Biometrie voor Sterke Authenticatie

Een State-of-the-Art scan

Project	:	P3 – Geïntegreerde Federatieve e-Infrastructuur
Project jaar	:	2015
Project manager	:	Michiel Schok
Auteur(s)	:	Arnout van Velzen, Martijn Oostdijk, Maarten Wegdam (InnoValor)
Reviewer(s)	:	Joost van Dijk, Arnout Terpstra (SURFnet), Bob Hulsebosch (InnoValor)
Datum	:	14 Januari 2016
Versie	:	1.0

Samenvatting

Dit rapport beschrijft een state-of-the-art analyse naar biometrie met een focus op biometrische authenticatie binnen SURFconext Sterke Authenticatie. Via desktoponderzoek en een expertsessie is een lijst van veelbelovende technologieën samengesteld die op basis van een vijftal criteria beoordeeld is. Naast prestatie van de technologieën is ook gekeken naar veiligheid/privacy, universaliteit, gebruiksgemak en geschiktheid voor SURFnet en haar achterban. Vingerafdruk en oogaderherkenning met behulp van beschikbare sensoren op smartphones zijn voor de hand liggende oplossingen. Alternatieve oplossingen worden beschreven. Een aantal oplossingen valt af omdat speciale hardware nodig is, of omdat de oplossing een continuous authentication karakter heeft waardoor deze niet goed past in een federatieve context.

COLOPHON

Programme line	:	P3 – Geïntegreerde Federatieve e-Infrastructuur – Project Trust & Identity
Part	:	Work Package 1 – Next Generation Trust & Identity
Activity	:	Sterke Authenticatie
Deliverable	:	03.01.01.15 – Verkenning Biometrische Authenticatie
Access rights	:	Publiek
External party	:	InnoValor

This project was made possible by the support of SURF, the collaborative organisation for higher education institutes and research institutes aimed at breakthrough innovations in ICT. More information on SURF is available on the website http://www.surf.nl.

MANAGEMENTSAMENVATTING

Biometrie belooft al geruime tijd om authenticatie veiliger en makkelijker te maken. Tot nu toe is deze belofte nog niet ingelost. De voordelen van biometrische authenticatie (“iets wat je bent”), wanneer ze vergeleken worden met de meer traditionele vormen van authenticatie (“iets wat je weet”, “iets wat je hebt”), zijn helder. Maar in de praktijk blijkt het wachtwoord toch nog steeds de meest gebruikte authenticatieoplossing te zijn. Daar lijkt langzaam maar zeker verandering in te komen:

- Multi-factor authenticatie is al geruime tijd met een opmars bezig, getuige bijvoorbeeld de oplossingen van de banken voor elektronisch bankieren, authenticatieapps op smartphone (Google Authenticator, tiqr), en SURFconext Sterke Authenticatie.
- Sensoren voor biometrische authenticatie worden steeds vaker geïntegreerd in smartphones: Apple’s Touch Id is het belangrijke voorbeeld.

Dit rapport beschrijft een state-of-the-art analyse naar biometrie. Via desktoponderzoek is een lijst van veelbelovende technologieën samengesteld die op basis van een vijftal criteria teruggebracht is tot een shortlist van technologieën die beschreven staan in dit rapport. In een expert sessie met SURFnet en externe biometrieexperts zijn deze bevindingen bediscussieerd en gevalideerd.

De shortlist bevat zowel traditionele als nieuwe middelen die gebruik maken van fysiologische maar ook van gedragsvormen van biometrie. Deze technologieën zijn: *Vingerafdruk*, *Irisscan*, *Netvliesscan*, *Vingeraderpatronen*, *Oogaderpatronen*, *Gezichtsherkenning*, *Hartslagherkenning*, *Sprekerherkenning*, *Handtekening*, *Gebruikersinteractie* en *Gebarenherkenning*.

De criteria waar de technologieën op beoordeeld werden zijn: *Prestatie*, *Veiligheid*, *Universaliteit*, *Gebruiksgemak* en *Geschiktheid voor SURFnet*. Prestatie is vanuit de wetenschappelijke analyse van biometrie van oudsher het belangrijkste criterium en wordt uitgedrukt in False Acceptance Rate, False Rejection Rate, etc. Maar dit is niet het enige criterium dat van belang is. Bovendien is het tegenwoordig vaak lastiger om dit criterium onafhankelijk te kunnen beoordelen (o.a. doordat sensors ingebed in secure hardware in smartphones geleverd worden). Veiligheid gaat met name over de mogelijkheden voor een aanvaller om een biometrisch authenticatiemiddel voor de gek te houden, bijvoorbeeld met een dummy kenmerk, maar ook over de mogelijkheden tot het beschermen van de privacy van de gebruiker. Universaliteit wordt met name beïnvloed door de beschikbaarheid van geschikte sensoren in consumentenproducten (i.e. smartphones). Gebruiksgemak hangt af van hoe de biometrische technologie ervaren wordt door gebruikers. Hierbij is rekening gehouden met de “intrusiveness” van de technologie en bijvoorbeeld de snelheid tijdens enrollment en authenticatie. Geschiktheid voor SURFnet houdt in dat de biometrische technologie relatief eenvoudig in te passen moet zijn in een federatieve context en/of geschikt moet zijn voor de typische achterban van SURFnet (studenten, medewerkers in hoger onderwijs & onderzoek).

Na het toepassen van bovenstaande criteria op de short list van biometrische technologieën lijken de meest veelbelovende oplossingen te zijn:

- Vingerafdruk via een ingebouwde sensor of via de device camera is een veilige keuze bezien vanuit prestatie-, universaliteit- en gebruiksgemak standpunt. Wel is de vingerafdruk vanuit veiligheid bezien enigszins omstreden (men laat ze overal en nergens achter, en ze zijn met huis-, tuin- en keukenmiddelen na te bootsen).
- Oogaderherkenning lijkt mogelijk te zijn met een gewone device camera op smartphones. Nadeel is dat de prestaties hiervan niet helemaal onafhankelijk vastgesteld (de technologie is ook recenter dan vingerafdruk) en er lijkt een achterliggende leverancier te zijn die de technologie geoctrooieerd heeft.

Alternatieven zijn gezichtsherkenning (met een smartphone device camera) en sprekerherkenning (met een smartphone microfoon), maar deze technologieën zijn minder geschikt vanwege prestaties en/of gebruiksgemak.

De andere technologieën vallen af doordat ze slecht presteren, speciale hardware nodig hebben die nog niet universeel aanwezig is, of omdat ze gebruikt moeten worden in een continuous authentication scenario waardoor ze minder makkelijk in te zetten zijn in een federatie zoals SURFconext.

INHOUDSOPGAVE

1. INTRODUCTIE

Biometrie wordt vaak genoemd als mogelijkheid om authenticatiemethodes veiliger te maken. In de praktijk bleken de verwachtingen van biometrie als vervanging van wachtwoorden vaak iets te hooggespannen te zijn: het wachtwoord is al vele malen dood verklaard.

Maar: het gebruik van tweede factor authenticatie, zoals SMS en andere One Time Password authenticatiemiddelen, heeft recentelijk een vlucht genomen, met name voor grootschalige consumententoepassingen. Ook biometrie is de laatste jaren bezig met een opmars in het consumentendomein: denk bijvoorbeeld aan de vingerafdruklezer op nieuwe iPhones, gezichtsherkenning op Android toestellen en stemherkenning in de ING mobiel bankieren app.

Dankzij een aantal succesvolle innovatietrajecten van SURFnet (zie [11]) is het architectureel al prima mogelijk om authenticatie met meer geavanceerde authenticatiemiddelen toe te passen binnen SURFconext. De Sterke Authenticatie functionaliteit van SURFconext, waarbij de instellingsidentiteit, op basis van username/password (“something you know”), wordt uitgebreid met een extra authenticatiefactor (en de daarbij horende verificatie), is intussen al getest met smartphone- en hardwaretokens (“something you have”). Maar of dit op dezelfde manier ook kan werken met de huidige generatie van biometrische authenticatiemiddelen (“something you are”) is nog onduidelijk. Een biometrische tweede factor is mogelijk eenvoudiger voor gebruikers, breidt de keuze in middelen in SURFconext Sterke Authenticatie uit, is mogelijk meer betrouwbaar dan “something you have”, en voorziet in een expliciete vraag van de instellingen in SURFnet’s achterban. Daarnaast zijn er mogelijk andere toepassingen van biometrie voor SURFnet of haar achterban.

SURFnet overweegt op korte termijn een PoC of pilot uit te voeren met een biometrisch authenticatiemiddel binnen de context van de Sterke Authenticatie functionaliteit van SURFconext.

1.1. Doel en aanpak

Het primaire doel van dit onderzoek is om een state-of-the-art overzicht te geven van biometrische authenticatiemiddelen en hun geschiktheid voor toepassing door SURFnet en haar achterban te bepalen. De focus ligt hierbij op korte termijn (2016) toepassing binnen de Sterke Authenticatie functionaliteit van SURFconext, inclusief hoe de biometrische authenticatiemiddelen architectureel ingepast kunnen worden.

Een tweede doel is om de achterban van SURFnet te informeren over ontwikkelingen op het gebied van biometrische authenticatiemiddelen.

