FAQ SURFsecureID

Waarom moet ik mij identificeren?

Jouw instelling wil zeker weten dat diensten en gegevens veilig en alleen toegankelijk zijn voor geautoriseerde personen. Voor toegang tot extra gevoelige diensten of gegevens wordt SURFsecureID ingezet. De instelling wil dan zekerder weten dat degene die toegang heeft ook is wie hij zegt dat hij is. Een deel van de oplossing is om dan een 2e factor te gebruiken om mee in te loggen. Maar alleen een 2e factor zorgt niet voor meer zekerheid over de identiteit van de persoon; als ik bijvoorbeeld bij Google een account aanmaak als Pietje Puk, dan kan ik daar ook prima een 2e factor bij activeren, maar dat maakt nog niet dat ik ook echt Pietje Puk ben. Daarom wordt je bij SURFsecureID, voordat de 2e factor wordt geactiveerd, gevraagd je te identificeren. Zo staat met een hogere mate van betrouwbaarheid vast dat jij ook bent wie je zegt dat je bent, en dat kun je in het vervolg aantonen met je SURFsecureID token.

Waarom wordt een deel van het documentnummer opgeslagen?

Een belangrijk onderdeel van SURFsecureID is dat tijdens het activeren van het token de identiteit van de gebruiker wordt gecontroleerd met een identiteitsbewijs. Om er zeker van te zijn dat er daadwerkelijk een identiteitsbewijs is gecontroleerd moet de servicedeskmedewerker de laatste 6 posities van het documentnummer registreren. Dit zorgt er aan de ene kant voor dat de servicedeskmedewerker de identificatie niet overslaat vanwege druk of gemak, en aan de andere kant dat er ook zorgvuldig naar het identiteitsbewijs is gekeken. Dit laatste kan bijvoorbeeld al voorkomen dat er een vals identiteitsbewijs wordt gebruikt.

Zie ook de regels van de Autoriteit Persoonsgegevens over het gebruik van je identiteitsbewijs door een organisatie.

Wat is een geldig identiteitsbewijs?

De volgende documenten zijn geldige identiteitsbewijzen in Nederland:

- een Nederlands paspoort of een paspoort of identiteitskaart van een land binnen EU of EER. Paspoorten van alle andere landen dienen een geldige verblijfssticker/stempel te hebben;
- een Nederlandse identiteitskaart;
- een vluchtelingen reisdocument uitgegeven door de Nederlandse overheid;
- een buitenlands reisdocument uitgegeven door de Nederlandse overheid;
- een verblijfsdocument of een W-document;
- een rijbewijs.

Let op:

- het identiteitsbewijs mag niet verlopen zijn
- het identiteitsbewijs mag geen kopie zijn
- een studentenkaart, bankpas etc. is geen geldig identiteitsbewijs

Welke gegevens van mij verwerkt SURFsecureID?

SURFsecureID verwerkt een aantal persoonsgegevens van zijn gebruikers. Deze gegevens worden door jouw instelling aangeleverd via SURFconext. De instelling heeft hier toestemming voor gegeven en heeft een verwerkersovereenkomst met SURF.

De volgende persoonsgegevens worden verwerkt:

- Volledige naam
- Email adres
- Instellingsnaam
- Jouw identifier bij de instelling
- De laatste 6 posities van het documentnummer van het identiteitsbewijs

Via https://profile.surfconext.nl/my-services kun je inzien wat de waarde van deze gegevens zijn (behalve de laatste 6 posities van je documentnummer).

Daarnaast wordt je telefoonnummer opgeslagen als je gekozen hebt om SMS te gebruiken als token. In het geval van tiqr wordt een tiqr identifier en het adres om push-berichten naar toe te sturen opgeslagen. In het geval van Yubikey wordt het serienummer van de gebruikte Yubikey opgeslagen.

Diensten die afgeschermd zijn met SURFsecureID kunnen ook persoonsgegevens krijgen om te kunnen functioneren. Deze gegevens worden dan via SURFconext aan die dienst ter beschikking gesteld. Lees hier meer over de soort gegevens en hoe SURFconext daarmee om gaat.

Hoe gaat SURFsecureID om met mijn gegevens?

SURF verwerkt jouw gegevens in opdracht van jouw instelling. Hiertoe heeft SURF met jouw instelling een verwerkersovereenkomst afgesloten in het kader van de AVG.

