Biometrie voor identiteitsverificatie

Verkenning van de mogelijkheden

Colofon

DATUM	20 januari 2020
VERSIE	1.1
PROJECT REFERENTIE	201800267.018.075
VERTROUWELIJKHEID	Publiek
STATUS	Eindversie
BEDRIJF	InnoValor
AUTEUR(S)	Bob Hulsebosch, Olga Kulyk, Henny de Vos

Inhoudsopgave

Managementsamenvatting

Inleiding biometrie

Het idee om de identiteit van personen te verifiëren aan de hand van hun lichamelijke kenmerken is bepaald niet nieuw. Volgens historici gebruikten Babylonische koningen vinger- en handafdrukken al meer dan 1700 jaar voor Christus om hun identiteit te bewijzen. Zij brachten de afdruk van hun hand aan op kleitabletten om deze een officiële status te geven. De meest gebruikelijke methode in de fysieke wereld was om op iemands geheugen te vertrouwen om de verschillende kenmerken en fysieke details van een andere persoon te identificeren. Tegenwoordig regelen computers en mobiele telefoons de identificatie van personen, waarbij lichamelijke kenmerken, ofwel biometrie, steeds vaker een onderdeel zijn. Vooral de introductie van biometrie in het consumentendomein door Apple heeft gezorgd voor een hernieuwde interesse in de mogelijkheden ervan. Biometrie op basis van vingerafdruk- en gezichtsherkenning is inmiddels gemeengoed en geadopteerd door vele mobiele gebruikers. Bijvoorbeeld mobiele apps voor bankieren gebruiken al volop de biometrische mogelijkheden van mobiele telefoons. Toepassingen van andere vormen van biometrie, zoals irisscan in combinatie met gezichtsherkenning zijn bij de e-gates op meerdere internationale luchthavens te vinden.

Biometrie verwijst naar metingen aan eigenschappen van het menselijk lichaam en gedrag. Biometrische persoonsgegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Deze kenmerken zijn uniek identificerend en worden gebruikt in biometrische systemen om iemand te herkennen en de identiteit vast te stellen.

Dit rapport verkent de mogelijkheden voor het inzetten van biometrie voor het verifiëren van de identiteit bij overheidsdiensten. Het richt zich daarbij op overheidsdiensten waarbij het vaststellen van de identiteit van één persoon centraal staat. Dit wordt ook wel aangeduid als 1-op-1 identificatie in de fysieke wereld of authenticatie in de digitale wereld. Andere vormen van biometrische identificatie zoals 1-op-n of n-op-n voor bijvoorbeeld forensisch onderzoek, opsporing of medische doeleinden vallen buiten de scope van het onderzoek. Dit onderzoek is uitgevoerd in opdracht van de Ministerie van de Binnenlandse Zaken en Koninkrijksrelaties.

Karakteristieken biometrie

Biometrie kent een aantal karakteristieken om rekening mee te houden bij het inzetten ervan voor het verifiëren van de identiteit. Onderstaand worden de belangrijkste benoemd:

- Biometrie is niet binair: in tegenstelling tot het gebruik van een wachtwoord of PIN levert biometrie geen binair goed of fout antwoord, maar een waarschijnlijkheid dat het iemand betreft. Er bestaat een kans op een onterecht match (False Acceptance Rate of FAR) of een onterecht afwijzing (False Rejection Rate of FRR). Daarnaast werkt biometrie gewoonweg niet bij bepaalde gebruikersgroepen (Failure To Enroll of FTE) waardoor er altijd een alternatief scenario moet blijven bestaan.
- Biometrie is niet geheim: daar waar wachtwoorden of PINs geheim zijn, is de biometrische factor dat niet. Er moet rekening worden gehouden met zogenaamde risico's als het hergebruik van biometrie door anderen (door een foto te laten zien van iemand anders).
- Biometrie is privacygevoelig: het verwerken van persoons- en biometrische gegevens is privacygevoelig en vereist passende maatregelen. De diverse manieren van opslag (centraal vs. decentraal) en verwerking van biometrische gegevens bepalen de gevoeligheid en welke maatregelen nodig zijn.

Biometrische modaliteiten

Er zijn verschillende vormen van biometrie om iemands identiteit te verifiëren. Om deze onderling te kunnen vergelijken is een beoordelingskader ontwikkeld. De onderstaande tabel geeft een overzicht van de meest gebruikte biometrische modaliteiten aan de hand van het beoordelingskader. De beoordeling in termen van goed, matig en onvoldoende (respectievelijk groen, oranje, rood) is relatief ten opzichte van andere modaliteiten. Bijvoorbeeld, de universaliteit van vingerafdruksensoren en gezichtsherkenning is door het gebruik ervan in mobiele telefoons veel beter dan die van handaderherkenning. Of, de privacy van een gezicht is veel minder goed te borgen dan dat van een vingeraderpatroon dat minder eenvoudig te verkrijgen is. Vanzelfsprekend is het van een concrete toepassing afhankelijk welke criteria belangrijker zijn.

Biometrische modaliteit	Beoordelingskader (kolommen)					
	Betrouwbaar-heid	Privacy	Veiligheid	Universaliteit	Gebruiksgemak	Praktische toepasbaarheid
Vingerafdruk						
Irisscan						
Netvliesscan						
Vingeraderpatronen						
Handaderherkenning						
Oogaderpatronen						
Gezichtsherkenning						
Hartslagherkenning						
Sprekerherkenning						
Handtekening						
Gebruikersinteractie						
Gebarenherkenning						

Uit de tabel volgt dat vingerafdruk, irisscan, gezichtsherkenning en oogaderpatroon de best beoordeelde modaliteiten zijn. Waarbij vingerafdruk en gezichtsherkenning erg populaire modaliteiten zijn voor mobiele biometrie; de andere modaliteiten worden vaker ingezet bij maatwerkoplossingen. Iris en oogaderpatroon zijn meer invasief voor de gebruiker en zijn op dit moment minder breed geadopteerd. Het combineren van meerdere biometrische modaliteiten – zoals vingerafdruk en vingeraderpatroon – is mogelijk om de betrouwbaarheid te vergroten. Andere modaliteiten zoals gebruikersinteractie en sprekerherkenning (wie spreekt), niet te verwarren met spraakherkenning (wat wordt er gezegd), scoren minder goed door de gevoeligheid van het registreren van het gedrag en matige gebruikersacceptatie.

Nieuwe ontwikkelingen

De opmars van kunstmatige intelligentie technologieën en real-time verwerking van grote hoeveelheden data hebben een positieve invloed op de betrouwbaarheid van de biometrische verificatie van de identiteit. Denk hierbij aan 3D gezichtsmodulering en meer geavanceerde biometrische algoritmes. Daarnaast worden ook de biometrische sensoren steeds hoogwaardiger. Er bestaan slimme privacy enhancing technologieën die bepaalde cryptografische verwerkingen op biometrische gegevens mogelijk maken om de privacy van de gebruiker beter te kunnen waarborgen.

Wettelijk kader, richtlijnen en standaarden

Het toepassen van biometrie en het verwerken van biometrische gegevens kent uitgebreide wet- en regelgeving. Denk aan de paspoort- en rijbewijzenwet waarin wordt gesteld hoe vingerafdrukken, pasfoto's en handtekeningen worden afgenomen en verwerkt. Opslag ervan vindt plaats op de chip van het identiteitsdocument. De onlangs in werking getreden EU verordening 2019/1157 verplicht het plaatsen van vingerdrukken op identiteitskaarten en wordt momenteel geïmplementeerd in Nederland. Hiermee neemt de beschikbaarheid van biometrische templates op wettelijke identiteitsdocumenten verder toe. Echter, de toegang ertoe en het gebruik ervan is wisselend. Toegang tot de pasfoto op de chip is geen probleem. Vingerafdrukken laten zich op dit moment minder eenvoudig ontsluiten; de-facto kunnen alleen gemeenten hier nu bij. Dientengevolge wordt alleen de pasfoto gebruikt voor identificatie- en authenticatiedoeleinden. De AVG bepaalt dat de verwerking van biometrische persoonsgegevens een verwerking van bijzondere persoonsgegevens is.

Volgens de AVG is het verwerken van biometrische gegevens om iemand te identificeren in beginsel verboden. Nederland heeft in de Uitvoeringswet AVG bijkomende voorwaarden hierover vastgesteld. Het verbod op het verwerken van biometrische gegevens is in Nederland niet van toepassing als de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Huidige internationale standaarden en richtlijnen voor biometrie zijn vooral gericht op gezicht- en vinger-biometrie en worden nog onvoldoende breed toegepast.

Bronnen biometrie

De volgende overheidsbronnen voor de biometrische verificatie van de identiteit zijn aanwezig, opsporing en grenscontrole zijn buiten de scope:

Bron biometrische gegevens	Architectuur	Soort gegeven	Partijen met toegang
Paspoort, Identiteitskaart, Rijbewijs, Verblijfsdocument	Decentraal	Gezicht	Iedereen die toegang heeft tot de chip, altijd op basis van MRZ.
Paspoort, Identiteitskaart	Decentraal	Vingerafdruk	KMar, gemeenten, Nederlandse ambassades en consulaten, uitgevende instanties in het Caribisch deel.
Verblijfsdocument	Decentraal	Vingerafdruk	IND, BZ, KMar, Nederlandse ambassades en consulaten, uitgevende instanties in het Caribisch deel.
Paspoort, Identiteitskaart, Rijbewijs, Verblijfsdocument	Decentraal	Handtekening	KMar, gemeenten, IND, Nederlandse ambassades en consulaten, uitgevende instanties in het Caribisch deel.
BVV	Centraal	Vingerafdruk	IND
RDW database	Centraal	Gezicht	RDW, Politie
Reisdocumenten Aanvraag- en Archiefstation (RAAS)	Centraal	Gezicht, Handtekening	Gemeenten, BZ, KMar. Vingerafdrukslechts tot het document is uitgegeven en max 90 dagen.

Toegang tot de chip in het paspoort in Nederland is voorbehouden aan gemeenten. Justitionele Informatiedienst regelt deze toegang. Drie biometrische modaliteiten zijn inzetbaar voor het verifiëren van de identiteit: vingerafdruk, gezicht en handtekening. Huidige bronnen van biometrische gegevens zijn zowel centraal als decentraal ingericht en niet verbonden met elkaar.

Use-cases biometrie

Om de toepasbaarheid van biometrische oplossingen voor het verifiëren van de identiteit verder te duiden zijn een tweetal use-cases in het overheidsdomein gedefinieerd. Per toepassing is bekeken of en hoe biometrie een bijdrage kan leveren om tot verdere optimalisatie van de huidige use-cases te komen, bijvoorbeeld door identificatie en authenticatie gebruikersvriendelijker, betrouwbaarder, of sneller te maken.

Een belangrijke toepassing betreft de aanvraag, het gebruik en de vernieuwing van identiteitsdocumenten, met name paspoort en identiteitskaart. Identiteitsdocumenten zoals het rijbewijs en de verblijfsvergunning vallen buiten de scope van deze verkenning, hoewel er natuurlijk ook raakvlakken zijn. Uit de analyse van deze toepassing komen de volgende aanbevelingen naar voren in relatie tot het gebruik van biometrie:

- Aanvraag: Zorg gedurende de registratie voor zo hoog mogelijke kwaliteit bij het vastleggen van de biometrische kenmerken.
- Aanvraag: De aanlevering van biometrie is gevoelig voor lage kwaliteit en manipulatie ten behoeve van fraude of, soms, ijdelheid. Beiden zijn te voorkomen door de aanlevering ter plekke te doen. Dit gebeurt al bij (het afnemen van) vingerafdrukken, maar nog niet bij (het maken van) pasfoto's. Een alternatief is het gecontroleerd aanleveren van de pasfoto middels erkende fotografen, zoals bijvoorbeeld bij het rijbewijs gebeurt.
- Uitgifte: Verbeter de identificatie van de gebruiker bij het overhandigen van het identiteitsdocument door biometrie in te zetten (vinger of gezicht).
- Gebruik (offline): Stimuleer het gebruik van de biometrie op de chip van het identiteitsdocument zodat betrouwbaardere identificatie mogelijk wordt (in plaats van op basis van geprinte biometrie op het identiteitsdocument of, nog minder betrouwbaar, een kopie van het document).
- Gebruik (online): Controleer de echtheid van het identiteitsdocument via de chip en zorg voor adequate 'presentation attack detection' (PAD) door bijvoorbeeld een goede liveness check uit te voeren.
- Vernieuwing: Maak met behulp van biometrie het proces van vernieuwing gedeeltelijk online mogelijk. Hierdoor hoeft de burger maar één in plaats van twee keer naar de balie te komen voor aanvraag en ophalen van het vernieuwde identiteitsdocument. Voor het rijbewijs wordt hier al mee geëxperimenteerd.
- Vernieuwing: Laat de gebruiker diens nieuwe pasfoto digitaal aanleveren via een erkende fotograaf en vergelijk deze met de oude, doormiddel van gezichtsherkenning. De oude pasfoto kan uit de chip worden uitgelezen of uit de systemen van betreffende gemeente worden gehaald om biometrisch te vergelijken met de nieuwe.

- Vernieuwing: Hergebruik de vingerafdruk templates van het oude identiteitsdocument; toegang tot de vingerafdruk op de chip is hiervoor noodzakelijk.

Nederland kent op dit moment een relatief decentrale aanpak voor het verwerken van biometrische gegevens. Pasfoto's zijn, naast opslag in de chip van het identiteitsdocument, ook semi-decentraal opgeslagen bij de gemeenten; vingerafdrukken staan alleen op de chip en dus helemaal decentraal. Een dergelijke decentrale aanpak kent diverse voor- en nadelen in termen van privacy, beveiliging en fraudedetectie. Echter, hetzelfde geldt voor een eventuele centrale aanpak voor biometrische gegevensopslag.

Een tweede relevante toepassing betreft de aanvraag, het gebruik en de vernieuwing van nationaal erkende digitale authenticatiemiddelen met een substantieel of hoog betrouwbaarheidsniveau:

- Aanvraag: Identificatie op afstand in plaats van fysiek aan de balie is mogelijk met behulp van biometrie en op basis van de pasfoto uit de chip van het identiteitsbewijs.
- Aanvraag: Controleer de echtheid van het identiteitsdocument via de chip in combinatie met de liveness detectie om fraude te voorkomen.
- Aanvraag: Zorg voor 'fall-back' scenario's in het geval een persoon zich via gezichtsbiometrie niet kan registreren. In plaats van gezicht, zou de vingerafdruk als alternatief kunnen worden ingezet. Dit laatste pleit voor ruimere ontsluiting van de vingerafdruk.
- Gebruik: Gebruik gezicht of vingerafdruk als tweede authenticatiefactor bij inloggen. Gebruik biometrie nooit als enige authenticatiefactor.
- Gebruik: Mensen vergeten door gebruik van biometrie snel de alternatieve 'wat-je-weet' factor (b.v. PIN), laat daarom de authenticatie software regelmatig (e.g. elke week) om een PIN vragen.
- Vernieuwing: Idem als aanvraag authenticatiemiddel.
- Vernieuwing: Gebruik biometrie voor een PIN- of wachtwoord-reset om het doorlopen van een volledig nieuwe registratie bij vergeten ervan te voorkomen.

Betrouwbaarheidsniveaus en biometrie

Authenticatiemiddelen worden geclassificeerd in termen van betrouwbaarheidsniveaus voor identiteitszekerheid: laag, substantieel of hoog. De bestaande normenkaders hiervoor bieden echter weinig houvast als het gaat om biometrie. Bijvoorbeeld, welke False Acceptance Rate is vereist om te voldoen aan niveau hoog? En hoe moet dit gemeten worden? En welke beveiligingsmaatregelen zijn vereist om te weerstand te bieden tegen een aanvaller met een substantieel respectievelijk hoog aanvalsprofiel tijdens de uitgifte en het gebruik van het middel? Om voor erkenning onder de Europese eIDAS verordening of de toekomstige wet Digitale Overheid in aanmerking te komen dienen authenticatiemiddelen te voldoen aan een bepaalde betrouwbaarheid. Zonder normen voor biometrie is het betrouwbaarheidsniveau lastig te bepalen en mogelijk een belemmering voor erkenning en adoptie ervan voor toegang tot overheidsdiensten. *Vereist is dus dat er normen komen om op biometrie gebaseerde authenticatieoplossingen in te schalen in termen van betrouwbaarheidsniveaus.* Dit betreft de uitgifte en het gebruik van het authenticatiemiddel.

Samenvatting

Het gebruik van biometrie voor identificatie- en authenticatiedoeleinden wordt steeds meer geaccepteerd. Belangrijke drijfveer hiervoor zijn de van vingerafdruk- en gezichtsherkenning voorziene mobiele telefoons die zorgen voor een groot bereik onder gebruikers. Door het gemak wordt biometrie steeds meer gemeengoed als een tweede authenticatiefactor, onder meer bij banken die er gebruik van maken voor toegang tot betaaldiensten en op afstand verifiëren van identiteit voor aanvragen bankrekeningen. Aandachtspunten zijn er nog wel aangaande de betrouwbaarheid van biometrie, normen hiervoor die de betrouwbaarheid op een objectieve manier kwantificeren inclusief Presentation Attack Detection (PAD), dat biometrie voor sommige mensen faalt (inclusie) en privacy. Met betrekking tot privacy is met name de manier van verwerking van biometrische data (centraal of decentrale opslag) een aandachtspunt, naast nieuwe privacy enhancing technologieën om de opslag op een privacy-vriendelijke manier te doen. Dat neemt niet weg dat biometrie zinvol kan worden ingezet om bestaande overheidsprocessen rondom de aanvraag, het gebruik en de vernieuwing van identiteitsdocumenten en authenticatiemiddelen te optimaliseren in termen van betrouwbaarheid, doorlooptijd en gebruikersvriendelijkheid.

1. Inleiding

Het idee om personen te identificeren aan de hand van hun lichamelijke kenmerken is bepaald niet nieuw. Volgens historici gebruikten Babylonische koningen vinger- en handafdrukken al meer dan 1700 jaar voor Christus om hun identiteit te bewijzen. Zij brachten de afdruk van hun hand aan op kleitabletten om deze een officiële status te geven, als een vorm van handtekening. Tegenwoordig regelen computers en mobiele telefoons de identificatie van personen.

Vooral de introductie van Apple's toegankelijke TouchID technologie op mobiele telefoons heeft geresulteerd in een opleving van op biometrie gebaseerde identificatie voor grootschalig gebruik. Ook hebben nieuwe standaarden, zoals FIDO[1], de potentie om de integratie van biometrische identificatie in online dienstverlening te vergemakkelijken door standaard interfaces aan te bieden voor (web)app programmeurs.

Het inzetten van biometrie en de bijbehorende nieuwe mogelijkheden biedt kansen voor de Nederlandse Overheid, in het bijzonder voor de afdeling Identiteit van de directe samenleving en Overheid van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK), om het zaken doen met de overheid veiliger en/of makkelijker te maken. Het biedt in het bijzonder mogelijkheden voor processen waarbij identificatie en authenticatie belangrijk zijn. Tegelijkertijd zijn biometrische gegevens persoonlijke data, waar zorgvuldig mee om dient te worden gegaan, en zijn er ondanks de forse opkomst van biometrische technologieën nog de nodige vraagtekens rondom de betrouwbaarheid.

Enkele jaren geleden zijn er diverse onderzoeken over biometrie uitgevoerd, waaronder die van de Wetenschappelijke Raad voor het Regeringsbeleid[2] (WRR) in 2010: "Het biometrisch paspoort in Nederland: crash of zachte landing". Recentere onderzoeken die zich richten op de publieke sector zijn niet bekend. Daarnaast gaan de ontwikkelingen snel. Naast de biometrie die al wordt gebruikt bestaan tegenwoordig ook andere mogelijkheden. Daarom gaf het ministerie van Binnenlandse Zaken en Koninkrijksrelaties opdracht aan InnoValor om onderzoek uit te voeren naar de theoretische en praktische mogelijkheden van biometrie voor identificatie en authenticatie bij overheidsdiensten.

1.1 Doel en scope van het onderzoek

Het doel van het onderzoek was de theoretische en praktische mogelijkheden van op biometrie gebaseerde technologieën voor identificatiedoeleinden ten behoeve van overheidsdienstverlening in kaart te brengen.

Het onderzoek is opgezet rondom de vraag:

Welke mogelijkheden zijn er in de biometrie voor identificatie van een persoon in theorie én in de praktijk?

Met 'theorie en in de praktijk' wordt bedoeld dat we kijken naar oplossingen die nu al in de praktijk worden ingezet, maar ook naar mogelijkheden die nog in de onderzoeks- of ontwikkelfase zitten en die in de komst wellicht beschikbaar worden voor de praktijk. In dat laatste geval zullen we in het algemeen ingaan op de verwachte bruikbaarheid met de bijbehorende verwachte voor- en nadelen. Voor de oplossingen die al in de praktijk beschikbaar zijn, wordt er een beeld geschetst van de oplossingen en waar deze worden ingezet, al dan niet in combinatie met een andere manier van identificeren (code, wachtwoord). Met daarbij de voor- en nadelen van de methoden, zoals die in de praktijk worden ervaren. We kijken daarbij naar de private sector in Nederland en andere landen en naar de publieke sector in andere landen. Biometrie voor forensisch onderzoek, opsporing of medische doeleinden valt buiten de scope van het onderzoek.

Het wettelijke kader van het toepassen van biometrie beschrijven we op hoofdlijnen. Specifieke juridische aspecten kunnen pas in detail worden onderzocht op basis van details van een voorgestelde

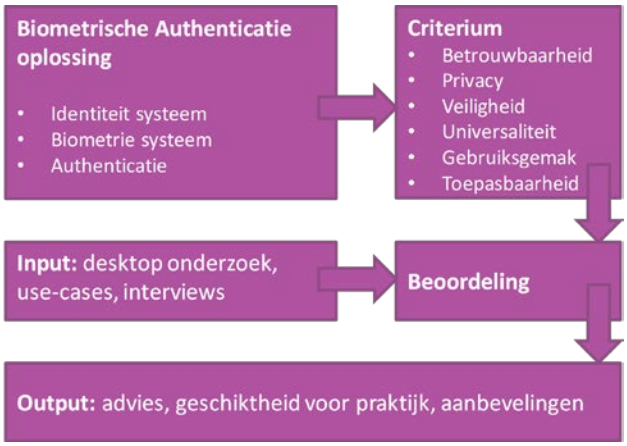
[1] FIDO Alliance, zie: https://fidoalliance.org/.
[2] WRR (2010) zie: https://www.wrr.nl/binaries/wrr/documenten/publicaties/2010/11/01/het-biometrisch-paspoort-in-nederland-crash-of-zachte-landing---51/Web051-Biometrisch-paspoort-Nederland.pdf.

beleidsoplossingen. Wij beschrijven de biometrische modaliteiten en mogelijkheden en gaan niet in op specifieke oplossingen van leveranciers.

Voor het beoordelen van de verschillende biometrische mogelijkheden maken we gebruik van een beoordelingskader die samen met een klankbordgroep is opgesteld.

1.2 Aanpak

Het onderzoek liep van januari 2019 tot en met september 2019. Figuur 1 vat het plan van aanpak voor het biometrie onderzoek samen. We schetsen de verschillende modaliteiten voor biometrie en analyseren onderscheidende kenmerken en voorwaarden. Hiervoor is gebruik gemaakt van desktop research en interviews met experts. Aan de hand van het beoordelingskader, vastgesteld op basis van de literatuur en interviewresultaten en afstemming met de stakeholders van de klankbordgroep, zijn de modaliteiten onderling beoordeeld. Vervolgens is voor een aantal use-cases beoordeeld welke biometrische oplossingen van meerwaarde zijn. Deze vormen de kern van het advies rondom de inzet van biometrie voor identificatie en authenticatie doeleinden bij de overheid.



Figuur 1: Plan van aanpak.

De begeleidingscommissie vanuit het ministerie van BZK is intensief betrokken geweest bij het tot stand komen van het plan van aanpak en tussentijdse resultaten. De resultaten zijn getoetst bij de klankbordgroep (zie Bijlage 2 Begeleidingscommissie en klankbordgroep).

De basis voor een overzicht van biometrische modaliteiten wordt gelegd door eerder onderzoek van InnoValor voor SURFnet[3]. Er wordt onderscheid gemaakt tussen oplossingen in de private sector in Nederland, de private sector in het buitenland, en de publieke sector in het buitenland. Via desktoponderzoek is dit verder aangevuld en uitgewerkt. Ook resultaten uit de interviews zijn hier verwerkt. Specifiek werd bij de geïnventariseerde oplossingen gekeken in welke sector ze worden ingezet (publiek, privaat), privacyaspecten, voor- en nadelen (betrouwbaarheid, snelheid van uitrollen en gebruik, etc.), wat de gebruikers ervan vinden en de veiligheidsaspecten. Naast oplossingen die al in gebruik zijn, zijn ook toekomstige oplossingen en oplossingen die nog in de ontwikkelingsfase zitten betrokken bij het onderzoek.

1.3 Leeswijzer

Na deze inleiding geeft hoofdstuk 2 een overzicht van de kenmerken van biometrie in het algemeen. Een beschrijving van de wettelijke context, standaarden, (internationale) richtlijnen, huidige biometrische bronnen, voor- en nadelen van centrale versus decentrale opslag van de biometrische gegevens staat in hoofdstuk 3. Hoofdstuk 4 geeft daarna een overzicht van de verschillende biometrische oplossingen. In hoofdstuk 5 gaan we in op het beoordelingskader. Hoofdstuk 6 beschrijft de use-cases. We ronden het onderzoek af in hoofdstuk 7 met conclusies, aanbevelingen en discussie.

[3] Zie: https://www.surf.nl/biometrie-voor-sterke-authenticatie-een-analyse.

2. Biometrie: essentiële aspecten en toekomstperspectief

In dit hoofdstuk schetsen we de context en kenmerken van biometrie en gaan we in op een de essentiële aspecten zoals prestatie, privacy, kwetsbaarheden, mitigerende maatregelen en de nieuwste ontwikkelingen. We starten met een introductie van biometrie voor identificatiedoeleinden.

2.1 Begrippen biometrie

Dit zijn de meest belangrijke biometrie begrippen:

Authenticatie: Er zijn meerdere definities bekend in de literatuur. Volgenst NIST betekent de *authenticatie*[4] het verifiëren van de identiteit van een gebruiker, proces of apparaat, vaak als een voorwaarde om toegang te bieden tot de bronnen van een systeem. *Digitale authenticatie* stelt vast of een persoon die toegang probeert te krijgen tot een digitale service, controle heeft over een of meer geldige authenticators die zijn gekoppeld aan de digitale identiteit van die persoon.
Binnen dit project houden we de definitie van de Nederlandse overheid (Logius, Min. van BZK)[5] aan: *authenticatie* is het proces waarbij nagegaan wordt of een persoon daadwerkelijk is wie hij/zij beweert te zijn, dat wil zeggen: daadwerkelijk de identiteit bezit die hij/zij opgeeft. Bij de authenticatie wordt bijvoorbeeld gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken. Voor authenticatie wordt daarom ook wel de term *verificatie* gehanteerd.

Authenticator: iets dat de eiser (gebruiker) bezit en beheert (meestal een cryptografische module of een wachtwoord) die wordt gebruikt om de identiteit van de eiser (gebruiker) te verifiëren. In eerdere NIST definities werd dit een *token* genoemd.

Verificatie: de identiteit van een al bekend persoon vaststellen doormiddel van 1-op-1 vergelijking. Ook wel 1-op-1 identificatie genoemd, of het controleren van de identiteit.

Identificatie: de identiteit van een nog onbekend persoon vaststellen. Ook wel 1-op-n identificatie genoemd.

Biometrische identiteit: Unieke set van onveranderlijke dan wel langdurig stabiele fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Deze kenmerken zijn uniek identificerend en worden gebruikt in biometrische systemen om iemand te herkennen en de identiteit vast te stellen.

Failure to enroll: onmogelijkheid tot afname van een biometrisch kenmerk.

False Acceptance Rate: kans op het ten onrechte accepteren van een persoonsherkenning.

False Rejection Rate: kans op het ten onrechte verwerpen van een persoonsherkenning.

Fall back: teruggrijpen op een andere methode als de (sensor) apparatuur en/of software niet werkt of de afname van een biometrisch kenmerk onmogelijk is.

Spoofing: als een ander voordoen door een biometrisch kenmerk na te maken of her te gebruiken.

Presentation Attack Detection: de controles die een biometrisch systeem uitvoert om er zeker van te zijn dat het te maken heeft met een levend persoon of dat er geen manipulatie van de biometrische identiteit plaats vindt.

[4] Grassi, P.A., Garcia, M.E., Fenton, J.L. *Digital Identity Guideline*, NIST Special Publication 800-63-1, 2017, zie: https://doi.org/10.6028/NIST.SP.800-63-3.
[5] Digikoppeling identificatie en authenticatie, Logius, Min. BZK, 2017. Zie: https://www.logius.nl/diensten/digikoppeling/documentatie.

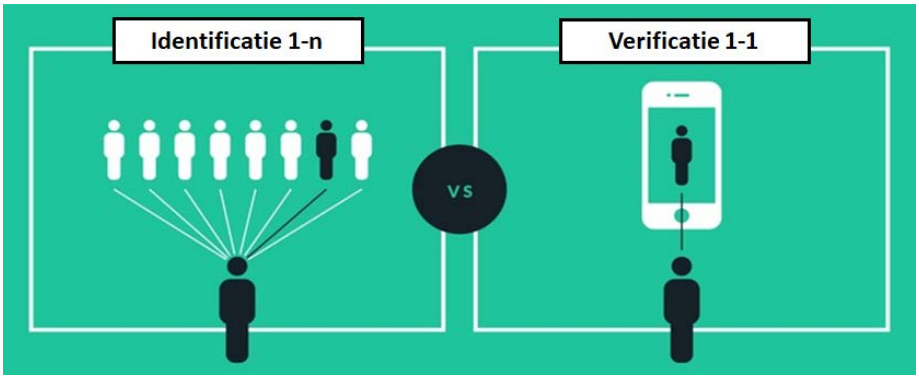
Mobiele biometrie: vaststellen/controleren van biometrische kenmerken middels het gebruik van de mobiele telefoon.

Internet of Things (IoT): netwerk van fysieke objecten die ingesloten technologie bevat om te communiceren met de interne toestand of de externe omgeving.

Artificial Intelligence (AI): De theorie en ontwikkeling van computersystemen die in staat zijn taken uit te voeren die normaal menselijke intelligentie vereisen, zoals visuele perceptie, spraakherkenning, besluitvorming en vertaling tussen talen.

2.2 Biometrie en identificatie

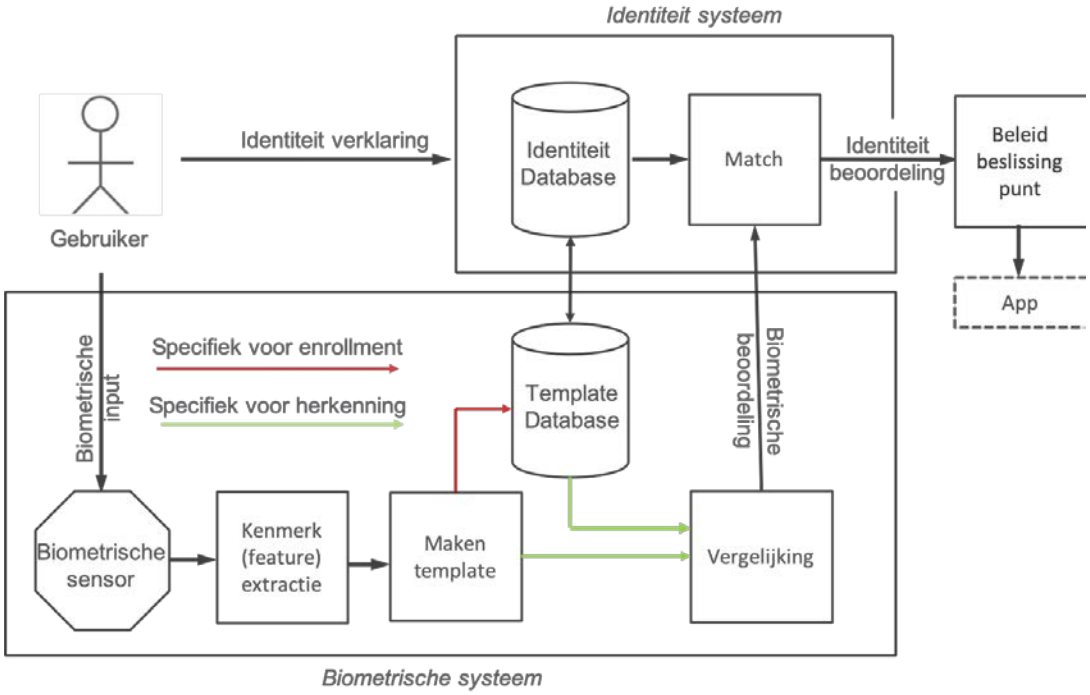
Biometrie verwijst naar metingen aan eigenschappen van het menselijk lichaam en gedrag. Biometrische persoonsgegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Deze kenmerken zijn identificerend, immers ze zijn uniek voor de persoon, en worden gebruikt in biometrische systemen om iemand te herkennen en de identiteit vast te stellen (**identificatie**). **Verificatie** is het controleren of een persoon is wie hij/zijn claimt te zijn (zie Figuur 2). Dit is het controleren van de identiteit, ook wel **authenticatie** genoemd in de online wereld. Het gaat om het vaststellen van de identiteit van één persoon, aangeduid als 1-op-1 verificatie, waarbij de gemeten biometrische data vergeleken met de eerder stadium vastgestelde (enrolled) biometrische data van de persoon. In tegenstelling tot 1-op-n, waarbij de gemeten biometrische wordt vergeleken met die van meerdere personen, om de identiteit te bepalen. De 1-op-1 identificatie wordt vaak verificatie genoemd in de literatuur, en 1-op-n wordt identificatie genoemd. De n-op-n situatie bestaat ook. In dat geval is de identiteit van de persoon onbekend en zoekt het systeem of er op basis van de biometrische kenmerken een match met een persoon gevonden kan worden. N-op-n wordt vaak toegepast voor opsporingsdoeleinden en valt buiten de scope van dit onderzoek.



