INF2C – groep 3

**Projectleden**

Tedjan Hulshof

Dennis Hartmann

Justin Bakker

Roy Heidotting

Melvin Bos

Tim Wennekes



**Hoe vindt de NFC verbinding met de tablet plaats?**

Inhoud

[Methode 3](#_Toc346192169)

[Hoe vindt de NFC verbinding met de tablet plaats? 4](#_Toc346192170)

[Veiligheid 4](#_Toc346192171)

[Literatuurlijst 5](#_Toc346192172)

# Methode

Voor dit onderzoek is gebruik gemaakt van literatuuronderzoek.

# Hoe vindt de NFC verbinding met de tablet plaats?

NFC staat voor Near Field Communication. Dit principe maakt het mogelijk om op korte afstand data data te lezen van of te schrijven naar een chip die geen elektriciteit nodig heeft. Deze methode wordt al breed ingezet in verschillende markten. Enkele voorbeelden zijn de Nederlandse ID-kaart, OV-chipkaart en toegangspasjes bij grotere bedrijven.

Om de tablet de mogelijkheid te geven om elke sensor die geregistreerd moet worden te herkennen is het mogelijk de modules te voorzien van RFID (Radio Frequentie Identification) tags. Deze tags kunnen een kleine hoeveelheid informatie bevatten die draadloos kan worden uitgelezen.

Deze RFID tags zijn een goedkope en gebruikersvriendelijke manier om elke module een soort serienummer te kunnen geven. Hiermee kan bijvoorbeeld een tablet- of smartphone applicatie automatisch de modules herkennen en aan de server registreren.

Android heeft voor NFC een library die het mogelijk maakt om gemakkelijk deze informatie te lezen en verwerken binnen een applicatie. Android werkt met de zogenaamde midfare RFID tags. Deze tags sturen informatie via radiogolven op een frequentie van 13.56MHz.

## Veiligheid

De tags zijn voor elk apparaat die er langs gaat leesbaar. Echter zijn er verschillen manieren om de tags te beveiligen. Zo is het mogelijk om de data op de chip te voorzien van een encryptie-sleutel. Hiermee is de informatie wel leesbaar, maar een mens nog computer zonder sleutel de informatie lezen.

Om tags te beveiligen tegen overschrijven kan een tag voorzien worden van een alleen lezen functie. Dit maakt het voor andere apparaten onmogelijk om de informatie te bewerken die op de chip staat.

Het project Social Greenhouse verwacht geen hoge beveiligingseisen voor de informatie die op de chip staat. Dit is omdat de enige informatie op de chip een unieke sleutel is die naar de sensor verwijst.

# Literatuurlijst

Android. (sd). *Android Developers*. Opgeroepen op Januari 2013, van Android Developers: http://developer.android.com/reference/android/nfc/package-summary.html

DealExtreme. (sd). *13.56Mhz*. Opgeroepen op Januari 2013, van DealExtreme: http://dx.com/s/13.56MHz

Wikipedia. (sd). *Radio frequency identification*. Opgeroepen op Januari 2013, van Wikipedia: http://nl.wikipedia.org/wiki/Radio\_frequency\_identification