Alle accountgegevens binnen SURFsecureID worden in Nederland verwerkt. De bewaartermijn voor accounts in SURFsecureID is zevenendertig maanden na laatste inlog. Loggegevens worden 6 maanden bewaard. Het wissen van accountgegevens binnen SURFsecureID is verder mogelijk op verzoek van de instelling of op verzoek van de betrokkene.

Maakt het uit of ik een werk- of privételefoon registreer?

Nee, het maakt niet uit of je een werk- of privételefoon registreert. Eenmalige codes ontvangen via SMS is gratis. Zorg ervoor dat je de bij SURFsecureID geregistreerde telefoon bij je hebt wanneer je gebruik wilt maken van deze dienst. Zonder geregistreerde telefoon is het niet mogelijk om in te loggen.

Kan ik tiqr op twee telefoons gebruiken?

Nee, je kunt je maar eenmaal registreren, dus ook maar eenmaal de tiqr app aan je instellingsaccount koppelen. Tenzij je op de ene telefoon een backup van je tiqr app maakt en die op de andere telefoon zet (voor gevorderden!).

Ik heb een account bij twee (of meer) instellingen. Kan ik hetzelfde token (SMS, tiqr, YubiKey) gebruiken om in te loggen bij applicaties met verschillende accounts?

Ja dat kan. Je kunt het registratieproces doorlopen voor ieder account. Dit is nodig, omdat het token wordt gekoppeld per instellingsaccount.

Kan ik mijn token (SMS, tiqr, YubiKey) delen met anderen?

Nee, je token is privé. Deel deze niet met anderen. Omdat je token is gekoppeld aan je instellingsaccount, en dus persoonlijk is, mogen anderen hiermee niet inloggen. Daarnaast zou de ander ook jouw inloggegevens van het instellingsaccount moeten weten (gebruikersnaam/wachtwoord).

Wat moet ik doen als mijn Activatiecode verlopen is?

De activatiecode die je ontvangt tijdens de registratie van je token (SMS, tiqr, YubiKey) verloopt na 14 dagen. Je kunt deze code daarna niet meer gebruiken om je token bij de Service Desk te laten activeren. Je zult dus eerst je bestaande token registratie moeten verwijderen. Begin daarna opnieuw met een registratie (https://sa.surfsecureid.nl) en rond de activatie van je token bij de Service Desk vervolgens binnen 14 dagen af.

Wat moet ik doen als mijn telefoonnummer verandert?

Alleen als je sms-authenticatie gebruikt moet je wat doen als je telefoonnummer verandert. Gebruik je tiqr of één van de andere methoden dan hoef je dus niets te doen.

Als eerste verwijder je de registratie van je oude telefoonnummer. Vervolgens doorloop je het registratieproces voor je nieuwe nummer/telefoon. Ga hiervoor naar het Registratie Portaal.

Wat moet ik doen als ik een andere telefoon krijg?

Als je hetzelfde nummer behoudt en sms-authenticatie gebruikt, dan hoef je niets te doen. Je kunt je andere telefoon gewoon gebruiken voor sterke authenticatie.

Gebruik je sms-authenticatie en wijzigt je nummer, verwijder dan eerst je oude token op het Registratie Portaal en registreer je dan opnieuw met je nieuwe telefoonnummer. Je moet dan wel weer langs de support desk van je instelling om je toestel te activeren.

Als je tiqr gebruikt, dan kun je proberen om je tiqr account via een backup van je oude telefoon over te zetten naar je nieuwe. **SURF levert hier verder geen support op, daarvoor kun je bij de fabrikant van je telefoon terecht.**

- Voor iOS: dit werkt alleen goed met een backup via iCloud of een encrypted backup met iTunes.
- Voor Android zijn er meerdere mogelijkheden, vaak afhankelijk van de fabrikant van de telefoon. Wij hebben ook niet alles kunnen uittesten, dus mogelijk dat ook andere methoden werken die we hier niet noemen:
    - Gebruik de Google backup functionaliteit. Deze is standaard aanwezig op Android telefoons.
    - Voor Samsung telefoons kun je Samsung Smart Switch gebruiken. De Samsung backup faciliteiten werkt niet en zal je tiqr account niet terug zetten.

Lukt dit niet, verwijder dan eerst je oude token op het Registratie Portaal en installeer vervolgens de tiqr app opnieuw. Registreer je dan op het Registratie Portaal en ga langs de support desk van je instelling om tiqr op je telefoon te activeren.

Wat moet ik doen als ik mijn telefoon of YubiKey heb verloren?

