For an institution

Introduction

An institution can use SURFsecureID to add a second authentication factor to any service or facility. This is most valuable when added to an existing, central (authentication) facility. For instance, if an institution uses Microsoft ADFS to secure internal or external services with username /password credentials, ADFS can use SURFsecureID to handle the second authentication factor. This mechanism is also called Second Factor Only (SFO) authentication because SURF only delivers the second factor while the service or facility needs to perform the first authentication factor.

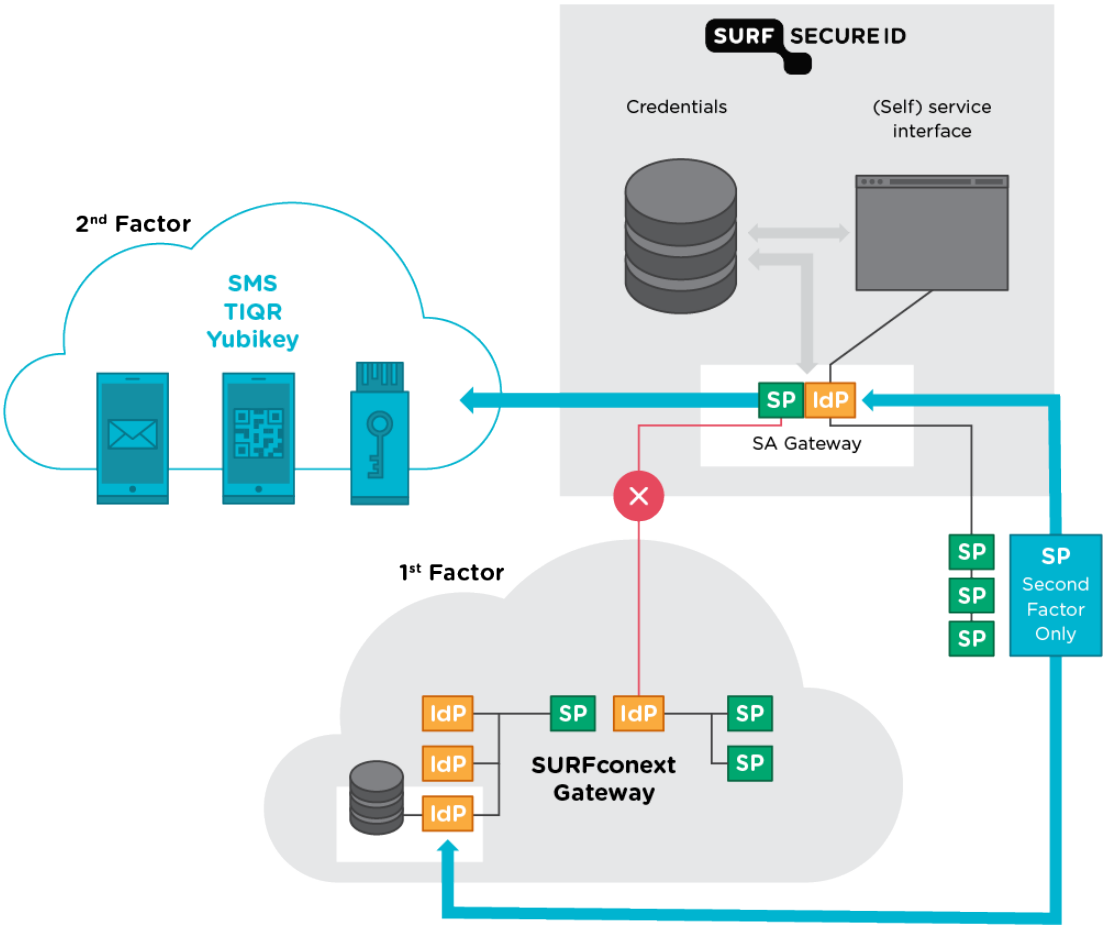
Second Factor Only authentication allows a SP to authenticate only the second factor of a user. With SFO you can add two factor authentication to your institutions application gateway (e.g. Citrix Netscaler or F5 BIG-IP) or to the authentication or authorization gateway (e.g. Microsoft ADFS or Novell/NetIQ). SFO has its own authentication endpoint at SURFsecureID.

