For a service

Introduction

A service can connect to SURFconext to handle it's strong authentication login. Previously, it was also possible to connect a service to SURFsecureID directly, but this has been deprecated. All necessary (and more) functionality to enable SURFsecureID for a service can be handled by SURFconext.

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.

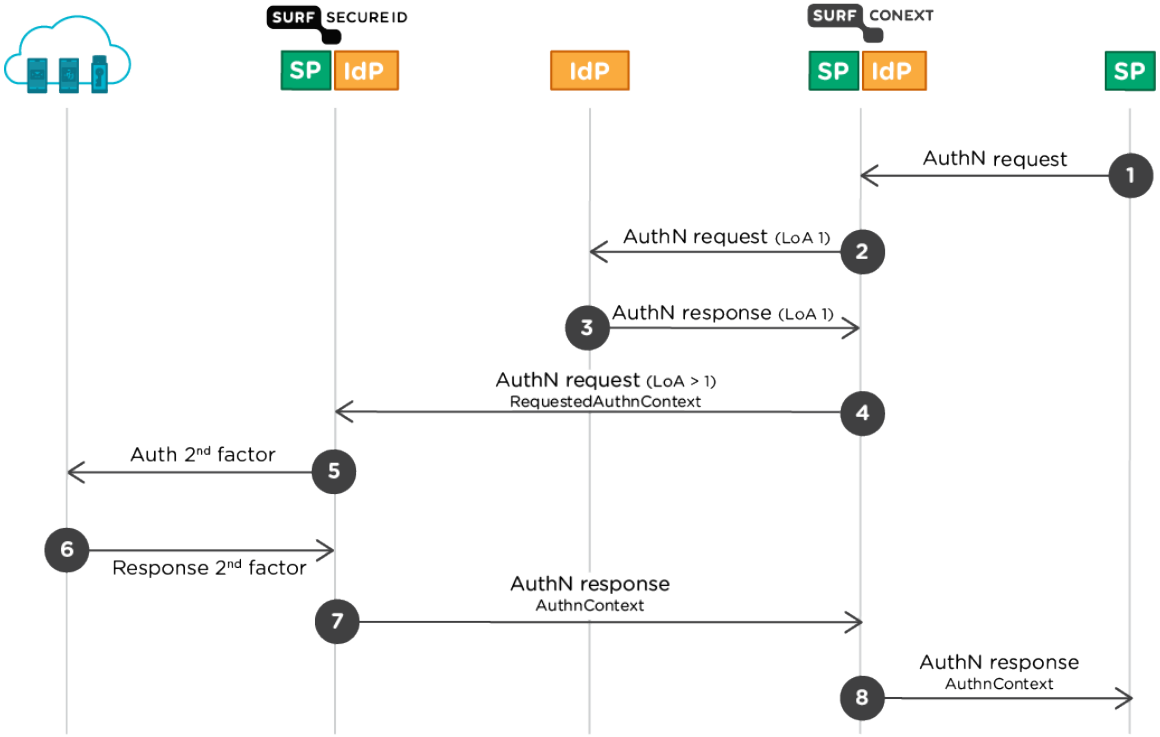
The service connects to SURFconext

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 can be done by the SURFconext-responsible person ("SURFconext-verantwoordelijke") from the institution in the SURFconext Dashboard by going to the specific service, go to the SURFsecureID tab and select an appropriate Level-of-assurance. The institution or service provider do not need to make any changes to their implementations.

Note that:

- The service can connect with SAML or OpenID Connect to SURFconext, both will work
- A step-up policy can be configured in SURFconext that determines for which persons SURFsecureID is called. This can be configured based on user-attributes or IP adres. See option 2 on this page.
- This integration also supports dynamic LoA request by the service.

Authentication flow



1. The SP sends a SAML 2.0 AuthnRequest or an OpenID Connect request 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 or OpenID Connect Response with 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).