Figuur 2: Identificatie (1-op-n) vs. verificatie (1-op-1).

2.3 Biometrisch systeem

Biometrische oplossingen werken altijd in twee fasen: registratie (enrolment), waarin de biometrische kenmerken van een persoon worden vastgelegd ten behoeve van latere verificatie en herkenning waarbij een persoon biometrische kenmerken afgeeft die worden vergeleken met de kenmerken van de enrolment. Figuur 3 toont een schematisch model van een biometrisch systeem voor de verificatie van de identiteit. Hierin zijn de fases voor de uitrol van de biometrisch identiteit (enrolment) en de verificatie ervan aangegeven. Bij de enrolment wordt via de sensor de biometrie van de gebruiker vastgelegd in een template database. Deze template is gekoppeld aan de identiteit van de gebruiker. Tijdens de verificatie wordt door de gebruiker aangeleverde biometrie vergeleken met de template in de database. In het geval van een match, wordt de identiteit van de gebruiker gecommuniceerd richting de toepassing voor bijvoorbeeld het verstrekken van toegang.



Figuur 3: Schematisch model van een biometrisch systeem voor de verificatie van de identiteit bestaande uit een enrolmentfase en een verificatiefase.

Een biometrisch systeem kan specifiek voor één toepassing worden ingezet, zoals Privium op Schiphol, of het kan worden hergebruikt voor meerdere toepassingen zoals Apple's TouchID op de mobiele telefoon.

2.4 Classificatie van de biometrische systemen en modaliteiten

In het algemeen zijn er twee classificaties van biometrie. De eerste gaat over wat er wordt gemeten:

- *Fysiologische biometrie* meet interne (niet zichtbaar van buiten) en externe (zichtbaar van buiten) lichamelijke kenmerken van een persoon, waaronder:
  - Vingerafdruk, iris, gezichtsherkenning, sprekerherkenning (*extern*);
  - Aderpatroon (vinger, gezicht, oog), hartslag of DNA (*intern*).
- *Gedragsbiometrie* meet gedrag van een persoon zoals handtekening of gebruikersinteractie.

Het spreekt voor zich dat de externe biometrische oplossingen het meest kwetsbaar zijn voor fraude. Een vingerafdruk van een slachtoffer is eenvoudiger te verkrijgen dan het aderpatroon van diens vinger.

Daarnaast kenmerken biometrische systemen zich door:

- *Uni-modale*: slechts één biometrisch kenmerk wordt gebruikt;
- *Multi-modale*: meerdere biometrische kenmerken geïntegreerd in een biometrische toepassing, bijvoorbeeld door vingerafdruk te combineren met het hartslagsignaal vastgelegd van de vinger.

Volgende classificatie maakt onderscheid tussen *lokale* biometrie versus biometrie *op afstand* (online scenario). Het is van belang voor de controle over de verificatie en de toepasbaarheid van diverse biometrische sensor (zie Figuur 3) voor de fysieke versus online enrolment, identificatie en authenticatie:

- *Lokale biometrie*: biometrische kenmerken worden afgenomen en geverifieerd met behulp van een fysieke externe ('dedicated') sensor. In dit geval hebben de volgende organisaties controle over de biometrische sensor:
  - *Overheid*, bijv. in het geval van het afnemen van de vingerafdrukken bij de balie van de gemeente, of bij de verificatie van het gezicht doormiddel van de externe camera tijdens de grenscontrole in het vliegveld;
  - *Technologie leverancier*, zoals Apple in het geval van de verificatie van de vingerafdrukken met TouchID.

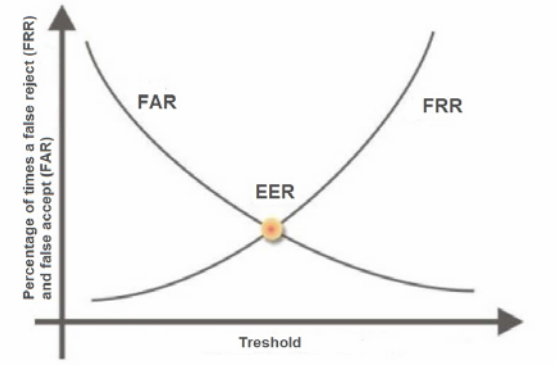
- *Biometrie op afstand (online)*: in dit geval ligt de controle over de (vaak mobiele) biometrische sensor bij de *gebruiker* zelf. Bijvoorbeeld, online authenticatie op afstand met behulp van een (mobiele) biometrische sensor (zie sectie 5.3).

2.5 Prestatie

Prestaties van de biometrische technologie worden kwantitatief gemeten. De meest gangbare prestatie-indicatoren voor 1-op-1 verificatie systemen zijn de False Acceptance Rate (FAR), False Rejection Rate (FRR), Failure To Enroll (FTE) en Presentation Attack Detection (PAD):

- *False Acceptance Rate*: betreft onnauwkeurigheid bij de verificatie, in het geval de biometrische meting wordt gematcht met de enrolled gegevens ondanks dat deze niet de persoon betreffen. De persoon krijgt onterecht toegang tot de dienstverlening, bijvoorbeeld doordat een afgenomen vingerafdruk onterecht wordt herkend en aan de verkeerde persoon wordt gerelateerd.
- *False Rejection Rate*: tegenstelling tot FAR, krijgt een persoon bij een FRR onterecht geen toegang omdat deze niet als zodanig biometrisch wordt herkend.
- *Failure to Enroll*: het is niet mogelijk om de biometrische gegevens van een persoon te enrollen en zo biometrische verificatie mogelijk te maken. Dit kan komen door een fysiek probleem, bijvoorbeeld een persoon kan geen vingerafdruk afgeven, een gebruikersprobleem, bijvoorbeeld iemand kan niet omgaan met de technologie die wordt gevraagd, of een technologisch probleem, bijvoorbeeld de technologie is van onvoldoende kwaliteit.
- *Presentation Attack Detection*: het controleren door het biometrische systeem of het een levend persoon betreft en er geen gebruik van afbeeldingen of, geavanceerder, maskers wordt gemaakt. Dit is een onmisbare risico-mitigerende maatregel van een betrouwbaar biometrisch systeem die misbruik van nagemaakte biometrische kenmerken moet voorkomen (zie sectie 2.8 voor verdere toelichting).

Het streven is om een juiste balans te vinden tussen FAR en FRR, afhankelijk van zelfgekozen drempel voor een bepaalde use-case. Het verlagen van de FAR gaat ten koste van de FRR. Het verhogen van FAR verlaagt de gebruikersvriendelijkheid. Prestatiekenmerken van biometrische oplossingen vertalen zich naar de betrouwbaarheid in onze beoordelingskader (zie hoofdstuk 4). Kritische applicaties vereisen een lage FAR wat een effect heeft op het verhoogde FRR, terwijl minder kritische applicaties minder veeleisend in termen van FAR zijn. De optimale prestatie van het biometrische systeem is afhankelijk van de toepassing. Vaak wordt er gestreefd de FAR gelijk te stellen aan de FRR voor optimale prestatie. Dit is de zogenaamde Equal Error Rate (EER). Onderstaande Figuur 4 wordt gebruikt ter visualisatie van FAR, FRR en EER.



Figuur 4: Visualisatie van de balans tussen FAR en FRR.

Naast de bovengenoemde metingen, wordt de prestatie van de biometrische oplossing ook beïnvloed door een aantal andere factoren (Corsetti et al., 2018). Deze factoren zijn gerelateerd aan de gebruikersinteractie met de biometrische applicatie (bijv. gebruikersacceptatie en tijd), ergonomie (bijv. de vorm van het apparaat, de maat van de biometrische sensor, postuur van de gebruiker tijdens interactie), en de doelgroep (bijv. hoog/laag opgeleid, kantoorwerkers of fabrieksarbeiders). Een sensor die te traag reageert op de biometrie van de gebruiker leidt vaak tot ontevredenheid (Conti et al., 2014). Van invloed zijn ook kwaliteit van de opname van de biometrische kenmerken, kwaliteit van de segmentatie van de kenmerken en de meetmethode van de kenmerken.

Het is belangrijk op te merken dat geen enkel biometrisch systeem 100% betrouwbaar of nauwkeurig is. Bij sommige mensen of zelfs bepaalde populaties ontbreken gewoonweg de specifieke biometrische kenmerken om ze uniek te kunnen identificeren, zoals gezichten van baby's (Spreeuwers, 2017). Daarnaast wordt de uitkomst van een biometrische match altijd in termen van waarschijnlijkheid uitgedrukt. Dit in tegenstelling tot een PIN of wachtwoord dat wel 100% goed moet zijn. Met andere woorden, biometrie is niet binair, een aspect om rekening mee te houden bij het inzetten ervan voor de verificatie van de identiteit.

2.6 Privacy

Privacy is een belangrijk aandachtspunt bij het verwerken van biometrische data voor de verificatie van de identiteit. Een informatiesysteem dat biometrische data opslaat en verwerkt impliceert potentiële privacy bedreigingen waarop moet worden geanticipeerd en die op gepaste wijze geadresseerd moeten worden. Biometrische gegevens bevatten vaak ook meer informatie dan strikt noodzakelijk is voor bijvoorbeeld identificatie. Zo kan er uit bepaalde lichaamskenmerken ook afgeleid worden wat iemands gezondheidstoestand of ras is. Bepaalde ziekte-gerelateerde gebeurtenissen, zoals bijvoorbeeld diabetes of een beroerte veroorzaken veranderingen in de bloedvaten in het netvlies, zijn met sommige biometrische technologieën te herkennen. Dergelijke gegevens zijn bijzonder gevoelig in termen van privacy.

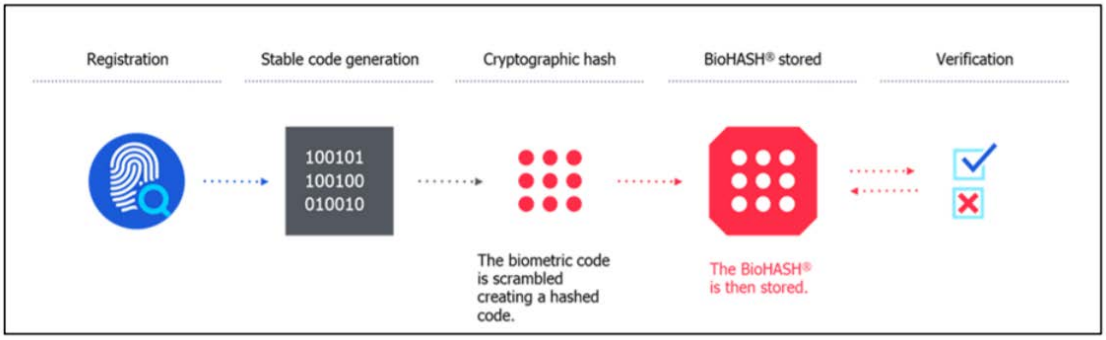
Privacy is een recht dat is verankerd in wetgeving. In de praktijk moeten informatiesystemen voldoen aan de databeschermingsprincipes en -eisen zoals rechtmatigheid, proportionaliteit, doelbinding, transparantie en de kwaliteit van data. Er moeten veiligheidscontroles zijn om de rechten van de betrokkenen te waarborgen met betrekking tot de bescherming van hun privéleven en persoonsgegevens. Met de komst van de Algemene Verordening Gegevensbescherming (AVG) vanaf 25 mei 2018, zijn de principes 'databeveiliging (ofwel privacy) by design' en 'databeveiliging by default' essentiële privacy-instrumenten binnen de EU[6]. Privacy by design (Hoepman, 2018) is een ontwerpprincipe voor de systeemontwikkeling waarbij privacy wordt ontworpen als een eigenschap in het hele systeem en wordt gewaarborgd in alle ontwerpfasen, vanaf het begin tot aan de implementatie, en zelfs tot het systeem helemaal niet meer wordt gebruikt.

Er zijn diverse privacy enhancing technologieën voorhanden om de privacy van biometrische gegevens te waarborgen. Standaarden is er daar een van. Toepassing van de Biometrische Open Protocol Standaard (BOPS, zie verder toegelicht in sectie 3.2) verzekert betrouwbare verwerking van templates in een biometrisch systeem door ervoor te zorgen dat de volledige biometrische gegevensset nooit op één plek opgeslagen is. Tijdens enrolment worden biometrische gegevens versleuteld en gescheiden in twee delen. Een deel wordt opgeslagen op de server en het andere deel wordt opgeslagen op het (mobiele) apparaat. In dit model is de complete biometrische template nog steeds veilig en herbruikbaar als een van de delen is aangetast, omdat de andere helft is opgeslagen in een andere locatie. De juiste implementatie van BOPS draagt op deze manier bij aan de privacy van de gebruiker.

Een andere privacy enhancing toepassing betreft het inzetten van versleuteling. De Universiteit Twente doet momenteel onderzoek naar de nieuwste homomorfische encryptie (HE) technieken die de verwerking van de versleutelde biometrische gegevens mogelijk maakt zonder dat de gegevens eerst ontsleuteld moeten worden[7]. Daarmee kan de biometrische herkenning uitgevoerd worden, zonder de versleutelde vingerafdrukken te ontsleutelen.

Een concrete toepassing ervan is BioHash dat de opslag van biometrische gegevens beveiligt door een cryptografische hash te genereren (zie Figuur 5 hieronder). BioHash wordt op dit moment toegepast in de zorgsector[8] in ontwikkelingslanden. Dergelijke landen kennen vaak geen centrale door de overheid gereguleerde persoonsregistratie, waardoor biometrie een uitkomst vormt voor het identificeren van de patiënt. Tevens kan er een biometrische 'digitale handtekening' worden gezet met een uit de biometrie afgeleide sleutel.

[6] Zie: https://fidoalliance.org/wp-content/uploads/FIDO_Authentication_and_GDPR_White_Paper_May2018-1.pdf.
[7] Zie: https://www.utwente.nl/en/eemcs/scs/research/running-projects/OBRE-project/.
[8] Zie: https://www.genkey.com/healthcare/.



Figuur 5: BioHASH concept [Bron: https://www.genkey.com/wp-content/uploads/2016/11/GenKey-BIOHASH_final.pdf]

2.7 Kwetsbaarheden biometrie

Naast voordelen zijn er ook een aantal risico's van de biometrische authenticatiesystemen, zoals bedreigeraanvallen (imposter attacks) en spoofing aanvallen (presentation attack). In deze sectie gaan we hier verder op in en in de volgende sectie 2.8 geven we het overzicht van de mitigerende maatregelen zoals Presentation Attack Detection (PAD), de wetenschappelijke term voor liveness detectie (Marcel et al., 2019).

Het omzeilen of voor de gek houden van biometrische systemen voor identiteitsverificatie is onderwerp van veel onderzoek. Er werken ook mensen aan het voorkomen van dit soort acties. In het kader van deze 'wapenwedloop' steunde de Europese Unie in het verleden het zogenaamde Tabula Rasa-project[9], dat zich richtte op de verdediging tegen zogenaamde 'spoofing' oftewel presentation attacks op biometrie (Kindt, 2019). Daarin kwamen bekende en minder bekende varianten van dit soort aanvallen terug. Een voorbeeld hiervan is de van latex, gelatine of zelfs met lijm nagemaakte vingerafdruk op basis van een door een persoon op een bepaald oppervlak achtergelaten afdruk.

Ook het namaken van gezichten is mogelijk. Met behulp van geavanceerde gezichtsherkenningstechnologie, spraakherkenning en kunstmatige intelligentie kan een statische foto zodanig gemanipuleerd worden dat deze realistisch tot leven komt. Een ludiek voorbeeld hiervan is het hoofd van Raspoetin dat het nummer Halo van Beyoncé playbackt[10]. Deze nieuwste trend van dergelijke foto en video manipulatie wordt ook wel 'deepfakes' genoemd. Hoewel de gemanipuleerde beelden steeds beter en realistischer worden, zijn de huidige deepfakes voorbespeeld en nog niet 'live', real-time uit te voeren. Op Youtube zijn diverse voorbeelden te vinden. Hieronder staan twee voorbeelden. Iemands gezicht wordt 'nagemaakt' door tientallen foto's van het slachtoffer te verzamelen en op basis daarvan een 3D-beeld te creëren (zie Figuur 6).

De foto links (Figuur 6) voegt nog een andere dimensie toe aan de morphing van video's: audio masking. Niet alleen lijkt de persoon op het slachtoffer, maar ook diens stem is dusdanig gemanipuleerd dat de aanvaller hem alles kan laten zeggen.

Biometrische oplossingen voor gezichtsherkenning kennen een aantal risico's en kwetsbaarheden. Hieronder worden de belangrijkste genoemd.

[9] Zie: https://ec.europa.eu/digital-single-market/en/content/tabula-rasa-protecting-biometric-recognition-external-attacks.
[10] Zie: https://www.nu.nl/273990/video/britse-wetenschappers-laten-foto-van-raspoetin-zingen.html.

Figuur 6: Voorbeelden van deepfakes: audio masking - manipulatie van de stem (links)[11] en 3D-beeld gecreëerd op basis van tientallen foto's van dezelfde persoon (rechts)[12].

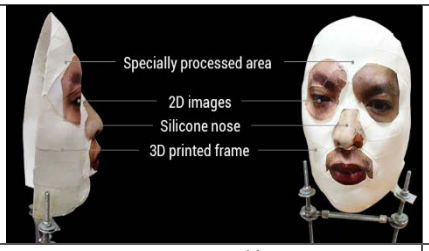
Kwaadwillende tweelingen

Een lastig te mitigeren risico is dat van twee- of meerlingen die kwaad willen. Gezichtsherkenning kan tweelingen niet onderscheiden. Andere biometrische modi zoals iris, stem en vingerafdruk bieden wel soelaas om tweeling te onderscheiden.

Make-up, maskers en 3D-prints

Relatief eenvoudige oplossingen om identificatie te manipuleren zijn het toepassen van make-up, het gebruik van maskers en door een 3D-print te maken van iemands gezicht (zie Tabel 1).

Tabel 1: Voorbeelden van de bekende gezichtsmanipulaties met make-up, maskers en 3D-prints [Bronen: links[13], midden[14], rechts[15]].

		
Make-up[13]	Maskers[14]	3D-prints[15]

Het toepassen van make-up en het gebruik van maskers maakt het mogelijk zich voor te doen als iemand anders op een relatief goedkope en eenvoudige manier. Maskers en 3D-prints van hoofden zijn middelen om in te zetten bij online verificatie van iemands identiteit, ofwel om gezichtsherkenningsoplossingen om de tuin te leiden.

Professionals zijn erop getraind om extreem gebruik van make-up of maskers te herkennen. Voor online verificatie van iemands gezicht is het beter om niet alleen te vertrouwen op uiterlijke kenmerken, maar ook innerlijke kenmerken als aderpatroon. Ook Presentation Attack Detection (PAD), ofwel liveness detectie is hier een risico-mitigerende maatregel (zie sectie 2.8).

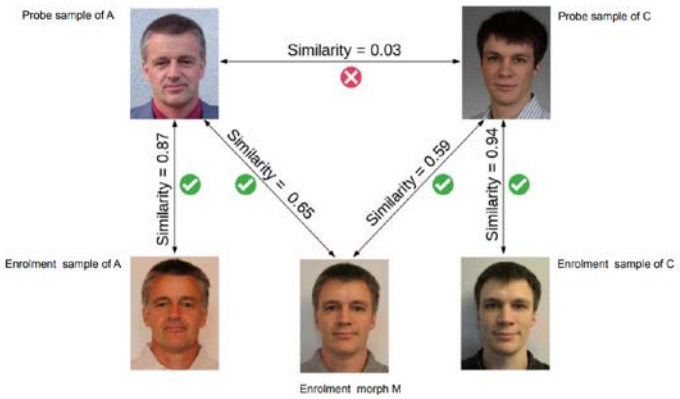
Morphing

Morphing is het samenvoegen van twee of meerdere biometrische kenmerken van verschillende personen. Het resultaat wordt een morph genoemd, gecreëerd op een dusdanige manier dat het resultaat lijkt op alle personen (van wie de afbeeldingen zijn gebruikt). Met behulp van een computerprogramma kan bijvoorbeeld een morph gemaakt worden van twee afbeeldingen van gezichten, zie een voorbeeld hieronder (Tabel 2).

[11] Zie: https://me.me/i/this-dude-can-make-donald-trump-say-anything-15749304.
[12] Zie: https://www.theverge.com/2016/3/21/11275462/facial-transfer-donald-trump-george-bush-video.
[13] Zie: https://rayanworld.com/20170709103243003/Before-and-After-Photos-Showing-the-Transformative-Power-of-Makeup.
[14] Zie: https://www.theverge.com/2017/11/13/16642690/bkav-iphone-x-faceid-mask.
[15] Zie: https://www.macrumors.com/2018/12/16/3d-printed-head-android-face-id/.

Tabel 2: Voorbeelden van morphs gemaakt met behulp van drie morphing software applicaties: MorphMan (links onderaan), MorphThing (middelste photo) en FantaMorph (rechts onderaan)[16].

Het risico van morphing is dat iemand zich voor een ander persoon kan uitgeven met als gevolg dat twee verschillende personen gebruik kunnen maken van hetzelfde identiteitsdocument (zie Figuur 7).



Figuur 7: Risico's van morphing [bron: Bush et al., Morphing Attack Detection Overview (2018).[17]]

Morphing vindt niet alleen plaats op basis van foto's. Bij op video gebaseerde identificatieoplossingen is real-time manipulatie van de videobeelden mogelijk, bijvoorbeeld morphing (gemanipuleerde foto presenteren aan de sensor / camera) of replay aanval (een aanvaller kan de video, verkregen van de legitieme gebruiker, afspelen op elk apparaat dat video reproduceert: smartphone, tablet, laptop, enz.). De Duitse BSI (Bundesamt für Sicherheit in der Informationstechnik – Federal Office for Information Security) heeft aangetoond dat het ook mogelijk is om real-time morphing van video te doen. Dat hoeft niet noodzakelijkerwijs van gezichten te zijn, maar kan ook het Wettelijk identiteitsmiddel betreffen. Bijvoorbeeld door holografische en andere optische beveiligingskenmerken te morphen met een op papier uitgeprint WID tijdens een video-identificatiesessie (zie Figuur 8).

[16] Disclaimer: alle afbeeldingen in Tabel 2 zijn slechts een illustratie gemaakt door de uitvoerders van het onderzoek zelf en worden gebruikt in dit rapport met toestemming van de desbetreffende personen.
[17] Bush et al., Morphing Attack Detection Overview (2018), zie: https://christoph-busch.de/files/Busch-NIST-IFPC-MAD-181128.pdf.

Figuur 8: Voorbeeld van real-time holografische en optische morphing tijdens video-identificatiesessie [Bron[18]].

2.8 Mitigerende maatregelen: Presentation Attack Detection

Een belangrijke risico mitigerende maatregel voor verschillende biometrische modaliteiten is *Presentation Attack Detection* (PAD), en wordt ook wel *liveness detectie* genoemd. Echter, strikt genomen wordt liveness detectie gedefinieerd als de meting en analyse van anatomische kenmerken of onvrijwillige of vrijwillige reacties, om te bepalen of een biometrische template wordt genomen van een levend persoon dat aanwezig is op het opnamepunt (ISO/IEC JTC1 SC37 Biometrics[19]). Volgens deze gestandaardiseerde definitie van de term kan liveness detectie worden beschouwd als een onderdeel van PAD, maar niet als een synoniem voor PAD zelf. De wetenschappelijke term Presentation Attack Detection verwijst naar fraudepreventie voor biometrie in het algemeen, terwijl liveness detectie van wordt specifiek gebruikt voor gezichtsherkenning.

NIST definieert PAD als volgt: een geautomatiseerde bepaling van een presentatie-aanval. Een subset van methoden voor het bepalen van presentatieaanvallen omvat meting en analyse van anatomische kenmerken of onvrijwillige of vrijwillige reacties, om te bepalen of een biometrisch kenmerk wordt afgenomen van een levende persoon dat aanwezig is op het opnamepunt[20].

PAD is ook een prestatie kenmerk geworden van biometrische herkenning en volgens vele deskundigen een onmisbaar onderdeel van elk biometrisch systeem (Marcel et al., 2019). Recent onderzoek rondom biometrische anti-spoofing heeft tientallen PAD technieken opgeleverd (Marcel et al., 2019; Korus en Memon, 2019; Spreeuwers et al., 2018). Resultaten van deze onderzoeken tonen aan dat er behoefte is aan validatie van diverse PAD technieken. ISO/IEC 30107 standaard[21] beschrijft het raamwerk voor de biometrische PAD en methodes voor het beoordelen van presentatieaanval-detectiemechanismen (zie ook sectie 3.2). NIST heeft het SOFA-B (The Strength of Function for Authenticators – Biometrics) model dat de volgende drie aspecten omvat: overeenkomende prestaties, detectie van presentatieaanvallen (aka spoof-detectie) en inspanning (om een systeem te omzeilen). Het uiteindelijke doel van SOFA-B raamwerk is een maatregel voor het vergelijken en combineren van authenticatietechnologieën, waarbij biometrie een van de factoren is. Een ander voorbeeld van een modaliteit-specifiek validatie-initiatief is het recent ontwikkelde testbed voor liveness detectie voor 3D gezichtsherkenning[22].

PAD methoden worden gecategoriseerd in *hardware-gebaseerd* of *software-gebaseerd* (Komulainen et al., 2019). Hardware-gebaseerde methoden vereisen speciale sensoren die in staat zijn om bijvoorbeeld specifieke intrinsieke verschillen tussen echte en kunstmatige gezichten te detecteren, zoals 3D-scanners om te

[18] Zie: https://www.teletrust.de/fileadmin/docs/veranstaltungen/Signaturtag_2018/11_Informationstag_Elektronische-Signatur-und-Vertrauensdienste_Frank-BSI.pdf.
[19] Zie: https://www.iso.org/committee/313770.html.
[20] Zie: https://csrc.nist.gov/glossary/term/Presentation-Attack-Detection.
[21] Zie: https://www.iso.org/standard/53227.html.
[22] Zie: https://www.zoomlogin.com/FaceTec_3D_Liveness_Testing_Methodology.pdf.

controleren of de vastgelegde gezichten geen 2D zijn, of thermische sensoren om de temperatuurverdeling te detecteren die hoort bij echte live gezichten. Deze aanpak is echter minder populair dan software-gebaseerde methodes, omdat de verijsde onconventionele hardware (sensoren) is meestal duur, niet compact en (nog) niet beschikbaar in persoonlijke apparaten, wat hun brede inzet verhindert.

Software-gebaseerde PAD-methoden zijn vaak onderverdeeld in de volgende twee groepen: *actief* (vereist een actie van de gebruiker, bijvoorbeeld door het hoofd te bewegen of een opdracht uit te voeren) of *passief* (automatische PAD detectie, geen actie van de gebruiker nodig, bijvoorbeeld door met gekleurde lichtflitsen te werken). Een voorbeeld van een passieve software-gebaseerde PAD methode is knipoog detectie. Andere voorbeeld van een actieve software-gebaseerde methode is het volgen van de blik van de gebruiker naar een vooraf gedefinieerde prikkel (challenge response).

Passieve software-gebaseerde PAD methoden zijn minder intrusief. Actieve methoden zijn in staat om goed te generaliseren over verschillende aanval scenario's, maar ten koste van de bruikbaarheid vanwege de langere authenticatietijd en systeemcomplexiteit. Ieder van deze PAD-methodes kent bepaalde voor- en nadelen. Volgens recent onderzoek, zou een combinatie van hardware- en software-gebaseerde methodes de meest optimale PAD aanpak zijn voor het vergroten van de betrouwbaarheid van biometrische systemen (Marcel et al., 2019).

Hieronder volgen een aantal modaliteit-specifieke voorbeelden. Bekende PAD methoden tegen gezichtsaanvallen zijn 3D metingen van het gezichtsmodel, de temperatuur van de huid, of de absorptie of reflectie van licht door het gezicht.

Wat betreft vingerafdrukken blijkt dat eenvoudige visuele inspectie van een afbeelding van een echte vingerafdruk en het bijbehorende nepmonster lastig is omdat de twee afbeeldingen erg op elkaar kunnen lijken en het menselijk oog moeilijk onderscheid kan maken. Toch kunnen sommige verschillen tussen de echte en nepbeelden duidelijk worden dankzij het feit dat vingerafdrukken, als 3D-objecten, hun eigen optische eigenschappen (absorptie, reflectie, verstrooiing, breking) hebben, die andere materialen (siliconen, gelatine, glycerine) of synthetisch geproduceerde monsters niet bezitten. Beeldkwaliteitsbeoordeling-gebaseerde PAD methodes analyseren deze specifieke optische eigenschappen van de vingerafdrukken. Andere PAD methodes voor vingerafdrukken meten ook de levende kenmerken van de vinger zelf: de temperatuur van de vingers; de hartslag in de vinger; zweet/vochtigheid van de vinger; de positie van de vinger; de afstand van de vinger tot de camera; de randdichtheid en de lichtreflectie veroorzaakt door het LED (light-emitting diode) scherm (bijv. op de mobiele telefoon).

Bij irisherkenning worden meerdere PAD metingen gedaan, zoals natuurlijke vibraties van de pupil (iris-spectroscopie), grootte van de pupil onder invloed van licht, vochtdetectie in het oog en knipoog-bewegingen.

Ook een synthetisch gegenereerde stem kan onderscheiden worden van een natuurlijk gegenereerde stem doormiddel van geavanceerde biometrische PAD-algoritmes. Bijvoorbeeld, door de gebruiker te vragen om een random-genereerde, steeds andere, zin live hardop te laten uitspreken.

Wat betreft biometrie op basis van een handtekening zijn de meest gebruikte PAD metingen gebaseerd op de dynamische kenmerken van de handtekening, zoals totaal aantal slagen en ondertekentijd (Tolosana et al., 2019).

Sommige multimodale biometrische toepassingen maken gebruik van de gedragsbiometrie kenmerken als aanvullende liveness factor op de fysiologische kenmerken (zie sectie 4).

Een preventieve maatregel tegen videoaanval is een digitaal watermerk in de videostream te verwerken. De digitale watermerken methode verbergt een watermerk in digitale media zodat het onmerkbaar is en het originele mediabestand hersteld kan worden naar de originele vorm, zodra het watermerk is onttrokken[23]. Morphing toepassingen hebben moeite om een dergelijk watermerk goed mee te manipuleren waardoor morphing detecteerbaar is voor de observant.

[23] Zie: https://www.zdnet.com/article/how-these-hidden-video-watermarks-can-help-spot-piracy-doctored-images/.

Daarnaast is er voor video-gebaseerde de verificatie van de identiteit de BaFin richtlijn[24]. De scope van BaFin is gericht op het hele verificatieproces met behulp van video en is dus breder dan alleen PAD. Deze richtlijn vereist o.a. het gebruik van een uniek transactienummer (TAN) voor elke video-identificatie sessie als extra veiligheid maatregel. De TAN wordt via SMS of e-mail naar de gebruiker gestuurd en wordt vervolgens door de gebruiker zelf ingevoerd tijdens de videosessie (dit is een vorm van actieve PAD). Tot slot strekt het de aanbeveling om het aantal video-gebaseerde verificatie pogingen te beperken om te voorkomen dat iemand door middel van trial en error toch een valse identiteit kan aannemen. NIST geeft aan dat maximaal vijf pogingen toegestaan zijn.

Recente ontwikkelingen tonen aan dat digitale watermerken in combinatie met de nieuwste AI-technieken kunnen worden gebruikt om de manipulatie van de foto's te herkennen. De resultaten van het onderzoek van Korus en Memon (2019) tonen een verhoging van fotomanipulatie herkenning van 45% naar 90%, zonder afname van de beeldkwaliteit, in forensische analyse use-case om een beslissing te nemen over de authenticiteit / verwerkingsgeschiedenis van de geanalyseerde foto. Replay aanvallen zijn moeilijker te detecteren dan foto spoofing aanvallen, omdat niet alleen de gezichtstextuur en -vorm wordt geëmuleerd, maar ook de dynamiek, zoals knipperende ogen, mond- en / of gezichtsbewegingen. PAD methoden die effectief zijn tegen foto aanvallen zullen slechter presteren met betrekking tot video aanvallen. Specifieke tegenmaatregelen moeten worden ontwikkeld en geïmplementeerd (Hernandez-Ortega et al, 2019).

Onderaan volgt een aantal voorbeelden van PAD technieken voor verschillende biometrische modaliteiten. Bijvoorbeeld, door een nagemaakte vingerafdruk te kunnen detecteren met behulp van liveness detectie mogelijkheden als zweet, temperatuur, hartslag of de flexibiliteit van de huid.

Tabel 3 hieronder vat per biometrische modaliteit de mogelijke aanvalsvectoren samen en beschrijft hoe PAD ze kan mitigeren.

Tabel 3: Overzicht van de mogelijke aanvallen en PAD gebaseerde mitigaties.