De aanpak bestond uit desktoponderzoek, aangevuld met een wisdom-of-the-crowd sessie waarbij ook externe biometrie experts (zie Appendix B) uitgenodigd waren.

2. ACHTERGROND

2.1. Biometrie

Biometrie verwijst naar metingen aan eigenschappen van het menselijk lichaam en gedrag. Deze eigenschappen zijn identificerend en worden daarom gebruikt voor het vaststellen van de identiteit van personen. Biometrie kan ook worden ingezet voor bijvoorbeeld medische of forensische doeleinden, maar dit rapport richt zich op de toepassingen binnen identiteitsmanagement. Hierbij wordt onderscheid gemaakt tussen het identificeren van onbekenden en het verifiëren van reeds bekende individuen tegen een database; dit rapport kijkt naar de laatste toepassing van biometrie. Vergeleken met andere vormen van authenticatie ("something you know", "something you have"), heeft biometrie belangrijke voordelen. Zo is een biometrisch kenmerk over het algemeen moeilijker te ontfutselen of kopiëren, beschikt bijna ieder individu al over geschikte kenmerken (wat distributie vereenvoudigt) en draagt een individu dit altijd bij zich (wat helpdesk kosten kan reduceren).

Identificerende biometrische kenmerken worden ook wel modi genoemd en kunnen *hard* (in hoge mate identificerend) of *soft* (in mindere mate identificerend) zijn, alsmede fysiologisch (gemeten aan het lichaam) of *behavioral* (gemeten aan gedrag). Multimodale biometrie combineert metingen van meer dan één kenmerk in biometrische toepassingen [14] [15].

Identiteitsverificatie verschilt, afhankelijk van het gekozen kenmerk, maar volgt grofweg de volgende stappen:

1. **Registratie:** bevestig de identiteit van het subject, bijvoorbeeld door controle van een paspoort of vragen om in te loggen met een wachtwoord en gebruikersnaam. Biometrische authenticatie is, net als elke credential voor authenticatie, slechts zo veilig als de rest van het verificatieproces.
2. **Enrolment:** maak een afdruk of opname van de biometrische eigenschap met behulp van sensors, bijvoorbeeld een foto voor gezichtsherkenning met een camera. Dit proces produceert een *template*, ofwel een afdruk of opname, welke in een database wordt opgeslagen.
3. **Authenticatie/verificatie:** wanneer iemand zich vervolgens moet authenticeren, wordt opnieuw een opname/afdruk afgenomen met behulp van een sensor en wordt deze vergeleken met de templates in de database. Wanneer de opname overeenkomt met een template in de database, is de identiteit bevestigd. Hierbij is het soms noodzakelijk te testen of het gepresenteerde kenmerk niet gesimuleerd is, bijvoorbeeld door *liveness* detectie. Ook kunnen bepaalde tresholds worden ingesteld voor de betrouwbaarheid waar een match aan moet voldoen. Hierbij moet de juiste balans tussen acceptabele betrouwbaarheid en privacy aspecten worden bewaakt. De opslag van een hoge resolutie oogscan van iemand met een oogziekte is bijvoorbeeld een verwerking van een bijzonder persoonsgegeven conform WBP Artikel 16 en derhalve verboden (Art 21).

De prestaties van een biometrische technologie kunnen worden uitgedrukt in kwantitatieve scores. Voor de enrolment fase kijkt men vaak naar de Failure to Enroll (FTE) maat, waarbij gemeten wordt welk deel van een populatie ge-enrolled kan worden. Voor de authenticatie fase zijn de voornaamste maten de False Acceptance Rate (FAR), en de False Rejection Rate (FRR)[1]. Ofwel: de risico's op onterechte toegang, respectievelijk onterechte afwijzing van toegang. Vaak kan de technologie geconfigureerd worden zodat de FAR en de FRR tegen elkaar uitgeruild kunnen worden. Zo kan de FAR worden vastgezet op basis van het accepteerbare risico op onterechte toelating, zodat gekeken kan worden of de corresponderende FRR vanuit gebruiksgemak acceptabel is.

Van sommige biometrische technologieën zijn dergelijke kwantitatieve scores experimenteel vastgesteld door de technologie los te laten op grote standaarddatabases. Dit is met name het geval voor vingerafdrukherkenning en gezichtsherkenning[2]. Maar veel leveranciers van biometrische technologieën bieden niet de mogelijkheid om zulke onafhankelijke tests uit te voeren, bijvoorbeeld omdat de sensor op een tamper-resistante manier in een smartphone ingebed is, en de matching algoritmen op een secure chip draaien.

Belangrijke uitdagingen voor biometrische authenticatie zijn beschadigingen of het ontbreken van de biometrische modus bij een aantal mensen, het veranderen van de biometrische eigenschap door veroudering, de invloed van de omgeving op sensors, de mogelijkheden voor het imiteren van een biometrisch kenmerk. Een ander risico is dwingen van toegangs-gerechtigden tot het 'lenen' van een template[3].

Een ander probleem met biometrie is dat het relatief privacygevoelig is. Biometrische authenticatie kan bijvoorbeeld onvoorziene medische condities of consequenties blootleggen, iemand ongewenst op afstand

[1] FAR en FRR worden ook wel met False Match Rate respectievelijk False Non Match Rate aangeduid.

[2] Zie http://www.nist.gov/itl/iad/ig/frgc.cfm, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf.

[3] Dit kan extreem ver gaan, zie bijvoorbeeld: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

identificeren, onveranderlijke informatie over personen verwerken (bijvoorbeeld ras), een hoge mate van herleidbaarheid creëren, of zelfs worden ervaren als een aantasting van de menselijke waardigheid. Een oplossingsrichting voor het privacyprobleem is het decentraal opslaan van templates, liefst zo dicht mogelijk bij de gebruiker zelf. Dit kan de vorm aannemen van een *tamper-resitant* apparaat (een smart card, bijvoorbeeld) waarbij dan ook nog het liefst de matching in dit apparaat gebeurt (zogenaamde "match-on-card"). Er zijn ook oplossingsrichtingen die het wel mogelijk maken om centrale opslag toch privacyvriendelijk te doen, bijvoorbeeld BioHash[4] van het Nederlandse bedrijf GenKey en het gebruik van gereduceerd opgeslagen vingerafdrukken voor de toegang tot een aantal universitaire sportcentra met DMS Solutions van DELCOM[5].

Bekende voorbeelden van biometrische authenticatie die grootschalig worden toegepast zijn vingerafdrukauthenticatie om smartphones te 'unlocken' en het gebruik van gezichtsherkenning voor grensbewaking. Een bijzondere toepassing van biometrische authenticatie is *continuous authentication*; het continu testen van een biometrisch kenmerk om voortdurend de identiteit te verifiëren. Vaak gebeurt dit door eerst het gedrag van de (authentieke) gebruiker over langere tijd te volgen. De online leeromgeving van Coursera past bijvoorbeeld analyse van typgedrag toe, om vast te stellen dat de gebruiker steeds dezelfde is als de persoon die is ingelogd. Een bijkomend voordeel van continuous authentication is dat verschillen in het kenmerk in de loop der tijd kunnen worden bemerkt, en het template automatisch kan worden bijgesteld; dit voorkomt dus re-enrolment.

Tijdens de enrollment fase worden templates opgeslagen. Hierbij kunnen privacy-enhancing technieken gebruikt worden. Vóór opslag is mogelijk dan nog bewerking nodig, bijvoorbeeld het verwijderen van ruis of het (onomkeerbaar) hashen van de template. Sensors voor het uitlezen van biometrische kenmerken zijn erg divers, en kunnen gangbare sensoren zijn, bijvoorbeeld een camera op een smartphone, of speciaal ontwikkeld voor biometrie, bijvoorbeeld een infraroodcamera op een dedicated device. De templates moeten zeer veilig worden opgeslagen en zijn soms gevoeliger dan andere authenticatiemiddelen; anders dan een wachtwoord kun je je vingerafdruk bijvoorbeeld niet wijzigen (al wordt gewerkt aan *cancelable biometrics* [13]). Een bekende methode voor templatebescherming is encryptie of het versleutelen van de data, e.g. BioHash van GenKey [18]. Wanneer een biometrisch kenmerk in de tijd zodanig is veranderd dat verificatie niet meer kan geschieden, dient een persoon opnieuw te worden enrolled.

Vanzelfsprekend is alle wet- en regelgeving ten aanzien van bescherming van persoonsgegevens van toepassing op biometrische authenticatie. In Nederland is dat met name de Wet Bescherming Persoonsgegevens, en de aangekondigde Europese Privacyverordening 95/46/EC. Voor de opslag en verwerking van biometrische gegevens gelden strenge regels, en worden afhankelijk van de modus aangemerkt als bijzondere persoonsgegevens. Wet- en regelgeving specifiek voor biometrie bevindt zich nog in een vroeg stadium van ontwikkeling. Er zijn al wel vroege initiatieven uit de Verenigde Staten die verdere wet- en regelgeving wel doen verwachten, zoals de Illinois Biometric Privacy Act en de Texas Business & Commerce Code Ann. § 503.001, waarin bijvoorbeeld staat dat moet worden gedocumenteerd hoe biometrische data wordt verkregen en restricties zijn opgenomen voor het verhandelen van biometrische data. Bovendien worden er forse boetes bepaald in het geval van het lekken van biometrische informatie. Daarnaast zijn er veel wettelijke verboden op het afnemen of delen van biometrische data, e.g. de staat New York verbiedt het afnemen van vingerafdrukken van werknemers, uitgesloten enkele uitzonderingen. Aan de andere kant is er ook veel wetgeving die sterke authenticatie vereist, zoals de Payment Services Directive II, waar biometrie een rol kan spelen als sterk authenticatiemiddel.

