Hoe koppelen we de IHM aan een schip?

AfstudeerStage

February 19, 2024

Joris Elfferich

HOGESCHOOL ROTTERDAM

Technische Informatica

Contents

[Inleiding 2](#_Toc159416501)

[Hoe voeren we de authenticatie van het personeel uit? 2](#_Toc159416502)

[Opties: 2](#_Toc159416503)

[Smart Cards (RFID & NFC): 2](#_Toc159416504)

[Biometrische scanners 2](#_Toc159416505)

[Wachtwoord 3](#_Toc159416506)

[Hardware security modules 3](#_Toc159416507)

[Bluetooth 3](#_Toc159416508)

[Two-factor Authentication 3](#_Toc159416509)

[Mobiele telefoon app 4](#_Toc159416510)

[Conclusie: 4](#_Toc159416511)

[Hoe verbinden we de module met de blockchainserver? 5](#_Toc159416512)

[Satelliet: 5](#_Toc159416513)

[Mobiele datanetwerken: 5](#_Toc159416514)

[LoRaWAN: 5](#_Toc159416515)

[Conclusie: 5](#_Toc159416516)

[Hoe gaat dit systeem er technisch uit zien? 6](#_Toc159416517)

[Microcontroller 6](#_Toc159416518)

[Architectuur 6](#_Toc159416519)

[Bronnen 7](#_Toc159416520)

[Changelog 7](#_Toc159416521)

# Inleiding

De “EU Ship Recycling Regulation” is op 31 december 2020 in gegaan en is van toepassing op elk schip van 500 GT (Gross tonnage) of meer dat een EU-haven of ankerplaats aandoet (ongeacht de vlag). Schepen moeten een geldige en gecertificeerde Inventory of Hazardous Materials (IHM) aan boord hebben) [1]. De IHM is een gedetailleerd document dat een overzicht biedt van alle gevaarlijke materialen die aan boord van het schip aanwezig zijn. Het digitaliseren de IHM is belangrijk omdat we de IHM beter kunnen beveiligen. Zo kan dit document minder goed worden vervalst of aangepast, Het IHM zal dus worden gedigitaliseerd maar het moet wel gekoppeld worden aan een schip. Er zou een apparaat moeten worden geïnstalleerd dat door personeel met de juiste autorisatie kan worden bekeken voor de status van de IHM en de laatste aanpassingen. Nu komen hier een paar belangrijke vraagstukken bij kijken.   
Hoe voeren we de authenticatie van het personeel uit?   
Hoe verbinden we de module met de blockchainserver?  
Hoe gaat dit systeem er technisch uit zien?

# Hoe voeren we de authenticatie van het personeel uit?

Hoe weet de module welke personen wel of niet toegang krijgen? Aangezien deze module fysiek is zijn er vele mogelijkheden voor deze authenticatie. Het moet niet te ingewikkeld en onhandig zijn voor de gebruiker, maar nog steeds veilig. Hieronder staan wat mogelijke oplossingen.

## Smart Cards (RFID & NFC):

Een smart cards is een fysieke kaart met een ingebouwde chip die werkt als een beveiligingstoken [2]. Deze zijn dezelfde grootte als een creditcard of rijbewijs. Deze kaarten kunnen fysiek contact gebruiken voor een verbinding maar tegenwoordig wordt vaker een draadloze verbinding gebruikt. Deze draadloze verbinding kan RFID (Radio Field Identification) of NFC (Near-field communication) gebruiken. Wat is het verschil tussen RFID en NFC?  
  
De twee grootste verschillen zijn[3]:  
- NFC bevat bidirectional communication (informatie wordt heen en terug gestuurd), RFID is unidirectional (informatie wordt alleen ontvangen, niet verstuurd)  
- NFC is voor kleine afstanden ontworpen terwijl RFID tot meters afstand gebruikt kan worden.

Tegenwoordig zijn NFC chips ook een stuk goedkoper dan RFID, en NFC past in dit geval een stuk beter bij onze use-case. RFID wordt vaak gebruikt voor het nagaan van informatie, zoals het volgen van een pakketje, producten in een inventaris en in honden of katten om de eigenaar terug te vinden. Terwijl NFC vaak wordt gebruikt voor contactloos betalen, informatie versturen en je kan de NFC tags niet alleen makkelijk lezen maar ook overschrijven dankzij de bidirectional communicatie.

