InCommon Federation Identity Provider as a Service Working Group Final Report

Repository ID: TI.145.1

Persistent URL: http://doi.org/10.26869/TI.145.1

Document Status: Submitted

Publication Date: mmmm, dd, yyyy

Sponsor: InCommon Technical Advisory Committee

Executive Summary

The Identity Provider as a Service Working Group was chartered by the InCommon Technical Advisory Committee (TAC) in March 2019 to analyze community needs and recommend how InCommon can make Federation participation more accessible through support of cloud-based Identity Provider as a Service (IdPaaS) solutions.

Key recommendations, outlined in greater detail later in this report, include:

- Developing a sustainable “Federation-Ready Identity Provider” program that recognizes IdPaaS solutions that support all requirements and standards needed for their customers to fully participate in Federation activities.

- Helping prospective customers to understand four common patterns (“integration models”) for IdPaaS integration into their IT infrastructure, determine which best aligns with their goals, and identify and compare Federation-ready products in that space.

- Placing particular focus on promoting the “Federation Connector” integration model, which allows institutions to maintain their existing single sign-on (SSO) products in conjunction with a lightweight product that bridges between campus SSO and the Federation.

The IdPaaS Working Group concludes that through the recommendations outlined in this report, InCommon can provide clearer guidelines and incentives for best practices among IdPaaS providers, simplify the product selection process for institutions, and simultaneously broaden InCommon’s participant base and realize accelerated progress in adoption of Federation standards.

Summary of Work

Survey

The Working Group began by discussing scope of what could be considered to be an Identity Provider as a Service offering and quickly determined that there is not a one-size-fits-all definition of the concept. In order to catalog the range of community needs and expectations for IdPaaS products, the group developed a survey to measure an institution's current Identity Provider (IdP) environment, their interest in a move to a cloud-based IdP, the motivating factors in such a move, and what features a commercial product would have to offer in order to be viable to the organization.

This survey was distributed to InCommon members and related communities. It received 74 responses[1].

IdPaaS Integration Models

The survey results confirmed the Working Group's impression that organizations turn to IdPaaS products with different goals in mind, so it would not be practical to suggest a common standard for all such products or create a tiered evaluation system (e.g., “basic” or “premium” products).

The Working Group found that organizational needs can more predictably be categorized by “integration model”, or the balance of how much responsibility they wish to delegate to the IdPaaS product vs. other products or in-house infrastructure.

The table below outlines the four most common integration models, each building on the previous one in terms of delegation potential. User stories illustrating use cases for each of these models can be found in the appendix.

[1] Survey results: https://spaces.at.internet2.edu/display/IDPAAS/Survey+Results

Integration Model	Institution Manages:	Provider Offers:
Federation Adapter A service that operates as a bridge between Federation and Intracampus single sign-on (SSO)	• Business rules • Identity store/registry • Credential management • Provisioning • User authentication	• Federation adapter
Full SAML SSO [1] A service that can serve as both intracampus and federated SSO, connecting to existing (separate) credential and attribute stores.	• Business rules • Identity store/registry • Credential management • Provisioning	• User authentication
Identity Provider + Credential Store [1] A full (intracampus + federated) SSO solution with an integrated/hosted credential and attribute store.	• Business rules • Identity store/registry • Provisioning	• Credential management • User authentication
Identity and Access Management as a Service A complete hosted IAM solution, **not in scope** for IdPaaS.	• Business rules	• Identity store/registry • Provisioning • Credential management • User authentication

[1] While support for alternate protocols (for example CAS or OIDC) is outside the scope of this Working Group's charter, this support is valuable and may be a deciding factor for campuses.

IdPaaS Features

Even more varied than the architectural intentions for an IdPaaS product were the features desired by prospective customers. Survey responses highlighted diverse priorities, and few of the commonly mentioned priorities (e.g., high availability, cost, security) were strongly tied to federation potential.

Community Need

Survey responses and other community discussions conducted by the Working Group underscored institutions' interest in IdPaaS products as a way to reduce staffing overhead and increase resiliency in IAM services.

