For a service

Introduction

A service can connect to SURFconext or SURFsecureID to handle it's strong authentication login. There are only a few differences between both options. But whenever possible, connect your service to SURFconext as this is the preferred method.

With SURFsecureID, the login process will not only perform the first factor (username/password at the institution's Identity Provider), but also the second factor as chosen by the end user.

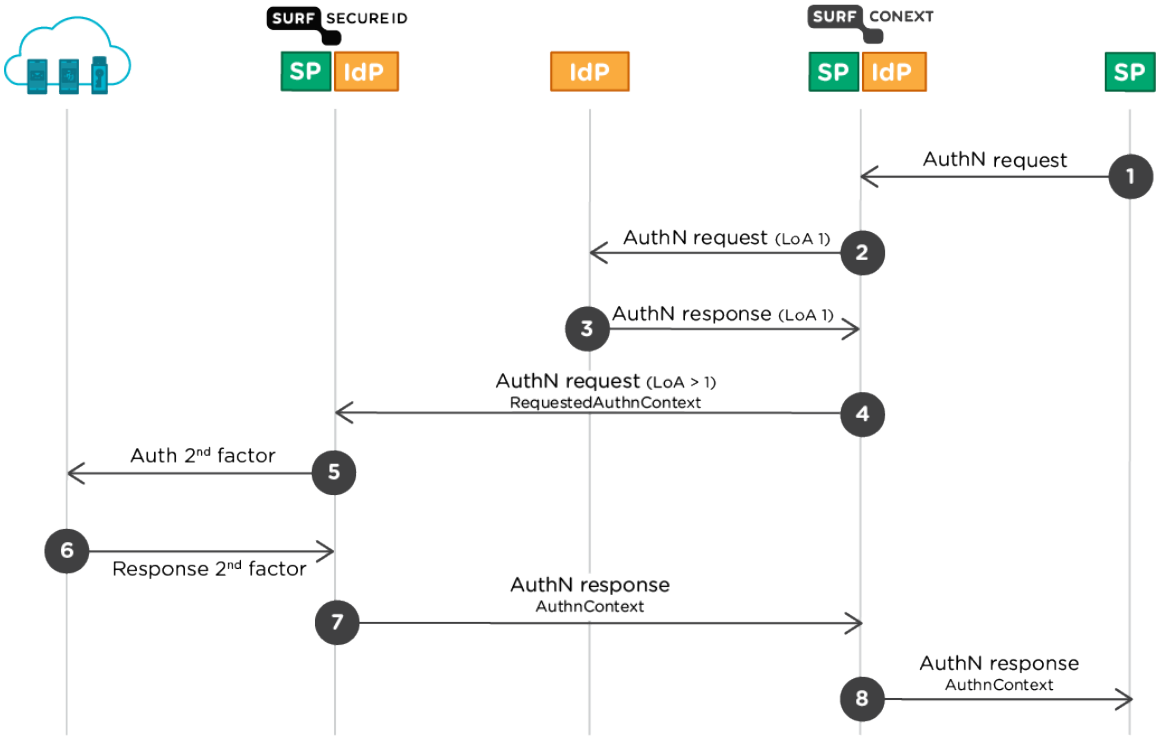
Option A: The service connects to SURFconext

Many services are already connected to SURFconext or can easily make such a connection. The service provider or the institution consuming the service can determine that strong authentication is needed for accessing the service. Enabling SURFsecureID is nothing more than a configuration in SURFconext and can be requested via support@surfconext.nl. The institution or service provider do not need to make any changes to their implementations.

Note that:

- This option is preferred above option B
- The service can connect with SAML or OpenID Connect to SURFconext, both will work
- This integration does not supports dynamic LoA request by the service. If the service wants to use this feature it needs to connect to SURFsecureID directly (see option B).
- This option works for the production and test environment, not for the pilot environment.

