

A detailed botanical illustration in a light gray tone serves as the background for the slide. It features a variety of plants, including a large, dark, textured leaf in the upper right, a cluster of small, delicate flowers in the lower right, and several long, thin, grass-like stalks extending from the top right towards the center. The overall style is reminiscent of 19th-century scientific illustrations.

Simplifying Federated Access to Scholarly Content and Services

Lisa Janicke Hinchliffe (@lisalibrarian)

University of Illinois at Urbana-Champaign

Ralph Youngen (@ryoungen)

American Chemical Society

IAM Online – May 13, 2020

Context

- Publishers license content/services to libraries that are then made available to entitled users.
 - Note: Not all who attempt access to a resource are entitled.
- Authentication/authorization systems support access for entitled users and prevent access for non entitled users.
- Considerations for managing personal data for access – especially with respect to privacy – include legal, contractual, and ethical frameworks.



Terminology

“Discovery”

- In scholarly communications: Conducting literature searches to discover disclosed research pertinent to one’s interest
- In federation operations: Searching for one’s identity provider to initiate a user authentication workflow

“Metadata”

- In scholarly communications: Information about a published research work
- In federation operations: Information about Identity Providers and Service Providers



The Scholarly Authentication/Authorization Ecosystem

Device Authorization

IP Address Recognition

- Device IP address in institution namespace
- Asserting that the user of the device is authorized user

Remote IP Recognition Options

- VPN
- Proxy Servers

Individual Authentication

Publisher-specific accounts

- Typically for personalized features only
- Typically do not provide authorization

Federated Authentication via SAML: Security Assertion Markup Language

- Validates the end user, not the device
- Provides authorization
- Shibboleth is a specific implementation of the SAML protocol

The Scholarly Authentication/Authorization Ecosystem

Device Authorization

IP Address

- Device name
- Asserting that the user of the device is authorized user

Remote IP Recognition Options

- VPN
- Proxy Servers

Individual Authentication

Library May be Using Any and/or All of These features

Do not provide authorization

0

Federated Authentication via SAML:
Security Assertion Markup Language

- Validates the end user, not the device
- Provides authorization
- Shibboleth is a specific implementation of the SAML protocol

The Scholarly Authentication/Authorization Ecosystem

Device Authorization

IP Address Recognition

- Device IP address in institution namespace
- Asserting that the user of the device is authorized user

