



Legisway

Single Sign-On using
SAML 2.0



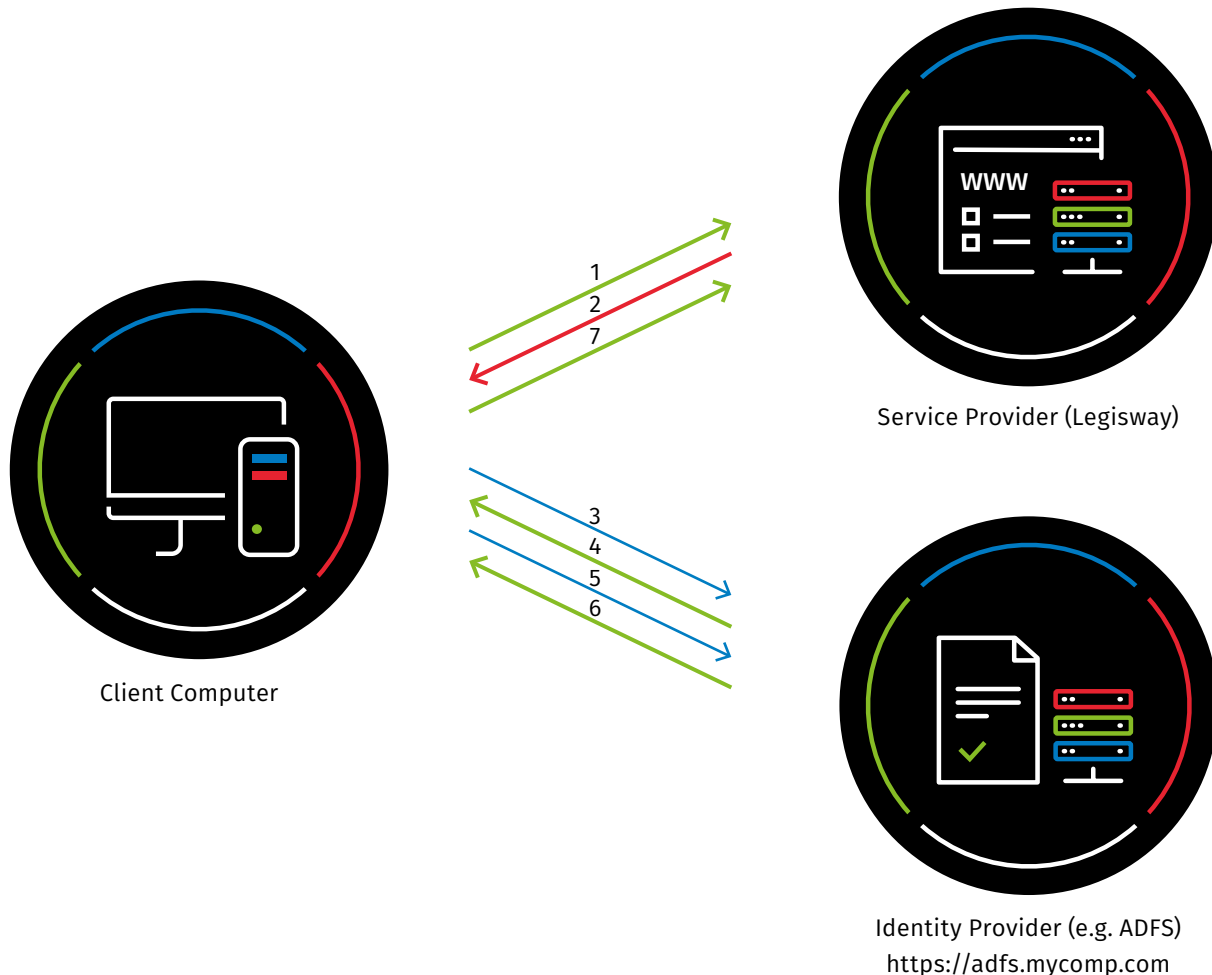
What is SAML?

SAML is a protocol that offers a unique and secure way for authenticating users on a corporate controlled authentication server to allow access to other web servers (both on premise and in the cloud). There is no direct communication required between the server that authenticates (called Identity Provider) and the actual web application (called Service Provider), in this case Legisway. Communication is done via the browser, therefore the browser should have access to both the Identity Provider and Legisway.

