Provided Information Resources: Results from the Resource Access in the 21st Century (RA21) Project". This service breaks IdP Discovery into two discrete and separable components:

the search and discovery of IdPs, and the persistence of a user's choice of IdP in their browser local storage. SeamlessAccess can be used by any entity that offers IdP discovery services, from SPs to federations themselves.

InCommon is looking to the TAC for guidance on if and how InCommon should incorporate SeamlessAccess as the default IdP discovery service for InCommon. The community needs to come to consensus on how the federation runs discovery services.

Promoting SeamlessAccess within InCommon by using SeamlessAccess itself for InCommon's WAYF; Describe the potential user stories that will help us to determine requirements and priorities; Decide on project requirements from InCommon; branding; IdP filtering; Decide on whether there should be a single WAYF offered by the federation, or encourage individual SP implementations.

Over the course of 2021, the TAC had several active touchpoints with the SeamlessAccess efforts, including Ann West (Internet2) who remains active on the SeamlessAccess Governance Committee, Albert Wu (Internet2) who remains active on the SeamlessAccess Operations Committee, and Heather Flanagan (TAC vice-chair, Spherical Cow Consulting) who held the position of Technical Liaison for SeamlessAccess. The TAC also drafted a white paper for InCommon Steering with recommendations regarding SeamlessAccess as a replacement for the existing InCommon discovery Service. That white paper will be shared with InCommon Steering in Q1 2022.

Browser Technology Changes

Protecting the security and privacy of users as they engage with the web is necessary from both a moral and a legal perspective. Unfortunately, while the goal of a privacy-preserving web is easy to say, it is much harder to implement when one takes into account the wildly varied requirements of different stakeholder groups.

On the one hand, an entire commercial ecosystem of third-party vendors is built on their ability to track individual users as they browse the web, collecting information on their interests and purchases with the goal of more effectively selling those individuals' specific products or ideas. They do this via third-party cookies, link decorations, and other low-level primitives. By blocking those primitives, cross-site tracking is no longer a viable option, and user privacy is protected.

On the other hand, those low-level primitives are also used by federated single sign-on (SSO) services. In the enterprise and in higher education, for example, services have a

business need to allow a user's authentication and authorization information to flow from one site to the next. Whether the protocol used is OIDC or SAML, information is stored in the browser about where a user comes from, and that information must be read by multiple parties.

InCommon needs eyes on this space, as there will be direct technical impact on the functioning of multilateral federations.

InCommon TAC has received regular updates from the liaison assigned to this effort, Heather Flanagan (TAC vice-chair, Spherical Cow Consulting). The immediate impact to federation services will be low, as the first area of change involves third-party cookies. Those are not used by SAML. As the work evolves, however, to touch on changes in link decoration and redirects, SAML-based services will definitely be impacted. While there are no guidelines or standards yet that would allow InCommon SPs and IdPs to prepare, the TAC will continue to monitor the effort as to capture and share that guidance as soon as it becomes available.

EDUCAUSE Federation Observations

EDUCAUSE operates a Proxy in front of several services for EDUCAUSE members. This proxy leverages 250+ InC identity providers to enable access. During the first 18 months of operation, EDUCAUSE, in conjunction with Cirrus Identity, have observed several recurring issues with InC IdPs operating in the field. The objective of this work effort is to raise awareness of these items and consider them where appropriate to support TAC work. Mark Rank (Cirrus Identity) has offered data from these findings to InCommon to assist in ongoing efforts. Some of the observations include:

- InC Organizations change their IdP and in the process register under a new entityID
- InC IdPs assert they support R&S attribute release, but do not
- An InC organization will attempt to register an ADFS IdP but will statically configure SP metadata and will not load metadata changes made by SP until something breaks
- IdPs releasing attributes that should have a scope without a scope (for example eduPersonPrincipalName, eduPersonScopedAffiliation)
- An InC organization has a name-based identifier that can change, thus breaking federated access to the service

The TAC believes that data from Educause and Cirrus Identity will be of use to the Federation Testing working group and will continue to keep this data in mind for other uses surrounding federation best practices and procedures. federation

Assurance

Several groups (CTAB, REFEDS) have focused community efforts around assurance. The National Institute of Health (NIH) is calling on InCommon Participants to support REFEDS Assurance Framework, REFEDS MFA Profile, and REFEDS Research & Scholarship (R&S) category in order to facilitate federated, secure access to NIH online resources. This call to action has more than doubled support for MFA Profile and R&S among InCommon Participants. At the same time, the increased activities have also raised technical and operational questions. REFEDS has updated MFA Profile support documentation and is working to update all three specifications in response to community feedback. CTAB has produced implementation guidance for the REFEDS Assurance Framework.

TAC continues to closely monitor these efforts and is ready to help support wider adoptions of these assurance standards among Participants.

HECVAT

Starting in 2020, a recurring TAC discussion was how to assess (and improve) vendor implementations of single sign-on technologies in general as well as the InCommon federation baseline expectations. In 2021, the opportunity to present feedback on the EDUCAUSE Higher Education Information Security Council's (HEISC) Higher Education Community Vendor Assessment Toolkit (HECVAT) presented itself. Representatives of the TAC met with representatives of HEISC and provided suggested edits which were incorporated to version 3.0 of both their "HECVAT FULL" and "HECVAT LITE" templates.

This effort is expected to reduce the pre-purchase evaluation and integration efforts of organizations that are members of InCommon (or those following the best practices and baseline expectations published by InCommon) who leverage the HECVAT during their procurement processes. It is expected that HEISC and TAC representatives will check in at least annually to ensure that feedback and other changes continue to be incorporated into future HECVAT updates.

https://er.educause.edu/articles/2021/10/hecvat-3-0-launches-to-outer-space