InCommon Discovery Futures

TAC Recommendations for the InCommon Steering Committee

Repository ID: TI.162.1
Persistent URL: https://doi.org/10.26869/TI.162.1
Publication Date: March 24, 2022
Sponsor: InCommon Technical Advisory Committee
Authors: Mary Mckee, Duke University
Mark Rank, Cirrus Identity
Janemarie Duh, Lafayette College
Eric Goodman, University of California Office of President
Albert Wu, Internet2

Revision 0002
This document was accepted via TAC consensus on March 24, 2022.

Contents

Executive Summary

Issue

InCommon offers a Federation-run discovery service. It will likely need to undergo significant updates in 2022 for InCommon to continue offering the service for participants.

Background

At its best, federation is frictionless: community members connect to resources securely and efficiently, with minimal direct interaction with the infrastructure making it all possible. There is one notable exception to this: identity provider discovery.

The community has traditionally favored Service Provider (SP) operators to run their own discovery service. This situation has led to end-user experience inconsistencies and missed opportunities at this critical point of interaction.

Assessment

An assessment of InCommon Discovery Service's future rests on a number of business strategy considerations (for example branding, financial, and resource allocation) -- these are the purview of Steering. To advise Steering, TAC has evaluated options for addressing scaling and sustainability of the InCommon Discovery Service and identified possible opportunities.

Recommendation

After considering the various opportunities, TAC recommends InCommon should adopt SeamlessAccess, in standard integration mode, as its central discovery service replacement. In addition, InCommon should encourage participants to use this new central, global discovery service instead of implementing its own.

Given the impact of this change, TAC proposes Steering endorse this recommendation so that an impact statement and proposal may be prepared by InCommon Operations.. The body of this document provides further details for consideration by Steering.

Background

At its best, federation is frictionless: community members connect to resources securely and efficiently, with minimal direct interaction with the infrastructure making it all possible.

There is one notable exception to this: identity provider discovery. Users are prompted to identify their institution of origin in order to be redirected to a familiar and appropriate institutional single sign-on experience before being routed to the requested resource. This singular touchpoint becomes the basis of that user's impressions about federation: was it easy? Was it intuitive? Did it look polished?

Due to past technical constraints, the community has traditionally favored recommending Service Provider (SP) operators to run their own discovery service. Some of these constraints have been:

- Concerns around dependencies on off-prem services
- Constraints around branding
- Constraints around including non-InCommon registered IdPs
- Constraints around excluding out-of-scope InCommon IdPs

This situation has led to end-user experience inconsistencies and missed opportunities at this critical point of interaction.

The alternative to SP-managed discovery services is a centralized, Federation-run discovery service. InCommon offers such a service today but it is not widely used. As of the end of 2021, the current discovery service is mostly used by some internal Internet2/InCommon services and services run by the University of California Office of the President.

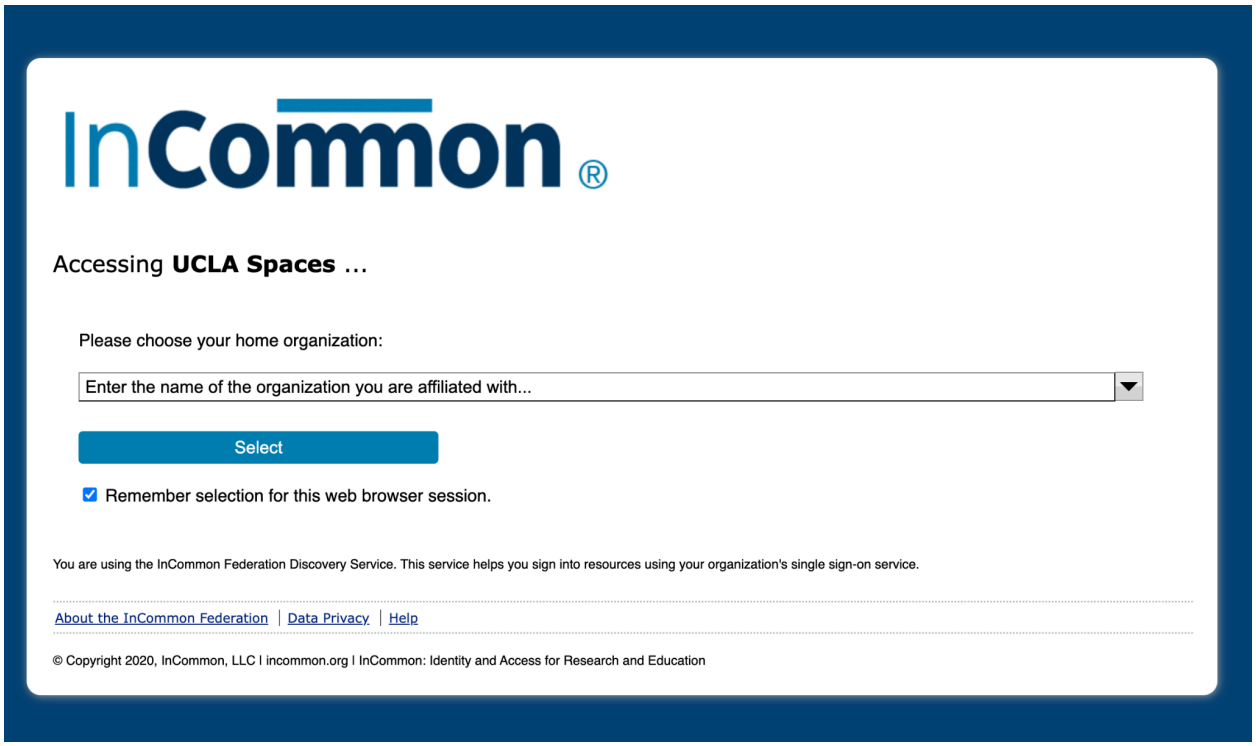
The current discovery service will likely need to undergo significant updates in 2022 for InCommon to continue to offer a common Discovery Service for its participants. This creates an opportunity to rethink InCommon discovery to make Federation a better experience for end-users, as well as SP operators.

