The TIER Shibboleth IdP Package and Lafayette College Customizations

Lafayette College is a long-time operator of a locally-run Shibboleth Identity Provider (IdP). When it came time to develop a web portal for the College and configure it and other services for Web SSO, we had to think about what we wanted our Web SSO behavior to look like. Providing a robust user experience was important, so we made the decision to make CAS central to our Web SSO strategy.

We integrated the shib-cas-authenticator plugin with our IdP for its capability of delegating authentication externally from Shibboleth to CAS, which serves as our SSO front end. This bridge between Shibboleth and CAS is a key piece of our authentication architecture. But when we became aware that being able to log into the InCommon Certificate Service using SSO would require supporting the REFEDS MFA Profile, we didn't know how the bridge would handle MFA signaling. Our interest in Internet2's TIER Initiative raised another question: could our customizations be added to the IdP packaging?

Though Lafayette couldn't attend the first TIER CSP F2F in person, we were able to work with the TIER SMEs remotely to get an idea of how this would be possible. Our engagement with Unicon for the Campus Success Program included helping us deploy the IdP package and incorporate our requirements for MFA signaling and the shib-cas-authenticator. They put together a beta release, shib-cas-authn3, that was able to handle the REFEDS MFA Profile. That solved one of our problems.

But what about adding it to the IdP package? The IdP component packaging owner saw no risk in adding a configuration option for Lafayette. Collaboration took place on the packaging front with Unicon and TIER to refine the package, incorporate Unicon's work, and provide fixes for misconfigurations that were introduced. The result was a solution for copying over required files.

A Dockerfile contains the "recipe" for executing command line instructions that create an image. Multiple arguments allow the basic recipe to be customized. After we tested and verified the behavior of the new shib-cas-authenticator with the MFA Profile support, it was ready to be added during image creation. We added build references to the JAR file from Unicon and to our local configuration files. An additional step rebuilds the IdP WAR file to include these artifacts that provide the local configuration options that we know and love.

Many thanks to Misagh Moayyed and Paul Caskey for rising to this challenge.