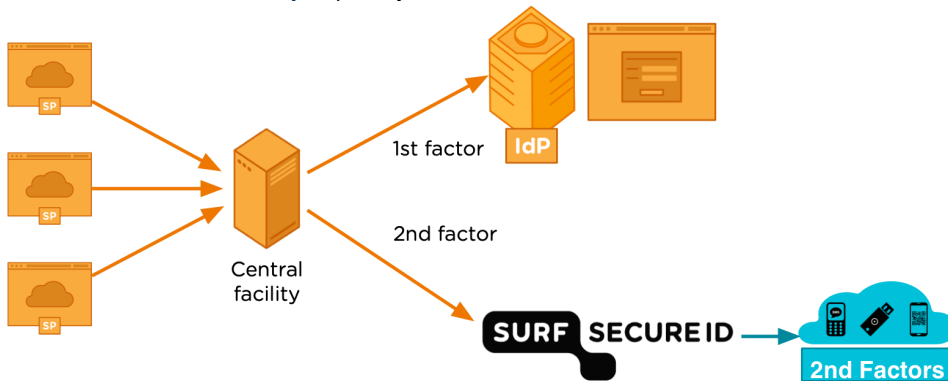


Introduction to SURFsecureID

SURFsecureID gives institutions secure access to services. Better security is particularly critical for services handling sensitive data. Such services require stronger forms of authentication than a username and password in order to limit the risk of security incidents.

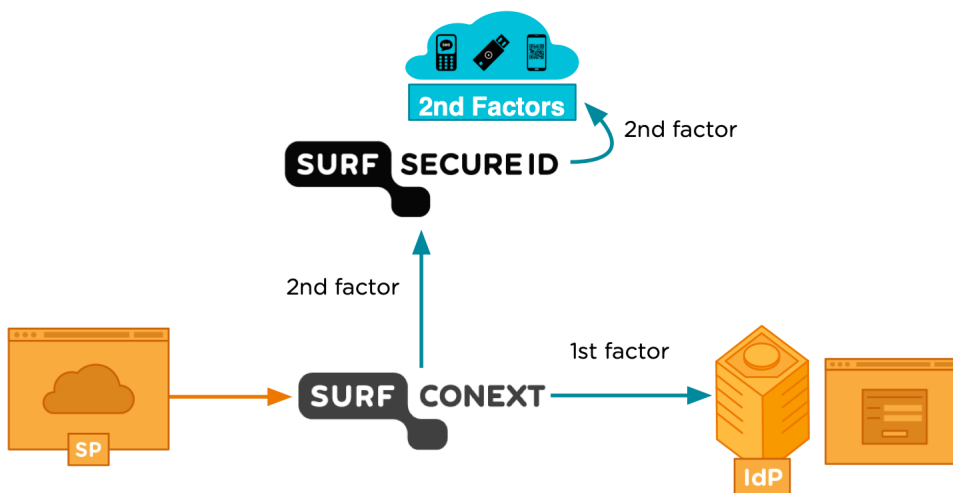
Institutions can use SURFsecureID in two ways. Both can be used at the same time:

1. **In addition to an existing institutional login.** SURFsecureID is only used for the 2nd factor. This is especially interesting for use by a central (authentication) facility such as ADFS, Citrix or F5 BIGIP. This facility handles the 1st factor itself and calls SURFsecureID for the 2nd factor if necessary. This makes strong authentication available for a range of internal and external (cloud) services. This option is also called **Second Factor Only**, especially in the more technical documentation.



2. **For a (cloud) service.** The service outsources the complete login (ie both the 1st and the 2nd factor) to SURFconext. The 1st factor (username / password) via the IdP and the 2nd factor via the available SURFsecureID tokens.

The service (Service Provider, or SP) is connected to SURFconext which is configured to call SURFsecureID for this service. This makes it especially easy for services already connected to SURFconext to use SURFsecureID as this is transparent for the service. The service can use either SAML or OpenID Connect to connect to SURFconext. You can [make use of step-up policies in SURFconext](#) to only request SURFsecureID for specific users (attribute based) or locations (IP adres based). Also, the service can request a [specific LoA level](#) in the request to SURFconext (NB: before june 2021, this was only possible when the service was connected to SURFsecureID directly).



SURFsecureID gives access to services via five different types of tokens: SMS, Tigr (smartphone app), Azure MFA, YubiKey (USB hardware token) or FIDO2 token. An institution can choose which tokens they want to allow for their users. Users first log in with their institutional account and are then prompted to confirm their identity with their token. In this way there is a second layer of security.

SURFsecureID is available at an additional fee for all institutions connected to SURFconext.

How does token registration work?

An institution can either allow their users to perform self-service token registration, or have a servicedesk validate the user's identity before a token can be used. These different processes result in a different [level of assurance](#) (LoA) for the registered token.

Self-service token registration:

1. The user registers his preferred token (SMS, Tigr, Azure MFA, Yubikey or FIDO2) in the registration portal
2. The user registers a recovery method (SMS or recovery code).
3. Now the user can log in to any service with a level of assurance lower or equal to LoA1.5.

Token registration via the institution's servicedesk:

1. The user registers his preferred token (SMS, Tigr, Azure MFA, Yubikey or FIDO2) in the registration portal
2. User must visit his institution's service desk to have an authorised employee verify his identity.
3. This employee will bind the user's token to his account. After that the user's token will be activated.
4. Now the user can log in to any service with a level of assurance lower or equal to LoA2 or LoA3 (depending on the registered token).