Seamless Access

The successor to IP Filtering

Rich Wenger

E-Resource Systems Manager, 4/1/2003 – 3/31/2019

MIT Library

Disclaimer

- IANL
- I am retired and do not speak for the MIT Library.

TOC

- Brief review of RA21 and its accomplishments
- A more detailed look at SeamlessAccess.org.
- A demo of the central services currently in beta status.
- The view ahead

In the beginning…

- Early days of the internet
- No portable devices or smart phones
- Static IP addresses
- Unspoken assumptions

The march of technology

- Portable PCs, laptops, tablets, smart phones
- DHCP: dynamic IP addresses
- ‘Off-campus’ users

Playing games

- **Pretending nothing had changed:** Proxy servers and VPN

- Virtualization at multiple levels: e.g. NAT

Bottom line

- The assumption that an IP address reliably indicates a user's physical location is **false**.
- The further assumption that a physical location reliably indicates an authenticated, authorized user is **false**.
- IP filtering is about **where** a user is (which is completely obscured by proxy servers and VPNs), not **who** the user is.

Bottom line

- **<u>IP filtering</u>**
  - Conflates IP address with location and identity.
  - Requires proprietary portals, in direct opposition to modern discovery practices.
  - Is a maintenance nightmare when IP ranges change.
  - Is unsecure and easily exploited.
    “Without IP filtering, Scihub could not exist”*

- * Atypon presentation on Data Piracy at SSP confernece in Boston, June 2017

Two major areas of concern

- Improve the user experience
- Respond to the security deficits

Improving the user experience

- The point of referral for authentication must be located at providers' sites, not in our portals.
- Institutional affiliation defaults must be preserved across browser sessions and vendors without compromising privacy.
- All devices must be supported appropriately.
- Patrons' privacy must be preserved.

Security

- Focus on who the patron is, not on where they are.
- Use institution credentials, not proprietary ones.
- In case of inappropriate downloading, individual sessions can be blocked.
- Support SSO across all devices.

A way forward

- **Federated Identity Management, robustly implemented by providers and subscribers.**
  - SAML-based: highly secure, stable, open source.
  - Federated metadata.
  - Authentication at the point of need, using institutional credentials.
  - Support for affiliation at multiple institutions.

RA21: 2016 - 2019

- **Two major outputs**
  - A detailed set of recommended best practices certified by NISO.
  - A small set of light-weight central services hosted by a non-profit consortium.
    - Standardized WAYF menu
    - Persistent storage of institutional affiliation(s).

STM The global voice of scholarly publishing

INTERNET2

NISO How the information world CONNECTS

ORCID Connecting Research and Researchers

GÉANT

IFLA International Federation of Library Associations and Institutions

(Early Discussions)

SeamlessAccess.org

Infrastructure Collaboration for FIM:
Federated Identity Management
for more streamlined digital authentication

Heather Flanagan, Program Director

What is SeamlessAccess.Org?

- The operational successor of RA21.

- Implementing the Best Practices as described in NISO document:

Recommended Practices for Improved Access to Institutionally-Provided Information Resources: Results from the Resource Access in the 21st Century (RA21) Project

- Built on thiss.io

Summary of NISO-certified best practices

- Guiding principles for:
  - Privacy
  - Security
  - User experience
  - Governance.

Summary of NISO-certified best practices

- Recommended practices:
  - 2.1 Adopt Multilateral **Federated** Authentication.
  - 2.2 Establish Multilateral Federations where they do not exist.
  - 2.3 Ensure Privacy is Preserved while Enabling Convenient SSO and Granular Authorization.
  - 2.4 Improve the User Experience of Identity Provider Discovery (WAYF menu).
  - 2.5 Establish a Cross-domain Identity Provider Persistence Service.

Summary of NISO-certified best practices

- Recommended practices:

2.6 Improve Metadata Quality and Apply Consistent Standards.

2.7 Set Session Timeout Periods based on Type of Resource and Institutional Risk Management Policy.

2.8 Establish Security Incident Reporting Frameworks

2.9 Leverage new or Existing Inter-federation Services for SP and IdP Interoperability.

Summary of NISO-certified best practices

- Endorsement of GÉANT Data Protection Code of Conduct:

  GDPR compliant.

Federated Identity Management, FIM: Why is FIM so important ?

- For streamlined online access from any place and any device into:
  - Library resources
  - Research facilities
  - Collaborative labs
  - Scholarly collaboration tools
  - Open Science platforms
  - Open Access authoring sites
  - Preprint servers, sharing sites, etc
- For preservation of user privacy via SAML federated authentication technology

FIM4R Federated Identity Management For Research

See initiatives for

FIM4R: Researchers

FIM4L: Libraries

Tackling several Big Issues:

- **Privacy** – leveraging a distributed technical approach, working with librarians, academia, infrastructure partners; a system from scholars for scholars, the data stays at and belongs to the institute
- **Transparency** - we are transparent with everyone about how it works, what the approach is, where the data remains
- **Interoperability** – this is infrastructure, operated by GÉANT, that works for all institutions. Any provider of resources can join,
- **Speed & Convenience & User Experience** – integrated design and architecture, serves as the backbone of the collaboration between GÉANT, STM, NISO, Internet2 and ORCID.

Made to support a shared research infrastructure

- For more Open Science
- For more international research collaboration.
- For access to resources from any place and any device.
- For secure identity management and network safety.
- For local management of data privacy issues.

