InCommon TAC 2023 Work Plan Items

Working Document

In an effort to make progress on the TAC Work Item Planning, please look at the topics below and add your thoughts or comments. **You might indicate:**

- What work needs to be done
- How TAC should approach the item - e.g. WG, Survey, Collaboration with REFEDS, Webinar
- What might be in a Charter (if WG seems to be a possibility, what you would expect to accomplish - just a few bullets) - more detail, outcomes, deliverables will created once TAC decides to sponsor a WG
- Either enter a specific Suggestion or Action Item, +1 another's entry, or add a comment on what's there
- Add suggestions to approach - e.g. collaborate with REFEDS, Spin up TAC WG, etc.
- **SIGN UP for projects you're interested in [NEW]**

Theme for 2023: Future-proofing InCommon

InCommon is a community-driven organization that aims to advance education and research by providing secure and easy-to-use identity and access management services. Our mission: to foster collaboration and trust among institutions, to promote the use of common standards for identity and access management, and to improve the security and efficiency of online interactions among members of the education and research communities.

Where (high level, thematic topic(s)) should TAC focus to help InCommon to continue to meet its mission?

This should guide the thinking, descriptions, goals, and milestones for the suggested work plan items

</>

Active 2023 Work Plan Items

1. Adopt SAML Deployment Profile & Subject Identifiers

Description

Develop implementation guidance; promote adoption; etc.

Proposed By

Mark Rank

Format, Requirements, Duration

This should be a TAC subgroup consisting of select TAC members and possibly additional community volunteers.

Expected work output include:

- **Release the value statement -** Finish edits for value statement, bring to TAC
- **Develop implementation guide / publish support documentation**

    - Create more detailed implementation/migration/configuration guidance: strategy, change mgmt / migration techniques;
    - Publish guidance as support documentation;Create more detailed implementation/migration/configuration guidance: strategy, change mgmt / migration techniques;
    - Publish guidance as support documentation;
- **Set adoption timeline and expectation**

+1's

- Steven Premeau
- Joanne Boomer

Notes

None.

✧ ✧ ✧ ✧ ✧ ✧ ✧

2. Anonymous, Pseudonymous, and Personalized Entity Categories - What does InCommon do with them?

Description

REFEDS will soon release the latest set of entity categories designed to further standardize/streamline attribute release among federation participants. InCommon has received requests to support these categories.

Draft versions of these documents are available:

- Entity Category Consultation: Anonymous Access
- Entity Category Consultation: Pseudonymous Access
- Entity Category Consultation: Personalized Access

While the effort to update Federation tooling (Federation Manager) to support these categories is minimal, there are potentially significant deployment implications among Participants before these categories will enjoy wide adoption.

We are seeking TAC's input to identify challenges and opportunities for our community in supporting the use of these categories and to help craft a deployment roadmap. Some of the questions include (but definitely not limited to):

- How does an SP make use of one or more of these categories? When is it appropriate?
- How does an IdP support one or more of these categories?
- What does "support" mean for InCommon? How do we measure success?
- Portions of these categories have dependencies. For example, where a user identifier is required, it needs to be a SAML subject-id or pairwise-id. What kind of guidance do we provide to the community when making a transition?
- Personalized Access category in theory will replace R&S over time. What does that mean? How do we do it as a community?

Proposed By

Joanne Boomer

Format, Requirements, Duration

TAC should convene a subgroup with limited scope

There is interest for CTAB as well; possibly enlist CTAB participation re: enhancing interoperability & trust.

Expected Deliverables:

- **Write up how R&S can be replaced by personalized, how federation membership provides guardrails around release of data** - The personalized entity category expresses the need/desire/use of data without the cross federation confusion about what constitutes R&S; attempt to ameliorate concern about releasing the attributes
- **Work with eduGAIN to determine when they would accept the entity categories -** Maybe they do know, i dunno. *blush* https://technical.edugain.org/documents

TAC should convene this group ASAP; work should last 9? months?

+1's

- Judith Bush
- Albert Wu
- Steven Premeau

Notes

None

✧ ✧ ✧ ✧ ✧ ✧ ✧

Candidate Work Plan Items

These items are candidate TAC work plan items. TAC will review each and schedule them to start as active workplan items complete in 2023.

3. SP Middlethings - Next Steps

Description

This is a placeholder for follow-on work from the 2022 SP Middlethings group.

Background

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?

Status

The 2022 group is wrapping up its report (Framing a Discussion to Foster SP Middlething Deployments). This item serves as a work plan placeholder to remind TAC to revisit this subject in midyear 2023 and if applicable, to charter follow-on work from the 2022 group's report.

Proposed By

Albert Wu

Format, Requirements, Duration

The 2022 group is still wrapping up its report. Hold this item pending the 2022 group report; revisit in mid 2023 to determine whether any work needs to spin up in the second half of 2023

+1's

- Mark Rank
- Derek Eiler

Notes

[Derek] Don't know what all would fall under this category, but having just recently worked through some middlething confusion, I think it's an area that could benefit from some clarity, even if TAC simply recommends that middlething providers publish a barebones practice statement of some sort. Maybe this is more appropriate for REFEDS though. Personal context: an SP relied on a middlething, which used another middlething, which used InCommon... and somewhere in the process a middlething's discovery service filtered out 2/3 of our IdPs because they filter R&S entities by InCommon member display name, rather than by individual IdPs.