## Biometrische scanners

Biometrische scanners zijn gefocust op het identificeren van personen via biologische kernmerken, zoals gezichten, vingerafdrukken, DNA of iris patronen [4]. Deze biometrische scanner zijn zeker een van de meest veilige oplossingen maar ook ingewikkeld voor de uitvoering. Van de gegeven voorbeelden is een vingerafdruk scanner het goedkoopst, maar hoe koppel je de vingerafdruk van een persoon aan een autoriteit niveau? Je zou een database moeten opstellen met de vingerafdrukken van de gemachtigde personen. Dit gaat best een gedoe zijn om de vingerafdrukken te bemachtigen en allemaal op te slaan in de database. Dit zou ook betekenen dat er een globale database zou moeten ontstaan opgeslagen in de Cloud die gebruikt kan worden door meerdere schepen. Hierbij komen weer veiligheid risico’s kijken, maar ook privacy risico’s. Het zou kunnen voortkomen dat niet iedereen het fijn vindt om zijn vingerafdruk in een grote database te zetten die niet van de overheid is. Vrijwel het enige pluspunt aan deze oplossing is de veiligheid. Je weet altijd precies wie de aanpassingen heeft gemaakt in de IHM en echt alleen de juiste personen hebben toegang.

## Wachtwoord

Een wachtwoord is een simpele oplossing waar wel wat problemen bij komen kijken. Waarschijnlijk zou voor de module een wachtwoord worden gebruikt, en als deze gelekt wordt kan iedereen bij de module. Je kan een dagelijks wachtwoord gebruiken, dat elke dag zichzelf verandert. Dan zou je wel dit wachtwoord ergens vandaag moeten halen, dit kan het personeel onhandig vinden. Want als ze vergeten waar ze het wachtwoord terug kunnen vinden is toegang niet meer mogelijk. Een one-time use password is mogelijk. De gebruiker zou dit wachtwoord van tevoren bemachtigen en na gebruik zou dit wachtwoord niet meer werken voor het inloggen op de module.

## Hardware security modules

Een HSM (hardware security module) is een beveiligd hardwarecomponent die wordt gebruikt om crypto grafische sleutels te beschermen en op te slaan [5]. Alleen geautoriseerde gebruikers hebben nog toegang tot de sleutels. Zo kun je de toegang controleren en beschermen van de privé sleutels. De HSM kan gebruiker invoer ontvangen en hiervoor een uitkomst terug geven, zoals het ophalen van de IHM. Maar de keys kunnen niet worden ge-exporteerd, of verwijderd van de HSM. Een hele veilige oplossing, maar valt het binnen onze use-case. Een HSM kan vrij duur zijn en het systeem erg complex maken. Je hebt gespecialiseerde kennis nodig voor het beheren en onderhouden van de HSM, en dit integreren met blockchain moet zorgvuldig worden uitgevoerd. En dan moet je ook nog een sterk authenticatie methode hebben voor de administrators wat de HSM niet helemaal behandeld. En aangezien authenticatie een van de belangrijke punten is, zou dit gecombineerd kunnen worden met een andere hardware authenticatie, wat voor een over complex systeem kan zorgen.

## Bluetooth

Bluetooth is een draadloze communicatietechnologie wat lijkt op Wifi. Het maakt een PAN (personal area netwerk), binnen dit 10m netwerk kan het communiceren met meerde apparaten [6]. Bluetooth vereist minder energie en is goedkoper dan Wifi, wel is de grootte en snelheid van het netwerk minder dan Wifi. Veel apparaten zoals laptops en telefoons hebben al een bluetooth radio. Als deze niet aanwezig is kan je vrij makkelijk een bluetooth adapter aan het apparaat koppelen. Voordat data kan worden verstuurd tussen bluetooth apparaten moeten ze eerst met elkaar koppelen. Nadat een koppeling is gemaakt kan de data veilig worden verstuurd. Hoe zou dit gebruikt kunnen worden voor de use case? Voor de IHM-module die op het schip wordt geplaatst zou alleen toegang gegeven worden voor personeel dat via hun telefoon verbindt met de module.

