Providing access for Library walk-in Users

Supporting Walk-In users with federated authentication

Moving to a scenario where federated authentication is the *only* scenario used, is tempting. However, one mayor challenge exits: the ability to offer access for so called Library Walk-In users. These users are members of the public who want access to electronic resources (where licensing conditions permit). Typically these walk into the library and use the dedicated computer terminals in the library to gain access to electronic resources. There is no access from off campus locations for these users. For this use case retaining IP access is still common.

Several scenarios for facilitating the walk-in users with the use of federated authentication exist:

- *Temporary credentials*
  In this case the library staff provides Walk-In users with temporary credentials so a 'regular' Identity provider can be used. The Walk-In user uses these credentials to authenticate. This is not very user friendly, error prone and involves work for the library staff. Furthermore this requires additional security measures, to make sure these credentials cannot be used off campus.
- *Extra Identity Provider*
  This requires setting up a special Identity Provider by the Institution which 'translates' authentications with a specific IP range on the campus to an anonymous authentication towards the Service.
  Several software products, including the Shibboleth Identity Provider allow such a set-up in conjunction with the 'regular' set-up which requires users to authenticate. Other products, like Microsoft's Active Directory Federation Services (ADFS) do not have these capabilities. Although Shibboleth is a commonly used product, especially ADFS is growing strongly, and for example in The Netherlands accounts for 80% of the Identity providers.

Next to the technical challenge, is some countries additional challenges exist as the policy of the federation does not allow walk-in users and other guests to be exposed to service providers. Typically only members, faculty and student affiliations are allowed. This policy makes it impossible for institutions to provide the walk-in users with federated credentials using the regular Campus Identity provider.

As part of the AARC project two scenarios were further investigated an piloted in the SA1 activity:

1. Campus IdP setup for regular and walk-in users authentication
   Configure a Shibboleth Identity Provider which authenticates both regular users, based on the campus LDAP system, as well as allowing authentication for Walk-In users, using a computer in a given IP range.
   This scenario facilitates libraries where the university already operates a Shibboleth based Identity Provider, and the national federation has no policy prohibiting walk-in library users.
2. Centralized walk-in authentication service for library consortia
   In this scenario, a Shibboleth Identity Provider, in combination with a management portal is set up. This provides a centralised service for all library walk-in users within a consortium of libraries, or within a country.
   This scenario allows a group of libraries to centrally manage the IP ranges of the terminals within the library, and does not require any configuration or adoption on the Identity Provider operated by the campus IT. In the presented scenario, it is assumed the library staff themselves do have the ability to authenticate using federated authentication with their university IdP. This is then used to allow them to manage IP ranges in the management portal of the central service. Next to providing an IdP and a management portal, the service also provides a portal for the walk-in users which will trigger Single sign-on and can also aid in terminating the session if the user leaves the terminal