


[DISCUSS] SAML 2.0 Service Provider feature

 This page contains topics supporting ongoing discussion at dev@syncope.apache.org.

Tracked as [SYNCOPE-1041](#).

Requirements

Once this feature is implemented, it will be possible to log into the Admin Console, the Enduser UI (and any other Java EE web application) by using the [Web Browser SSO Profile](#) and an external SAML 2.0 [Identity Provider](#).

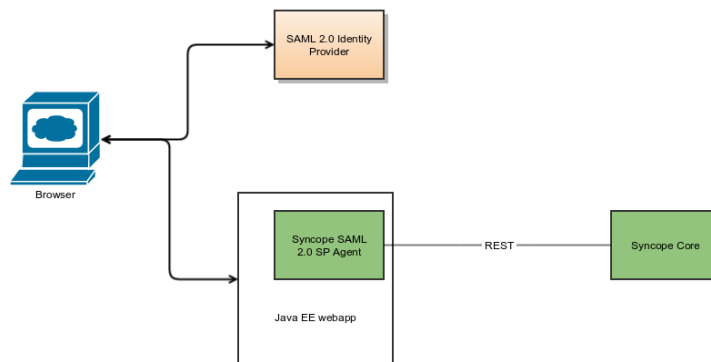
An important requirement is to maintain all authentication / authorization aspects into the Syncope Core.

Design

The idea is to provide a new [Java EE web-fragment](#) named *SAML 2.0 SP Agent*, meant to be deployed, as separated JAR file, alongside with the Admin Console, the Enduser UI (and any other Java EE web application).

The operation's flow will be something like as follows:

1. both for IdP-initiated and SP-initiated scenarios, the new SAML 2.0 SP Agent will take care of the SAML 2.0 assertion exchange with user's browser
2. the actual assertion generation and validation is performed by invoking the Syncope Core via REST (for this reason the IdP metadata will be maintained by the Core); at the end of the process, a JWT (introduced by [SYNCOPE-1035](#)) will be returned by the Core to the SAML 2.0 SP Agent
3. the new SAML 2.0 SP Agent will store the JWT received by the Syncope Core into the Java EE web application's session
4. the Java EE web application will use the JWT for invoking the Syncope Core



Implementation

For several reasons - including the need to introduce additional library dependencies for manipulating SAML 2.0 assertions - the ideal candidate for this implementation is a new [extension](#).

The [OpenSAML 3.0 library](#) looks like an adequate fit for this job.