For a service

Introduction

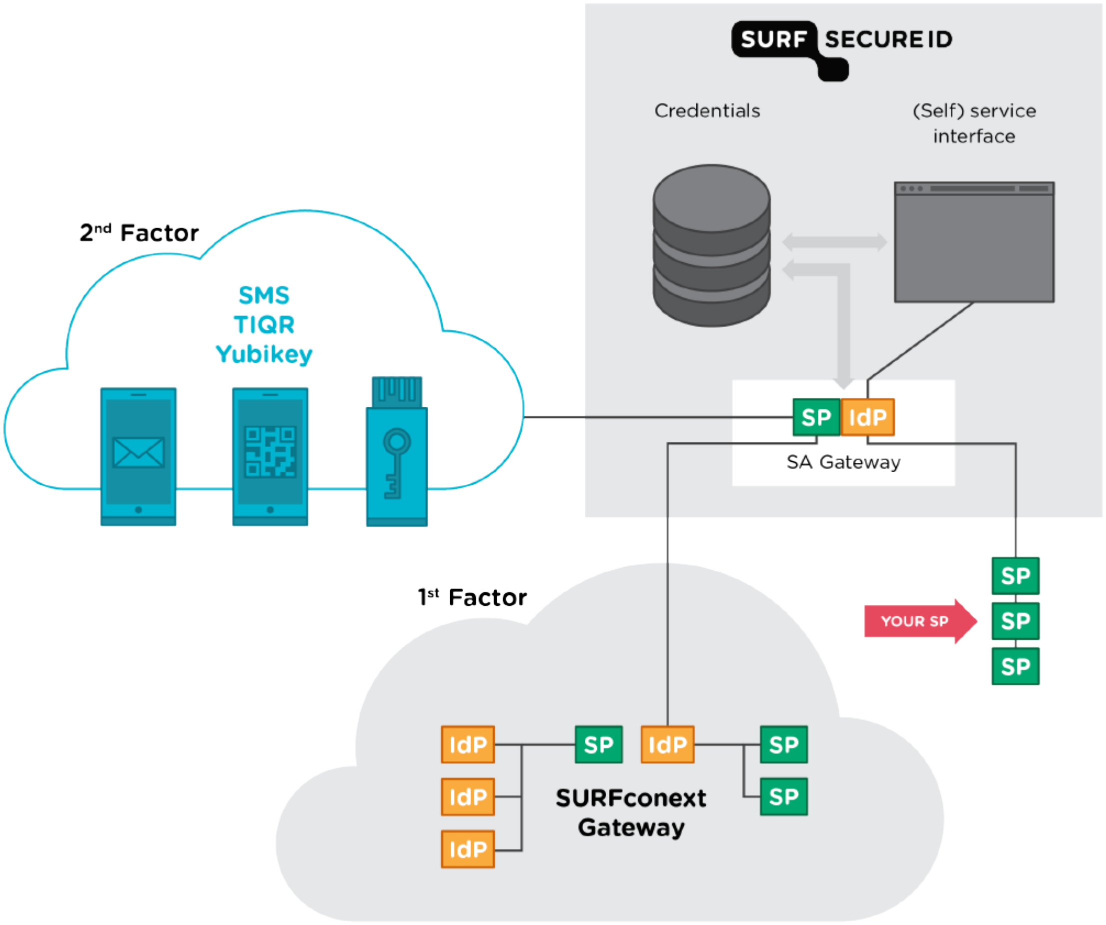
A service can use SURFsecureID to handle it's login, much like SURFconext is used to perform user login for services. There are only a few differences between a SURFconext and the SURFsecureID connection. With SURFsecureID, the login process will not only perform the first factor (username/password at the institution's Identity Provider), but also the second factor as chosen by the end user.

Usually, a Service Provider and institution together determine if strong authentication is needed for a specific service. The Service Provider connects 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)

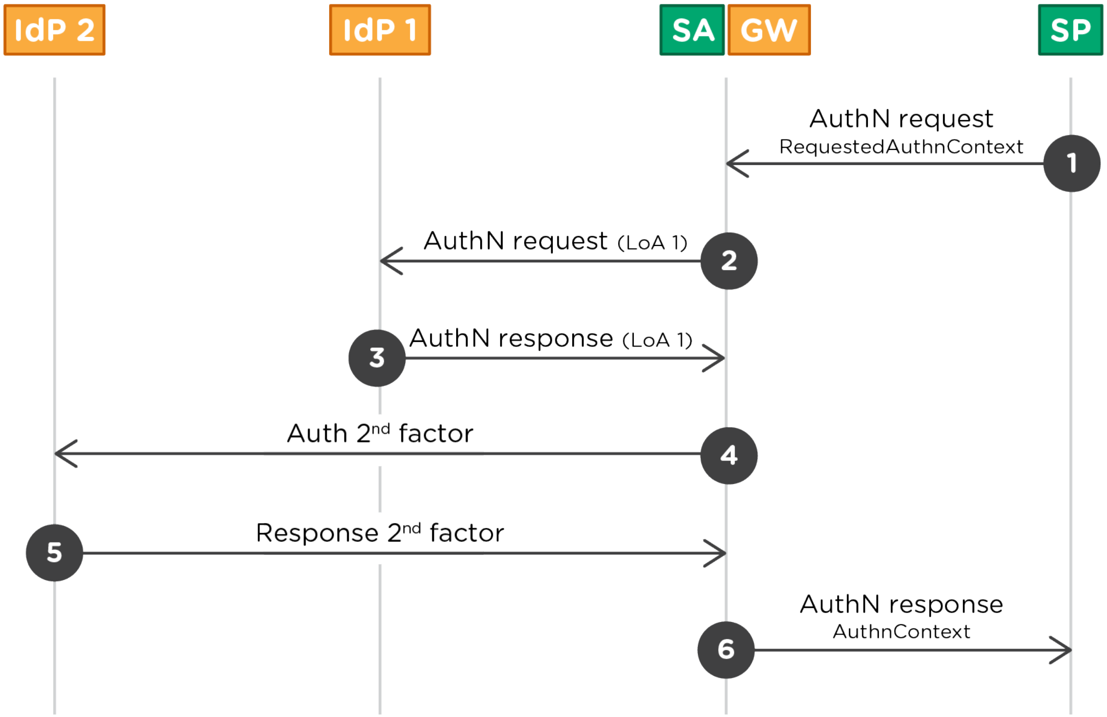


Note that:

- There are no technical changes required for IdPs. They still connect to SURFconext.

- SPs connect to the SURFsecureID Authentication gateway. 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 (SA-GW).
   The SP may use a RequestedAuthnConext to specify the minimal LoA at which a user must be authenticated.
2. The SA-GW sends a Authn request to SURFconext (IdP1).
   SURFconext takes care of the authentication of the user at their home IdP (not shown) and applies policies: attribute release, user consent and institutional consent.
3. The SA-GW receives a response from SURFconext (IdP1) with the identity and attributes of the user.
4. The SA-GW determines whether strong authentication is required and if so sends the user to the authentication provider (IdP2) for the 2nd factor.
5. The 2nd factor authentication provider (IdP2) returns the response to the SA-GW.
6. The SA-GW 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 6 are visible.

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