2025

Biometrisch Toegangssysteem

Onderzoek naar de ontwikkeling van een veilig en schaalbaar biometrisch toegangscontrolesysteem

BIOMETRISCH TOEGANGSSYSTEEM
PIOTR TADRALA | INFORDB

O-PP-CMK

I. MANAGEMENT & SAMENVATTING

//TODO: Compleet samenvatting

II. VERSIEBEHEER & DISTRIBUTIE

VERSIEBEHEER

Versie	*Omschrijving*	*Auteur*
0.1	Eerste opzet van het document *(Hoofdstuk 1 t/m 5)*	Piotr Tadrala
0.2		
0.3		

DISTRIBUTIEBEHEER

Versie	*Ontvangers*
0.1	• Lennart de Graaf • Ton Scheres
0.2	
0.3	

III. WOORDENLIJST

Begrip	*Omschrijving*
Biometrische Verificatie	Authenticatiemethode op basis van unieke lichaamskenmerken, zoals gezichtsherkenning of vingerafdruk
Spoofing	Een techniek waarbij en systeem misleidt wordt met nep gegevens.
Liveness-detectie	Technologie die controleert of een biometrisch kenmerk afkomstig is van een levende persoon.
Deepfake	Door AI gegenereerde beelden of video's
MFA	Een beveiligingsmethode waarbij meerdere verificatiestappen worden gebruikt.
SDK	Software Development Kit
EDK	Embedded Development Kit
RFID	Radio Frequency Identification
BLE	Low Energy Bluetooth
SaaS	Software as a Service

INHOUDSOPGAVE

1.0 INLEIDING

InforDB BV is opgericht in 2005 en begon als specialist in softwareontwikkeling en database-consultancy, met een focus op de financiële sector. Het bedrijf ontwikkelde data architecturen voor organisaties zoals ABN Amro, ABP en ING Bank. In 2012 werd InforDB Development opgericht om zich te richten op apps en webapplicaties. Inmiddels levert InforDB maatwerksoftware voor diverse branches en heeft diverse applicaties ontwikkeld die door verschillende organisaties worden gebruikt.

Het bedrijf ziet potentie in de ontwikkeling van een toegangssysteem dat zowel betrouwbaar als gebruikersvriendelijk is, met nadruk op de integratiemogelijkheden in de bestaande applicaties van InforDB.

Biometrische technologie biedt hiervoor een oplossing, maar wordt steeds makkelijker te omzeilen, bijvoorbeeld door AI. InforDB ziet potentie in de ontwikkeling van een systeem dat niet beperkt is tot een verificatiemethode, zoals een vingerafdruk- of gezichtsherkenning, maar een bredere set van (biometrische) verificatietechnieken toepast voor toegangscontrole. Eisen voor het uiteindelijke product zijn dat het plug-and-play, gebruiksvriendelijk en veilig moet zijn.

2.0 CONTEXT

2.1 INLEIDING

Biometrische verificatie wordt steeds vaker ingezet voor toegangssystemen, omdat het betrouwbaarder en gebruiksvriendelijker is dan traditionele methoden zoals fysieke sleutels. Toch geven veel systemen een valse hoop van veiligheid door beperkte maatregelen tegen spoofing.

2.2 HUIDIGE SITUATIE

Momenteel maken veel toegangscontrolesystemen gebruik van biometrische verificatie, zoals gezichtsherkenning en vingerafdrukscanners. Hoewel deze technieken goede beveiliging bieden, hebben ze enkele beperkingen:

- **Kwetsbaarheid voor spoofing**: Biometrische systemen kunnen worden misleid door foto's, video's of deepfake-technologie.
- **Gebrek aan liveness-detectie**: Veel systemen controleren niet of de biometrische input afkomstig is van een levende persoon.
- **Afhankelijkheid van één verificatiemethode**: De meeste systemen gebruiken slechts één verificatiemethode, waardoor ze minder robuust zijn tegen aanvallen.
- **Beperkte implementatie van anti-spoofingtechnieken**: Door kosten, infrastructuurbeperkingen of een gebrek aan regelgeving worden deze technieken niet altijd toegepast.
- **Privacyrisico's en angst voor datalek:** Biometrische gegevens zijn zeer gevoelig. Wanneer deze gegevens worden gelekt of gestolen, zijn ze niet eenvoudig te wijzigen zoals wachtwoorden.
- **Foutmarges en onnauwkeurigheid:** Biometrische systemen zijn niet altijd 100% nauwkeurig. Slechte lichtomstandigheden, verouderde algoritmes of wijzigingen in het uiterlijk van de gebruiker kan leiden tot onnauwkeurigheid van het systeem.
- **Hoge kosten:** De implementatie van geavanceerde biometrische systemen, zoals die met liveness-detectie of geavanceerde sensoren, kan hoge initiële kosten en onderhoudskosten met zich meebrengen.
- **Afhankelijkheid van technologie bij storingen:** Storingen in het systeem, zoals netwerkproblemen of hardwarefouten, kunnen de toegang blokkeren of het systeem onbetrouwbaar maken. Er dient dus altijd een back-upmethode aanwezig te zijn.

