EZ proxy pilot description

EZ proxy showcasing the benefits of federated authentication

Showcasing the possibility to easily configure federated authentication (thus exploiting the benefits it provides with respect of the IP-based one) is the main goal of Scenario 1.

A very popular reference tool used by libraries worldwide is the EZproxy tool provided by the OCLC consortium. EZproxy foresees - in addition to the IP proxy functionality - also the possibility to act as a SSO proxy, redirecting user session to federated publishers' endpoint (SAML Service Providers), but this configuration option is mostly unknown and poorly exploited by libraries. In fact, EZproxy can act as an access mode switch, to support libraries in a hybrid environment where both federated and non federated endpoints have to be reached.

An additional, relevant goal of this pilot is to write and share within the libraries community a comprehensive guide supporting Library EZ proxy administrators to configure EZ proxy to act as access mode switch, a feature mostly unknown to many library admins, which have it available but ignore the potential of this configuration option, enabling their users to be Authenticated through the library IDP each time this is possible and establishing an SSO session to the federated publisher SP endpoint, each time this is available.

The guide has been produced while implementing pilot n.1 and published on the AARC wiki pages on https://wiki.geant.org/download/attachments/58131750/guidaEzproxyShibboleth-en-2.pdf

A description of the scenarios for this pilot is available on the AARC wiki at https://wiki.geant.org/display/AARC/TSA1.1.3LibrariesPilot

This use case is meant to be supporting libraries having to deal with hybrid Authentication infrastructure to access online resources (SPs) by means of a SSO-proxy: users will experience no differences while accessing resources through a library portal irrespective of whether these are SAML-compliant or IP-based.

A Single-Sign-On proxy will be set up to which users Authenticate to by means of the Library Identity Provider - which is linked to the local Library IDM tool.

Once users are logged in via the IDP to the SSO proxy, they will be able to access both kind of online resources, federated and non federated (IP-Auth), with absolutely no operational difference for them.

One SSO proxy solution one can refer to is OCLC EZproxy which is a very popular tool among libraries. EZ-proxy is a rewriting proxy which means that URLs are rewritten in a WAYF-less syntax and made available to users requesting them.

To be able to include Library Walk-in users, and IP based plugin Shibboleth extension has been configured, such that local walk in users would get a "Walk In" attribute while logging in on the SSO proxy, after registration on the local IDM, going through the library IDP, entitling them to access a subset of the subscribed resources allowed for such kind of users.

This is meant to be provided by a specific extension of the Shibboleth v3 Identity Provider.

(Attribute value eduPersonScopedaffiliation "Walk In user")