Remote IP Recognition Options

- VPN
- Proxy Servers

Individual Authentication

Publisher-specific accounts

- Typically for personalized features only
- Do not provide authorization

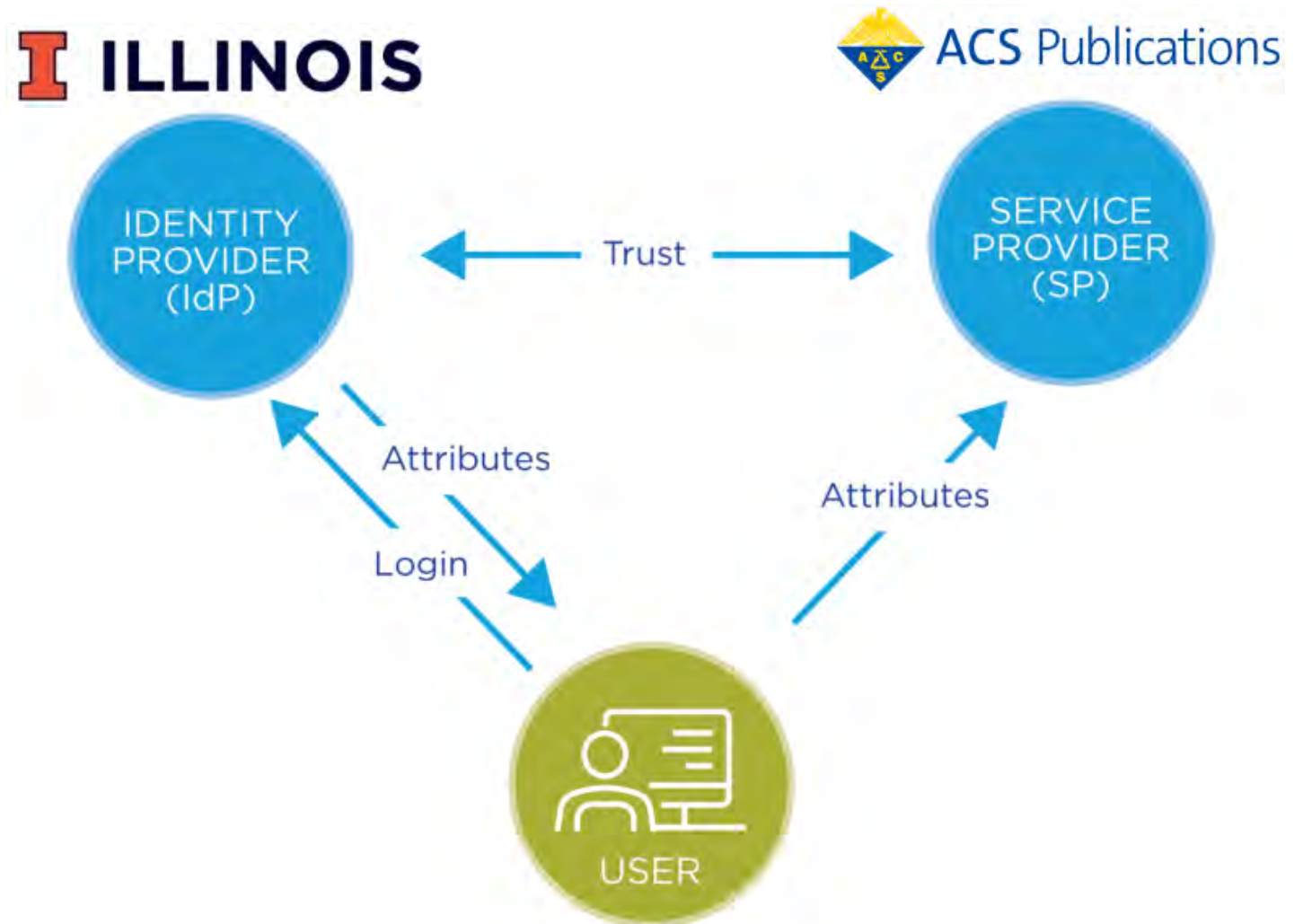
**Today's
Focus**

Federated Authentication via SAML: Security Assertion Markup Language

- Validates the end user, not the device
- Provides authorization
- Shibboleth is a specific implementation of the SAML protocol

Federated Authentication/SAML/Shibboleth

- Built upon system of trust between identity providers (e.g. academic institutions) and service providers (e.g. publishers)
- Identity provider controls the information (i.e. attributes) about its users that gets sent to service providers



What is (was) RA21?

RA21 Initiative

- Resource Access in the 21st Century
- Sponsored by NISO and STM
- Began in 2016
- Pilot projects to test various technical solutions and user experiences, including a pilot with corporate librarians from pharma companies
- Ended June 2019

Outcome

- NISO Recommended Practice, published in June 2019



What is SeamlessAccess?

A **coalition** of 5 founding organizations:

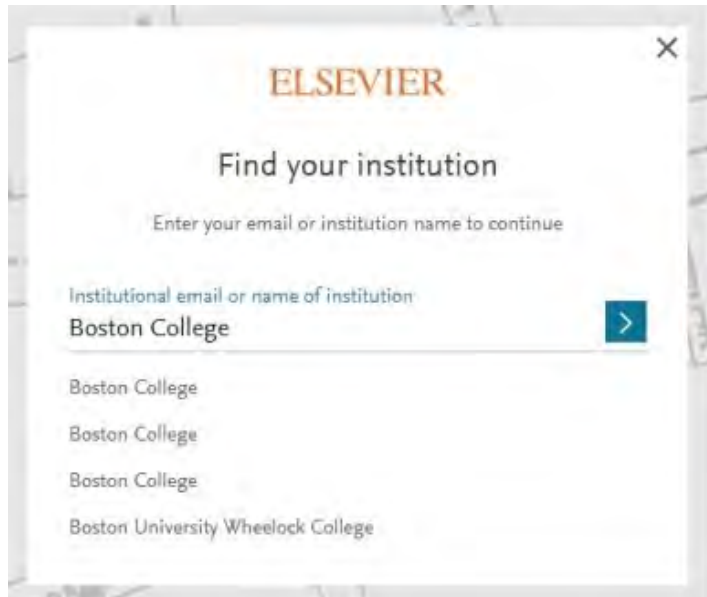


Community-driven effort to support seamless access to information resources, scholarly collaboration tools, and shared research infrastructure

SeamlessAccess is creating an operational service based upon the RA21 recommended practices

SeamlessAccess Provides an Improved User Experience

Makes SAML “Where Are You From” Easier to Navigate for End User



ELSEVIER

Find your institution

Enter your email or institution name to continue

Institutional email or name of institution
Boston College

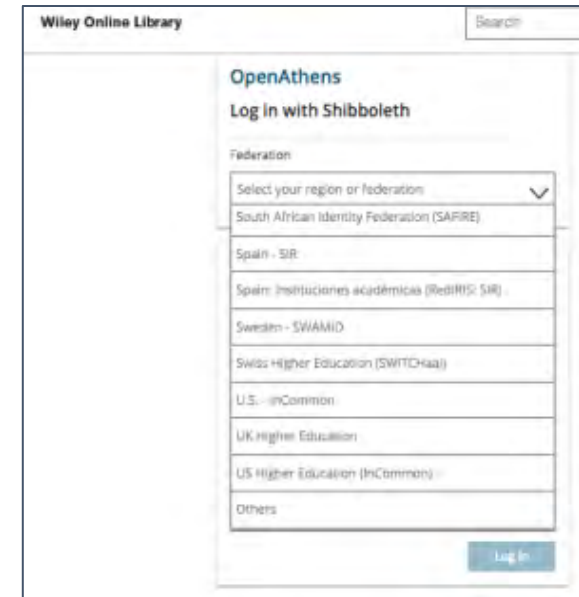
Boston College
Boston College
Boston College
Boston University Wheelock College

>

Information about user's institution(s)
saved in the local browser

Trusted service providers are able to
access this institution data

Reduces the number of times a user
must search for their institution



Wiley Online Library

OpenAthens

Log In with Shibboleth

Federation

Select your region or federation

South African Identity Federation (SAIF)

Spain - SIF

Spain: Instituciones académicas (RedIRIS: SIF)

Sweden - SWAMID

Swiss Higher Education (SWITCHaa)