2.2. Standaarden

Er zijn verschillende technische standaarden die normen voorschrijven voor biometrische authenticatie. De belangrijkste zijn:

2.2.1. BIOAPI (ISO 19784, ISO 24708 EN ISO 24709)

Biometric Application Programming Interface (BioAPI) beschrijft de communicatie tussen verschillende modules of systemen in een biometrische toepassing op basis van het Biometric Interworking protocol (BIP). De architectuur van een softwaretoepassing die gebruik maakt van biometrische technologie met behulp van BioAPI wordt beschreven in ISO 19784. Uitwisseling van BIP-berichten wordt beschreven in ISO 24708. Helaas is de adoptie van de BioAPI standaard nog erg laag. ISO 24709 biedt een testraamwerk voor BioAPI.

2.2.1. ISO 19794 EN ISO 29109

ISO 19794 beschrijft uitwisselingsformaten voor biometrische data. Biometrische data als vingerafdrukken en foto's op paspoorten dienen hieraan te voldoen. ISO 19794 staat zowel formaten toe waarin biometrische kenmerken als ruwe plaatjes uitgewisseld worden, als formaten waarin specifieke kenmerken ("minutiae") uitgewisseld worden. ISO 29109 beschrijft een testraamwerk hiervoor.

[4] Zie http://www.genkey.com/en/technology/biohashr-sdk. Hierbij wordt slechts een hash van de biometrische template opgeslagen van waaruit het originele template niet te herleiden is, terwijl wel de match gedaan kan worden in het bereik van de hash functie.

[5] Zie http://dmssolutions.nl/.

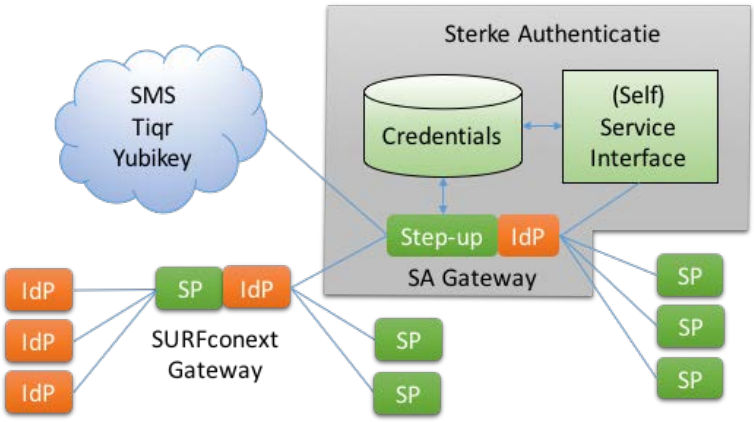
2.2.1. FIDO EN BOPS

De FIDO alliantie, een consortium van organisaties waaronder Paypal en Lenovo, heeft in 2013 FIDO (Fast Identity Online) geïntroduceerd. FIDO is een nieuwe authenticatiestandaard met een indrukwekkende lijst bedrijven die het steunen. FIDO moet het makkelijker gaan maken om niet alleen gebruikersnaam/wachtwoord te gebruiken voor authenticatie. Denk hierbij aan een losse USB token of de vingerafdruksensors van een smartphone, bijvoorbeeld betalen bij Paypal met de Samsung S5 vingersensor. Er zijn twee varianten van FIDO: U2F, om een authenticatiemiddel als tweede factor in te zetten, en UAF, voor het inzetten van een authenticatiemiddel als eerste factor. FIDO is een communicatieprotocol dat versleutelde communicatie voorschrijft tussen gebruikers, diensten en een FIDO server waar de sleutels veilig worden opgeslagen. In een typische implementatie van een biometrisch authenticatiemiddel op basis van FIDO (UAF) blijft de template op het apparaat dat gebruikt wordt, bijvoorbeeld de smartphone.

De Biometric Open Protocol Standard (BOPS), ontwikkeld 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 FIDO.

2.3. Sterke Authenticatie in SURFconext

Sterke authenticatie is op modulaire wijze ingebouwd in SURFconext [11]. Het Sterke Authenticatie bouwblok (“SA Gateway”, in Figuur 1) kan zich zowel voordoen als Identity Provider (IdP) als als Service Provider (SP). Een gebruiker die toegang wenst tot een gevoelige dienst bij een SP binnen SURFconext wordt, na wachtwoord gebaseerde eerste-factor authenticatie bij de instelling-IdP doorgeleid naar de SA Gateway voor sterke tweede factor authenticatie. SURFconext biedt op deze manier de mogelijkheid aan instellingen om centraal gebruik te maken van “cloud” authenticatieoplossingen die door derde partijen (denk bijvoorbeeld aan SMS, tiqr of Yubikey) worden aangeboden.



Figuur 1: SURFConext Sterke Authenticatie

Een biometrisch authenticatiemiddel is in theorie op vergelijkbare wijze in te passen in deze architectuur.

Het daadwerkelijke authenticeren (het matchen van een live capture tegen een opgeslagen template) vindt dan niet op een server bij SURFnet plaats, maar op een authenticatieserver van de leverancier, lokaal bij de gebruiker op een apparaat (bijvoorbeeld een smartphone), of – eventueel – bij de instellings-IdP.

Bij enrolment van een biometrisch authenticatiemiddel is het van belang dat de gebruiker bij de Registration Authority (RA) in eigen persoon verschijnt en dat de RA kan controleren dat de biometrische eigenschappen van de daadwerkelijke gebruiker worden ge-enrolled. De RA moet dus, bijvoorbeeld, kunnen controleren dat de gebruiker niet een nep-vingerafdruk over de eigen vinger heeft.

Het centraal opslaan van templates op de SA Gateway is niet een voor de hand liggende stap vanwege de privacy en security implicaties voor SURFnet. Immers, deze templates moeten erg veilig opgeslagen worden met technische en procedurele maatregelen om misbruik te voorkomen.

Standaarden zoals FIDO en BOPS lijken hier goed bij aan te sluiten: biometrische authenticatiemiddelen worden in deze opkomende standaarden beschouwd als alle andere authenticatiemiddelen. In FIDO ontsluit een biometrisch template eigenlijk een private sleutel die typisch opgeslagen is op een smartphone. De afhankelijke partij (in dit geval kan dit de SA Gateway zijn) beschikt over de corresponderende publieke sleutel. In dit geval bevat de credentials store (zie Figuur 1) van SURFconext Sterke Authenticatie dus gewone certificaten. In feite zijn FIDO en BOPS dus biometrie-agnostisch[6].

[6] Alhoewel BOPS versie 2 (in voorbereiding) ook toe lijkt te staan dat templates deels op de server worden opgeslagen.

Een nadeel van het opslaan van het biometrische kenmerk op een smartphone, of ander apparaat van de gebruiker, is wel dat er typisch opnieuw ge-enrolled moet worden als de gebruiker dit apparaat verliest of op een andere manier van apparaat wisselt.

Middelen die het gedrag van gebruikers tijdens het afnemen van de dienst moeten meten (“continuous authentication”, bijvoorbeeld het meten van karakteristieken van toetsenbordaanslagen) vereisen een embedding in de SP. Dit past echter niet in een federatieve identiteitsoplossing zoals SURFconext, waar de SP en IdP verschillende partijen zijn. Het heeft ook verdere privacyimplicaties dan wanneer biometrie slechts kort wordt gebruikt bij inloggen. In andere sectoren, zoals de financiële sector en in de enterprise wereld, wordt deze vorm van biometrie wel gebruikt.

3. CRITERIA

Op basis van literatuur en overleggen met SURFnet zijn een aantal criteria voor een biometrische tweede factor voor SURFconext Sterke Authenticatie opgesteld. Het is belangrijk dat deze criteria goed kunnen worden gemeten: er moet data beschikbaar zijn zodanig dat de criteria getoetst kunnen worden. Dat geldt met name voor het criterium “prestatie”: aanbieders moeten transparant zijn over of onafhankelijk beoordeeld zijn of kunnen worden op de prestatie van hun biometrische oplossingen. In het geval dat de prestatie van een modus over het algemeen slecht te testen is, scoort deze dus alsnog lager op prestatie in de beoordeling.

Deze criteria zijn bedoeld als een generieke schatting per biometrische modus; veel hangt af van de uiteindelijke toepassing. Desalniettemin is een dergelijke ruwe schatting zinvol om een eerste selectie te kunnen maken in geschikte middelen. Let op, “geschiktheid” in onderstaand overzicht is niet de optelsom van voorgaande criteria, maar verwijst naar de geschiktheid voor SURFconext Sterke Authenticatie. Een middel kan dus goed scoren op de eerste vier criteria, en toch niet geschikt zijn, bijvoorbeeld omdat die oplossing te kostbaar is of niet schaalbaar. Tenslotte moet elke oplossing voldoen aan normen, wet- en regelgeving, en bestaan hierin verschillen tussen de modi, maar dit is voor de eerste selectie niet onderscheidend.

