Aanvragen SURFsecureID

Het aanvraagproces voor instellingen die gebruik willen maken van SURFsecureID kent een aantal stappen. In overleg met de betrokken instelling kunnen een aantal van deze stappen parallel of in een andere volgorde uitgevoerd worden.

> Weet u nog niet zeker of u wilt aansluiten op SURFsecureID en wilt u eerst meer informatie? Neem dan contact met ons op via support @surfconext.nl.
>
> Wilt u eerst aansluiten op de pilot- of testomgeving, dan geldt een aangepaste procedure.

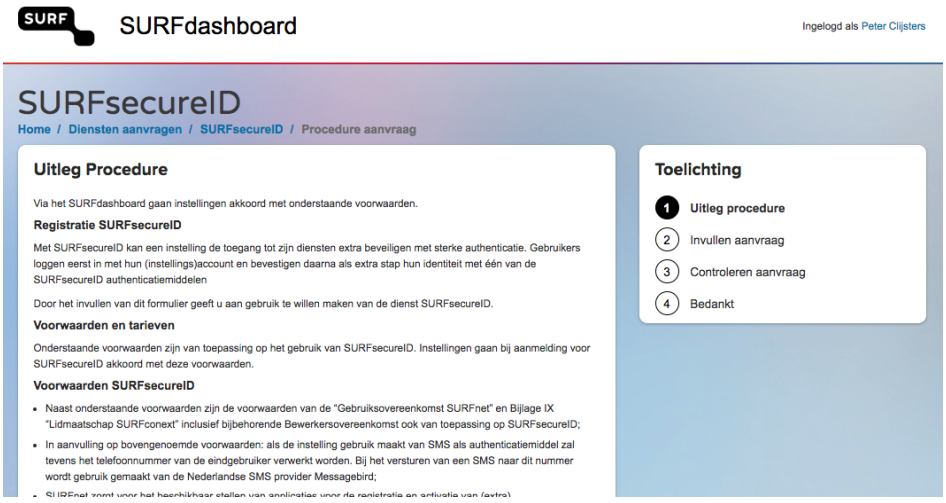
Stap 1 - Instelling aanmelden

Instellingen kunnen SURFsecureID aanvragen via het SURFdashboard. Alleen contactpersonen van de instelling die bij SURFnet bekend zijn als Instellingscontactpersoon (ICP) of Instellingsbevoegde (BVI) kunnen deze aanvraag doen. NB: SURFsecureID is alleen beschikbaar voor instellingen die reeds als Identity Provider zijn aangesloten op SURFconext.

De aanvrager gaat bij aanmelding akkoord met de gestelde voorwaarden en tarieven voor het gebruik van SURFsecureID.

Bij aanmelding geeft de aanvrager aan wie binnen de instelling de primaire contactpersoon wordt voor het in gebruik nemen van SURFsecureID. Het is aan te raden om dit te beleggen bij een medewerker die binnen de instelling nauw betrokken is bij informatiebeveiliging en/ of identity management, en die in staat is nauwe contacten te onderhouden met ondersteunende afdelingen die mogelijk een rol zullen krijgen in het uitgifteproces van authenticatiemiddelen (bijv. IT Helpdesk, Service Desk of HR).

Start de aanvraag door als ICP of BVI naar de SURFsecureID pagina in het SURFdashboard te gaan en daar op de "Aanvragen" knop te drukken.



Stap 2 - Intake

De Productmanager SURFsecureID neemt contact op met de primaire contactpersoon zoals vermeld bij aanmelding. Tijdens een telefonische intake zal de Productmanager o.a. de volgende zaken willen inventariseren:

- Algemeen: per wanneer en voor welke SPs wil de instelling SURFsecureID afnemen, voor welke gebruikers en met welke middelen (SMS, Tiqr, YubiKey)
- Organisatorisch: hoe wil de instelling het uitgifteproces van authenticatiemiddelen organiseren? Welke personen worden verantwoordelijk voor het uitgifteproces, hoe is de support voor eindgebruikers georganiseerd etc. Met wie kunnen we contact opnemen als er onderhoud gepleegd wordt of als er een verstoring is?
- Technisch: welke tokens wil de instelling gaan gebruiken (zie de overwegingen over SMS als token)? RA locaties gebruiken? Ondersteunen van meerdere tokens? Email verificatie in het registratieproces aan of uit?

Daarnaast worden er vervolgafspraken vastgelegd over het ingebruiknemen van SURFsecureID.

