

Registratie- en activatieproces

Het proces waarin een fysieke persoon gelinkt wordt aan zijn digitale identiteit en zijn authenticatiemiddel is cruciaal om misbruik en identiteitsfraude tegen te gaan. SURFsecureID is daarom zo ontworpen dat een token met zekerheid gekoppeld kan worden aan de identiteit van de juiste gebruiker. Daarnaast ondersteunt SURFsecureID token zelfregistratie waarbij gebruikersgemak en eenvoud voorop staat.

- [Betrouwbaarheidsniveau en registratie- en activatieproces](#)
- [Gebruiker registreert token](#)
- [Activatie van het token](#)
 - [1. Zelf activatie](#)
 - [2. Activatie door de servicedesk](#)
 - [3. Activatie met bestaand token](#)
- [Gebruiker laten kiezen tussen activatie methodes](#)
- [Meer informatie](#)

Betrouwbaarheidsniveau en registratie- en activatieproces

Voordat een gebruiker een token kan gebruiken moet deze het token registreren en moet het token geactiveerd worden:

- Registreren: de gebruiker kiest een token uit de set van tokens die zijn instelling heeft bepaald
- Activeren: na het registreren moet het token nog geactiveerd worden. Dit kan door:
 - de gebruiker zelf gedaan worden en gebeurt dan direct na het registreren van het token.
 - de servicedesk van zijn instelling gedaan worden. De gebruiker gaat naar de servicedesk van de instelling waar zijn identiteit wordt gecontroleerd en het token wordt geactiveerd. Het proces waarin een fysieke persoon gelinkt wordt aan zijn digitale identiteit en zijn authenticatiemiddel is cruciaal om misbruik en identiteitsfraude tegen te gaan

Afhankelijk van de gebruikte activatie methode en het token type heeft het token een bepaald [betrouwbaarheidsniveau \(level of assurance, LoA\)](#).

Betrouwbaarheidsniveau	Token type	Activatiemethode
LoA 1.5	alle token types	gebruiker
LoA 2	tiqr, AzureMFA, SMS	servicedesk of gebruiker met bestaand token
LoA 3	Yubikey, FIDO2	servicedesk of gebruiker met bestaand token



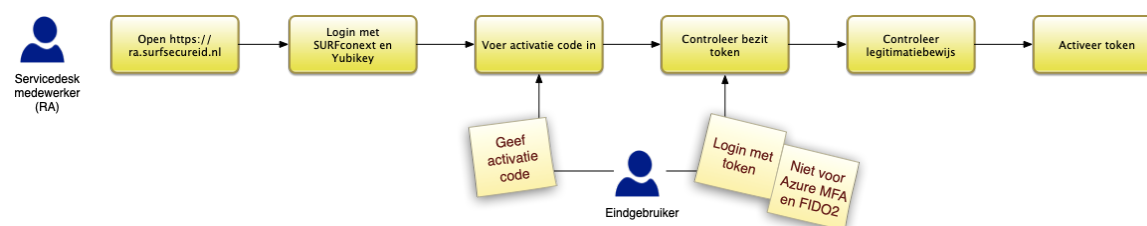
Als een instelling SURFsecureID afneemt dan heeft deze de keuze om LoA 1.5 wel of niet te ondersteunen. Daarnaast heeft de instelling nog de keuze om activatie met een bestaand token toe te staan. [Deze en andere configuratie opties](#) worden besproken bij de intake of kunnen later aangezet worden.

Gebruiker registreert token

Allereerst logt de gebruiker in op het [Registratieportal](#) met zijn instellingsaccount (username/password) via SURFconext. In dit registratieportal selecteert de gebruiker zijn gewenste token, bewijst hij met een authenticatie dat hij controle heeft over het token en verifieert hij zijn email adres (optioneel, een instelling kan ervoor kiezen de email verificatie uit te laten zetten). Het token moet vervolgens geactiveerd worden. Dit kan op drie manieren die uiteindelijk het LoA van het token bepaalt, zie daarvoor de volgende stap.

2. Activatie door de servicedesk

De activatie door de servicedesk van de instelling is altijd beschikbaar als optie. De gebruiker heeft een activatie code gekregen en gaat daarmee langs bij de servicedesk om zijn token te laten activeren door een geautoriseerde medewerker (RA). De RA logt middels sterke authenticatie in bij de [RA Managementportal](#). Daar zoekt de RA de tokenregistratie van de gebruiker op in het systeem op basis van de activatiecode die de gebruiker mee brengt. Voor SMS, Yubikey en tiqr moet de gebruiker het bezit van dit token aantonen. Na een succesvolle ID-controle, wordt het token voor de gebruiker geactiveerd. De tiqr, AzureMFA en SMS tokens hebben dan LoA2, de Yubikey en FIDO2 tokens hebben dan LoA3.



3. Activatie met bestaand token

Als de gebruiker al een ander token had, krijgt hij de mogelijkheid om hiermee zijn nieuwe token te activeren. Voorwaarde is dat het bestaande token waarmee geactiveerd wordt van voldoende niveau is; een [LoA](#) groter of gelijk aan het nieuwe token. Zo kan een FIDO2 token wel met een Yubikey geactiveerd worden, maar niet met een tiqr token. Deze activatie methode is optioneel en moet voor een instelling aan staan. Voorwaarde is wel dat de instelling meerdere tokens per gebruiker aan heeft staan, of dit tegelijk aan laat zetten.

Gebruiker laten kiezen tussen activatie methodes

Vooral in het geval een instelling zelf activatie toestaat kan het nuttig zijn om de gebruiker naar een specifieke activatie methode te sturen. Hiervoor zijn twee mogelijkheden:

- Op de pagina waar de gebruiker een keuze moet maken tussen de activatie methodes kan een [hulptekst](#) getoond worden die de gebruiker begeleidt in zijn keuze. De RAA van de instelling kan deze tekst zelf aanmaken en aanpassen in het [RA portaal](#) in de tab "Activatie hulpteksten".
- De instelling kan specifieke URL's voor het registratieportaal gebruiken in zijn communicatie met gebruikers. De URL zorgt er dan voor dat de gebruiker maar één van de methodes te zien krijgt.
 - URL voor activatie door de servicedesk: <https://sa.surfconext.nl/?activate=ra>
 - URL voor zelf activatie: <https://sa.surfconext.nl/?activate=self>

Meer informatie

Op de volgende pagina's vindt u meer info over de inrichting van registratieproces.

- [RA-rollen toewijzen](#)
- [Handleiding RA Management portal](#)
- [Handleiding RA-admin](#)
- [Aandachtspunten voor RA](#)
- [Noodprocedure registratieproces](#)