Symbool	Criterium	Definitie	Uitleg
	Prestatie	Hoe presteert de biometrische factor of applicatie in kwantitatieve scores.	• FAR: false acceptance rate • FRR: false rejection rate • Meetbaarheid
	Veiligheid	Hoe veilig is deze biometrische modus voor authenticatie.	• Bescherming tegen onrechtmatige toegang • Mogelijkheden voor omzeilen
	Universaliteit	In hoeverre deze biometrische modus universeel inzetbaar is.	• Beschikbaarheid sensors, bijv. op smartphone, 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 identiteitsverificatie.	• Complexiteit en effort • Hoe intrusive deze oplossing is
	Geschiktheid	Leent zich voor SURFconext sterke authenticatie.	• Geschikt voor achterban • Geschikt voor authenticatie/2 factor authenticatie • Schaalbaarheid • Gunstige business case • Volwassenheid van de technologie • Volwassenheid van de markt

Legenda kleurcodes

 : goed

 : matig

 : onvoldoende

4. SHORTLIST

Er is op basis van desktoponderzoek een shortlist gemaakt van biometrische modi, en deze lijst is getoetst door externe experts. Zie Appendix A voor de longlist van alle modi die zijn meegenomen in onderliggend onderzoek.

De tabel hierover bevat een overzicht van de shortlist (in willekeurige volgorde), deze worden in aparte secties verder uitgelegd.

Biometrische modus	**Uitleg**
Vingerafdruk	De vingerafdruk kan op verschillende manieren worden afgenomen en steeds meer smartphones beschikken over een vingerafdruksensor. 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.
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.
Sprekerherkenning	Sprekerherkenning (wie spreekt), niet te verwarren met spraakherkenning (wat wordt er gezegd), is ook geschikt voor biometrische authenticatie. Dit is echter 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.

4.1. Vingerafdruk

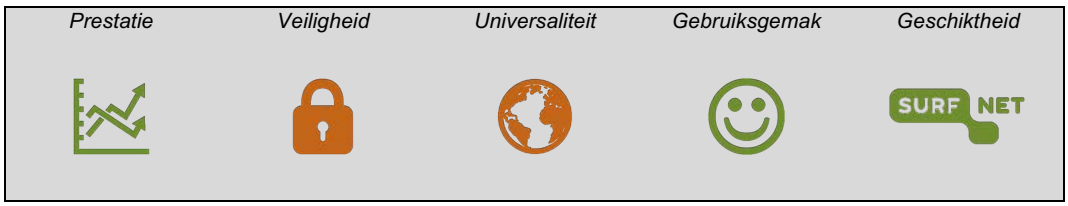
Huidpapillen op de oppervlakte van de vingers vormen afdrukken van papillaire lijnen, beter bekend als vingerafdrukken. Deze patronen zijn identificerend en blijven relatief ongewijzigd tijdens het ouder worden. Vingerafdrukken kunnen voor forensische opsporingsdoeleinden gebruikt worden, maar ook voor identificatie- en authenticatiedoeleinden. Typisch worden hiervoor de uiterste vingerkootjes benut. Ook meerdere vingers zijn mogelijk.

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 komt 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 fingerprint reader zal hebben[7]. Qualcomm heeft zelfs een fingerprint 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[8]. Hoyos Labs heeft een oplossing die vier vingers gelijktijdig scant met de gewone smartphone camera[9], gebruik makend van de flitser. Volgens een onderzoek van IHS[10] 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 apps die vingerafdrukken ondersteunen.

Qua universaliteit scoort vingerafdruk nog niet heel hoog, maar dit zal in de nabije toekomst waarschijnlijk verbeteren, mede door integratie in smartphones en door standaardisatie in bijvoorbeeld FIDO. Dit maakt deze technologie geschikt voor een pilot met de achterban van SURFnet.

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.

Een uitdaging is dat de sensor in veel gevallen gevoelig is voor vocht en vuiligheid. 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[11]. Liveness detectie blijkt moeilijk met gangbare sensoren, dit zorgt ervoor dat de technologie op veiligheid slechts gemiddeld scoort.



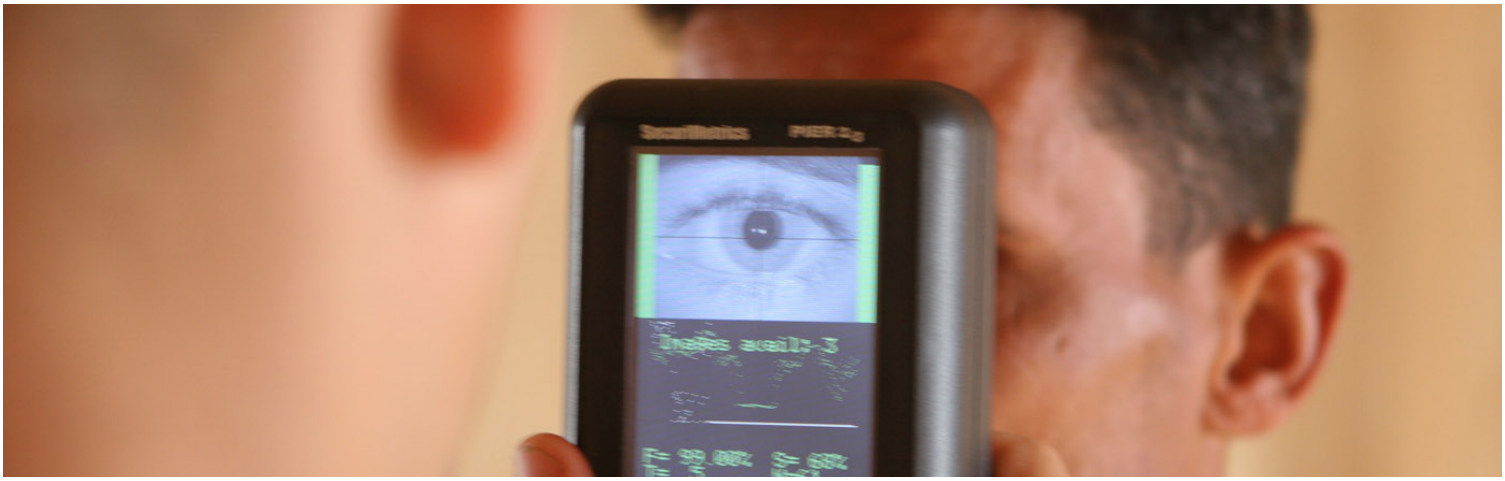
[7] Zie http://paymentweek.com/2015-6-17-a-billion-fingerprint-readers-in-mobile-devices-by-2021-7494/.

[8] Zie http://www.theverge.com/2015/3/2/8130505/qualcomm-snapdragon-sense-id-fingerprint-sensor-announced.

[9] Zie http://www.prnewswire.com/news-releases/hoyos-labs-to-demonstrate-new-four-finger-technology-at-biometrics-2015-in-london-300157675.html.

[10] Zie http://www.forbes.com/sites/aarontilley/2014/10/10/fingerprint-sensor-market-growth-2020/.

[11] Zie http://www.dailymail.co.uk/sciencetech/article-2889860/Hackers-steal-fingerprint-PHOTO-Copycat-print-used-criminals-fool-security-systems.html.



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.

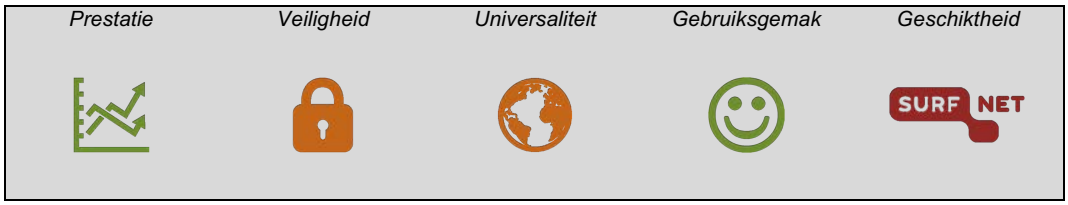
Er wordt gebruik gemaakt van een camera om gedetailleerde opnamen te maken van de structuur van de iris. Deze worden als digitale templates opgeslagen en bij identificatie weer gebruikt om te matchen. Vrijwel alle irisherkenningssystemen maken opnamen van de iris onder belichting met een nabij infrarood 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 donderbruine 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. Dit zorgt ervoor dat de technologie op universaliteit en geschiktheid voor SURFnet laag scoort.

De irisscan wordt onder andere gebruikt voor paspoortloze grensbewaking, 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 nog alleen in Japan. Er gaan geruchten dat LG en Samsung spoedig deze technologie in hun smartphones aanbieden[12].

De technologie presteert goed en werkt snel [4], het prestatie criterium is daarom groen. 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[13].

