FIDO Authentication for Shibboleth IdPv3

Degree programme: BSc in Computer Science | Specialisation: IT-Security
Thesis advisor: Gerhard Hassenstein
Expert: Dr. Andreas Spichiger

Weak and often reused passwords are still one of the biggest vulnerabilities today. The FIDO alliance offers a stronger, more secure and easier-to-use authentication for online services. The medium-term goal of the FIDO consortium is to replace the simple ‹password› by a flexible system of different, but standardized authentication method.
This thesis evaluates the integration of the FIDO authentication mechanisms into a Shibboleth identity provider environment.

Reto Stähli

Initial Situation

The Shibboleth IdP Version 3 has been published in December 2014. Out of the box, Shibboleth V3 supports the standard user authentication schemes like username/password and PKI-based certificates. The authentication process within the new Shibboleth V3 IdP is based on ‹Spring Web Flow›. The use of flows to realize new authentication schemes allows developers a high degree of flexibility in customizing behaviour. The FIDO (Fast IDentity Online) Alliance on the other hand is an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices. The aim of FIDO is the support of a full range of authentication technologies, including biometrics (e.g. fingerprint) as well as existing solutions and communications standards. Therefore FIDO will be a promising authentication solution for Shibboleth IdP V3 to boost the diversity of new authentication means.

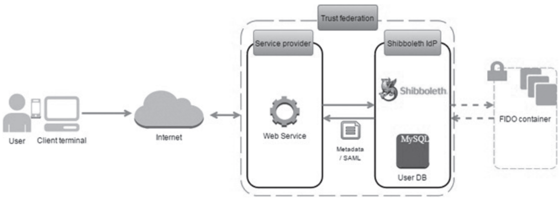
Vision

The main objective of this thesis will be the integration of the FIDO authentication protocol in Shibboleth IdP V3. This includes the building of a design and concept to integrate FIDO authentication in Shibboleth, the implementation of FIDO authentication and the set-up of a working Shibboleth environment to demonstrate FIDO authentication. The FIDO implementation should also support authenticator registration, where the user's client device creates a new key pair and registers the public key with the Shibboleth IdP.
The solution built should minimize depedencies between the Shibboleth IdP and the actual FIDO implementation. It should be easy to reuse and to incorporate within an existing Shibboleth IdP environment. A service provider who wishes to protect its resources with a second factor should be able to demand so. The Shibboleth IdP should be able to fulfill this request and report back that the user has been authenticated accordingly.

Realization

The integration of FIDO authentication within Shibboleth was realized by using the «External Authentication»-interface. The authentication is passed to an external point where the FIDO implementation is located. The FIDO implementation takes the necessary steps to authenticate the user. The location and usage of the external implementation is defined in a «Spring Web Flow» so that the IdP can forward the authentication request correctly. After authenticating the user, the external implementation (in this case FIDO) reports back to the IdP how and whether the user has been authenticated.

The Shibboleth IdP generates a signed SAML token which the service provider validates and uses to grant access to the protected resource. This token contains – among other things – an authentication class, which indicates to the service provider, how the user has been authenticated. The service provider may also request a specific authentication class by redirecting the user to the IdP. The various authentication flows within the Shibboleth IdP can be configured to satisfy certain authentication classes. So upon receiving a request, the Shibboleth IdP will then select a suitable authentication flow to fulfill the request accordingly.



Simplified architecture of the solution