

IdP as a Service Working Group Charter

Problem Statement

It's the long tail problem. Many campuses don't have IT staff with the time or skills to operate an on-premises, federation-capable Identity Provider (IdP). Their strategy for providing IT services to their campus leans heavily on cloud service offerings. Adding IdP as a Service (IdPaaS) options to their menu will enable more organizations to participate in federation, improving its value both to enterprises and to research communities, who need the long tail included in federation.

There are IdPaaS options out there and a few more may be under development, though there's only marginal uptake so far. The IdPaaS Working Group will do research and develop recommendations with the goal of making the IdPaaS market a viable alternative, perhaps the preferred alternative, for future participation in the InCommon Federation.

Areas of focus for the IdPaaS Working Group include:

- What does an IdPaaS offering need to be and do so that its customers can be good federation participants?
- How will prospective customers know that, and why should they care?
- How will [service] providers know that, and why should they care?
- What role or steps should InCommon, or other organizations such as JISC, GÉANT, and commercial providers, take to develop this market?

There are many things that might address the long tail problem. This working group will focus on optimizing how an IdPaaS offering can take as big a bite as possible out of that problem.

Stakeholders/Influencers/Influences

- Current and potential commercial and non-profit IdPaaS providers
- Current InCommon Participants that may wish to switch from on-premises to IdPaaS
- Prospective InCommon Participants, especially their CIOs or senior IT managers with responsibility for campus IT infrastructure
- IAM architects at InCommon participants organizations
- Commercial and non-profit IdM providers, including Identity Management as a Service (IdMaaS) providers
- InCommon Federation (Internet2) management
- Internet2 research engagement
- REFEDS
- Federated Identity Management for Research (FIM4R)
- Canadian Access Federation
- UK Access Management Federation
- Australian Access Federation

Charter

The IdPaaS Working Group will:

1. Identify who does or plans to provide an IdPaaS that would be available to customers in North America.
2. Identify the top IdM solutions used by US, Canadian, and UK higher ed institutions, whose integrations with an IdPaaS would maximize the number of customers that could easily get it up and running.
3. Drawing on recommendations in the [SAML V2.0 Implementation Profile for Federation Interoperability](#), the [SAML V2.0 Interoperability Deployment Profile V2.0 \(Draft\)](#) and [Baseline Expectations for Trust in Federation](#), identify technical and operational requirements that an InCommon IdPaaS must meet and should meet in order to maximize the potential for customers to federate and integrate with diverse service providers. Where the working group identifies a need that does not map to a clearly defined community interoperability standard or recommendation, the working group will escalate the matter to the InCommon Technical Advisory Committee.
4. Gather input for items 1-3 by consulting with industry analysts, where feasible, and representative sets of corresponding stakeholders.
5. Recommend whether IdPaaS should be classified into one or more "levels" (e.g., Basic, Plus, etc.) of complexity/granularity of service, and if so, what criteria would be used to define these.
6. Recommend one or more models for how responsibility for meeting the requirements in item 3 should be shared among an IdPaaS provider, its customer, and any other parties, with special attention to clarifying the responsibilities an IdPaaS can and cannot assume on a customer's behalf.
7. Recommend how InCommon or another third party can objectively ascertain that a given IdPaaS meets requirements identified in items 3 and 5.
8. Recommend operational or programmatic steps that InCommon or other parties should take to realize the other recommendations and clarify a recommended stance on InCommon's ability to identify/endorse/certify/recommend IdPaaS as part of a larger outreach strategy.

Explicitly out of scope are:

- Promoting TIER or any particular IdM solution or IdPaaS provider.
- Choosing the best IdPaaS provider.

- Classifying all InCommon IdPs into “levels” as in item 5.
- Developing marketing materials, although recommendations may include ideas of value for that purpose.

Membership

Membership in the IdPaaS Working Group is open to all interested parties. Solicitation will take place on lists such as the InCommon Participants list and the REFEDS list, explicitly seeking international participation. Some stakeholders may be explicitly solicited by the Co-Chairs or other Working Group members for participation, e.g., providers who do not ordinarily participate on the above lists. Members join the Working Group by subscribing to the mailing list and Slack channel, participating on the calls, and otherwise actively engaging in the work of the group.

Work Products

1. Recommendations referenced in Charter items 3, 5, 6, 7, and 8.
2. Summary report of the IdPaaS Working Group proceedings, including any notables not included in the recommendations.