Modaliteit	Aanvalsvector	PAD methode
Vingerafdruk (extern)	Namaken vingerafdruk m.b.v. siliconengel of soortgelijk materiaal.	Beeldkwaliteitsbeoordeling. Zweet/vochtigheid van de vinger meten.
Vingerafdruk (extern)	Tonen van een foto van een vingerafdruk voor de scanner.	Beeldkwaliteitsbeoordeling. Temperatuur van de vinger meten.
Vingerafdruk (extern en intern)	Afgehakte vinger plaatsen op scanner of het slachtoffer dwingen diens vinger op de scanner te plaatsen.	Percentage zuurstof in bloed meten. Absorptie of reflectie van licht door vinger meten. Hartslag meten.
Gezicht	Dragen van een hard of zacht masker, of het dragen van make-up.	Inzoomen op gebieden waar maskers slecht aansluiten op het gezicht zoals de ogen en de mond. Automatische make-up herkenning ingebed in gezichtsherkenning algoritme. Menselijke interactie waarbij het opvalt dat iemand veel make-up op heeft.
Gezicht	Morphing van de foto: samenvoegen van twee of meerdere gezicht afbeeldingen.	Geautomatiseerde gezicht aanval detectie.
Gezicht	Tonen van nagemaakt 3D-hoofd (van gips of klei).	Infrarood meten (temperatuur). Kleurverschillen van het gezicht meten door in/uit ademen.
Gezicht	Tonen van een 2D of 3D foto voor de camera.	3D metingen doen. Temperatuur (zie hierboven). Absorptie of reflectie van licht door het gezicht.
Gezicht	Afspelen van een vooraf opgenomen video van het slachtoffer.	Video challenge-response (knipogen, draaien, lachen, etc.)
Iris	Tonen van een nagemaakt 3D oog van het slachtoffer.	Natuurlijke vibraties pupil meten (iris-spectroscopie).

[24] Zie: BaFin Circular 3/2017 (GW) - Video Identification Process
https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html.

		Grootte pupil beïnvloeden door licht. Vochtdetectie in het oog. Knipogen.
Iris	Tonen van een foto van het oog van het slachtoffer.	Zie hierboven.
Stem	Audio masking, synthetisch gegenereerde stem en afdraaien van een vooraf opgenomen stemopname van het slachtoffer.	Stem challenge-response. Digitale watermerken.
Handtekening	Kopie van de handtekening van het slachtoffer gebruiken.	Snelheid, drukpunten, hoek van de pen ten opzichte van de oppervlakte, de tijd tussen het schrijven en optillen meten (air moves).

2.9 Sectorspecifieke biometrietoepassingen

Biometrische technologie wordt veel gebruikt in de luchtvaart, financiële, zorg en telecom sector. Vergeleken met andere sectoren wordt biometrische authenticatie nog relatief weinig toegepast binnen de overheidssector. Hieronder geven we per sector enkele voorbeelden van biometrische toepassingen.

Biometrie op luchthavens

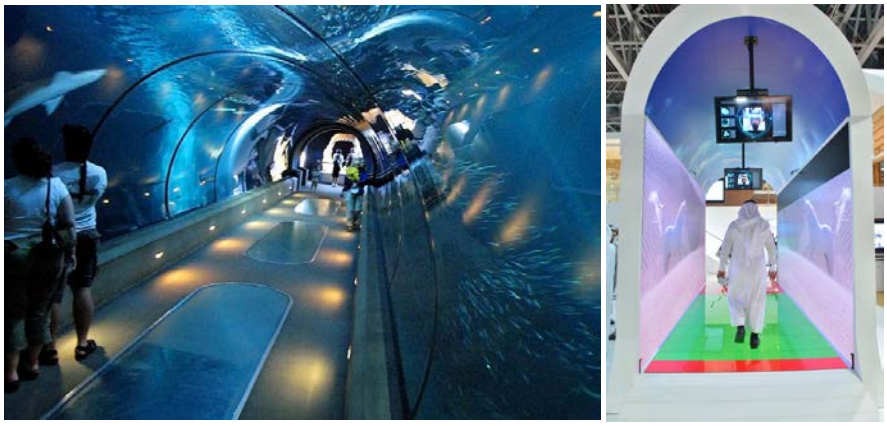
Voor het verifiëren van de identiteit bij de grenscontrole op Schiphol worden al enige tijd de zogenaamde eGates gebruikt. Het paspoort van een reiziger wordt bij de eGate uitgelezen en het gezichtsherkenningssysteem vergelijkt de foto in het paspoort met de ter plekke door een camera gemaakte foto. Inmiddels maken meerdere luchthavens gebruik van deze op gezichtsherkenning gebaseerde systemen (Figuur 9 rechts). Frequente reizigers kunnen op Schiphol ook het Privium[25] systeem gebruiken dat werkt op basis van irisherkenning (Figuur 9 links). Irisherkenning werkt minder goed voor personen met bril of lenzen. Ook lukt de gezichtsherkenning aan de eGates soms niet. In dergelijke situaties is er altijd een fall-back scenario aanwezig: een fysieke, niet-geautomatiseerde verificatie van de identiteit door de Koninklijke Marechaussee.

Figuur 9: Biometrie voor de grenscontrole: Privium systeem op Schiphol (links)[25] en eGates op het vliegveld in Hong Kong (rechts)[26].

De internationale luchthaven van Dubai heeft een virtuele aquarium-tunnel ingericht als een soort van ‘smart gate’ waarin 80 camera’s voor automatische gezichtsherkenning en irisscan aanwezig zijn. Reizigers kunnen hun gezichtsscans en irisscans laten registreren bij de slimme kiosken rondom de luchthaven, in een aantal winkelcentra en hotels. Wanneer de passagiers door de tunnel lopen worden ze geïdentificeerd (zie Figuur 10). Het rustgevende aquarium nodigt uit om rond te kijken en zorgt voor een verbeterde prestatie van de biometrische herkenning op een gebruikersvriendelijke en weinig opdringerige manier. Wanneer de passagier aan het eind van de tunnel is gekomen, worden de gezichtsscan beelden vergeleken met de reeds opgeslagen templates en krijgt de passagier groen licht en mag doorlopen. In het geval van een rood licht volgt een controle door een vliegveldmedewerker. De tunnels vervangen de veiligheidsmachtiging die momenteel aan de

[25] Zie: https://www.schiphol.nl/nl/privium/zo-werkt-de-irisscan/.
[26] Zie: https://www.businesstraveller.com/business-travel/2018/09/20/hong-kong-airport-now-has-facial-recognition-technology-at-its-security-gates/.

loketten van luchthavens wordt uitgevoerd. In 2020 worden dergelijke aquarium-tunnels ook op de andere terminals in Dubai in gebruik genomen.



Figuur 10: De aquarium-tunnel in Luchthaven Dubai is een voorbeeld van de naadloze (seamless) verificatie van de identiteit en no-cue trend bij de grenscontrole[27].

Biometrie in de financiële sector

In de financiële sector wordt vaak de onboarding van nieuwe klanten en de authenticatie van bestaande klanten gedaan met behulp van biometrie. In Nederland gebruiken diverse banken vingerafdruk- en/of gezichtsbiometrie als authenticatiefactor. De ING mobiel bankieren applicatie bijvoorbeeld maakt gebruik van de biometrische technologie die ingebed zijn in de smartphone, zoals TouchID en FaceID op iPhone, voor de toegang tot hun online bankieren app. De bank maakt zelf de keuze welke smartphones worden vertrouwd als het gaat om de biometrische vingerafdruk of gezichtsherkenning authenticatie. Op sommige, wat oudere en minder geavanceerde mobiele toestellen staan mobiele apps het gebruik biometrie niet toe omdat de technologie vaak minder goed presteert.
Onboarding geschiedt in toenemende mate ook met behulp van identificatie op afstand en biometrie. Bijvoorbeeld door selfies te vergelijken met de uit de chip van het paspoort gelezen pasfoto of middels video-identificatie in combinatie met biometrie. Deze laatste oplossing is vooral in Duitsland populair.

ING met TouchID

Rabobank met FaceID

[27] Zie: https://www.internationalairportreview.com/news/64213/iris-facial-recognition-gates-go-live-dubai-airport/.

Om er zeker van te zijn dat de aanvrager ook dezelfde is als de persoon op het identiteitsdocument vragen enkele banken tevens om een selfie (ABN Amro, ING, Moneyou en Revolut), of meer specifiek een selfie waarbij de klant het paspoort in de hand houdt (N26) of een selfiefilm met zogeheten 'liveness check'. Dat maakt identiteitsfraude lastiger.

Behalve vingerafdruk en gezichtsherkenning worden ook andere biometrische kenmerken gebruikt voor authenticatie. Bunq gebruikt bijvoorbeeld als extra factor een stemopname. ING deed dit overigens ook in het verleden maar is er mee gestopt wegens te weinig gebruik. Bovendien was dit een eigen biometrisch oplossing. Dit in tegenstelling tot de vingerafdruk- en gezichtsherkenning oplossingen die gebruik maken van in de mobiele telefoon geïntegreerde sensoren en functionaliteit.

Biometrie in de zorgsector

Volgens de statistieken zijn 67% van de fouten in bloedtransfusies en 13% van alle bijwerkingen die patiënten in operaties schaden te wijten aan verkeerde identificaties. ID-polsbandjes verminderen fouten slechts met 50%[28]. Daarom is er veel behoefte aan de betrouwbare verificatie van de identiteit in de sector; biometrie speelt daarin toenemende een rol. Een voorbeeld van een biometrische toepassing is een Spaans ziekenhuis dat patiënten identificeert op basis van een vingerafdruk, gezicht en iris combinatie[29]. Ook in VS wordt biometrische identificatie steeds vaker ingezet in ziekenhuizen[30].

Biometrische technologie wordt ook ingezet om ziekenhuispersoneel te identificeren en de toegang tot specifieke gebieden en systemen binnen een ziekenhuis te beperken. In veel ziekenhuissituaties is het onhandig om een gebruikersnaam en wachtwoord in te toetsen, dan is biometrie een uitkomst.

Een ander eerdergenoemde voorbeeld is de vingerafdruk-gebaseerde ID-card[31] voor de toegang tot zorgdiensten in ontwikkelingslanden. In dergelijke landen is vaak geen centrale, door de overheid gereguleerde persoonsregistratie. Biometrische gegevens op een ID-card maken het identificeren van de patiënt in dat geval wel mogelijk.

Biometrie in de telecomsector

In de telecom sector zien we de mobiele biometrie toepassingen breed geïmplementeerd, bijvoorbeeld voor het ontgrendelen van de smartphone door middel van de standaard geïntegreerde vingerafdruk en/of gezichtsherkenning oplossingen. Zie ook sectie 2.10 voor nadere toelichting en voorbeelden.

Biometrie in overheidssector

Vergeleken met andere bovengenoemde sectoren zijn er relatief weinig biometrische toepassingen voor het verifiëren van de identiteit binnen de overheidssector (opsporing daarbuiten gelaten).

Binnenlandse Zaken in het Verenigd Koninkrijk (Home Office) past biometrie toe op drie lagen: vastleggen van de biometrie van een persoon, gebruiken van biometrie voor verificatie (1-op-1, ofwel is deze persoon wie hij zegt te zijn?) en identificatie (1-op-n, ofwel wie is deze persoon wiens biometrie is afgegeven?)[32]. Home Office heeft een strategierichtlijn voor biometrie opgesteld die zich primair richt op forensisch onderzoek van de politie, immigratiediensten en nationale veiligheid, en gebaseerd is op vingerafdruk, gezichtsherkenning en DNA biometrie. DNA en vingerafdrukken worden al langere tijd gebruikt in Home Office diensten. De politie gebruikt een mobiel apparaat met vingerafdruktechnologie voor het identificeren van personen in het veld. Gezichtsherkenning wordt sinds kort door Home Office ingezet voor (a) 1-op-1 verificatie; en (b) 1-op-n identificatie. DNA wordt primair gebruikt voor opsporingsdoeleinden, bijvoorbeeld voor identificatie van de personen die betrokken zijn bij criminele activiteiten. De huidige strategie is gericht op de centralisatie van biometrische data zodat de biometrische diensten efficiënter, flexibeler, meer geïntegreerd en

[28] Zie: http://www.iritech.com/iris-healthcare-umanick.
[29] Zie: http://www.umanick.com/en/success-story-arrixaca-hospital/.
[30] Zie: https://www.wsj.com/articles/hospitals-turn-to-biometrics-to-identify-patients-11549508640.
[31] Zie: https://www.genkey.com/healthcare/.
[32] Home Office Biometrics Strategy - Better public services, Maintaining public trust (juni 2018). Zie: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf.

geautomatiseerd aangeboden kunnen worden. Home Office is momenteel bezig met het uitvoeren van Data Protection Impact Assessments (DPIAs) van de nieuwe biometrische technologie en applicaties, en het opstellen van de nieuwe richtlijnen vanuit wettelijke, operationele, beleid, ethische en privacy perspectieven, inclusief een toegewijde adviesboord voor de gezichtsherkenning, standaarden voor de regulatie van de geautomatiseerde gezichtsherkenning gebruik voor de opsporing en praktische gedragscode voor de bewakingscamera's.

Een ander voorbeeld betreft het toepassen van biometrische in de context van immigratiedienstverlening in het Verenigd Koninkrijk. In het geval van een eventuele Brexit, dienen niet-ingezetenen zich opnieuw te identificeren. Hiervoor is een mobiele app ontwikkeld die hieraan invulling geeft middels het scannen van de gegevens op de chip van het paspoort met NFC, waaronder de pasfoto, en deze foto te vergelijken met een selfie.[33].

Frankrijk is sinds kort bezig met het nieuwe nationale digital identiteit programma Alicem[34]. Onderdeel ervan is het integreren van gezichtsherkenning voor de makkelijke toegang tot overheid diensten door de burgers, zoals belastingaangifte en sociale diensten.

Diverse nationale digitale identiteitsoplossingen maken gebruik van biometrie als authenticatiefactor. Een voorbeeld hiervan is de Belgische Mobile ID applicatie Itsme.[35] De Itsme gebruiker kan, als alternatief voor de PIN, de vingerafdruk- of gezichtsherkenningsfunctionaliteit van de mobiele telefoon zelf inschakelen. Onlangs is Itsme aangemeld om voor Europese erkenning in aanmerking te komen in de context van de eIDAS verordening. Tijdens de peer-review van Itsme is gebleken dat het gebruik van deze biometrische authenticatiefactor onvoldoende betrouwbaar zijn voor eIDAS niveau Hoog. Dezelfde uitkomst was van toepassing op de aangemelde nationale eID van Letland. Op niveau Substantieel is biometrie wel toegestaan, mits extra maatregelen zijn getroffen.

Momenteel loopt er in Nederland een experiment m.b.t. het digitaal aanvragen van het verlengen van het rijbewijs bij de Rijksdienst Wegverkeer (RDW)[36]. De aanvraag start nadat de gebruiker heeft ingelogd met DigiD Substantieel. Onderdeel van de aanvraag is het aanleveren van een digitale pasfoto van de gebruiker door een door RDW erkende fotograaf. Ook de handtekening wordt door de fotograaf afgenomen en digitaal verwerkt. De fotograaf zendt deze gegevens naar de RDW tezamen met het rijbewijsnummer van het rijbewijs van de aanvrager en eventueel diens e-mailadres. Onmiddellijk na de bevestiging van ontvangst door de RDW vernietigt de fotograaf alle gegevens. De digitale foto wordt in het rijbewijzenregister vergeleken met de foto van het laatst afgegeven rijbewijs en moet voldoende overeenkomen om de aanvraag elektronisch verder te laten plaatsvinden. De digitale pasfoto en digitaal vastgelegde handtekening worden vervolgens opgenomen in het rijbewijzenregister en verwerkt op het nieuwe rijbewijs. Als de aanvraag niet wordt doorgezet worden na zes maanden de gegevens vernietigd. Na enkele dagen kan de gebruiker het verlengde rijbewijs ophalen op het gemeentehuis. Bij het afhalen moet de gebruiker zich identificeren en het oude rijbewijs inleveren.

Biometrie in andere sectoren

Enkele andere voorbeelden van specifieke biometrische toepassingen zijn: leeftijdsverificatie voor drankverkoop,[37] smartcard met handscan- en/of vingeraderbiometrie in de Rotterdamse haven voor de chauffeurs[38] en smartcard met vingerafdruk als twee-factor biometrische authenticatie voor de toegang tot grote data centra[39].

[33] Zie: https://www.gov.uk/guidance/using-the-eu-exit-id-document-check-app.
[34] Zie: https://www.technologyreview.com/f/614469/france-plans-to-use-facial-recognition-to-let-citizens-access-government-services/.
[35] Zie: https://www.itsme.be/security.
[36] Zie: https://www.rdw.nl/particulier/voertuigen/auto/het-rijbewijs/nederlands-rijbewijs-verlengen/voorwaarden-en-uitleg-proef-digitaal-aanvragen-rijbewijs.
[37] Zie: https://www.jumio.com/age-verification/.
[38] Zie: https://seaport-magazine.nl/secure-logistics-cruciaal-voor-snelle-en-veilige-haven/.
[39] Zie: https://bioconnect.com/data-centers/.

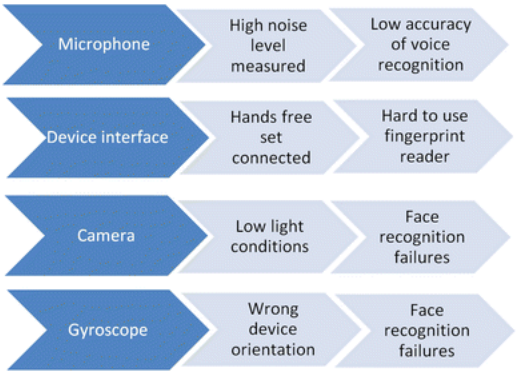
2.10 Theoretische ontwikkelingen en toekomstsperspectief

Naast de beschreven biometrische toepassingen voor het verifiëren van de identiteit die in meer of meerdere mate in de praktijk worden ingezet, is er ook een aantal nieuwe en veelbelovende ontwikkelingen. In deze paragraaf beschrijven we een aantal van deze ontwikkelingen.

Kunstmatige Intelligentie, Internet of Things en biometrie

Dankzij de opmars van kunstmatige intelligentie (AI) technologieën[40] en Internet of Things (IoT)[41] zijn de mogelijkheden van de biometrische verificatie van de identiteit enorm gegroeid.

Kunstmatige intelligentie en IoT worden in feite al dagelijks toegepast in onze moderne smartphones met gezichtsherkenning[42] en slimme domotica-apparaten die bijvoorbeeld de stem herkennen[43]. Dezelfde technologie wordt ook ingezet voor de nieuwe biometrische toepassingen. Bijvoorbeeld om de betrouwbaarheid van de biometrie te verbeteren door middel van IoT technologie (Hulsebosch en Ebben, 2008). De locatie van de gebruiker kan bijvoorbeeld effectief worden ingezet om de betrouwbaarheid van gezichtsherkenning bij een bepaalde camera te verbeteren. Ook is een context-gebaseerd model ontwikkeld voor continue authenticatie op de smartphones met de ingebouwde sensoren (Wójtowicz & Joachimiak, 2016). Dit model maakt gebruik van de mobiele context data (locatie, geluidsgegevens, gebruik instellingen) om de meest geschikte biometrische modaliteit te selecteren om zich te kunnen authentiseren bij een mobiel bankieren applicatie. Bijvoorbeeld, in het geval van gedetecteerde slechte lichtomstandigheden zal de app op de mobiele telefoon alleen vingerafdrukken toestaan omdat het te voorspellen is dat gezichtsherkenning niet goed zal werken (zie
Figuur 11[44]).



Figuur 11: Context-gebaseerde model voor continu authenticatie voor mobiele biometrie toepassingen (Wójtowicz & Joachimiak, 2016): op basis van de context data (locatie, geluidsgegevens, enz.) wordt de meest geschikte biometrische modaliteit geselecteerd.

Kunstmatige intelligentie wordt ook vaak in combinatie met biometrie ingezet om het beveiligingsniveau van workflows in de gezondheidszorg te verhogen, bijvoorbeeld om patiëntverwisselingen te voorkomen[45]. Een ander voorbeeld van een AI-gebaseerde ontwikkeling in opkomst is SABI (System of Adaptive Biometric Identification).[46] SABI is een biometrisch systeem op basis van elektromagnetische radiatie (EMR). De onderliggende technologie is gebaseerd op zelflerende[47] *neurale netwerken* (computers bouwen zoals onze hersenen werken) en *blockchain* (online register waarin transacties worden geregistreerd, als een digitaal gedecentraliseerd grootboek). De ambitie is om de huidige biometrie systemen te vervangen en continue authenticatie mogelijk te maken zonder actie van de gebruiker. Ondanks deze interessante trend in

[40] Realistic neural talking head models. Zie: arxiv.org/abs/1905.08233.
[41] Zie: https://eurekalert.org/pub_releases/2019-10/uod-etu101119.php.
[42] Zie: https://www.wired.com/story/future-of-facial-recognition-technology/.
[43] Zie: https://emerj.com/ai-sector-overviews/artificial-intelligence-plus-the-internet-of-things-iot-3-examples-worth-learning-from/.
[44] Gyroscope - Een gyroscoop is een meetinstrument dat registreert wanneer een smartphone om zijn as draait of kantelt.
[45] Zie: https://www.biometricupdate.com/201808/biometrics-obstacles-and-opportunities-in-healthcare.
[46] Zie: https://sabiglobal.io/docs/WhitePaperEN.pdf.
[47] Een zelflerend systeem combineert en gebruikt voornamelijk zelflerende en andere vormen van data-analytische methodes om vaardigheden te kunnen uitvoeren die worden beschouwd als kunstmatige intelligentie.

wetenschappelijke biometrie onderzoek, is SABI nog in ontwikkeling en heeft het de consumentenmarkt nog niet bereikt.

Mobiele biometrie

Een 'klassiek' biometrie systeem bestaat vaak uit een vaste, 'stand-alone' applicatie, met eigen sensoren en achterliggende databases voor de templates. Typisch voor een dergelijk systeem is dat het niet herbruikbaar is over toepassingen heen. Een mobiel biometrisch systeem heeft diverse eigen biometrische sensoren en functionaliteiten die hergebruikt kunnen worden door meerdere mobiele applicaties (Das et al., 2018). Een dergelijk systeem kan een onderdeel zijn van een smartphone, tablet of een toegewijde biometrische mobiele apparaat met geintegreerde vingerafdruk sensor[48] (zie Figuur 12). Mobiele biometrie bereikt ook het consumentendomein, waar klassieke biometrische oplossingen vaak niet op toegerust zijn.

Figuur 12: Mobiele apparaat met geïntegreerde vingerafdruk sensor[49].

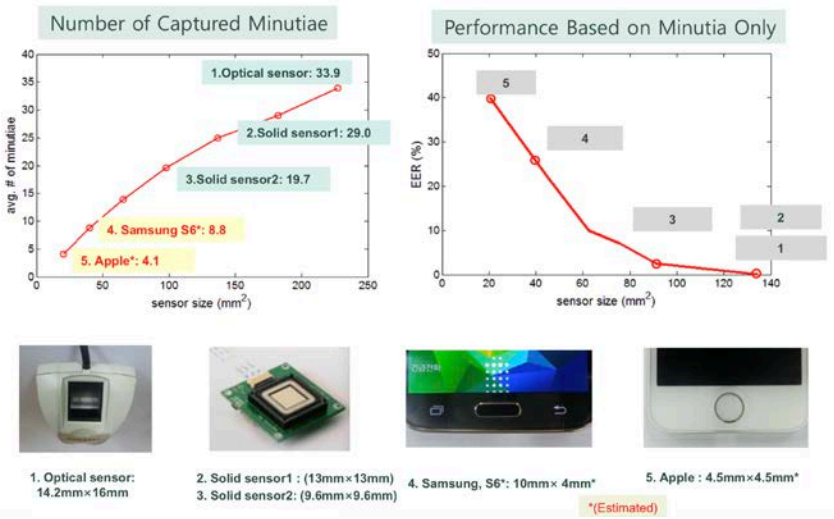
Voordelen van de mobiele biometrische toepassingen zijn toegankelijkheid voor het consumentendomein, gebruikersgemak, portabiliteit, hoge acceptatie door de gebruikers en continue authenticatie.

Nadelen zijn veel verschillen in de kwaliteit van de camera's (zie ook hoofdstuk 4) en de vingerafdruksensoren op de mobiele telefoons en de beveiliging van de templates erop. Door onbeperkte toegang van de gebruiker tot de biometrische sensor is het voorkomen van 'knoeien' met en spoofing van de sensor lastiger. De beveiliging van de communicatie tussen de mobiele app en de sensoren zijn een uitdaging. Hetzelfde geldt voor het geval als er gekozen wordt om de biometrische templates lokaal op te slaan op de mobiel. Het inzetten van de secure enclave of *Trusted Execution Environment* (TEE) van de mobiele telefoon is hiervoor vereist - een omgeving voor het uitvoeren van code, waarin degenen die de code uitvoeren veel vertrouwen kunnen hebben in het activabeheer van die omgeving, omdat het bedreigingen van de "onbekende" rest van het mobiele apparaat kan negeren. Lokale opslag is niet noodzakelijk, zie hoofdstuk 3.

De prestatie van de mobiele vingerafdrukbiometrie varieert afhankelijk van het type en de grootte van de vingerafdruksensor in de smartphone (zie Figuur 13).

Onderzoekers in Japan hebben recent een nieuwe vingerafdruksensor ontwikkeld die ook de zweetporiën in vingers herkent en die op korte termijn geschikt zou zijn voor de integratie in mobiele telefoons[50]. Naar verwachting zal een dergelijke sensor niet alleen helpen de prestatie van de mobiele authenticatie te verbeteren, maar ook om spoofing aanvallen tegen te gaan.

[48] Zie: https://www.biometricupdate.com/201803/dataworks-plus-launches-mobile-device-for-law-enforcement-with-integrated-biometrics-sensor
[49] Zie: https://tascent.com/2019/06/tascent-announces-m1/.
[50] Zie: https://asia.nikkei.com/Business/Technology/Sweat-pores-improve-fingerprint-recognition-tenfold-researchers-say.



Figuur 13: Prestatie van de diverse externe en geïntegreerde mobiele vingerafdruk sensoren [Bron: Kim, J. Mobile Biometrics: Trends and Issues[51]].

Mobiele multimodale toepassingen ontwikkelen zich ook razendsnel, zoals sprekerherkenning aangevuld met gezichtsherkenning voor betere liveness detectie van de gebruiker (
Figuur *14*) of door de toetsaanslagdynamiek tijdens het invoeren van de gebruikersnaam of pincode te combineren met gezichtsherkenning. Een interessante trend is ook het fuseren van fysiologische kenmerken met gedragskenmerken, waardoor biometrische authenticatie betrouwbaarder worden en continue kan worden uitgevoerd (bijvoorbeeld als het gedrag ineens verandert).

Figuur 14: Biometrische mobiele applicatie Knomi gebruikt gezicht en sprekerherkenning.

2.11 Samenvatting

Samengevat kan het volgende worden vastgesteld over biometrie voor het verifiëren van de identiteit:

- Biometrie is niet binair: in tegenstelling tot het gebruik van een wachtwoord of PIN levert biometrie geen binair goed of fout antwoord, maar een waarschijnlijkheid dat het iemand betreft. Er bestaat een kans op een onterecht match (False Acceptance Rate of FAR) of een onterecht afwijzing (False Rejection Rate of FRR). Daarnaast werkt biometrie gewoonweg niet bij bepaalde gebruikersgroepen (Failure To Enroll of FTE) waardoor er altijd een alternatief scenario moet blijven bestaan.
- Biometrische informatie is zeer gevoelig en persoonlijk en moet op een hoog veilige manier behandeld worden. Standaarden, privacy by design en cryptografische technologieën zijn beschikbaar om hierin te voorzien.
- Biometrische systemen zijn relatief eenvoudig te misleiden. Presentation Attack Detection (PAD) oplossingen zijn vereist om dit te voorkomen en de betrouwbaarheid te verhogen.

[51] Zie: http://www.comp.hkbu.edu.hk/wsb17/slides/Jaihie_Kim.pdf.

- De opmars van kunstmatige intelligentie technologieën en IoT hebben een positieve invloed op de betrouwbaarheid en gebruikersvriendelijkheid van de biometrische verificatie.
- Mobiele biometrie is sterk in opkomst getuige het gebruik ervan in de financiële, zorg en telecom sectoren.
- De meest gebruikte en geaccepteerde vormen van biometrie zijn gezichtsherkenning, vingerafdruk en iris.

3. Wettelijke context, standaarden en richtlijnen

Dit hoofdstuk geeft een overzicht van wet- en regelgeving, standaarden en richtlijnen die relevant zijn voor biometrie.

3.1 Wet- en regelgeving rondom biometrie

Hieronder een overzicht van wet- en regelgeving relevant voor gebruik van biometrie voor identificatie en authenticatie in de context van digitale en fysieke overheidsdienstverlening.

De ***Paspoortwet***[52] bevat regelgeving over het Nederlandse paspoort, de (Nederlandse) identiteitskaart en reisdocumenten voor niet-Nederlanders. Reisdocumenten bevatten de volgende biometrische gegevens: gezichtsopname, twee vingerafdrukken en handtekening van de houder. Een uitzondering daarop zijn de Nederlandse identiteitskaart en de vervangende Nederlandse identiteitskaart die niet zijn voorzien van vingerafdrukken. Ook een noodpaspoort bevat geen vingerafdrukken. Op de chip staan de gezichtsopname en de vingerafdrukken; niet de handtekening. De gezichtsopname en de handtekening worden bewaard door de autoriteit die het reisdocument heeft verstrekt, in een administratie die zowel op naam als op documentnummer toegankelijk is. De vingerafdrukken worden maximaal drie maanden bewaard voor verstrekking en (niet-)uitreiking. Biometrische gegevens worden niet opgeslagen in het basisregister reisdocumenten (BR). BR registreert de reisdocumenten die niet in omloop mogen zijn omdat ze van rechtswege zijn vervallen en kan worden geraadpleegd door organisaties met een gerechtvaardigd belang. Reisdocumenten moeten worden aangevraagd bij een bevoegde autoriteit en worden alleen door hen verstrekt aan de aanvrager. De bevoegde autoriteit verschaft zich de nodige zekerheid over de identiteit en de nationaliteit van de aanvrager. De aanvrager moet daarvoor persoonlijk verschijnen en alle in zijn of haar bezit zijnde reisdocumenten overleggen.

Paspoortuitvoeringsregelingen[53] regelen de verstrekking van reisdocumenten door bevoegde instanties, er zijn verschillende varianten: voor Nederland, buiten Nederland, voor de Caribische landen en voor de Koninklijke Marchaussee. De opname van biometrische gegeven pasfoto moet goedgelijkend zijn en voldoen aan het fotomatrix model. De ambtenaar die de aanvraag afhandelt moet dit controleren en (op het oog) beoordelen of de foto van de aanvrager is. De foto wordt bevestigd op het foto- en handtekeningenformulier. Daarop moet de aanvrager in het bijzijn van de ambtenaar een handtekening plaatsen. Twee vingerafdrukken (linker- en rechterwijsvinger) worden afgenomen via het aanvraagstation of een mobile vingerafdrukopname apparaat. Aanvragen lopen via het Reisdocumenten Aanvraag- en Archiefstation (RAAS). Alle biometrische kenmerken worden in de aanvraagmodule opgenomen en doorgestuurd naar het reisdocumentenstation waar de gegevens worden samengevat in een aanvraagbestand dat naar de leverancier gaat. In de paspoortuitvoeringsregeling worden autorisaties voor de administratieve afhandeling geregeld. Alle gegevens bij de aanvraag worden 11 of 16 jaar bewaard. Een aantal daartoe bevoegde personen/instanties hebben toegang tot RAAS. De autorisatiebevoegde reisdocumenten (ABR) bepaalt welke medewerkers welke handelingen op het RAAS mogen verrichten. Per afgiftepunt moeten er minimaal twee autorisatiebevoegden zijn.

EU Verordening Biometrie op reis- en identiteitsdocumenten[54]. Deze verordening treedt in werking in augustus 2021. Om te komen tot een hogere standaard voor de verschillende documenten stelt de Commissie de volgende maatregelen voor:

- Voor ID-kaarten:
  - Een set minimumeisen aan veiligheidskenmerken. Het betreft de ICAO 9303 standaard.

[52] Zie: https://wetten.overheid.nl/BWBR0005212/2017-10-01.
[53] Zie: https://wetten.overheid.nl/BWBR0012811/2018-10-01.
[54] EU Verordening 2019/1157: Enrolment Guidelines. Best Practice Recommendations for the Enrolment of Face and Fingerprint biometric samples for Travel and Identity Documents. EU Commission. Approved by the Article 6 Committee on 27 February 2019. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32019R1157&from=EN.

    - Het opnemen van vingerafdrukken als biometrisch kenmerk in de chip.
- Voor verblijfsdocumenten (o.a. visa, verblijfsvergunningen):
    - Een set minimumeisen aan veiligheidskenmerken op verblijfsdocumenten van EU-burgers die in een ander dan het eigen EU-land wonen. De Commissie hanteert hiervoor dezelfde minimumnormen zoals gesteld in de EU Verordening 1030/2002.
    - Een set minimumeisen aan veiligheidskenmerken op verblijfsdocumenten van gezinsleden van EU-burgers die niet zelf EU-burger zijn. De Commissie hanteert hiervoor dezelfde minimumnormen zoals gesteld in de EU Verordening 1030/2002 en 380/2008.
    - Het opnemen van vingerafdrukken als biometrisch kenmerk in de chip.
- Documenten die voldoen aan de gestelde ICAO-standaard in tien jaar (voor identiteitskaarten) en vijf jaar voor de identiteitsdocumenten die niet voldoen aan ICAO.
- Regels voor het veilig verwerken van de data, zoals biometrische gegevens en persoonsgegevens.

Met deze verordening worden alle reis-, identiteits- en verblijfsdocumenten gelijkgetrokken aan de functionaliteit van het paspoort. Wel heeft Nederland een kanttekening gemaakt bij de te behalen resultaten voor het tegengaan van fraude middels het plaatsen van vingerafdrukken op de chip van de ID-kaart. De reden is dat controle van vingerafdrukken aan de grens nauwelijks wordt toegepast. Overigens ligt dat ook aan het feit dat landen nog niet goed en veilig sleutels kunnen uitwisselen, zodat ze elkaars identiteitsdocumenten kunnen uitlezen. Op dit moment wordt vooral ingezet op (automatische) gezichtsherkenning m.b.v. de foto op het document. Merk op dat het Nederlandse rijbewijs buiten de scope van de verordening valt. Het is alleen binnen Nederland als identiteitsdocument aangewezen (Wet op de Identificatieplicht); in het buitenland is het dus niet geschikt als identificatiemiddel.

