Requesting MFA in SAML and OIDC

ELIXIR AAI Task

Author: Dominik František Bučík [bucik@ics.muni.cz]

Date: 7. 11. 2019

This document is deprecated. The new version is available at ELIXIR MFA in LifeScience AAI - RP/SP perspective .

!!! ATTENTION - NOT MAINTAINED !!!

ELIXIR AAI has been migrated into the LifeScience AAI. This document is relevant only to the ELIXIR AAI, thus not maintained and has become outdated.

Purpose

This document describes the process of how Multi-Factor Authentication (MFA) works in the ELIXIR AAI and how the relying services can request it both in SAML and OIDC. The document expects some basic prior knowledge of these protocols.

There is a separate document User Instructions for Multi-Factor Authentication.

Introduction

ELIXIR AAI supports so-called step-up authentication. A relying service can request ELIXIR AAI for MFA, and after authenticating the user against their home organisation or other authentication providers, ELIXIR AAI requests the user to step up their authentication with ELIXIR MFA. If the user's home organisation has native support for MFA and signals it following standard protocols, step-up authentication is not needed.

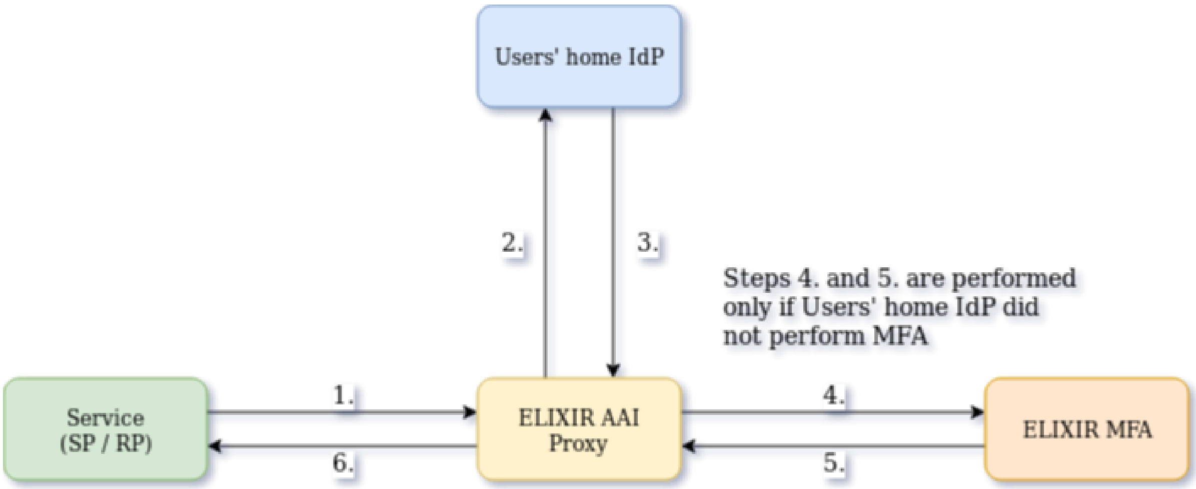
ELIXIR MFA is currently implemented using the TOTP standard (Time-based one-time password, RFC 6238) and expects a user has a TOTP token (for instance, a smartphone app with a secret registered to the ELIXIR MFA server). To register a secret, ELIXIR AAI sends the user an SMS code that they need to present to the ELIXIR MFA server. This requires ELIXIR AAI has the user's trusted cellphone number for SMS delivery.

Definitions

- **MFA (Multi Factor Authentication)** - The user presents at least two independent authentication factors of different types (something you know, something you have, something you are, something you do) to verify their identity.

MFA flow in ELIXIR AAI

The image below describes the flow when a relying service requires the user to perform MFA.


