# Federated access to digital resources at libraries

## 1 What is federated access management?

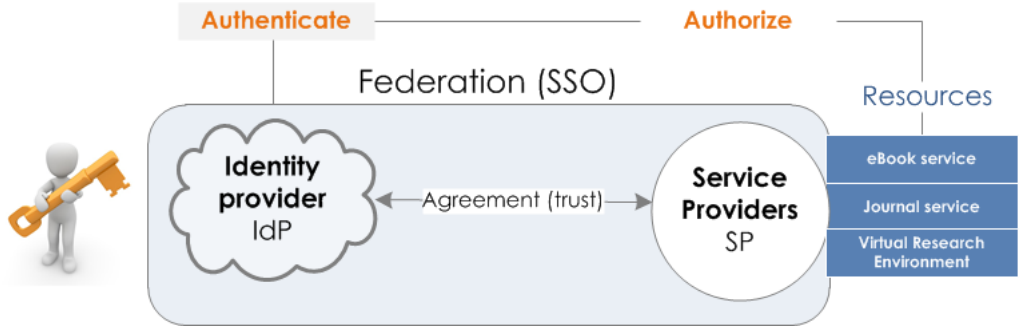
Federated access refers to the cooperation between a group of institutions for managing user identities to grant access to digital resources and services offered within the same group. In the digital domain, granting permanent and remote access to resources has become a major challenge for individual organizations in the academic, enterprise or public sectors. Significant efforts have been devoted during the last decade to provide users with unique credentials avoiding the need for separate identities for each information system they are entitled to access.

The access to digital resources is increasingly collaborative and ubiquitous. There is a need to go beyond the institution boundaries and cooperate with other organisations to ease the access to resources while protecting users' identity information. The current approach for this cooperation is federated identity management (FIM). This requires agreement upon standards, policies, processes and technologies that support and rule authorization and authentication processes across multiple organizations.

## 2 How does it work?

Federated access is based on a two entities model: a Service Provider (SP) or Content Provider (CP), that protects the content against unauthorized access (authorization) and an Identity Provider (IdP) installed centrally at an organisation (authentication) that ensures that the user is authenticated.

As a result in an identity federation participant identity providers maintain information about their users, like role, affiliation, entitlements, name, or identifier, that are referred to as attributes. These attributes allow the service provider to check the user rights for accessing specific services or resources while maintaining and protecting privacy.




When a user initiates an access request to a SP, which could be a member organization or an external provider, the request is forwarded to the home organization or IdP, that is responsible for verifying the user's credentials, and confirming back to the service provider. Based on this verification, the SP then grants or denies access to particular resou

## 3 Why is this important for libraries?

Research libraries provide their communities access to information resources (journals, e-books, databases) mostly licenced from external providers. These require the libraries to assure the user is entitled to access a specific resource. A common procedure is to apply IP control and restrict access to resources within a specific IP range. However the IP approach has a number of shortcomings. To start with, the IP approach does not allow accessing resources outside the IP address range of the institution. Secondly, there are challenges with sharing IP ranges among more than one institution or department with different access privileges. Thirdly, there are difficulties in setting different access levels to different roles for specific resources or being able to obtain clear statistics by type of users or any other parameters. A federated access approach would help to overcome these limitations. Although it requires some initial investments, the long-term benefits are noteworthy:

- Authentication and authorization will be easier in the long term, as identity management processes are shared at the organisation level.
- As the processes for Identity Management are simplified at campus or at a higher organisational level, and libraries do not need to maintain their own user credentials, costs are also reduced.
- The unified management of credentials can improve the security levels both for digital resources and for users' personal information, also relieving libraries of their responsibility for securement.
- Libraries whose users' home organisations have joined a national identity federation get benefits on the authentication process; and if joining a negotiation consortium they will also benefit on license scale. Libraries can stimulate collaborations between their national identity federation and their negotiation consortium in order to have a greater weight in negotiating licenses and requiring standardised procedures for authentication and enhanced services from publishers.
- Libraries can also play the role of Service and Content Providers for their own developed or hosted collections and services. Being part of an identity federation simplifies the access control for these resources, and avoids the need of maintaining their own database for external users credentials.
- Libraries would benefit from a more visible role when asking users to be identified by their federated identity instead of just granting access through IP recognition.
- Libraries would be in a better position for integrating their services into virtual research environments where scientific resources and content can be accessed, used, stored and shared.
- Libraries can obtain fine-grained statistics about the use of their resources for reporting and strategic planning, as a base for collection development decisions.

