Biometrisch Toegangssysteem  
Onderzoek naar de ontwikkeling van een veilig en schaalbaar biometrisch toegangscontrolesysteem

O-PP-CMK

Biometrisch toegangssysteem

Piotr Tadrala | InforDB

2025

# I. Management & Samenvatting

//TODO: Compleet samenvatting

# II. Versiebeheer & Distributie

## Versiebeheer

|  |  |  |
| --- | --- | --- |
| Versie | *Omschrijving* | *Auteur* |
| 0.1 | Eerste opzet van het document | Piotr Tadrala |
| 0.2 |  |  |
| 0.3 |  |  |

## Distributiebeheer

|  |  |
| --- | --- |
| Versie | *Ontvangers* |
| 0.1 |  |
| 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 |

Inhoudsopgave

[I. Management & Samenvatting 1](#_Toc192229281)

[II. Versiebeheer & Distributie 2](#_Toc192229282)

[Versiebeheer 2](#_Toc192229283)

[Distributiebeheer 2](#_Toc192229284)

[III. Woordenlijst 3](#_Toc192229285)

[1.0 Inleiding 5](#_Toc192229286)

[2.0 Context 6](#_Toc192229287)

[2.1 Inleiding 6](#_Toc192229288)

[2.2 Huidige situatie 6](#_Toc192229289)

[2.3 Probleemstelling 6](#_Toc192229290)

[2.4 Doelstelling 6](#_Toc192229291)

[3.0 Onderzoeksaanpak 7](#_Toc192229292)

[3.1 Inleiding 7](#_Toc192229293)

[3.2 Hoofdvraag 7](#_Toc192229294)

[3.3 Deelvragen 7](#_Toc192229295)

[3.4 Onderzoeksmethoden 7](#_Toc192229296)

[3.5 Verwachte onderzoeksuitkomsten 7](#_Toc192229297)

[3.6 Scope 8](#_Toc192229298)

[3.7 Conclusie 8](#_Toc192229299)

[4.0 Zijn er al vergelijkbare systemen op de markt? 9](#_Toc192229300)

[4.1 Inleiding 9](#_Toc192229301)

[4.2 Bestaande oplossingen 9](#_Toc192229302)

[4.3 Good & Bad practices 9](#_Toc192229303)

[4.4 Huidige Marktstandaarden 10](#_Toc192229304)

[4.5 Conclusie 10](#_Toc192229305)

[5.0 Welke verificatiemethodes zijn er beschikbaar? 11](#_Toc192229306)

[x.0 Bronnen 12](#_Toc192229307)

# 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 applicaties 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 het enkele white-label applicaties ontwikkeld die door verschillende organisaties worden gebruikt.

Het bedrijf ziet er 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 er 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.

# 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.

## 2.3 Probleemstelling

Huidige biometrische toegangssystemen zijn niet voldoende bestaand tegen misleidpogingen, zoals deepfakes en spoofing. Daarnast zijn er veel systemen afhankelijk van één enkele verificatiemethode waardoor de veiligheid beperkt blijft.

## 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 maatregelen kunnen worden genomen om biometrische data te beschermen tegen vervalsing en diefstal? |
| **D4** | Welke software- en hardwarearchitectuur & platform is het meest geschikt voor een schaalbaar en uitbreidbaar toegangscontrolesysteem? |
| **D5** | Welke componenten zijn er nodig 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 eerder 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.

## 3.7 Conclusie

Dit hoofdstuk heeft de hoofd- en deelvragen in kaart gebracht en de onderzoeksmethoden bepaald. Het onderzoek richt zich op het ontwikkelen van een veilig en gebruiksvriendelijk biometrisch toegangscontrolesysteem dat bestand is tegen misleiding en eenvoudig te integreren is.

Door middel van literatuuronderzoek, data-analyse en prototyping worden bestaande systemen, verificatiemethoden, anti-spoofingtechnieken en geschikte software- en hardwareoplossingen onderzocht. De uitkomsten vormen de basis voor een functioneel prototype.

# 4.0 Zijn er al vergelijkbare systemen op de markt?

## 4.1 Inleiding

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

## 4.2 Bestaande oplossingen

#### Paxton

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

Paxton, ( Onbekend ) [Hoe maak ik een veilig toegangscontrole systeem nog veiliger?](https://www.paxton-access.com/nl/technische-support/veiligere-toegangscontrole/)

#### 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.

Anviz, ( Onbekend ) [Slimme oplossing voor toegangscontrole](https://www.anviz.com/nl/access-control-solution.html)

#### 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, ( Onbekend ) [Biometrische toegangscontrole](https://www.boschsecurity.com/nl/nl/oplossingen/toegangscontrolesystemen/biometric-access-control/)

## 4.3 Good & Bad practices

#### Paxton

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

#### 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.

## 4.5 Conclusie

Bestaande systemen bieden goede API-integraties, maar anti-spoofing blijft vaak beperkt tot liveness-detectie op gezichtskenmerken. MFA is nog geen standaard en wordt meestal beperkt tot traditionele technieken smartcards en PIN-codes. Hoewel er stappen worden gezet richting betere beveiliging, ontbreekt er in meeste gevallen MFA en geavanceerde anti-spoofing.

# 5.0 Welke verificatiemethodes zijn er beschikbaar?

# x.0 Bronnen

* Paxton, ( Onbekend ) [Hoe maak ik een veilig toegangscontrole systeem nog veiliger?](https://www.paxton-access.com/nl/technische-support/veiligere-toegangscontrole/)
* Anviz, ( Onbekend ) [Slimme oplossing voor toegangscontrole](https://www.anviz.com/nl/access-control-solution.html)
* Bosch, ( Onbekend ) [Biometrische toegangscontrole](https://www.boschsecurity.com/nl/nl/oplossingen/toegangscontrolesystemen/toegangscontrolesoftware/)