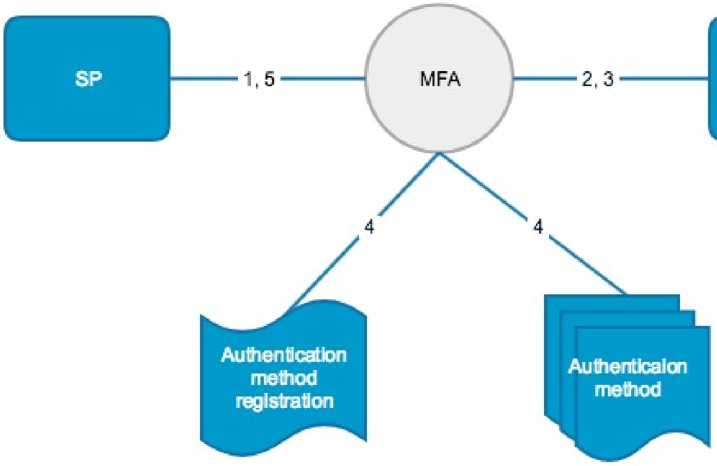
Haka MFA

Multi-factor authentication (MFA) implemented in Haka identity federation provides multi-factor authentication as a service that is easy to adopt for the home organizations and relying services. It uses standards based protocols for message transfer and user authentication. The target audience for the solution is mainly higher education organization employees. The solution can be extended to cover also the students.

Haka MFA implements two use scenarios: service provider and identity provider initiated MFA.

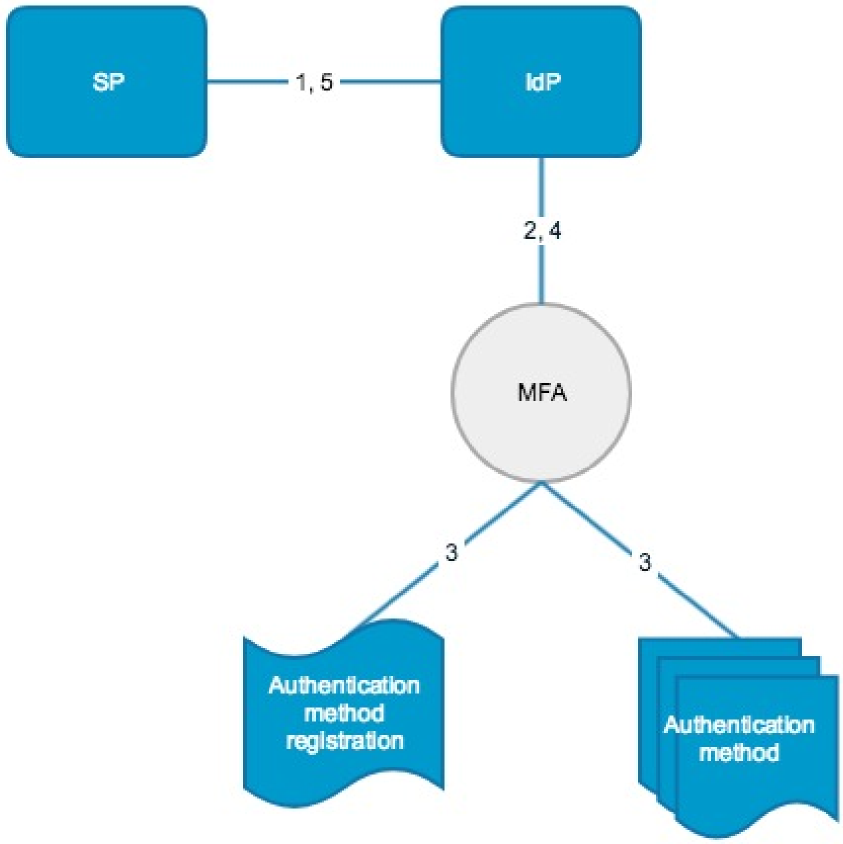
Service Provider (SP) initiated MFA (flow: SP MFA IdP)



In the SP initiated use scenario a service provider directs all authentication requests to the MFA service with a keyword requesting a certain authentication level in it's authentication request. The MFA service first redirects the users to their home organization IdP for an ordinary (password) authentication. After that the MFA service performs an authentication using the second factor.

In the SP use scenario the IdPs observe the MFA service as the relying service. This is done by registering the MFA server's SAML assertion consumer URL to the relying service's federation metadata. This allows IdPs to release only relevant user attributes intended for the service.

Identity Provider (IdP) initiated MFA (flow: SP IdP MFA)



In the IdP use scenario the MFA service is integrated to an IdP as another authentication method. Based on the authentication request and the policy rules an IdP can decide to request a MFA from the MFA service. If the IdP decides MFA is required, user is redirected to the MFA service after first performing an ordinary (password) authentication at the IdP. The IdP then redirects the user to the MFA service together with their authenticated identifier.

In the IdP use scenario the IdP and MFA service agree on the integration method. The Haka federation operator provides a Shibboleth IdP authentication handler that the home organisations can install to their IdP. The plugin and the MFA service use OpenID Connect protocol in their message exchange, enabling also IdP products other than Shibboleth to use the MFA with the IdP initiated use scenario. The MFA service accepts authentication requests in both SAML2 and OpenID Connect protocols. OpenID Connect is used in the IdP integration to MFA. The SP integration can be done using either protocol.

Authentication methods

Currently the Haka MFA service uses Time-based One-Time Password algorithm (TOTP) standard RFC 6238 as an authentication method. In practice, the user can for instance have a TOTP compliant app (such as, Google authenticator) in their smartphone.

The Haka MFA service counts on the IdPs for identity proofing. The IdPs are assumed to release the user's reliable cellphone number that is used for delivering a registration code as an SMS. New MFA users need to present the registration SMS to the MFA service to associate the MFA token to the proper IdP-authenticated user.

Getting started with Haka MFA

Haka MFA supports any SAML2 compatible service provider software and currently Shibboleth based identity provider.

If you wish to integrate Haka MFA to your Haka service, please contact Haka servicedesk.

Documentation

The source code is available at https://github.com/CSCfi/stepup-proxy

Integration to service provider (in Finnish): Käyttöönotto palvelussa

integration to identity provider (in Finnish): Käyttöönotto organisaatiossa