## Two-factor Authentication

Na toegang verkregen te hebben door het hoofd authenticatie proces, dit kan een van de andere genoemde oplossingen zijn, voor veiligheidsmaatregelen sturen we een extra check. Deze zou in principe alleen verstuurd moeten worden naar personeel met de juiste machtigingen. Dus als NFC als authenticatie wordt gebruikt zouden er smart cards worden verdeeld onder de gemachtigde. Als een van deze kaarten wordt gestolen zou nog steeds alleen de gemachtigde toegang hebben tot bewerkingsrechten aangezien in het systeem onder die kaart een persoonlijk wachtwoord of verificatie code is vereist om in te loggen. Two-factor authenticatie is dus een extra stap om het systeem nog wat veiliger te maken die verder op een andere oplossing gebouwd kan worden. Maar hiervoor zulle alle stakeholders die op het schip de IHM status of updates willen bekijken hun email of telefoonnummer afgeven. Dit zou dan in een database moeten worden opgeslagen.

## Mobiele telefoon app

Tegenwoordig heeft iedereen wel een telefoon. Deze telefoons hebben vaak ook bluetooth en NFC-functionaliteit. Kunnen we het niet makkelijk maken en NFC of Bluetooth via onze telefoons gebruiken? Google of Apple wallet geeft je telefoon de mogelijkheid om een NFC kaart na te bootsen via je telefoon. Helaas is het niet mogelijk om zelf een NFC-kaart hieraan toe te voegen, want je kan alleen geverifieerde kaarten zoals creditcards hieraan toevoegen. Het is mogelijk om een aparte app te gebruiken voor NFC lezen of schrijven, maar het emuleren van een NFC kaart zelf is alleen mogelijk als je telefoon “geroot” is. Dit omdat NFC kaart ID naar de configuratie van de telefoon moet worden gestuurd waarvoor root privileges nodig voor zijn. Het zou mogelijk zijn een app te ontwikkelen die gebruik maakt van de NFC-functionaliteit, maar dit is een complexe oplossing. Zelf een hele app voor de ingebouwde NFC-reader ontwikkelen is erg uitdagend. Bluetooth is makkelijk te gebruiken, er zijn al apps ontwikkel die te gebruiken zijn om data te versturen. En zelf een app ontwikkelen die gebruik maakt van bluetooth is zeker uitvoerbaar.

## Conclusie:

Uit alle oplossing zijn de meest geschikte NFC en bluetooth. Andere oplossingen zijn soms veiliger maar vaak wel veel complexer. Te complex voor deze use-case aangezien de module op het schip toch geen toegang heeft tot het hele IHM. NFC smart cards kunnen op het schip gegeven worden aan de eigenaar van het schip en eventueel nog een kaart aan de tweede in lijn. Als de IHM module benaderd moet worden kan de desbetreffende stakeholder naar de kapitein gaan om zo met smart card toegang te kunnen krijgen. Met de smartcard oplossing moet er wel een scherm gekoppeld zijn aan de module om de resultaten te zien.

Bluetooth zou geen scherm nodig hebben, de module zou via bluetooth op je telefoon het bericht kunnen laten zien. Als bluetooth gebruikt gaat worden zal dit via telefoon gaan, dit is makkelijker want tegenwoordig heeft iedereen een mobiele telefoon met bluetooth. Wel moet nog een maatregel genomen worden dat niet iedereen via bluetooth kan verbinden met de module. Bij het gebruik van een wachtwoord komen nog steeds problemen kijken, maar het gebruik van tokens of een eenmalig wachtwoord zou hierbij kunnen werken.

Hoewel NFC zeker een goede oplossing is, het gebruik van fysieke kaarten die beveiligd op een schip moeten zijn is toch minder handig dan het gebruik van je telefoon en bluetooth. Waarschijnlijk zal de token of het eenmalig wachtwoord gegeven worden door hetzelfde server waar de blockchain op zal staan. Bluetooth is in dit geval de betere oplossing.

# Hoe verbinden we de module met de blockchainserver?

Er zijn verschillende manieren om met het internet te verbinden op een schip. Maar voor ons geval zal dit alleen nodig zijn wanneer het schip aan wal staat. Wat is de beste methode om te gebruiken voor onze use-case?

## Satelliet:

Op dit moment is de meest populaire internetverbinding via satelliet, starlink. Op dit moment is dit nog steeds niet over de hele wereld maar heeft al een bereik op veel grote gebieden zoals Europa en Noord-Amerika [7]. Qua bereik is het een van de beste en vrij snelle oplossingen maar ook een van de duurdere. Zo zal er een maandelijkse afschriften zijn en een groter eenmalig afschrift.

