InCommon TAC 2022 Work Plan

InCommon TAC 2022 Work Plan

This is final version of the InCommon Technical Advisory Committee's 2022 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.

(Working document of this work plan in Google Doc)

2022 Work Plan Items

These are TAC's focused work items for 2022.

Adopt SAML Deployment Profile - Next Steps

Now that InCommon Steering Committee has officially endorsed TAC's recommendation to adopt SAML Deployment Profile, TAC turns its attention to developing strategy, roadmap, and support materials to help Participants making the transition.

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**
Develop a roadmap to adoption across the federation; how to get started; who first? Sequencing; timing, etc.	Albert W		Mark R
Understand implication to organizations; develop measures to help	Albert W		Mark R
Devise communication/outreach plan	Albert W		Mark R
Identify incentives (killer app) to motivate orgs to make the changes	Albert W		Mark R
Deal with Single Logout	Mark R		
What type of work is expected? Working Group, Liaison Efforts, Other?		TAC to convene a sub group, similar to the group that drafted the original recommendation	
TAC Sponsor(s)/Champion(s)		Mark Rank	

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**
volunteers			Matt E Mark R Steven P Joanne B Chris Phillips *(CACTI volunteer)* Kevin Hickey *(CACTI volunteer)*
Develop a roadmap to adoption across the federation; how to get started; who first? Sequencing; timing, etc.	Albert W		Matt E Mark R
Understand implication to organizations; develop measures to help	Albert W		Mark R Matt E
Devise communication/outreach plan	Albert W		Matt E
Identify incentives (killer app) to motivate orgs to make the changes	Albert W		Mark R Matt E
change/migration/parallel support guidance - how do IdPs and SPs deal with the transition period where old and new identifiers are in use in parallel?	Albert W		Mark R Matt E
Expectations for product makers and for product deployers	Albert W		Matt E
Strategies for dealing with RL realities, e.g., products demanding email address as identifiers	Albert W		Matt E
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

The TAC is preparing InCommon to adopt the Deployment Profile. The Fed Test working group will support this effort by working through the specifics of how to allow InCommon, deployers, and implementers measure against the testable statements in the Deployment Profile. In order to clearly measure an entity's success in meeting the requirements of the statements, there needs to be a set of reference / compliance testing tools on which the community can rely.

Link to related materials

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

Suggestion/Action Item	Submitter	Description	+1s
Find participants	Judith B		
Develop out a plan of attack and have a clear ask of the people we recruit	Judith B	This could provide a clear work scope and be less open ended: “Can you write testing requirements for the deployment profile/SAML spec X?” “Can you review the list of testing priorities for IdPs/SPs for missing test targets?	
What type of work is expected? Working Group, Liaison Efforts, Other?		Working Group	
TAC Sponsor(s)/Champion(s)		Judith Bush	

Standing Items

In addition to focused work items, TAC tracks additional work and happenings in the community and industry. As appropriate, TAC will react/escalate.

Browser Technology Changes (user tracking) and impact on Federation

Champion: Heather Flanagan

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.

Actions

- Lightweight tracking, reporting through the Slack channel.

Link to related materials

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

Next Steps with HECVAT: ongoing evolution/keeping

Champion: Steven P

TAC contributed a number of federated IAM related elements to the latest HECVAT release. REN-ISAC has asked InCommon to remained engaged.

Actions

- Maintain contact with REN-ISAC; report request for updates / engagement as appropriate.

Guidance for EntityID creation, change, and use.

Champion: Mark Rank

Volunteers: Jim Basney; Scott Korenda; Albert Wu

A number of institutions have recently migrated its IdP from one platform to another. In the process, they are changing their IdP entity ID. On the other side, some SPs implement rules binding a user’s access to a particular entity ID. If the IdP’s entity ID changes, the user loses access

This phenomenon seems to be happening more frequently with staff turnovers and campuses facing major upgrade/migration of their IdPs. How can TAC /InCommon help to resolve this matter?

Questions include:

- What is the IdP operator’s responsibility when making such transition?
- What should be the SP’s expectations regarding the IdP’s entity ID?

Potential Actions

- Survey of cloud provider options: how many require the provider’s entity ID, how many default to a provider entity ID? - could be the basis of a guide to prevent inappropriate entity ID switch overs
- Best practices in migration between IdPs? Best practice’s when your institution’s branding changes? Explanation that the entity Id need not be the same URL as the IdP? - Could clear up misconceptions about entity IDs

Link to related materials

- InCommon TAC 2021 Work Plan