U.S. - InCommon

UK higher Education

US Higher Education (InCommon)

Others

Log In



Find your partner institution:

Boston College

CONTINUE →

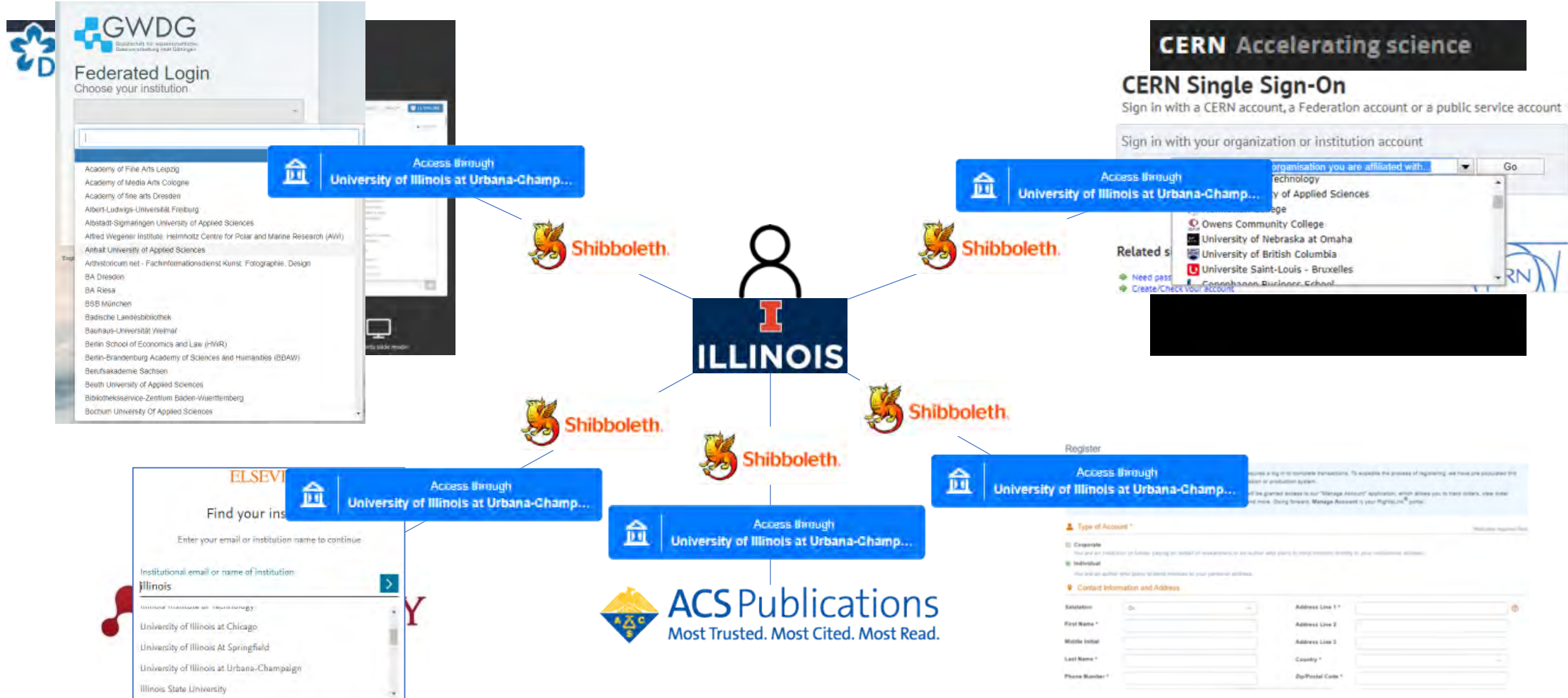


