InCommon TAC 2021 Work Plan

InCommon TAC 2021 Work Plan

This is final version of the InCommon Technical Advisory Committee's 2021 work plan. The TAC provides recommendations related to the technical operation and management of InCommon. The work plan outlines the proposed technical priorities, particularly for the InCommon Federation.

If you have a new work item to propose, please copy the Template below and paste at the bottom of the work items, filling in a title and brief high-level description.

Alternatively, if you would like to comment on any of the existing items, please add a comment to the wiki page. *Note that you need to sign into Confluence in order to edit or leave a comment.*Lastly, if you have a work item you'd like to propose but aren't comfortable using the wiki editor, enter it in the comments at the bottom of the page.

The TAC's 2021 work plan is a synergistic portfolio of items with two overarching themes:

1. **Making federation easier:** Lowering the barriers to getting on the federation highway for institutions that are unable or unwilling to run their own IdPs and for SPs wanting to join InCommon
2. **Increasing the value of participating in InCommon:** Increasing value proposition by thinking which wants and needs are valuable to the most people. This means solving the business case to maximize investments.

2021 Work Plan Items

- Adopt SAML Deployment Profile
- Subject Identifier
- Federation Testing
- SeamlessAccess
- Browser Technology Changes
- EDUCAUSE Federation Observations
- Assurance
- HECVAT

(Working document of this work plan in Google Doc)

Adopt SAML Deployment Profile

Evaluate the Kantara SAML2 Deployment Profile; produce recommendations on which/how/when InCommon should adopt elements of the SAML2 Deployment Profile:

- Which statements should be immediately required?
- Which should be required in near term (allow time for transition)
- Which should be considered for longer term requirements
- Which should remain best practice (e.g., they are not federation-related)
- Which needs update/amendment?
- How does this relate to Baseline?

Link to related materials

- Final Report of the Deployment Profile Working Group
- Responses from the DPWG recommendations survey
- [Part1] SAML2Int Adoption Analysis - Common Requirements
- [Part2] SAML2Int Adoption Analysis - Service Provider Requirements
- [Part3] SAML2Int Adoption Analysis - Identity Provider Requirements

Suggestion/Action Item	Submitter	Description	+1s

Task group to analyze profile and drafting recommendation for TAC review/adoption	Keith W		Albert W Judith B Mark R Steve P Janemarie
Consider R&E layer profile	Keith W		
What type of work is expected? Working Group, Liaison Efforts, Other?		Existing subgroup	
TAC Sponsor(s)/Champion(s)		Keith Wessel	

Subject Identifier

Develop rationale and recommendations regarding adoption of SAML Subject Identifier Attributes Profile across InCommon; recommend implementation and transition strategy.

Link to related materials

- OASIS Committee Specification, SAMLV2.0 Subject Identifier Attributes Profile Version 1.0, January 2019
- Comparison of identifiers used in Federation
- Strategies for Working with Identifiers in Federation (working draft)
- Next Step on Identifiers (Deploying SAML Subject Identifiers in InCommon) (working draft)

Suggestion/Action Item	**Submitter**	**Description**	**+1s**
			Steven Premeau
Complete the Strategies for Working with Identifiers in Federation document			Mary McKee Judith Bush Janemarie Duh
Flesh out the Deploy SAML Subject Identifier in InCommon plan			Mary McKee Judith Bush Janemarie Duh
What type of work is expected? Working Group, Liaison Efforts, Other?		Working Group Consider instead a subgroup that will watch the space and gather the data about where things are going. Outcome would be a set of requirements/recommendations and a proposed charter or report for next steps	
TAC Sponsor(s)/Champion(s)		Mark Rank (tend)	

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.

Link to related materials

- Federation Testing ACAMP Session
- Proposed WG Charter
- Fedlab
- (Canadian Access Federation is also developing testing tool. No link yet)

Suggestion/Action Item	**Submitter**	**Description**	**+1s**
Describe user stories for the user of a test federation			Matt B Judith Bush
Draft requirements			Janemarie Duh
What type of work is expected? Working Group, Liaison Efforts, Other?		Working Group	

TAC Sponsor(s)/Champion(s)	Janemarie Duh

SeamlessAccess

Problem description: 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". T his 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.

