InCommon®

Powered by INTERNET2

From Barriers to Best Practices: Community Conversation on Federated Identity in Academic Libraries

Thread Meetup Report

Virtual Session:

March 3, 2026

Table of Contents

Overview 3
Conversation Highlights 3
Considerations for Next Steps 5
    A Path Forward 6
APPENDIX 8
Meeting Recording & Transcripts 8

Overview

The March 2026 Thread Meetup “From Barriers to Best Practices: Community Conversation on Federated Identity in Academic Libraries” brought together librarians, IAM practitioners, identity federation operators, and content vendors for an open dialogue on one of academic libraries’ most persistent challenges: Moving beyond IP-based authentication toward federated identity. Amanda Ferrante, Principal Product Manager, Identity & Access Management at EBSCO and Zhaneille Green, E-Access Librarian at Duke University, opened with a brief recap of their November 2025 “Bridging the Gap” webinar, setting the context before opening the floor to participant discussion. Albert Wu, InCommon Federation Manager at Internet, joined to provide a federation operator perspective.

The conversation highlighted a shared challenge wherein libraries and IAM teams are often solving the same problem from different angles, with little communication between them. That disconnect is a root cause of slow adoption.

Conversation Highlights

- **Large Scale problem**: Amanda Ferrante shared that of the roughly 8,.000 academic libraries that are EBSCO customers and belong to federated identity providers, about 70% are not using their federation for access. Even within the InCommon Federation, where uptake might be expected to be strongest, only about 10% of academic libraries are using it for EBSCO access. The technical solution exists and is available but there are organizational, cultural, and workflow-based barriers.
- **Legacy access is deeply entrenched**: IP-based authentication made sense when research happened primarily on campus, but over time it became baked into licensing agreements, library workflows, and vendor platforms. Today it increasingly fails as users work remotely and arrive from search engines or AI tools. Libraries rarely receive information notifying them of these failures, which makes the case for change difficult to build internally.

- **Library staff and IAM teams operate in separate silos:** From the library side, Zhaneille Green explained how federated authentication introduces friction around institutional fit, capacity, and implementation. Libraries worry about losing control over access decisions, struggle with patron groups that don't fit neatly into IAM systems (especially walk-in users), and often lack the staffing or expertise to navigate SSO terminology, attribute release, and vendor negotiations. From the IAM side, federation was largely built around simpler, research-collaboration use cases, not the complex licensing, patron group, and privacy requirements that libraries must navigate. .
- **Granular access control**: Institutional participants described the real-world complexity of multi-campus systems sharing a single IDP, where licenses apply to only one campus or one department (the law library example came up repeatedly). Configuring bilateral SAML connection with vendors directly while technically possible, is not scalable. One participant described timelines of two months or more per vendor. This reflects a gap in the federation's original design which assumed institution-wide access rather than the department and group level licensing many libraries currently navigate.
- **Privacy is a concern and a misconception**: A recurring theme was that librarians often perceive federation as a privacy risk, assuming it means releasing more patron data to vendors. Albert Wu (InCommon) pushed back on this, noting that privacy is actually a foundational principle of R&E identity federation and that the identity provider has control over what is released. One participant noted that their institution has begun incorporating SSO and attribute release language into licensing agreements to establish data-sharing expectations before implementation begins. The challenge is that many librarians may not be aware that identity providers retain control over what data is released.
- **Access entity categories**: The REFEDS access entity categories (anonymous, pseudonymous, and personalized) could be a key part of the solution but adoption is slow. These categories provide a framework for standardizing what data is shared under what circumstances, and could automate privacy protections in ways that would address many library concerns. However, IDPs must implement supporting identifiers

(Subject ID and Pairwise ID) and assert appropriate assurance levels, which takes meaningful effort. Deployment is not yet widespread and thus creates a chicken-and-egg problem. Vendors won't invest until IDPs adopt and IDPs won't prioritize it until vendors require it.

Considerations for Next Steps

1. **Audit your current authentication mix**
   If your library hasn't recently examined what percentage of e-resource access is happening via IP versus federated identity, now is a good time to start. Many libraries are surprised to learn how much IP access is quietly failing and vendors may not be proactively sharing that data.

2. **Start the conversation between library staff and your campus IAM team**
   If those two groups aren't already in regular communication, that's a good place to begin. Even informal relationship building can open the door to understanding what federation capabilities your institution already has and what patron group or licensing nuances your IAM team may not be aware of.

3. **Understand what attributes your institution currently releases and what you'd what to protect**
   Libraries that have been through federated identity implementation recommend getting clear on your data and privacy policies before engaging vendors. Building attribute release expectations directly into licensing language is a practical model worth considering.

4. **Explore Grouper (or equivalent group management tools) for access control**
   For institutions dealing with multi-campus or sub-group licensing complexity, tools like Grouper can help manage access restrictions without requiring individual bilateral SAML configurations for every vendor. This isn't a complete solution, but can reduce the manual overhead.

5. **Ask your vendors about their federation capabilities and entity category support**
   Many smaller vendors haven't invested in federated identity because demand hasn't been loud enough. Libraries asking pointed questions about SAML support, attribute inspection, and access entity category compatibility can begin to shift that dynamic, especially when asked collectively across institutions.

A Path Forward

The session closed with a sense that this community is at an inflection point. The problems are well understood, and the technical solutions exist, but adoption requires coordination across groups that haven't traditionally worked together. Key areas where the community identified a path forward include:

- **Developing shared language for library-specific access entitlements.** The federation community needs vocabulary that reflects how library licensing actually works, not just broad site licenses, but department-level, patron group-level, and program specific access. This can't be defined by the campus IAM office alone. It requires librarians, content vendors, and federation operators at the same table.
- **Increasing deployment of REFEDS across entity categories.** Getting more IDPs to implement the anonymous and pseudonymous categories is a near-term, achievable goal that could meaningfully reduce the perceived privacy risk of federation for libraries. InCommon is exploring ways to make this an expectation rather than an option.

- **Bringing large content aggregators into the standards conversation.** As Albert Wu noted, when major platforms begin requiring compliance with federation standards as a condition of doing business, adoption accelerates across the ecosystem. Advocacy toward the largest players could have an outsized impact.
- **Continued community convenings like this one.** Participants were asked to complete a post-session survey indicating what programming would be most useful. Future sessions may focus on specific topics such as multi-campus IDP configuration, vendor readiness, or privacy and attribute release frameworks.

InCommon Academy will use feedback from this session to shape upcoming programming and resources. Continue the conversation and learn about upcoming offerings by signing up to join the Federated identity in Academic Libraries Slack Channel hosted by InCommon. This is a space to share resources, lessons learned, and next steps as we work to bridge the gap between library access needs and modern authentication.

APPENDIX

Meeting Recording & Transcripts

Select the following link to access the recording and transcripts:

Zoom Recording Passcode: ^tatP7#S

Please note that audio and chat transcripts are available within the recording.