Approach

An assessment of InCommon Discovery Service's future rests significantly with Steering's preference on a number of business strategy considerations (for example branding, financial, and resource allocation). However, Steering is likely to look to TAC to answer a number of technical/operational questions. This TAC discussion is meant to help TAC prepare for any questions from Steering, and to better advise the InCommon operational teams on deployment paths and any communication to the InCommon community.

Current State

Several recent developments have led to an opportunity to re-evaluate the future of Federation discovery services in the context of the current InCommon Discovery Service deployment (see below):



Scaling Concerns

As the InCommon Federation (and peer federations through eduGAIN) grows, the increased compute requirements to operate a discovery interface has become a significant technical challenge. With nearly five thousand institution IdPs in eduGAIN and growing, the computation overhead to load, parse, and render this large number of entries using existing tools (at InCommon and those deployed using service provider installed discovery modules) creates delays and degrades the user experience.

Further, increased use of federated single sign-on have created surges to access the Discovery Services that are overwhelming current infrastructure and causing service degradation.

Opportunities

In evaluating options for addressing scaling and sustainability of the InCommon Discovery Service, the TAC has identified the following opportunities:

Rethinking SP-hosted Discovery

An SP-hosted discovery model affords the SP operator flexibility to customize and incorporate the discovery experience with its environment. The downside is that it introduces additional infrastructure to maintain for an SP operator. The TAC is interested in “making it easy” to federate the recommended way for all parties.

Branding and User Experience

Discovery is one of the only places where a user visually experiences federation in action. By investing in a good discovery service experience, InCommon can capitalize on a valuable opportunity to convey the value of federation to our users in an intuitive way.

Encouraging the use of a centralized discovery service over an SP-hosted model reduces overhead for SP operators, ensures quality control in the login experience, and simplifies support communication.

Alignment with SeamlessAccess and global federation community’s position regarding Home Organization Discovery

Organizations in the global federation community have begun adoption. GÉANT, REFEDS, SUNET/SWAMID (the Swedish federation), among others, have begun deploying SeamlessAccess as its Discovery interface. Joining the community to adopt a globally scalable discovery service lets us leverage the significant investments already made into researching and implementing a discovery experience tailored to the needs of the R&E community.

TAC’s Recommendation to Steering Committee

SeamlessAccess (What is SeamlessAccess?) was developed as a collaboration between the R&E federation community and the journal publishing community as a way to introduce a uniform, intuitive, and easily recognized federated single sign-on experience across federations around the world. TAC conducted an analysis of several possible courses of action to evaluate InCommon’s best path forward. TAC concluded that in order to best seize the opportunity to present a positive and intuitive impression of “federation” to a user and to address immediate technical challenges, InCommon should adopt SeamlessAccess, in standard integration mode, as its central discovery service. In addition, InCommon should encourage participants to use this new central, global discovery service instead of implementing its own.