These key goals highlight that federation potential is not a major driver of interest in moving an institution's primary SSO infrastructure into the cloud, and we can observe from the "Federation adapter" market that institutions interested in federation can still commit to infrastructure that doesn't advance that goal. Survey responses revealed that prospective customers of other IdPaaS models are likely to follow the same path. Those most interested in deploying an IdPaaS product were the least confident in their ability to assess or validate federation capability, inviting conclusions that this goal is not only lower priority than features pertaining to intracampus single sign-on, but also higher effort.

IdPaaS deployments extend or replace some of an institution's most critical IT infrastructure, and customers are wise to take a conservative approach to such a deployment. The recommendations in this report focus on positioning InCommon as a community resource that can independently validate Federation readiness, adding value to the product selection process without adding complexity.

Recommendations for InCommon

To maximize accessibility of Federation participation among IdPaaS customers, the Working Group recommends that InCommon take the following steps:

- **Publish and promote an article on the InCommon website pertaining to the advantages of multilateral federation** - Ambiguity about the differences between bilateral and multilateral federation creates confusion in discussions about how IdPaaS providers can get the most from their relationship with InCommon. A concise and easily citable summary of these advantages would support the community in advocating for a shared vision for the Federation.
- **Formally adopt, support, and promote interoperation best practices** - InCommon should adopt the SAML v2.0 Deployment Profile for Federation Interoperability and SAML V2.0 Subject Identifier Attributes Profile Version 1.0, developing a transition plan to ensure widespread conformance of these profiles among Federation participants.
- **Develop a "Federation-Ready" program for IdPaaS solution providers** - IdPaaS products that meet the program's criteria should be represented in documentation for

institutions to help them choose products that meet the requirements they tend to understand well without having to be experts in Federation standards.

    - This program should cover technical standards, metadata use, security practices, and configuration requirements to enable a customer to configure the IdP to meet all Federation best practices.

    - The process for being recognized by InCommon as “Federation-ready” should be straightforward and transparent so as to encourage participation in the program.

    - The program should continually evolve requirements for a “Federation-Ready” Identity Provider and ensure that participants have at least six months lead time on adopting new requirements. Active engagement with the community should be encouraged to allow participants to anticipate and contribute to the development of new requirements. The program should include a dispute resolution process similar to Baseline Dispute Resolution to address any concerns.

- **Support institutions with guidance on product selection** - To support institutions in choosing a “Federation-ready” IdPaaS product, InCommon should develop a Institution Adoption Guide for prospective IdPaaS customers to help them:

    - Determine which integration model best fits their architecture and goals.

    - Review a list of products recognized as “Federation-ready” by InCommon for the selected model, with the goal of empowering institutions to look at federation capability as a straightforward feature that can be validated by a trustworthy third party (InCommon), rather than a nebulous topic requiring deep technical expertise to evaluate internally.

    - Consider a list of commonly requested (“differentiating”) features for IdPaaS products to support the product selection process. Institutions surveyed had strong and varied priorities for features, so the nature of this guidance should be one of sharing relevant community feedback rather than assessing the importance of these features. This guide should help customers feel more confident that their selection process included evaluation of features relevant to peer institutions prior to committing to a particular solution.

- **Launch program with special emphasis on “Federation Adapter” products** - The Working Group believes this use case to offer the most immediate benefit to our community, creating a path for institutions committed to a particular campus SSO solution to participate in and reap the benefits of federation without replacing critical infrastructure, and there are currently enough products in this space to make for a reasonable pilot.

Technical Requirements for Federation-Ready IdPaaS Products

The Working Group recommends that InCommon limits the scope of technical requirements of IdPaaS providers to factors directly related to federation capability. Through the proposed "Federation-Ready" program, InCommon can express and validate what makes an IdPaaS provider's customers capable of taking full advantage of their InCommon membership.

A "Federation-Ready" IdP should not be responsible for their customers meeting Federation requirements, but rather support all technical requirements and standards necessary for them to do so.