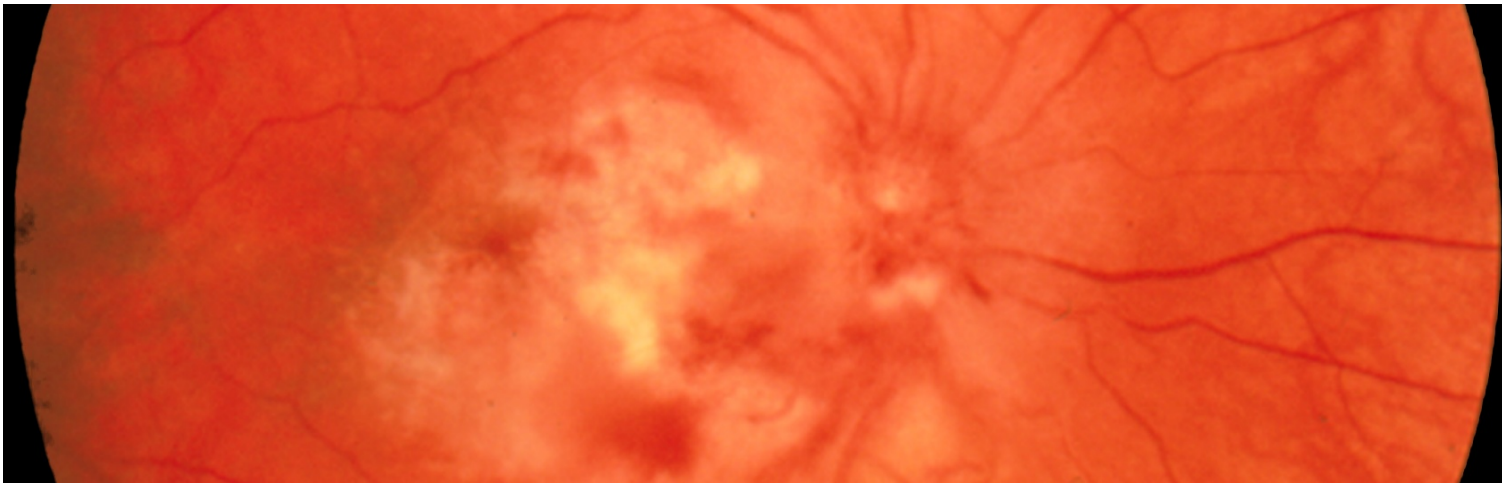
Het voornaamste risico, buiten slechte foto's door gebrekkige opnameprocessen of techniek, is spoofing met behulp van hoge resolutie foto's[14] of zelfs lenzen met een valse iris. Dit zorgt ervoor dat de technologie op veiligheid slechts oranje scoort. Een vorm van liveness detectie is dus raadzaam, bijvoorbeeld door de iris te laten bewegen door veranderingen in het omgevingslicht.



[12] Zie http://www.phonearena.com/news/Samsung-Galaxy-S7-and-LG-G5-rumored-to-come-with-iris-scanning-authentication_id70581.

[13] Zie https://en.wikipedia.org/wiki/Iris_recognition.

[14] Dat iris informatie afgelezen kan worden uit hoge resolutie foto's wordt geïllustreerd door John Daugman aan de hand van het verhaal van het Afghaanse meisje van de National Geographic cover, zie http://www.cl.cam.ac.uk/~jgd1000/afghan.html en http://ngm.nationalgeographic.com/2002/04/afghan-girl/index-text.



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.

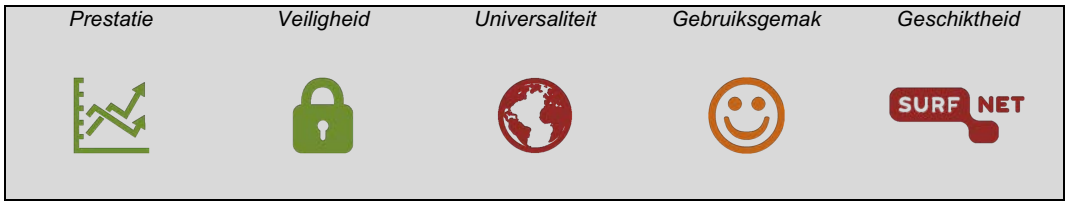
Hoewel bloedvatpatronen in het netvlies kunnen wijzigen door aandoeningen als diabetes en staar, blijft het netvlies normaal gesproken ongewijzigd gedurende eenieders leven. Door de unieke en onveranderlijke aard van het netvlies is het een zeer betrouwbaar biometrisch kenmerk wat qua performance te 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 van schrijven nog geen commerciële smartphones die deze technologie bevatten. Wel is er een interessant open source project uit Nieuw Zeeland dat met additionele hardware smartphones in staat stelt het netvlies te scannen[15]. PCMag beweert dat de Chinese telefoon ontwikkelaar ZTE netvliesscanning-technologie in een smartphone aanbiedt[16], maar dit blijkt in werkelijkheid oogaderpatroonherkenning (zie 4.5) te zijn[17]. Op universaliteit en geschiktheid voor SURFnet 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.



[15] Zie http://www.medgadget.com/2015/05/worlds-first-open-source-smartphone-retinal-camera.html.

[16] Zie http://www.pcmag.com/article2/0,2817,2477800,00.asp.

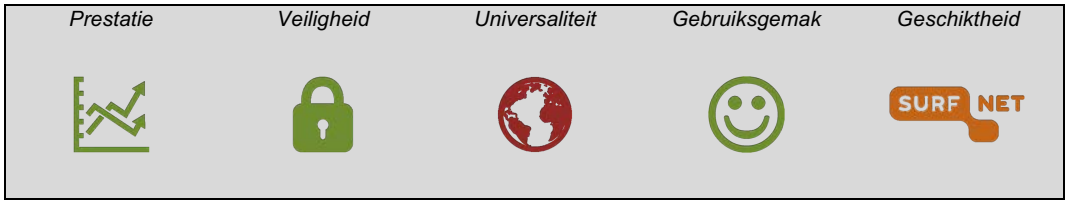
[17] Zie http://webcusp.com/list-of-all-eye-scanner-iris-retina-recognition-smartphones/.

4.4. Vingeraderpatronen

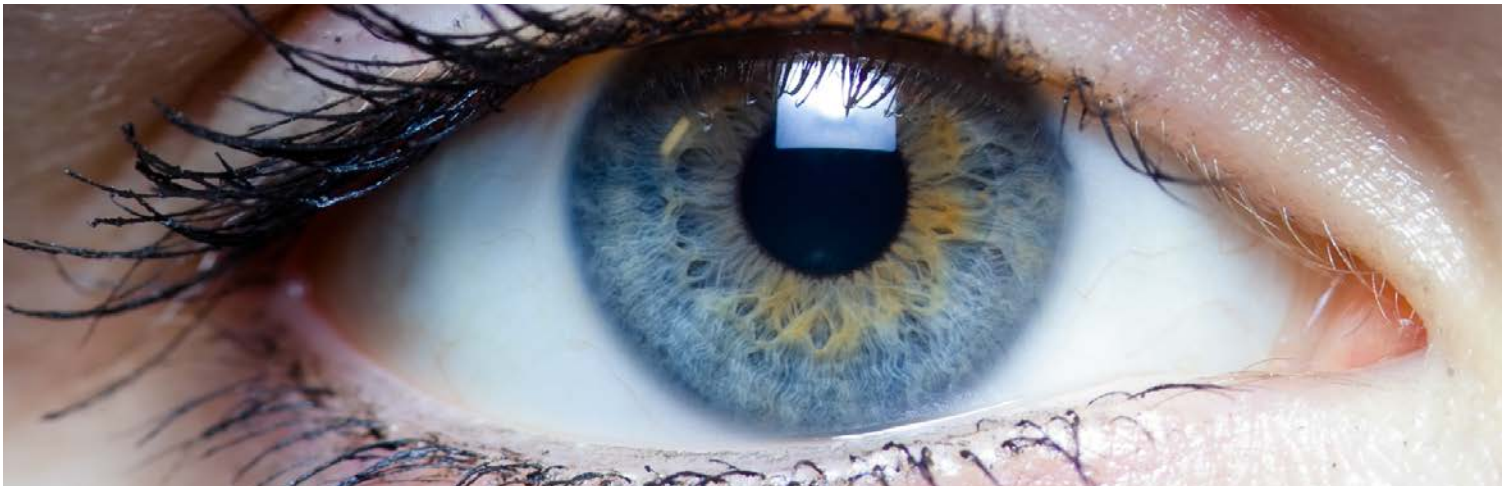
Aderpatroonherkenning voor biometrische authenticatie maakt gebruik van patronen van bloedvaten in bij voorkeur de vinger, maar is ook mogelijk met de handpalm, pols, achterkant van de hand, of elders in het lichaam. Bloedvatpatronen zijn uniek identificerend. Hierbij wordt Near Infrared (NIR) licht op de vinger geschenen. De bloedvaten absorberen het infrarode licht, waardoor zij donkere lijnen nalaten op een foto. Van de foto wordt een biometische template gemaakt voor matching. Authenticatie kan binnen 2 seconden 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[18]. 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. Helaas zijn er nog geen non-dedicated devices zoals smartphones die vingeraderherkenning ondersteunen. Buiten het ontbreken van vingers en enkele zeldzame aandoeningen, beschikt vrijwel iedereen over vingeraders.



[18] Zie http://www.theguardian.com/business/2014/sep/05/barclays-introduce-finger-vein-id-readers.



4.5. 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 [3]. 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[19] heeft een patent op deze technologie. EyeVerify biedt softwaretoepassingen voor oogaderherkenning en wordt al door een wijde range aan smartphones ondersteund, inclusief de meeste Samsung en Apple toestellen. EyeVerify biedt ook een SDK en lijkt te partneren met Chinese smartphone fabrikanten ZTE en Vivo[20].