Verwijder de registratie via het Registratie Portaal. Vanaf dat moment kan het token niet meer misbruikt worden. De Service Desk van jouw instelling kan de registratie ook voor je intrekken.

Als je vermoedt dat anderen je telefoon of YubiKey misbruikt hebben om gebruik te maken van diensten die SURFsecureID vereisen, meld dit dan bij de Service Desk van jouw instelling.

Mijn Tiqr account is geblokkeerd. Wat moet ik nu doen?

Je Tiqr account kan geblokkeerd worden. Dit gebeurt als je te vaak achter elkaar een onjuist PIN code hebt opgegeven bij een Tiqr authenticatie. Als je authentiseert met Tiqr krijg je dan op `tiqr.surfconext.nl` de melding "Error - Je account is geblokkeerd". Alle Tiqr accounts in je telefoon zijn dan ook geblokkeerd. Deze blokkade is definitief en kan dus niet ongedaan gemaakt worden. In het SURFsecureID self service portaal is dit niet zichtbaar. Om weer in te kunnen loggen via SURFsecureID met Tiqr moet je opnieuw een Tiqr token registreren. Die doe je als volgt:

1. Ga naar het SURFsecureID self-service portal: https://sa.surfconext.nl
2. Verwijder daar je Tiqr token in het overzicht
3. Nu kun je in het self-service protal een nieuw Tiqr token registreren. Hiervoor volg je weer het registratieproces. Zie hiervoor: Handleiding Registratieportal

Het lukt me niet om de Tiqr QR code te scannen. Wat kan ik doen?

> Update 23 Feb 2021 In release 3.1.0 van Tiqr voor Android hebben we problemen met het scannen van de QR code op Android verholpen. Als je nog problemen heb, controleer dan of je deze release gerbuikt.

Met name Android toestellen hebben soms moeite met het scannen van de QR code. Wat je kunt proberen:

- Beweeg de camera langzaam naar het scherm met de QR code toe en er weer vanaf. Soms heeft de camera moeite met focussen, en het heen en weer bewegen helpt daarbij.
- Scan de QR code met een andere scanner app, dit werkt zowel met de Tiqr QR codes voor registratie (`tiqrenroll://`...) als voor de QR codes voor authenticatie (`tiqrauth://`...). Twee QR scanners apps waarmee we dit getest hebben zijn:
  - de QR & Barcodescanner van Gamma Play. Kies in deze app na het scannen van de QR code voor "Browser openen".
  - de Scanner voor QR- en barcodes van TeaCapps. Kies in deze app na het scannen van de QR code voor "URL openen".
- De camera app kan vaak ook QR codes scannen. Als het om een tiqr QR code gaat, zal je telefoon vragen de tiqr app te openen.

Waar kan ik terecht met supportvragen?

Heb je in deze FAQ niet gevonden waar je naar op zoek was? Als je verdere vragen hebt over het registratie-, vervang- of verwijderproces, of het gebruik van het token (SMS, tiqr, YubiKey) neem dan contact op met de servicedesk van je instelling.

Welk telefoontoestel heb ik nodig voor Tiqr?

Je kunt Tiqr gebruiken op iOS en op Android toestellen. Voor Android is minimaal versie 5.0 (Lollipop) vereist, ofwel SDK 21.

Ik ontvang geen SMS. Wat kan ik doen?

Als SURFsecureID een SMS heeft verstuurd, is deze normaal gesproken een paar seconden later ontvangen door de telefoon. Soms duurt het langer of lijken SMS-berichten helemaal niet aan te komen. SURFsecureID maakt gebruik van een SMS Gateway – een bedrijf dat gespecialiseerd is in het versturen van SMS – dat wereldwijd SMS verstuurt. Als je geen foutmelding krijgt van SURFsecureID dan betekent dat dat de SMS bij de SMS Gateway is afgeleverd.

Hieronder wat je zelf kunt doen als een SMS niet aankomt:

- Controleer of je mobiel bereik hebt, voor het ontvangen van SMS heb je een mobiel netwerk nodig
- Start je telefoon opnieuw op. Je telefoon meldt zich dan opnieuw aan op het mobiele netwerk
- Probeer het later nogmaals, de ervaring leert dat het probleem zich meestal na enige tijd vanzelf oplost
- Log in op het Self-Service portaal (https://sa.surfconext.nl) en gebruik "Test een token" om een SMS te versturen

Blijft het probleem bestaan, neem dan contact op met de ICT servicedesk van je instelling.