**Verschillende soorten inlog methodes:**

* Email en wachtwoord
* Gebruikersnaam en wachtwoord
* Email en bevestigingslink
* Sociale media-account
* Biometrische methode: vingerscan, gezichts- & stemherkenning
* Authenticatie apps (google, Microsoft)
* Via QR-code scannen en bevestiging geven

Voor OntdekStation013 is er een inlogsysteem nodig waarbij de gebruiker in kan loggen bij een persoonlijk account. Dit is nodig omdat er een koppeling moet kunnen worden gemaakt tussen de gebruiker en het desbetreffende meetstation.

Hierbij is het belangrijk dat er bij de keuze voor een methode rekening wordt gehouden met de doelgroep van de applicatie. De doelgroep is namelijk erg breed en het systeem moet dus makkelijk te begrijpen zijn voor iedereen. Hierdoor vallen bijvoorbeeld de opties: Sociale media-account, Authenticatie apps en QR-code al af. Dit omdat dit mogelijk als lastig kan worden ervaren door de jongere en/of oudere gebruikers van het systeem, maar ook kan het zijn dat hiervoor een smartphone of account nodig is en hier bij deze selectie van de doelgroep mogelijk een gebrek aan is.

Ook valt de optie biometrische inlogmethode eigenlijk al af. Hierbij als reden dat het apparaat waar mee ingelogd wordt dan aan speciale eisen moet voldoen, bijvoorbeeld dat deze in bezit moet zijn van een functie dat deze vingers moet kunnen scannen.

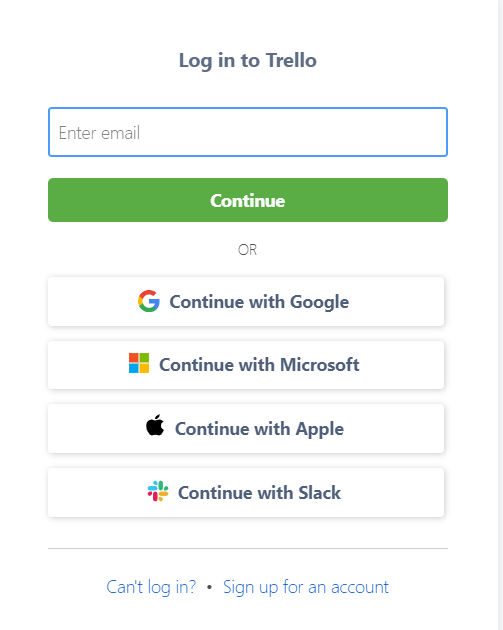
Hierna blijven de opties: Email/gebruikersnaam en wachtwoord en email met bevestigingslink over. Als we met de laatste optie beginnen: email met bevestigingslink, dan is dat de methode die op dit moment gebruikt wordt. Hierbij wordt er voornamelijk tegen het feit aangelopen dat het niet een optimale manier is, doordat er nogal veel mouse clicks voor nodig zijn en je ook nog bij je mail moet inloggen. Daarbij ontvang je elke keer een mail als je wilt inloggen. Wel is het fijne eraan dat je geen wachtwoord nodig hebt en het is twee-stap verificatie.

Bij de optie email/gebruikersnaam met wachtwoord zijn er een aantal voor- en nadelen op te noemen. De voordelen zijn dat eigenlijk iedereen uit de doelgroep wel bekend is met zo’n dergelijke methode, simpelweg omdat veel andere systemen, zoals bijvoorbeeld de grootste sociale media Facebook bestaan met zo’n inlogsysteem. Ook dat er relatief makkelijk een twee-stap verificatie van gemaakt kan worden, door bijvoorbeeld een mail of SMS te sturen. Als we voor deze methode zouden kiezen, dan staat het email adres als ‘gebruikersnaam’ wel voor de mogelijkheid van gebruikersnaam. Dit omdat wij voor de meetstations toch al een email nodig hebben en als we zouden kiezen voor een gebruikersnaam dan meer ‘persoonlijke’ data zouden moeten opslaan terwijl dit niet nodig is. Toch is een gebruikersnaam wel veiliger omdat er dan toch meer anonimiteit is.