The IdPaaS Working Group recommends that this program be designed to help drive adoption of future requirements and emerging standards as well as existing ones, suggesting the following items for inclusion in a “Federation-Ready” IdPaaS provider assessment:

Technical Requirement	**Relevant Standards/Guidelines**
InCommon Baseline Expectations	https://www.incommon.org/federation/baseline/
Support of automated data release per REFEDS R&S Entity Category	https://refeds.org/category/research-and-scholarship
REFEDS Sirtfi	https://refeds.org/sirtfi https://wiki.refeds.org/display/CON/Consultation:+eduGAIN+Security+Incident+Response+Handbook
Signalling REFEDS assurance profile elements (including REFEDS SFA/MFA)	https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0 https://refeds.org/profile/sfa https://refeds.org/profile/mfa
Ability to support evolving Federation attribute standards - be able to flexibly map and transform attribute names and syntax from sources to desired syntax used in SAML assertions	https://wiki.refeds.org/display/STAN/eduPerson https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html

(note to program developer: consider clarifying any SAML assertion syntax requirements)	
Support for InCommon Metadata ● Registering IdP metadata with InCommon ● Defining a process for keeping IdP metadata up to date ● Configuring IdP to verify the signature on metadata ● Support of long lived certificates, self-signed certificates and multiple certificates per entity.	https://spaces.at.internet2.edu/display/mdq https://spaces.at.internet2.edu/display/InCFederation/X.509+Certificates+in+Metadata https://kantarainitiative.github.io/SAMLprofiles/saml2int.html (see doc for guidance on certificates)
Implements required and recommended practices outlined in SAML Deployment Profile and Implementation Profile	SAML v2.0 Deployment Profile for Federation Interoperability SAML V2.0 Subject Identifier Attributes Profile Version 1.0

Additional Recommendations for Federation-Ready IdPaaS Products

The Working Group advises limiting additional recommendations to upcoming requirements for "Federation-Ready" program eligibility, and a few call-outs to key community work that would be valuable for an institution to consider:

Recommendation	**Purpose**
Provider supply a HECVAT	Allows institutions to compare IdPaaS providers' positions on matters of security,

	compliance, and privacy.
Provider supply a PAT	Allows institutions to review product accessibility.

Product features not directly related to federation capabilities should be incorporated into the proposed Institution Adoption Guide (examples) for organizations to review, consider, prioritize, and use as a differentiator between IdPaaS products.

Deliverables

The Working Group has produced the following deliverables as linked on the IdPaaS Working Group wiki:

- Survey Results comparing Federation participant responses about current infrastructure, gaps, and needs.
- Supplementary lists of commercial IdPaaS providers and IdPaaS solutions run by federations and networks.
- Example formats for an Institution Adoption Guide.

References

- **[SAML2Int]** SAML V2.0 Deployment Profile for Federation Interoperability 2.00; https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
- **[SubjectId]** SAML V2.0 Subject Identifier Attributes Profile Version 1.0; https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.pdf
- **[Baseline]** InCommon Baseline Expectations for Trust in Federation; https://incommon.org/federation/baseline/
- **[Sirtfi]** REFEDS Security Incident Response Trust Framework for Federated Identity; https://refeds.org/sirtfi
- **[MFA]** REFEDS Multifactor Authentication (MFA) Profile ; https://refeds.org/profile/mfa

Appendix - User Stories

The following are example user stories for each of the four IdPaaS deployment models:

1. Federation Adapter
2. Full SAML SSO
3. Identity Provider + Credential Store
4. Identity and Access Management as a Service

Federation Adapter

Alice Johnson Public University (ajpu.edu) is a large public university (Carnegie Classification R2: Doctoral Universities – High research activity) and is a current member of InCommon. Their current identity management system had been built over years by a small team of system programmers. The technology stack is a combination of custom solutions (coded in Perl and FORTRAN) as well as open source solutions (CAS, Shibboleth, and OpenLDAP). The last member of this original team plans to retire at the end of the calendar year. Recruiting and training replacement staff has been difficult.

A new Vice-Chancellor of Technology (aka CIO) joined the organization at the start of the current term. After a period of assessment, she has started a modernization program with a cloud-first strategy at the core. Student and staff email will be moving from on-prem to either GSuite or Office365. On campus directory services and SSO will be moving to one of a short list of commercial identity providers (Azure AD if Office365 is selected for mail; one of a number of cloud IAM solutions if GSuite is selected).

The remaining gap in this plan is having a solution that will provide multilateral federation support for AJPU's library services and current research activity (especially significant grants with the US Dept. of Energy and National Institutes of Health). AJPU also leverages some InCommon service providers to support instructor assessment, athletic eligibility compliance, and student health center appointment scheduling.

AJPU is looking for an adapter that will allow the selected cloud IAM solution to have multilateral federation support so that the solution will function within the InCommon Trust Federation.