Users' home IdP
2.
3.
Steps 4. and 5. are performed only if Users' home IdP did not perform MFA
Service (SP / RP)
1.
6.
ELIXIR AAI Proxy
4.
5.
ELIXIR MFA

As the first step (1), the relying service (SAML SP/OIDC RP) initiates the login flow by requesting MFA. ELIXIR AAI Proxy consumes the request and asks users to select their identity provider (IdP). After the user selects their IdP, the ELIXIR AAI Proxy sends an authentication request to it (2). The user logs in using their credentials at the IdP and, if the IdP supports it, carries out MFA and signals that to the ELIXIR AAI Proxy. If the ELIXIR AAI proxy learns the IdP carried out MFA, it will redirect the user directly back to the relying service (6) with a response indicating an MFA has been performed. Otherwise, the ELIXIR AAI proxy invokes the ELIXIR MFA (4). The user performs step-up authentication at the ELIXIR MFA and is finally sent back to the service via Proxy (5 and 6) with an authentication response indicating MFA has been performed.

If the user has not activated ELIXIR MFA (i.e. does not have TOTP secret nor WebAuthn device registered at ELIXIR MFA), the activation is done between steps (4) and (5).

How to request MFA - SAML

The relying service initiates the login process by sending an authentication request to the ELIXIR AAI Proxy. To force MFA, request has to have the following authnContextClassRef:

```
<samlp:RequestedAuthnContext>
   <saml:AuthnContextClassRef
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      https://refeds.org/profile/mfa
   </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

When ELIXIR proxy receives such authentication request, it carries out the process described above and finally indicates a successful MFA as follows:

```
<saml:AuthnStatement AuthnInstant="2014-07-17T01:01:48Z"
SessionNotOnOrAfter="2024-07-17T09:01:48Z"
SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
    <saml:AuthnContext>
```

```
         <saml:AuthnContextClassRef>
             https://refeds.org/profile/mfa
         </saml:AuthnContextClassRef>
     </saml:AuthnContext>
 </saml:AuthnStatement>
```

If the *saml:AuthnContextClassRef* element contains value *https://refeds.org/profile/mfa*, the MFA has been successful. Any other value indicates that the user has been logged in, but did not perform MFA.

How to request MFA - OIDC

The service initiates the login process by including a special parameter in the request sent to the */authorize* endpoint of the ELIXIR AAI OpenID Provider. The request then looks as follows:

```
https://login.elixir-czech.org/oidc/authorize?
    response_type=<response_type>
    &scope=<scopes>
    &client_id=<client_id>
    &redirect_uri=<where_to_redirect_back>
    &state=<random_value_against_XSRF_attack>
    &acr_values=<acr_values>
```

with acr_values parameter set to “space” separated list of authnContextClassRef values including *https://refeds.org/profile/mfa* at the start of the list. Remember to

- URL encode the acr values.
- configure your service to use *id_token* as the response type.
- register your OIDC client at the ELIXIR OIDC provider to use *id_token* as the response type.

If the user has performed MFA, the relying party will receive an id_token, where a special claim *acr* should be present. This claim should contain value *https://refeds.org/profile/mfa*.

Please note that the *acr* claim is present only in the id_token and not in the access_token. Therefore, the service has to have the configuration of *response_type=id_token* enabled. Also, note that only the first id_token will contain the *acr* claim; if you later use a refresh token to obtain a new id_token it will not contain the acr claim.

The ELIXIR OIDC Provider currently supports requesting MFA only via passing *acr_values* parameter. It does not support requesting the *acr* claim via the claims request parameter.

Word of advice

We strongly encourage you to include multiple values for the requested *authnContextClassRef* (SAML) or *acr_values* (OIDC), especially including value *urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport* at the end of the list.

The reason for doing so is that most Identity Providers will fail to read the *https://refeds.org/profile/mfa* as authnContextClassRef without any backup value. When the fallback value of *urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport* is included, IdPs will perform at least basic authentication and the ELIXIR MFA component can step into the process.

Secondly, perform validation of the value for authnContextClassRef in SAML authentication response or the value of the claim acr in id_token. Check that it really contains the value *https://refeds.org/profile/mfa*.