Find my institution | Log In

My Activity

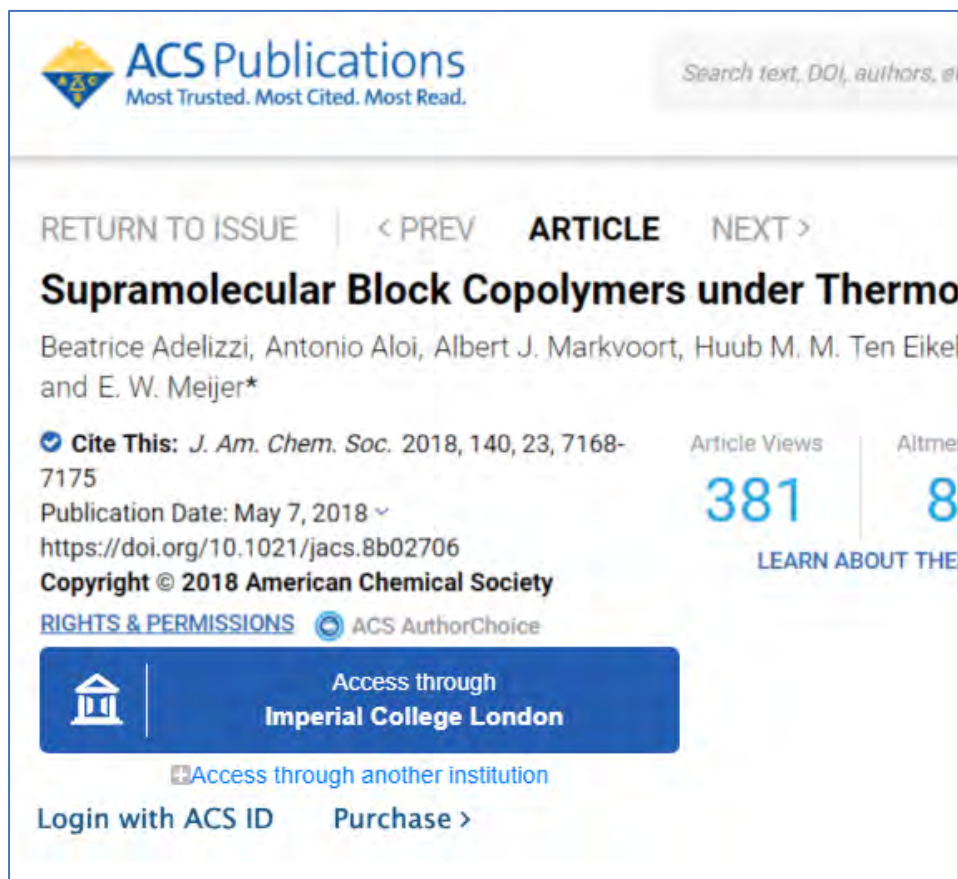
Publications

Toward A More Seamless World

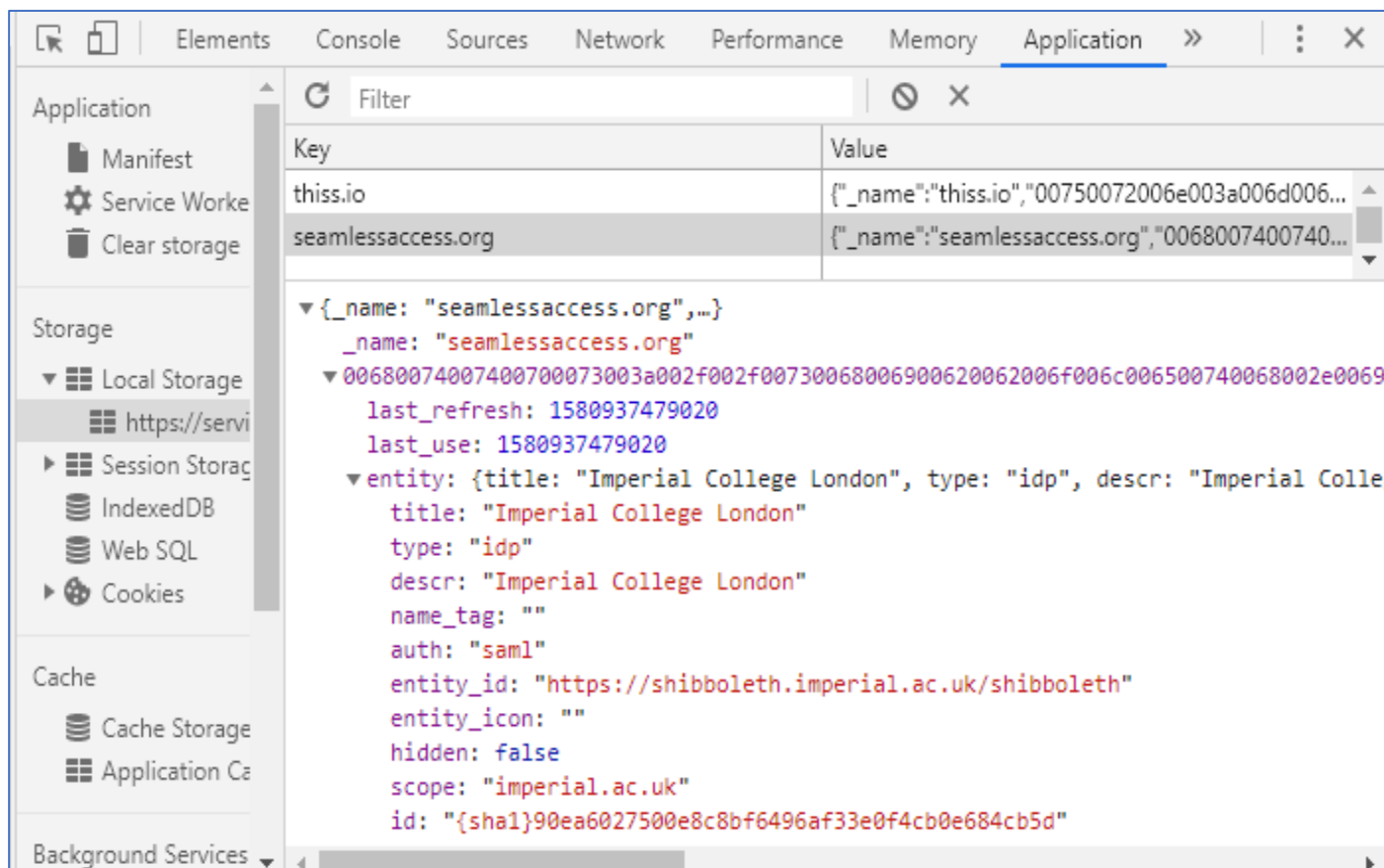


What does SeamlessAccess do, specifically?