2.3 PROBLEEMSTELLING

Hoewel biometrische toegangssystemen een hoger beveiligingsniveau bieden dan traditionele methoden, zijn ze kwetsbaar voor misleidingspogingen zoals deepfakes en spoofing. Daarnaast vertrouwen veel systemen op slechts één enkele verificatiemethode, wat de veiligheid beperkt en de kans op ongeautoriseerde toegang vergroot. Bovendien brengen deze systemen privacyrisico's, foutmarges en hoge implementatiekosten met zich mee.

2.4 DOELSTELLING

Het doel van dit document is te onderzoeken hoe een toegangssysteem kan worden ontwikkeld dat zowel gebruiksvriendelijk is, bestand is tegen spoofing-attacks en eenvoudig kan worden geïntegreerd in bestaande systemen.

3.0 ONDERZOEKSAANPAK

3.1 INLEIDING

In dit hoofdstuk laat ik zien waar dit document zich op richt. De hoofdvraag en de bijbehorende deelvragen worden in kaart gebracht, en wordt gekeken hoe deze vragen beantwoord kunnen worden.

3.2 HOOFDVRAAG

Hoe kan een biometrisch toegangscontrolesysteem worden ontworpen en ontwikkeld dat zowel gebruiksvriendelijk als veilig is tegen misleidingspogingen, zoals deepfakes, en eenvoudig te integreren is met andere systemen?

3.3 DEELVRAGEN

Index	Deelvraag
D1	Zijn er al vergelijkbare systemen op de markt?
D2	Welke verificatiemethodes zijn er beschikbaar?
D3	Welke anti-spoofing maatregelen kunnen er worden genomen?
D4	Welke architectuur en welk platform zijn het meest geschikt voor een schaalbaar toegangssysteem?
D5	Welke componenten zijn er nodig en wat zijn de kosten om het systeem te realiseren?

3.4 ONDERZOEKSMETHODEN

Index	Onderzoeksmethode
D1	Literatuuronderzoek
D2	Literatuuronderzoek
D3	Literatuuronderzoek, Data-analyse, Prototyping
D4	Literatuuronderzoek, prototyping
D5	Literatuuronderzoek, Prototyping

3.5 VERWACHTE ONDERZOEKSUITKOMSTEN

Index	Verwachte uitkomst
D1	Eventuele bestaande systemen
D2	Potentiele verificatiemethodes
D3	Anti-spoofing methodes
D4	Meest geschikt software & hardware architectuur & platform
D5	Te realiseren hardware en software componenten

3.6 SCOPE

Dit document richt zich op het onderzoeken van de bovenstaand genoemde onderzoeksvragen die beantwoord moeten worden om een prototype te kunnen ontwikkelen. Het beschrijft niet hoe het prototype kan worden omgezet tot een commercieel product.

4.0 ZIJN ER AL VERGELIJKBARE SYSTEMEN OP DE MARKT?

4.1 INLEIDING

Bij het ontwikkelen van een biometrisch toegangscontrolesysteem leek het verstandig om eerst te onderzoeken welke systemen al op de markt beschikbaar zijn. Dit geeft meer inzicht in bestaande functionaliteiten, zwakke punten en innovaties. Dit helpt bij het identificeren van good & bad practices, en het vaststellen van de huidige marktstandaarden. In dit hoofdstuk vergelijk ik bestaande oplossingen.

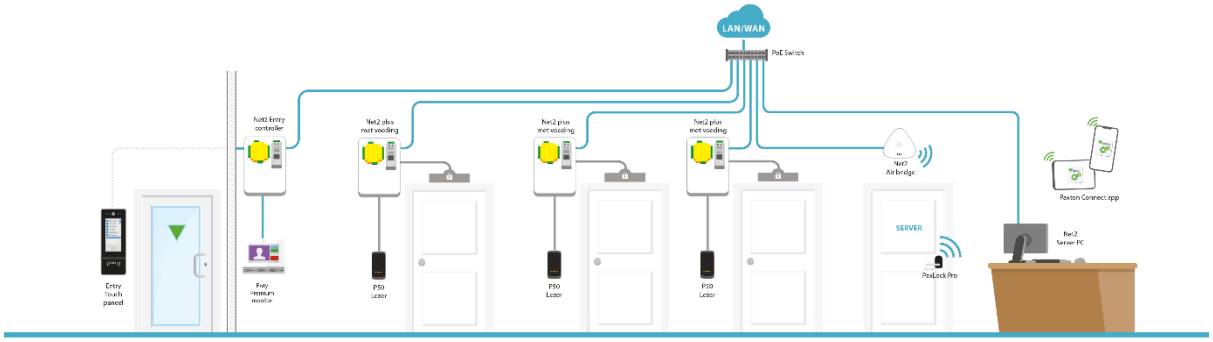
4.2 BESTAANDE OPLOSSINGEN

PAXTON

Paxton is een flexibel toegangscontrolesysteem dat integratie met biometrische lezers mogelijk maakt. Het systeem ondersteunt API-integraties, waardoor het kan samenwerken met andere systemen.

Systemen van Paxton, zijn ontworpen met een modulaire opbouw. Voor elke deur die u wilt beveiligen, is één deurcontroller nodig. Deze architectuur maakt het mogelijk om klein te beginnen en het systeem vervolgens eenvoudig uit te breiden.

