Televic Education

Single Sign-On (SSO)

13 March 2019

Created by Staelens Nicolas

televic
education

Table of contents

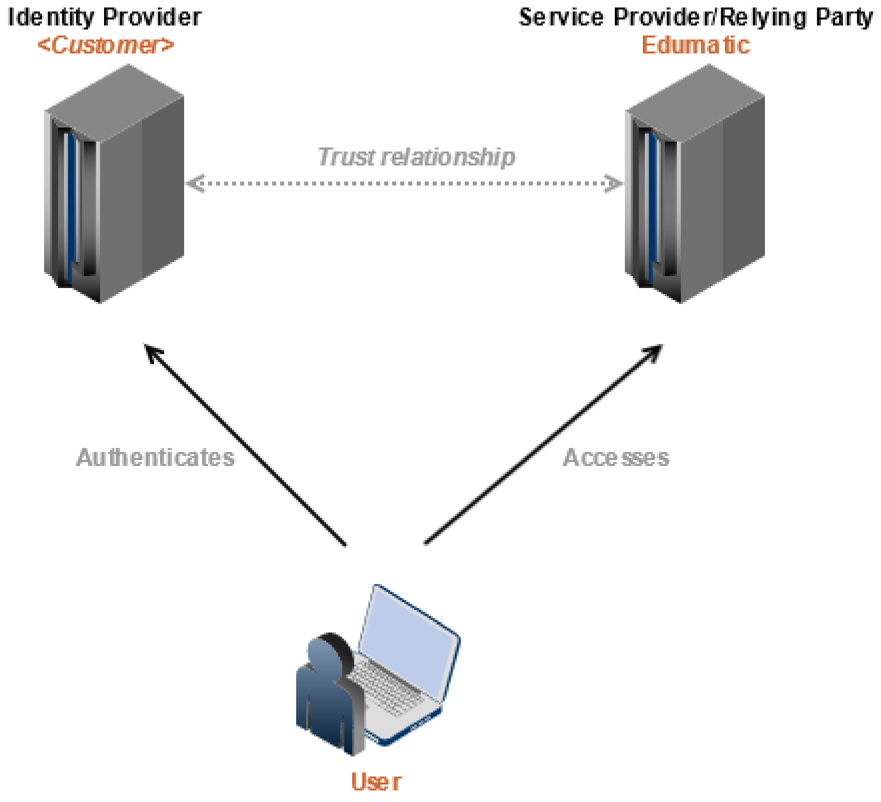
1 Introduction

1.1 General

Single Sign-On (SSO) enables a user to login once and access multiple applications and resources across different networks and domains. As an example, let's take the network/domain of a customer and Edumatic. Typically, a user is authenticated in the customer's domain using, for example, Active Directory when logging on to his/her computer. This enables the user to access the different network resources (network shares, printers, webpage logins, ...) within the domain without requiring the enter his/her login credentials each time. Edumatic also requires login credentials in order to gain access to the portal or the backend. However, since Edumatic is not part of the customer's domain/network, the user needs to enter his/her credentials manually.

By setting up an SSO between Edumatic and the customer's domain/network, users no longer need to enter their login credentials manually in order to get access to the Edumatic portal and/or backend.

Single Sign-On is based around the principle of a trust relationship between Edumatic (Service Provider/Relying Party) and the Identity Provider (IdP) of the customer. The identity provider offers user authentication as a service and acts on behalf of the customer. This authentication service can then be used by Edumatic. A high level overview of the SSO principle is depicted in the diagram below.



1.2 Claim-based Single Sign-On

Claims-based identity is a common way for applications to acquire the identity information they need about users inside their own or another organization/network/domain.

A claim is a statement that one subject, such as a person or organization, makes about itself or another subject. For example, the statement can be about a name, e-mail address, group, date of birth, ... It is the responsibility of the Identity Provider to provide the necessary claims.