Juridisch gezien raakt de EU verordening de Nederlandse Paspoortwet. Daar is nu expliciet geregeld dat de identiteitskaart geen vingerafdrukken bevat.

Het doel van de verordening is een verbetering van de kwaliteit van de documenten en daardoor een verbetering van de controle daarvan. De controle wordt verder vergemakkelijkt doordat de documenten binnen Europa uniformer zijn. Dit geldt zowel voor grenscontroles als andere controles. ‘Veilige’ documenten maken vervalsingen lastiger.

Het vaststellen en vastleggen van identiteiten van personen is één van de taken van het gemeentelijke deel burgerzaken. Daarvoor is het ***ID-protocol Burgerzaken***[55] opgesteld door de NVVB. Deze heeft als doel een eenduidige handelswijze te geven voor medewerkers Burgerzaken, zodat de kwaliteit van de identiteitsvaststelling hoog is om identiteitsfraude te voorkomen. Het bevat instructies, stappenplannen, checklists en formats. Er is een ID-protocol voor managers en voor medewerkers. Het ID-protocol presenteert een gedetailleerd proces voor medewerkers ten aanzien van het controleren van ID documenten en houder verificatie en is daarmee een praktische uitwerking van de Paspoortwet en de Paspoortuitvoeringsregelingen.

Algemene Verordening Gegevensbescherming[56] (AVG) gaat in Artikel 9 in op de verwerking van bijzondere categorieën van persoonsgegevens. Hierin staat dat het verboden is genetische gegevens en biometrische gegevens te verwerken ten behoeve van unieke identificatie van een persoon. Dit geldt niet wanneer de betrokkene nadrukkelijk toestemming heeft gegeven voor bepaalde doeleinden. Het moet dan wel gaan om vrije keuze en zonder negatieve consequenties. Het moet een actieve toestemming zijn op basis van voldoende informatie in begrijpelijke taal. Toestemming van de gebruiker is niet nodig in het geval van het uitvoeren van de wettelijke taak (door de overheid). Verwerking is ook toegestaan wanneer noodzakelijk met het oog op uitvoering van verplichtingen of uitoefening van specifieke rechten voor arbeidsrecht of sociale zekerheids- en sociale beschermingsrecht, ten behoeve van bescherming van vitale belangen van betrokkene, in bepaalde gevallen voor gerechtvaardigde activiteiten of rechtsbevoegdheid, of wanneer deze persoonsgegevens door de betrokkene openbaar zijn gemaakt.

De uitvoeringsverordening van AVG (UAVG) bevat nog een uitzondering voor het verwerken van biometrische gegevens. Deze uitzondering is terug te vinden in art. 29: *“Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te*

[55] https://nvvb.nl/media/cms_page_media/258/ID_protocol_Medewerkers_O21cBfQ.pdf
[56] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/algemene-informatie-avg

verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden."

Dat betekent dat biometrische gegevens verwerkt mogen worden voor identificatie, maar dat dit alleen kan als dit daadwerkelijk noodzakelijk is en er geen minder ingrijpende middelen zijn.

Europese ***eIDAS verordening***[57] over elektronische identiteiten en vertrouwensdiensten. eIDAS is de algemene benaming voor de EU-verordening (EU) nr. 910/2014 die nieuwe regels voor elektronische identificatie en vertrouwensdiensten vaststelt voor elektronische transacties binnen de Europese Unie. Door de certificering van aanbieders van vertrouwensdiensten (Trust Service Providers, TSPs), streeft de eIDAS regulatie naar het verhogen van de interoperabiliteit en rechtszekerheid in grensoverschrijdende online transacties en het bevorderen van een "digitale interne markt" binnen de EU. Binnen eIDAS gekwalificeerde TSPs en hun diensten hebben in alle lidstaten dezelfde status en middelen worden door alle lidstaten erkend wanneer het notificatieproces is doorlopen. Biometrie kan onderdeel zijn van bepaalde gekwalificeerde middelen.

Concept ***Wet Digitale Overheid***[58] is een nieuwe wet in de maak – een Nederlandse vertaling van de eIDAS verordening aangaande toegelaten authenticatiemiddelen.

Webrichtlijnen 2018 / DigiToegankelijk[59] regelt dat websites in het (semi-)overheidsdomein voor iedereen toegankelijk zijn en moet verplicht worden toegepast. De regels gaan in op techniek en vormgevingselementen die ervoor zorgen dat gebruikers de inhoud kunnen begrijpen en toepassen. Dit kan van toepassing zijn op de manier waarop biometrie onderdeel is van het authenticatie proces voor digitale dienstverlening.

Handreiking betrouwbaarheidsniveaus[60] van Forum Standaardisatie. De handreiking adviseert in betrouwbaarheidsniveaus voor digitaal machtigingen, communicatie tussen applicaties, retourstromen, eenmalig inloggen en digitaal ondertekenen. De handreiking promoot toepassing van algemeen inzetbare oplossingen. Biometrie kan als authenticatiefactor worden ingezet om (beter) te voldoen aan betrouwbaarheidsniveaus.

Wegenverkeerswet en het Reglement Rijbewijzen[61] bevat het wettelijke kader voor het rijbewijs, waarin ook de Europese richtlijnen voor het rijbewijs zijn verwerkt. O.a. worden de eisen aan het rijbewijs beschreven, de verschillende voertuigcategorieën en de rijbewijsplicht. Het rijbewijs wordt aangevraagd in de gemeente waar de aanvrager staat ingeschreven. De gemeente moet zich zekerheid verschaffen over de identiteit van de aanvrager. Deze legitimeert zich met een eerder afgegeven en nog geldig rijbewijs, of anders met een reisdocument. Bij twijfel over de juistheid van gegevens of identiteit van de aanvrager wordt het rijbewijzenregister geraadpleegd. De aanvrager moet een foto overleggen die voldoet aan gestelde eisen. De aanvraag wordt geregistreerd in het rijbewijzenregister, daartoe worden gebruikerscodes afgegeven. Er gelden beveiligingseisen voor de afgegeven rijbewijzen en apparatuur voor toegang tot het rijbewijzenregister. Productie, transport en aflevering van een rijbewijs valt onder de verantwoordelijkheid van de Dienst Wegverkeer. Het rijbewijzenregister bevat naast persoonlijke gegevens, gegevens over rijvaardigheid en gegevens over het afgegeven rijbewijs, ook biometrische gegevens als een pasfoto en handtekening. Deze biometrische gegevens staan ook op de chip van het rijbewijs.

De ***Wet op de identificatieplicht***[62] stelt dat de identiteit van een persoon kan worden vastgesteld door middel van de volgende documenten (mits geldig): reisdocumenten, Nederlandse identiteitskaart, diplomatiek of dienstpaspoort, documenten ingevolge de Vreemdelingenwet en het rijbewijs. Vanaf 14 jaar moet iemand zich op verzoek van een bevoegde persoon kunnen legitimeren met één van de genoemde documenten (toonplicht).

[57] Zie: https://www.digitaleoverheid.nl/dossiers/eidas/.
[58] Zie: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/voortgang-wet-digitale-overheid/.
[59] Zie: https://www.digitoegankelijk.nl/.
[60] Zie: https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus.
[61] Zie: https://rijbewijs.nl/wet-regelgeving/.
[62] Zie: https://wetten.overheid.nl/BWBR0006297/2017-03-01

In de ***Politiewet***[63] worden de bevoegdheden van politie en marechaussee geregeld, o.a. met betrekking tot het identificeren. Hierin staat dat politieambtenaren, opsporingsambtenaren en militairen van de marechaussee bevoegd zijn een identiteitsbewijs te vorderen t.b.v. inzage wanneer dat redelijkerwijs noodzakelijk is voor de uitvoering van hun politie- of opsporingstaak. Identificatieplicht strekt zich verder uit tot toezichthouders, beveiligers, conducteurs, financiële instellingen voor gedefinieerde doeleinden[64].

De politie mag een verdachte dwingen om zijn eigen smartphone met een vingerafdrukscan te ontgrendelen. De methode is niet in strijd met het beginsel dat een verdachte niet mee hoeft te werken aan zijn eigen veroordeling, zo oordeelde recentelijk de rechtbank Noord-Holland[65]. Een verdachte kan niet gedwongen worden om de toegangscode van een smartphone af te staan, omdat deze verklaring wél valt onder het beginsel dat verdachten niet gedwongen kunnen worden aan hun eigen veroordeling mee te werken. Een ontgrendeling door middel van biometrische gegevens valt hier niet onder, stelde de rechter, omdat het van de verdachte geen "actieve medewerking" eist.

Immigratie- en Naturalisatie Dienst (IND) in Nederland is verantwoordelijk voor de afgifte van het verblijfsdocument[66]. Tijdens een aanvraag en vernieuwing van het verblijfsdocument worden de volgende biometrische kenmerken afgenomen: gezichtsopname, tien vingerafdrukken en de handtekening. Afname en vastlegging van de biometrische kenmerken vindt momenteel fysiek plaats op een van de IND-loketten. Deze biometrische gegevens worden centraal opgeslagen in de Basisvoorziening Vreemdelingen (BVV). Er is een fysieke verschijningsplicht voor het ophalen van het verblijfsdocument.

3.2 Standaarden voor biometrische verificatie

Er zijn verschillende technische standaarden die normen voorschrijven voor biometrische verificatie van de identiteit of die de interoperabiliteit bevorderen. Deze zijn belangrijk voor de praktische toepassing van biometrische verificatie. De belangrijkste zijn:

- ***BioAPI – Biometric Application Programming Interface (BioAPI)***[67]: beschrijft de communicatie tussen verschillende modules of systemen in een biometrische toepassing op basis van het Biometric Interworking protocol (BIP). De adoptie van de BioAPI standaard is overigens nog erg laag. ISO 24709 biedt een testraamwerk voor BioAPI.
- ***ISO/IEC 24745:2011***[68]: beschrijft eisen voor de beveiliging en verwerking van biometrische informatie, inclusief eisen voor vertrouwelijkheid, integriteit en vernieuwbaarheid/herroepbaarheid tijdens opslag en uitwisseling.
- ***ISO 19794 en ISO 29109 – ISO 19794***[69]***:*** beschrijven uitwisselingsformaten voor biometrische data. Biometrische data op paspoorten (vingerafdrukken en foto) dienen hieraan te voldoen. ISO 19794 staat zowel formaten toe waarin biometrische kenmerken als originele 'ruwe' beelden uitgewisseld worden, als formaten waarin specifieke kenmerken ("minutiae") uitgewisseld worden. ISO 29109 beschrijft een testraamwerk hiervoor.
- ***FIDO – De FIDO alliantie***: een consortium van organisaties waaronder PayPal en Lenovo, heeft in 2013 FIDO (Fast Identity Online) geïntroduceerd. FIDO is een authenticatiestandaard die wordt ondersteund door een lijst van bedrijven. FIDO maakt het makkelijker om niet alleen gebruikersnaam/wachtwoord te gebruiken voor authenticatie, maar ook andere vormen zoals biometrie, bijvoorbeeld de vingerafdruksensor van een smartphone. FIDO voorziet in het 'bring-your-own-identity' paradigma, waarbij de gebruiker zelf bepaalt hoe hij/zij zichzelf wenst te authentiseren.
- ***BOPS – De Biometric Open Protocol Standard (BOPS)***[70] :ontwikkelt op initiatief van biometrie-aanbieder Hoyos Labs, werd in September 2015 door IEEE geadopteerd als IEEE 2410-2015. De standaard beschrijft een systeem voor online biometrische authenticatie en identificatie, en is op veel punten vergelijkbaar met

[63] Zie: https://wetten.overheid.nl/BWBR0031788/2019-02-01.
[64] Zie: https://www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn-identiteitsbewijs-en-wanneer.
[65] Zie: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Noord-Holland/Nieuws/Paginas/Phishing-bende-veroordeeld-gedwongen-ontgrendeling-iPhone-met-vingersensor-rechtmatig.aspx.
[66] Zie: https://ind.nl/Paginas/Afspraak-afnemen-biometrie.aspx.
[67] Zie: https://www.nist.gov/itl/csd/biometrics/bioapi-conformance-test-suite/bioapi-cts-user-guide-and-download.
[68] Zie: https://www.iso.org/standard/52946.html.
[69] Zie: https://www.iso.org/standard/73505.html.
[70] Zie: https://ieeexplore.ieee.org/document/8089818.

FIDO. Specifiek kenmerk van BOPS is het splitsen van de biometrische template in twee delen zodat het compromitteren van een van de delen niet leidt tot het compromitteren van het algeheel biometrische kenmerk.

- ***ISO/IEC 30107-1:2016 Presentation Attack Detection***[71]: beschrijft hoe een biometrisch systeem met "Presentation Attack Detection" (PAD) is opgebouwd. Deel 1 beschrijft het PAD raamwerk voor de specificatie, detectie en categorisatie van presentation attack events, deel 2 – data formats en deel 3 – PAD testen en rapporteren van resultaten.
- ***ISO 19092:2008 – Financial services - Biometrics - Security framework***: beschrijft een beveiligingsraamwerk voor het gebruik van biometrie voor het authentiseren van personen door financiële dienstverleners. Het introduceert verschillende soorten biometrische oplossingen en aandachtspunten. Ook wordt een architectuur voor het inzetten ervan beschreven.
- ***NFIQ2: NIST Fingerprint Image Quality***: beschrijft een gestandaardiseerde oplossing voor het bepalen van de kwaliteit van vingerafdrukken.

3.3 Richtlijnen biometrie en (online) authenticatie

Naast de bovengenoemde biometrie standaarden, zijn er diverse internationale en nationale richtlijnen voor biometrie en digitale authenticatie. Deze sectie geeft het overzicht van de belangrijkste richtlijnen die relevant zijn voor dit onderzoek.

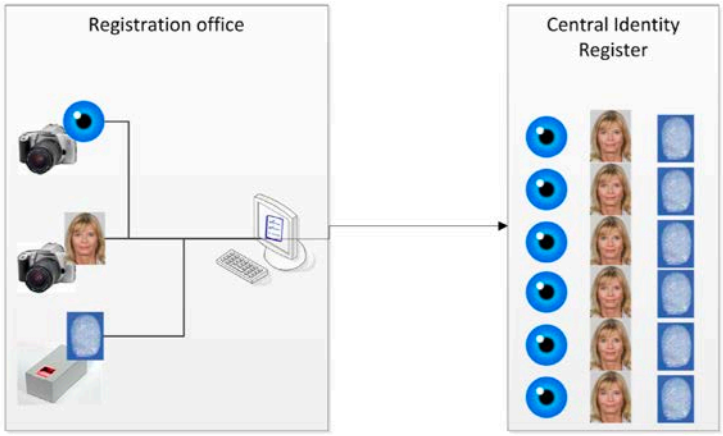
NIST 800-63-3 Digital Identity Guidelines[72] – Deze richtlijn beschrijft de eisen voor de evaluatie van de authenticatie-oplossingen, die ook toegepast kunnen worden voor (online) biometrische authenticatie. NIST doet hierin ook uitspraken over de biometrische authenticatie-oplossingen en met name over de prestaties van de biometrische component om tot een bepaald niveau van betrouwbaarheid te komen.

Vanwege de beperkingen van biometrie worden de volgende technische eisen opgelegd voor toepassing van biometrie[73]:

- Biometrie mag alleen worden toegepast wanneer het een onderdeel is van multi-factor authenticatie.
- Opzetten van een beveiligd communicatiekanaal tussen de sensor of het eindpunt voor de biometrie en de dienst.
- De biometrie oplossing past een False Match Rate (FMR ofwel FAR), zoals gedefinieerd in ISO/IEC 2382-37, toe van 1 op 1000 of beter. Deze wordt bepaald door een "zero-effort impostor attempt": een bedrieger-poging wordt geclassificeerd als "nul-inspanning" als de persoon zijn/haar eigen biometrische kenmerk indient alsof hij/zij een succesvolle verificatie probeert uit te voeren met zijn/haar eigen biometrische template, maar de vergelijking wordt gemaakt met de template van een andere gebruiker.
- De biometrie oplossing past PAD toe. Testen moet volgens artikel 12 van ISO/IEC 30107-3.
- Om 'brute force' aanvallen tegen te gaan: na 5 pogingen voor authenticatie via biometrie (en 10 wanneer PAD wordt toegepast) moet er een pauze van minimaal 30 seconden worden ingelast voordat de volgende poging wordt gedaan, daarna voor elke mislukte de pauzes exponentieel verlengen of de biometrie authenticatie wordt afgebroken en een andere (extra) authenticator wordt aangeboden (een andere biometrie oplossing, PIN of Passcode).
- Het biometrische verificatiesysteem zal zorgen voor het vaststellen van de nauwkeurigheid, integriteit, en authenticiteit van de sensor en het eindpunt.
- De biometrische vergelijking kan decentraal (lokaal) of centraal (server) worden uitgevoerd. Omdat het potentieel voor grootschalige aanvallen groter is bij centrale verificateurs, heeft lokale vergelijking de voorkeur. Wanneer de vergelijking centraal wordt uitgevoerd, dan gelden de volgende eisen:
  - Er zijn enkele specifieke aangewezen apparaten voor de verwerking die goedgekeurde cryptografie toepassen. Dit is niet dezelfde cryptografie sleutel als die voor de identificatie van het apparaat.
  - Een revocatie proces (biometric template protection in ISO/IEC 24745) moet worden toegepast.
  - Transport van biometrische gegevens over een beveiligde communicatielijn.

[71] Zie: https://www.iso.org/standard/53227.html.
[72] Zie: https://doi.org/10.6028/NIST.SP.800-63-3.
[73] NIST 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management, zie: https://doi.org/10.6028/NIST.SP.800-63b.

De richtlijn voor het gebruik van biometrie in de publieke sector van de ***Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI)***[74] beschrijft de technische specificaties voor het gebruik van biometrische systemen in de publieke sector, gebaseerd op de internationale biometrie standaarden en wettelijke kaders. Er zijn twee use-cases voor biometrie gedefinieerd. De eerst use-case is grenscontrole door de politie en beschrijft het de eisen voor technologie leveranciers ten behoeve van de verificatie van ePassport en identiteitsdocument tijdens grenscontrole. De scope van BSI is gezichtsbiometrie, vingerafdruk en irisscan. Biometrische verificatie wordt mogelijk gemaakt doormiddel van Centrale Identiteiten Register (CIR) die faciliteert alle verzoeken voor de opslag en het creëren van templates voor de biometrische matching van de biometrische en biografische gegevens. Een identiteitsprofiel bestaat uit een gezichtsfoto, tien vingerafdrukken en twee iris beelden. Deze worden vastgelegd bij een registratiekantoor en daarna gecodeerd naar CIR gestuurd. CIR bewaart deze profielen centraal of desgewenst decentraal (zie ook Figuur 15).



Figuur 15: Richtlijn BSI voor opslag van biometrische gegevens [Bron: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03121/index_htm.html]

Een hoge kwaliteit van de live waargenomen biometrische kenmerken is een belangrijke voorwaarde voor een betrouwbare vergelijking met de reeds opgeslagen biometrie (referentie beeld) in het ePassport.

De tweede BSI use-case beschrijft de enrolment van de specifieke identiteitsdocumenten: elektronische Passport, Duitse identiteitskaart en Duitse elektronische verblijfsvergunning. Dit betreft zowel de fysieke enrolment aan de balie als de 'live' enrolment bij een speciaal station. In de fysieke enrolment scenario wordt de geprinte foto gemaakt door de fotograaf en aangeleverd door de aanvrager. In het geval van live enrolment wordt de foto elektronisch gemaakt en elektronisch aangeleverd. De vingerafdrukken worden nog extra aan de balie afgenomen voor de latere verificatie. Verificatie vindt plaats tegen de reeds enrolde vingerafdrukken om te controleren dat de legitieme vingerafdrukken afgenomen zijn bij het live enrolment station. In het geval van een mislukte verificatie moet de enrolment herhaald worden aan de balie. In het geval van de Duitse identiteitskaart, is de foto verplicht en de vingerafdrukken zijn optioneel volgens de Duitse wetgeving. De kwaliteit van de biometrische template wordt gewaarborgd door een softwarematige Quality Assurance module die geïntegreerd is in de live enrolment stations.

3.4 Toegang tot biometrische gegevens en huidige voorzieningen

Tot 2002 was inzage door de politie in de toenmalige vingerafdrukkendatabank van asielzoekers en ongedocumenteerden in Nederland standaard toegestaan. Daaraan kwam een eind door de Wet bescherming persoonsgegevens. In Duitsland is politietoegang wel standaard toegestaan.

De plannen van de Nederlandse overheid om vingerafdrukken centraal vast te leggen is door diverse redenen niet door gegaan. In 2011 gaf toenmalig minister Donner aan hiervan voorlopig af te zien. Er is destijds gekozen om de vingerafdrukken alleen op te slaan in de chip van het paspoort.

[74] BSI TR-03121 Biometrie in hoheitlichen Anwendungen, zie: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03121/index_htm.html.

Tabel 4 toont een overzicht van de voor de Nederlandse overheid beschikbare bronnen op basis waarvan biometrische verificatie van de identiteit gedaan zou kunnen worden. Opsporing en grenscontrole zijn buiten de scope.

Tabel 4: Overzicht van de huidige overheidsbronnen van biometrische gegevens voor reisdocumenten.

Bron biometrische gegevens	Architectuur	Soort gegeven	Toegang
Paspoort, Identiteitskaart, Rijbewijs, Verblijfsdocument	Decentraal (digitaal in een document)	Gezicht	Iedereen die toegang heeft tot de chip, altijd op basis van MRZ.
Paspoort, Identiteitskaart	Decentraal (digitaal in een document)	Vingerafdruk	KMar, gemeenten, Nederlandse ambassades en consulaten, uitgevende instanties in het Caribisch deel.
Verblijfsdocument	Decentraal (digitaal in een document)	Vingerafdruk	IND, BZ, KMar, Nederlandse ambassades en consulaten, uitgevende instanties in het Caribisch deel.
Paspoort, Identiteitskaart, Rijbewijs, Verblijfsdocument	Decentraal (digitaal in een document)	Handtekening	KMar, gemeenten, IND, Nederlandse ambassades en consulaten, uitgevende instanties in het Caribisch deel.
Basisvoorziening Vreemdelingen (BVV)	Centraal	Vingerafdruk	IND
RDW database	Centraal	Gezicht	RDW, Politie
Reisdocumenten Aanvraag- en Archiefstation (RAAS)	Centraal	Gezicht, Handtekening	Gemeenten, BZ, KMar. Vingerafdruk slechts tot het document is uitgegeven en max 90 dagen.

De nieuwe wet EU verordening biometrie op identiteitskaarten staat toe dat de vingerafdrukken uitgelezen mogen worden voor het verifiëren van de identiteit van de reizigers op het moment dat ze zich in een ander EU-land bevinden. Hierdoor ontstaat binnenkort mogelijk de situatie dat de Nederlandse politie bij een controle wel de gegevens van de ID-kaart mogen inzien, maar niet die op het paspoort. Momenteel identificeert de politie alleen onbekende doden aan de hand van de vingerafdrukken in het paspoort. De politie moet dat wel naar een gemeente op de gegevens uit de chip in het paspoort te laten uitlezen.

Huidige voorzieningen in Nederland en de EU

De Europese Unie heeft de visumdatabank VIS[75], waarin alle vingerafdrukken komen van mensen die een visum aanvragen voor één van de EU-landen[76]. Asielzoekers moeten nu al hun vingerafdruk afgeven wanneer ze zich in een EU-land melden. De huidige databank die daarbij hoort, Eurodac, wordt gekoppeld aan VIS. Eurodac is een databank met vingerafdrukken van asielzoekers die wordt gebruikt ter ondersteuning van het gemeenschappelijk asielbeleid van de Europese Unie.

Een ander bronsysteem betreft het vernieuwde Schengen Informatie Systeem (SIS II) [77], waar arrestatiebevelen en gegevens over personen en goederen als gestolen auto's in staan. SIS II bevat ook pasfoto's en vingerafdrukken. SIS II moet de lidstaten helpen om grensoverschrijdende criminaliteit en mensensmokkel aan te pakken. De biometrie wordt gebruikt door diverse instanties om personen te kunnen identificeren en opsporen.

3.5 Centrale versus decentrale opslag van biometrische gegevens

Als we kijken naar de huidige bronnen van biometrische gegevens (zie vorige sectie 3.4), zien we zowel centrale als decentrale oplossingen. Het uitvoeren van de biometrische verificatie van de identiteit kan met gegevens die centraal of decentraal zijn opgeslagen. Deze sectie beschouwt de voor- en nadelen van beide opslagopties.

[75] Zie: https://www.gegevensbeschermingsautoriteit.be/visa-informatie-systeem.
[76] Zie: https://www.nrc.nl/nieuws/2008/05/14/veiliger-dan-een-wachtwoord-maar-niet-waterdicht-11537330-a137966.
[77] Zie: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=LEGISSUM%3Al14544

Het aanleggen van centrale databases met biometrische informatie kan grote privacy-gevolgen hebben. Zo wordt Facebook ervan beschuldigd biometrische informatie van gebruikers te verzamelen zonder hun toestemming[78]. In Europa past Facebook geen automatische gezichtsherkenning toe.

Dergelijke bezwaren tegen een centrale database komen terug in de zienswijze van de Artikel 29-werkgroep[79], waarin alle privacy-toezichthouders van Europa zijn verenigd. De werkgroep schrijft bijvoorbeeld in zijn opiniedocument het volgende: "De centrale opslag van gegevens, vooral in grote databases, brengt risico's met zich mee op het gebied van beveiliging, het koppelen aan personen en function creep. Dit kan er bij de afwezigheid van waarborgen voor zorgen dat vingerafdrukken voor een ander doel worden gebruikt dan waarvoor ze in eerste instantie zijn verkregen." Centrale opslag moet volgens de werkgroep dan ook vermeden worden, tenzij het nodig is voor specifieke doeleinden. In Nederland speelde deze discussie rond de opslag van vingerafdrukken door de overheid, waarbij het Gerechtshof Den Haag in 2014 oordeelde dat centrale opslag niet was toegestaan, omdat dit niet betrouwbaar genoeg is[80]. De Raad van State sprak zich later ook tegen centrale opslag uit.

Centrale opslag is meestal vereist wanneer 1:n identificatie plaats moet vinden en waarbij biometrische gegevens van meerdere personen moet worden vergeleken. Een voordeel van centrale opslag is dat de beveiliging ervan veel beter in te richten is[81]. Een centrale database is middels maatregelen als firewalls, toegangsrestricties, logging en monitoring en certificeringen/audits veel beter en efficiënter te beveiliging dan een decentrale oplossing. Deze laatste oplossing is bijvoorbeeld het geval bij mobiele biometrie. Daar is het door een diversiteit aan platformen en de inherente beperkte mogelijkheden van de mobiel zelf veel lastiger om de veiligheid van de biometrische gegevens te borgen.

Een groot risico is dat als de centrale database gecompromitteerd raakt en kwaadwillenden toegang krijgen tot biometrische gegevens, er veel identiteitsslachtoffers kunnen vallen. Zaak is dus om niet de ruwe biometrische gegevens te verwerken maar afgeleide vormen hiervan zoals templates en gebruik te maken van versleuteling. Bijvoorbeeld door gebruik te maken van de homomorfische encryptie (zie sectie 2.6).

Een decentrale oplossing voor het verwerken van biometrische gegevens is door ze op een aparte drager zoals het paspoort of een smartcard op te slaan. Deze oplossing is relatief duur maar heeft als voordeel dat het veel minder privacyrisico's met zich meebrengt. Er is minder sprake van function creep en er hoeven veel minder privacygevoelige gegevens te worden gecommuniceerd over internetkanalen. De schade van één gecompromitteerd biometrisch paspoort is veel minder groot dan dat bij een centrale database met biometrie.

Betreffende performance scoort een centraal systeem beter. Door de veel grotere processing capaciteit van een centrale server zal er sneller een uitspraak kunnen worden gedaan over de identiteit van de persoon. Een decentrale oplossing, bijvoorbeeld lokaal op de mobiele telefoon of op de chip van een document, is hierin meer beperkt. Een ander voordeel van een centrale oplossing is dat fraudedetectie veel eenvoudiger en effectiever in te richten is ten opzichte van een decentraal systeem. Wanneer de vergelijking centraal wordt uitgevoerd, moet het biometrische systeem aan de volgende eisen van NIST[82] voldoen:

- Er zijn enkele specifieke aangewezen apparaten voor de verwerking die goedgekeurde cryptografie toepassen. Dit is niet dezelfde cryptografie sleutel als die voor de identificatie van het apparaat.
- Een revocatie proces (biometric template protection in ISO/IEC 24745) moet worden toegepast.
- Transport van biometrische gegevens over een beveiligde communicatielijn.

De onderstaande Tabel 5 zet de voor- en nadelen van centrale en decentrale biometrische systemen op een rijtje.

[78] Zie: https://www.theverge.com/2019/8/8/20792326/facebook-facial-recognition-appeals-decision-damages-payment-court.
[79] Zie: https://ec.europa.eu/newsroom/article29/news-overview.cfm.
[80] Zie: https://tweakers.net/nieuws/94397/hof-overheid-mag-vingerafdrukken-niet-centraal-opslaan.html.
[81] Zie: https://www.aware.com/blog/portfolio-items/server-device-based-mobile-authentication/.
[82] Zie: https://doi.org/10.6028/NIST.SP.800-63-3.

Tabel 5: Voor- en nadelen van een centrale vs. decentrale biometrische systeem.

Architectuur	Voordelen	Nadelen
Centraal	Beter te beveiligen Betere performance (nauwkeuriger) Goedkoop Fraudedetectie eenvoudiger Geschikt voor identificatie toepassingen	Grote risico indien gecompromitteerd Privacy Function creep Politiek gevoelig Toegangscontrole uitdagend
Decentraal	Toegangscontrole simpeler Privacy Minder function creep Minder politiek gevoelig Geschikt voor verificatie toepassingen	Slechter te beveiligen Revocatie lastiger Mindere performance Duur Fraudedetectie lastiger

3.6 Samenvatting

Samengevat zijn de volgende aspecten rondom wettelijke kaders, standaarden, richtlijnen en opslag van biometrische gegevens van belang:

- Het toepassen van biometrie en het verwerken van biometrische gegevens kent uitgebreide wet- en regelgeving. Denk aan de paspoortwet en onderliggende regelgeving en de wet- en regelgeving rondom rijbewijzen waarin wordt gesteld hoe pasfoto's, vingerafdrukken en handtekeningen worden afgenomen en verwerkt. Opslag ervan vindt plaats op de chip van het identiteitsdocument. Gezicht, vingerafdruk en handtekening staan op de chip van het paspoort en de identiteitskaart. Gezicht en handtekening kenmerken staan op de chip van het rijbewijs, maar geen vingerafdrukken.
- De onlangs in werking getreden EU verordening 2019/1157 verplicht het plaatsen van vingerdrukken op identiteitskaarten en wordt momenteel geïmplementeerd in Nederland. Hiermee neemt de beschikbaarheid van biometrische templates op wettelijke identiteitsdocumenten verder toe.
- De toegang tot biometrische gegevens in huidige Nederlandse identiteitsdocumenten en het gebruik ervan is wisselend. Toegang tot de pasfoto op de chip is geen probleem. Vingerafdrukken laten zich op dit moment minder eenvoudig ontsluiten; de-facto kunnen alleen gemeenten hier nu bij. Dientengevolge wordt alleen de pasfoto gebruikt voor identificatie- en authenticatiedoeleinden.
- De AVG bepaalt dat de verwerking van biometrische persoonsgegevens een verwerking van bijzondere persoonsgegevens is. Volgens de AVG is het verwerken van biometrische gegevens om iemand te identificeren in beginsel verboden. Nederland heeft in de Uitvoeringswet AVG bijkomende voorwaarden hierover vastgesteld. Het verbod op het verwerken van biometrische gegevens is in Nederland niet van toepassing als de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.
- Huidige internationale standaarden en richtlijnen voor biometrie zijn vooral gericht op gezicht- en vinger-biometrie en worden nog onvoldoende breed toegepast.
- Toegang tot de chip in het paspoort in Nederland is voorbehouden aan gemeenten en de marechaussee. De Justitionele Informatiedienst regelt deze toegang. Drie biometrische modaliteiten zijn inzetbaar voor de verificatie van de identiteit: gezicht, vinger en handtekening.
- Huidige opslag van biometrische gegevens is zowel centraal als decentraal ingericht en niet verbonden met elkaar.
- De manier van verwerking van biometrische gegevens (centraal of decentrale opslag) is een aandachtspunt met betrekking tot privacy en veiligheid. Zowel centraal als decentraal opslagopties kennen zijn voor- en nadelen. De afweging moet voor elke toepassing gemaakt worden, afhankelijk van het doel en de specifieke use-case.
- NIST eisen gelden voor centrale vergelijking van biometrische templates.

De manier van verwerking van biometrische gegevens (centraal of decentrale opslag) is een aandachtspunt met betrekking tot privacy en veiligheid. Zowel centraal als decentraal opslagopties kennen voor- en nadelen. De afweging moet voor elke toepassing gemaakt worden, afhankelijk van het doel en specifieke use-case. NIST eisen gelden voor centrale vergelijking van biometrische templates.

4. Overzicht van biometrie oplossingen

In dit hoofdstuk geven we een overzicht van mogelijke biometrische oplossingen. Op basis van literatuuronderzoek en interviews met experts is een shortlist gemaakt van biometrische modaliteiten die momenteel in de praktijk worden toegepast[83]. Een overzicht wordt gegeven in Tabel 6 en in de navolgende secties worden de verschillende modaliteiten verder toegelicht.

Tabel 6: Overzicht van biometrische modaliteiten.

