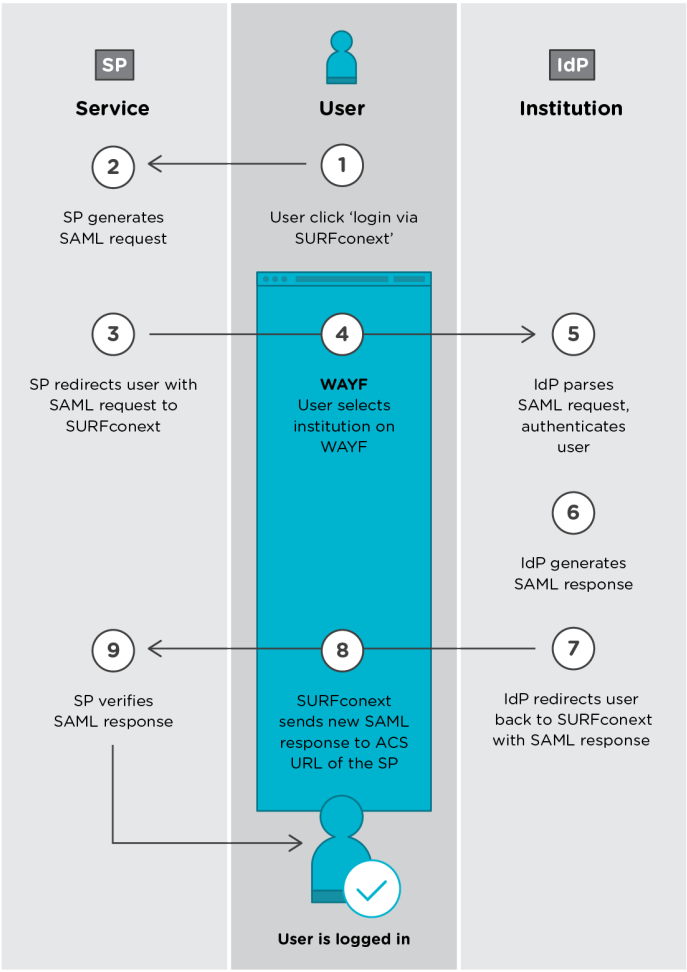
SAML authentication flow

With SAML, trust is established between all parties by exchanging metadata. These metadata contain all the information necessary for one entity to send a message to another (like endpoint locations, bindings and signing certificates). SURFconext couples the SP and the IdP based on specific rules. Note that SURFconext itself does not authenticate users, this is done by the connected Identity Providers.

SAML authentication process in steps

The figure shows you the sign-on process step-by-step. Let's imagine Alice want's to sign-on to a Google Mail instance that is registered for her institution on SURFconext. The authentication will be as shown in the figure below. All messages are send from the user's browser. In blue you see what happens in the user's browser at SURFconext. Let's dive into this.



1. Alice will access the remote application using a link on the intranet, a bookmark or similar and the application will load. Let's assume the **URL** is http s://mail.google.com/a/my-university.nl
2. The application identifies the user's origin by the application subdomain, user IP address or similar and redirects the user back to the identity provider, asking for authentication. When connected to SURFconext, SURFconext is

the Identity Provider to the service. This is the **authentication request** and the SP will generate a **SAML Request**.
3. The SP will instruct the browser to **redirect** the user to SURFconext with a request to authenticate the user.
4. When Alice's browser arrives at the SURFconext she must select her IdP for authentication. This is done using the so-called **WAYF (Were Are You From) page**. Alice chooses the institution she has an account with.
5. Embedded in the redirection is a **SAML Authentication Request**. This message is compressed to save space in the URL and encoded because some characters are not allowed in URL's. Simply said, this message is: "This is a request from the SP with EntityID ' https://mail.google.com/a/my-university.nl'. Please authenticate the user and send the result back to me." *For detailed information about the authentication request read our page about authentication requests.* The IdP will continue to the next step.
6. After successful authentication, the IdP builds the **authentication response** in the form of an XML-document, signs it using an X.509 certificate, and posts this information to the service provider, which is SURFconext for the IdP. This is the **SAML Response** and this message also contains the user's attributes.
7. The IdP sends the **Encoded SAML Response** to Alice's browser. Basically this says “This is a message from idp.my-university.nl, I have successfully authenticated a user. Take note that this message will expire in a couple of minutes”. The message contains an XML digital signature, proving that the message was sent by idp.my-university.nl. The signature was made using a public key algorithm, the public key being embedded in a certificate known to the SP.
8. SURFconext validates the response message and if OK makes some alterations, e.g. rewriting the user's identifier and adding or modifying attributes. According to the attribute release policy applied, SURFconext determines the attributes that are allowed through to the Service Provider. The **SAML Response** instructs Alice's browser to send the response to the **Assertion Consumer Service (ACS) URL** of the SP. An Assertion is a set of security statements about a subject created by an Asserting Party, being an IdP.
9. The SP **verifies the XML signature**, **checks** if the authentication was **successful** and if the message is **not expired**. Then it extracts the **user’s identifier and attributes** as known to SP. If this step is OK, Alice is logged on, her mailbox is retrieved and she can read her mail.

Most services will use the flow as described. You will have noticed that the service only needs to connect to SURFconext, which is the identity provider to the service. All the user data (such as passwords) are managed by IdPs, and attributes are managed by SURFconext, which will save you a lot of hassle. SURFconext acts both as an IdP and as an SP. It is an IdP to SPs and an SP to IdPs.

Navigate