2022 InCommon Technical Advisory Committee Accomplishments

Repository ID: TI.165.1
Persistent URL: http://doi.org/10.26869/TI.165.1
Publication Date: mmmm dd, yyyy
Sponsor: InCommon Technical Advisory Committee

Introduction

It was a very busy and productive year for the InCommon Technical Advisory Committee. Our work centered around two areas: making federation easier, and the future of federation. The committee already had a full and ambitious work plan at the start of the year, and several additional and time-sensitive items came up during the year to add to the work. As a result, the group made considerable progress on a number of fronts, but nothing can really be considered done. As the committee looked ahead at 2023, we considered all of the current items to be good candidates to continue in the year ahead.

"Making federation easier" has been a theme for the Technical Advisory Committee for the past couple of years. Items in this area focused on simplifying the process of deploying service providers and identity providers that can interoperate with the federation with minimal effort or configuration. Notably, our work adopting the SAML 2.0 deployment profile and new SAML subject identifiers along with creating federating testing all work toward this goal. The TAC also continues to keep an eye on the HECVAT and how it can be used to simplify and improve federated services.

In the area of "the future of federation", the committee tracked several standing items this year such as upcoming browser technology changes which will very definitely impact federation in the near future, the challenge of integrating SP "middlethings" into the federation properly, and policies around entity IDs. During the latter half of the year, we also spent a lot of time understanding the impact of digital wallets and verifiable credentials and how they fit into federation. The following sections detail our progress on each of the year's work plan items.

Work Items for 2022

Adopt SAML Deployment Profile - Next Steps

In Fall 2021, the InCommon Steering Committee endorsed TAC's recommendation for InCommon to formally adopt the SAML Deployment Profile for Federation Interoperability. **[AdoptSAML2Int]**

The published roadmap wiki page served as a central point of reference throughout the multi-year process of profile adoption. TAC convened a sub-group in the first half of 2022 to identify next steps for Deployment Profile adoption and what that looked like in terms of specific federation and participant changes. The group drafted a value statement to be included on that page and initial communications to explain why these changes are being made. The hope is to merge this work into other InCommon changes in the near future. The initial steps are ready to go; it just needs to be decided when to start.

Subject Identifier

This work is part of the SAML 2.0 profile adoption. Migrating from one set of identifiers to another is obviously no small task. This is definitely a multi-year initiative. It has to start somewhere, though. Starting back in 2020 and continuing into this year, the TAC has developed a staged roll-out of the new subject identifiers. This work is part of the schedule for SAML 2.0 deployment profile adoption and will probably start in the near future.

Federation Testing

In 2021, in response to community interest for an easier, more tangible way to validate a service's Federation interoperability, TAC attempted to convene a community working group to develop testing requirements. We learned that although many welcomed such testing solutions, few volunteered to develop their requirements.

In 2022, TAC changed its approach and tasked an internal group to examine the topic. The group discussed different models and goals of testing: are we building technical/policy compliance tests, or is it more meaningful to have helpful diagnostic tools to help participants evaluate their services' ability to successfully interoperate in Federation?

The group converged on being helpful: concentrate efforts to develop blackbox testing cases to observe a service (IdP or SP)'s behavior from the outside to evaluate its ability to interact with fellow federation services according to the behaviors defined in federation standards.

As of the end of 2022, we have models for how testing specifications can be provided. Continued work is needed to develop additional cases.

Finally, the group had focused primarily on behaviors described in the SAML Deployment Profile (SAML2Int). The group recognizes that there are additional criterias important to successful Federation interoperation that are not included in the SAML2Int profile. More work will be needed to develop testing requirements in those areas.

The Future of Federations and Digital Wallets

While the goal of a working group did not gain traction, both TAC and CACTI enjoyed many discussions on the topics. Two guests speakers were brought in to bring new perspectives to the discussion: Kerri Lemoie, PhD, Director of Technology, Digital Credentials Consortium, and Niels van Dijk, Technical Project Manager for Trust and Security at SURF. The TAC will continue to give this topic attention as we consider how best to advise InCommon on the next steps associated with evolving with this new technology.

Related: TAC Meeting minutes from October 6, 2022 (Niels' presentation) **[20221006]**

Standing Items

Browser Technology Changes

Heather Flanagan, Vice-Chair for TAC, provided regular reports on the state of changes being made to web browsers that will impact federated authentication services. These reports culminated in a flurry of activity during the Internet2 TechEx in December 2022 (related: TechEx session on Browser Technology changes **[Browser]**). The global community is collaborating to put together a hackathon that will provide concrete feedback to the key browser effort in this space, the FedCM API.

The efforts in this space will ramp up significantly in 2023.

HECVAT v.next

The HECVAT team performs major revisions of the HECVAT template on a two-year cycle, placing major revisions in 2021 and 2023. Activities during 2022 were minimal, primarily focused on checking for time-critical feedback or questions from the last major release. In 2023, the HECVAT team is discussing a larger overhaul of the format that will require input on the usage of the tool as well as a focused review of the IAM related questions.

