Home Institution Adoption Guide for Cloud-based Identity Providers

ABOUT THIS PAGE

The content below is intended to present two example formats for the guide for institutions recommended by the IdPaaS Working Group's proposed "Federation-Ready Identity Provider" program.

This guide is intended to help take the guesswork out of federation readiness for prospective customers, allowing them to easily identify IdPaaS solutions that will meet their architectural needs and allow them to fully participate in federation. Users of this guide should be able to quickly narrow their product search to options that will not limit their federation potential, and conduct their normal institutional process to help establish the most desirable offering based on more easily observable features.

Identity Provider as a Service

An Adoption Assessment Guide for Home Institutions

About this guide

Cloud-based Identity Provider services cover a range of goals and capabilities. The best solution for your campus will depend in part on whether you seek to complement the functionality of your existing infrastructure, or (partially or fully) replace it.

This document will help you identify what type of IdPaaS service will best address your institution’s needs, access information about (link to program info) Federation-Ready (/link) products in the desired category, and review considerations to keep in mind when selecting a vendor.

OPTION 1: TEXT OVERVIEW

This option exposes the IdPaaS integration model table and "Federation-Ready" vendors for easy skimming.

Categories and Vendors

The following chart summarizes four common models for IdPaaS usage, how responsibility is shared between an institution and vendor, and federation-ready products that accommodate the use case.

A glossary at the end of this document explains these business functions in greater detail.

Model	Institution Manages:	Vendor Provides:	Vendors

OPTION 2: INTERACTIVE SURVEY

This option presents similar information, but in a more interactive survey format.

Adoption Assessment

1 Identity and Access Management Infrastructure

1.x Vendor/IT Strategy dependency

Does your institution have an existing strategic commitment to a particular vendor or IAM product that you must use for your enterprise IAM solution?

1. Yes. Microsoft Active Directory Federation Services or Azure AD
2. Yes. (others)
3. We have something, but are open to change.
4. We don’t have an enterprise IAM solution

1.1 Identity store/registry

An identity registry is the source of identity information for all IAM purposes.

1. I already have an identity registry and would like to integrate it with the IdP as a Service
2. I don’t have one yet, but will implement one on my own
3. I would like the offered solution to include an identity registry
4. I am not sure

1.2 Managing user account/credentials

This includes creating usernames and storing associated password hashes.

1. I have an existing user credential system and would like to integrate it with the IdP as a Service
2. I don’t have one yet, but will implement one on my own

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	Product A Product B Product C
Full SAML SSO 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	Product B Product C Product D
Identity Provider + **Credential Store** A full (intracampus + federated) SSO solution with an integrated/hosted credential and attribute store.	Business rules Identity store/registry Provisioning	Credential management User authentication	Product B Product D

3. I would like to manage user accounts and credentials in the offered solution
4. I am not sure

1.3 Managing user roles/groups

Group tools can be integrated or external, and are most often used for permissions/authorization, management of entitlements, communications, and reporting.

1. I have an existing user group/role solution and would like to leverage it with the IdP as a Service
2. I don’t have one yet, but will implement one on my own
3. I would like to manage user roles and groups in the offered solution
4. I am not sure

1.4 Provisioning

Provisioning most often includes initiating user records in downstream systems, but can also include sourcing identity data from upstream systems of record.

1. I have an existing provisioning solution
2. I don’t have one yet, but will implement one on my own
3. I would like the offered solution to include provisioning capabilities
4. I am not sure

1.5 User Authentication/Login Page

This refers to the web-based user interface a user interacts with to log in to campus services. This is usually implemented at the Identity Provider level, but can be maintained externally to that infrastructure if desired.

1. I have an existing user authentication UI I’d like to integrate with the offered solution
2. I would like for the offered solution to provide a login page UI
3. I am not sure

1.6 Multi-factor Authentication (MFA) / Strong Authentication

You may prefer to have a product that integrates with a preferred MFA solution, or bundle this with the vendor.

1. I will bring my own MFA solution
2. I would like the offered solution to include MFA
3. I am not sure

1.8 Manage SP metadata, integration, and data release with my IdP

<options>

1.9 Data Management Policies and Practices

<options>

Identity and Access Management as a Service A complete hosted IAM solution.	- Business rules	- Identity store/registry - Provisioning - Credential management - User authentication	Not currently in scope for evaluation

Differentiating Features

When choosing between comparable products, the following considerations may inform the best choice for your institution:

- **Multi-factor/strong authentication:** would you like the IdPaaS product to include support for multi-factor authentication, or integrate with an existing campus solution? If part of the IdPaaS product, is site-specific MFA policy supported?

- **Institutional branding:** how can the product’s user interfaces be customized to reflect the institutional brand?

- **System/protocol integrations:** does the product integrate with any desired protocols, such as CAS or OIDC?
- **User role/group management:** would you like the IdPaaS product to integrate with an existing campus group/role management solution, or allow for management within the IdPaaS product?
- **Service Provider (SP) metadata and integration:** how can institutional and third party sites be configured to integrate with the IdP product? Can non-InCommon vendors be integrated? What support does the vendor offer for challenging integrations?
- **Service Provider (SP) data release from Identity Provider:** how can user attributes be approved for release to an integrated site (SP)? Can policies be site-specific? Are custom attributes supported?
- **Data Management Policies and Practices:** are the IdPaaS provider’s attribute release mechanisms compatible with your institutional policies and data governance processes?
- **SIEM/Logging:** what logging and security event tracking capabilities does the product offer?
- **Resiliency/availability:** what assurances will the vendor make about availability of the service?
- **Enhanced Client or Proxy (ECP):** does the Identity Provider support non-browser-based login?

- **Attribute release consent:** does the product support user consent for personal information shared by the Identity Provider with integrated sites at the time of login?
- **Social-to-SAML:** does the product support linking of personal accounts (such as Google or Facebook) for login where institutional credentials are not available? If so, how is registration handled?
- **Admin UI:** what administrative capabilities does the service offer? Are granular or delegated permissions supported? How do these capabilities fit with institutional data governance processes?
- **Password reset:** if the product manages user credentials, how is password reset handled?
- **Support:** how much institutional staff time will be required to support functionality offered by the product? Can the product support delegation of management responsibilities if desired?
- **API access:** Do you intend to build automation between the IdPaaS product and other campus infrastructure? If so, does the product feature an API or similar mechanism for such automation?

Either option should include a glossary to cover any key terms:

Glossary

To ensure clarity, we define several key terms referenced in this document. These terms have specific, commonly adopted meanings in the higher education identity management community that may differ subtly from other uses in commercial or other settings.

Federation adapter

A solution that allows campus Single Sign-On (SSO) that is not implemented with SAML to interoperate with InCommon and other eduGAIN member federations.

This is most useful for institutions committed to using a particular IAM product that does not natively support the ability for users to access Federation member sites with their institutional credentials.

Identity store/registry

An identity registry is an essential component of any identity and access management infrastructure. It is the authoritative source of a person’s digital identity in an organization.

Credential management

Responsibility that includes issuing, management, and revocation of institutional usernames and passwords or other electronic authentication credentials.

Provisioning

Tooling to support providing of user/identity information to downstream (dependent) systems.

User Authentication

Support for institutional login. This usually includes hosting the login page users use to authenticate.