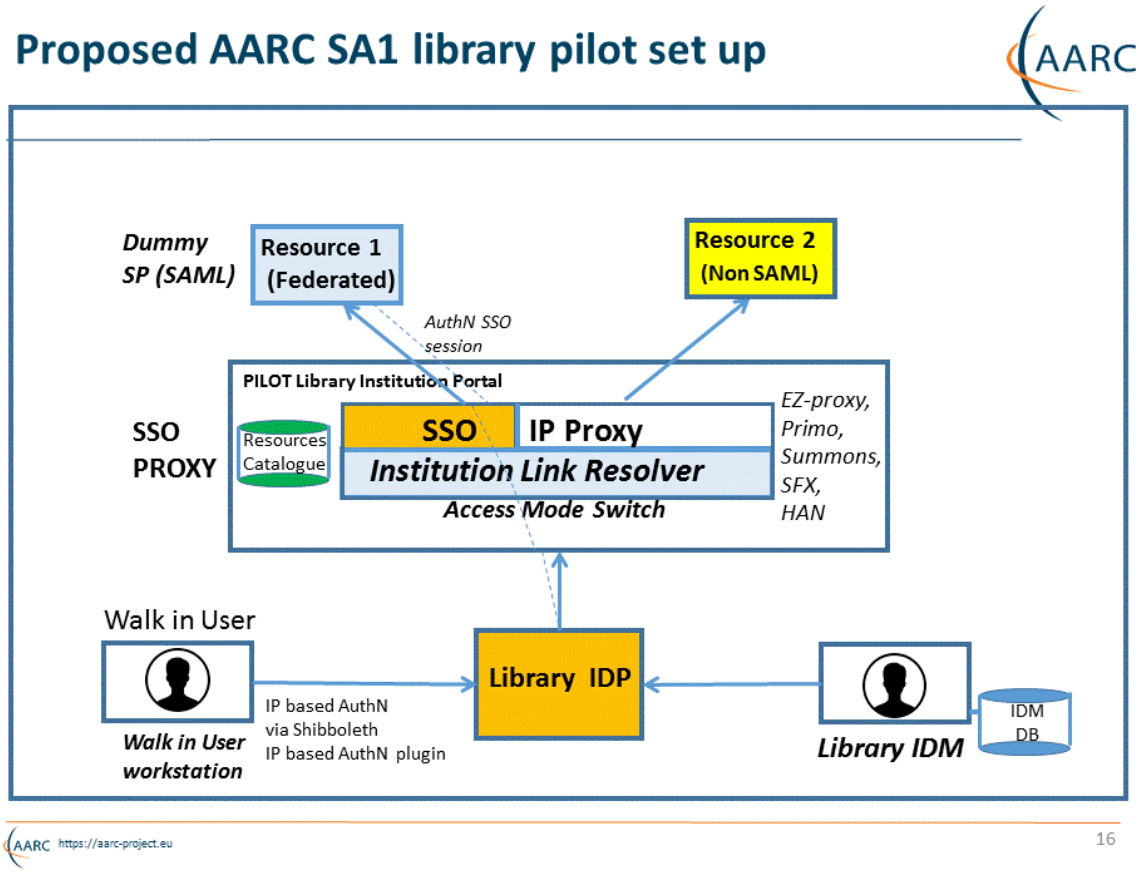

Figure 1: Architecture of Library Pilot N.1 - Scenario 1 - EZproxy as access mode switch

Among the tools which are available acting as an access mode switch (Option A) local to the library, EZproxy (https://www.oclc.org/ezproxy.en.html) is one of the most popular tool many libraries are already familiar with. EZproxy is a comprehensive product provided by OCLC, a full-fledge rewriting proxy capable of managing both SAML and IP-based Authentication for users against online SPs. It also foresees the option to be provided in a hosted fashion, if needed.

It allows the proxy administrators to configure resources which need to be accessed in a federated fashion- provided a user authenticated on a local IdP - and those which will be accessed in an IP-proxy fashion, based on the source IP of the EZ-proxy tool itself.

In the same category fall a set of similar tools aiming at allowing users to smoothly access different kind of resources: HAN (http://www.hh-han.com/en/default.cfm).

IP-based authentication plugin of the Shibboleth IdP can be used to Authenticate local walk in users based on the IP address of the terminal used by them to access online resources once on premises of a given library, providing them with eduPersonEntitlement valued as "walk-in user" attribute .

Overall, the aim is to provide user with a smooth experience while accessing resources, irrespective of the way (Authentication) they are accessed.

End-user would be the main focus: the overall goal is also to showcase the benefits of federated authentication for both Users and Libraries; to showcase a DEMO showing the advantages of Federated AuthN.

The end user experience is simplified by the solution represented by the picture below, which represents the required steps to configure the SSO proxy - taken from a well known article from the NISO organization (http://www.niso.org/workrooms/sso):