Paxton biedt draadloze deurbeslagen, zoals PaxLock, die rechtstreeks op de deur kunnen worden gemonteerd zonder noodzaak voor bekabeling. Deze beslagen communiceren volledig draadloos.

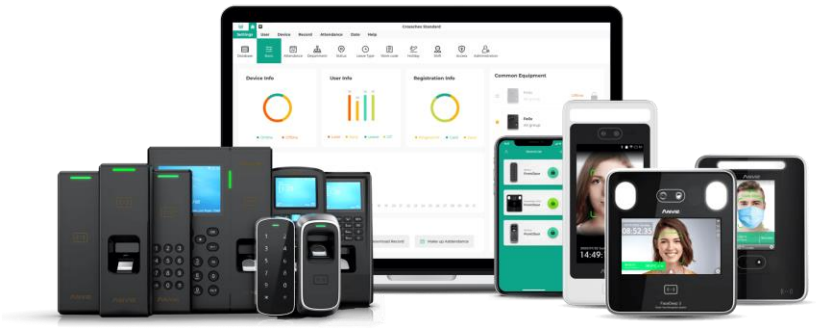


• Paxton, (Onbekend) Hoe maak ik een veilig toegangscontrole systeem nog veiliger?

ANVIZ

Anviz biedt oplossingen met liveness-detectie die zowel biometrische verificatie als traditionele methoden, zoals smartcards, ondersteunen. Het grootste verkoopargument van Anviz is de eenvoudige integratie dankzij hun EDK en SDK, gecombineerd met diverse toegangsbeheerfuncties, zoals gebruikersbeheer en apparaatbeheer.

Toegangscontrolesystemen van Anviz worden eenvoudig aan de muur bevestigd en aangesloten op een 12V DC-voeding en netwerk via Ethernet of Wi-Fi. De configuratie verloopt via de CrossChex-software, waarin gebruikers worden geregistreerd met biometrische gegevens of RFID-kaarten, en toegangsrechten worden ingesteld. Ook is mobiele toegang via een app mogelijk. De installatie is snel en gebruiksvriendelijk.



- Anviz, (Onbekend) Slimme oplossing voor toegangscontrole

BOSCH SECURITY

Biometrische oplossingen van Bosch Security bieden zowel hoge verificatie naukeurigheid, als anti-spoofing technieken zoals Presentation Attack Detection (PAD) uitgevoerd door iBeta.

Bosch Security-toegangscontrolesystemen bieden een eenvoudige installatie met zowel bekabelde als draadloze opties. De apparaten worden aangesloten op een centrale controller en geïntegreerd met bestaande infrastructuur via Ethernet of RS485. Configuratie verloopt via Bosch's beheersoftware, waarin gebruikers biometrische gegevens of RFID-kaarten registreren en toegangsrechten beheren. De systemen ondersteunen ook contactloze toegang en kunnen eenvoudig worden beheerd via een webinterface of mobiele app.

- Bosch, (Onbekend) Biometrische toegangscontrole

4.3 GOOD & BAD PRACTICES

PAXTON

	Omschrijving
Good	MFA.
Good	API Integraties mogelijkheden.
Good	Modulaire opbouw.
Bad	MFA werkt alleen met de traditionele technieken zoals cards of pin.
Bad	Geen informatie met betrekking tot anti-spoofing.

ANVIZ

	Omschrijving
Good	Eenvoudige API integraties dankzij hun EDK & SDK.
Good	Liveness-detectie.
Good	Toegangsbeheer portal.
Bad	Geen MFA mogelijkheden.
Bad	Liveness-detectie is puur op gezichtskenmerken gebaseerd.

BOSCH SECURITY

	Omschrijving
Good	Hoge verificatie nauwkeurigheid.
Good	Anti-spoofing.
Good	API Integraties mogelijkheden.
Bad	Geen MFA.
Bad	Anti-spoofing is puur op gezichtskenmerken gebaseerd.

4.4 HUIDIGE MARKTSTANDAARDEN

Huidige oplossingen nemen stappen om zich te beschermen tegen spoofing, maar dit blijft in de meeste gevallen beperkt tot liveness-detectie op basis van gezichtskenmerken. Multi-Factor Authenticatie is nog geen standaardpraktijk. Hoewel sommige systemen MFA ondersteunen, is deze vaak beperkt tot traditionele methoden zoals een smartcard in combinatie met een PIN-code. API integratie mogelijkheden lijken in de meeste gevallen wel aanwezig te zijn, maar worden soms beperkt tot de lokale omgeving. Installatieprocessen verschillen per leverancier, maar de meeste systemen bieden eenvoudige, modulaire installatieopties met beheer via software of mobiele applicaties

4.5 CONCLUSIE

Bestaande toegangscontrolesystemen bieden flexibele API-integraties en modulaire installatieopties. Anti-spoofing is aanwezig, maar vaak beperkt tot basale liveness-detectie op gezichtskenmerken. MFA wordt ondersteund, maar voornamelijk via traditionele methoden zoals smartcards en PIN-codes. Hoewel deze oplossingen een goede basis bieden, ontbreekt het vaak aan geavanceerde anti-spoofingtechnieken en moderne MFA-opties die de algehele veiligheid verder kunnen versterken.