Authentication flow



1. The SP sends a SAML 2.0 AuthnRequest or an OpenID Connect to SURFconext.
2. The user chooses the Identity Provider (institution) where to login for the 1st factor and SURFconext sends this IdP a SAML AuthnRequest
3. The user logs in at the IdP and a SAML response is sent back to SURFconext with the identity and attributes of the user
4. In this case, SURFconext is configured for this SP or SP-IDP combination to call SURFsecureID with a minimum LoA (>1).
5. SURFsecureID gateway sends the user to the authentication provider for the 2nd factor

6. The 2nd factor authentication provider returns the response to the SURFsecureID gateway.
7. The SURFsecureID gateway sends a SAML Response back to SURFconext
8. SURFconext sends a SAML Response with Assertion and the attributes and the identity of the user to the SP.

For the SP only steps 1 and 8 are visible.

Note that the SP chooses where to send the AuthNrequest (i.e. SP initiated authentication).

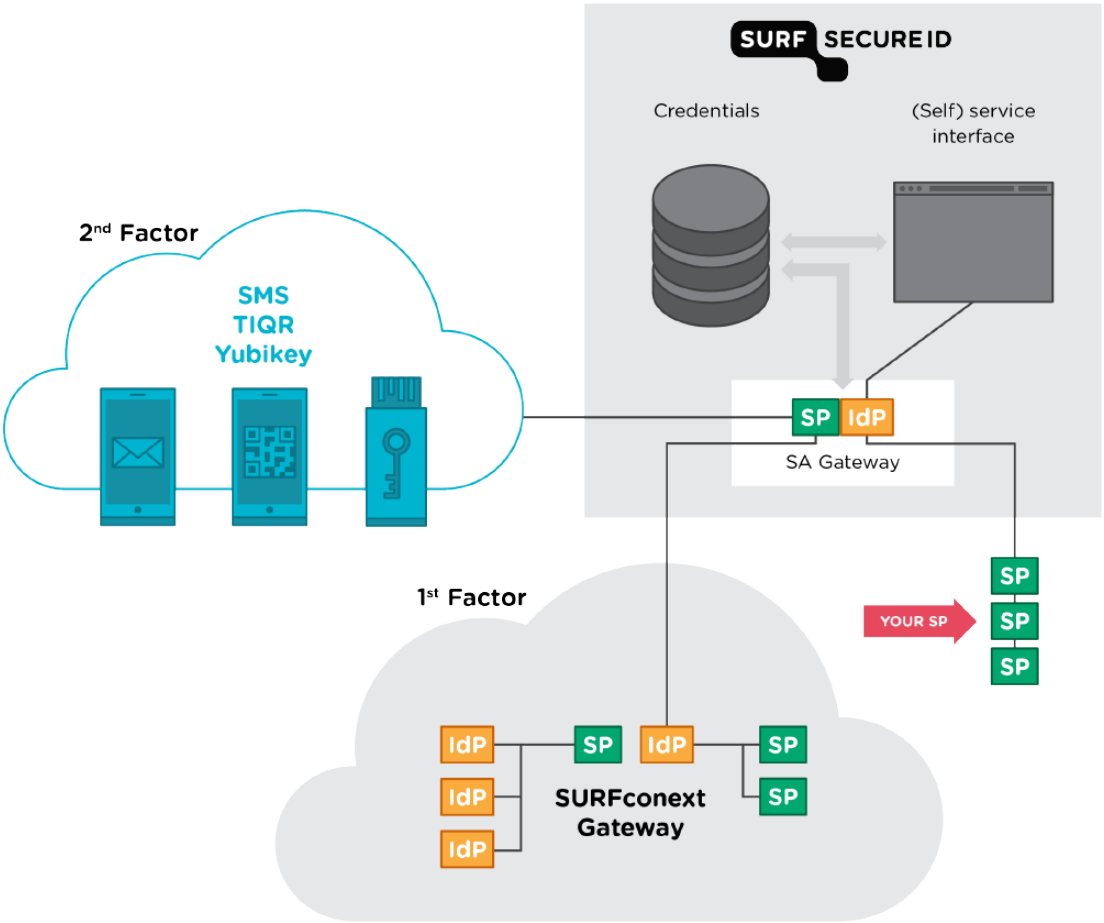
Option B: The service connects to SURFsecureID

Usually, a Service Provider and institution together determine if strong authentication is needed for a specific service. The Service Provider can connect its service to the SURFsecureID endpoint, and the institution makes sure the users are properly registered with their strong authentication token. Institutions do not need to make any changes to their Identity Providers to implement this option.