## Mobiele datanetwerken:

Een mobiel netwerk werkt hetzelfde als je telefoonverbinding. Dus dat betekent ook dat je een sim kaart en abonnement nodig hebt. Je zou een internationale sim card kunnen aanschaffen die je bereik geeft in de meeste landen op de wereld. Overtijd zal dit een best dure oplossing zijn. Wel heb je vaak tenminste 10GB per maand beschikbaar.

## LoRaWAN:

LoRa is een draadloze modulatie techniek, die informatie via radio golven verstuurt in pulsen waardoor ze een vrij grote afstand kunnen overbruggen [8]. LoRaWAN is een netwerk protocol dat gebruikt wordt bovenop de LoRa technologie, zo kan de LoRa verzender via een LoRaWAN gateway verbinding maken met het internet. LoRa heeft een bereik van 2-5 Km in bebouwde gebieden. Wel heeft LoRa een lagere bandbreedte en is niet geschikt voor het versturen van grote aantallen data. Ook moet er een LoRaWAN gateway binnen het bereik zijn voor toegang tot de blockchain server.   
Binnen Europa en bijna over de hele wereld zijn er al LoRaWAN gateways beschikbaar [9]. De kans dat er een gateway binnen het bereik van 2-5km van het aangemeerde schip bevindt is vrij hoog. Ook zijn er verschillende frequenties die worden gebruikt. Zo hebben de US, de EU en China allemaal verschillende frequentieplannen. Voor het verkrijgen van het volledige IHM is LoRa niet geschikt, want deze bestandsgrootte is te hoog, maar voor het verkijgen van de laatste aanpassingen in het IHM is dit mogelijk indien er een LoraWAN gateway zich binnen het bereik bevind.

## Conclusie:

Na het afwegen van de opties zal LoRaWAN de goedkoopste en makkelijkste implementatie hebben. Satelliet zal het beste zijn voor op zee, maar aangezien dat voor onze use-case niet erg belangrijk valt deze af vanwege de prijs. Een Mobiel datanetwerk en LoRa zijn het beste voor aan wal. De mobiele datanetwerken zijn sneller, met beschikking tot een grotere data overdracht. LoRa als goedkoopste optie past toch het beste binnen de use case. Er hoeft niet veel data verstuurd te worden dus een mobiel datanetwerk zou overbodig zijn. Ook zijn er inmiddels al erg veel LoRaWAN gateways over de hele wereld dus is het bereik erg goed op veel plekken.

# Hoe gaat dit systeem er technisch uit zien?

## Microcontroller

De microcontroller, oftewel de hersenen van het systeem. Het moet mogelijk zijn om een LoRa module en een bluetooth module aan te sluiten hierop. In het beste geval is er al een ingebouwde bluetooth module in de microcontroller. De microcontroller hoeft niet al te krachtig te zijn en zal alleen het informatie pakketje van de blockchain server doorsturen over bluetooth naar de gebruiker’s telefoon. Een paar microcontrollers hebben al toegang tot bluetooth zonder het gebruik van een extra module, zoals Raspberry PI of ESP32. Een rapsberry Pi heeft zijn eigen besturingsysteem en meer rekenkracht, maar dit is niet nodig voor deze use-case. Een ESP32 is energiezuiniger en past beter bij deze opdracht. Andere microcontrollers zoals arduino’s of STM’s zijn ook te gebruiken met een bluetooth module aangesloten. Aannemelijk zal de module aan de stroom van het schip worden verbonden dus is een laag energiegebruik niet een enorm grote prioriteit. Voor dit prototype is de keuze niet van erg groot belang, aangezien alle voorgenoemde opties mogelijk zijn. Waarschijnlijk gaat de keuze voor dit prototype naar een ESP32 of een arduino voor de snelle ontwikkelsnelheid. De ESP32 heeft al ingebouwde bluetooth ondersteuning dus dit zal de keuze worden voor het prototype.