5.0 WELKE VERIFICATIEMETHODES ZIJN ER BESCHIKBAAR?

5.1 INLEIDING

In dit hoofdstuk onderzoek ik de beschikbare (biometrische) verificatiemethodes die toegepast kunnen worden binnen het toegangscontrolesysteem. Het doel is om inzicht te krijgen in de verschillende methodes. Hiermee is het doel om uiteindelijk tot de conclusie te komen welke verificatiemethodes het meest geschikt zijn voor dit project.

5.2 BEOORDELINGCRITERIA

Om de meest geschikte verificatiemethode te bepalen, is het belangrijk om eerst de beoordelingscriteria vast te stellen. Vervolgens kunnen de onderzochte verificatiemethodes worden beoordeeld. Op basis van deze scores kan de meest geschikte methode worden gekozen. De belangrijkste factoren die hierbij een rol spelen, zijn:

- **Veiligheid:** Hoe veilig en betrouwbaaar is de methode?
- **Gebruikersgemak:** Hoe gebruikersvriendelijk en seamless is de verificatie?
- **Snelheid:** Hoe snel kan de gebruiker worden geverifieerd?
- **Kosten:** Wat zijn de kosten van implementatie?

5.3 BIOMETRISCHE VERIFICATIEMETHODES

GEZICHTSHERKENNING

Gezichtskenmerken, zowel afzonderlijk als in combinatie, worden gebruikt voor biometrische verificatie. Dit houdt meestal in dat een face match-algoritme controleert of twee gezichten (het geregistreerde en het gepresenteerde) overeenkomen om de identiteit te verifiëren.

SPRAAKHERKENNING

Dankzij spraakherkenning is het mogelijk om gebruikers te onderscheiden en authenticeren op basis van hun unieke stemafdruk. Bij spraakherkenning evalueert het programma kenmerken zoals toonhoogte, intonatie, ritme en frequentie van de stem. Het systeem vergelijkt deze kenmerken met een eerder opgeslagen stemprofiel om de identiteit van de gebruiker te bevestigen

VINGERAFDRUK

Bij een authenticatie via de vingerafdruk, wordt de vingerafdruk gescand en gedigitaliseerd. Zo wordt een digitaal beeld van de kenmerken van de vingerafdruk gemaakt. Dit wordt opgeslagen in een beveiligde database. Iedereen heeft een uniek patroon van lijnen op de vingers, waardoor vingerafdrukken een effectieve manier zijn om iemand te identificeren.

OVERIGE VERIFICATIEMETHODES

Naast de genoemde methodes zijn er nog andere verschillende biometrische verificatiemethodes, zoals irisscans, vinger- of handgeometrie en hartslagmeting. Deze worden echter niet in overweging genomen vanwege lagere gebruiksvriendelijkheid, hoge kosten of beperkte implementatiemogelijkheden binnen de software.

- Shaip, (2024) Wat is spraakherkenning.

- Seon, (Onbekend) Biometric Verification
- Veiliginternetten, (Onbekend) Wat is biometrische authenticatie? En wanneer gebruik je het?
- Biometrisc Institute, (Onbekend), Types of Biometrics

5.4 TRADITIONELE VERIFICATIEMETHODES

Naast de biometrische methoden kunnen we ook gebruik maken van traditionele methodes, die als secundaire verificatie stap van de MFA functioneren. Denk hierbij aan een verificatieflow waarbij gezichtsherkenning de primaire methode is, maar waarbij de gebruiker daarnaast aan een secundaire, niet perse biometrische, verificatie moet voldoen. Mogelijke opties hiervoor zijn:

- **RFID:** Een tag gekoppeld aan de gebruiker, die binnen een bepaalde afstand gedetecteerd moet worden tijdens de gezichtsverificatie.
- **BLE:** In plaats van een tag kan een mobiele telefoon worden gebruikt, waarvan de BLE-signaal binnen een bepaalde afstand gedetecteerd moet worden.
- **GPS (Mobiele App) :** Om verificatie op basis van de locatie van de gebruiker uit te voeren, kan een geautoriseerde mobiele applicatie die op de achtergrond automatisch een request naar het systeem sturen zodra de gebruiker zich binnen een bepaald bereik bevindt.
- **Pincode:** De gebruiker voert een vooraf ingestelde pincode in via een keypad of touchscreen.
- **Push-notificatie:** De gebruiker ontvangt een pushmelding op zijn smartphone en moet de toegang handmatig goedkeuren of weigeren.

- Cie-group, (Onbekend) Access control contactless authentication methods

5.5 VERGELIJKINGSMATRIX

De onderstaande matrix geeft een visuele vergelijking van de verschillende verificatiemethoden op basis van vier belangrijke criteria: Veiligheid, Gebruiksgemak, Snelheid en Kosten. De kleuren in de tabel vertegenwoordigen de score per criteria.

De veiligheid score staat los van de eventuele anti-spoofing maatregelen die in de volgende hoofdstuk worden onderzocht.

