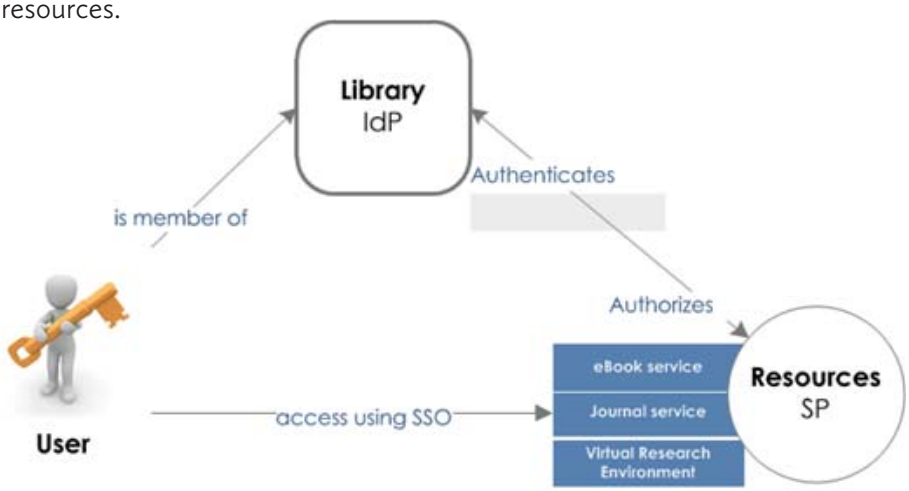
Federated access
information for libraries

Federated access management in a nutshell

Imagine a group of institutions managing digital user identities together at the organizational level. Now imagine the users of this group easily accessing all digital resources and services available in this group of institutions. Sounds good? That's what federated access is all about.

Now let's get a little more technical. Federated access is based on a two entities model. The first entity is the Identity Provider (IdP), one of the member organizations, who has information about the user, for example role, affiliation, entitlement, name or identifier. With this information, the Identity Provider can authenticate the user. The second entity is the Service Provider (SP) that can authorize users to get access to resources. Service Providers can be member organizations or external providers, for instance virtual research environments or journals.

When a user initiates an access request to a Service Provider, the request is forwarded to the Identity Provider. The Identity Provider checks the user's credentials, and confirms this back to the Service Provider. Based on this verification, the Service Provider grants or denies access to particular resources.



Benefits for libraries

Federated access may require some investments, but it will help to overcome some of the problems associated with IP-based access, like limitation to a specific IP-range, or fuzzy statistics. Here are some of the long-term benefits for libraries:

- **Easier authentication and authorization in the long term**, as identity management processes are shared at the organisation level. Libraries don't have to maintain their own user credentials.
- **Higher security levels** for both, digital resources and for users' personal information, because of the unified management of credentials. This also relieves libraries of their responsibility for securement.
- **A more visible role for libraries** when asking users to be identified by their federated identity, instead of just granting access through IP recognition.
- **Easier integration of library services with virtual research environments** where scientific resources and content can be accessed, used, stored and shared.
- **Better statistics about the use of library resources**, that can be used for reporting or strategic planning.

Benefits for end-users

- **Single set of credentials** Users only need one set of credentials that is maintained by their home institution as the IdP. It can be used for services and content offered by their library, as well as any other system or service offered by the members of the federation.
- **Security and Protection** The privacy of users is protected, as only the minimum number of necessary attributes are shared with other federation participants. The user also needs less passwords: only one complex password at their home organisation, instead of multiple weak or duplicate credentials.
- **Accessibility** Users do not need to be physically present at the institution facilities in order to have access to resources, and they do not need to use VPN or a specific equipment or technology.
- **Mobility** Users have a great flexibility and freedom regarding the location and the device they are using to access the resources, thus fostering their mobility.

Take the lead

- **Guide IT departments and decision makers** to resources that explain the benefits and arguments for the adoption of identity federation and management
- **Collaborate with IT departments** at the campus level, in order to integrate the library services into the range of systems for which the institution adopts federated identity management.
- **Join efforts at the national level** in order to negotiate licenses with publishers and request them to offer identity federated access to their products.
- **Collaborate with other libraries** in order to have a common approach towards the adoption of federated access technologies and protocols.
- **Set up federated login** at resources available at your library, so library patrons can easily use institutional login when they reach library e-resources.
- **Provide WAYFless links** on the website of your library, for convenient access to e-resources.
- **Promote federated login** on seminars, library guides, so that library patrons feel comfortable about federated login and single sign on at library e-resources.

How AARC can help you

- AARC offers training materials and sessions targeted to Identity Providers and Service Providers.
- AARC provides information support as suggestions for IdP hosting solutions and best practices guides for the implementation of particular federated technologies.
- AARC champions the harmonization of policies at the national and international levels.
- AARC works on facilitating better federation login negotiations with e-resources providers.
- AARC has developed and collected several resources about federated access for libraries, varying from online training modules to factsheets. Visit **www.aarc-project.eu/libraries** and find out more.

AARC (Authorization and Authentication for Research and Collaboration) is an EC funded project that brings together 20 different partners among National Research and Education Networks (NRENs), e-Infrastructures Service Providers and libraries to develop an integrated cross-discipline AAI framework, built on production and existing federated access services.

For more information, visit: https://aarc-project.eu or contact aarc-contacts@lists.geant.org.