Stap 3 - Toegang tot SURFsecureID portals

Om gebruik te kunnen maken van SURFsecureID is toegang tot enkele applicaties nodig. Via het SURFconext Dashboard kan de 'SURFconextverantwoordelijke' van de instelling de onderdelen van SURFsecureID (de Registratieportal, de RA Management portal en de gateway) activeren. De SURFconextverantwoordelijke dient vervolgens akkoord te gaan met de Attribute Release Policies van beide portals:

SURFsecureID onderdeel	Gebruikte attributen

SURFsecureID Registratieportal | SURFnet	`urn:mace:dir:attribute-def:cn`
	`urn:mace:dir:attribute-def:mail`
	`urn:mace:terena.org:attribute-def:schacHomeOrganization`

SURFsecureID RA Management Portal | SURFnet	`urn:mace:dir:attribute-def:cn`
	`urn:mace:dir:attribute-def:mail`
	`urn:mace:terena.org:attribute-def:schacHomeOrganization`

SURFsecureID gateway | SURFnet	-

Na akkoord van de SURFconextverantwoordelijke van de instelling via het SURFconext Dashboard zal SURFconext de toegang tot deze portals activeren.

Stap 4 - Registreren van de RAA

De RAA (Registration Authority Administrator) rol wordt vervuld door één of enkele medewerker(s) van de instelling. Dit gaat om bijvoorbeeld instellingscontactpersonen (ICP's), SURFconext contactpersonen of security officers. Tijdens de entryprocedure wordt de eerste RAA geautoriseerd door een een medewerker van SURFnet. Daarna kan hij of zij andere personen binnen de instelling RA(A) maken.

In deze stap bepaalt de instelling wie de RAA rol krijgt en wordt er met hem of haar een persoonlijke afspraak gemaakt om zijn token te activeren. Zie de RAA handleiding voor meer details.

Stap 5 - Relevante diensten selecteren

Tijdens de intake is reeds besproken voor welke diensten de instelling SURFsecureID wil gaan inzetten. Het is van belang om te weten om wat voor diensten het hier gaat, omdat dit veel uitmaakt voor het vervolgtraject en eventuele doorlooptijd. Een dienst kan SURFsecureID via een van de twee ondersteunde use-cases gebruiken.

Onderstaand overzicht laat zien wat er in welke situatie nodig is om een dienst met SURFsecureID in gebruik te kunnen nemen, met een indicatie van de doorlooptijd die daarmee gemoeid is. Let wel: een en ander is sterk afhankelijk van de medewerking door de betreffende leverancier en de gekozen implementatie. Instelling, SURFnet en de dienstleverancier zullen wanneer zij dit proces ingaan het verwachtingsmanagement goed op elkaar moeten afstemmen.

Startsituatie	Proces	Use-case	Doorlooptijd
1. Dienst is reeds aangesloten op SURFsecureID gateway	Er is alleen een akkoord nodig van de SURFconextverantwoordelijke bij de instelling om deze dienst in gebruik te nemen.	2	Kort. ca. 1-2 werkdagen
2. Dienst is aangesloten op SURFconext, maar nog niet op de SURFsecureID gateway	Er is actie van de dienstleverancier nodig om de dienst technisch aan te sluiten op de SURFsecureID gateway. Contractueel zijn er geen aanpassingen nodig. In onze documentatie voor dienstleveranciers (Service Providers) staat beschreven wat moet gebeuren om aan te sluiten op SURFsecureID Gateway. Hoeveel werk dit is, hangt helemaal af van de gekozen implementatie. Wanneer de dienstleverancier besluit om de dienst aan de 'buitenkant' in zijn geheel met sterke authenticatie af te schermen, dan is dit releatief weinig werk. In feite hoeft de dienst alleen een ander endpoint te configureren. Soms is het echter wenselijk om de sterke authenticatie meer als een step-up authenticatie te laten functioneren. D.w.z. dat sterke authenticatie pas getriggerd wordt wanneer de gebruiker een bepaalde functie in de dienst benadert, bijv. bij alleen het invoeren van tentamencijfers en niet bij het inzien van deze cijfers. Dit vergt meer logica dieper in de dienst en kost daarom ook meer ontwikkeltijd.	2	Gemiddeld. ca. 1-16 weken.