Popular implementations of SAML Identity Providers are Microsoft ADFS and Azure Active Directory SSO. Both system integrate with the corporate Active Directory system so the users will authenticate to Legisway with the same password and/or token as they do for the Windows network. Once a user account is disabled, this person will no longer be able to log on to all the Service Providers that depend on this Identity Provider.

How does it work?

The following diagram briefly shows the process of a user that is accessing the Legisway application and needs to authenticate on **<https://adfs.mycomp.com/>**:



Step 1: The user enters the Legisway address in their browser to navigate to the application.

Steps 2 and 3: The Legisway application notices that the user was not logged onto first system yet and automatically redirects the browser to the Identity Provider to authenticate.

Step 4: The Identity Provider presents an authentication page to the browser asking for the user's login credentials, e.g. a username and password in combination and a onetime password. This page is the first page that the user will see after entering the URL in the address bar.

Step 5: The user enters their credentials and posts the information to the Identity Provider where it is checked (e.g. when Active Directory is used it will check whether the username and password are valid).

Step 6: The identity provider prepares the assertion message and sends it back to the browser. Basically this assertion message is a small XML message that has information about the user, the exact time that he is allowed to start the session (current time plus or minus a few seconds) and the service provider to which the access is granted. This message is digitally signed by the Identity Provider.

Step 7: The browser automatically passes this assertion through to the Service Provider. The application will check whether the digital signature is valid and is generated by the trusted Identity Provider and checks the content of this message. If all is well, a new session is established for the client and the user can start to work in Legisway.

Most of the above steps are done automatically, so from the user's perspective it will look easier:

1: The user navigates to the Legisway application and will immediately see the corporate login page.

2: The user enters their (Windows) username and password and clicks 'Login'.

3: The user will now see the main dashboard of the Legisway application and can continue to work.

When the user accesses the system from a computer that is part of the same Active Directory domain as the Identity Provider it could even be simpler than this because the Identity Provider can authenticate the user via SSPI/Integrated Windows authentication. In this case the user does not need to enter a username and password but will see the main dashboard immediately after entering the Legisway URL. The Identity Provider does of course do the authentication but this is invisible to the user.

So ADFS is capable to see if it should display a login screen or not, the user will always start with the same URL to enter Legisway.

How to configure it with ADFS

To start using Single Sign-On via SAML, the company will have to set up an Identity Provider like ADFS. ADFS is a standard component on Windows Active Directory servers. ADFS publishes a website via IIS that should be available to users on the local network and on the internet. IIS needs a valid SSL certificate and the firewall should be configured to allow users from the Internet to access it.

The next step is to register the domain name in Legisway under which the application can be accessed, this name can be chosen freely.

In the Identity Provider management console we can add a new service provider for Legisway and let it refer to a generic domain name, that includes your company name.

The identity provider publishes a federation metadata document in Legisway. We will use the content of this document to do the final settings:



The location of the Identity Provider where the unauthenticated users will be redirected to



The digital certificate of the Identity Provider that will be used by Legisway to check the assertion messages



The unique ID of the Service provider as it is generated by the Identity Provider



The location of the data in the assertion messages that will match the usernames in Legisway

In Legisway new users can be created for which the username should match the username or email in Active Directory.

Legisway

Built specifically for legal departments and backed by our deep legal expertise, Legisway enables immediate digital transformation and provides rapid return on investment. The Legisway portfolio of products is designed to fulfil from basic to advanced needs. Our solutions can be configured and scaled to cover the changing needs as your legal department evolves. We empower legal professionals to boost efficiency, increase collaboration across the business, and enable business growth.

To learn more about Legisway or to arrange a demo:

→ wolterskluwer.com/en-gb/solutions/legisway

Wolters Kluwer Legal Software

Wolters Kluwer's Legal Software unit, part of the group's Legal & Regulatory division, is a global leading provider of innovative and practical software solutions for corporate legal departments and law firms. Its cloud-based and on-premise portfolio of solutions is developed side by side with customers, enabling legal professionals to increase efficiency, performance and mitigate risk. State of the art, ISO-certified technology and teams of experts ensure the highest security and quality of service for more than 100,000 legal professionals across nine countries in Europe and the US.

To discover more:

→ wolterskluwer.com/en-gb/solutions/legal-software