Biometrische modus	Uitleg
Vingerafdruk	De vingerafdruk kan op verschillende manieren worden afgenomen. Vingerafdruksensoren worden steeds nauwkeuriger en toegankelijk voor dagelijks gebruik, zelfs via eigen smartphone. Dit maakt vingerafdruk makkelijk in het gebruik, maar ze werken niet altijd optimaal en vingerafdrukken die men overal achterlaat zijn te kopiëren.
Irisscan	De iris is consistent in de tijd, en presteert goed. Hiervoor is Near Infrared (NIR) infrarood licht vereist, bijvoorbeeld middels een extra LED op een smartphone, en een camera. Irisscans zijn moeilijk te simuleren, maar dit is soms mogelijk met een hoge resolutiefoto, dus idealiter gaat dit gecombineerd met liveness detectie.
Netvliesscan	Het netvlies wordt vaak verward met de iris, maar is een ander biometrisch kenmerk. Ook voor netvliesscans is NIR licht nodig. Een nadeel is dat de camera relatief dicht bij het gezicht gehouden moet worden en dat aantasting van de ogen verificatie in de weg kan staan. In 2015 is de eerste smartphone gepresenteerd die netvliesherkenning ondersteunt.
Vingeraderpatronen	De aderpatronen in handen en vingers zijn ook identificerend. Hier is wel een speciale sensor voor nodig. Als biometrisch kenmerk wordt dit bijvoorbeeld toegepast in chipkaarten met aderscan-technologie.
Handaderherkenning[84]	Handaderherkenning is een van de recente biometrie technologieën; een contactlosse sensor gebruikt NIR infrarood licht om de unieke vasculaire patronen in de palm bloot te stellen. Fujitsu heeft een patent op de handader biometrie technologie. In 2019 is de eerste smartphone LG G8 THinQ met mobiele handader authenticatie gelanceerd. Zeer veilige en nauwkeurige technologie, uniek zelfs voor de tweelingen (Sabhanayagam et al., 2018; Parihar and Jain, 2019). Nadelen: nog in ontwikkeling en niet voldoende getest.
Oogaderpatronen	De aderpatronen in het oogwit zijn ook identificerend. Dit kan als biometrisch kenmerk worden afgenomen met een conventionele camera op bijvoorbeeld een smartphone. De firma EyeVerify heeft een patent op deze technologie.
Gezichtsherkenning	Gezichtsherkenning vindt plaats met een gewone camera op bijvoorbeeld een smartphone en is een zeer volwassen biometrische technologie. Recentelijk is er ook veel aandacht voor 3-dimensionale opnames van gezichten voor biometrische toepassingen. Gezichtsherkenning is echter niet altijd betrouwbaar of functioneel.
Hartslagherkenning	De hartslag is een biometrisch kenmerk dat middels een elektrocardiogram wordt afgenomen. Apparaten als smartphones en wearables bevatten sensoren die deze toepassing mogelijk maken. Een voordeel is dat de hartslag ook gebruikt kan worden voor continue authenticatie. Het nadeel is dat de hartslag is invasief.
Sprekerherkenning	Sprekerherkenning (wie spreekt), niet te verwarren met spraakherkenning (wat wordt er gezegd), is ook geschikt voor biometrische authenticatie. Dit is echter

[83] *DNA* wordt wel onderaan beschreven maar is niet in de shortlist meegenomen doordat de DNA-gebaseerde biometrische oplossingen momenteel niet toegankelijk zijn voor breed publiek en worden momenteel vooral toegepast in de context van opsporing wat buiten de scope van dit onderzoek valt.

[84] *Handgeometrie* (gebruikers identificeren aan de hand van de vorm van hun handen) is niet meegenomen in de shortlist omdat het minder uniek dan handader, vingerafdruk en iris biometrie. Handgeometrie wordt daardoor veel minder toegepast.

	lastig te registreren, verschillende microfoons beïnvloeden het proces, het is niet optimaal betrouwbaar, en vaak onpraktisch voor de gebruiker. Het is als tweede factor in authenticatie wel groeiende, mede door de opkomst van persoonlijke assistentietoepassingen als Siri en Cortana die gebruik maken van spraakherkenning.
Handtekening	Het handschrift, met name een handgeschreven handtekening, is geschikt voor biometrische authenticatie, bijvoorbeeld door een handtekening op het scherm van een smartphone te zetten. Hiervoor bestaat al een beperkte markt met apps. Een stylus of speciale pen is vaak noodzakelijk.
Gebruikersinteractie	De interactie van de gebruiker met software is ook identificerend. Bijvoorbeeld in de vorm van toetsaanslagen-herkenning of vergelijking van de context van het gebruik (eerder gebruik, tijd, locatie, etc.). Hoewel dit geschikt is voor continue authenticatie, is het minder geschikt als tweede factor en kleven er privacy-bezwaren aan deze aanpak.

Beoordelingscriteria

Om de verschillende biometrische identificatie-oplossingen op een objectieve manier te kunnen beoordelen is een beoordelingskader essentieel. Het globale beoordelingskader is gebaseerd op de literatuur (German en Barber, 2017), theoretische kader en het beoordelingskader dat InnoValor voor SURFnet ontwikkeld heeft in 2016, en ook daarna aangescherpt werd in andere opdrachten. Het definitieve beoordelingskader dat in dit rapport wordt gebruikt is afgestemd met de begeleidingscommissie en met de klankbordgroep. Onderstaande tabel geeft een overzicht en toelichting van de gekozen beoordelingscriteria[85].

Symbool	Criterium	Definitie	Uitleg
	**Betrouwbaarheid**	Hoe presteert de biometrische factor of applicatie in kwantitatieve scores.	FTE: failure to enrol; FAR: false acceptance rate; FRR: false rejection rate; Meetbaarheid; Presentation Attack Detection (PAD).
	**Privacy**	In hoeverre is de privacy waarborging mogelijk tijdens het verifiëren van de identiteit.	Privacy risico's, bescherming persoonsgegeven conform AVG.
	**Veiligheid**	Hoe veilig is deze biometrische modus voor het verifiëren van de identiteit.	Bescherming tegen onrechtmatige toegang; Mogelijkheden voor omzeilen.
	**Universaliteit**	In hoeverre deze biometrische modus universeel inzetbaar is.	Beschikbaarheid sensors, bijv. in fysieke en online authenticatie scenario, mede afhankelijk van penetratie; Functioneert onder alle omstandigheden, e.g. op alle locaties; Functioneert in de tijd, e.g. het biometrisch kenmerk blijft herkenbaar.
	**Gebruiksgemak**	Hoe gebruiksvriendelijk is deze biometrische modus voor het verifiëren van de identiteit?	Complexiteit en effort; Hoe intrusief is deze oplossing.
	**Praktische toepasbaarheid**	Leent de oplossing zich voor de Nederlandse overheid?	Geschikt voor doelgroep Geschikt voor authenticatie/2 factor authenticatie; Schaalbaarheid; Gunstige business case; Volwassenheid van de technologie; Volwassenheid van de markt.

[85] Onderscheidend vermogen van biometrie is meegenomen in de keuze van biometrische modaliteiten, maar niet als een aparte criteria opgenomen. Er is bewust gekozen om een beperkte set van de belangrijkste beoordelingscriteria aan te houden in afstemming met de klankbordgroep.

De gekozen beoordelingscriteria zijn iteratief opgesteld. In de eerste iteratie zijn de gekozen criteria gebaseerd op de resultaten van het desktoponderzoek, geschiktheid voor de beoordeling van de biometrische authenticatie oplossing, resultaten van de interviews, eerdere onderzoeken. In de tweede iteratie is de lijst van criteria gevalideerd met de klankbordgroep en op basis van de validatie is privacy als aparte criteria opgenomen.

4.1 Vingerafdruk

Huidpapillen op de oppervlakte van de vingers vormen afdrukken van papillaire lijnen, beter bekend als vingerafdrukken. Deze patronen zijn identificerend en blijven relatief ongewijzigd tijdens het ouder worden. Vingerafdrukken kunnen voor forensische opsporingsdoeleinden gebruikt worden, maar ook voor identificatie- en authenticatiedoeleinden. Typisch worden hiervoor de uiterste vingerkootjes benut. Ook meerdere vingers zijn mogelijk. De vingerafdruk is een zeer stabiel biometrisch kenmerk vanaf 12 jaar en re-enrolment is wenselijk elke 5-10 jaar (Galbally et al., 2018; Yoon en Jain, 2015).

Naast traditionele registratie met inkt en papier, wordt nu vooral elektronische registratie gebruikt via optische, ultrasone, capacitieve (huidgeleidende) of thermische sensoren. De opkomst van vingerafdruk-biometrie op smartphones heeft deze vorm van biometrie naar de massa gebracht, meestal via een capacitieve sensor, maar gebruik van een camera (optisch) of ultrasone sensoren komen in toenemende mate ook voor. Motorola was een van de eerste ontwikkelaars die een dergelijke technologie aanbood, maar inmiddels bieden vrijwel alle grote smartphoneleveranciers deze technologie. Apple introduceerde in de iPhone 5S in 2013 Touch ID technologie. Er wordt voorspeld dat in 2020 tenminste 34% van alle mobiele devices een vingerafdruk reader zal hebben. Qualcomm heeft zelfs een vingerafdruk reader in ontwikkeling die ultrasoon een afdruk neemt in 3D, dus op afstand. Dit werkt ook als een vinger vochtig of vuil is, en scant zelfs door glas of plastic heen. Hoyos Labs heeft een oplossing die vier vingers gelijktijdig scant met de gewone smartphone camera, gebruik makend van de flitser. Volgens een onderzoek van IHS zal de markt voor vingerafdruk sensors groeien tot $1.7 miljard in 2020. Naast de markt voor vingerafdruksensors is er ook een groot aanbod aan vingerafdruksoftware. Er zijn verschillende aanbieders voor generieke 2-factor authenticatie applicaties die vingerafdrukken ondersteunen, met name voor de identificatie en authenticatie bij de opsporing, grenscontrole, bankeren en toegang tot zorgdiensten.

TouchID van Apple is een voorbeeld van een zeer breed geadopteerde mobiele vingerafdruk toepassing. Met behulp van Touch ID kun je je vingerafdruk gebruiken om de iPhone te ontgrendelen in plaat van met een codeslot. Je hoeft dan ook geen wachtwoord meer in te voeren tijdens het downloaden van de nieuwe apps van de App Store. Sinds iOS 8 kunnen ook de externe appontwikkelaars de TouchID gebruiken om bijvoorbeeld de toegang tot een mobiel bankieren app met de vingerafdruk van TouchID mogelijk te maken. Dankzijn de hoogwaardige vingerafdruk sensor ligt de prestatie van de TouchID aanzienlijk hoger dan bij de andere mobiele vingerafdruk sensoren, terwijl de maat van de sensor zelf veel kleiner is dan die van andere externe sensoren (zie Figuur 6). Apple heeft een capacitieve vingerafdruk sensor gekozen die nauwkeuriger en veilgier is dan een optische sensor, omdat de capacitieve sensor een 3D-beeld van de vingerafdruk maakt gebruikmakende van het feit dat de buitenste laag van je huid niet-geleidend is, terwijl de vlak daaronder liggende laag wel elektriciteit geleidt. Wanneer je de sensor aanraakt, meet Touch ID de veranderingen in geleiding door de structuur in huidlagen, op basis daarvan wordt een 3D-beeld gemaakt.

Volgens Apple wordt niet de vingerafdruk zelf opgeslagen op Apple servers of in de iCloud, maar alleen de versleutelde data afgeleid van de vingerafdruk. Dat zorgt voor extra beveiliging tegen potentiele aanvallen. Apple geeft de ontwikkelaars geen toegang tot de vingerafdrukgegevens zelf. Apple voert zelf de verificatie uit en de applicatie krijgt alleen het resultaat terug of de matching wel of niet succesvol is. Deze oplossing heeft privacy voordelen.

Qua universaliteit scoort vingerafdruk hoog, mede dankzijn de integratie in smartphones en door de standaardisatie in bijvoorbeeld FIDO.

De prestatie van vingerafdrukken voor authenticatie (in termen van FAR en FRR) is redelijk goed. Vingerafdruk-oplossingen van grote leveranciers worden regelmatig vergeleken tegen gestandaardiseerde databases. Voor de mobiele vingerafdruk toepassingen is een verschil tussen optische biometrische scan doormiddel van een

mobiele camera, zoals de TouchlessID[86] oplossing van Veridium, en de geïntegreerde vingerafdruk sensoren zoals de Apple TouchID. TouchID is een gesloten systeem waar je niet veel meer mee kan anders dan authenticatie. Hergebruik van templates is onmogelijk. Optisch is meer open: er is vanuit de app controle over de camera op de smartphone en de toegang tot de gefotografeerde beelden. Optisch afgenomen vingerafdrukken verschillen enigszins van de afdrukken die middels capacitieve of ultrasone scanners zijn afgenomen. Dat kan matchingsproblemen geven.

Een uitdaging is dat de sensor in veel gevallen gevoelig is voor vocht en vuil. Bovendien kunnen vingers beschadigd zijn en is de technologie kwetsbaar voor veroudering. Een ander probleem is dat vingerafdrukken opzettelijk kunnen worden overgenomen. Bijvoorbeeld door ongemerkt een achtergelaten vingerafdruk van een slachtoffer af te nemen en vervolgens een kunststof afgietsel over de eigen vinger te leggen. Dit kan relatief eenvoudig met huishoudelijke middelen. PAD methodes voor vingerafdrukken moeten bijvoorbeeld levende kenmerken van de vinger zelf kunnen meten: de temperatuur van de vingers; de hartslag in de vinger; zweet/vochtigheid van de vinger enz. De meeste gangbare vingerafdruk sensoren kunnen de levende kenmerken op dit moment nog niet meten. Dit zorgt ervoor dat de technologie op veiligheid slechts gemiddeld scoort.

Onderstaande Figuur 16 geeft het overzicht van de meest recente resultaten van FVC on-Going – de internationale evaluatie systeem voor de vingerafdruk herkenning algoritmes – aangaande de betrouwbaarheid van vingerafdrukbiometrie[87]:

Published on ▼	Benchmark	Participant	Type	Algorithm	Version	EER	FMR_{1000}	FMR_{10000}	Show details
24/01/2019	FV-HARD-1.0	Neurotechnology	Company	MM_FV	11.0	0,543%	0,756%	1,118%	
24/01/2019	FV-STD-1.0	Neurotechnology	Company	MM_FV	11.0	0,027%	0,011%	0,043%	
01/01/2019	FV-STD-1.0	NADRA	Company	Nadra_UltraMatcher	1.0.1	0,710%	1,255%	1,840%	
02/02/2018	FV-HARD-1.0	Sonda Technologies Ltd.	Company	FPM	4.1.19	0,754%	1,035%	1,330%	
28/07/2017	FV-HARD-1.0	Beijing Hisign Bio-info Institute	Company	HXKJ	2.4	0,530%	0,797%	1,879%	
27/07/2017	FV-STD-1.0	Beijing Hisign Bio-info Institute	Company	HXKJ	2.4	0,022%	0,007%	0,036%	

Figuur 16: Resultaten FVC on-Going: Int. evaluatie systeem voor de vingerafdruk herkenning algorithmes; EER (Equal Error Rate): Error rate als FAR(False Accept Rate)=FRR(False Reject Rate).

4.2 Irisscan

Irisherkenning is een vorm van biometrische identificatie waarin herkenning wordt toegepast op beeldopnamen van één of beide irissen. Irisherkenning wordt vaak verward met netvliesscanning; dit is een andere techniek waarbij de unieke patronen van bloedvaten in het netvlies worden geanalyseerd.

Er wordt gebruik gemaakt van een camera om gedetailleerde opnamen te maken van de structuur van de iris. Deze worden als digitale templates opgeslagen en bij identificatie weer gebruikt om te matchen. Vrijwel alle irisherkenningssystemen maken opnamen van de iris onder belichting met een nabij infrarood golflengte (Near Infrared Wavelength, NIR, 700-900nm). De reden hiervoor is dat hoewel lichtgekleurde ogen wel de structuur prijsgeven onder gewone belichting (zichtbare golflengte), de meeste mensen donkerbruine ogen hebben die alleen in het NIR spectrum patronen voldoende prijsgeven. Smartphones die irisscanning ondersteunen, hebben daarom een extra infrarood LED nodig en een infrarood camera.

De irisscan wordt onder andere gebruikt voor delen van het grensbewakingsproces zoals Privium in Nederland. De Verenigde Arabische Emiraten gebruiken dit zelfs al sinds 2001 voor haar grensbewaking. Er wordt veelal gebruik gemaakt van dedicated devices. Deze markt is volwassen met veel aanbieders. Aanbieders van dergelijke technologie op smartphones zijn er helaas nog niet veel. Fujitsu is de eerste met een toepassing voor smartphones, nu alleen nog in Japan. Samsung Galaxy S8, S9 en LG G7 hebben een geïntegreerde irisscanner.

[86] Zie: https://info.veridiumid.com/hubfs/Content/Datasheets/datasheet-4-fingers-touchless-id.pdf?utm_campaign=4%20Fingers%20Datasheet&utm_source=Website&utm_medium=Datasheet.
[87] Zie: FVC-onGoing: evaluatie systeem voor de vingerafdruk herkenning algoritmes, opvolger van de Int. Vingerafdruk Verificatie Competitie https://biolab.csr.unibo.it/FvcOnGoing/UI/Form/Home.aspx.

Irisherkenning in de Galaxy S8 is niet betrouwbaar genoeg. De mobiel werd volgens CNET in 2017 door de Duitse hackers voor de gek gehouden met een lens over een foto.

De technologie presteert goed en werkt snel (Daugman, 2006). De iris is ook een consistente eigenschap (irisherkenning werkt tot wel 30 jaar na registratie), omdat de iris van buiten zichtbaar is, maar wel beschermd is tegen de omgeving.

De technologie is eenvoudig te gebruiken, vereist bijvoorbeeld geen contact met een device. Een irisscan kan op 10 cm tot zelfs enkele meters afstand worden afgenomen, en werkt zelfs met kleurloze contactlezen, brillen en niet-spiegelende zonnebrillen. Dit zorgt ervoor dat de technologie op universaliteit hoog scoort.

Het voornaamste risico, buiten slechte foto's door gebrekkige opnameprocessen of techniek, is spoofing met behulp van hoge resolutie foto's of zelfs lenzen met een valse iris. Dit zorgt ervoor dat de technologie op veiligheid slechts oranje scoort. Een vorm van liveness detectie is dus raadzaam, bijvoorbeeld door de iris te laten bewegen door veranderingen in het omgevingslicht.

4.3 Netvliesscan

Het netvlies is een dunne laag weefsel bestaande uit zenuwcellen tegen de achterwand van het oog. Door de complexe structuur van bloedvaten in het netvlies zijn de patronen van deze bloedvaten voor iedereen uniek. Dit netwerk van bloedvaten is niet geheel genetisch bepaald en dus zelfs voor identieke tweelingen niet hetzelfde.

Hoewel bloedvatpatronen in het netvlies kunnen wijzigen door aandoeningen als diabetes en staar, blijft het netvlies normaal gesproken ongewijzigd gedurende eenieders leven. Door de unieke en onveranderlijke aard van het netvlies is het een zeer betrouwbaar biometrisch kenmerk wat qua performance te vergelijken is met een irisscan en vingerafdruk.

Een netvliesscan wordt gemaakt door een onzichtbare straal van nabij infrarood (NIR) licht in iemands oog te schijnen terwijl zij in de scanner kijken. Hier wordt een foto van gemaakt. Omdat de bloedvaten meer licht absorberen, geven zij een donkere reflectie af en zijn dus zichtbaar in het scanresultaat. Het patroon van deze variatie wordt vervolgens digitaal opgeslagen in een database.

Netvliesscans worden gebruikt voor authenticatie en identificatie. Er is ook een medische toepassing van netvliesscans, omdat bepaalde overdraagbare en erfelijke aandoeningen in het oog waarneembaar zijn, zoals bijvoorbeeld AIDS of leukemie. Soms wordt deze technologie verward met irisscans of oogaderpatroonherkenning.

Er zijn op het moment nog geen commerciële smartphones die deze technologie bevatten, ondanks de lijst in internet die de netvliesscan met iris- en oogaderpatroonherkenning verwarren[88]. Een interessante nieuwe ontwikkeling is de optische netvlies technologie van een startup in Ierland iKey[89]. Het eerste prototype is in 2019 ontwikkeld en moet nog getest worden voor biometrische identificatie, leeftijd verificatie en glaucoma risico detectie. Op universaliteit en geschiktheid scoort de technologie dus laag.

Hoewel netvliesscans snel en betrouwbaar zijn, zijn er bepaalde aandoeningen die het netvlies aantasten en vereist deze methode additionele apparatuur. Omdat de persoon de camera relatief dicht op de ogen moet houden scoort de technologie ook laag op gebruiksgemak.

4.4 Vingeraderpatronen

Aderpatroonherkenning voor biometrische authenticatie maakt gebruik van patronen van bloedvaten in de vinger. Bloedvatpatronen zijn uniek identificerend. Hierbij wordt Near Infrared (NIR) licht op de vinger geschenen. De bloedvaten absorberen het infrarode licht, waardoor zij donkere lijnen nalaten op een foto. Van de foto wordt een biometrische template gemaakt voor matching. Authenticatie kan binnen 2 seconden

[88] Zie: https://webcusp.com/list-of-all-eye-scanner-iris-retina-recognition-smartphones/.
[89] Zie: https://www.biometricupdate.com/201903/irish-startup-develops-retina-scanning-technology-for-user-biometrics-and-age-verification.

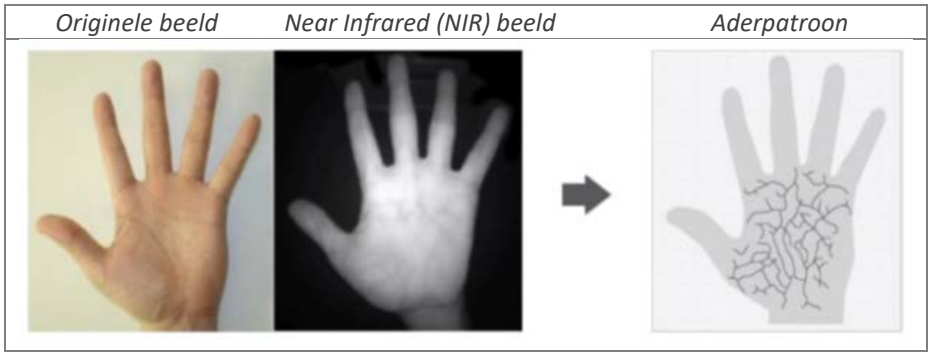
geschieden. Meestal zijn er speciaal ontwikkelde apparaten nodig voor vingeraderherkenning. Deze techniek kan eenvoudig worden gecombineerd met vingerafdrukherkenning.

Hitachi heeft een systeem voor vingeraderherkenning ontwikkeld en gepatenteerd in 2005, welke wordt gebruikt voor creditcards, auto's, aanwezigheidsregistratie, pinautomaten, en computerauthenticatie. Het apparaat bestaat uit een NIR LED lampje, een CCD camera en een versleutelde SIM kaart. Barclay's bank kondigde in 2015 aan deze VeinID technologie te gaan gebruiken voor online bankieren. Andere aanbieders zijn Mofiria, NEC en M2Sys. Sony biedt zelfs een sensor die geschikt is voor implementatie in een smart card waarmee match-on-card mogelijk is.

Bloedvaten zijn bijna onmogelijk te kopiëren zonder medewerking van de persoon en buitengewoon uniek identificerend en daarom veiliger dan bijvoorbeeld een vingerafdruk. Op prestatie en veiligheid scoort deze technologie dus goed. Vingeraderherkenning wordt weinig beïnvloed door omgevingsfactoren. Er zijn nog geen non-dedicated devices zoals smartphones die vingeraderherkenning ondersteunen. Buiten het ontbreken van vingers en enkele zeldzame aandoeningen, beschikt vrijwel iedereen over vingeraders.

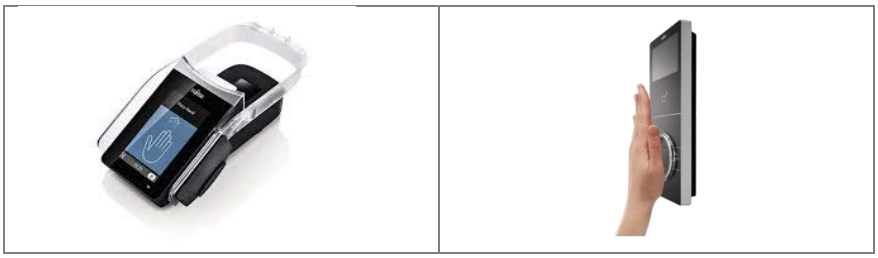
4.5 Handaderherkenning

Handaderherkenning is een recente biometrie technologieën die de unieke aderpatronen in hele hand gebruikt, terwijl vingeraderpatroon biometrie alleen gebruik maakt van de bloedvaatpatronen in de vinger. Een contactloze sensor maakt gebruik van NIR imaging techniek (zie Figuur 17) om de unieke vasculaire patronen in de handpalm bloot te stellen (Sabhanayagam et al., 2018; Parihar and Jain, 2019). In 2019 is de eerste smartphone LG G8 THinQ met mobiele handaderauthenticatie gelanceerd. Handaderherkenning is een zeer veilige en nauwkeurige technologie, uniek zelfs voor genetisch identieke tweelingen.



Figuur 17: Handaderherkenning.

Fujitsu heeft een patent op de handader biometrie technologie PalmSecure[90] (zie Figuur 18). Sinds maart 2019 wordt PalmSecure geïntegreerd in de grenscontrole biometrische systemen op de Koreaanse vliegvelden.



Figuur 18: Meetapparatuur voor het meten van handader.

Nadelen van de handaderherkenning is dat het relatief duur is en dat de kwaliteit van het beeld afhankelijk is van diverse factoren zoals de lichaamstemperatuur en omgevingstemperatuur. Deze biometrie techniek is nog volop in ontwikkeling en nog onvoldoende getest. De markt wordt momenteel door Japanse vendors

[90] Zie: https://www.fujitsu.com/global/services/security/offerings/biometrics/palmsecure/.

gedomineerd en vanuit veiligheidsperspectief van de templates dataopslag is het voor de Nederlandse overheid niet wenselijk om er afhankelijk te zijn van de Japanse vendors als enige leveranciers.

Onderzoekers in Duitsland hebben in 2018 laten zien hoe de aderherkenning omzeild kan worden door het patroon te achterhalen en vervolgens na te bootsen met een nep hand gemaakt van gele was met erop geplaatste aderpatroon[91] (Figuur 19). De handaderscanner van Fujitsu en de vingeraderscanner van Hitachi werden omzeild, beide zijn de marktleiders. Fujitsu reageerde sceptisch met de kritiek dat dit experiment niet herhaalbaar is buiten het lab. Duitse veiligheidsdienst BDO en geldautomaten in Japan maken gebruik van op handaderherkenning gebaseerde biometrische authenticatie.

Figuur 19: Nep hand gemaakt van gele was met erop geplaatste aderpatroon[91].

4.6 Oogaderpatronen

De aderen in de sclera, het oogwit, kunnen worden opgenomen voor biometrische herkenning. Patronen van deze aderen worden opgeslagen als template voor latere vergelijking. Het patroon van deze bloedvaten vormt een stabiel kenmerk dat weinig verandert door leeftijd, alcoholconsumptie, allergie of algehele roodheid van het oog (Das et al., 3013). De standaardcamera op de meeste smartphones is geschikt voor oogaderherkenning. Ook werkt dit met lenzen of zelfs brillen, maar niet met zonnebrillen. Soms wordt infrarood licht gebruikt voor het maken van een afbeelding van het oogwit zodat ook in donkere omstandigheden gewerkt kan worden (dit vergt dan een aanpassing aan de smartphone).

De firma EyeVerify heeft een patent op deze technologie. EyeVerify biedt softwaretoepassingen voor oogaderherkenning en wordt al door een groot aantal smartphones ondersteund, inclusief de meeste Samsung en Apple toestellen. EyeVerify biedt ook een software development kit (SDK) en lijkt samen te werken met de Chinese smartphone fabrikanten ZTE en Vivo.

Er zijn een tweetal studies gedaan naar de technologie van EyeVerify welke aangeven dat de implementatie van oogaderpatroonherkenning goed presteert. Deze onderzoeken zijn echter wel in opdracht van EyeVerify uitgevoerd. De technologie is vrij invasief en heeft niet dezelfde grootschalige onafhankelijke testen doorstaan als bijvoorbeeld vingerafdrukherkenning en gezichtsherkenning. Op prestatie scoort de technologie voorlopig nog matig, maar dit zou goed kunnen worden verbeterd als meer onafhankelijk onderzoek gedaan wordt.

Het opnametoestel dient dicht bij het gezicht te worden gehouden, hetgeen mogelijk wat ongemakkelijk is voor de gebruiker.

Nadeel van de retina scan biometrie is dat het relatief duur is, niet heel gebruikersvriendelijk en er kunnen medische aandoeningen (zoals diabetes) van afgeleid worden waardoor de privacy van de gebruiker in gevaar komt.

[91] Palm vein security bypassed using wax hand models, 2018, zie: https://hexus.net/business/news/components/125744-palm-vein-security-bypassed-using-wax-hand-models/.

4.7 Gezichtsherkenning

Voor gezichtsherkenning worden foto of video-opnamen gemaakt van het gelaat tijdens enrolment en matching. Er zijn verschillende algoritmische aanpakken mogelijk[92], waaronder geometrie gebaseerde algoritmes (analyseren lokale gezichtskenmerken en hun geometrische relaties, ook feature-methode genoemd) en template gebaseerde algoritmes (gebouwd met behulp van statistische methodes zoals belangrijkste componentenanalyse - PCA). Relatief nieuw is om het gelaat in 3D te modelleren. Gewone camera's kunnen voor gezichtsherkenning worden gebruikt, maar er zijn ook gezichtsherkenning-toepassingen op basis van infrarood thermografische opnamen.

Gezichtsherkenning wordt als biometrisch kenmerk ingezet voor forensische doeleinden, identificatie bij grenscontrole of face-in-the-crowd herkenning. Andere toepassingen zijn identificatie bij geldautomaten, aanwezigheidscontrole op de werkvloer of foto applicaties die mensen herkennen en taggen (waaronder iPhoto, Picasa, Live Photo Gallery en Facebook). MasterCard test sinds kort "SelfiePay", waarbij men met een foto van het gezicht een betaling autoriseert, en Alibaba biedt zelfs "Smile to Pay" aan. Android telefoons beschikken over Face Unlock, dat met cumulatieve template-opslag en liveness detectie kan worden versterkt door de gebruiker. In de Chinese stad Peking worden in 2019 120.000 woningen voorzien van slimme sloten met gezichtsherkenning. Zo komen alleen inwoners en familieleden binnen[93]. Autoverhuurder Hertz maakt gebruik van gezichtsherkenning (of vingerafdruk) om het uitleenproces van auto's te versnellen[94].

Er is een zeer volwassen markt voor gezichtsherkenning-toepassingen. Een rapport van Tractica[95] verwacht een groei van 28.5 miljoen apparaten met gezichtsherkenning in 2015 naar 122.8 miljoen in 2024, met een jaarlijkse industriegroei van 22% van $150 miljoen naar $882 miljoen. Met name toepassingen op mobiele devices zullen naar verwachting in aantal toenemen. Op universaliteit scoort de technologie dus goed. Voorbeelden van aanbieders van smartphone apps voor gezichtsherkenning als tweede factor zijn VeriLook, FacialNetwork, Bioscrypt, Mitek en Keylemon.

Vergeleken met andere biometrische technieken als vingerafdruk en irisscan is gezichtsherkenning niet het meest betrouwbaar of efficiënt. Qua prestatie scoort de technologie dus matig.

Een voordeel vanuit gebruiksgemak perspectief is dat het passief kan worden afgenomen, bijvoorbeeld via een camera bij de receptie. Daarentegen, vanuit burger perspectief is het bediscussieerbaar of de passieve afname van gezicht als invasief kan worden ervaren. Gezichtsherkenning is gevoelig voor verschillen als gezichtsuitdrukking of de hoek waaronder de foto wordt genomen, en voor de omgevingsfactoren als belichting. Er zijn ISO standaarden (zie sectie 3.3) die voorschrijven hoe opnames optimaal genomen moeten worden voor optimale resultaten.

Sommige toepassingen van gezichtsherkenning kunnen eenvoudig worden omzeild door een foto van een gezicht voor de camera te houden, liveness detectie is hier dus ook van belang voor extra veiligheid. Recente experimenten van Spreeuwers et al. (2018) tonen aan dat geautomatiseerde gezichtsaanvaldetectie een oplossing kan zijn, mits deze getraind is met meerdere gezichten in de dataset.

Steeds meer smartphones kun je ontgrendelen door simpelweg je gezicht voor de mobiel te houden. Dankzij gezichtsherkenning weet de telefoon dat jij het bent. Het is wel zo makkelijk, maar blijkt vaak niet veilig. De Consumentenbond testte de gezichtsherkenningsfunctie van 110 toestellen en maar liefst 42 toestellen bleken met een goede foto te ontgrendelen[96]. Onder meer telefoons van Samsung (de Galaxy A7 en A8), Huawei (de P20, P20 Lite en P20 Pro), Nokia (model 3.1 en 7.1) en Sony (Xperia XZ2 en XZ2 Compact) blijken kwetsbaar voor de 'fotohack'. Niet álle modellen van de genoemde merken hebben een zwakke gezichtsherkennings-functie. De Samsung Galaxy S9, S9+ en Note 9 en de Huawei Mate 20 en Mate 20 Pro laten zich niet om de tuin leiden met een foto. Ook de geteste iPhones scoren goed. De prestatie en veiligheid van FaceID van Apple is veel beter dan vergelijkbare functies op andere nieuwste smartphones dankzij de toepassing van 3D gezichtsherkenning en geavanceerde liveness detectie. FaceID meet de dieptepunten in het hoofd om een 3D

[92] Zie: https://towardsdatascience.com/face-recognition-for-beginners-a7a9bd5eb5c2.
[93] Zie: https://www.nu.nl/tech/5658251/peking-voorziet-120000-woningen-van-gezichtsherkenning.html.
[94] Zie: https://www.cnbc.com/2018/12/12/hertz-launches-biometric-lanes-to-make-car-renting-faster.html.
[95] Zie: http://www.cheatsheet.com/gear-style/when-will-your-smartphone-have-facial-recognition.html/?a=viewall.
[96] Onderzoek Consumentenbond naar het omzeilen van gezichtsherkenning smartphones, 3 januari 2019, zie: https://www.consumentenbond.nl/nieuws/2019/gezichtsherkenning-smartphones-eenvoudig-te-omzeilen.

model te maken, gecombineerd met de analyse van de huid. IPhone slaat de digitale sleutel afgeleid van het gezichtsmodel van het gezicht die wordt opgeslagen op een aparte deel van de processor; de andere deel van de telefoon processor kan dat aparte deel nooit zien. Verificatie wordt gedaan vergelijkbaar met TouchID, volgens de veilige en privacy vriendelijke principes waarbij de verificatie applicatie alleen 'ja' of 'nee' terugkrijgt.