3. Dienst is aangesloten op een centrale authenticatie voorziening van de instelling zoals ADFS, Citrix, BigIP F5.	In deze situatie sluit niet de dienst aan op SURFsecureID, maar is het de centrale authenticatie voorziening die dit doet. Deze voorziening moet zelf de 1e factor (gebruikersnaam/wachtwoord) controleren en roept indien nodig SURFsecureID aan voor de 2e factor. Zo kan de instelling tweefactorauthenticatie aan- of uitzetten voor verschillende diensten en groepen gebruikers met 1 koppeling tussen de centrale voorziening en SURFsecureID. Voor een aantal centrale authenticatie voorzieningen bestaan kant-en-klare oplossingen die snel te implementeren zijn: • Voor MS ADFS heeft SURFnet een plugin ontwikkeld die eenvoudig geinstalleerd en geconfigureerd kan worden. • Voor Citrix Netscaler vanaf firmware versie 12 (nog niet getest). Voor eerder versies kan met een proxy worden gewerkt. • Voor BigIP F5 zijn custom rules beschikbaar (hier) Andere authenticatie voorzieningen die op deze manier SURFsecureID willen inzetten zullen zelf de SFO koppeling moeten realiseren. Dit kost meer ontwikkeltijd. Als de centrale authenticatie voorziening van een instelling is zijn er contractueel geen aanpassingen nodig. Mocht een dienstleverancier deze methode gebruiken, dan zal eerst het reguliere aansluitproces voor Service Providers doorlopen moeten worden.	1	Gemiddeld. ca. 1-16 weken.
4. Dienst is niet aangesloten op SURFconext, SURFsecureID of via een centrale authenticatie voorziening	Samen met de instelling zal de dienstleverancier eerst moeten bepalen hoe zijn dienst gekoppeld kan worden aan SURFsecureID. Dit kan via een van de twee ondersteunde use-cases; direct aan SURFsecureID (zie scenario 2 hierboven) of via een centrale authenticatie voorziening (zie scenario 3 hierboven). Indien de dienst direct op SURFsecureID aansluit zal eerst het reguliere aansluitproces voor Service Providers doorlopen moeten worden om aan te sluiten op SURFconext. Dit aansluitproces bestaat uit een technische en organisatorische component. Aanvullend dient ook nog een koppeling met de SURFsecureID gateway gemaakt te worden. Hierbij geldt ook weer: de hoeveelheid werk die hiermee gemoeid is, hangt helemaal af van de gekozen implementatie.	1 of 2	Langer. ca. 4-24 weken

Stap 6 - Testen

Zodra de relevante dienst beschikbaar is via de SURFsecureID gateway kan de instelling in samenwerking met SURFconext en de dienstleverancier een functionele test uitvoeren om vast te stellen dat Sterke Authenticatie via SURFconext werkt. Tijdens een finale check tussen instelling, SURFnet en dienstleverancier wordt een go/ no go beslissing genomen voor het in gebruik nemen van de koppeling met SURFsecureID. De koppeling wordt dan overgeheveld naar onze productieomgeving en is daarna klaar voor gebruik.

Stap 7 - Operationaliseren binnen instelling

Wanneer de door u gewenste dienst beschikbaar is via de SURFsecureID gateway en deze naar tevredenheid getest is, kunt u verder met de uitrol van SURFsecureID binnen uw instelling. We denken hierover graag met u mee. Aandachtspunten waar u als instelling in ieder geval aan moet denken zijn onder andere:

- Opstellen beleid voor sterke authenticatie. Voor welke diensten en welke gebruikers is dat wel/ niet wenselijk?
- Inrichten uitgifteproces
- Inrichten supportorganisatie
- Bestellen YubiKey tokens (indien van toepassing)
- Planning: in welk tempo gaan welke gebruikers gebruik maken van SURFsecureID.
- Communicatie richting gebruikers en stakeholders, zowel bij lancering als in exploitatiefase.

Stap 8 - Klaar voor gebruik

Zodra de techniek en organisatorische kant voor uitrol van de dienst geregeld is, kan de instelling gebruikers uitnodigen om een tokenregistratie te starten en deze te laten activeren. Na activatie van hun token kunnen gebruikers via SURFsecureID inloggen bij online diensten waarvoor sterke authenticatie ingeregeld is. Natuurlijk kan de tokenregistratie van gebruikers eerder starten dan dat de dienst in productie is, dit is voor sommige diensten zelfs noodzakelijk om gebruikers toegang te kunnen geven.

Wanneer de instelling op een later tijdstip ook andere diensten via SURFsecureID wil gaan gebruiken, dan kan de instelling dat kenbaar maken via support@surfconext.nl. In overleg worden stap 4 en 5 uit dit stappenplan dan nogmaals doorlopen.

SURFnet zal tevens de facturatie voor het gebruik van SURFsecureID starten vanaf de maand na in productiename.