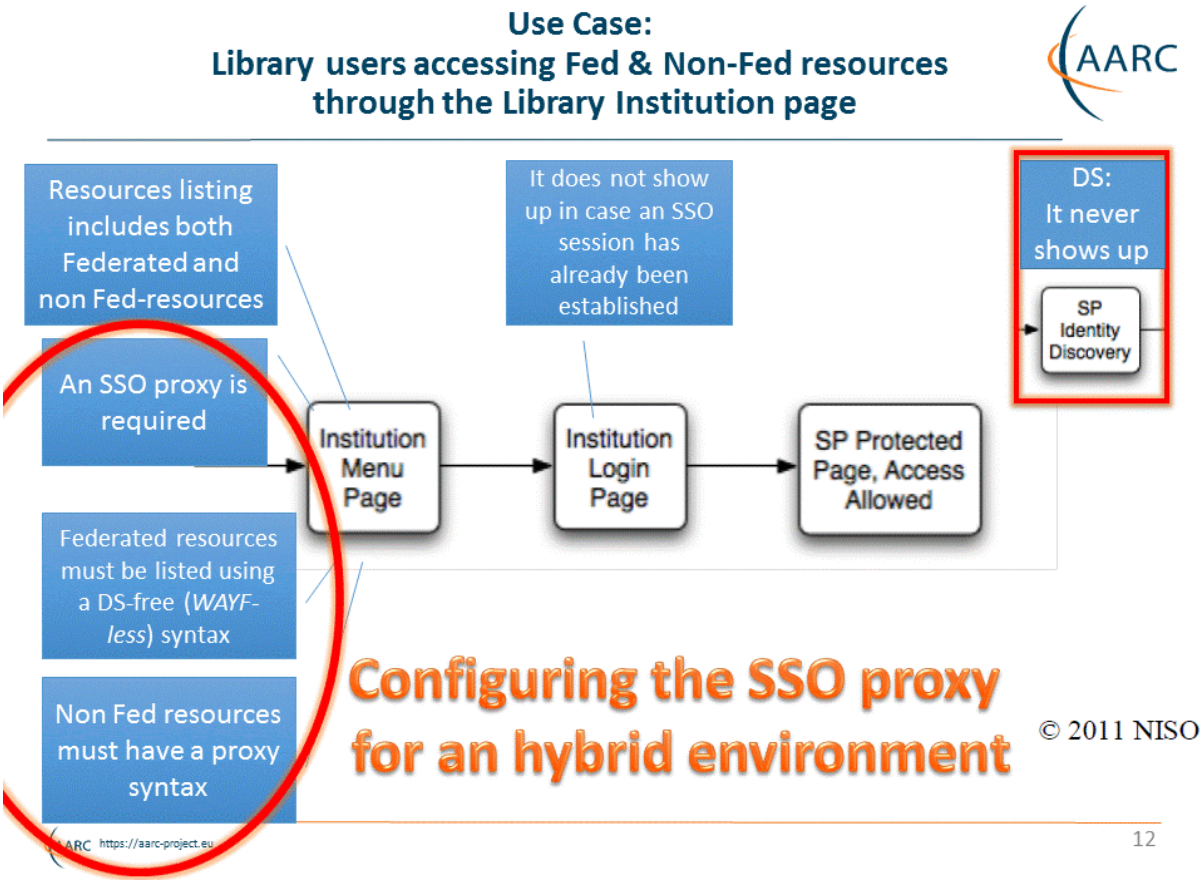

Figure 2: Configuring the SSO proxy for an hybrid (federated / non federated) environment

Implementation of Scenario 1 (EZproxy as access mode switch)

Coming to the implementation of Scenario 1, the practical steps carried out during the implementation of the pilot have been the following ones:

- Successfully configured EZproxy with test IDP (at GARR - Florence offices)
- EZproxy configured as a Shibboleth SP
- Made online resources available to the tool
- User can login using SSO, having many resources to be reached.
- The next step was to use the fact that some resources like ScienceDirect or Scopus are already SHib-enabled
- Configured EZproxy (SPU-edit..) to make it chose resources already enabled through SSO, and make users pass through the active SSO session.
- In this way users do not need to use the proxing power of the proxy - one only rely on SSO.
- A user logs in through Shibboleth and logs in to an enabled resources, EZproxy does not proxy anything. Connection goes through the SSO session.

For other resources, the EZProxy does its proxing job, in the URL bar users find name of resources encoded under the proxy URL. So that, in this respect, you can tell when you're proxying or not.

EZproxy - to classify accessible online resources - is based on the usage of a database stanzas: a list of resources and DBs from various providers, this DB is not a SSO-enabled DB. The public URLs from the providers. To correctly configure EZproxy in this respect one needs to use a list of directive to reach directly the request initiator of single SPs; it is not completely intuitive and straightforward, and the required steps have thus been written in the guide provided by the pilot.

It is also not very easy to have a complete list of Request Initiator from service providers in the library domain.