Link to related materials

- SeamlessAccess UX Documentation
- Code Repositories
- Code Documentation
    - thiss-ds-js: A set of clients for the discovery service. Can be used to implement a DS connected to a central persistence service.
    - thiss-jquery-plugin: A jQuery plugin for building search-based identity selectors.
    - this-mdq: An implementation of the metadata query protocol (MDQ) for JSON metadata only.

Suggestion/Action Item	Submitter	Description	+1s
Promoting SeamlessAccess within InCommon by using SeamlessAccess itself for InCommon's WAYF.			Janemarie
Describe the potential user stories that will help us to determine requirements and priorities.			
Decide on project requirements from InCommon • branding • IdP filtering			Mary McKee Janemarie
Decide on whether there should be a single WAYF offered by the federation, or encourage individual SP implementations.			Mary McKee Janemarie
What type of work is expected? Working Group, Liaison Efforts, Other?		Subcommittee with community consultation	
TAC Sponsor(s)/Champion(s)		Heather Flanagan	

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 to the functioning of multilateral federations.

Link to related materials

- https://bitbucket.org/openid/connect/wiki/Browser%20Interactions%20Special%20Topics%20Call
- Internet2 Slack channel: #inc-browsers-and-sso

Suggestion/Action Item	Submitter	Description	+1s

Lightweight tracking, reporting through the Slack channel.	Heather Flanagan	Hold for working group creation until 2022 (or something urgent happens)	Mark Rank Matt B Judith Bush Janemarie Eric G.
What type of work is expected? Working Group, Liaison Efforts, Other?		Observe and report back	
TAC Sponsor(s)/Champion(s)		Heather Flanagan	

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. Some of the observations are outlined in the table of suggested actions.

Link to related materials

- https://www.educause.edu/

Suggestion/Action Item	**Submitter**	**Description**	**+1s**
Observation: InC Organizations change their IdP and in the process register under a new entityID	Mark		Judith Bush Janemarie Duh
Observation: InC IdPs assert they support R&S attribute release, but do not	Mark		
Observation: 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	Mark		Judith Bush
Observation: IdPs releasing attributes that should have a scope without a scope (for example eduPersonPrincipalName, eduPersonScopedAffiliation)	Mark		Judith Bush
First-hand observation: An InC organization has a name-based identifier that can change, thus breaking federated access to the service	Janemarie		Judith Bush
What type of work is expected? Working Group, Liaison Efforts, Other?		Observe and report back -- possibly consult for established working groups or committees	
TAC Sponsor(s)/Champion(s)		Mark Rank	

Assurance

Several groups (CTAB, REFEDS) have focused community efforts around assurance. TAC needs to stay aware of those efforts.

Link to related materials

- CTAB Assured Access Work Group
- REFEDS Assurance Working Group

Suggestion/Action Item	**Submitter**	**Description**	**+1s**
Keep tabs on CTAB AAWG		Eric	
Keep tabs on REFEDS AWG		Albert	
What type of work is expected? Working Group, Liaison Efforts, Other?		Observe and report back	
TAC Sponsor(s)/Champion(s)		N/A	

HECVAT

Adding/improving federated IAM related criteria in HECVAT.

Link to related materials

- https://docs.google.com/spreadsheets/d/1-Ftr7o6Vee5WRtFbQuJfjIfFvoBuY4fvhW9Y1lrM-98

Suggestion/Action Item	Submitter	Description	+1s
What type of work is expected? Working Group, Liaison Efforts, Other?		Convene small group with HECVAT core team to develop details and action items	
TAC Sponsor(s)/Champion(s)		Mary McKee; Steven Premeau; Nicole Roy	

Template for New Proposed Work Item

High-level description of new work item.

Suggestion/Action Item	Comments or Elaboration	Name, Organization