Enables the ability for sites to display the “Access through <<your institution>>” button by using data about the user’s institution(s) via browser storage



The screenshot shows the top of an ACS Publications article page. The article title is "Supramolecular Block Copolymers under Thermo". Below the title, the authors are listed: Beatrice Adelizzi, Antonio Aloï, Albert J. Markvoort, Huub M. M. Ten Eike, and E. W. Meijer*. The article is from J. Am. Chem. Soc. 2018, 140, 23, 7168-7175. The page has 381 article views and 8 altmetrics. A blue button labeled "Access through Imperial College London" is prominently displayed. Below it, there is a link to "Access through another institution". At the bottom, there are links for "Login with ACS ID" and "Purchase >".



The screenshot shows a browser's developer tools with the Application tab selected. The left sidebar shows the Storage section, with Local Storage expanded. The right pane shows the data for the key "seamlessaccess.org". The data is a JSON object with the following structure:

```
{_name: "seamlessaccess.org", ...}
  _name: "seamlessaccess.org"
  00680074007400700073003a002f002f00730068006900620062006f006c006500740068002e0069
    last_refresh: 1580937479020
    last_use: 1580937479020
    entity: {title: "Imperial College London", type: "idp", descr: "Imperial Colle
      title: "Imperial College London"
      type: "idp"
      descr: "Imperial College London"
      name_tag: ""
      auth: "saml"
      entity_id: "https://shibboleth.imperial.ac.uk/shibboleth"
      entity_icon: ""
      hidden: false
      scope: "imperial.ac.uk"
      id: "{sha1}90ea6027500e8c8bf6496af33e0f4cb0e684cb5d"
```

What does SeamlessAccess not do?

- SeamlessAccess is not involved in the actual federated authentication process.
- Service providers (e.g. publishers) and identity providers (e.g. academic institutions) must already have an existing relationship that supports SAML-based federated authentication for SeamlessAccess to work.
- Example:
 - A campus running Shibboleth is a member of an identity federation like InCommon
 - A publisher is also a member of InCommon and supports SAML federated authentication
 - The InCommon federation governs the policy framework and facilitates the exchange of SAML configuration details between all parties in a federation

Dependencies for SeamlessAccess to Work:

- Institution must have SAML service.
- Library must request SAML be enabled for publisher platform.
- Publisher must enable SAML on platform.
- Publisher must implement Seamless Access service.
- User must authenticate through SAML on a Seamless Access enabled publisher platform.
- If user is using the same browser on the same device, then Seamless Access will work on all enabled platforms.
- User authenticates.

Who is SeamlessAccess?

A **governance committee** with representatives from across the stakeholder groups

An **implementation team** including:

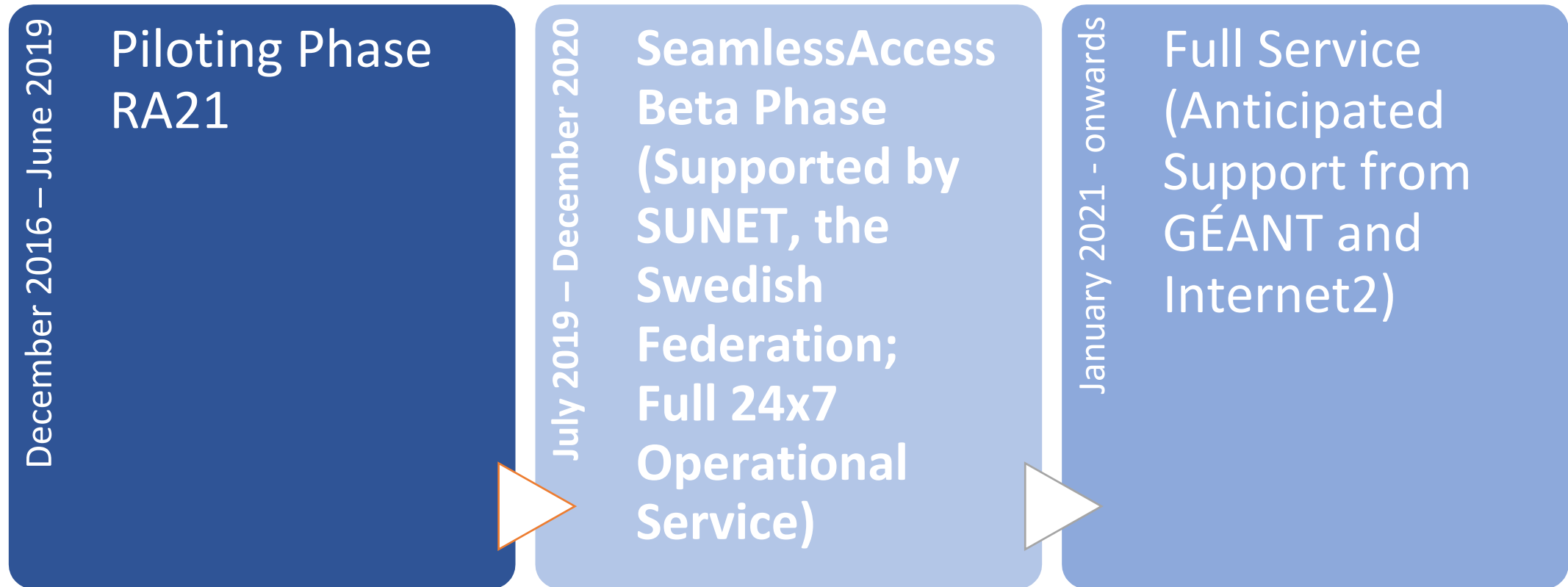
- Project Director
- Publisher Outreach
- Technical support from SUNET (with funding from GÉANT)
- Library Outreach
- User Experience

An **outreach committee** including representatives from 6 libraries

An **attribute release working group**

A **contract language working group (coming soon)**

What is the current status of SeamlessAccess?



