InCommon TAC 2021 Work Plan

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
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

<table>
<thead>
<tr>
<th>Suggestion/Action Item</th>
<th>Submitter</th>
<th>Description</th>
<th>+1s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete the Strategies for Working with Identifiers in Federation document</td>
<td>Mary McKee, Judith Bush, Janemarie Duh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flesh out the Deploy SAML Subject Identifier in InCommon plan</td>
<td>Mary McKee, Judith Bush, Janemarie Duh</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Suggestion/Action Item</th>
<th>Submitter</th>
<th>Description</th>
<th>+1s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe user stories for the user of a test federation</td>
<td>Matt B, Judith Bush</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Draft requirements</td>
<td>Janemarie Duh</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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)
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”. 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.

Link to related materials
- SeamlessAccess UX Documentation
- Code Repositories
  - thiss-ds-js: A set of clients for the discovery service. Can be used to implement a DS connected to a central persistence service.
  - this-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

<table>
<thead>
<tr>
<th>Suggestion/Action Item</th>
<th>Submitter</th>
<th>Description</th>
<th>+1s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promoting SeamlessAccess within InCommon by using SeamlessAccess itself for InCommon’s WAYF.</td>
<td>Janemarie</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe the potential user stories that will help us to determine requirements and priorities.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decide on project requirements from InCommon</td>
<td>Mary McKee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- branding</td>
<td>Janemarie</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- IdP filtering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decide on whether there should be a single WAYF offered by the federation, or encourage individual SP implementations.</td>
<td>Mary McKee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What type of work is expected? Working Group, Liaison Efforts, Other?</td>
<td>Subcommittee with community consultation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
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/

<table>
<thead>
<tr>
<th>Suggestion/Action Item</th>
<th>Submitter</th>
<th>Description</th>
<th>+1s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observation: InC Organizations change their IdP and in the process register under a new entityID</td>
<td>Mark</td>
<td>Judith Bush</td>
<td>Janemarie Duh</td>
</tr>
<tr>
<td>Observation: InC IdPs assert they support R&amp;S attribute release, but do not</td>
<td>Mark</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>Mark</td>
<td>Judith Bush</td>
<td></td>
</tr>
<tr>
<td>Observation: IdPs releasing attributes that should have a scope without a scope (for example, eduPersonPrincipalName, eduPersonScopedAffiliation)</td>
<td>Mark</td>
<td>Judith Bush</td>
<td></td>
</tr>
<tr>
<td>First-hand observation: An InC organization has a name-based identifier that can change, thus breaking federated access to the service</td>
<td>Jane marie</td>
<td>Judith Bush</td>
<td></td>
</tr>
</tbody>
</table>

**What type of work is expected? Working Group, Liaison Efforts, Other?**
Observe and report back

**TAC Sponsor(s)/Champion(s)**
Heather Flanagan

---

**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

<table>
<thead>
<tr>
<th>Suggestion/Action Item</th>
<th>Submitter</th>
<th>Description</th>
<th>+1s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep tabs on CTAB AAWG</td>
<td>Eric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keep tabs on REFEDS AWG</td>
<td>Albert</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**
### Template for New Proposed Work Item

High-level description of new work item.

<table>
<thead>
<tr>
<th>Suggestion/Action Item</th>
<th>Comments or Elaboration</th>
<th>Name, Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of work is expected? Working Group, Liaison Efforts, Other?</td>
<td>Convene small group with HECVAT core team to develop details and action items</td>
<td>Mary McKee; Steven Premeau; Nicole Roy</td>
</tr>
</tbody>
</table>