✧ ✧ ✧ ✧ ✧ ✧ ✧

4. Federation Testing - continued

Description

This is a continuation of the 2022 TAC sub group: to develop testing requirements for Federation testing. In 2022, 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: concentrating 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.

We’d like to continue work to flesh out these use cases.

Proposed By

<todo:proposer>List the name(s) of TAC members proposing this item.</>

Format, Requirements, Duration

<todo:proposer>

Suggest working format, e.g., community working group, sub-group, liaison efforts, etc

Describe expected deliverable, e.g., report, survey, etc.

Suggest work item duration, expected start and end date, note any timing constraints, etc.

</>

+1’s

- Derek

Notes

Todo: link to the git repo containing work from 2022.

✧ ✧ ✧ ✧ ✧ ✧ ✧

Additional Items TAC to Track

Items TAC will monitor, track, observe, participate, and react when appropriate.

5. The Future of Federations and Digital Wallets

Description

A joint working group between TAC and CACTI to discuss how digital wallets might impact the future of identity federations.

Proposed By

Judith Bush

Format, Requirements, Duration

TAC to elect participation roster.

Activities include:

- Provide feedback on FedCM API
- Develop a list of IAM Online sessions for presentations
    - Types of assertions and controls and trust - when are claims just trusted by the wallet RP, when might backchannel verification happen
    - Compare and contrast different wallets (crypto vs google/apple vs EU vs MIT's credentials)

+1's

- Mark Rank

Notes

None.

✧ ✧ ✧ ✧ ✧ ✧ ✧

6. NIST 800-63-4 Consultation - Review and Feedback

Description

NIST is requesting comments on the draft fourth revision to the four-volume suite of Special Publication 800-63, Digital Identity Guidelines. This publication presents the process and technical requirements for meeting the digital identity management assurance levels specified in each volume. They also provide considerations for enhancing privacy, equity, and usability of digital identity solutions and technology.

Link: SP 800-63-4 (Draft), Digital Identity Guidelines | CSRC

The comments are due on March 24, 2023. NIST guidelines underpin much of US agencies and research infrastructure's identity and access requirements. To ensure the InCommon community can continue to support federated access to these research and education resources, it is critical that InCommon reviews and provide insightful response to these updates.

We are seeking a joint effort from key InCommon community representatives (CTAB, TAC, others?) to review these documents and to compose a coordinated response on InCommon's behalf.

Proposed By

Albert Wu

Format, Requirements, Duration

TAC is requesting committee volunteers to participate in a cross-committee group to review and draft a consolidated response on behalf of InCommon to NIST's request for comment on NIST-800-64 Rev 4.

The group should compose its response by the end of February 2023 so that InCommon leadership (Steering, Kevin/Ann etc) has sufficient time to review the material before submission.

Comment submission is due by March 24, 2023.

+1's

- (from CTAB) Tom Barton

- Albert Wu
- Judith Bush
- Eric Goodman
- Joanne Boomer
- Keith Wessel

Notes

- NIST 800-63-4 documents

✧ ✧ ✧ ✧ ✧ ✧ ✧

Description

NIST is requesting comments on the draft fourth revision to the four-volume suite of Special Publication 800-63, Digital Identity Guidelines. This publication presents the process and technical requirements for meeting the digital identity management assurance levels specified in each volume. They also provide considerations for enhancing privacy, equity, and usability of digital identity solutions and technology.

Link: SP 800-63-4 (Draft), Digital Identity Guidelines | CSRC

The comments are due on March 24, 2023. NIST guidelines underpin much of US agencies and research infrastructure's identity and access requirements. To ensure the InCommon community can continue to support federated access to these research and education resources, it is critical that InCommon reviews and provide insightful response to these updates.

We are seeking a joint effort from key InCommon community representatives (CTAB, TAC, others?) to review these documents and to compose a coordinated response on InCommon's behalf.

Proposed By

Albert Wu

Format, Requirements, Duration

TAC is requesting committee volunteers to participate in a cross-committee group to review and draft a consolidated response on behalf of InCommon to NIST's request for comment on NIST-800-64 Rev 4.

The group should compose its response by the end of February 2023 so that InCommon leadership (Steering, Kevin/Ann etc) has sufficient time to review the material before submission.

Comment submission is due by March 24, 2023.

+1's

- (from CTAB) Tom Barton
- Albert Wu
- Judith Bush
- Eric Goodman
- Joanne Boomer
- Keith Wessel

Notes

- NIST 800-63-4 documents

✧ ✧ ✧ ✧ ✧ ✧ ✧

7. Browser Changes (user tracking) and impact on Federation

Description

<todo:proposer />

Status / Notes

None.

8. Next Steps with HECVAT: How will TAC be involved in its ongoing evolution/keeping?

Description

Working group(s) involving Higher Education Information Security Council (HEISC) and TAC to propose, discuss, and review changes for the next HECVAT release.

Proposed By

Steven Premeau

Format, Requirements, Duration

TAC form subgroup of volunteer(s) and connect with HEISC representatives.

History

- 2022 TAC Work Plan Working Document
- 2021 TAC Work Plan Working Document
- 2019 TAC Work Plan Working Document
- 2017 TAC Work Plan Working Document