Where is SeamlessAccess Implemented?

In Progress

- CCC
- DARIAH
- Elsevier
- O'Reilly
- Silverchair platform
- Taylor & Francis
- Wiley

Integrated

- ACS
- Atypon platform
- Springer Nature
- SUNET
- TENET

COVID-19: Expanding Federated Access

February 2020:



赛尔网络
CERNET



中国教育和科研计算机网
China Education and Research Network

“As you may know, a new outbreak of coronavirus has recently occurred in China. ... all students are required to study online at home. However, now traditional remote access faces significant pressure by the limitation of VPN capacity ... CERNET is actively promoting service providers to join CARSI (CERNET Authentication and Resource Sharing Infrastructure) to help users access ... CARSI bases on the Shibboleth system, it's among the world's most widely deployed federated identity solutions”

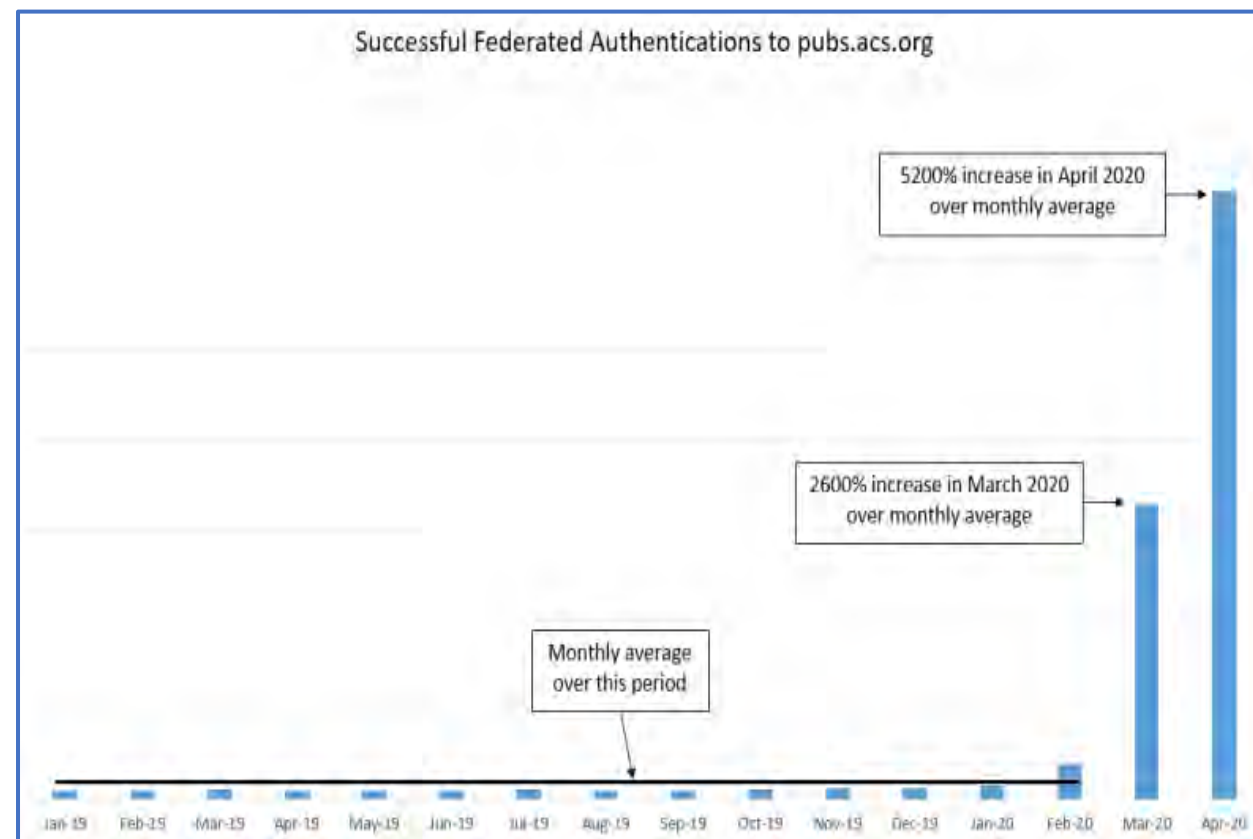
March 2020:



ACS Publications' Experience

March/April saw a significant increase in federated authentications, likely due to:

- Shift in demand for remote access due to campus closures
- Deployment of the SeamlessAccess user experience on March 1, 2020
- Expansion of institutions enabled for federated access:
 - For existing federations, associating an IdP's EntityID with subscription record enables WAYF discovery
 - Also joining many new federations



Lessons Learned – Attributes

Many IdPs are asserting personally identifiable attributes even though ACS is not requesting them

- A bug on the ACS site displayed the user's first name if supplied via attributes:

Access provided by University of Illinois at Urbana-Champaign Library | Welcome: Mary | Logout

- Now corrected even if personally identifiable attributes are received:

Access provided by University of Illinois at Urbana-Champaign Library | Log In

- SeamlessAccess is sponsoring an Entity Categories and Attribute Bundles Working Group to help IdPs select the appropriate attribute set for a given SP
 - Authorization Only (no attributes), Anonymous, and Pseudonymous
 - Publisher SPs likely will request Pseudonymous to assist campuses with credential theft

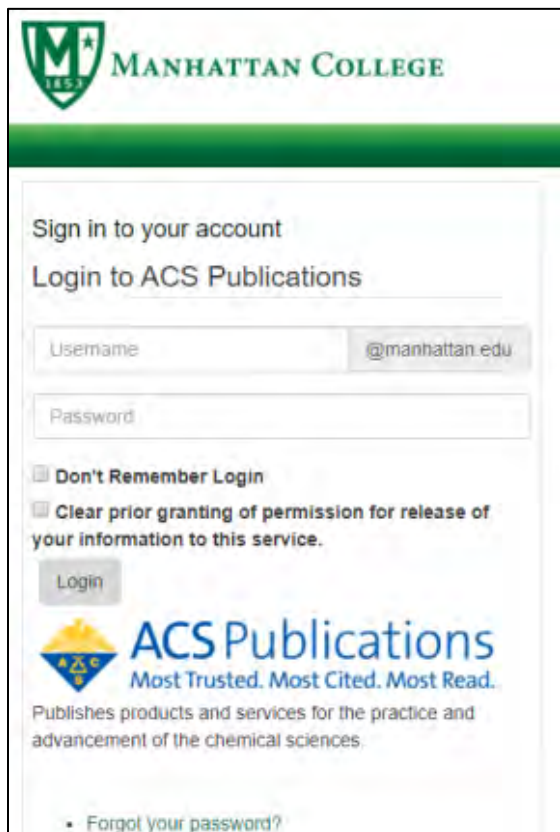
Lessons Learned – IdPs for University Systems

- Some university systems run a single IdP for multiple campuses
 - E.g. Indiana University system, University of Alaska system
- No standard way to associate users with their affiliated campuses using attributes
 - Important both for authorization and for usage reporting
- Discussing a concept with David Bantz (Chair, InCommon Community Trust and Assurance Board)
 - IdP asserts both primary affiliation and list of all affiliated campuses
 - SP would check authorization at primary affiliation, then others as needed

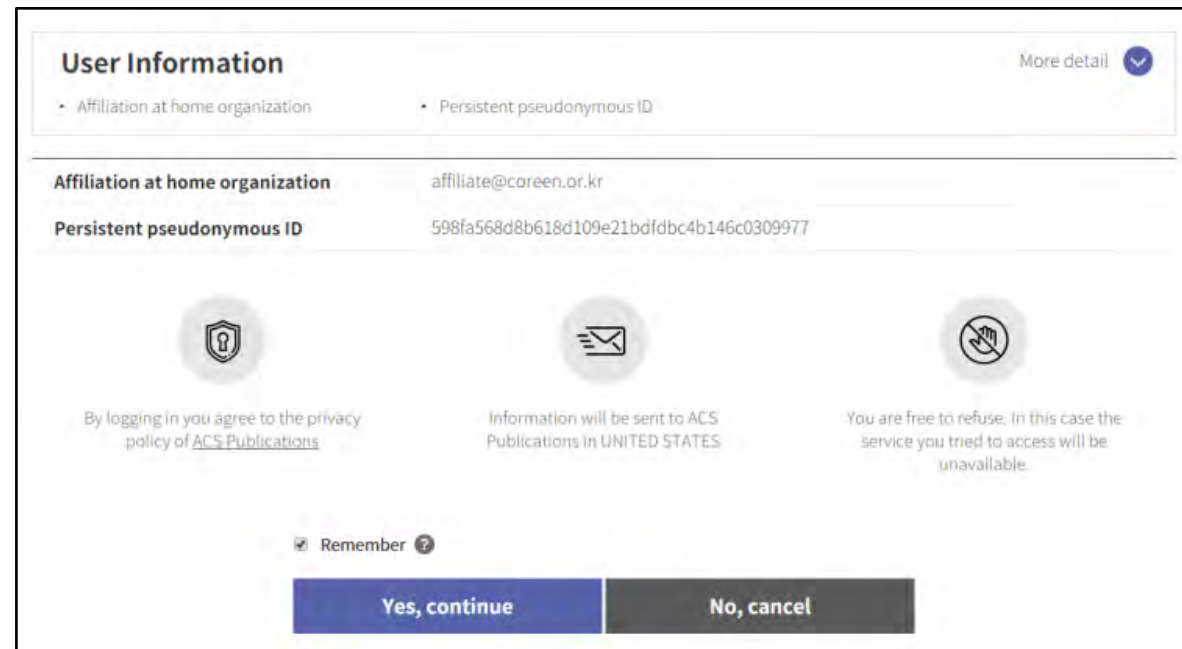
```
<saml2:Attribute
  FriendlyName="https://iam.alaska.edu/trac/wiki/mauAffiliations"
  Name="urn:oid:2.5.4.11" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xsd:string">UAA</saml2:AttributeValue>
  <saml2:AttributeValue
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xsd:string">UAF</saml2:AttributeValue>
  </saml2:Attribute>
<saml2:Attribute
  FriendlyName="https://iam.alaska.edu/trac/wiki/mauPrimaryAffiliation"
  Name="urn:oid:1.2.840.113556.1.4.261" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xsd:string">UAA</saml2:AttributeValue>
  </saml2:Attribute>
```

Lessons Learned – User Experience

User consent for attribute release is sorely needed, e.g.:



The screenshot shows the Manhattan College login page. At the top is the college's logo and name. Below is a green header bar. The main content area has a light blue background with the text "Sign in to your account" and "Login to ACS Publications". There are input fields for "Username" (with "@manhattan.edu" as a placeholder) and "Password". Below these are two checkboxes: "Don't Remember Login" and "Clear prior granting of permission for release of your information to this service.". A "Login" button is present. At the bottom is the ACS Publications logo and tagline "Most Trusted. Most Cited. Most Read." with a brief description of their services and a link for "Forgot your password?".