Er zijn een tweetal studies gedaan naar de technologie van EyeVerify[21] welke aangeven dat de implementatie van oogaderpatroonherkenning goed presteert. Deze onderzoeken zijn echter wel in opdracht van EyeVerify uitgevoerd. De technologie 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.

Prestatie	*Veiligheid*	*Universaliteit*	*Gebruiksgemak*	*Geschiktheid*
				

[19] Zie http://www.eyeverify.com/.

[20] Zie http://webcusp.com/list-of-all-eye-scanner-iris-retina-recognition-smartphones/.

[21] Zie http://www.eyeverify.com/independent-accuracy-studies.

4.6. Gezichtsherkenning

Voor gezichtsherkenning worden foto of video-opnamen gemaakt van het gelaat tijdens enrolment en matching. Er zijn verschillende algoritmische aanpakken mogelijk, waaronder eigenface analyse, lineaire discriminante analyse en Hidden Markov modellen. Relatief nieuw is om het gelaat in 3D te modelleren[22]. Gewone camera's kunnen voor gezichtsherkenning worden gebruikt, maar er zijn ook gezichtsherkenning-toepassingen op basis van infrarood thermografische opnamen.

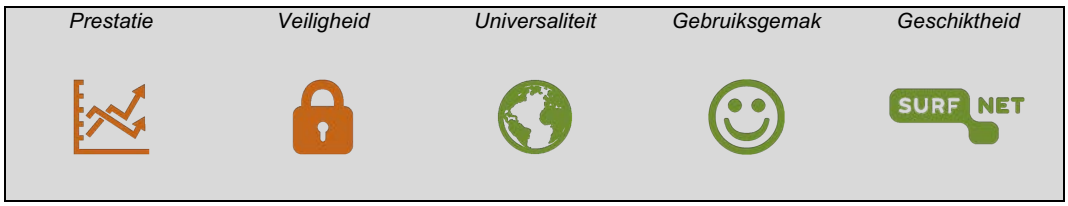
Gezichtsherkenning wordt als biometrisch kenmerk ingezet voor forensische doeleinden, identificatie bij grenscontrole of face-in-the-crowd herkenning. Andere toepassingen zijn identificatie bij geldautomaten, aanwezigheidscontrole op de werkvloer of foto applicaties die mensen herkennen en taggen (waaronder 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"[23] aan. Android telefoons beschikken over Face Unlock, dat met cumulatieve template-opslag en liveness detectie kan worden versterkt door de gebruiker.

Er is een zeer volwassen markt voor gezichtsherkenning-toepassingen. Een rapport van Tractica 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[24]. 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, IdChecker 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 is dat het ook passief kan worden afgenomen. Het is gevoelig voor verschillen als gezichtsuitdrukking of de hoek waaronder de foto wordt genomen, alsmede omgevingsfactoren als belichting. Er zijn ISO standaarden (zie Sectie 2.2.1) 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. Gezichtsherkenning is ook meer privacygevoelig dan bijvoorbeeld een vingerafdruk, omdat een foto veel zegt over zaken als etniciteit en leeftijd.



[22] Zie http://findbiometrics.com/facialnetwork-3d-facial-recognition-27102/.

[23] Zie https://selfiepay.co/ resp. http://www.cnbc.com/2015/03/15/alibaba-teases-new-face-recognition-tool-for-mobile-pay.html.

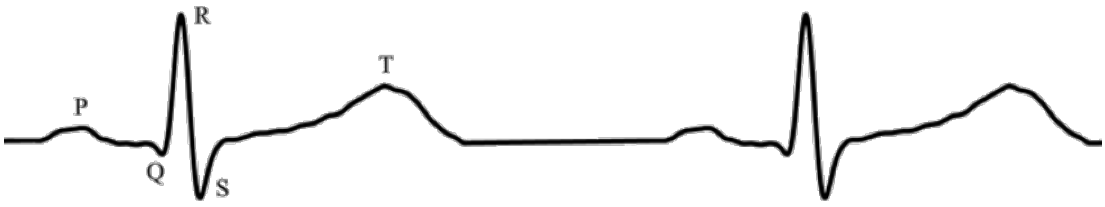
[24] Zie http://www.cheatsheet.com/gear-style/when-will-your-smartphone-have-facial-recognition.html/?a=viewall.

4.7. 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.

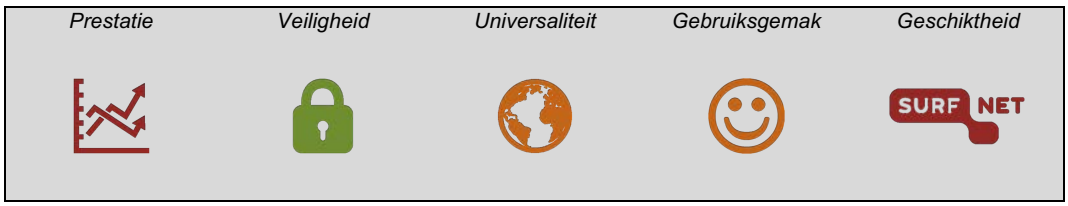
Veel smartphones beschikken al over een hartslagmeter, daarnaast zijn er veel wearables zoals smartwatches en fitness trackers die het hartritme meten. Voorbeelden zijn Samsung en Apple smartphones, AliveCor Mobile ECG en het Fitbit fitness tracker. Het meten van de eigen hartslag, onder andere voor gezondheidsredenen, is een trend: in 2018 zal naar verwachting een derde van alle Amerikanen geregeld een hartslagmeter op zich dragen[25]. En wanneer iemand de hartslagmeter nog niet om heeft, duurt het enkele seconden (~10) voor de meting is verricht. 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[26]. Een vergelijkbaar product is Olea's Heart Signature[27].

Wearables en smartphones met geschikte sensor zijn nog niet voldoende beschikbaar om de technologie op universaliteit op groen te zetten, voorlopig blijft deze oranje.



Helaas lijken de prestaties van ECG tegen te vallen[28]. Singh en Singh [16] noemen de performance "moderate" en 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[29].



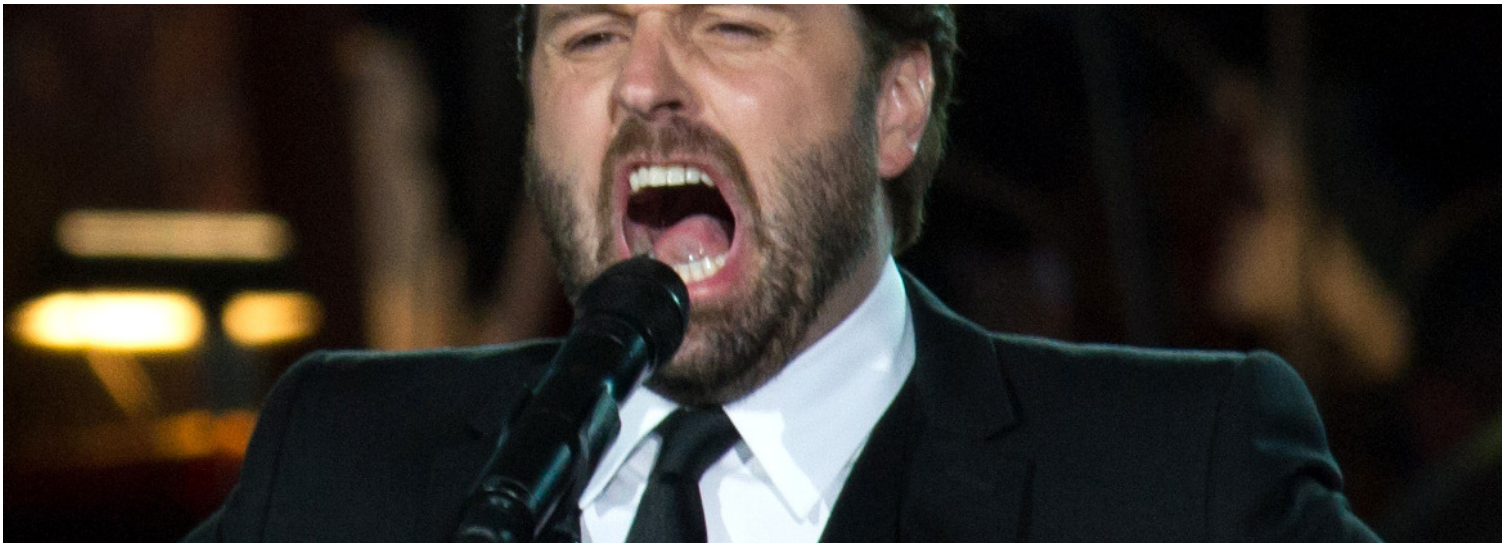
[25] Zie http://www.hrsonline.org/News/Press-Releases/20154/05/ECG-On-Smartphones.

[26] Zie http://www.theguardian.com/technology/2015/mar/13/halifax-trials-heartbeat-id-technology-for-online-banking.

[27] Zie http://www.biometricupdate.com/201506/olea-introduces-continuous-heart-pattern-authentication-solution.

[28] Zie http://www.physionet.org/pn3/ecgiddb/biometric.shtml.

[29] Zie http://www.vitalsignscamera.com/.