With respect to the SSO coupling between Edumatic and the customer's Identity Provider, following claims are mandatory:

- NameId or Sub (unique identifier for a user, e.g. User-Principal-Name) (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier)
- E-mail (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress)
- First name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname)
- Last name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname)

Optional claims are:

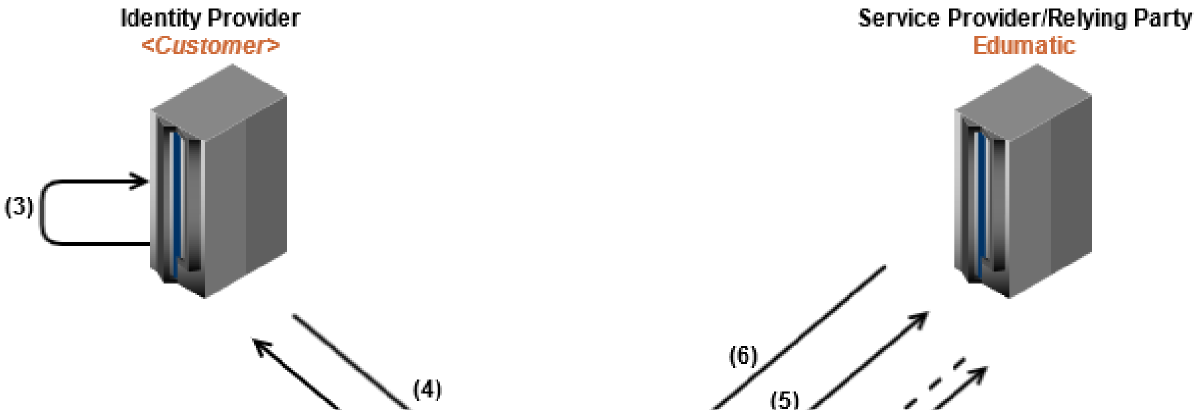
- User name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name)
  This field can be used for personal reference number of user within the organization/company. If this claim is omitted, the email adress will be used
- Televic group membership (http://schemas.televic.com/2017/02/claims/Group)
- Date of birth (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth)
- User language (http://schemas.televic.com/2017/02/claims/UserLanguage)

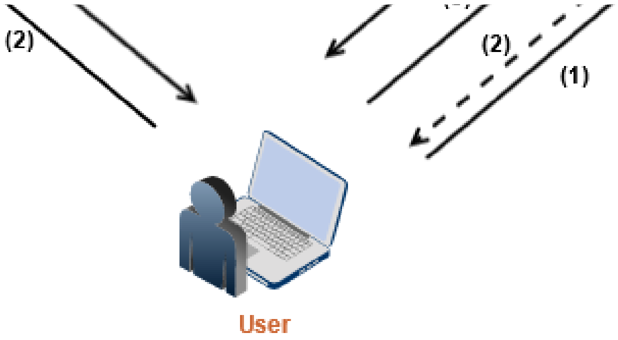
Remark: in this case, the password is not synced. A dummy password is automatically generated for the user.

It is highly recommended to also provide the 'Televic group membership' claim as this facilitates the creation and planning of Edumatic publications for specific target groups. This is important as users will only be known in Edumatic after their first login.

1.3 SSO authentication process

In the case of a SSO coupling, the Identity Provider and Service Provider (Edumatic) actually do not communicate directly with each other, but rely on the client browser's redirection (using standard HTTP GET and POST messages). Hence, the SSO authentication process can be explained in more details in the picture below:





1. The user is authenticated in the domain of the customer and navigates to the Edumatic portal or backend.
2. Edumatic is configured with an SSO coupling for the domain of the customer. As such, Edumatic needs to now the URL for the IdP of the customer.
3. If the user is not yet authenticated, he/she gets the possibility to login with his/her customer domain credentials.
4. The Identity Provider verifies the user's authentication and issues a token (with proper claims) back to the client.
5. The browser is redirected to Edumatic and uses the token for authentication
6. Edumatic accepts the token (and corresponding claims) and the user is automatically logged in to Edumatic.