Forbes heeft recent de gezichtsherkenning getest doormiddel van een 3D model van het hoofd. Resultaten van deze test tonen aan dat de gezichtsherkenning technologie op een aantal Android telefoons niet veilig is en dat FaceID van Apple met deze aanval niet te omzeilen is[97].

Door liveness detectie, 3D gezichtsmodulering technieken en hoogwaardige biometrische sensoren voor de interne biometrische kenmerken zoals aderpatronen zijn gezichtsherkenning algoritmes nauwkeurige en sneller geworden waardoor de betrouwbaarheid en aantal toepassingen is toegenomen.

Gezichtsherkenning is ook meer privacygevoelig dan bijvoorbeeld een vingerafdruk, omdat een foto veel zegt over zaken als etniciteit en leeftijd. Vanwege de snelle opmars van het gebruik van gezichtsherkenningstechnologie door kunstmatige intelligentie (AI) moet er beter zicht komen op de privacy risico's van deze technologie. Privacy risico's bij 1-op-1 verificatie zijn met name de mogelijke ethische bias en discriminatie[98,99]. Echter moeten de ethische kaders in specifieke context worden opgesteld. De gezichtsherkenning om een mobiele telefoon te ontgrendelen moet aan andere eisen voldoen dan het gebruik binnen de vluchthaven om sneller veilig door te kunnen lopen. Grotere privacy risico's zijn verbonden aan de gezichtsdetectie bij de n-op-n identificatie, het publiek videotoezicht op straat met de potentiele risico van verkeerde identificatie en schending van de rechten van de burgers op gegevens privacy. Deze laatste n-op-n identificatie use-case is buiten de scope van dit onderzoek. Het bijzondere van gezichtsherkenning is namelijk dat het zowel gebruikt kan worden om je identiteit te beschermen, als om er inbreuk op te maken. Toepassing van de internationale richtlijnen zoals BaFin[100] voor video identificatie (zie sectie 5.3) en de regulering van AI en gezichtsherkenning vanuit overheid[101] zijn noodzakelijk om te zorgen voor rechtsgeldig gebruik van deze techniek.

4.8 Hartslagherkenning

De hartslag kent ook patronen die identificerend kunnen zijn voor een individu. Dit kan worden gemeten middels een elektrocardiogram (ECG). Na het verwijderen van ruis kunnen zogenaamde fiduciaire punten worden bepaald van waaruit patronen kunnen worden opgesteld, ook wel bekend als een PQRST patroon. De eigenschap is weinig afhankelijk van waar op het lichaam de sensor geplaatst is.

Er zijn veel wearables zoals smartwatches en fitness trackers die het hartritme meten. Voorbeelden zijn Samsung en Apple smartwatch, AliveCor Mobile ECG en het Fitbit fitness tracker. Het meten van de eigen hartslag, onder andere voor gezondheidsredenen, is een trend ook wel 'quantified-self' genoemd. Echter is de betrouwbaarheid van de wearable hartslag sensoren nog niet voldoende en wordt medisch ook niet nauwkeurig genoeg beschouwd. De hartslag is geschikt voor continue authenticatie. Halifax Bank uit Canada gaat bijvoorbeeld een proef starten om hartslagverificatie via de Nymi armband te gebruiken voor online bankieren. Een vergelijkbaar product is Olea's Heart Signature.

Daarnaast kunnen de smartphone apps de hartslag meten[102] met behulp van de camera door veranderingen in bloedvolume onder het huidoppervlak te detecteren. Door de vinger op de cameralens plaatsen wordt het scannen vanuit de app activeren en binnen enkele seconden wordt de hartslag gedetecteerd en weergegeven. Het hart klopt, zwelt de hoeveelheid bloed die de haarvaten in je vingers en gezicht bereikt op en trekt zich vervolgens terug. Omdat bloed licht absorbeert, kunnen apps deze eb en vloed opvangen door de flitser of de camera van je telefoon te gebruiken om de huid te verlichten en een reflectie te creëren. De nauwkeurigheid

[97] Zie: https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#97f467213307.
[98] Zie: https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/.
[99] Zie: https://www.nrc.nl/nieuws/2019/12/04/gezichtsherkenning-mag-dat-helaas-zo-werkt-ethiek-niet-a3982702.
[100] BaFin Circular 3/2017 (GW) - Video Identification Process, zie: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html.
[101] Zie: https://www.biometricupdate.com/202001/eu-no-longer-considering-facial-recognition-ban-in-public-spaces.
[102] Zie: https://www.cnet.com/how-to/how-to-track-your-heart-rate-with-a-smartphone/.

van deze hartslag metende apps is zeer diverse en de recente onderzoeksresultaten duiden op de verschillen meer dan 20 slagen tussen vier verschillende hartslag apps en meer dan 20% verschil vergeleken met klinische goudstandaardmetingen[102] (ECG - een grafische weergave van de elektrische activiteit in de hartspier; en puls oximetrie - een test die wordt gebruikt om zuurstofniveaus van het bloed te meten).

Wearables en smartphones met geschikte sensor zijn nog niet voldoende beschikbaar om de technologie op universaliteit op groen te zetten, voorlopig blijft deze oranje. De prestaties van ECG worden steeds beter, hoewel Hammad et al. (2018) suggereren om deze modus te combineren met andere modi zoals vingerafdruk of gezichtsherkenning.

Er is nog een andere methode dan een ECG, namelijk fotoplethysmografie. Hierbij wordt met een gewone camera met flits het hartritme afgeleid uit kleurverandering van de huid door uitzetting van de haarvaten in de huid. Echter, deze methode is minder accuraat voor authenticatie en biedt ook niet de mogelijkheid tot continue authenticatie. Een voorbeeld van deze techniek is Phillips' Vital Signs app.

4.9 Sprekerherkenning

Sprekerherkenning, dat wil zeggen: wie spreekt, niet te verwarren met spraakherkenning (wat er wordt gezegd). Akoestische patronen in spraak zijn uniek voor iedereen en worden veroorzaakt door zowel de anatomie (vorm van de keel) en aangeleerde gedragspatronen (toon en stijl). Het wordt daarom vaak beschouwd als gedragsbiometrie en wordt gebruikt voor onder andere de verificatie van de identiteit. Net als gezichtsherkenning kan sprekerherkenning ongemerkt worden gedaan door afluisteren.

Tijdens het enrolment proces wordt de stem van de spreker opgenomen, van waaruit een aantal kenmerken worden omgezet in een voiceprint. Gedurende de verificatie wordt een spraaksample ("utterance") vergeleken met voice prints in de database. Hiervan bestaan twee categorieën: tekstafhankelijk en tekstonafhankelijk. Wanneer de tekst tijdens verificatie dezelfde moet zijn als tijdens enrolment, betreft de tekstafhankelijke verificatie. Bij tekstonafhankelijke verificatie is de utterance niet dezelfde als tijdens enrolment, daarom zijn de algoritmes voor de vergelijking van voiceprints complexer. Tekstonafhankelijke verificatie wordt vaker gebruikt voor de verificatie dan voor de identificatie, soms in combinatie met spraakherkenning.

Sprekerherkenning is gevoelig voor omgevingsgeluiden, gedragsveranderingen en emotie, gezondheid (denk aan een verkoudheid) en invloed van de microfoon. Bovendien kan spraak eenvoudig worden opgenomen en gesimuleerd.

Microfoons zijn beschikbaar op heel veel apparaten, waaronder PC's en smartphones. Tevens is continue authenticatie mogelijk gedurende gesproken interactie, bijvoorbeeld in telefoongesprekken of door de opkomst van spreeksturing (denk aan persoonlijke assistenten als Siri of Cortana op smartphones). Veel banken maken gebruik van spraak- en sprekerherkenning in voice response systemen. De Nederlandse bank ING gebruikte sprekerherkenning voor toegang tot hun app, maar is daar recent mee gestopt omdat het te weinig werd gebruikt.

Er bestaat een volwassen markt voor eerste en tweede factor authenticatietoepassingen van sprekerherkenning. Aanbieders zijn onder andere DigitalPersona, Daon, BioID, Authentify en Keylemon. Volgens Tractica zal de markt voor spraak- en sprekerherkenning groeien tot $5 miljard in 2024, met een grote verscheidenheid aan apps.

Qua prestatie is het niet de meest betrouwbare vorm van authenticatie. Gebruikers kunnen het bovendien als invasief beschouwen ofwel: het kan niet "onder-de-tafel" worden gebruikt; de gebruiker is niet altijd in de gelegenheid hardop te spreken.

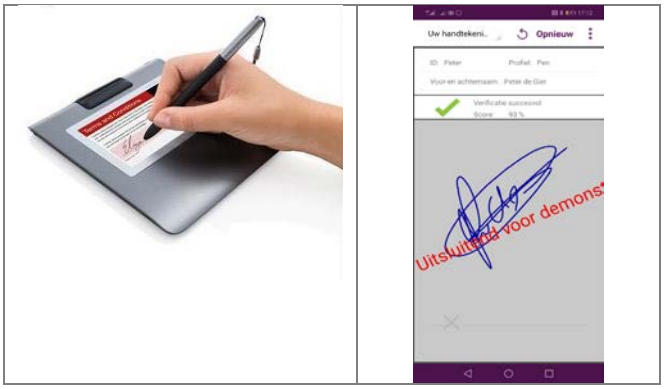
4.10 Handtekening

Het handschrift is relatief uniek voor elk individu en wordt daarom steeds populairder voor authenticatietoepassingen. Veel systemen maken gebruik van driedimensionale analyse van een handschriftsample waarbij de vorm en druk van het schrift worden beschouwd. Handschriftanalyse kan zowel dynamisch (online, in real-time) als statisch (offline, achteraf ingescand) plaatsvinden. Een belangrijke vorm van handschriftanalyse voor authenticatie is handtekeninganalyse. Een handtekening is in de niet-digitale wereld een geaccepteerde vorm van authenticatie. De meeste mensen hebben een handtekening. Een handtekening

kent bovendien een extra factor 'iets wat je weet' ("something you know"). Dynamische handtekeningherkenning wordt gebruikt als gedragsmatige authenticatiemethode. De handtekening wordt geanalyseerd aan de hand van ritme, vorm, tijd, fluctuatie en druk. Voor deze toepassing wordt veelal een drukgevoelig touchscreen gebruikt op bijvoorbeeld een tablet, smartphone, PDA of dedicated device. Dit is anders dan een gewone foto of andere één-dimensionale afbeelding van een handtekening, wat bijvoorbeeld veel wordt gebruikt voor een handtekening ter goedkeuring. Van de handtekening wordt vervolgens een digitale template gemaakt voor latere matching. Het is ook mogelijk om veranderingen in handtekeningen in de tijd te registreren bij regelmatige verificatie. Behalve voor authenticatie, wordt deze technologie ook veel gebruikt voor het vaststellen van de authenticiteit van handtekeningen, bijvoorbeeld op documenten of getekende memorabilia door beroemdheden.

Hoewel het achterhalen van iemands handtekening vaak relatief makkelijk is, blijkt het goed nadoen van iemands handtekening toch relatief complex. Dynamische handtekeningauthenticatie is daarom een veilige authenticatiemethode, echter het accuraat vaststellen van iemands handtekening is ook erg complex, wat resulteert in een hoge FRR door kleine veranderingen in het handschrift, wat weer ten koste gaat van de gebruiksvriendelijkheid. Bovendien werkt handschriftherkenning het beste met een pen of stylus en heeft de gebruiker dit niet altijd bij zich. Handtekeningen zetten met een vinger op een touchscreen boet in op de accuratesse van de authenticatie.

Er is een beperkt aantal apps in omloop voor handtekeningauthenticatie, vaak als eerste factor of voor digitale ondertekening, maar weinig betrouwbare of gebruiksvriendelijke apps. Voorbeelden zijn Lucom e-Signing (zie Figuur 20), SutiDsignature van Sutisoft en CIC's iSign voor digitale ondertekening, BioWallet's password manager, screen lock apps als Signature Unlock en KinWrite (voor de Microsoft Kinect interface). De Samsung Galaxy Note 10 tablet wordt standaard geleverd met handtekeningherkenningssoftware. Een toepassing van deze technologie is Sign2Pay.



Figuur 20: Voorbeeld handtekening authenticatie oplossing[103].

4.11 Gebruikersinteractie

Verschillende eigenschappen van de interactie van de gebruiker (human computer interaction, HCI) met een systeem zijn identificerend en kunnen worden benut voor biometrische gedragsauthenticatie. Bijvoorbeeld de toetsaanslagen dynamiek en klikgedrag (directe interactie, ook mogelijk op touchscreen), maar ook de inhoud van de interactie (indirecte interactie, gebaseerd op kennis, vaardigheid en strategie, denk aan gebruik van diverse applicaties) zijn hiervoor geschikt. Een voordeel is dat het geschikt is voor continue authenticatie, dit betekent echter dat het minder geschikt is als eerste factor omdat het niet één authenticatiemoment kent, maar een bepaald tijdsinterval nodig heeft, en dus ook een relatief intensieve enrolment procedure kent.

Toetsenborddynamiek kijkt naar de manier en het ritme van typen op een toetsenbord. Deze patronen vormen een biometrisch template voor latere herkenning. Een algoritme analyseert bijvoorbeeld hoe lang toetsen worden ingedrukt, welke toetsen werden gebruikt voor hoofdletters, of hoe vaak backspace wordt gebruikt, en de gelogde resulterende tekst. De nauwkeurigheid van deze technieken verschillen sterk in succes en precisie, en variëren van eenvoudige statistische analyse tot kunstmatige intelligentie zoals neurale netwerken. Vanzelfsprekend is deze techniek vooral bedoeld voor PC's met toetsenborden. De online leeromgeving van

[103] Zie: https://www.thehaguesecuritydelta.com/partners/partner/369-lucom-benelux-bv.

Coursera gebruikt bijvoorbeeld de handtekening track technologie op basis van toetsenborddynamiek om continue de identiteit van gebruikers te verifiëren. In vorige sectie 4.10 is de handtekening biometrie verder toegelicht. De markt voor typgedragherkenning is relatief volwassen met veel aanbieders. Voorbeelden zijn TypeWATCH, Intensity Analytics, AdmitOneSecurity, BioTracker, KeyTrac, KeystrokeID, TypeSense, Psylock, Authenware, bioChec, Probayes en BehavioSec. Toetsenbordauthenticatie is complex omdat typegedrag varieert afhankelijk van de menselijke toestand, omgevingsfactoren en gebruikte toepassingen, deze variatie kan leiden tot slechte prestatie van de biometrische authenticatie. Bovendien is key logging, het registreren van wat men typt, erg privacygevoelig, of zelf verboden onder de Wet bijzondere opsporingsbevoegdheden (Wet BOB). Vanzelfsprekend is toetsenborddynamiek alleen relevant voor PC's en niet voor bijvoorbeeld smartphones.

De recente biometrie ontwikkelingen voor mobiele toepassingen combineren de sensor data (bijv. accelerometer) met de toetsaanslagen voor de continu authenticatie (Buriro, 2017). Bijvoorbeeld de accelerometer sensor data in combinatie met de toetsaanslagen timing van de telefoon. Vingerbeweging, micro-handbeweging terwijl de gebruiker tekent of schrijft op het touchscreen van de smartphone, worden ook gebruikt als gebruikersinteractie biometrie.

Een andere component van biometrische authenticatie op basis van gebruikersinteractie is te kijken naar de inhoud, ofwel wat de gebruiker invoert, anders dan hoe de invoering tot stand komt. Denk hierbij aan zaken als frequentie van gebruik en navigatie. Deze activiteit kan worden waargenomen door registers van het operating system of monitoring software te exploiteren. Bekende voorbeelden zijn email-gedrag, programmeerstijl, speelstijl in videogames, tekenstijl (Passdoodles, draw-a-secret), en commando's in een command line interface.

Qua prestaties scoort met name toetsendynamiek beter dan indirecte interactie (Jorgensen en Yu, 2011), maar dit is tevens de volgorde van volwassenheid. Het voordeel van interactiegedrag is dat het zeer moeilijk te kopiëren is als biometrische factor. De privacygevoeligheid aangaande het vastleggen en registreren van het gedrag beperkt de gebruikersacceptatie.

4.12 Gebarenherkenning

Gebarenherkenning heeft tot doel menselijke gebaren te herkennen. Gebaren kunnen van over het hele lichaam komen, maar typisch van de handen of het gezicht. Dit vakgebied richt zich vooral op emotieherkenning en handgebaren. Een bijzondere toepassing is om doventaal te kunnen interpreteren met computers. Registratie van gebaren kan plaatsvinden door speciale handschoenen, stereocamera's, of accelerometers in bijvoorbeeld een smartphone. Ook gebaargestuurde invoerapparaten zoals Kinect of Leap en multi-touch schermen in bijvoorbeeld smartphone en tablet kunnen hiervoor worden gebruikt.

Als biometrisch gedragskenmerk zijn gebaren geschikt voor gebruik in authenticatietoepassingen. Een persoonlijk gebaar kan ook dienen als wachtwoord, wat een extra factor is in authenticatie ("something you know").

Een voorbeeld is AirAuth, een toepassing waarbij gebruikers gebaren maken voor een camera om toegang te krijgen. Er zijn diverse toepassingen voor gebaren op een multi-touch scherm zoals een tablet of smartphone. Lockheed Martin biedt bijvoorbeeld Mandrake, Georgia Tech ontwikkelde LatentGesture, en er bestaan diverse "swipe-lock" apps voor smartphones. Microsoft Photo-Touch laat de gebruiker zich authentiseren door een patroon te tekenen op een foto. Onderzoekers ontwikkelden samen met Motorola uWave (Liu et al., 2009), een accelerometer gebaseerde gebaarherkenningstoepassing.

Er zijn toepassingen waarin de gebruiker een PIN-code of patroon op het scherm moet tappen in een muzikaal ritme. Er zijn al een aantal apps voor tap-authenticatie met wisselende gebruiksvriendelijkheid en betrouwbaarheid, waaronder Tap tap app, Tap unlock, Knockr en AuthenWare's Tap-a-tune.

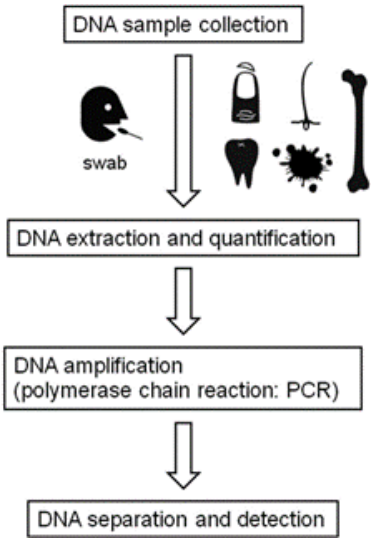
De prestaties en veiligheid van gebaarherkenning zijn minder accuraat dan bijvoorbeeld een vingerafdruk. De ontwikkelingen op dit gebied zijn nog jong. Gebaarherkenning is redelijk gebruiksvriendelijk en privacy-neutraal, hoewel minder discreet.

4.13 DNA

DNA is een zeer onderscheidend menselijk kenmerk en bied een hoog betrouwbaarheidsniveau voor identificatie. Alleen identieke tweeling hebben dezelfde DNA. De kans dat twee mensen herkend worden met hetzelfde DNA profiel is minder dan een op honderd biljoen. Er worden diverse pogingen gedaan om systemen te ontwikkelen die de real-time authenticatie mogelijk maken door middel van DNA (Sabhanayagam et al., 2018).

DNA-gebaseerde biometrische oplossingen zijn niet toegankelijk voor breed publiek en de vraag is of dit in de toekomst gaat veranderen. Dergelijke oplossingen worden momenteel vooral toegepast in de context van opsporing. DNA-matching proces (zie Figuur 21) is duur, tijdrovend en daardoor nog niet geschikt voor de grootschalige biometrische toepassingen voor burgerlijk gebruik (Jain en Kumar, 2012).

Biometrische identificatie op basis van DNA heeft ook nadelen vanuit privacy oogpunt. Gevoelige medische gegevens kunnen potentieel inzichtelijk worden, zoals informatie over een verhoogde kans op bepaalde erfelijke ziektes met als gevolg verhoogt risico van een inbreuk op de privacy van niet alleen de persoon waarvan de DNA biometrie wordt geanalyseerd, maar ook die van zijn verwanten.



Figuur 21: DNA-matching proces.

4.14 Multimodale biometrie

Aan een kant is de snelheid en de nauwkeurigheid van de biometrische matching de laatste tijd enorm verbeterd voor bepaalde hierboven beschreven individuele modaliteiten zoals vingerafdruk, gezichtsherkenning en iris. Aan de andere blijft de template-gebaseerde *interoperabiliteit* (interoperabiliteit van de biometrische templates tussen verschillende sensoren, algoritmes en leveranciers) van individuele modaliteiten nog beperkt, bijvoorbeeld voor vingerafdruk templates (Jain en Kumar, 2012). Daarnaast kan het gebrek aan kwaliteit en uniciteit van de individuele biometrische kenmerken voor sommige gebruikerspopulaties problemen opleveren voor grootschalige toepassingen.

Het combineren van meerdere biometrische modaliteiten kan resulteren in een hogere betrouwbaarheid van de identiteitsvaststelling. Dit wordt ook wel multimodale biometrie genoemd. Een ander voordeel van multimodale biometrie is dat het veel moeilijker is om meerdere kenmerken tegelijk te vervalsen. Daardoor is de kans op een spoofing aanval veel minder waarschijnlijk. Een nadeel betreft de afname van de gebruikersvriendelijkheid, hogere kosten en minder privacy.

Experimentele resultaten van recent onderzoek tonen aan dat de gecombineerde toepassing van EEG en vingerafdruk (Hammad et al., 2018) zeer betrouwbaar en efficiënt is, met als voordelen een hogere veiligheid door liveness detectie en meer robuustheid tegen spoofing aanvallen. Deze combinatie is gebruikersvriendelijk omdat de EEG signaal van de vinger wordt gelezen.

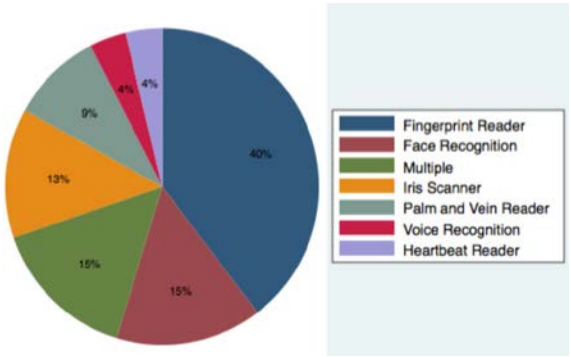
Een ander voorbeeld van multimodale biometrie betreft een systeem dat is gebaseerd op een fusie van iris- en gezichtsherkenning (Wang et al., 2011). Voorbeeld van dergelijke oplossing is OneLook technologie[104] die afhankelijk is van de externe 'on-site' sensoren en kan met name voor grenscontroles worden gebruikt. Deze oplossing is niet geschikt voor een online authenticatie scenario.

Apple werk aan een nieuwe wearable oplossing met behulp van een camera aan de onderkant van een toekomstige Apple Watch voor biometrische authenticatie uitgerust met multimodale biometrie[105] op basis van huidkleur, aderherkenning, botten, poriën of pezen[106]. Royal Bank of Scotland gebruikt multimodale gedragsbiometrie om het bezoek naar hun websites en (mobiele) applicaties te monitoren. Geavanceerde software slaat meer dan 2,000 gebaren, schermbewegingen, swipe en tap bewegingen op het moment dan de gebruiker inlogt in de mobile app[107]. De app logt zelfs de positie waarin de gebruiker zijn/haar mobiele telefoon vasthoudt. De risico van dergelijke oplossing is dat kwaadwillende op deze manier de PIN-code kunnen afleiden die iemand op het scherm intoetst.

4.15 Adoptie van biometrische modaliteiten

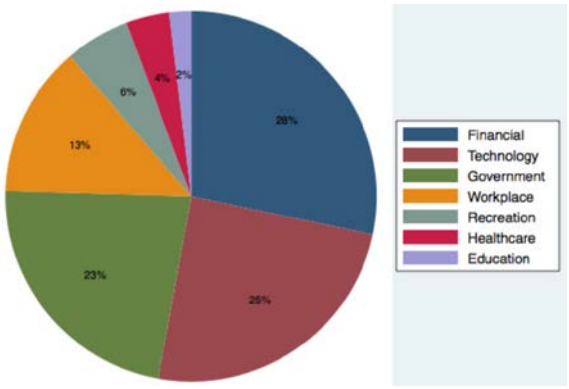
Center voor identiteiten van de Universiteit van Texas heeft in 2017 een onderzoek gedaan naar de adoptie van diverse modaliteiten voor de biometrische authenticatie in diverse sectoren (financiële, technologie, overheid, bedrijfsleven, recreatie, zorg, onderwijs) en op diverse platformen (ter-plekke of 'on-site', mobiele apparaat, vaste PC, wearable) (German en Barber, 2017). Hieronder geven wij een overzicht van de belangrijkste uitkomsten van het onderzoek.

Vingerafdruk kwam naar voor als de meest geadopteerde biometrisch modaliteit (zie Figuur 22). Biometrische authenticatie wordt met name in de financiële, technologie en overheidssector toegepast (zie Figuur 23). Binnen de overheidssector zijn biometrische authenticatie oplossingen vooral gebaseerd op vingerafdruk- en gezichtsherkenning (Zie Figuur 24). Het meest gebruikte platform is 'on-site', ofwel hardware-afhankelijke biometrische oplossingen met behulp van een losstaande toegewijde sensors zoals bij eGates met de gezichtsherkenning op luchthavens (zie Figuur 25).

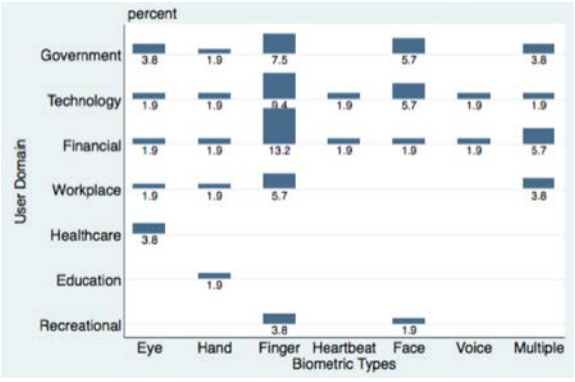


Figuur 22: Adoptie per modaliteit [Bron: https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf].

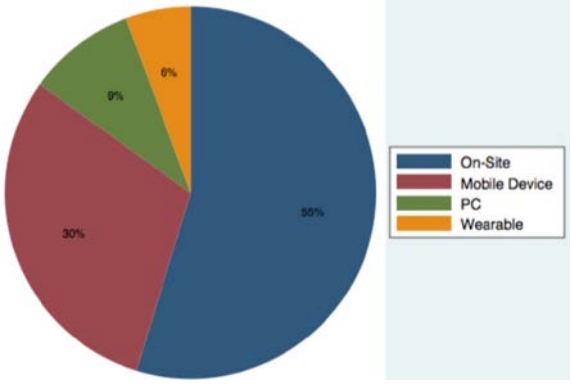
[104] Zie: https://www.idemia.com/onelook.
[105] Zie: https://mobileidworld.com/apple-patent-brings-new-biometric-authentication-options-apple-watch/.
[106] Een *pees* of zeen is een verbinding tussen een spier en een bot, waarmee de spieractiviteit op het bot wordt overgedragen. Een pees is een vaste en witglanzende structuur, die rond (als een koord of een kabel) of vlak (als een veiligheidsgordel) kan zijn. Zie: https://www.encyclo.nl/begrip/pees.
[107] Zie: https://futurescot.com/behavioural-biometrics-rbs/.



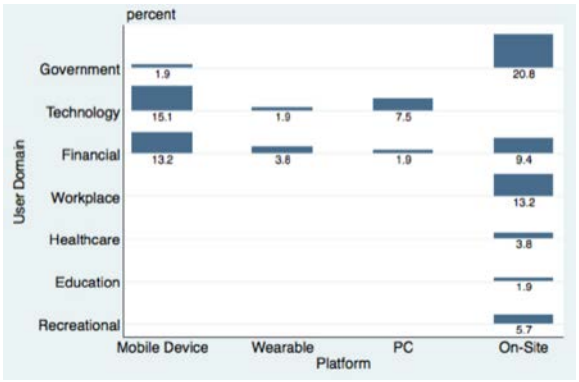
Figuur 23: Adoptie per domein.



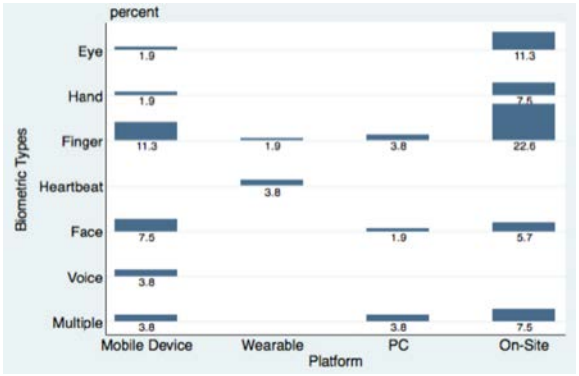
Figuur 24: Adoptie modaliteit per domein.



Figuur 25: Adoptie per platform.



Figuur 26: Adoptie per sector per platform.



Figuur 27: Adoptie per modaliteit per platform.

4.16 Samenvatting

De tabel hieronder vat de beoordeling[108] van de verschillende biometrische modaliteiten met behulp van het gedefinieerde beoordelingskader samen (zie sectie 1.3). Modaliteiten zijn onderling vergeleken, op basis van volwassenheid, voordelen en nadelen. De beoordeling in termen van goed, matig en onvoldoende[109] (respectievelijk groen, oranje, rood) is relatief ten opzichte van andere modaliteiten. Bijvoorbeeld, de universaliteit van vingerafdruksensoren is door het gebruik ervan in mobiele telefoons veel beter dan die van handaderherkenning. Of, de privacy van een gezicht is veel minder goed te borgen dan dat van een vingeraderpatroon omdat die veel minder eenvoudig te verkrijgen is.

Vingerafdruk, iris, gezicht en oogaderpatronen zijn best beoordeelde modaliteiten. Vingerafdruk scoorde het hoogst. Met name door gebruiksgemak en snelheid is er opmars van de toepassingen gebaseerd op de vingerafdruk en gezichtsherkenning biometrie, met name in de financiële, technologie en overheid domeinen. Iris en oogaderpatronen zijn meer invasief voor de gebruiker en zijn op dit moment minder breed geadopteerd. Andere modaliteiten zoals gebruikersinteractie en sprekerherkenning scoren minder goed door de gevoeligheid van het registreren van het gedrag en matige gebruikersacceptatie.

Multimodale biometrische toepassingen zijn nauwkeuriger en veiliger dan uni-modale, doordat het extreem moeilijk is om meerder kenmerken tegelijk te vervalsen waardoor kleinere kans op spoofing aanval. Hierdoor zijn ze meer geschikt voor de authenticatie. Wel gaan ze ten koste van de privacy en gebruikersvriendelijkheid.

[108] *Disclaimer:* deze beoordeling betreft een subjectieve mening en is bedoeld voor de specifieke use-cases, moet niet absoluut genomen worden.

[109] *Legenda:*
: goed : matig : onvoldoende

Biometrische modaliteit	Beoordelingscriteria (kolommen)					
	Betrouwbaar-heid	Privacy	Veiligheid	Universaliteit	Gebruiksgemak	Praktische toepasbaarheid
Vingerafdruk						
Irisscan						
Netvliesscan						
Vingeraderpatronen						
Handaderherkenning						
Oogaderpatronen						
Gezichtsherkenning						
Hartslagherkenning						
Sprekerherkenning						
Handtekening						
Gebruikersinteractie						
Gebarenherkenning						

In het volgende hoofdstuk beschrijven we aan de hand van een aantal use-case welke van deze biometrische modaliteiten hiervoor het beste toepasbaar zijn.

5. Use-cases

In de vorige hoofdstukken hebben we de biometrie modaliteiten in het algemeen besproken. Dit hoofdstuk beschouwt het toepassen van de biometrische verificatie van de identiteit voor twee concrete use-cases:

1. Aanvraag, gebruik en vernieuwing identiteitsdocumenten;
2. Aanvraag, gebruik en vernieuwing authenticatiemiddelen.

Hierna schetsen we kort de use-cases en bespreken de rol van biometrie in de toepassing. We benoemen kwetsbaarheden en mogelijkheden van biometrie om deze te mitigeren. De processen in de use-cases worden momenteel merendeels in fysieke situaties uitgevoerd, bijvoorbeeld aan een balie. In de toekomst verwachten we dat, gefaciliteerd door technologische vooruitgang en de eis van gebruikers om 24/7 zaken digitaal te kunnen regelen, de use-cases zich meer moeten richten naar dienstverlening op afstand. Bij dergelijke op afstand ofwel online dienstverlening is een betrouwbare identiteitsvaststelling en verificatie essentieel. Biometrie kan hierbij een rol spelen.