4.8. Sprekerherkenning

Sprekerherkenning, i.e. wie spreekt, moet niet worden verward met spraakherkenning, i.e. 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 identiteitsverificatie. Net als gezichtsherkenning kan sprekerherkenning ongemerkt worden gedaan door afluisteren.

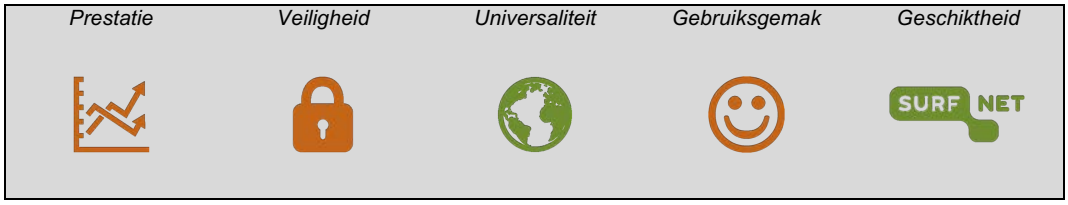
Tijdens het enrolment proces wordt de stem van de spreker opgenomen, van waaruit een aantal kenmerken worden omgezet in een voiceprint. Gedurende de verificatie wordt een spraaksample (“utterance”) vergeleken met voice prints in de database. Hiervan bestaan twee categorieën: tekstafhankelijk en tekstonafhankelijk. Wanneer de tekst tijdens verificatie dezelfde moet zijn als tijdens enrolment, betreft het 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 identificatie dan voor verificatie, 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 gebruikt sprekerherkenning voor toegang tot hun app[30].

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[31].

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



[30] Zie http://www.emerce.nl/nieuws/honderdduizend-ingklanten-praten-tegen-bankapp.

[31] Zie http://www.biometricupdate.com/201506/voice-and-speech-recognition-software-market-to-reach-5-1b-by-2024-tractica-report.

4.9. Handtekening

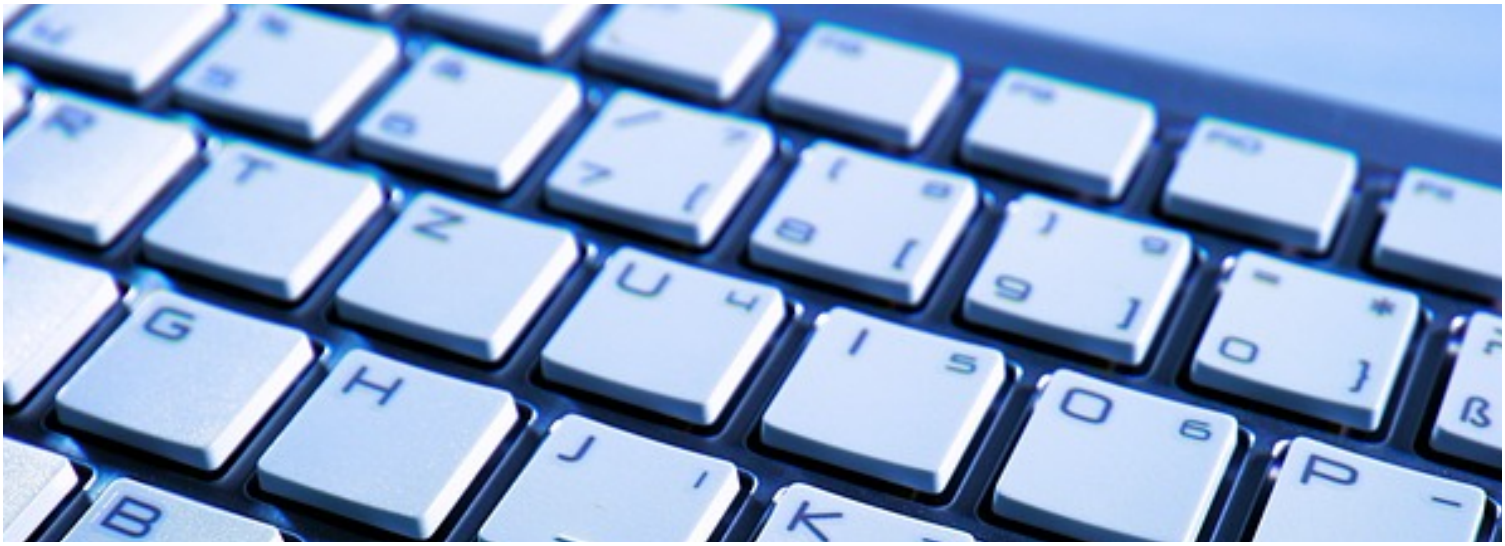
Het handschrift is relatief uniek voor elk individu en wordt daarom steeds populairder voor authenticatietoepassingen. Veel systemen maken gebruik van driedimensionale analyse van een handschriftsample waarbij de vorm en druk van het schrift worden beschouwd. Handschriftanalyse kan zowel dynamisch (online, 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 ("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 touch screen 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, blijft het nadoen van iemands handtekening erg 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 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[32].

Prestatie	*Veiligheid*	*Universaliteit*	*Gebruiksgemak*	*Geschiktheid*
				

[32] Zie http://www.sign2pay.com/.



4.10. Gebruikersinteractie

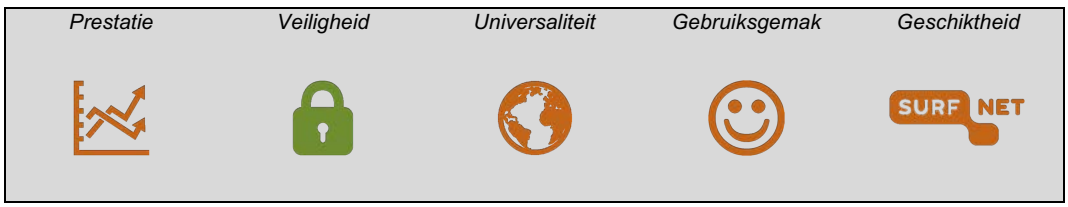
Verschillende eigenschappen van de interactie van de gebruiker (human computer interaction, HCI) met een systeem zijn identificerend en kunnen worden benut voor biometrische gedragsauthenticatie. Met name toetsenbord- en muisdynamiek (directe interactie), maar ook de inhoud van de interactie (indirecte interactie, gebaseerd op kennis, vaardigheid en strategie, denk aan gebruik van 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 Coursera gebruikt bijvoorbeeld signature track technologie op basis van toetsenborddynamiek om continue de identiteit van gebruikers te verifiëren. De markt voor typegedragherkenning 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 keylogging, het registreren van wat men typt, erg privacygevoelig, of zelf verboden onder afluisterwetten.

Muisdynamiek is erg vergelijkbaar met toetsenborddynamiek, waarbij de muisbeweging en klikgedrag worden geanalyseerd. Muisgedrag is echter minder geschikt, mede omdat er minder gebruik van wordt gemaakt en de patronen meer entropie kennen. Bovendien is deze technologie minder volwassen dan toetsenborddynamiek. Vaak wordt dit dan ook gecombineerd met toetsenborddynamiek, bijvoorbeeld door BehavioSec. Biometrie op basis van andere invoerapparaten, zoals een stylus of touchscreen, is mogelijk.

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 toetsenborddynamiek redelijk, muisdynamiek slechter, en indirecte interactie het slechtst [9], maar dit is tevens de volgorde van volwassenheid. Interactiegedrag is zeer moeilijk te kopiëren als biometrische factor. Vanzelfsprekend is toetsenborddynamiek alleen relevant voor PC's en niet voor bijvoorbeeld smartphones. De privacygevoeligheid van het registreren van het gedrag beperken de gebruikersacceptatie.



4.11. 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[33] of Leap[34] 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[35], Georgia Tech ontwikkelde LatentGesture[36], en er bestaan diverse "swipe-lock" apps voor smartphones. Microsoft Photo-Touch laat de gebruiker zich authenticeren door een patroon te tekenen op een foto. Onderzoekers ontwikkelden samen met Motorola uWave [10], een accelerometer gebaseerde gebaarherkenningstoepassing.

Er zijn toepassingen waarin de gebruiker een PIN-code of patroon op het scherm moet tappen in een muzikaal ritme[37]. 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[38].

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.

Prestatie	*Veiligheid*	*Universaliteit*	*Gebruiksgemak*	*Geschiktheid*
				

[33] Zie http://www.xbox.com/en-US/xbox-one/accessories/kinect-for-xbox-one.

[34] Zie https://www.leapmotion.com/.

[35] Zie http://www.lockheedmartin.com/us/news/press-releases/2013/february/isgs-fixmo-0220.html.

[36] Zie http://www.news.gatech.edu/2014/04/07/personal-touch-signature-makes-mobile-devices-more-secure.

[37] Zie http://www.di.fc.ul.pt/~tjvg/amc/taptap/bhci_tap.pdf.

[38] Zie http://www.biometricupdate.com/201401/authenware-launches-finger-tapping-rhythm-recognizing-behavioral-authentication-app.

5. CONCLUSIE & ADVIES

Tabel 1 geeft de verschillende middelen uit voorgaande hoofdstukken weer zoals gescoord op de criteria zoals besproken in eerdere hoofdstukken.