Guidance for EntityID creation, change, and use.

When registering a service, the InCommon Federation enforces several validation rules to ensure a service's SAML metadata's entity ID (the unique system identifier for that service, or entity). In addition to meeting syntax and uniqueness requirements described in SAML specification, InCommon enforces additional restrictions not defined in SAML in an attempt to further safeguard the "quality" of an entity ID. These additional rules include limiting an entity ID to be formatted as a universal resource locator (URL), whereas SAML allows any universal resource identifier, which can be a URL or a universal resource name, or URN. InCommon also performs domain control validation on a domain used in an entity ID.

InCommon Participants are increasingly adopting cloud-based, commercial IAM solutions. These solutions often issue programmatically assigned, non-customizable SAML entity IDs under the vendor's domain, These IDs meet SAML specifications requirements, but cannot meet InCommon's proof of domain control requirements.

In 2022, InCommon operations introduced a proposal to amend its entity ID validation procedure to better align with the increased use of commercial solutions while continuing to maintain the quality of data, including the entity ID, registered in InCommon. TAC reviewed the proposal (**[20220606]**; TAC Minutes June 2, 2022) and subsequently concluded to endorsed moving forward with implementations (Option 1 described in TAC Minutes July 28, 2022 **[20220728]**; recording of consensus and signal of additional discussions in Standing Items #3 in TAC Minutes August 11, 2022 **[20220811]**).

SP Middlethings

The architecture of today's R&E federations presumes a secure end-to-end communication channel between Identity Providers (IdPs) and Service Providers (SPs). Over time, multiple use cases have arisen requiring (automated) mediation of that communication. This mediator breaks the assumption of the end-to-end channel. Reasons for this mediation include protocol translation, enhancement and/or transformation of the information exchanged, managing the complexity of interacting within a multilateral federation when doing so within the SP is not possible or undermines its function, or aggregation of common applications and data sets into a single service for commonality of the user interface or the technical architecture.

In the Summer of 2022, the InCommon Technical Advisory Committee formed an ad hoc group to study the potential impacts of this mediation on federation policy, privacy, transparency, usability, and technical architecture. The intent was to answer this question: is it necessary or critical for InCommon to update its trust model and operating practices to account for these evolutions to continue to ensure trust, transparency, good user experience, and streamlined access?

The group developed a draft document **[SPMiddlething]** to set context and to stimulate more involved discussions at the 2022 TechEx conference. The topic was presented during TechEx (**[RiseOfMiddlething]**; presentation slides). A related presentation (presentation slides; **[SNCTFI]**) also took place during the FIM4R meeting, co-hosted with TechEx). The presentations led to subsequent ACAMP session discussions.

The group is reconvening in early 2023 and will incorporate feedback and lessons learned from the conference in its final report.

References

[AdoptSAML2Int] InCommon adopts the SAML 2.0 Deployment Profile for Federation Interoperability, https://spaces.at.internet2.edu/display/federation/adopt-saml-deployment-profile

[Browser] TechEx2022 Presentation: The Web is for Everyone, Sort of. How changes in the consumer web impact academia, https://internet2.edu/wp-content/uploads/2022/12/techex22-IAM-The-Web-Is-for-Everyone-flanagan.pdf

[20220606] TAC Meeting minutes from June 6, 2022, https://spaces.at.internet2.edu/display/inctac/InCommon+TAC+Meeting+2022-06-02

[20220728] TAC Meeting minutes from July 28, 2022, https://spaces.at.internet2.edu/display/inctac/InCommon+TAC+Meeting+2022-07-28

[20220811] TAC Meeting minutes from August 11, 2022, https://spaces.at.internet2.edu/display/inctac/InCommon+TAC+Meeting+2022-08-11

[20221006] TAC Meeting minutes from October 6, 2022 (with link to Niels' presentation), https://spaces.at.internet2.edu/display/inctac/InCommon+TAC+Meeting+2022-10-06

[SPMiddlething] Framing a Discussion to Foster SP Middlething Deployments, https://docs.google.com/document/d/1RwWn2oXJqa3YwFF_vKuTsqoJkLQ7BJ9hYFOUStbJ1IY/edit#heading=h.o4axeamjc10h

[RiseOfMiddlething] TechEx 2022 Presentation: The Rise of Middlethings, https://internet2.edu/wp-content/uploads/2022/12/techex22-IAM-Rise-of-Middlethings-Wu.pdf

[SNCTFI] FIM4R (at TechEx 2022) Presenation: Snctfi: Scalable Negotiator for a Community Trust Framework in Federated Infrastructures, https://indico.cern.ch/event/1202335/contributions/5149516/attachments/2559953/4412209/Kelsey4dec22-snctfi.pdf