Aandachtspunten voor RA

Er zijn een aantal aandachtspunten waar een instelling bij het inrichten van het registratieproces rekening mee moet houden:

Geldige legitimatiebewijzen

De volgende documenten gelden als geldig legitimatiebewijs:

- Paspoort
- Rijbewijs
- Identiteitskaart

NB: een collegekaart, bankpas of OV-jaarkaart zijn dus GEEN geldig legitimatiebewijs.
Breek de token-activatie af wanneer gebruikers met een dergelijk bewijs proberen hun authenticatiemiddel te activeren en voltooi deze pas wanneer de gebruiker terug keert met een geldig legitimatiebewijs zoals hierboven beschreven.

Controle legitimatiebewijs gebruiker

Controleer:

- Of de gebruiker lijkt op de foto op het legitimatiebewijs
- Of het legitimatiebewijs nog geldig is
- Of gegevens op het scherm overeen komen met hetgeen je in het legitimatiebewijs ziet

Vul laatste 6 karakters van documentnummer in (ivm evt. controle achteraf)
Zijn de gegevens **correct**? Vink dan het hokje 'Ik heb de identiteit van de gebruiker geverifieerd' aan en klik op 'Verifieer identiteit'
Zijn de gegevens **niet correct**? Of **twijfel** je over de geldigheid van het legitimatiebewijs? Breek dan de registratie af en neem contact op met je RA admin.

Tokenregistraties intrekken

Elke instelling dient processen in te richten voor het intrekken (=revocatie) van verloren, gestolen of gecompromitteerde SURFsecureID tokens. Revocatie zou bij voorkeur binnen 72 uur na het betreffende incident plaats te vinden, om het risico op misbruik van tokens te minimaliseren.

Het revocatieproces kan gestart worden door:

Gebruiker	De gebruiker kan inloggen met zijn instellingsaccount (i.e. username/password) op de SURFsecureID Registratieportal om de koppeling tussen zijn instellingsaccount en zijn token (SMS, Tiqr, YubiKey) te verwijderen. SURFsecureID logt deze actie.
RA (A)	De RA(A) van een instelling mag de binding tussen het instellingsaccount van de gebruiker en zijn token (SMS, Tiqr, YubiKey) verwijderen wanneer er vermoedens zijn van misbruik. De gebruiker zal een notificatie van deze actie per mail krijgen, en SURFconext Sterke Authenticatie logt deze actie. De RA mag de binding tussen het instellingsaccount van de gebruiker en zijn token (SMS, Tiqr, YubiKey) ook verwijderen als de gebruiker niet langer staat ingeschreven bij de instelling. De gebruiker zal een notificatie van deze actie per mail krijgen, en SURFsecureID logt deze actie.

SURFnet	SURFnet is geauthoriseerd om een token te verwijderen wanneer het gecompromitteerd is. SURFnet zal deze extreme maatregel alleen nemen in overleg met de RAA van de instelling. De gebruiker zal een notificatie van deze actie per mail krijgen, en SURFsecureID logt deze actie.

Gebruik SMS niet voor password reset

Sommige instellingen gebruiken SMS ook als middel voor gebruikers om een password reset te doen. Gebruikers die een password reset aanvragen, bijv. via een self-service portal, ontvangen dan via SMS een nieuw wachtwoord. Een dergelijk scenario verlaagt echter de security SMS als tweede factor tot slechts een enkele factor.

SMS mag daarom **nooit** gebruikt worden voor password reset, wanneer SMS ook als authenticatiemiddel voor sterke authenticatie wordt ingezet.

Schakel SMS niet door naar e-mail

Zorg dat je instelling SMS-jes niet doorstuurt naar een e-mail adres, wanneer je SMS als authenticatiemiddel voor sterke authenticatie inzet. Een dergelijk scenario verlaagt echter de security SMS als tweede factor tot slechts een enkele factor.