OTPUseCases

Use this page to collect use cases, deployment experience, and general wisdom regarding one-time password (OTP) authentication mechanisms, especially in conjunction with SAML Web Browser SSO.

Fredrik Thulin has contributed an OTP login handler for IdP v2.2.1 (although it may work with other versions of the IdP).

University of Minnesota

The M Key is an event-synchronous OTP (push button to get next passcode) implemented with Safeword Silver tokens. The two factors are the token passcode and a user-selected PIN.

To request M Key authentication, an SP sends a RequestedAuthnContext with the class ref "https://www.umn.edu/shibboleth/classes/authncontext/mkey". This triggers a UI change in the login page to prompt the user for their M Key token code and PIN rather than a password.

If the user logs in with M Key, our IdP sets the returned AuthnContextClassRef to "https://www.umn.edu/shibboleth/classes/authncontext/mkey". The SP can check for this value to ensure that M Key was used.

It is also possible to sign in using the M Key if an SP did not request it (or more commonly, if you signed into an application requiring M Key, then went to another application using SSO).

From the IdP side, this is currently implemented through integration with our existing locally-developed web SSO system. We implemented a custom LoginHandler based on RemoteUser, but adding a second RemoteUser servlet endpoint. The LoginHandler chooses which endpoint to redirect to based on the RequestedAuthnContext. The M Key endpoint requires M Key authentication from our web SSO; the other one just requires normal password authn. Regardless of which servlet is used, the actual authentication method used is determined from our web SSO, and the M Key AuthnContextClassRef is set if M Key was used to authenticate.

We are currently working on a standalone LoginHandler that does not depend on our local web SSO system. It will do LDAP authentication for passwords and RADIUS authentication to our Safeword server. Like our current LoginHandler, an SP requesting M Key will cause the UI to change for the login form, and like our current handler, it will report M Key use through AuthenContextClassRef.

There is a diagram detailing the flows; the current implementation is on page 2 and the future implementation is on page 3. More details are available at our local shib wiki.