Frequently Asked Questions

Should my application be web based to connect to SURFsecureID?

Yes. The main technical prerequisite is that a Service Provider must connect via SAML 2.0 using the Web Browser SSO profile.

Can institutions from secondary vocational-, higher education and research connect their own services to SURFsecureID?

Yes. Every institution connected to SURFconext as an Identity Provider can connect its services to SURFsecureID.

How can an application enforce a specific level of assurance?

This is done via the authentication request to the SURFsecureID gateway. Enforcing a specific level of assurance can be done in two ways:

- **Dynamically** by communicating the required level of assurance with "AuthnContextClassRef". In this way the required level can be defined for each authentication request individually (based on the user authenticating or the selected feature in the application). In most cases modifications to the application are required to facilitate this.
- **Statically**: in the SURFsecureID gateway a minimum level of assurance can be configured (based on the IdP and SP involved). In this way the application does not have to be modified. Authentication for all users from one institution to one application will always require the same minimum level of assurance.

Why is remote registration not supported?

Remote registration is vulnerable to threats and technically complex to achieve. In person registration is therefore the most efficient option. In Q4 of 2017, Innovalor reviewed the options for remote registration. This has resulted in a design an POC phase in the first half of 2019.

Why is Google Authenticator not supported?

Google offers second factor authentication in the form of an SMS service and a smart phone OTP app, but has no face-to-face registration processes. For an individual Google user this will be fine. But for an educational institute, protecting its organisational assets and its reputation, a self-asserted second factor is not enough. They want to determine that a service provider (e.g. a student information system) is dealing with a legitimate user. Face-to-face registration is inevitable to achieve this.

Can a second factor authentication be re-used in one browser session?

No. For reasons of simplicity, transparency and security SURFsecureID does not support Single Sign On (SSO) on the second factor. This means that every authentication request from an SP with a LoA > 1 (every step-up request) requires a new authentication with the user's token.

SSO on the first factor is enabled!

When using the Second Factor Only functionality, the central facility (like ADFS) controls SSO.

How does single logout work with SURFsecureID?

SURFsecureID does not support Single Sign On (SSO). As a result there is no active session on the SURFsecureID gateway for a user to logout. For first factor login SURFsecureID relies on SURFconext. Therefore, the same issues for single logout apply.

Can an institution implement strong authentication on their own IdP and then forward the level of assurance to SURFsecureID?

No. SURFsecureID does not support the transfer of levels of assurance via the local IdP.

LoA 2 and LoA 3 authentication requires (1) strong authentication, (2) strong identification and (3) a solid binding between the user identity and his token. Local implementations of strong authentication (at the IdP) do not guarantee the same solid binding between the user identity and his token. This means that SURFconext cannot guarantee that such an IdP-specific LoA2 and LoA3 implementation is equal to LoA2 and LoA3 facilitated by SURFsecureID. Therefore this is not supported.

Can an institution re-use its own strong authentication tokens?

No, SURFsecureID supports only Yubikey hardware tokens, Tiqr and SMS. Other tokens like the ones from Vasco and Safenet cannot be re-used at the moment. However, SURFsecureID has succesfully carried out a proof-of-concept with Vasco and Azure MFA to use their tokens with SURFsecureID. Depending on user demand SURFconext could enable this option.

Why is the activation code designed as it is?

The activation code should have enough entropy to prevent a guessing attack and yet short enough to be written down by the user.

How long is the activation code valid?

14 days after registering a token. To get a new activation code a user must delete the registered token and start a new registration.

How can SURFsecureID ensure that tokens are bound to the right identity?

Threat	Description	Controls
Impersonation	An applicant claims an incorrect identity, supporting the claim with a specific set of attributes created over time or by presenting false credentials.	During the registration process different methods are used to determine that the applicant is the right person: • federated login • e-mail verification • possession of activation code • face-to-face ID-proofing
Compromise or malfeasance of the infrastructure	Lack or poor implementation of security measures undermine the reliability of the registration.	Infrastructure threats are addressed by normal computer security controls: • separation of duties • record keeping • independent audits Also a third party security audit on software code and infrastructure was conducted.

How can I order YubiKey tokens?

There are several options where you can buy YubiKeys.

Can a user register multiple tokens?

Yes. If the user's institution allows the use of multiple tokens, the user can register multiple tokens as long as each one is of a different type. For example, a user can register a tiqr and a Yubikey, but not two tiqr apps or two Yubikeys.

Can I install the Tiqr app on multiple devices after registering once?

No. For security reasons only one token registration per user is allowed.

What is the length of the session of your second factor at an SP?

The length of the session is SP specific. For usability reasons it should not be too short (< 30 min), for security reasons it should not be too long (> 4-8 hours).

Can I activate the token of a user who cannot come personally to the service desk?

No. Our policy - in line with ISO29115 - explicitly requires a user to appear in person.

How can I revoke the token of a user?

There are three ways to achieve this:

- The easiest way is to remove the first factor of the user (= username/password) through your regular exit proces/ IDM-lifecycle. Once the first factor is removed, the user can no longer use his second factor.
- Ask the RA of your institution to remove the second factor registration through the RA Management portal.
- Users who have not used their token for 6 months receive a reminder by e-mail. If they do not react, SURFconext will remove their token registrations.

Yes. The user identifiers and attributes provided by both gateways are the same. When a SP is connected to the SURFsecureID Gateway, it can also connect to the SURFconext gateway (connect = can use the gateway to authenticate users). The SP chooses where to authenticate and whether to accept the provided authentication. Usually authentication starts at the SP (i.e. SP-initiated login). For SURFsecureID this is the only flow supported. SURFconext also supports the IdP-initiated flow, where a SP receives an unsolicited SAML Response. It is up to the SP whether to accept such a response.

Single-sign-on (SSO) on the first factor is supported when using both endpoints simultaneously. So a scenario where a SP uses the SURFsecureID gateway only for LoA 2 and higher authentications and continues to use the SURFconext gateway for other authentications can be used without impacting the user experience.

What certificate must my SP use to sign the SAML authentication request (AuthnRequest)?

The SAML AuthnRequest must be signed with a X.509 certificate. We recommend that you generate a self signed certificate for this purpose, and that you do not reuse the SSL/TLS certificate of your server for this. So you do not need to buy an additional certificate for signing the SAML AuthnRequest.

The SAML Signing certificate:

- must be self-signed
- must contain a RSA public key with a public modulus between 2048 and 4096 bits

The SURFsecureID Gateway did not receive the eduPersonTargetedID (EPTI) attribute. This attribute is required when authenticating to a Service Provider (SP) that uses SURFsecureID. Ask SURFconext support to release this attribute. Please include the SAML EntityID of the SP and the error code in your message.

If you are using the OneGini.me guest IdP ensure that your email address is validated at the OneGini service.

No, only production identities are available in the Pilot environment. OneGini is available in the Pilot environment: for authentication with LoA > 1 this identity must be vetted first. If you want to use the DIY IdP you can make use of the SURFsecureID test environment. See here for an overview of the SURFsecureID environments.