## 4 Which are the benefits for end-users?

- **Single set of credentials** Users only need one credential at a single database that is maintained by their home institution as the IdP, and that could be used for the services and content offered by their library but also for any other system and service offered by the members of the federation.
- **Security and Protection** Users privacy is protected, as only the minimum number of necessary attributes are typically shared with other federation participants. The number of passwords managed by end-users is also reduced; having one complex password at their home organisation, instead of multiple weak or duplicate credentials, protects the user's online security.
- **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 going to use to access the resources, thus fostering their mobility.

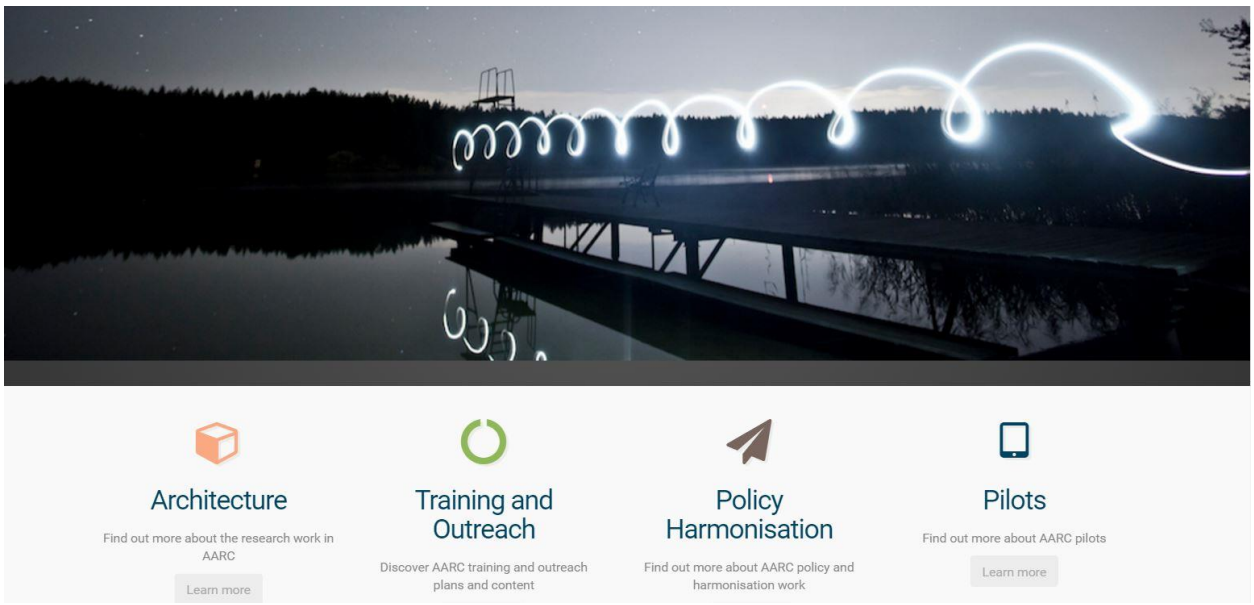
## 5 How can libraries take the lead?

- Guiding IT departments and decision makers to resources that explain the benefits and argument for the adoption of identity federation and management
- Collaborating 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.
- Joining efforts at the national level in order to negotiate licenses with publishers and request them to offer identity federated access to their products.
- Collaborating 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 library so library patrons can easily use institutional login when they reach library e-resources.
- Providing WAYFless links on library website for convenient access e-resources when accessing them from library website.
- Promoting federated login on seminars, library guides so library patrons feel comfortable about federated login and single sign on at library e-resources.

# 6 What can the AARC project do for you?

The AARC project's objectives are to deliver the design of an integrated cross-discipline AAI framework, built on federated access production services (e.g. eduGAIN) and to increase the uptake of federated access within different research communities.

- 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.




## ABOUT AARC

AARC 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.

## FURTHER READINGS

- **Federation 101** training module, AARC Project: https://aarc-project.eu/documents/training-modules/federations-101.
- **Federated Access Management. What it is and why it is important,** JISC UK Access Management Federation: https://youtu.be/wBHiASr-pwk.
- **REFEDS Value Proposition for Identity Federations.** https://wiki.refeds.org/display/OUT/The+Value+Proposition+for+Identity+Federations
- **7 Things you should know about Federated Identity Management,** EDUCAUSE paper. https://library.educause.edu:443/resources/2009/9/7-things-you-should-know-about-federated-identity-management