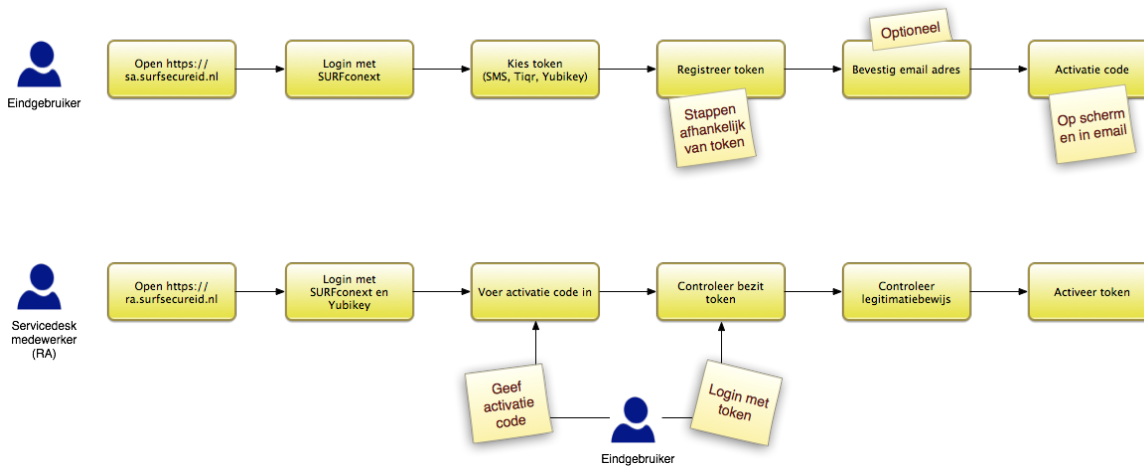


Inrichten registratieproces

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 wordt aan de identiteit van de juiste gebruiker.



Het registratieproces van tokens (SMS, Tigr, YubiKey) is op hoofdlijnen als volgt opgezet:

1. Allereerst logt de gebruiker in op een Registratieportal met zijn instellingsaccount (username/password). In deze registratieportal selecteert de gebruiker zijn gewenste token (SMS, tigr of YubiKey), bewijst hij via e-mailverificatie dat hij inderdaad de geauthenticeerde gebruiker is die deze aanvraag doet en bewijst hij met een authenticatie dat hij controle heeft over het token. De gebruiker ontvangt daarna een activatiecode per e-mail.
2. Vervolgens gaat de gebruiker fysiek langs bij een Service Desk 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. Na een succesvolle authenticatie met het aangevraagde token door de gebruiker en een succesvolle ID-controle, wordt het token voor de gebruiker geactiveerd.

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](#)
- [Manual RA Management portal](#)