## Architectuur

De module op het schip zal niet te complex zijn. Een microcontroller direct aan een stopcontact verbinden kan niet zomaar, want het stopcontact geeft hiervoor teveel stroom dus er zou een speciale adapter moeten worden gebruikt. Een batterij zou makkelijker zijn, maar deze zou om de tijd vervangen moeten worden. Aan de microcontroller zou een LoRa module zitten die informatie kan ophalen en sturen uit het LoRaWAN netwerk. Je kan dus met de module verbinden via bluetooth, vervolgens kun je de status van het IHM opvragen vanuit het blockchain netwerk. Dit bericht zal dan op je telefoon verschijnen.

# Conclusie

Binnen de EU moeten schepen een geldige en gecertificeerde Inventory of Hazardous Materials aan boord hebben. De IHM is een gedetailleerd document dat een overzicht biedt van alle gevaarlijke materialen die aan boord van het schip aanwezig zijn. De IHM slaan we digitaal op, maardeze moet wel aan het schip gekoppeld zijn met een fysieke module. Via deze module zou de port authority kunnen zien wat de status van de IHM is, of deze nog up to date is en kloppend. Deze module moet wel beveiligd zijn zodat alleen gemachtigde personen hierbij zouden komen.   
  
In dit onderzoek is er naar verschillende opties gekeken zoals: Smart cards, biometrische sensoren, hardware security modules en bluetooth. Uit deze opties bleek dat smart cards met NFC en bluetooth wel degelijk goede opties waren. Smart cards zouden fysieke kaarten zijn die toegang brengen tot de module. Deze kaarten zouden gemachtigd moeten worden door de kapitein en de tweede in lijn. Bij bluetooth kan de gebruiker zijn telefoon gebruiken, dus dan is er geen behoefte aan een fysieke sleutel. Wel vereist dit een digitale sleutel, zoals een token of eenmalig wachtwoord.   
  
Eenmaal verbonden met de module moet deze toegang krijgen tot de server. Toegang tot het internet kan via satelliet communicatie, mobiele datanetwerken en LoRaWAN. Uit deze opties bleek LoRaWAN al snel de goedkoopste oplossing. LoRA gebruikt radiogolven die tot 2-5 km ver komen om een open gateway te vinden waarmee deze verbind met het internet. De internetsnelheid over dit netwerk is vrij traag maar aangezien de IHM status en updates alleen via tekst over dit netwerk hoeven worden gestuurd is dit acceptabel. Binnen Europa zijn er genoeg LoRAWAN gateways bij de grote steden en havens dat er altijd wel internet toegang te vinden is.

Dit systeem zal een microcontroller zoals de ESP32 gebruiken voor de bluetooth verbinding, en hieraan zal een LoRa module gekoppeld worden zodat deze kan communiceren met de server.

# Bronnen

[1] Official Journal of the European Union, “Regulation (EU) no 1257/2013 of the European Parliament” <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:330:0001:0020:EN:PDF>

[2] B. Lutkevich, L. Rosencrance, and M. Cobb, “What is smart card?” TechTarget, <https://www.techtarget.com/searchsecurity/definition/smart-card>

[3] Nathan Chandler "What's the difference between RFID and NFC?" 7 March 2012. HowStuffWorks.com. <https://electronics.howstuffworks.com/difference-between-rfid-and-nfc.htm>

[4] RecFaces, “What are biometric devices: Definition, types and use in Authentication & Security,” RecFaces, <https://recfaces.com/articles/articles-biometric-devices>

[5] C. Crane, “What is a hardware security module? HSMS explained,” Hashed Out by The SSL StoreTM, <https://www.thesslstore.com/blog/what-is-a-hardware-security-module-hsms-explained/>

[6] M. Uy, “What is bluetooth? the ultimate guide,” Lifewire, <https://www.lifewire.com/what-is-bluetooth-2377412>

[7] Starlink, “Starlink map” <https://www.starlink.com/map>

[8] The Things Network, “What are Lora and Lorawan?,” The Things Network, <https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/>

[9] The Things Network, “Community,” The Things Network, <https://www.thethingsnetwork.org/community>

# Changelog

|  |  |  |
| --- | --- | --- |
| Versie | Verandering | Datum |
| 0.1 | Opzet gemaakt | 07/02/24 |
| 0.2 | Opties geschreven | 13/02/24 |
| 0.3 | Verbinden met blockchain af | 16/02/24 |
| 0.4 | Authenticatie af + bronnen | 20/02/24 |
| 0.5 | Hoe gaat dit systeem er uit zien? | 21/02/24 |