Score	Betekenis	Kleur
1	Slecht	Rood
2	Gemiddeld	Geel
3	Goed	Groen

Methode	Veiligheid	Gebruikersgemak	Snelheid	Kosten	Totaal
Gezichtsherkenning	2	3	3	1	9
Spraakherkenning	1	2	1	2	6

Vingerafdruk	3	1	2	1	7
RFID	2	2	2	1	6
BLE	3	2	2	3	10
GPS (Mobiele APP)	3	2	2	3	10
Pincode	2	2	1	3	8
Push-Notificatie	3	2	2	3	10

5.6 ONDERBOUWING VAN DE VERGLIJKINGSMATRIX

GEZICHTSHERKENNING

- **Veiligheid:** Gezichtsherkenning is relatief veilig wanneer het goed wordt geïmplementeerd, maar blijft kwetsbaar voor spoofing.
- **Gebruikersgemak:** De gebruiker hoeft enkel naar de camera te kijken.
- **Snelheid:** Gezichtsherkenning kan, indien de hardware dit toelaat, plaatsvinden nog voordat de gebruiker zich bewust is van het proces, bijvoorbeeld tijdens het benaderen van de deur. Hoewel het algoritme mogelijk niet sneller is dan bijvoorbeeld een vingerafdrukscan, het feit dat de verificatie al vooraf kan plaatsvinden zorgt voor een snellere totale proces.
- **Kosten:** Voor efficiënte gezichtsherkenning is krachtige hardware vereist, wat kan leiden tot hogere kosten.

SPRAAKHERKENNING

- **Veiligheid:** Gevoelig voor imitatie en weining anti-spoofing methodes.
- **Gebruikersgemak:** Vereist een handeling aan de hardware.
- **Snelheid:** Langzamer vanwege meerdere woorden die de gebruiker dient uit te spreken.
- **Kosten:** Gemiddeld, afhankelijk van de gebruikte hardware.

VINGERAFDRUK

- **Veiligheid:** Vingerafdrukken zijn uniek en moeilijk te spoofen.
- **Gebruikersgemak:** De methode vereist dat de gebruiker fysiek contact maakt met de hardware.
- **Snelheid:** Hoewel de verificatie zelf vrijwel instant is, zorgt de extra handeling van de gebruiker ervoor dat het totale proces iets langer duurt.
- **Kosten:** De kosten van vingerafdrukscanners kunnen oplopen tot enkele honderden euro's, afhankelijk van de kwaliteit.

RFID

- **Veiligheid:** Redelijk veilig, maar kwetsbaar voor kwijtraking en skimming.
- **Gebruikersgemak:** De methode vereist dat de gebruiker fysiek contact maakt met de hardware.
- **Snelheid:** De verificatie zelf is relatief snel, maar kan iets langer duren vanwege de handeling van de gebruiker.
- **Kosten:** Prijzen voor goede scanners & cards snel tot enkle honderden euro’s oplopen

BLE / GPS

- **Veiligheid:** De telefoon van de gebruiker dient op locatie aanwezig te zijn wat het best veilig maakt.
- **Gebruikersgemak:** Gebruiker dient de telefoon bij zich te hebben.

- **Snelheid:** Verificatiesnelheid is afhankelijk van de Bleutooth /internet snelheid van de smartphone.
- **Kosten:** Geen extra kosten bij gebruik van persoonlijke smartphones

PINCODE

- **Veiligheid:** Afhankelijk van de complexiteit van de pincode.
- **Gebruikersgemak:** De methode vereist dat de gebruiker fysiek contact maakt met de hardware en zijn pincode onthoudt.
- **Snelheid:** De verificatie zelf is relatief snel, maar kan iets langer duren vanwege de handeling van de gebruiker.
- **Kosten:** Lage kosten dankzij lage complexiteit van zowel hardware als software.

PUSH NOTIFICATIE

- **Veiligheid:** De gebruiker moet op zijn telefoon toegang bevestigen.
- **Gebruikersgemak:** Gebruiker dient de telefoon bij zich te hebben.
- **Snelheid:** Verificatiesnelheid is afhankelijk van de internet snelheid van de smartphone.
- **Kosten:** Geen extra kosten bij gebruik van persoonlijke smartphones

5.7 CONCLUSIE

Voor de primaire verificatiemethode lijkt gezichtsherkenning de beste keuze. Het is snel, veilig en gebruiksvriendelijk. Een nadeel zijn de hogere kosten en het feit dat gezichtsherkenning relatief makkelijk te spoofen is, maar dit wordt in het volgende hoofdstuk verder onderzocht. Voor de secundaire verificatie kiezen we voor combinatie van een pincode of een push-notificatie, waarbij de gebruiker aan eentje moet voldoen. De pincode biedt extra zekerheid, omdat het de gebruiker op basis van kennis verifieert, naast de biometrische gegevens. Een push-notificatie verhoogt het gebruiksgemak, omdat de gebruiker zijn telefoon al kan voorbereiden voordat hij de deur komt. Zodra het gezicht gescand is, hoeft de gebruiker alleen nog de melding te bevestigen.

6.0 WELKE ANTI-SPOOFING MAATREGELEN KUNNEN ER WORDEN GENOMEN?

Facial-recognition => detection
Facial-recognition => thermal facial scan
Facial-recognition => proximity sensors

https://bioconnect.com/blog/2024/01/30/anti-spoofing-facial-authentication-hardware-what-you-need-to-know#:~:text=Liveness%20Detection%3A%20Implement%20liveness%20detection,depth%20estimation%2C%20or%20infrared%20sensors.

https://paperswithcode.com/task/face-anti-spoofing

7.0 WELKE ARCHITECTUUR EN WELK PLATFORM ZIJN HET MEEST GESCHIKT VOOR EEN SCHAALBAAR TOEGANGSSYSTEEM?

7.1 INLEIDING

Het toegangssysteem moet gebruiksvriendelijk, schaalbaar en veilig zijn. Daarom is het cruciaal om goede keuzes te maken over de architectuur en het te gebruiken platform. InforDB wilt het systeem eenvoudig integreerbaar te maken met bestaande softwareoplossingen, waardoor goede integratiemogelijkheden cruciaal zijn.