Adoption Challenges and Operations Implications

While SeamlessAccess provides a robust, user-friendly discovery experience, there remain issues requiring Steering’s input before InCommon can deploy SeamlessAccess as its official central discovery service:

Ensuring service availability

A central discovery service used federation-wide is a mission-critical federation component, not unlike a DNS is to networking. Disruption to Discovery Service impacts authentication for all federation users. The current infrastructure is operated by GÉANT from European data centers. Network interruptions outside the US can disrupt service in the US. Ideally, InCommon should provide a redundant US mirror of the SeamlessAccess infrastructure.

One note worth mentioning is that today, InCommon isn't staffed to operate a 24/7, highly available, mission-critical system. Additional resources will likely be necessary to upgrade InCommon operations to provide mission-critical incident handling and service recovery functions.

Enforcing/conveying trust

SeamlessAccess is designed to be inclusive. It accommodates (i.e. lists) identity providers from eduGAIN member federations as well as additional organizations outside eduGAIN. Not all organizations adhere to the same operating and security policies common to R&E federations.

When deploying SeamlessAccess as InCommon's Discovery Service, the community needs to weigh several key issues in order to ensure a user can readily identify, therefore choose the correct, trusted identity provider registered by their home institution. Answers to these questions may drive future enhancements in SeamlessAccess. Issues to ponder include:

Which Identity Providers should be included in the InCommon Discovery Service?

An InCommon-registered resource provider may have users who need to sign in from other national federations in eduGAIN (e.g., UK researchers accessing NIH resources). Therefore, only listing InCommon-registered IdPs isn't sufficient. Today's default is to list every identity provider published in eduGAIN. Should we include those identity providers outside eduGAIN?

Some service providers wish to filter the IdP list in such a way that only organizations with established business relationships (e.g., customers) are listed in order to reduce user confusion. This has been one of the key drivers for resource providers to operate a discovery service on their own. Should a central service accommodate such a need?

What should InCommon's position be regarding the use of the new Discovery Service?

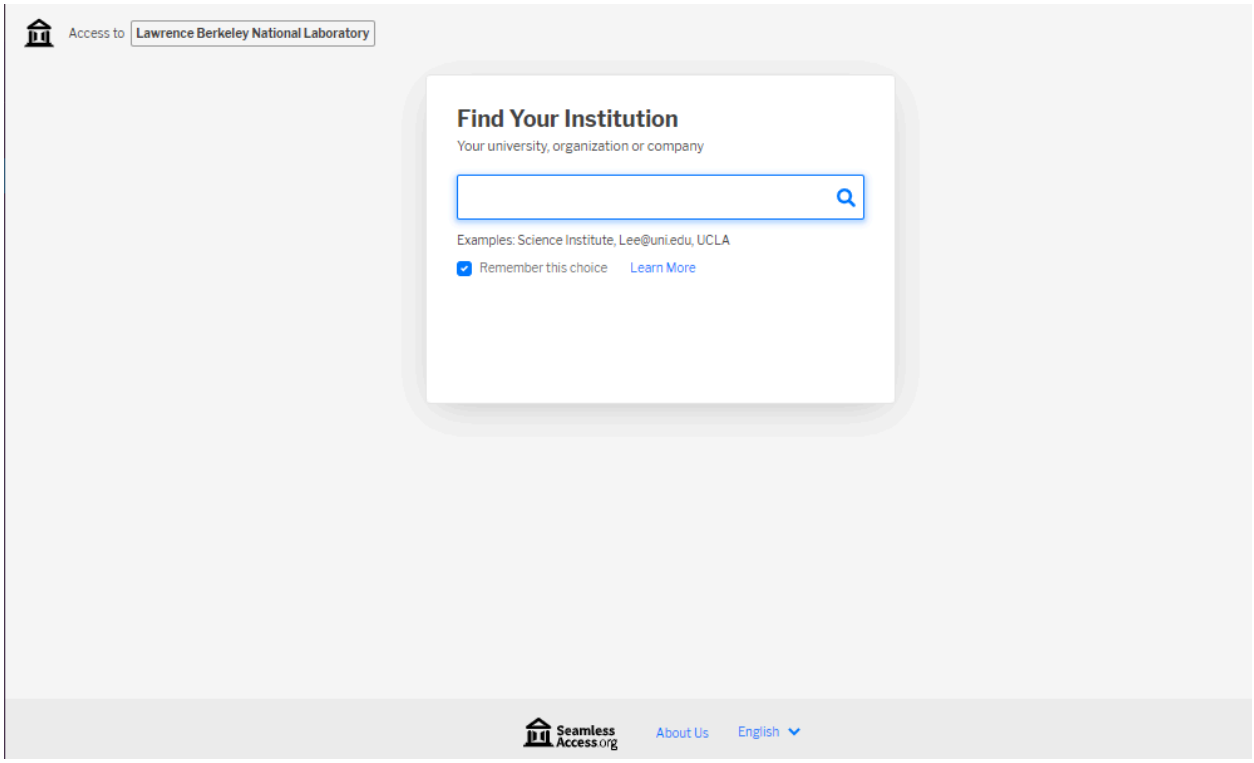
InCommon historically has not pushed for the use of the central discovery service. If our goal is to establish a trusted, uniform visual identity for "InCommon", do we require all participants to use this central discovery service? If not, do we need to establish additional guidance on what is considered an "InCommon-compatible" discovery service?