Mapping to the Blue print architecture

Overall, framed in the context of the Blueprint reference common Architecture defined by AARC JR1, the architectural layers and functional bits involved in the implementation of library pilot n. 1 based on the Access Mode Switch provided by EZproxy and additional components are the following ones, as shown by figure 6 below:

- IP based authentication (User Identity layer)
- SAML Federated Identity Provider (User Identity layer)
- EZproxy access mode switch (Translation layer)
- Publishers' endpoint (both IP and Fed) (End Services)

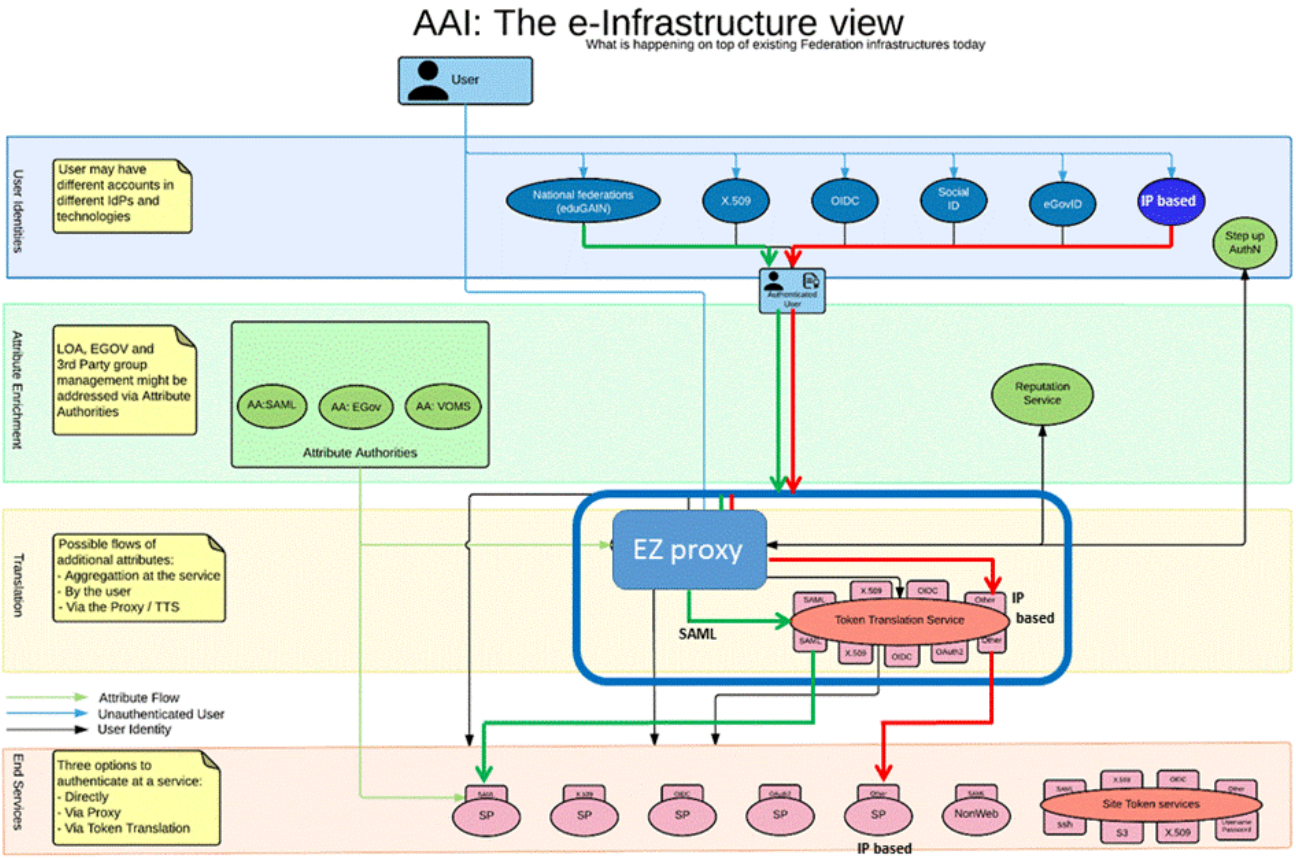

Figure 6: Architectural components implemented by Library pilot n.1 (Access Mode Switch)