7.2 REQUIREMENTS

7.2.1 FUNCTIONELE EISEN

- Het systeem moet biometrische verificatie ondersteunen.
- Het systeem moet niet afhankelijk zijn van een verificatiemethode.
- Het systeem moet een slot kunnen aansturen op basis van succesvolle verificatie.
- Het systeem moet logging en monitoring van verificatiepogingen ondersteunen.
- Het systeem moet een gebruikersbeheerfunctie hebben voor toegangscontrole.
- Het systeem moet schaalbaar zijn voor eventuele toekomstige uitbreidingen.

7.2.3 TECHNISCHE EISEN

- De backend moet REST API ondersteunen.
- Het systeem moet compatibel zijn met bestaande sloten.
- Het systeem moet gebruik maken van encryptie voor databeveiliging.
- De hardware moet geschikt zijn voor gebruik in diverse omgevingen (binnen/buiten).
- Voor de software moet het best mogelijke platform worden gekozen (embedded systems, cloud, on-premise).

7.3 HARDWARE ARCHITECTUUR

7.3.1 POTENTIELE OPTIES

Voor het platform zijn er meerdere opties. We kunnen kiezen voor een **embedded opzet**, waarbij het volledige systeem in één hardwarecomponent is geïntegreerd. Dit is de meest gebruiksvriendelijke optie, omdat de gebruiker enkel het kastje hoeft te monteren en te installeren—daarna is het systeem direct operationeel.

Een andere optie is een **on-premise opzet**, waarbij het kastje bij de voordeur gegevens verzamelt, zoals camerabeelden en pincodes. Deze data wordt vervolgens via het lokale netwerk verstuurd naar een centrale hub binnen het gebouw. De hub verwerkt de data en neemt de uiteindelijke beslissingen, zoals het openen van de deur.

Tot slot is er de **cloud-opzet**, waarbij het kastje eveneens de data verzamelt, maar deze direct naar de cloud stuurt voor verwerking. Beslissingen en logica worden hierbij extern afgehandeld, wat het beheer en schaalbaarheid eenvoudiger kan maken, maar afhankelijk is van een stabiele internetverbinding.

7.3.2 VERGELIJKING

Om te bepalen welke opzet het meest geschikt is voor ons systeem, moeten de voor- en nadelen van de verschillende architectuuropties worden vergeleken. Hieronder een overzicht van de genoemde opties.

Embedded	
Voordelen	Plug & Play
	Snelle verwerking, omdat alles lokaal gebeurt, is er geen vertraging door netwerkcommunicatie
	Onafhankelijk van het network
	Hogere privacy dankzij alle data die lokaal blijft opgeslagen
Nadelen	Beperkte rekenkracht
	Niet schaalbaar
	Beperkte functionaliteiten zonder netwerktverbinding
	Beperkte management opties

On-Premise	
Voordelen	Hogere privacy dankzij alle data die lokaal blijft opgeslagen
	Schaalbaar
	Vereist geen internetverbinding
	Voldoende rekenkracht
Nadelen	Complexere installatie
	Beperkte functionaliteiten zonder netwerktverbinding
	Beperkte management opties

Cloud	
Voordelen	Makkelijke installatie
	Geen fysieke onderhoudkosten
	Management mogelijkheden op afstand
	Schaalbaar
Nadelen	SaaS opzet wat waarschijnlijk maandelijkse abonnement zal vereisen
	Beperkte privacy
	Afhankelijkheid van internetverbinding

- Robert Chamberlin, (2024) Key differences between on-premise and cloud based access control systems
- Sailpoint, (2025) Cloud based access control vs. on-premise

7.3.3 BEOORDELINGSCRITERIA

Nu de voor- en nadelen van elk platform globaal in kaart zijn gebracht, kunnen we de belangrijkste criteria voor ons systeem bepalen. Door een vergelijkingsmatrix op te stellen en de platforms te beoordelen op deze criteria, kunnen we concluderen welk platform het meest geschikt is.

- **API Integraties**: Hoe makkelijk is het systeem integreerbaar andere systemen?
- **Scalability**: Hoe schaalbaar is het systeem voor eventuele toekomstige uitbreidigingen?
- **Data Privacy:** Hoe goed wordt data bescherm tijdens opslag en overdracht?
- **Snelheid & Latency:** Hoe snel kan het systeem verificaties uitvoeren?
- **Betrouwbaarheid:** Hoe robuust is het systeem?
- **Management:** Hoe beheerbaar is het systeem?