(DEPRECATED) The service connects to SURFsecureID

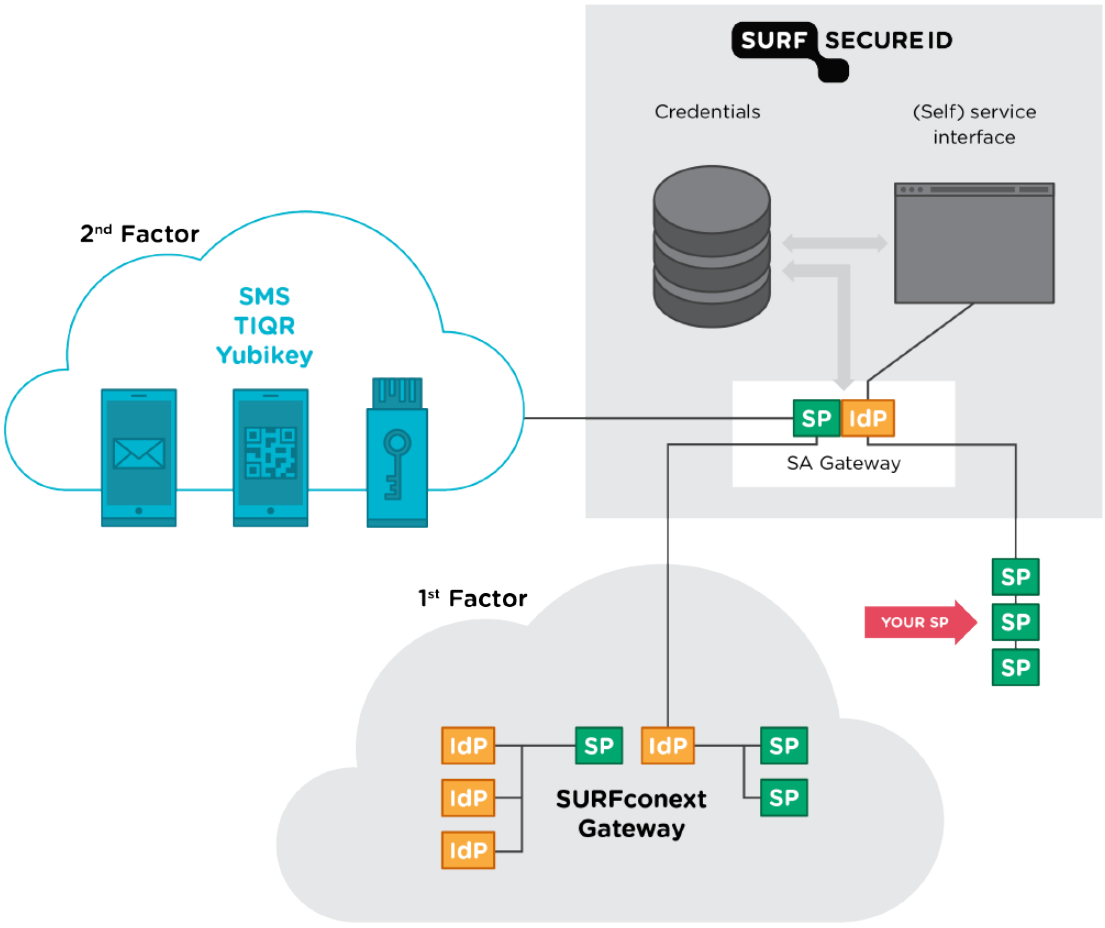
For test and production systems, there is no need any more to connect a service directly to SURFsecureID. Instead, connect the service directly to SURFconext and configure SURFsecureID there. All (and more) functionality is present in SURFconext to protect a service with SURFsecureID.

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:

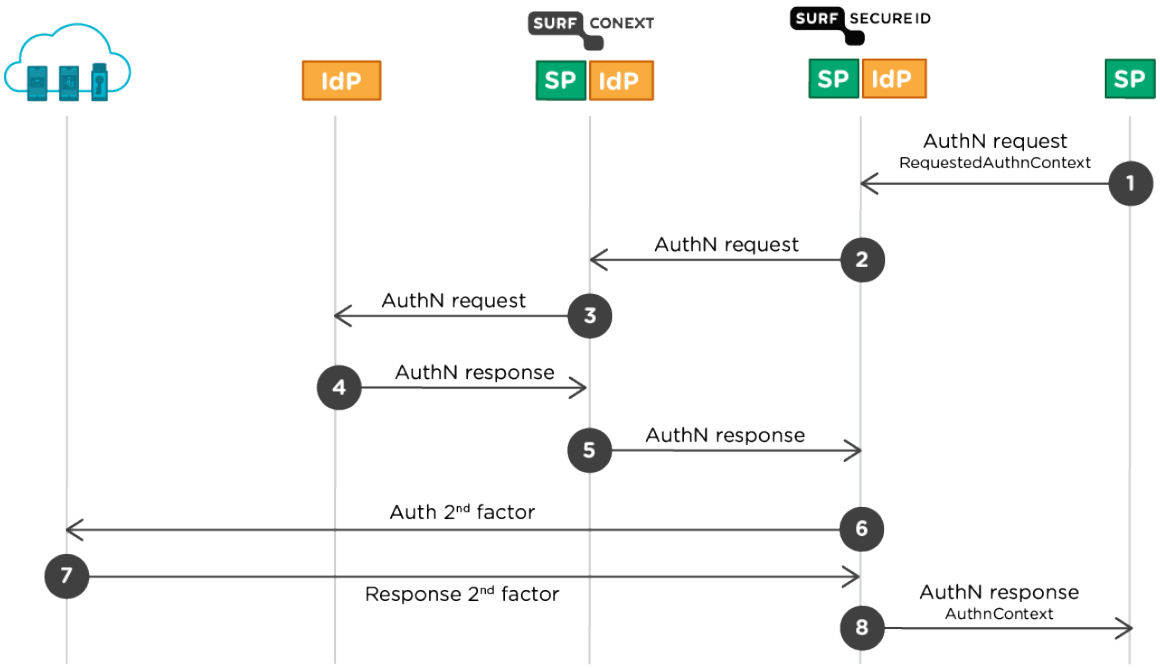
- SURFsecureID gateway
- SURFconext gateway
- SPs
- Second factors used for SURFsecureID (SMS, Tiqr, Azure MFA, YubiKey and FIDO2)



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).