How do we communicate in an intuitive way to an end-user that a listed entry is the correct IdP registered by their home to the end-user?

“InCommon” is not a household name among end-users. Simply tagging an entry with the label “InCommon” doesn’t necessarily increase recognition or convey trust. This question brings up the global perspective as well: should such Trustmark be a global one (e.g., eduroam)?

Branding implications

By adopting SeamlessAccess, we hope to leverage its intuitive user interface (see below) to create a positive impression of federated access, particularly with the InCommon Federation.



The current SeamlessAccess interface is branded only as SeamlessAccess, with no indication that R&E federations are behind it. The TAC feels that Federation-specific branding does not advance the general goals of trust federations.

Appendix A: TAC's Analysis on Possible Courses of Action

The TAC has identified the following paths forward for InCommon:

Option 1: Retire the InCommon's Central Discovery Service

If determined that a central discovery service is not needed, InCommon could require all SPs to operate their own discovery service. This may include recommendations to SP operators of one or more discovery services to implement locally, including Seamless Access.

Retirement of the existing Federation discovery service would address concerns about scalability, streamline InCommon's infrastructure, and (due to current usage volume) have minimal impact on SPs. However, the retirement of this tool with no replacement keeps the burden of discovery service management on SP operators and entails the loss of the only visual interaction between the Federation and end-users. It is the opinion of the TAC that this is a significant missed opportunity.

Option 2: Upgrade the existing InCommon Discovery infrastructure

Even with its current limited use, InCommon is seeing dramatic increase in traffic to the existing Discovery Service, presumably due to increased adoption of federated single sign-on among research organizations. This spike in usage has at times overwhelmed the infrastructure and caused service outages. InCommon operation anticipates the usage will continue to increase.

InCommon can continue to operate the current Discovery Service, however, it will need to invest in infrastructure and software upgrades to ensure adequate quality of service.

This option gives the most control over the user experience for users of the discovery service. It also minimizes impact to current users of the Discovery Service.

However, given the cost involved in pursuing this option, the TAC was unable to identify a significant differentiating advantage of this option over transitioning to a competing product.

Option 3: InCommon adopts SeamlessAccess Standard Integration

With this option, InCommon follows SWITCH in adopting Seamless Access as a centralized, Federation-run discovery service.

The TAC favors this direction due to Seamless Access' active development and support, as well as the cost and community advantages to supporting Seamless Access as the emerging standard for discovery services in the R&E community.

The following items were raised by the TAC for consideration with regard to this option:

- SA lacks federation-specific branding today… Although, considering R&E collaboration is increasingly global, is not having a nation-specific branding necessarily a bad thing? (e.g., eduroam)
- Dependency on external infrastructure … we can mitigate this by hosting a load-balanced instance in North America
- (This is where many open questions remain around branding and ability to filter IdP listing. discuss…)
- Because SPs must be registered in a federation to utilize Seamless Access (see beta terms-of-service – https://www.google.com/url?q=https://seamlessaccess.org/services/tos/&sa=D&source=docs&ust=1642032054174079&usg=AOvVaw0kTyMuqsE6xcWKUfj5UBUZ), there may be an increase of test SPs registered.

Appendix B: What is SeamlessAccess?

SeamlessAccess is a service designed to help foster a more streamlined online access experience when using scholarly collaboration tools, information resources, and shared research infrastructure. The service promotes digital authentication leveraging an existing single-sign-on infrastructure through one's home institution while maintaining an environment that protects personal data and privacy.

The direction and implementation for the service came from the RA21 Initiative, a joint project of the International Association of STM Publishers and the National Information Standards Organization. While the origin of the effort was in the scholarly publishing and library communities, the applicability of SeamlessAccess is for all parties that want to use federated identity as part of their authentication and authorization workflows.

Governance of this service is through the Coalition for Seamless Access, a collaboration between four organizations–GÉANT, Internet2, the National Information Standards Organization (NISO), and the International Association of STM Publishers (STM). Each organization participating in the governance committee offers either financial or in-kind support for the operation of the service.

To learn more, visit https://seamlessaccess.org/about/.