Once a user is registered with a second factor both SFO authentication and SURFsecureID can be used.

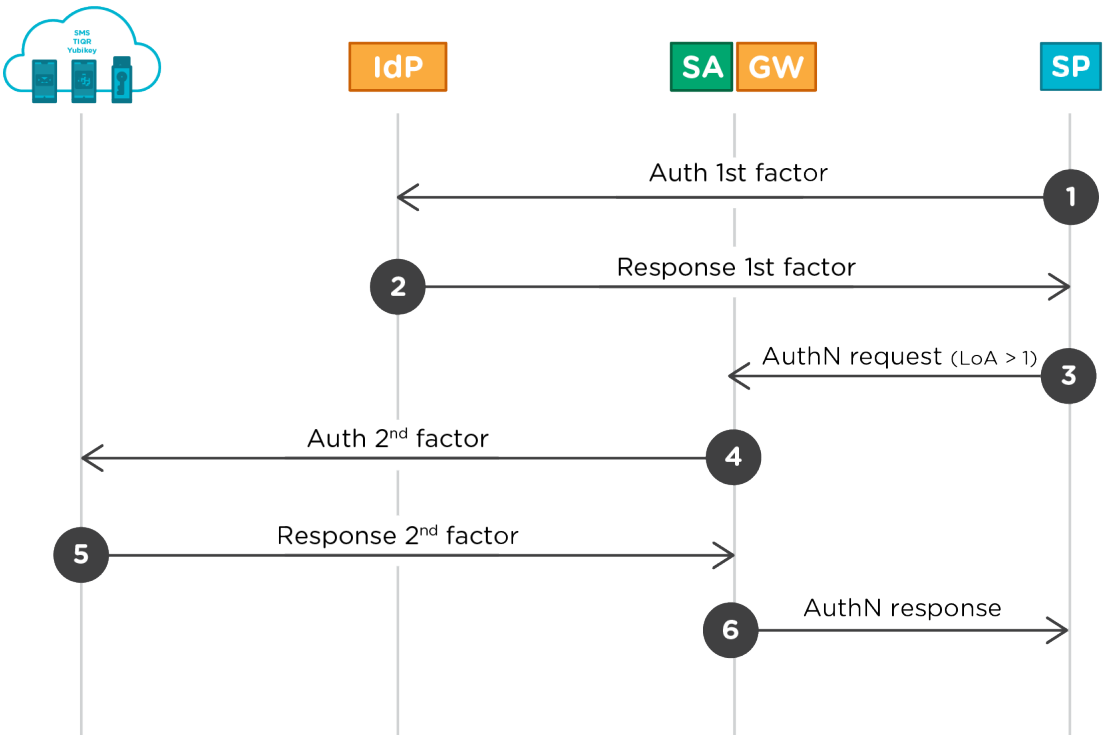
Architecture overview

With SFO the authentication via SURFconext is bypassed (see image below). This means that SURFconext functionality (e.g. attributes from the user's home IdP, the definition of authorization rules and persistent user identifiers) is not available.

Note that also with SFO the registration of users will be done by the institutions (IdP's): there is no work to be done for the SP.



Authentication flow



In the above diagram the authentication flow for SFO is shown.

1. The service (SP, like ADFS, Citrix, F5 or any other capable system) performs the 1st authentication factor itself, outside of SURFsecureID. This is usually done directly against the IDP of the institution.
2. The user's credentials (usually username/password) are validated by the IDP and the result of the 1st authentication factor is sent back tot he service.
3. The service then starts the 2nd factor authentication by sending the user to the SURFsecureID Authentication gateway (SA-GW) using a SAML authnrequest. There, the user selects his 2nd factor token type and the 2nd factor authentication is started.
4. The user's 2nd factor token is validated.
5. The result is sent back to the SA-GW.
6. If the 2nd factor authentication was successful, the user is sent back to the service with a SAML response indicating the result of the process. The user is now successfully authenticated at the service.