5.1 Aanvraag, gebruik en vernieuwing van identiteitsdocumenten

Het aanvragen of vernieuwen van identiteitsdocumenten, zoals een paspoort, rijbewijs, identiteitskaart of verblijfsdocument, is momenteel een grotendeels fysiek ingericht proces. Mensen komen naar een balie (gemeentehuis, IND loket) en worden daar gezien door een medewerker die de gegevens opneemt, controles uitvoert en daarna de aanvraag invoert. Bij een aanvraag of vernieuwing moet de aanvrager zich legitimeren. Hiervoor moet de aanvrager identificerende documenten overleggen. Bij vernieuwing is dat typisch het huidige identiteitsdocument. Bij een eerste aanvraag is dat een ander identiteitsdocument, bijvoorbeeld een paspoort bij aanvraag van een rijbewijs of een paspoort uit het huidige land van herkomst bij een verblijfsdocument. Als er geen identiteitsdocument beschikbaar is, dan is dat bijvoorbeeld het trouwboekje of geboorteakte, aangevuld met identificerende vragen. In alle gevallen zal de BRP worden geraadpleegd. De medewerker moet vaststellen of de aanvrager juist geïdentificeerd kan worden, door een visuele inspectie van de persoon en het aangeboden document en eventueel ondersteund met het resultaat van een geautomatiseerde verificatie van het identiteitsdocument, waarmee de authenticiteit van het identiteitsdocument wordt geverifieerd door de authenticiteit van en informatie op de chip te verifiëren.

Het gebruik van een identiteitsdocument betreft het controleren van het identiteitsdocument op echtheid en geldigheid en het verifiëren of degene die zich legitimeert hoort bij het document. Dit gebeurt door een visuele inspectie van het document (echtheidskenmerken) en het beoordelen van de op het document beschikbare gegevens (geldigheidsdatum, persoonsgegevens, foto) door een medewerker en/of het uitlezen van het document door een scanner, bijvoorbeeld een documentscanner. Het uitlezen van een op het identiteitsdocument aanwezig chip behoort ook tot de mogelijkheden. De uitgelezen gegevens zijn identiek aan die op het document zelf. Het paspoort bevat aanvullend de vingerafdruk. Aan de hand van de digitale handtekening over de gegevens kan de authenticiteit van de gegevens worden gecontroleerd.

Een groot nadeel van het huidige proces van het verstrekken van identiteitsdocumenten is dat gebruikers twee keer naar de balie toe moeten: een keer om de aanvraag te doen en biometrie te verstrekken en een keer om het document af te halen. Hoewel de gemeentes ervoor kunnen kiezen om het document per post op te sturen, heeft het bezorgen aan de deur ook veiligheidsrisico's.

We zoomen in op de biometrische gegevens op een identiteitsdocument:

- De ***handtekening*** wordt afgedrukt op het document. De handtekening wordt aan de balie op het foto- en handtekeningenformulier geplaatst en daarna ingescand en digitaal verwerkt. Nederlandse Staat kiest momenteel voor om handtekening niet op te slaan op de chip van de ID kaart en het paspoort. De handtekening blijft een aantal jaren in het aanvraagsysteem opgeslagen. Voor het rijbewijs wordt de handtekening in een lage resolutie opgeslagen op de chip, deze is te laag voor zinvol (geautomatiseerd) gebruik voor authenticatie. Op dit moment loopt er een proef met het digitaal aanvragen van een rijbewijs, waarbij een geautoriseerde fotograaf de handtekening afneemt en klaarzet voor digitale verwerking.

- Bij aanvraag of vernieuwing moet de aanvrager een recente ***pasfoto*** afgeven. Dit is een geprinte pasfoto in kleur, meestal door de fotograaf geprint vanuit een digitale foto. Deze foto moet voldoen aan bepaalde voorwaarden (zie hoofdstuk wet- en regelgeving). De foto wordt gecontroleerd door de medewerker. Bij akkoord wordt de foto op het foto- en handtekeningenformulier geplakt en ingescand voor verdere digitale verwerking. De foto wordt samen met de andere aanvraaggegevens een aantal jaren bewaard door de gemeente van aanvraag in het aanvraagstation. De foto wordt in zwart wit op het identiteitsdocument afgedrukt en in kleur op de chip opgeslagen. De foto op de chip is toegankelijk voor apparaten of apps die de chip kunnen uitlezen. De MRZ (Machine Readable Zone) van het document levert de toegangssleutel.
- Voor paspoorten en verblijfsdocumenten moet de aanvrager ***vingerafdrukken*** afgeven. Voor een paspoort zijn dat er twee. De IND neemt bij binnenkomst tien vingerafdrukken af, die centraal voor IND worden opgeslagen. Bij vernieuwing wordt door de IND de vingerafdruk weer afgenomen en geverifieerd tegen de opgeslagen vingerafdrukken. Vingerafdrukken voor het paspoort worden niet centraal opgeslagen. Vingerafdrukken worden opgeslagen op de chip van het identiteitsdocument en zijn alleen toegankelijk voor uitlezen met een speciale beveiligingssleutel beheerd wordt door JustID. Bij het afhalen van een paspoort kan, bij twijfel over de identiteit van een persoon, een vingerafdruk worden gevraagd die vervolgens wordt vergeleken met die in het uit te reiken paspoort. Op dit moment hebben rijbewijs en identiteitskaart geen vingerafdruk op de chip. In het verleden stonden de vingerafdrukken wel op de ID kaart. Wegens politieke druk en publieke weerstand werd de Paspoortwet in 2013 gewijzigd zodat de identiteitskaart geen verplicht reisdocument werd en de verplichting aan EU-wetgeving niet meer golden voor ID kaarten. De vingerafdrukken werden van de ID kaart afgehaald. Voor identiteitskaarten gaat dit, in 2021 weer veranderen door nieuwe Europese wetgeving.

Hoe kunnen biometrische oplossingen worden ingezet voor het aanvragen, gebruiken en vernieuwen van identiteitsdocumenten? Op hoofdlijnen is dat voor de volgende situaties:

- Versterken van het huidige (fysieke) proces van aanvraag/vernieuwen.
- De online aanvraagroute, waarbij personen niet meer aan de balie hoeven te verschijnen voor het aanvragen van een (nieuw) identiteitsdocument.
- Online gebruik t.b.v. toegang tot diensten.
- Beperken fysieke contact overheid-burger tot maximaal één keer.

5.2 Versterken huidige processen voor aanvraag/vernieuwen

Het identificeren van personen is een specialistische activiteit. Medewerkers van burgerzaken zijn hiervoor opgeleid, maar dat maakt het identificatieproces niet waterdicht. Ook het cognitieve vermogen van de mens is op dit punt minder betrouwbaar dan tot nu toe wordt aangenomen, zo blijkt uit onderzoek van de University of New South Wales in Australië[110]. Biometrische oplossingen zouden hierbij extra ondersteuning kunnen bieden. Hierbij kun je denken aan:

- Een camera bij de balie, of op andere plek of centraal in een hal met toezicht van de ambtenaar, die een gezichtsopname doet. Deze wordt automatisch vergeleken met de foto die de medewerker uitleest van de chip van het oude identiteitsdocument. Het resultaat wordt getoond op bijvoorbeeld het aanvraagstation van de medewerker ter ondersteuning van de eigen visuele vergelijking om zich ervan te vergewissen dat de burger aan de balie inderdaad de persoon op het getoonde identiteitsdocument is.

Een andere kwetsbaarheid in het aanvraagproces is het feit dat de burger zelf een pasfoto moet meenemen. Hoewel er diverse eisen worden gesteld aan deze pasfoto, is het nog steeds mogelijk om deze aan te passen. Bijvoorbeeld door deze te combineren (‘morphen’) met een andere foto (zie sectie 2.4). Dit heeft recentelijk tot een aantal incidenten geleid[111]. Een oplossing voor deze kwetsbaarheid is de pasfoto ter plekke en/of onder gecontroleerde omstandigheden te nemen. Indien dit niet haalbaar is, is het zaak morphing te kunnen

[110] Passport Officers’ Errors in Face Matching, White et al., 2014, zie: https://journals.plos.org/plosone/article?id=10%2E1371%2Fjournal%2Epone%2E0103510.
[111] Zie: bijvoorbeeld https://www.vice.com/en_us/article/pa9vyb/peng-collective-artists-hack-german-passport.

detecteren. Hieraan wordt gewerkt binnen het Europese SOTAMD project waarin Nederland ook participeert[112].

Online aanvraag of vernieuwen

In Finland is het mogelijk om het paspoort online te vernieuwen, met de voorwaarde dat de biometrische data zijn opgeslagen tijdens de eerdere paspoortaanvraag in het face-to-face proces met fysieke verschijning aan de balie, en als de vingerafdrukken niet ouder zijn dan 6 jaar[113]. De foto wordt bij de gecertificeerde fotograaf afgenomen en de aanvrager krijgt een unieke code. Als volgende stap kan de aanvrager naar de politiewebsite gaan en moet zich authentiseren op niveau hoog met de nationale eID-voorziening. Vervolgens moet de aanvrager eigen data controleren, de fotocode invoeren die is verkregen bij de fotograaf of een eigen foto uploaden en kan de aanvraag ingediend worden. Na acht dagen ontvangt de aanvrager een bericht inclusief een trackcode waarin aangegeven is dat het vernieuwde paspoort kan worden opgehaald bij een van de aangewezen gecertificeerde locaties in de buurt. Bij het afhalen moet de persoon zich identificeren.

De proef[114] die nu in Nederland bij een aantal gemeenten loop voor het digitaal aanvragen van een verlening van het rijbewijs werkt op een vergelijkbare manier. Een gecertificeerde fotograaf maakt een foto en neemt de handtekening op. Hij stuurt dit met het huidige rijbewijsnummer naar RDW. Foto en handtekening worden door RDW gecontroleerd en geverifieerd aan de hand van de foto en handtekening op het huidige rijbewijs die zijn opgeslagen bij RDW. Daarna vraag je het rijbewijs online aan na authenticatie met DigiD Substantieel. Via email krijg je bericht dat het rijbewijs kan worden afgehaald bij je gemeente. Bij afhalen dien je je te legitimeren.

Om deze lijn door te trekken voor het online vernieuwen van een paspoort of identiteitskaart moet aan een aantal voorwaarden worden voldaan:

- Veilige en betrouwbare authenticatie, bijvoorbeeld middels DigiD Substantieel of Hoog. De dekkingsgraad van DigiD Substantieel is echter nog zeer beperkt. DigiD Hoog bevindt zich nog slechts in een pilotfase en bestaat de facto dus nog niet. Dit vormt een belemmerende factor voor een brede uitrol van online vernieuwen. Als alternatief kan de digitale verificatie van de identiteit met een identiteitsdocument worden ingezet. Bij dat laatste is het controleren of het identiteitsdocument hoort bij degene die de aanvraag doet een belangrijke factor. Verificatie van de authenticiteit van het identiteitsdocument in combinatie met de verificatie van die identiteit aan de hand van biometrische kenmerken is daarbij essentieel. Dit werken we hierna verder uit onder ‘online gebruik van een identiteitsdocument’.
- Ten aanzien van het opnemen van de biometrische kenmerken, kan een proces zoals nu ingezet door RDW en in Finland goed werken voor de foto en de handtekening. Belangrijk is dat zowel de organisatie (met geregistreerde fotografen) als de technologie voor het aanleveren van de data aan RDW veilig en betrouwbaar is. Een proces waarbij mensen zelf een foto en handtekening uploaden heeft zeker niet de voorkeur, vanwege een inconsistente kwaliteit van de aangeleverde gegevens en een hoog risico op fouten en fraude.
- Aandachtspunt is de vingerafdruk op het paspoort. Ook hier zou de fotograaf een rol in kunnen spelen, door ze af te nemen en met de pasfoto op te sturen. Het zelf laten afnemen van de vingerafdruk, bijvoorbeeld met behulp van de smartphone, is alleen optisch mogelijk. De hardware vingerafdruksensoren van mobiele telefoons zijn slecht toegankelijk; Apple’s TouchID is volledig gesloten en staat niet toe dat vingerafdrukken worden geëxporteerd. Daarnaast mist momenteel het benodigde toezicht op spoofing preventie op mobiele telefoons met vingerafdruk sensoren. Tevens zijn het vaak eigen oplossingen die hergebruik van vingerafdrukken bemoeilijken. Het maken van een foto van de vingerafdruk via de camera van de mobiele telefoon is mogelijk. Daarbij moet wel rekening worden gehouden met de kwaliteit van de camera op de mobiele telefoon. Hoewel die steeds beter wordt, zijn er nog steeds veel relatief oude telefoons in gebruik waarvan de camera kwalitatief te kort schiet. Richtlijnen en toezicht vanuit overheid is noodzakelijk om de kwaliteit en betrouwbaarheid van dergelijke toepassingen te waarborgen.

[112] SOTAMD – State Of The Art of Morphing Detection, EU project, 2019-2020, zie: https://www.utwente.nl/en/eemcs/ds/research/sotamd/.
[113] Zie: https://www.poliisi.fi/passport.
[114] Zie: https://www.rdw.nl/particulier/voertuigen/auto/het-rijbewijs/nederlands-rijbewijs-verlengen/voorwaarden-en-uitleg-proef-digitaal-aanvragen-rijbewijs.

- Verstandiger is dus om vingerafdrukken te hergebruiken die door een officiële instantie zijn afgenomen. Omdat vingerafdrukken over een langere periode nauwelijks wijzigen, zou een nieuwe afname van vingerafdrukken kunnen worden vervangen door hergebruik van eerder afgenomen vingerafdrukken. Nu staat de vingerafdruk alleen op de chip van het paspoort of de identiteitskaart. Dit betekent dat de aanvrager de vingerafdruk uit de chip van het huidige identiteitsdocument moet lezen, bijv. met de NFC technologie van de mobiele telefoon. Hiervoor dient de uitlezende mobiele applicatie toegang tot te hebben tot de betreffende datagroep. Het regelen van deze toegang is niet triviaal maar niet onmogelijk. Gezien de vingerafdruk template momenteel in zijn geheel op de chip van het passpoort wordt opgeslagen, is de distributie van het certificaat aan consumenten device is zeer risicovol. Een alternatief is de vingerafdrukken templates versleutelen en voor een eerste uitgifte van een identiteitsdocument centraal op te slaan. Voor het vernieuwen van het identiteitsdocument kan de vingerafdruk uit de centrale database worden gehaald en hergebruikt. Een centrale database met vingerafdrukken kent echter diverse beveiligings- en privacy-uitdagingen (zie sectie 3.5).
- De uitgifte van het vernieuwde paspoort kan een fysiek proces blijven. Essentieel hierbij is dat het paspoort inderdaad aan de juiste persoon wordt uitgegeven. Vooral omdat de persoon de aanvraag online heeft gedaan en, in tegenstelling tot het huidige proces, niet fysiek op het gemeentehuis is geweest. De identiteit van de persoon zou bijvoorbeeld bij afhalen van het paspoort geverifieerd kunnen worden door een vingerafdruk af te nemen en deze te vergelijken met de afdruk op het uit te reiken paspoort. De afgifte van het vernieuwde identiteitsdocument is een belangrijk moment waarbij de verificatie van de identiteit en de vingerafdrukken een zeer belangrijke rol speelt.

Voor het aanvragen van een eerste paspoort of in het geval de gebruiker geen paspoort of identiteitskaart meer heeft, zal deze gebruik moeten maken van het huidige proces.

Online gebruik van een identiteitsdocument

Het gebruik van een identiteitsdocument voor de online verificatie van de identiteit wordt steeds populairder. Eerder ging dat vaak middels het uploaden van een foto van een identiteitsdocument. Dit is erg fraudegevoelig. Tegenwoordig zijn er oplossingen waarmee de gegevens op de chip van het document kunnen worden uitgelezen met NFC-technologie die aanwezig is op bijvoorbeeld smartphones. Veel banken maken hiervan gebruik bij het onboarden van nieuwe klanten en waarmee ze moeten voldoen aan vigerende ‘know your customer’, ‘customer due dilligence’ en ‘anti-money laundering’ wet en regelgeving.

De zogenaamde ‘houderverificatie’ is essentieel bij een dergelijk online gebruik van een identiteitsdocument. Dat is een controle waarbij gecheckt wordt of het document inderdaad bij de houder ervan hoort. Een invulling hiervan is de van chip uitgelezen foto van de gebruiker te vergelijken met een door de gebruiker zelf gemaakte selfie. Met een vingerafdruk zou dit theoretisch ook kunnen, echter, de templates hiervan op de chip zijn niet toegankelijk voor breed gebruik. Bij het afnemen van selfie is het uitvoeren van een liveness check cruciaal om fraude te voorkomen.

Mocht een vingerafdruk ook toegankelijk worden voor biometrische verificatie, dan is het de vraag of oplossingen die de gebruiker zelf kan toepassen voldoende kwaliteit leveren en/of de juiste template toepassen om een betrouwbare verificatie te realiseren. Standaardisatie is dan wenselijk. Daarnaast is liveness detectie van vingerafdrukken bij optische en ultrasone scanners een uitdaging. Vooral in vergelijking met liveness detectie voor gezichtsherkenning.

Samenvatting

Maak voor het aanvragen van een identiteitsdocument gebruik van het huidige proces waarbij de aanvrager zich fysiek aan de balie moet identificeren en een medewerker de aanvraag afhandelt. Bij vernieuwing van een identiteitsdocument aan de balie kan biometrie op basis van gezichtsherkenning worden ingezet om de identiteit van de aanvrager beter vast te stellen. Neem ter plekke en/of onder gecontroleerde omstandigheden de biometrie van het gezicht (i.e. pasfoto) en vingerafdruk af. Ter plekke afnemen van het gezicht heeft meerdere voordelen, zoals betere kwaliteit van een direct digitaal opgenomen foto met betrekking tot de resolutie, waardoor de consistentie van kwaliteit kan beter geborgd worden, en het voorkomen van morphen. Overweeg voor het vernieuwen van een document een gedeeltelijk online proces. Dit kan door inzet van DigiD op niveau Substantieel of Hoog of door middel van online gebruik van het oude identiteitsdocument met behulp van NFC en gezichtsherkenning met liveness detectie. Maak hergebruik van de bestaande vingerafdruk door deze van de chip te halen of uit een nieuw te ontwikkelen centrale database. De aanvrager dient diens

nieuwe document fysiek af te halen. Zet hiervoor vingerafdrukherkenning in om de identiteit van de afhaler te controleren en hiermee het huidige proces te versterken. Immers, de betreffende persoon komt dan nog maar één keer aan de balie. Indien het identiteitsdocument per post wordt verstuurd moet de aanvrager het verouderde identiteitsdocument verifiëren met behulp van NFC en gezichtsherkenning met liveness detectie. In dit geval moet de aanvrager eenmalig aan de balie verschijnen bij het indienen van het vernieuwingsverzoek.

5.3 Aanvraag, gebruik en vernieuwen van een authenticatiemiddel

In Nederland zijn er op dit moment twee door de overheid erkende digitale authenticatieoplossingen die worden gebruikt voor authenticatie voor overheidsdienstverlening:

- DigiD voor authenticatie van burgers die gebruik willen maken van persoonlijke overheidsdiensten, bijvoorbeeld toegang tot MijnOverheid, UWV, gemeentelijke diensten, zorgverzekeringen
- eHerkenning voor authenticatie van gebruikers die namens een bedrijf willen inloggen bij de overheidsdiensten.

Hoewel er ook andere oplossingen zijn, zoals iDIN voor consumenten, is de focus van dit onderzoek op de overheidsoplossingen en dus de eerste twee oplossingen (DigiD en eHerkenning). Vanuit de eIDAS verordening moeten Europese burgers zich ook kunnen authentiseren met hun eigen nationale en erkende digitale oplossing voor toegang tot Nederlandse overheidsdiensten. Op dit moment zijn diverse nationale middelen genotificeerd, waaronder die van Duitsland, Italië, Estland, België, Spanje en Luxemburg. Overheidsdiensten geven aan welk betrouwbaarheidsniveau nodig is voor authenticatie. Hiervoor kent eIDAS drie niveaus van betrouwbaarheid:

- **Laag**: weinig zekerheid, één factor toegestaan, erkenning op vrijwillige basis.
- **Substantieel**: hoge mate van zekerheid, altijd twee factoren, verplichte erkenning.
- **Hoog**: zeer hoge mate van zekerheid, altijd twee factoren, verplichte erkenning.

Zowel eHerkenning als DigiD kennen verschillende betrouwbaarheidsniveaus van authenticatie. Als het gaat over biometrie, dan wordt dit binnen de eIDAS verordening niet uitgesloten. Uit de recente notificatietrajecten van België en Letland is gebleken dat het inzetten van biometrie als authenticatiefactor betrouwbaarheidsniveau Hoog voorlopig niet toegestaan is. Onduidelijk is of en hoe biometrische oplossingen weerstand kunnen bieden tegen aanvallers met een hoog aanvalspotentieel, een van de eisen uit een onderliggende eIDAS uitvoeringsverordening. Het gebrek aan normen of richtlijnen voor het inschalen van op biometrie gebaseerde authenticatie oplossingen helpt hierbij niet. Op Substantieel is het toegestaan mits additionele maatregelen zijn getroffen om de betrouwbaarheid van de biometrische oplossing te borgen. Dit betreft bijvoorbeeld het uitsluiten van mobiele telefoons waarvan bewezen is dat de biometrie eenvoudig te misleiden is met foto's of nagemaakt vingerafdrukken of waarbij geen gebruik wordt gemaakt van de Secure Enclave of Trusted Execution Environments voor het opslaan van kritische authenticatie credentials.

Over eHerkenning & DigiD

eHerkenning kent een verscheidenheid aan authenticatiemiddelen op verschillende betrouwbaarheidsniveaus die door private leveranciers worden aangeboden. De middelen op betrouwbaarheidsniveaus Substantieel en Hoog zijn het meest relevant voor biometrische mogelijkheden. eHerkenning Substantieel en Hoog bestaan altijd uit twee factoren: wat je weet en wat je hebt[115]. Voorbeelden van middelen op niveau Substantieel zijn wachtwoord + SMS OTP, wachtwoord en hardware token, PIN en mobiele app. De Hoog middelen bestaan typisch uit een smartcard met daarop een gekwalificeerd (PKI-overheid) certificaat.

Ook DigiD heeft verschillende betrouwbaarheidsniveaus[116]:

1. Basis: gebruikersnaam en wachtwoord.
2. Midden: DigiD Basis in combinatie met DigiD app of sms-controle.
3. Substantieel: Upgrade van de DigiD Midden app door een eenmalige ID-check op basis van wettelijk identiteitsdocument dat via NFC wordt uitgelezen. Hier zit geen selfie-check bij.

[115] Een overzicht van eHerkenningsmiddelen per leverancier en per niveau is hier te vinden: https://www.eherkenning.nl/inloggen-met-eherkenning/leveranciers/leveranciersoverzicht.
[116] Meer informatie over DigiD is hier te vinden: www.digid.nl.

4. Hoog: Het wettelijk identiteitsdocument is tweede authenticatiefactor naast een PIN voor de DigiD app waarmee het identiteitsdocument wordt gescand middels NFC.

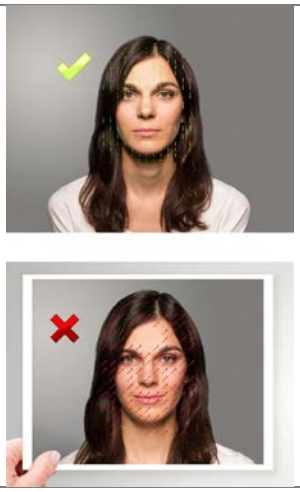
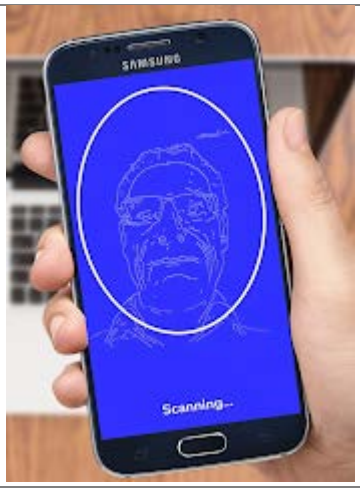
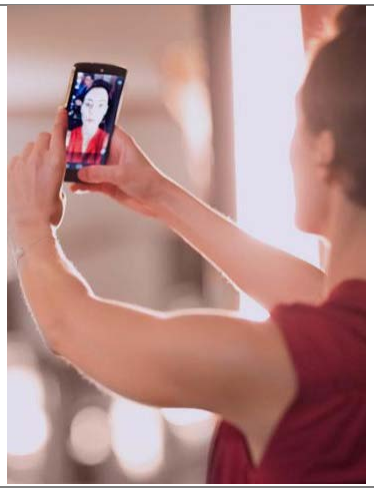
eHerkenning	DigiD

Biometrische gegevens kunnen de “wat je weet” factor, ofwel de PIN of wachtwoord, van een twee-factor authenticatie vervangen. De tweede factor blijft de “wat je hebt” ofwel een mobiele app of smartcard. Aandachtspunt van biometrie als authenticatiefactor is de betrouwbaarheid ervan. Immers, in tegenstelling tot een PIN-code die juist of onjuist is ingevoerd, zijn biometrische factoren niet binair.

Aanvragen van een authenticatiemiddel

In het aanvraagproces voor een authenticatiemiddel is een goede identificatie van essentieel belang. Het hoogste betrouwbaarheidsniveau eist grote zekerheid over de identiteit van de gebruiker. Dit wordt momenteel gerealiseerd door fysieke identificatie van de gebruiker aan de balie en op basis van een wettelijk identiteitsdocument. Voor het lagere niveau substantieel is identificatie op afstand steeds meer een best practice. Dit is goedkoper (geen dure balies meer) en gebruikersvriendelijker (de klant hoeft niet meer naar de balie toe). Voor het verstrekken van eHerkenningsmiddelen wordt bijvoorbeeld gebruik gemaakt van identificatie op afstand op basis van selfies van de gebruiker voor houderverificatie. Deze selfies worden vergeleken met de pasfoto van de gebruiker op diens wettelijke identiteitsdocument. De pasfoto kan zijn uitgelezen van de chip van het identiteitsdocument met behulp van NFC-technologie in de smartphone of via een foto van het document. Het vergelijken van de foto met de selfie is nog een handmatig proces waarbij een back-office medewerker van de middelenverstrekker op afstand beoordeeld of de foto overeenkomt met de selfie. Merk op dat een foto die rechtstreeks van de chip wordt uitgelezen een veel hogere kwaliteit, scherpte, resolutie heeft dan een foto die is gemaakt van de fotoprint op het identiteitsdocument. Dit heeft invloed op de kwaliteit van de handmatige vergelijking.

NB: Een belangrijke uitdaging in het identificatieproces is het controleren van de echtheid van het identiteitsdocument. Bij de NFC variant worden automatische echtheidscontroles van de chip uitgevoerd en de verificatie van het document. Wanneer gewerkt wordt met een foto of kopie van het identiteitsdocument is echtheidscontrole bijna niet te doen.

		
BioID bewegingsdetectie.	Liveness detectie met kleuren.	Video challenge response.

Er zijn ontwikkelingen gaande om het identificatieproces te automatiseren door biometrische oplossingen voor gezichtsherkenning in te zetten. Op dit moment maken de middelenuitgevers in eHerkenning nog geen gebruik van biometrie in het aanvraagproces. Door inzet van biometrie wordt zogenaamde ‘straight-through processing’ mogelijk wat tot veel meer efficiëntie leidt (dus meer gebruiksgemak en lagere kosten voor enrolment). De belangrijkste uitdaging bij gezichtsherkenning is het uitvoeren van liveness detectie

(bewegingsdetectie, kleurpatronen, video-challenge-respons) om te vermijden dat mensen met een foto van iemand de gezichtsherkenning voor de gek houden. Daarnaast zijn er andere manier om gezichtsherkenning te manipuleren (bijv. maskers of make-up). Zie hoofdstuk 2, sectie 2.8. Andere uitdaging is om aan goed/betrouwbaar referentiemateriaal te komen, met name een database met voldoende aantal gezichtsafbeeldingen om de gezichtsherkenning algoritme te kunnen testen.

Een aantal middelenleveranciers gebruiken video-gebaseerde identificatie. De gebruiker wordt dan door een medewerker van de middelenverstrekker via een video verbinden geïdentificeerd. Typisch voor betrouwbaarheidsniveau Substantieel. Uitdagingen voor video-identificatie zijn:

- Het betrouwbaar vaststellen van de identiteit van de gebruiker op basis van de pasfoto in het getoonde identiteitsdocument via een videokanaal. De (kleine) pasfoto is nauwelijks goed waar te nemen via video.
- Echtheidscontrole van het getoonde identiteitsdocument. Echter is het ondoenlijk omdat de echtheidskenmerken zoals papiersoort, inkt en microtest vallen weg tijdens een video-opname.
- Voorkomen van real-time manipulatie van videobeelden.

De Duitse BaFin[117] heeft allerlei eisen gespecificeerd waaraan dergelijke video-gebaseerde identificatieoplossingen moeten voldoen. Het voordeel van de video-gebaseerde identificatie is dat de gebruiker geen reis naar het loket hoeft te ondernemen. Een belangrijk nadeel is de schaalbaarheid. Een video-sessie duurt relatief lang (~10 minuten) waardoor het verwerken van grote hoeveelheden gebruikers per dag een uitdaging is.

Identificatie op afstand op niveau Substantieel wordt bijvoorbeeld ook toegepast in de financiële sector, bijvoorbeeld voor het onboarden van nieuwe klanten. Door zogenaamde Know Your Customer (KYC) en Anti-Money Laundering (AML) wetgeving dienen banken de identiteit van hun klanten goed vast te stellen. In het hoger onderwijs is SURF aan het experimenteren met identificatie op afstand voor sterke authenticatie[118]. Identificatie op afstand voor een middel op niveau Hoog is niet uitgesloten in eIDAS wetgeving. Echter, onduidelijk is waar oplossingen dan aan moeten voldoen. In ieder geval dienen de hierboven genoemde uitdagingen te zijn geadresseerd. Volgend uit eIDAS is eHerkenning als identificatie op afstand voor Hoog niet toegestaan; er dient altijd een fysieke identificatie aan de balie plaats te vinden door hiervoor opgeleide baliemedewerkers.

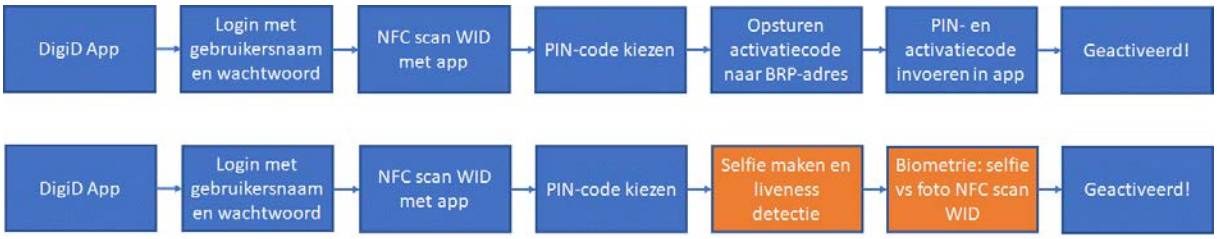
Waar voor eHerkenning biometrie stilaan een onderdeel wordt in het aanvraagproces, is dat voor DigiD nog niet in beeld. Het uitgifteproces van DigiD is grotendeels gebaseerd op de Basisregistratie Personen (BRP) en het burgerservicenummer (BSN). Een DigiD aanvraag verloopt simpelweg via opgave van het BSN op de DigiD-website. Daarna wordt binnen 3 werkdagen een activatiecode gestuurd naar het adres dat bekend is in het BRP. Na invoeren van de code kan de burger een wachtwoord aanmaken voor DigiD Laag. Daarna is 'opwaarderen' naar DigiD Midden mogelijk door de mobiele app te installeren, te identificeren met NFC en WID, waarna wederom een activatiecode per post wordt gestuurd. Aanvragen van DigiD Substantieel duurt enkele dagen. Het is voorgekomen dat activatiecodes uit brievenbussen worden gevist[119] waardoor ze in sommige gebieden persoonlijk worden overhandigd door de postbode.

DigiD Hoog bevindt zich nog in een pilot-fase. DigiD Hoog maakt gebruik van een WID als tweede-factor ("wat je hebt") in combinatie met een PIN-code ("wat je weet"). Iedere keer als de burger zich wil authentiseren dient deze zijn WID te scannen middels NFC via de app op de mobiele telefoon. Het uitgifteproces wijkt niet af van dat voor Substantieel.

Kan het inzetten van biometrie het uitgifteproces van DigiD sneller en betrouwbaarder maken? Een goed voorbeeld is de Indiase eID oplossing Aadhaar, waar een twee-dagen durend bureaucratisch registratieproces om de identiteit van de burger vast te stellen vervangen is door het afnemen van een vingerafdruk in 30-seconden[120]. Dit laatste maakt dat je kan terugvallen op de identificatie die destijds heeft plaatsgevonden. Bij DigiD is er één stap in het proces dat relatief veel tijd in beslag neemt: het via de post versturen van de

[117] BaFin Circular 3/2017 (GW) - Video Identification Process, zie: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html.
[118] Remote vetting voor SURFsecureID, SURF, 2018, zie https://blog.surf.nl/remote-vetting-voor-surfsecureid/.
[119] DigiD phishing fraude, zie bijvoorbeeld https://www.security.nl/posting/372385/Identiteitsdieven+stelen+tonnen+via+DigiD-fraude.
[120] Vindu Goel, "India's top court limits sweep of biometric ID program," New York Times, September 25, 2018, zie: https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html.

activatiecode naar het fysieke BRP-adres van de burger. Dit 'breekt' het aanvraagproces aanzienlijk: de burger kan pas enige dagen later diens DigiD activeren. De reden waarom deze stap in het proces zit is om er zeker van te zijn dat het inderdaad de juiste burger is die een DigiD wil aanvragen, en niet een fraudeur. Hiervoor gebruikt de overheid een voor haar bekend en onafhankelijk kanaal: het adres van de burger. Een dergelijke zekerheid zou ook met biometrie kunnen worden verkregen door gezichtsherkenning toe te passen, vergelijkbaar met aanvraag van eHerkenning op basis van NFC en selfie-check in combinatie met liveness detectie. Voor DigiD Substantieel is dit haalbaar. Onderstaande figuur (Figuur 28) schetst het huidige proces voor het opwaarderen van de app naar Substantieel (bovenste proces) en een alternatief proces (onderste proces) waarin biometrie is verwerkt[121]. De biometrie aanvulling in oranje, vervangt de activatiecode.



