

LOGGING IN IN TWO EASY STEPS

TEXT MESSAGE, TIQR AND YUBIKEY

SURF SECUREID

When using services that handle sensitive data, logging in using your institutional account is not secure enough, which is why a 2-step login process is required for some services from now on.

You log in using your institutional account, after which you verify your identity using text message, tiqr or YubiKey.

What do you need?



SMS/ TEXT MESSAGE

- A mobile phone you can use to receive text messages
- Access to your institutional account (email)



TIQR

- A smartphone (iOS/Android) on which you can install the tiqr app
- Access to your institutional account (email)
- Activate push notifications for the tiqr app



YUBIKEY

- A YubiKey (v5, v4, Standard, Edge or Neo)
- A device with a USB port (e.g. a PC or laptop) to which you can connect your YubiKey
- Access to your institutional account (email)

LOGGING IN IN TWO EASY STEPS

TEXT MESSAGE, TIQR AND YUBIKEY

More information

- Check the Frequently Asked Questions on <https://support.surfsecureid.nl>
- Having trouble? Please contact the Service Desk at your institution

How do you log in to services?



SMS/ TEXT MESSAGE

- Select your institution and log in using your institutional account
- Click 'send code' to receive a one-time pass code on your registered mobile phone
- Enter the pass code, and you are logged in successfully



TIQR

- Select your institution and log in using your institutional account
- You will now receive a push notification on your smartphone
- Enter your tiqr PIN, use your fingerprint or Face ID
- If you have not received a push notification, you must scan the QR code using the tiqr app on your smartphone
- You have successfully logged in



YUBIKEY

- Select your institution and log in using your institutional account
- Connect your YubiKey to one of your computer's USB ports
- Press the button on your YubiKey, and you are logged in successfully