7.3.4 VERGELIJKINGSMATRIX

Score	Betekenis	Kleur
1	Slecht	Rood
2	Gemiddeld	Geel
3	Goed	Groen

Criteria	Embedded	On-Premise	Cloud
Api Integraties	1	1	3
Scalability	1	2	3
Data Privacy	3	3	2
Snelheid & Latency	3	2	2
Betrouwbaarheid	3	2	2
Management	2	2	3
Totaal	13	13	17

7.3.5 ONDERBOUWING VAN DE VERGELIJKINGSMATRIX

EMBEDDED

- **API Integraties:** Geen API integraties mogelijk zonder internetverbinding.
- **Scalability:** Beperkt tot één apparat.
- **Data Privacy:** Alle gegevens blijven lokaal opgeslagen.
- **Snelheid & Latency:** Geen netwerkvertraging omdat alles lokaal wordt verwerkt.
- **Betrouwbaarheid:** Werking is onafhankelijk van het internet, en heeft minder points of failure.
- **Management:** Alleen mogelijk via het lokale netwerk.

ON-PREMISE

- **API Integraties:** Geen API integraties mogelijk zonder internetverbinding.
- **Scalability:** Schaalbaar maar vereist handmatige updates/aanpassingen aan de hardware.

- **Data Privacy:** Alle gegevens blijven lokaal opgeslagen.
- **Snelheid & Latency:** Iets hogere latency door netwerkcommunicatie.
- **Betrouwbaarheid:** Werking is onafhankelijk van het internet, maar wel van internet infrastructuur.
- **Management:** Alleen mogelijk via het lokale netwerk.

CLOUD

- **API Integraties:** API-mogelijkheden voor integraties met externe systemen.
- **Scalability:** Onbeperkt schaalbaar.
- **Data Privacy:** Gegevensverwerking buiten eigen infrastructuur.
- **Snelheid & Latency:**Vertraging door netwerkafhankelijkheid.
- **Betrouwbaarheid:** Afhankelijk van het internetsnelheid en cloud backend.
- **Management:** Eenvoudig beheer via een webinterface.

7.3.6 CONCLUSIE

Uit het onderzoek naar de platforms is het te concluderen dat geen enkel platform volledig voldoet aan alle eisen. Elk platform heeft zijn eigen sterke en zwakke punten. Daarom zal de oplossing bestaan uit een **hybride opzet van on-premise en cloud**. In deze opzet draait de hardware lokaal en communiceert met een centrale hub, die vervolgens verbinding maakt met een cloud-backend voor extra functionaliteiten, zoals API-integraties en beheer op afstand.

7.4 COMMUNICATIEPROTOCOLLEN

7.4.1 ON-PREMISE COMMUNICATIE

Bij een on-premise opzet, dienen de individuele componenten met elkaar te kunnen communiceren. Hiervoor is het noodzakelijk om een geschikt communicatieprotocol te kiezen. Hieronder enkele potentiele opties.

MQTT

MQTT is een publish/subscribe-protocol dat werkt op basis van berichten. Het gebruikt het TCP-protocol voor betrouwbare communicatie tussen de broker en de aangesloten clients (publishers en subscribers).

De MQTT-broker functioneert als de centrale server die verantwoordelijk is voor het ontvangen, filteren en doorsturen van berichten naar de juiste clients. De publishers verzenden berichten naar specifieke topics op de broker, terwijl de subscribers zich subscriben op deze topics om de berichten te ontvangen.

COAP

CoAP maakt gebruik van een client-server request-response model, vergelijkbaar met HTTP. Een client stuurt een CoAP-request naar de server, die vervolgens reageert met een antwoord. De

request-methodes van CoAP komen overeen met die van HTTP (GET, POST, PUT en DELETE). Net als bij HTTP worden CoAP-endpoints gedefinieerd als URI's.

Het belangrijkste verschil met HTTP is dat CoAP gebruikmaakt van UDP in plaats van TCP, waardoor het lichter en sneller is, maar minder betrouwbaar. CoAP bevat echter mechanismen zoals confirmable messages (CON) en acknowledgments (ACK) om betrouwbaarheid te verhogen.

HTTP

HTTP werkt via een request-response model, waarbij een client een request naar de server stuurt en een response terugkrijgt. Dit is vergelijkbaar met hoe CoAP functioneert, maar HTTP maakt gebruik van TCP in plaats van UDP, wat zorgt voor een betrouwbare, maar minder efficiënte communicatie.

Het protocol wordt voornamelijk gebruikt voor webgebaseerde toepassingen en API-communicatie, waardoor het ideaal is voor cloud-integraties en configuratiebeheer.

LORA

LoRa WAN staat voor Long Range Wide Area Network. Het netwerk bestaat uit nodes (sensoren of apparaten) die via LoRa-verbindingen communiceren met gateways. Een kenmerkende eigenschap van LoRa is het grote bereik, onder ideale omstandigheden kan het network zelfs 15km bereieken met een enkele zender.

LoRa-nodes hebben geen directe internetverbinding nodig. In plaats daarvan communiceren ze met LoRa-gateways via radiogolven op lage frequenties, zoals 868 MHz in Europa en 915 MHz in de VS.

Een van de grootste voordelen van LoRa is de kosten-efficiëntie. Dankzij de lage complexiteit van de modules zijn LoRa-apparaten relatief goedkoop en kunnen ze, door hun zeer lage energieverbruik, enkele jaren functioneren op slechts een paar batterijen.

