Literatuur Onderzoek: Authenticatie

# Inleiding

De IHM moet gekoppeld worden aan een schip. Dus er zou een apparaat moeten worden geïnstalleerd dat voor personeel met de juiste autorisatie kan worden bekeken voor aanpassingen in de IHM. De hele IHM hoeft niet zichtbaar te zijn, alleen dat de IHM aanwezig is, en wat de laatste aanpassingen zijn. Maar hoe voeren we de authenticatie van het personeel uit? En hoe verbinden we deze module de server waar het IHM op staat.

# Naleving veiligheid?

De belangrijkste eis van het systeem is het differentiëren van de verschillende autoriteiten. We zoeken een soort technologie waarmee iedereen bij de microcontroller de IHM kan bekijken, maar voor het geautoriseerde personeel dat komt valideren of aanpassen zou er een uitzondering moeten worden gemaakt die dan de IHM kunnen beheren.

# Opties:

## Smart Cards (RFID & NFC):

Een smart cards is een fysieke kaart met een ingebouwde chip die werkt als een beveiligingstoken. 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 vervinding kan RFID (Radio Field Identification) of NFC (Near-field communication) gebruiken. Wat is het verschil tussen RFID en NFC?  
  
De twee grootste verschillen zijn:  
- 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. 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.

## 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. 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.

## Blue tooth LE (tags)

…

## 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.

## Mobiele telefoon app

……

# Hoe krijgen we de autorisatie bij de juiste mensen?

Blockchain, IOT (lora), database, smart contracts

# Hoe verbinden we met de blockchain server?

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. 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. En 4G-5G in het buitenland is vaak duurder dan in Nederland dus dit zal ook een dure oplossing zijn.

## (Long-Range) Wifi:

Wifi op schip?

## LoRaWAN:

LoRa is een draadloze modulatie techniek, die informatie via radio golven verstuurt in pulsen waardoor ze een vrij grote afstand kunnen overbruggen. 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. Voor het verkrijgen van het volledige IHM is LoRa niet geschikt maar voor het verkijgen van de laatste aanpassingen is dit mogelijk indien er een LoraWAN gateway zich binnen het bereik bevind.

# Vereisten microcontroller?

De microcontroller, oftewel de hersenen van het systeem. Moet de software voortgekomen uit het software literatuuronderzoek kunnen uitvoeren en koppelen met de hardware oplossing die voortkomt uit dit onderzoek. Ook moet deze toegang hebben tot het internet, via wifi of ethernet. Een opslagsysteem en besturingssysteem is ook vereist, want misschien willen we de IHM wel (encrypted) lokaal opslaan en alleen de hash in de blockchain zetten.

Bronnen

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:330:0001:0020:EN:PDF>

<https://www.techtarget.com/searchsecurity/definition/smart-card>

<https://recfaces.com/articles/articles-biometric-devices>

<https://www.thesslstore.com/blog/what-is-a-hardware-security-module-hsms-explained/>

<https://www.starlink.com/map>

<https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/>

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>  
7 February 2024

|  |  |  |
| --- | --- | --- |
| Versie | Verandering | Datum |
| 0.1 | Opzet gemaakt | 07/02/24 |