Governed and initiated by:

STM

NISO

GÉANT

Internet2

ORCID

(Invitation extended to IFLA

Int'l Federation of Library Associations**)**

SeamlessAccess.org preserves user privacy and maintains institutional control for secure access

A Modern and Reliable Approach to Resource Access

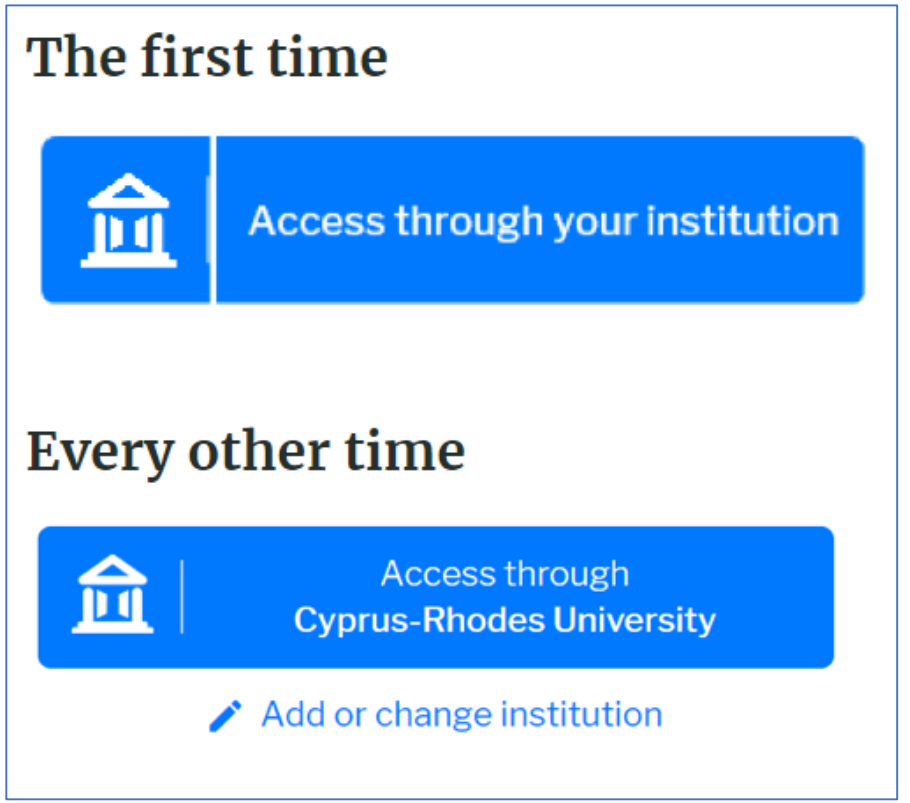
- Ensure access to resources and services to those entitled to have it. It is increasingly complex to identify legitimate users. Seamless Access enables access using individual's federated authentication (sign on.)

Proven User Experience

- The Seamless Access solution remembers user's last sign-on choice, simplifies institution search, and uses clear language and images to meet user expectations.

Single Sign On… For Real!

- Seamless Access enables true Single Sign On. Users will be able to sign in using their preferred sign in credentials (for example, those from their institution), and will not be bothered for them again for all Seamless Access-enabled sites.



Project timeline of SeamlessAccess.org

December 2016 – June 2019
Piloting phase
RA21

July 2019 – June 2020
SeamlessAccess
Beta Phase
Operational

July 2020 - onwards
Full service
operational

A look ahead

Broad implementation of the NISO-certified best practices by providers and subscribers. (SpringerNature is the first major vendor to support SeamlessAccess. They went live last week.)

Entity Categories and Attribute Bundles working group has just been launched.

See Section 3. Future Work Items page 40.

Seamless Access central services in action

Demo

A collaborative multi-stakeholder effort

Individuals from more than 60 different organizations have been involved in RA21 since its inception in late 2016.

AbbVie Pharmaceuticals
American Medical Association / JAMA
American Chemical Society
American University
American Psychological Association
Association of Research Libraries
American Society of Civil Engineers
Atypon Systems
BASF
Bibliotheksservice-Zentrum
Brill Publishers
Brown University
Centre for Agriculture and Bioscience
Carnegie Mellon University
Clarivate Analytics
Cambridge University Press
Copyright Clearance Center
Denver University
EBSCO Information Services
Eduserv
Elsevier Publishing
Emerald Publishing Group
Erasumus University Rotterdam
ETHZ
GEANT
GlaxoSmithKline Pharmaceuticals
Harvard
Highwire Press
Hypothes.is
IEEE
Informed Strategies LLC
Internet2
Institute of Physics Publishing
JISC
Johns Hopkins University
KTH Royal Institute of Technology
Liblynx
MIT
MyUniDys
NISO
Novartis
OCLC
Open University
ORCID
Opitcal Society of America
Oxford University Press
Proquest
Ringgold
Roche Holding AGG
Sage Publications
Silverchair Information Systems
Springer Nature
STM
SUNET
Switch
Taylor & Francis Group
Thieme Medical Publishers
Tilburg University
UC Davis
Universiti Putra Malaysia
University at Buffalo
University of Bath
University of Nottingham
University of Surrey
Wiley
Wolters Kluwer Publishing

Corporation
Academic Institution
Software/Service Provider
Publisher

Closing the Policy Void

- Getting serious about privacy
- Technical evaluation of connections to new providers
- Contract language is underutilized

Finis

Seamlessaccess.org

Rich Wenger rwenger@mit.edu

Phone 339-368-1436