Linking SSO Systems Working Group Charter

February 2022

Document Title: Linking SSO Systems Working Group Charter
Document Repository ID: TI.163.1
DOI: 10.26869/TI.163.1
Persistent URL: http://doi.org/10.26869/TI.163.1
Authors:

- Community Architecture Committee for Trust and Identity (CACTI)
  - Rob Carter https://orcid.org/0000-0002-5903-5799
  - Keith Wessel https://orcid.org/0000-0002-8047-3187
Publication Date: February 2022
Sponsor: Community Architecture Committee for Trust and Identity (CACTI)

Linking SSO Systems Working Group Charter

Problem Statement

A number of factors have, in recent years, led to increasing deployment of multiple single sign-on (SSO) solutions within individual organizations. Different consumers of SSO services may require different SSO protocols/APIs (eg., SAML vs. OIDC vs. WS-* vs. CAS); implementations of the same protocol may differ in ways that require different SSO providers due to variant interpretations of standards; some (primarily commercial) services may even provide their own self-contained SSO solutions. Apart from the expense of operating multiple SSO systems, this fragmentation of SSO services produces an undesirable, high-friction user experience, and can threaten the consistency and security of identity and access management (IAM) across disparate systems. Required to interact with multiple, unlinked SSO services, users may become confused as to what credentials to use when, and which "sign on" service(s) they should trust. They may quite rightly question how their experience can be termed "single" sign on at all.

A common, and in many cases the only viable approach to reducing friction and limiting the negative impact of SSO service fragmentation on users involves linking disparate SSO systems together, usually with the goal of providing a consistent point of authentication for the end user while allowing SSO consumers (relying parties) to integrate with different linked component services as necessary.

Multiple strategies for linking particular SSO systems may be used, each with different effects on the user experience, security, and federation capabilities. The choice, for example, of which SSO system will be responsible for end-user interaction, and how the integration between linked systems is accomplished, may expand or limit options for such important features as multi-factor authentication (MFA). No single linking strategy may be "optimal" for all sites and all scenarios, but each strategy has strengths and weaknesses which need to be considered when an organization designs a solution.

Discussions during the 2021 ACAMP event led to a request from the community for a working group to look in more detail at these issues.

The goal of this working group is to identify and classify the most common use cases from the community for linking SSO systems, evaluate the different linkage strategies available and in use today, and document effective recipes for their application and provide guidance regarding their strengths and weaknesses in different scenarios.

Stakeholder vetting

- CACTI (to sponsor the WG)
- TAC (to be kept apprised via CACTI of WG progress)

- The wider IAM community (including but not limited to InCommon participants)

Deliverables from the Working Group will be presented to CACTI for approval upon completion. CACTI will designate a CACTI member to act as liaison with the Working Group and facilitate communication between the Working Group and CACTI.

Charter

The Linking SSO Systems Working Group will:

- Be open to participation by any community member, with participation not limited by number (but with a minimum of six participants)
- Meet at least every other week
- Be responsible for selecting its own Chair, and if desired, co-Chair, who will have the responsibilities outlined for Working Group chairs and co-chairs here.
- Persist until its deliverables are completed or it is dissolved with the agreement of its participants and CACTI
- Publish its meeting proceedings in a timely fashion (subject to approval by the meeting participants), maintain an open-subscription mailing list for informal participation with the group, and, as appropriate, communicate with the community via blog posts and other community fora

The Working Group's deliverables, to be provided at completion to CACTI for publication to the community at large, will include:

- Identification of common use cases and common strategies for linking frequently deployed SSO systems, and in particular, linking SAML and non-SAML-based SSO systems. This may entail engagement with the broader IAM community to collect use cases.
- Documentation of implications for IAM for those use cases. For example, the implications of a Google-based cloud strategy on participation in Academic Interfederation, or the IAM effort required to integrate Sharepoint into an already-federated environment.
- Documentation of recipes for those strategies, along with guidance regarding the benefits and risks of different strategies and key differentiating and selection factors (eg. REFEDS MFA support, exposure of relying party identities, SLO, etc.)
- Recommendations for improvements to community-sourced (and/or commercial) SSO solutions in support of either reducing the need for or facilitating the linking of SSO systems.

Duration for this Working Group will be dependent on completion of its deliverables, but is expected to be between three and six months. Depending on start-up timing, it's expected that this Working Group can release its findings by September, 2022.