Full SAML SSO

Bob Smith Private College (bspc.edu) is a smaller private college (Carnegie Classification M3: Master's Colleges and Universities – Smaller programs) that distinguishes itself by offering a

masters in public health (MPH) with an emphasis in serving diverse populations. Because of this, BSPC has received a large multi-year grant to develop an online version of their masters in public health with the aim of increasing the number of public health professionals in Native American tribes. The grant will be phased over several years and funded by both a large private foundation, and matching grants from the Department of Education and the Department of Interior.

BSPC is not a current member of InCommon, but this has to change. BSPC currently operates an on-prem identity management solution (loosely based around Active Directory) and currently doesn't leverage SSO. Most services authenticate directly to Active Directory. To support a broader online learning initiative as well as the online MPH program, BSPC needs to move to services that are cloud-oriented and use SSO. This will include moving to a cloud-based learning management system (Canvas) as well as other learning and library services accessible from the InCommon Federation.

Because the MPH program grant is phased, the college cannot hire all the needed faculty. BSPC has worked out agreements with several other universities to have faculty teach the needed coursework. Part of these agreements is that, while the coursework will be BSPC, faculty will use their home credentials (all InCommon members) to access any needed services to minimize support costs. This further increases the need for multilateral federation capabilities. The MPH program also has several grant administration obligations that require having an InCommon IdP.

BSPC is looking for a cloud-hosted SSO solution that can leverage the existing Active Directory as a credential store, and also be used as a multilateral federation-aware SSO Identity Provider in the InCommon Trust Federation.

Identity Provider + Credential Store

Community College of Everywhere (cce.edu) was recently formed by the merging of several single campus community colleges in the rural midwest. A major focus for CCE is to provide advanced vocational training as well as career retraining for the communities it serves.

A core component of the merger is moving to a shared services model. Office productivity (Office365/GSuite), ERP, CRM, and learning management platforms are all being evaluated. Previously each community college had some form of local IT primarily to support computer labs and email. Another planned shared service is a consolidated (or virtual) credential store and SSO solution to support the other shared services, and allow the now distributed IT team to better support end users.

CCE is also looking for a solution that will provide multi-factor authentication capabilities (MFA). While some of the CCE campuses have used DUO locally, CCE is open to another provider if it is well integrated with the SSO/credential store. A SaaS solution is also desirable to support

service availability. None of the CCE campuses has a data facility that meets modern business continuity requirements. It is anticipated that each of the campuses will continue to handle provisioning locally, both because of local academic program needs and also varied business practices.

The planned productivity, ERP, CRM, learning management platform, as well as cloud-hosted ticketing systems (ServiceNow), and online library resources motivate a desire to join InCommon. CCE is also looking to collaborate with advanced vocational programs in Europe and other countries. This will require CCE students and faculty to be able to access services available in the broader eduGAIN Federation. The goal would be to have an SSO solution that could support registration with InCommon.

CCE is looking for a cloud-hosted Identity Provider (SSO) solution that is multilateral federation aware and will also address their need for consolidated credential management.

Identity and Access Management as a Service

Doris Williams Museum (dwm.org) is a small art museum with an extensive permanent collection of polymer clay, beading, and LEGO modern art pieces. In response to the COVID-19 pandemic, a major benefactor has come forward with funding to both put DWM's collection online, and also support outreach programs so that DWM can offer virtual art classes for children learning from home.

While DWM has a "scrappy" two person technical team -- the extent of the IT operations has been maintaining a few computers at the front office, the audio tour system, and wireless for the exhibits. In a short time, DWM needs to provide access to staff, instructors from the surrounding community (three major universities are within a 50 mile radius), and volunteers to accomplish this new mission. Access will be to a suite of services: digital archiving, content authoring, learning management, and various administrative functions. To date, DWM's wireless has been for public access. To support this project, DWM also needs to deploy a parallel authenticated wireless solution. Having support for RADIUS or another wireless authentication method is also desired.

DWM is looking for a full identity and access management solution that will provide credentialing, provisioning, SSO solutions, and wireless authentication for the handful of web-based applications, and about 100 end users. A SaaS solution is desired. While an additional IT person will be added to the team, the focus will be on the services directly needed to accomplish the mission. It is anticipated there will be little time to dedicate to learning and maintaining access management solutions.