Architecture overview

The picture below shows the relation between:

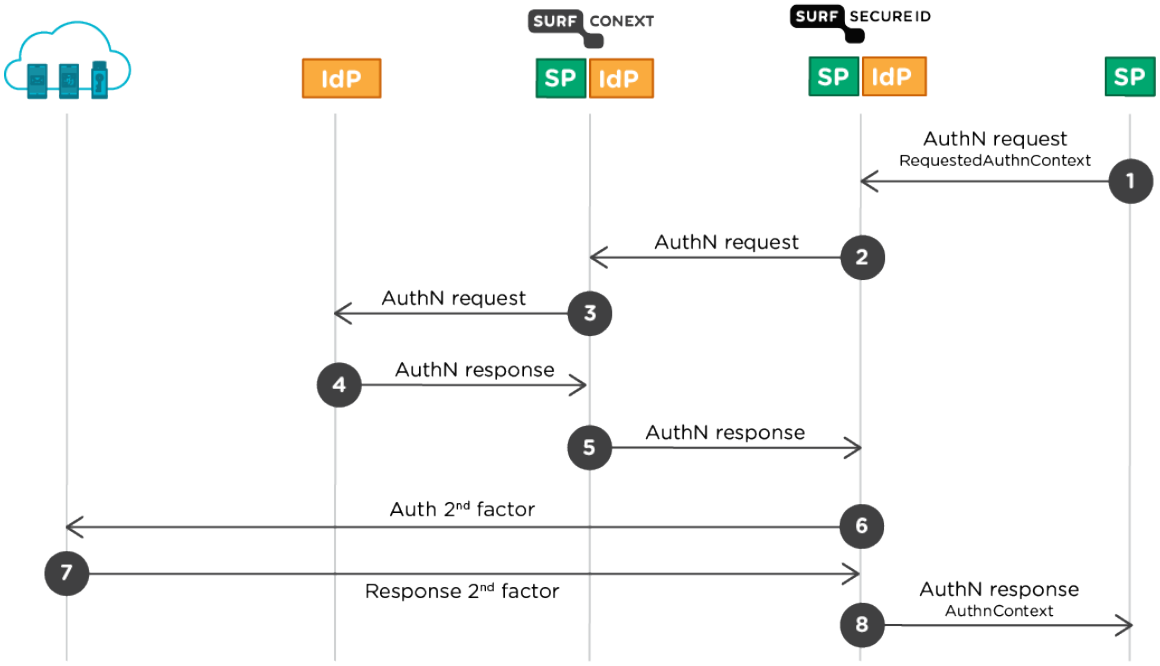
- SURFsecureID gateway
- SURFconext gateway
- SPs
- Second factors used for SURFsecureID (SMS, Tiqr and YubiKey)



Note that:

- There are no technical changes required for IdPs. They still connect to SURFconext.
- SPs connect to the SURFsecureID Authentication gateway using SAML. No connection with SURFconext or integration with second factor authentication devices is required.

Authentication flow



1. The SP sends a SAML 2.0 AuthnRequest to the SURFsecureID gateway.
   The SP may use a RequestedAuthnConext to specify the minimal LoA at which a user must be authenticated.
2. The SURFsecureID gateway sends a Authn request to SURFconext.
3. SURFconext takes care of the authentication of the user at their home IdP.
4. The user logs in at his home IdP and is returned with a SAML response to SURFconext. SURFconext applies policies: attribute release, user consent and institutional consent
5. The SURFsecureID gateway receives a response from SURFconext with the identity and attributes of the user.
6. The SURFsecureID gateway determines whether strong authentication is required and if so sends the user to the authentication provider for the 2nd factor.
7. The 2nd factor authentication provider returns the response to the SURFsecureID gateway.
8. The SURFsecureID gateway sends a SAML Response with Assertion and the attributes and the identity of the user to the SP.

For the SP only steps 1 and 8 are visible.

Note that the SP chooses where to send the AuthNrequest (i.e. SP initiated authentication).