ZIGBEE

Zigbee is een energiezuinig draadloos protocol dat werkt via een mesh-netwerk, waarbij apparaten onderling communiceren en het signaal doorgeven, waardoor het bereik vergroot en niet afhankelijk is van wifi. Dit maakt Zigbee betrouwbaar, omdat het netwerk blijft functioneren, zelfs als een apparaat uitvalt. In tegenstelling tot wifi worden Zigbee-apparaten niet direct met de router verbonden, wat de netwerkbelasting verlaagt. Dit protocol wordt veel gebruikt in smart home- en IoT-toepassingen, zoals toegangscontrole, dankzij de lage energieconsumptie en veilige AES-128 encryptie.

- Sob, (2017) What are the differences between MQTT, HTTP, CoAP devices (besides communication protocol)?
- Ian Craggs, (2022) MQTT vs CoAP for IoT
- Jonathan Beri, (2020) A field Guide to CoAP – Part 1
- Thingsdata, (Onbekend) LoRa
- Bram, (2022) Wat is het protocol Zigbee en wat kun je ermee

7.4.2 MEEST GESCHIKTE PROTOCOL

HTTP en CoAP lijken minder geschikt voor de on-premise communicatie, vanwege hun hogere overhead en lagere efficiëntie in vergelijking met MQTT.

Zigbee kan een mogelijke optie zijn, maar vereist een Zigbee-coördinator, wat de complexiteit van het systeem verhoogt. Voor een eenvoudige plug-and-play installatie is het toevoegen van extra hardware en configuratiestappen niet ideaal.

Daardoor blijven LoRa en MQTT als potentiele opties over.

//TODO: Criteria, prototypes en Vergelijking tussen LoRa en MQTT

7.4.3 IMPLICATIES

//Implicaties van de gekozen protocol

7.5 SOFTWARE ARCHITECTUUR

7.5.1 HUB

De hub vormt het centrale punt van het systeem, waar data van de nodes wordt verwerkt, toegangsbeslissingen worden genomen en de communicatie met de cloudomgeving plaatsvindt. Een van de belangrijkste requirements is dat het systeem schaalbaar moet zijn voor toekomstige uitbreidingen. Daarom is het essentieel om bij het kiezen van de juiste architectuur te bepalen welk aspect van het systeem prioriteit heeft.

Wanneer **Maintability** de grootste rol speelt, is een layered design de meest geschikte keuze. Dit komt doordat de individuele layers, indien goed gestructureerd, onafhankelijk van elkaar kunnen worden geüpdatet, wat het systeem flexibeler en eenvoudiger te beheren maakt.

Als **Performance** cruciaal is, om ervoor te zorgen dat software snel en efficiënt reageert onder zowel normale als piekomstandigheden. Is een event-driven architectuur een optimale keuze, die real-time datastromen verwerkt en latency minimaliseert.

Als de applicatie relatief **Simpel** is, is een monolithische architectuur een goede keuze. In dit model draait de volledige code binnen één framework, waardoor wijzigingen kunnen worden doorgevoerd zonder dat elke individuele service apart geüpdatet hoeft te worden net als in het geval van microservices.

In ons geval ligt de nadruk op **Scalability**, omdat het systeem moet kunnen groeien. Daarom is een microservices-architectuur de meest geschikte keuze. Microservices maken het mogelijk om individuele componenten onafhankelijk van elkaar te scalen.

- Alexandra Mendes, (2025) Best Types of Software Architecture Patterns Explained

7.5.3 CLOUD APPLICATIE

Het doel van de cloudapplicatie is om functionaliteiten zoals beheer en API-integraties te bieden. Omdat de complexiteit van de applicatie relatief laag is, is een monolithische architectuur een geschikte keuze.

Er zijn veel mogelijke frameworks voor de cloudomgeving. Om de consistentie te behouden met de rest van de applicaties, is gekozen voor een Node.js environment in combinatie met het NestJS framework. Andere potentiële frameworks zijn onder andere Express.js, Meteor, Koa.js en Sails.js. De keuze voor NestJS is gemaakt vanwege de focus op de backend en de modulaire opzet, die het systeem schaalbaar maakt.

X.0 BRONNEN

- Paxton, (Onbekend) Hoe maak ik een veilig toegangscontrole systeem nog veiliger?
- Anviz, (Onbekend) Slimme oplossing voor toegangscontrole
- Bosch, (Onbekend) Biometrische toegangscontrole
- Seon, (Onbekend) Biometric Verification
- Shaip, (2024) Wat is spraakherkenning.
- Veiliginternetten, (Onbekend) Wat is biometrische authenticatie? En wanneer gebruik je het?
- Cie-group, (Onbekend) Access control contactless authentication methods
- Robert Chamberlin, (2024) Key differences between on-premise and cloud based access control systems
- Sailpoint, (2025) Cloud based access control vs. on-premise
- Ian Craggs, (2022) MQTT vs CoAP for IoT
- Sob, (2017) What are the differences between MQTT, HTTP, CoAP devices (besides communication protocol)?
- Biometrisc Institute, (Onbekend), Types of Biometrics
- Jonathan Beri, (2020) A field Guide to CoAP – Part 1
- Thingsdata, (Onbekend) LoRa
- Bram, (2022) Wat is het protocol Zigbee en wat kun je ermee
- Alexandra Mendes, (2025) Best Types of Software Architecture Patterns Explained