Figuur 28: DigiD Substantieel app activatie met en zonder biometrie (gezichtsherkenning).

In termen van aantallen stappen zijn beide processen gelijkwaardig. Echter, qua doorlooptijd, is de biometrische variant sneller. Wel kan het selfie-proces minder gebruikersvriendelijk overkomen. Een variant zou kunnen zijn gebruik te maken van een vingerafdruk. Toegang tot de vingerafdruk op het WID is op dit moment niet mogelijk voor dit soort toepassingen. Bovendien dient de DigiD app toegang te hebben tot de vingerafdruklezer van de mobiele telefoon voor het importeren van de met NFC uitgelezen vingerafdruk. De software van de DigiD app kan deze vervolgens vergelijken met de door de lezer uitgelezen afdruk. Door de geslotenheid van de vingerafdruk op de chip van der identiteitsdocument is dit momenteel niet mogelijk.

Voor een online aanvraagproces op niveau Hoog lijkt biometrie nog een stap te ver: de huidige identificatie op afstand en gezichtsherkenningsoplossingen zijn (nog) niet betrouwbaar genoeg om hiervoor in aanmerking te komen.

5.4 Biometrie als onderdeel van het gebruik van authenticatiemiddelen

Hiervoor ging het over biometrie als onderdeel van het authenticatieproces. Een andere toepassing van biometrie in de context van authenticatiemiddelen is het gebruik van biometrie in plaats van de PIN-code. Voor veel toepassingen is dit al een gebruikelijke manier van werken. Denk aan TouchID of FaceID op de Apple toestellen of varianten hiervan op de Android telefoons die toegang verlenen tot de telefoon. Of bijvoorbeeld ING en Rabobank die dergelijke technologie toepassen voor toegang tot financiële diensten. Het is gebruikersvriendelijk en daardoor populair bij gebruikers. Voor banken is dit een ideale aanpak: leunen op bestaande en bekende technologie en niet zelf iets hoeven aan te bieden.

Echter, de betrouwbaarheid van deze oplossingen laat te wensen over of is niet helemaal duidelijk en transparant. Banken kiezen er daarom bijvoorbeeld voor om Apple oplossingen wel te vertrouwen en sommige Android-oplossingen niet. Vooral bij de wat goedkopere Android gebaseerde telefoons is het redelijk eenvoudig om de vingerafdruk of gezichtsherkenningsoplossing voor de gek te houden (zie sectie 2.6). Wanneer de betrouwbaarheid niet gegarandeerd is, dan moet de dienstverlener afwegen of biometrie als (enige) factor voor authenticatie verantwoord is.

Voor authenticatiemiddelen zoals eHerkenning en DigiD is dat zeker niet verantwoord, zeker niet op niveau Hoog. Een andere vraag is of het wenselijk is dat nationale authenticatieoplossingen als DigiD en eHerkenning afhankelijk zijn van mobiele biometrische oplossingen van platform leveranciers als Apple en Google. Wat als deze partijen besluiten te stoppen met hun oplossingen, dat ze hier geld voor gaan vragen, of als er een achterdeurtje is waarmee te kunnen meekijken bij al onze logins? Belangrijk is dat alternatieve

[121] Op basis van het proces zoals geschetst op https://www.digid.nl/over-digid/app/activeren/stappenplan-digid-app-activeren/.

authenticatiefactoren blijven bestaan, zoals de PIN-code of het wachtwoord. Wel ontstaat de situatie dat een biometrie-gebruiker zijn PIN of wachtwoord snel zal vergeten. Een efficiënt reset proces is dan wenselijk. Een andere strategie om te voorkomen dat de gebruiker door biometrie zijn PIN/wachtwoord vergeet is deze met enige regelmaat toch te vragen (bijvoorbeeld na elke 10de inlog met biometrie).

Een bijkomende uitdaging van op biometrie gebaseerde authenticatie en betrouwbaarheidsniveaus is dat er geen eenduidig normkader bestaat. Welke betrouwbaarheid moet een biometrische authenticatie-oplossing hebben in termen van FAR/FRR om in aanmerking te komen voor Substantieel of Hoog? Waaraan dient de beveiliging van de biometrische oplossing te voldoen in het geval van aanvallers met een gemiddeld of hoog aanvalspotentieel? Zijn certificeringen wenselijk en praktisch te handhaven? Etc. Zowel de bestaande normenkaders van eIDAS als eHerkenning geven hiervoor geen houvast.

5.5 Beoordeling biometrie in de use-cases

Op dit moment beperkt biometrie in de use-cases zich tot de handtekening, de foto en de vingerafdruk omdat deze direct gekoppeld kunnen worden aan identiteitsdocumenten. Een paspoort en een verblijfsvergunning bevatten een vingerafdruk, een foto en een handtekening. Rijbewijzen en identiteitskaarten bevatten de foto en de handtekening. De handtekening is afgedrukt in een klein formaat. Op het rijbewijs staat de handtekening ook op de chip in een lage resolutie. De vingerafdruk staat op de chip en is niet toegankelijk zonder de beveiligingssleutel die in de praktijk alleen bedoeld is voor specifieke opsporing. Wanneer het gaat over geautomatiseerde biometrische oplossing is eigenlijk alleen de foto geschikt om te gebruiken.

Voor beide use-cases is een hoge mate van zekerheid over de identiteit van een persoon gewenst. De betrouwbaarheid van biometrische oplossingen is ook afhankelijk van de processen er omheen en is lastig te bepalen, in het bijzonder in relatie tot de niveaus van eIDAS. Hier zijn simpelweg nog geen normen voor. In het beoordelingskader stelden we dat de betrouwbaarheid van gezichtsherkenning nog wat aandachtspunten heeft, dat geldt ook voor vingerafdrukken en zeker voor handtekeningen.

Hieronder volgt een overzicht van de aanbevelingen per use-case wat betreft de mogelijke biometrie toepassingen. Per toepassing is bekeken of en hoe biometrie een bijdrage kan leveren om tot verdere optimalisatie van de huidige situatie te komen, bijvoorbeeld door het gebruikersvriendelijker, betrouwbaarder, of sneller te maken.

Een belangrijke toepassing betreft de aanvraag, het gebruik en de vernieuwing van identiteitsdocumenten. Uit de analyse van deze toepassing komen de volgende aanbevelingen naar voren in relatie tot het gebruik van biometrie:

- Aanvraag: Streef gedurende de registratie naar een zo hoog mogelijke kwaliteit bij het vastleggen van de biometrische kenmerken ter plekke ter voorkoming van fraude (zoals het aanleveren van aangepaste/gemorphde pasfoto's).
- Aanvraag: Verbeter de identificatie van de gebruiker bij het overhandigen van het identiteitsdocument doormiddel van de geautomatiseerde biometrische vergelijking in te zetten (vinger of gezicht).
- Gebruik (offline): Stimuleer het gebruik van de biometrie op de chip van het identiteitsdocument zodat betrouwbaardere identificatie mogelijk wordt (in plaats van op basis van een kopie van het document). Bijvoorbeeld tijdens de verificatie van de identiteit bij de gemeente, doormiddel van de geautomatiseerde biometrische vergelijking in te zetten (vinger of gezicht).
- Gebruik (online): Verifieer de authenticiteit van het identiteitsdocument door de authenticiteit van en informatie op de chip te verifiëren en voer te allen tijde een liveness check uit, bijvoorbeeld op de website van de gemeente om een aanvraag voor het vernieuwen van een identiteitskaart in te dienen.
- Vernieuwing: Verken de online vernieuwing mogelijkheid op basis van biometrie en de implementatie voorwaarden ervan. Hierdoor hoeft de burger niet twee keer naar de balie te komen voor aanvraag en ophalen van het vernieuwde identiteitsdocument.
- Vernieuwing: Laat de gebruiker diens nieuwe pasfoto digitaal aanleveren en vergelijk deze met de oude, doormiddel van gezichtsherkenning. De oude pasfoto kan uit de chip worden uitgelezen of uit de systemen van betreffende gemeente worden gehaald.

- Vernieuwing: Maak gebruik van de vingerafdruk templates; toegang tot de vingerafdruk op de chip is hiervoor noodzakelijk of richt hiervoor als alternatief een (centrale) overheidsdatabase in voor vingerafdrukken.

Een tweede relevante toepassing betreft de aanvraag, het gebruik en de vernieuwing van nationaal erkende authenticatiemiddelen:

- Aanvraag: Identificatie op afstand in plaats van fysiek aan de balie is mogelijk met behulp van biometrie en op basis van de pasfoto uit de chip van het identiteitsbewijs.
- Aanvraag: Verifieer de authenticiteit van het identiteitsdocument door de authenticiteit van en informatie op de chip te verifiëren en voer te allen tijde een liveness check uit om fraude te voorkomen.
- Gebruik: Gezicht of vingerafdruk als tweede authenticatiefactor gebruiken bij inloggen in plaats van wachtwoord of PIN-code. Gebruik biometrie nooit als enige factor.
- Gebruik: Altijd 'fall-back' scenario nodig, bijvoorbeeld als een persoon zich via biometrie niet kan registreren.
- Gebruik: mensen vergeten snel 'wat je weet' (PIN), laat daarom de authenticatie software regelmatig (e.g. elke week) om een PIN vragen i.p.v. biometrie.
- Vernieuwing: Idem als aanvraag authenticatiemiddel.
- Vernieuwing: Gebruik biometrie voor een PIN- of wachtwoord-reset om het doorlopen van een volledig nieuwe registratie bij vergeten ervan te voorkomen.

Use-case: aanvraag identiteitsdocument

In het huidige aanvraagproces van identiteitsdocumenten zijn volgende kwetsbaarheden geconstateerd:

- Manipulatie van de aangeleverde (afgedrukte) foto
- 'Look-alike' fraude
- Geen verificatie van de vingerafdrukken bij de gemeente, terwijl de infrastructuur er is.

Aanbevelingen

- Foto real time maken tijdens aanvraag aan de balie
- Ondersteunen baliemedewerker met geautomatiseerde gezichtsherkenning
- Streef naar zo hoge mogelijke kwaliteit van het biometrische kenmerk bij de enrolment en leg het ook met zo hoog mogelijke kwaliteit vast
- Identiteit vaststelling bij het overhandigen. Dat zorgt voor de veilige overgang van het overheidsdomein naar het private domein (dus het overdragen aan de burger).

Use-case: gebruik identiteitsdocument

Volgende internationale en nationale trends zijn actueel voor deze use-case, wat betreft het gebruik van de identiteitsdocumenten en biometrie:

- Onboarding bij banken
- Identificatie persoon door de politie
- Toename online gebruik identiteitsdocumenten.

Aanbevelingen

- Maak geen gebruik van de optische scan van de foto op ID document, maar de foto uit de chip
    - NFC technologie, mobiele verificatie
- Verifieer de authenticiteit van het identiteitsdocument door de authenticiteit van en informatie op de chip te verifiëren en voer te allen tijde een liveness check uit.

Use-case: vernieuwing identiteitsdocument

In het huidige proces zijn een aantal verbeterpunten geconstateerd:

- Nu twee keer aan de balie: aanvraag en bij het ophalen

Aanbevelingen: online vernieuwing

- Nieuwe foto digitaal aanleveren en vergelijken met de oude (gezichtsherkenning)
- Overweeg hergebruik vingerafdruk templates (alleen voor nieuwe ID kaart en paspoort)
    - Voorwaarde: toegang vingerafdruk op de chip noodzakelijk.
    - Aanbeloven frequentie van re-enrollment van de vingerafdrukken is elke 5-10 jaar.

Use-case: aanvraag authenticatiemiddel

Bij de online aanvraag van het authenticatiemiddel kan biometrie zeker een belangrijke rol spelen, bijvoorbeeld voor de aanvraag van DigiD, PKI-overheid certificaat of eHerkenning middel. Vooral voor het betrouwbaarheidsniveau substantieel en hoog. Volgende uitdagingen zijn essentieel:

- Liveness detectie
- Echtheid identiteitsdocument
- Koppeling aan de gebruiker - houderverificatie
- Straight through processing (in plaats van tot 3 dagen wachten).

Aanbevelingen:

- Maak gebruik van de NFC chip voor het verifiëren van de biometrische gegevens daarop
- Verifieer de authenticiteit van het WID document via NFC op mobiel door de authenticiteit van en informatie op de chip te verifiëren en voer te allen tijde een liveness check uit.
- Zet biometrie in voor de matching (gezichtsherkenning).

Use-case: gebruik authenticatiemiddel

Volgende aanbevelingen zijn actueel voor het gebruik van de biometrie als het authenticatiemiddel:

Aanbevelingen:

- Gezicht of vingerafdruk als 2de factor gebruiken voor inloggen
- Biometrie nooit als enige factor bij een authenticatie oplossing
- Altijd fall back scenario nodig, bijvoorbeeld als een person niet kan enrollen
- Gebruikersgemak: mensen vergeten snel ‘wat je weet’ (PIN), daarom:
    - Laat de authenticatie software regelmatig (e.g. elke week) om een PIN vragen i.p.v. biometrie
- Definieer een eenduidig normenkader voor het bepalen van het betrouwbaarheidsniveau van authenticatieoplossingen die gebruik maken van biometrie.

Use-case: vernieuwing authenticatiemiddel

Voor de vernieuwing van de authenticatiemiddel gelden dezelfde aanbevelingen als voor de aanvraag van de authenticatiemiddel. Daarnaast zou biometrie ingezet kunnen worden voor de pin reset.

Aanbevelingen:

- Idem als aanvraag authenticatiemiddel;
- Gebruik biometrie voor een PIN-reset om het doorlopen van een volledig nieuwe registratie bij vergeten ervan te voorkomen.

5.6 Discussie (online) use-cases

Nederland kent op dit moment een relatief decentrale aanpak voor het verwerken van biometrische gegevens. Foto’s zijn, naast opslag in de chip van het identiteitsdocument, ook decentraal opgeslagen bij de gemeenten; vingerafdrukken staan alleen op de chip en dus decentraal. Een dergelijke decentrale aanpak kent diverse voor- en nadelen in termen van privacy, beveiliging en fraudedetectie. Echter, hetzelfde geldt voor een eventuele

centrale aanpak voor biometrische gegevensopslag. *Nader onderzoek is nodig om uitsluitsel te geven welk architectuurmodel de voorkeur heeft bij een grootschaliger toekomstig gebruik van biometrie in het kader van het verwerken van identiteitsdocumenten.*

Authenticatiemiddelen worden geclassificeerd in termen van betrouwbaarheidsniveaus voor identiteitszekerheid: laag, substantieel of hoog. De bestaande normenkaders hiervoor bieden echter weinig houvast als het gaat om biometrie. Bijvoorbeeld, aan welke kwaliteit van de enrolment moeten biometrische authenticatiemiddelen voldoen? Welke False Acceptance Rate is vereist om te voldoen aan niveau hoog? En welke beveiligingsmaatregelen zijn vereist om weerstand te bieden tegen een aanvaller met een gemiddeld respectievelijk hoog aanvalsprofiel? Om voor erkenning in aanmerking te komen dienen authenticatieoplossingen te voldoen aan een bepaalde betrouwbaarheid. Dit geldt voor eIDAS erkenning op Europese schaal en in de toekomst op basis van de Wet digitale overheid op nationale schaal. Zonder normen voor biometrie is het betrouwbaarheidsniveau lastig te bepalen en mogelijk een belemmering voor erkenning en adoptie ervan voor toegang tot overheidsdiensten. *Vereist is dus dat er normen komen om op biometrie gebaseerde authenticatieoplossingen in te schalen in termen van betrouwbaarheidsniveaus.*

Gebaseerd op de use-cases analyse en de beoordeling van diverse modaliteiten, zijn gezichtsherkenning en vingerafdruk meest geschikte modaliteiten voor de verificatie van de identiteit. Iris is niet uitgesloten, hoewel een risico op afgeleide medische informatie minder pleit voor deze modaliteit.

Als het gaat om prestaties van een biometrie oplossing dan kijken we vooral naar de False Acceptance Rate (FAR) dat inzicht geeft in het onterecht matchen van de gegevens van de aanvrager met de biometrische gegevens op de chip van het identiteitsdocument. Voor de vingerafdrukoplossing TouchID van Apple is dat 1 op 50.000 en voor de gezichtsherkenningoplossing FaceID is dat 1 op 1.000.000. Deze foutenpercentages worden door Apple zelf vermeld zonder details over de populatie variatie[122]. De Amerikaanse standaardisatie organisatie NIST zegt dat maximaal 1 op 1.000 voldoende is, maar specificeert niet het niveau van betrouwbaarheid dat hierbij past. Deze statistiek is volgens Apple anders voor tweelingen en broers en zussen die op jezelf lijken en bij kinderen jonger dan 13 jaar, omdat hun verschillende gelaatstrekken mogelijk niet volledig zijn ontwikkeld. Daarnaast is onduidelijk wat er van dergelijke getallen overblijft als iemand gericht probeert het systeem te manipuleren. Bij de vingerafdruk oplossing van Apple is het bovendien mogelijk voor de gebruiker om meerdere vingers te enrollen (maximaal 5). Dit heeft een negatieve invloed op de FAR: bij 3 vingers neemt de FAR met een factor 3 toe. Daarnaast is het zelfs mogelijk om vingers van verschillende gebruikers te enrollen.

Een ander aandachtspunt is de mate van controle op dergelijke mobiele biometrische oplossingen. De toegang tot de vingersensor is lastig en volledig bepaald door de leverancier. Hierdoor is het bijvoorbeeld lastig om, in het geval van DigiD, de vingerafdruk op het identiteitsdocument te gebruiken (bij de aanname dat deze kan worden ontsloten voor authenticatiedoeleinden). Voor gezichtsherkenning ligt dit wat eenvoudiger; toegang vanuit applicaties tot de camera is meer open en biedt dus meer mogelijkheden voor controle, mits er ook een referentie bestand is. Echter, de vraag is of met app-specifieke gezichtsherkenningsoplossingen op basis van camerabeelden van de telefoon op hoge kwaliteit te realiseren is zoals het gesloten FaceID.

Wat betreft de vingerafdrukken en de use-case vernieuwen identiteitsdocument: het blijft een toekomstscenario totdat toegang tot de vingerafdrukken op de chip in de documenten mogelijk is. De vingerafdruk blijkt een relatief stabiele biometrie en geschikt voor langdurig (her)gebruik, vooral voor gebruikers in de leeftijdscategorie van 12-65 jaar zo blijkt uit diverse grootschalige internationale onderzoeken (Galbally et al., 2018; Yoon en Jain, 2015). Dit wordt ook bevestigd door geïnterviewde experts. Het beste is om om de 5-10 jaar de vingerafdrukken af te nemen om de toekomstige mismatchproblemen te voorkomen. Zelfs een permanent litteken kan ervoor zorgen dat de vingerafdruk van een persoon er aanzienlijk anders uitziet en een ernstige impact kan hebben op de herkenning. Bij her-enrollment kan het litteken echter worden gezien als een onderscheidend kenmerk van een persoon. Er moet ook het belang overwogen worden van het contactmoment van de aanvrager met de gemeente, welke andere doelen het dient behalve de biometrie afname.

[122] Zie: https://support.apple.com/en-us/HT208108.

6. Conclusies en aanbevelingen

Het gebruik van biometrie voor identificatie- en authenticatiedoeleinden wordt steeds meer geaccepteerd. Belangrijke drijfveer hiervoor zijn de van vingerafdruk- en gezichtsherkenning voorziene mobiele telefoons die zorgen voor een groot bereik onder gebruikers. Door het gemak wordt biometrie steeds meer gemeengoed als een tweede authenticatiefactor, onder meer bij banken die er gebruik van maken voor toegang tot betaaldiensten en op afstand verifiëren van identiteit voor aanvragen bankrekeningen. Aandachtspunten zijn er nog wel aangaande de betrouwbaarheid van biometrie, normen hiervoor die de betrouwbaarheid op een objectieve manier kwantificeren inclusief presentation attack detection (PAD), dat biometrie voor sommige mensen faalt (inclusie) en privacy. Met betrekking tot privacy is met name de manier van verwerking van biometrische data (centraal of decentrale opslag) een aandachtspunt, naast nieuwe privacy enhancing technologieën om de opslag op een privacy-vriendelijke manier te doen. Dat neemt niet weg dat biometrie zinvol kan worden ingezet om bestaande overheidsprocessen rondom de aanvraag, het gebruik en de vernieuwing van identiteitsdocumenten en authenticatiemiddelen te optimaliseren in termen van betrouwbaarheid, doorlooptijd en gebruiksvriendelijkheid.

De belangrijkste algemene aanbevelingen voor het inzetten van biometrie voor het verifiëren van de identiteit en use-case specifieke aanbevelingen voor het aanvragen, gebruiken en vernieuwen van identiteitsdocumenten zijn:

- Het gebruik van biometrie voor identificatie- en authenticatiedoeleinden wordt steeds meer geaccepteerd. Belangrijke drijfveer hiervoor zijn de van vingerafdruk- en gezichtsherkenning voorziene mobiele telefoons die zorgen voor een groot bereik onder gebruikers. Door het gemak wordt biometrie steeds meer gemeengoed als een tweede authenticatiefactor, onder meer bij banken die er gebruik van maken voor toegang tot betaaldiensten en op afstand verifiëren van identiteit voor aanvragen bankrekeningen.
- Vingerafdruk en gezichtsherkenning zijn de meest voor de hand liggende biometrische oplossingen voor het verifiëren van de identiteit, wegens veel kennis en informatie aanwezig in dit domein en breed beschikbare sensoren op smartphones. Dat zorgt voor een brede adoptie onder gebruikers. Ga hiermee aan de slag om de processen voor het verstrekken en gebruiken van identiteitsdocumenten en authenticatiemiddelen te verbeteren.
- Gebruik biometrie als tweede factor, met altijd een alternatieve authenticatie oplossing als een fall-back scenario in het geval biometrie niet werkt. Zorg ervoor dat er altijd andere factoren aanwezig zijn om de identiteit te verifiëren, zowel op afstand als eventuele fysiek verschijnen zijn hiervoor een optie.
- Zorg daarbij voor adequate Presentation Attack Detection (PAD) oplossingen door bijvoorbeeld een goede liveness check uit te voeren. Pas de NIST 800-63-3 richtlijn voor PAD testen toe.
- Pas bestaande biometrie standaarden en richtlijnen toe voor het optimale evenwicht tussen privacy en veiligheid.
- Ontwikkel een normenkader om op biometrie gebaseerde authenticatieoplossingen in te schalen in termen van betrouwbaarheidsniveaus. Onderdelen van dit normenkader zijn o.a. de eisen aan de enrolment, verificatie, het gebruik van bepaalde standaarden, multimodale biometrie, PAD, FAR/FRR criteria per niveau, beveiliging tegen aanvallers met een bepaald potentieel en certificeringen.
- De nauwkeurigheid van de biometrische verificatie van de identiteit is afhankelijk van de kwaliteit van de biometrische kenmerken. De kwaliteit van het huidige gezicht kenmerk staat onder druk doordat de burger zelf een pasfoto moet aanleveren en dit gevoelig is voor morphing. Verbeter het aanleverproces van biometrische kenmerken voor identiteitsdocumenten. Neem ter plekke en/of onder gecontroleerde omstandigheden de biometrie van het gezicht (i.e. pasfoto) en vingerafdruk af. Of, als alternatief, richt voorzieningen in om morphing van de aangeleverde pasfoto te detecteren.
- Bij vernieuwing van een identiteitsdocument aan de balie kan geautomatiseerde biometrische oplossing de baliemedewerker ondersteunen met het verifiëren van de identiteit. Zet de gezichtsherkenning in om de identiteit van de aanvrager beter vast te stellen en identiteitsfraude te voorkomen. De baliemedewerker bij de gemeente krijgt een signaal op het moment dat foto van de burger niet overeenkomt met de foto op een eerder aangevraagd identiteitsdocument. Uiteraard moet de mens alert blijven en weten dat de gezichtsherkenningssysteem fouten kan maken.

- Laat de technische, organisatorische en juridische voor- en nadelen van een centrale database of decentrale database voor vingerafdrukken onderzoeken.
- Door dagelijks gebruik van mobiele biometrie op smartphones, bijvoorbeeld van de vingerafdruk voor bankdiensten, verwachten de burgers dezelfde snelheid, toegankelijkheid en gebruikersgemak van de overheidsdiensten. Verken en benut de mogelijkheden die de mobiele biometrie op dit moment te bieden heeft. Waak voor vendor lock-in risico's bij specifieke oplossingen.
- Het voordeel van een zelf ontwikkelde overheid-specifieke mobiele biometrische authenticatie applicatie voor toegang tot overheidsdiensten is de controle over de dataopslag en veiligheid keuzes. Verken dit alternatief, met eventuele integratie van een bestande biometrische verificatie oplossing die voldoet aan het zelf-ontwikkeld normenkader.
- Start in het verlengde van de RDW pilot voor het online verlengen van het rijbewijs een soortgelijke pilot rondom het online vernieuwen van het paspoort. Overweeg de harmonisatie van de identiteitsdocumenten processen met als voordeel efficiëntere gebruik van elkaars systemen en de infrastructuur voor de snellere en veiligere verificatie van de biometrische kenmerken. Bijvoorbeeld, voor het online vernieuwen van een identiteitsdocument moeten de vingerafdrukken hergebruikt kunnen worden. Het is belangrijk om op te merken dat tijdens dergelijke pilot de voorwaarden en consequenties nog verder onderzocht moeten worden in termen van de infrastructuur, veiligheid, privacy aspecten en maatschappelijke discussie.
- Onderzoek verder de mogelijkheden voor hergebruik van de vingerafdruk op het oude document of laat deze naast de pasfoto aanleveren door een erkende fotograaf of een gecertificeerde enrolment station.
- Vingerafdrukherkenning bij afhalen document is wenselijk in het geval de aanvraag online is gedaan. Standaardiseer dit proces en richt het in bij de betreffende afhaalpunten.
- Multi-modale biometrische toepassingen zijn nauwkeuriger en veiliger voor continu authenticatie dan uni-modale biometrie, dankzij de robuustheid tegen spoofing aanvallen. Gezien hoge kosten en lage gebruikersvriendelijkheid, zijn de multi-modale toepassingen op korte termijn niet geschikt voor het verifiëren van de identiteit. Hou deze ontwikkelingen wel goed in de gaten voor eventuele nieuwe mogelijkheden op langere termijn.

7. Referenties

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009) Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2 (3), 13—28.

Buriri, A. (2017) Behavioral Biometrics for Smartphone User Authentication, PhD Thesis, Department of Information Engineering and Computer Science, Univ. Of Trento, Italy.

Conti, V., Collotta, M., Pau, G. and Vitabile, S. (2014) Usability Analysis of a Novel Biometric Authentication Approach for Android-based Mobile Devices, In: *Telecomm. Information Technology*, vol. 4.

Corsetti, B., Blanco-Gonzalo, R. and Sanchez-Reillo, R. (2018) User Interaction in Mobile Biometrics, In: *26th European Signal Processing Conference (EUSIPCO)*, 543—547. DOI: 10.23919/EUSIPCO.2018.8553284

Das, A., Galdi, C., Han, H., Ramachandra, R., Dugelay, J.-L. et al. (2018) Recent Advances in Biometric Technology for Mobile Devices. In: Proceedings of the *9th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS'18)*, Oct 2018, Los Angeles, United States.

Das, A., Pal, U., Blumenstein, M., & Ferrer Ballester, M. A. (2013) Sclera Recognition - A Survey. In: *2nd IAPR Asian Conference on Pattern Recognition (ACPR)*, IEEE, 917—921.

Daugman, J. (2006) Probing the uniqueness and randomness of Iris Codes: Results from 200 billion iris pair comparisons, in: *Proc. of the IEEE*, vol. 94 (11), 1927—1935.

Galbally, J., Haraksim R. and Beslay, L. A study of age and ageing in fingerprint biometrics (2018) IEEE Trans. on Information Forensics and Security. PP(99):1-1 DOI: 10.1109/TIFS.2018.2878160.

German, R. and Barber, S. (2017) Current Biometric Adoption and Trends. UT CID Report #18-02, Center for Identity, University of Texas, Austin, United States of America.

Hanvit, K., et al. (2018) A Wearable Wrist Band-Type System for Multimodal Biometrics Integrated with Multispectral Skin Photomatrix and Electrocardiogram Sensors, *Sensors*, 18 (2738).

Hoepman, J.-H. (2018) Making Privacy By Design Concrete. In: *European Cyber Security Perspectives*, 26-28, KPN CISO Office, The Hague, The Netherlands.

Hulsebosch, R.J. and Ebben, P.W. (2008). Enhancing Face Recognition with Location Information. In: *Third International Conference on Availability, Reliability and Security*, 397-403.

Jain, A.K. and Kumar, A. (2012). Biometrics Recognition: an Overview. In: *Second Generation Biometrics*, Springer, 49-79.

Jorgensen, Z. and Yu, T. (2011) On Mouse Dynamics as a Behavioral Biometric for Authentication. *In: Proc. ASIACCS '11*, ACM.

Kindt, E. (2019) A legal perspective on the relevance of biometric presentation attack detection (PAD) for payment services under PSDII and the GDPR. *Handbook of Biometric Anti-Spoofing – Presentation Attack*, Second edition, Advances in Computer Vision and Pattern Recognition, Springer, 81 – 501.

Komulainen J., Boulkenafet Z., Akhtar Z. (2019) *Review of Face Presentation Attack Detection Competitions.* In: Marcel S., Nixon M., Fierrez J., Evans N. (eds) Handbook of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-92627-8_14.

Korus, P. and Memon, N.D. (2019) *Content Authentication for Neural Imaging Pipelines: End-to-end Optimization of Photo Provenance in Complex Distribution Channels*. Computer Vision and Pattern Recognition.

Liu, J. et al. (2009) uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications *In: Proc. Pervasive Computing and Communications*, 10.1109/PERCOM.2009.4912759.

Marcel, S., Nixon, M.S., Fierrez, J. and Evans, N. W.D. (2019) Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, Advances in Computer Vision and Pattern Recognition, Second Edition. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-92627-8.

Hernandez-Ortega J., Fierrez J., Morales A., Galbally J. (2019) *Introduction to Face Presentation Attack Detection*. In: Marcel S., Nixon M., Fierrez J., Evans N. (eds) Handbook of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-92627-8_9.

Parihar, R.S. and Jain, S. Palm (2019) Vein Recognition System for Human Authentication: A Review. *Int. Journal for Research in Applied Science & Engineering Technology*, 7(2), 472-477.

Sabhanayagam, T., V. Prasanna Venkatesan, and K. Senthamaraikannan. (2018) A Comprehensive Survey on Various Biometric Systems. *International Journal of Applied Engineering Research,* 13 (5), 2276-2297.

Singh, Yogendra Narain and Singh, S. K. (2012) Evaluation of Electrocadriogram for Biometric Authentication, *Journal of Information Security*, 3 (1), 39—48. DOI: 10.4236/jis.2012.31005

Spreeuwers, L. , Veldhuis, R. N. J., & Schils, M. (2018) Towards Robust Evaluation of Face Morphing Detection. In *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 1027-1031.

Spreeuwers, L. (2017) De-Duplication Using Automated Face Recognition: A Mathematical Model and All Babies Are Equally Cute. In *International Conference of the Biometrics Special Interest Group (BIOSIG 2017).*

Tolosana R., Vera-Rodriguez R., Fierrez J., Ortega-Garcia J. (2019) *Presentation Attacks in Signature Biometrics: Types and Introduction to Attack Detection.* In: Marcel S., Nixon M., Fierrez J., Evans N. (eds) Handbook of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition. Springer, Cham. DOI: 10.1007/978-3-319-92627-8_19

Wang, Zhifang, et al. (2011) Multimodal Biometric System Using Face-Iris Fusion Feature. *Journal of Computers*, 6 (5) 931–938.

Wójtowicz, A., and Joachimiak, K. (2016) Model for adaptable context-based biometric authentication for mobile devices, Personal and Ubiquitous Computing 20 (2), 195-207. DOI: 10.1007/s00779-016-0905-0.

Yoon, S., Jain, A.K. (2015) Longitudinal study of fingerprint recognition. Proceedings of the National Academy of Sciences 112 (28), 8555-8560; DOI: 10.1073/pnas.1410272112.

Bijlage 1 Lijst met geïnterviewde organisaties

AEGON

Rijksdienst voor Identiteitsgegevens (RvIG)

ING Bank

Datamanagement en Biometrie (DMB), Universiteit Twente

GenKey

Expertisecentrum Identiteitsfraude en Documenten (ECID), Koninklijke Marechaussee (KMar), Ministerie van Defentie (Min.Def)

Ministerie van Justitie en Veiligheid (Min.JenV)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Min. BZK)

Immigratie- en Naturalisatiedienst (IND)

Justitiële Informatiedienst

Bijlage 2 Begeleidingscommissie en klankbordgroep

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Min.BZK)

Rijksdienst voor Identiteitsgegevens (RvIG)

Koninklijke Marechaussee (KMar), Ministerie van Defentie (Min.Def)

Ministerie van Justitie en Veiligheid (Min.JenV)

RDW

Immigratie- en Naturalisatiedienst (IND)

Justitiële Informatiedienst

Nederlandse Vereniging voor Burgerzaken (NVVB)

Vereniging van Nederlandse Gemeenten (VNG)