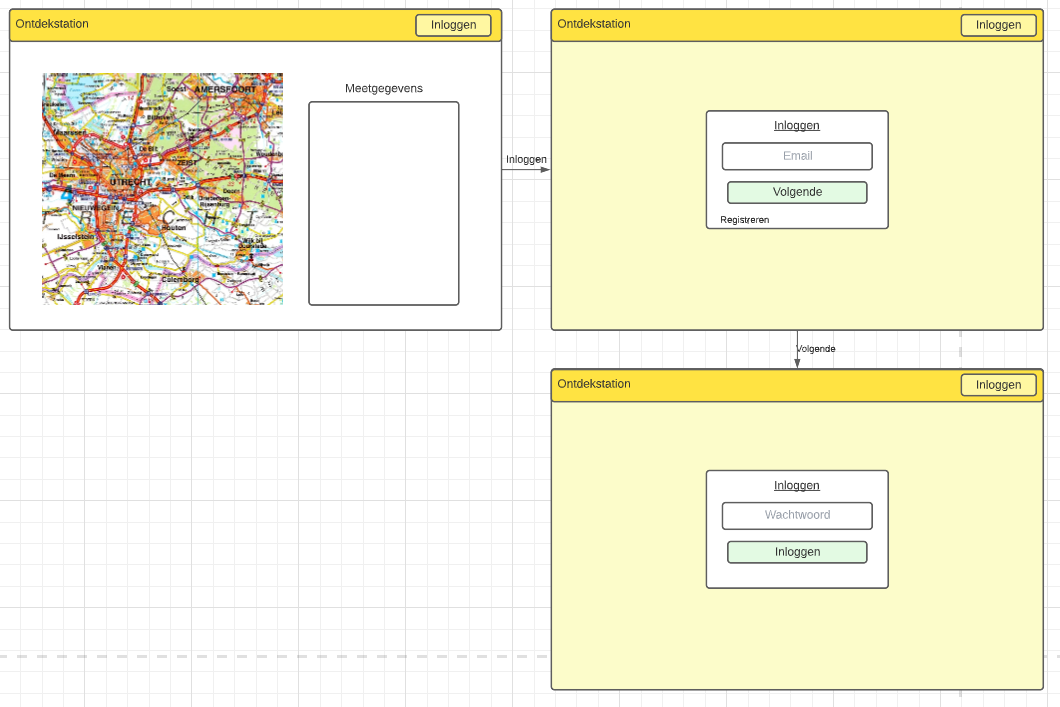
De nadelen zijn dat de wachtwoorden die mensen hebben vaak niet ‘veilig’ zijn en dat ze meestal dezelfde wachtwoorden gebruiken. Ook dat als je wilt voldoen aan twee-stap verificatie dat je dan weer zit met de ‘onhandigheid’ van elke keer een mail ontvangen of we zouden onnodig persoonlijke data opslaan met het telefoonnummer voor een SMS.

Hieruit kan je opmaken dat de keuze vooral ligt tussen het gebruik van een email of gebruikersnaam met wachtwoord en de keuze om er dan nog twee-stap verificatie aan toe te voegen.

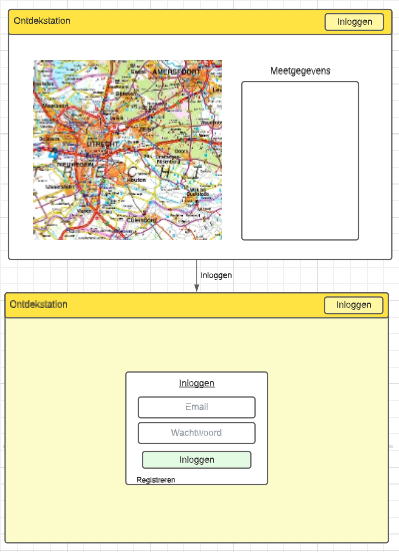
Ook kan je er nog voor kiezen om hier een combinatie van te maken. Bijvoorbeeld dat je kan kiezen om ‘normaal’ in te loggen met een email en wachtwoord, maar er ook een keuzemogelijkheid is om met facebook of Gmail in te loggen.

Je ziet hier dat je ook de keuze hebt om met andere systemen in te loggen. Met betrekking tot de doelgroep waarbij onderzoek gaan doen. Is het waarschijnlijk het nuttigst om in te loggen met Facebook, omdat 40 procent tussen de 40 en 64 jaar is. Verder zou LinkedIn ook een mogelijkheid kunnen zijn om mee in te loggen, omdat hier maar liefst 50 procent tussen de 40 en 64 jaar is. Hierbij moet je wel rekeninghouden met het feit dat dit niet open source is. Er zijn wel alternatieven die wel open source zijn, zoals OAuth. Dit staat voor Open Authorisation, dit is een manier voor gebruikers om in te loggen bij applicaties via andere websites zonder dat ze hun wachtwoord opgeven. Voorbeelden van gebruikers hiervan zijn, Google, Facebook en Microsoft.

In dit voorbeeld zie je ook dat je eerst alleen je email in moet vullen en bij de volgende stap pas je wachtwoord. Dit zou voor ons ook een goede optie zijn, agz het dan heel duidelijk is wat je moet doen.



Verder is het nog discutabel om gebruik te maken van verschillende stappen of van inloggen in 1 stap. Hiervoor is namelijk een best belangrijke reden voor. Dat als je de verificatie met meerdere stappen doet, en bijvoorbeeld in stap 1 al controleert of het email adres bestaat, dat dit voor hackers het ‘makkelijker’ maakt en het dus een stuk minder veilig maakt. Hierbij moet dus de afweging tussen veiligheid en gebruiksvriendelijkheid worden gemaakt.



Salting en hashing

[What is password salting and why you need it - IPVanish](https://www.ipvanish.com/blog/password-salting/#:~:text=Hashing%20is%20a%20term%20from%20cryptography%20that%20essentially,hackers%20to%20discover%20and%20exploit%20during%20a%20breach.)

[Facebook gebruikers: Wie zitten er op Facebook? - CommunicatieVogel.com](https://www.communicatievogel.com/facebook-gebruikers-wie-zitten-er-op-facebook/#:~:text=Leeftijd%3A%20Volgens%20Facebook%20zitten%20mensen%20van%20tussen%20de,ouder%20of%20jonger%20dan%2064%20of%2025%20jaar.)

[Inloggen: veilig, makkelijk en flexibel – Software Assist (software-assist.nl)](https://www.software-assist.nl/veilig-makkelijk-flexibel-inloggen/)

[Leeftijd Social Media gebruikers Nederland ⋆ iDees online](https://www.ideesonline.nl/leeftijd-social-media-gebruikers-nederland/)