The screenshot shows a "User Information" consent screen. At the top, it says "User Information" with a "More detail" link. Below are two sections: "Affiliation at home organization" with the value "affiliate@coreen.or.kr" and "Persistent pseudonymous ID" with a long alphanumeric string. Below these are three icons with corresponding text: a shield icon for "By logging in you agree to the privacy policy of ACS Publications", an envelope icon for "Information will be sent to ACS Publications in UNITED STATES", and a hand with a slash icon for "You are free to refuse. In this case the service you tried to access will be unavailable.". At the bottom are two buttons: "Yes, continue" and "No, cancel".

Use of SP's MDUI elements (i.e. DisplayName, Description, Logo) can help users understand the federated authentication workflow

What is GetFTR (Get Full Text Research)?

- A new service under development by the scholarly publishing community that also leverages federated authentication.
- Provides on-the-fly verification of a user's entitlement rights to a research article based on the user's institutional affiliation.
- Works with publisher platforms to determine entitlement status using two pieces of information:
 - Unique identifier for a document (DOI)
 - Unique identifier for an institution (EntityID)
- Compatible with (all of) today's research discovery tools, scientific collaboration networks, library resource management systems, etc.

How Does GetFTR Work?

- Returns “smart links” (WAYFless URLs) customized for the user’s institution

Effect of thermal treatments on anti-nutritional factors and antioxidant capabilities in yellow soybeans and green-cotyledon small black soybeans

Authors: Huai-Wen Yang, Cheng-Kuang Hsu, Yu-Fei Yang

Journal: Journal of the Science of Food and Agriculture

Publisher: Wiley

DOI: 10.1002/jsfa.6494

 View PDF

Your institution provides access to this article

- These links work regardless of the user’s physical location.
 - If connected to a campus network with a recognized IP address, institutional access is provided based upon IP address recognition.
 - If away from a campus network, institutional access is provided via federated authentication.
 - GetFTR plays no role in the federated authentication workflow between the user and the publisher.

Final Thoughts

- Campus IT and campus libraries need to work together.
 - Determine appropriate attribute release policies for SPs procured via the library.
 - Implement an attribute release user experience for your campus.
 - Determine contract language, where appropriate.
- Findings from recent survey conducted by SeamlessAccess indicates some areas for improvement between campus IT and campus libraries:
 - 72% of IT respondents said they had implemented federated authentication for library resources, while only 46% of library respondents said they had.
 - 88% of library respondents who had implemented federated authentication said they worked with IT.
 - 94% of IT respondents indicated the library was minimally involved; only 20% said library was very involved.

Final Thoughts (cont.)

- Send publisher SPs pseudonymous identifiers for users.
 - Stop sending personally identifiable attributes.
 - Pseudonymous attributes (e.g. eduPersonTargetedID) can greatly assist campuses to identify compromised user credentials without compromising privacy.
- Expansion of federated authentication is underway and will likely continue.
 - Logging for SeamlessAccess service is very limited by design to protect user privacy
 - Taking a conservative approach, in April 2020 SeamlessAccess observed between 1-2 million user flows, mostly from ACS and nature.com.
- A new divide is emerging between institutions that already support federated authentication and those that do not.
 - U.S. Department of Education lists more than 4,000 degree-granting academic institutions, compared to 558 IdP members of InCommon.
 - Large institutions are more likely to support federated authentication. Better support is needed to help smaller institutions to learn how to get started.

Comments?
Questions?
Discussion?



IAM Online - Special Edition - How do YOU use eduroam?

May 18, 2020 - 2 pm ET | 1 pm CT | Noon MT | 11 am PT

A look at how three organizations have leveraged eduroam to meet new and emerging needs for online learning.

June IAM Online - Hiring for Identity and Access Management

June 10, 2020 - 2 pm ET | 1 pm CT | Noon MT | 11 am PT

Challenges and opportunities for both CIOs and identity management professionals in higher education.

InCommon Trusted Access Platform Training

<https://incommon.org/academy/software-training/>

Software Component	Virtual Training Dates	Early-Bird Rate Deadline
COmanage	May 19-20, 2020	Passed
Grouper	June 2-3, 2020	Passed
midPoint	June 16-18, 2020	May 15, 2020

InCommon Virtual BaseCAMP

July 20-24, 2020 (Noon - 4 pm ET each day)

- An introduction to identity and access management basics
- An introduction to the InCommon Federation
- An overview of the community-built InCommon Trusted Access Platform services and software

Program and registration information: <https://meetings.internet2.edu/2020-basecamp/>

IAM Online Evaluation

<https://www.surveymonkey.com/r/IAMOnline-May-2020>