Note: in this case we assume a *passive* SSO coupling. In case of an *active* SSO coupling, there is direct communication between the Service Provider and the Identity Provider.

2 Setting up an SSO coupling with Edumatic

With respect to setting up the SSO, the customer takes the role of the Identity Provider (IdP) and Televic Education takes the role of the Service Provider (SP).

Televic Education makes use of IdentityServer 3 (https://identityserver.github.io/Documentation/) for authenticating its users for all products. IdentityServer 3 implements the OpenID connect protocol.

2.1 Requirements

The IdP must support one of the following protocols:

- OAuth2
- OpenID connect (e.g. IdentityServer)
- WS-Federation (e.g. ADFS)
- SAML2P (e.g. Toledo)

The IdP must provide the following claims:

- NameId or Sub (unique identifier for a user, e.g. User-Principal-Name)
- E-mail
- First name
- Last name
- User name (personal reference number of user; if not available copy of email address)

The IdP should provide the following claim(s):

- Televic group membership (http://schemas.televic.com/2017/02/claims/Group)

The IdP may provide the following claims:

- Date of birth
- User language (http://schemas.televic.com/2017/02/claims/UserLanguage)

3 Access to Edumatic outside the customer's domain/network

How to access Edumatic outside the customer's domain/network depends on the accessibility of the IdP.

If the IdP can be accessed from outside the customer's network, nothing changes for the users. In this case, the user simply navigates to https://*<channel>*.edumaticonline.com/edumatic5 (for the portal) or https://*<channel>*.edumaticonline.com/teachandlearn (for the backend).

In case the IdP cannot be accessed from outside the customer's network, the user needs to navigate to https://www.edumaticonline.com/edumatic5 (for the portal) or https://www.edumaticonline.com/teachandlearn (for the backend). In this case, the user does not browse directly to the channel.

Another point of attention in case the IdP is not accessible outside the customer's network is that the user should follow a specific flow when he/she want to log on to Edumatic (outside the customer's network/domain) for the very first time:

1. The user navigates to the Edumatic website (portal or player)
2. The standard Edumatic sign-in form will be shown
3. The user clicks the "Forgot your password?" link
4. The user fills in his/her e-mail address and clicks on the "Send" button
5. The user will receive an e-mail with the password
6. The user navigates back to the Edumatic login page and sign in using his/her e-mail address and the password sent in the e-mail
7. The user can now change his/her password in his/her profile page after succesfull login to Edumatic

4 Sources

Below is a list of sources used for creating this page.

- https://documentation.sisense.com/sso-via-jwt/ [last visited 12 Jan 2018]
- https://nl.wikipedia.org/wiki/Single_sign-on [last visited 12 Jan 2018]
- https://help.salesforce.com/articleView?id=identity_provider_examples_3p_adfs.htm [last visited 12 Jan 2018]
- https://en.wikipedia.org/wiki/Claims-based_identity [last visited 12 Jan 2018]
- https://support.code42.com/Administrator/5/Configuring/Single_sign-on/Introduction_to_single_sign-on [last visited 12 Jan 2018]
- https://www.linkedin.com/pulse/how-implement-sso-aspnet-mvc-application-adfs-tuomas-kesti/ [last visited 12 Jan 2018]
- https://www.mandsconsulting.com/federated-sso-a-primer-saml-oauth-2-0-openid-connect/ [last visited 15 Jan 2018]

- https://www.red-gate.com/simple-talk/dotnet/asp-net/introducing-single-sign-on-to-an-existing-asp-net-mvc-application/ [last visited 17 Jan 2018]
- https://www.mutuallyhuman.com/blog/2013/05/09/choosing-an-sso-strategy-saml-vs-oauth2/ [last visited 17 Jan 2018]