# 2 Factor Authentication

Kan op verschillende manieren, maar allereerst de meest gangbare manier:

* Gebruiker logt in met **username**/**email** & **password**
* Gebruiker krijgt een code opgestuurd via

**Email** - iedereen heeft email en weet hoe je dit gebruikt

**SMS** – iedereen heeft sms en weet hoe je dit gebruikt, maar deze optie gaat 100% geld kosten en moet via een externe partij

**2FA app** – Kan een stap te veel zijn voor sommige gebruikers

# Registratie meetstation

Via een admin portaal kan Miriam gebruikers

1. Ter plekke aan hun meetstation koppelen, TIJDENS de workshop
2. Uitnodigen om registratie van hun meetstation te voltooien, NA de workshop

Hierin wordt doorlopen:

* 1. Het koppelen van email aan meetstationID
  2. Het instellen van de privacyvoorkeur

# Ophangen meetstation

Instructies hiervoor worden getoond op:

1. De website, onder kopje ‘meetstation installeren’
2. Tijdens registratie van het meetstation
3. Na de eerste keer inloggen met je account

# Voorstel implementatie

## Backend

In de backend is er al een keer een start gemaakt aan het implementeren van JWT voor het authenticeren van gebruikers. Op dit moment is deze functionaliteit niet werkend, maar zijn de benodigde packages waaronder Spring security en jjwt in de pomfile gedefineerd. Het wordt aangeraden om de JWT te gebruiken en implementeren. JWT zijn stateless en hoeven dus niet opgeslagen te worden in een database wat dus extra database operaties en processes vermijd. Daarnaast zijn de tokens ook self-expiring wat betekent dat ze er een bepaalde levensduur aan meegegeven wordt.