	Prestatie	Veiligheid	Universaliteit	Gebruiksgemak	Geschiktheid
Vingerafdruk	+	☐	☐	+	+
Irisscan	+	☐	☐	+	-
Netvliesscan	+	+	-	☐	-
Vingeraderpatronen	+	+	-	+	☐
Oogaderpatronen	☐	+	+	☐	+
Gezichtsherkenning	☐	☐	+	+	+
Hartslagherkenning	-	+	☐	☐	-
Sprekerherkenning	☐	☐	+	☐	+
Handtekening	-	☐	☐	+	-
Gebruikersinteractie	☐	+	☐	☐	☐
Gebarenherkenning	-	+	☐	+	☐

Tabel 1: De biometrische middelen gescoord op de criteria.

Middelen die er op een positieve manier uitspringen zijn:

- Vingerafdruk: Deze technologie presteert goed, is op dit moment nog niet universeel aanwezig - maar dit verandert naar verwachting vanwege toenemende inbedding van een geschikte sensor in smartphones. Bovendien past vingerafdrukherkenning (bijvoorbeeld via FIDO of BOPS) op de korte termijn goed in SURFconext Sterke Authenticatie. Er zijn oplossingen die met een gewone smartphone camera vier vingers tegelijkertijd opnemen[39].
- Oogaderpatronen: Ook deze lijkt goed te presteren (al weten we dit minder precies dan bij bijvoorbeeld vingerafdruk, irisscan en gezichtsherkenning: het is een relatief jonge technologie en er zijn slechts een handvol studies gedaan[40]). Dit kenmerk kan afgenomen worden met een gewone smartphone camera.

Mogelijke alternatieven zijn:

- Gezichtsherkenning, hoewel niet heel goed presterend kan deze met de standaard camera op een smartphone gebruikt worden.
- Sprekerherkenning, presteert vergelijkbaar als gezichtsherkenning, en ook hier geldt dat de sensor (microfoon) in elke smartphone zit. Maar dit kenmerk zal niet voor alle gebruikers even prettig werken, en is niet in alle omgevingen bruikbaar.

Irisscan, netvliesscan en vingeraderpatronen hebben speciale hardware nodig, en gebruik is mogelijk indringender (obtrusive). Deze middelen zijn voor de gemiddelde bij SURFnet aangesloten instelling daardoor in eerste instantie minder geschikt. Mogelijk zijn ze wel van toepassing in speciale use cases binnen de SURFnet

[39] Deze oplossing zou een FRR van 6% hebben bij FAR 1/1,000,000 (privécommunicatie met leverancier), maar dit is niet onafhankelijk vastgesteld.

achterban, bijvoorbeeld in de context van academische ziekenhuizen waar een smartphone met touchscreen bediening om hygiënische redenen minder geschikt is. Elektronische handtekeningherkenning heeft wat minder aandacht van de biometrie (onderzoeks-) gemeenschap gehad de laatste jaren, hierbij is idealiter ook een stylus of speciale pen nodig.

Gebruikersinteractie, gebarenherkenning en hartslagherkenning zijn interessant vanwege toepassing voor continue authenticatie. Deze middelen passen op de korte termijn niet goed genoeg in de architectuur van SURFconext Sterke Authenticatie en hebben consequenties voor de privacy. Voor individuele instellingen in de achterban van SURFnet in specifieke use cases zijn deze technologieën misschien wel interessant. In andere domeinen (bijvoorbeeld de bancaire sector) is gebruikersinteractie een belangrijk onderdeel in verband met zogenaamde risk based authenticatie.

Appendix A : LONGLIST

Gebaseerd op:

- [1] [2] [6] [7] [8] [12]
- http://www.biometrics.gov/documents/biooverview.pdf
- http://fingerchip.pagesperso-orange.fr/biometrics/types.htm
- http://www.biometricsinstitute.org/pages/types-of-biometrics.html

Biometrische modus	Beschrijving	Voornaamste reden deselectie
Hard biometrics		
Vingerafdruk	Beschreven in 4.1.	Wel geselecteerd.
Irisscan	Beschreven in 4.2.	Wel geselecteerd.
Netvliesscan	Beschreven in 4.3.	Wel geselecteerd.
Vingeraderpatronen	Beschreven in 4.4.	Wel geselecteerd.
Oogaderpatronen	Beschreven in 4.5.	Wel geselecteerd.
Gezichtsherkenning	Beschreven in 4.6.	Wel geselecteerd.
Palmafdruk	Net als vingerafdrukken, beschikt de handpalm over een afdruk.	Onpraktisch omdat een te groot registratieoppervlak nodig is.
DNA		Niet eenvoudig te meten, erg privacygevoelig.
Hand geometrie	De verhoudingen van de hand en vingers.	Onpraktisch omdat een te groot registratieoppervlak nodig is.
Soft physiological biometrics		
Hartslagherkenning	Beschreven in 4.7.	Wel geselecteerd.
Sprekerherkenning	Beschreven in 4.8.	Wel geselecteerd.
Skelet, e.g. frontale sinus	Röntgen of radiografische patroon van neusholte.	Onpraktisch, opnameapparatuur niet universeel beschikbaar.
Perioculaire informatie, vorm van gezichtsherkenning	Omgeving van het oog; verhoudingen wenkbrauwen, neus en oog.	Inferieur aan volledige gezichtsherkenning.
Hoofddimensies	De afmetingen van het hoofd.	Moeilijk meetbaar, hoofdafdruk.
Oor (geometrie, echogram, infrarood)	De afmetingen en vorm van het oor.	Technologie nog niet genoeg ontwikkeld.
Vingernagel	Lezen van structuur nagelbed met gepolariseerd licht.	Onpraktisch, sensors niet aanwezig.
Knokkels en vingers	Lijnen en vouwen in de vingers en knokkels.	Niet betrouwbaar genoeg, onpraktisch.
Neusafmetingen en poriën		Niet betrouwbaar genoeg, onpraktisch.
Huid: littekens, huid, tattoeages		Niet betrouwbaar genoeg, onpraktisch.

Absorptiespectrum huid	Lichtabsorptie van de huid onder LED's, techniek van Lumidigm.	Ongeschikt.
Voetafdruk		Onpraktisch.
Oogkleur, haarkleur, lengte		Niet betrouwbaar.
Afgeleide informatie: geslacht, leeftijd, etniciteit		Niet betrouwbaar.
Huidgeleiding, bio-elektrische lading		Onpraktisch.
Topografie van het hoornvlies	Gefotografeerd met NIR LED.	Inferieur aan iris en netvliesscan.
EEG	De hersenactiviteit gemeten met elektro-encefalogram.	Onpraktisch, niet betrouwbaar.
Kontafdruk	Japanse toepassing in zitkussen.	Onpraktisch, niet betrouwbaar.
Tandafdrukken	Zoals bij de tandarts.	Onpraktisch.
Lippen	Lipvorm (zoals gezichtsherkenning), afdruk (zoals vingerafdruk) en beweging.	Inferieur aan andere technieken, bijvoorbeeld gezichtsherkenning.
Lichaamsgeur		Onpraktisch, technologie nog niet genoeg ontwikkeld.
Behavioral biometrics		
Gebruikersinteractie	Beschreven in 4.10.	Wel geselecteerd.
Gebarenherkenning	Beschreven in 4.11.	Wel geselecteerd.
Oogbeweging	Vaak met speciale bril gemeten.	Inferieur aan andere technieken, zoals gezichtsherkenning.
Drukprofielen, bv. handdruk	Gemeten met druksensoren.	Technologie nog niet genoeg ontwikkeld.
Dynamische grip	Dynamisch drukprofiel, e.g. in vuurwapen	Technologie nog niet genoeg ontwikkeld.
Loopbeweging	Gemeten met accelerometer, bijvoorbeeld in smartphone.	Technologie nog niet genoeg ontwikkeld, onpraktisch.

Appendix B : EXPERTSESSIE DEELNEMERS

Onderstaande personen hebben deelgenomen aan de expertsessie op 30 september 2015. De auteurs bedanken de deelnemers van die sessie hartelijk.

- Max Snijder, European Biometric Group
- Ton van der Putte, onafhankelijk
- George Poel, Rabobank
- Beer Franken, Academisch Medisch Centrum
- Luuk Spreeuwers, Universiteit Twente

- Eefje van der Harst, SURFnet
- Michiel Schok, SURFnet
- Arnout Terpstra, SURFnet
- Thijs Kinkhorst, SURFnet
- Alf Moens, SURFnet
- Joost van Dijk, SURFnet

- Maarten Wegdam, InnoValor
- Martijn Oostdijk, InnoValor
- Arnout van Velzen, InnoValor

REFERENTIES

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

[2] Dantcheva, A., Velardo, C., D'angelo, A., & Dugelay, J. L., Bag of soft biometrics for person identification. *Multimedia Tools and Applications*, *51*(2), 739—777, 2011

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

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

[5] Daugman, John, New Methods in Iris Recognition, IEEE Transactions on Systems, Man, and Cybernetics – Part B: Cybernetics, 37(5), 1167—1175, http://www.cl.cam.ac.uk/~jgd1000/NewMethodsInIrisRecog.pdf, October 2007

[6] Delac, K., & Grgic, M., A survey of biometric recognition methods. In *Electronics in Marine, 2004, Proceedings Elmar 2004. 46th International Symposium*, 184—193, IEEE, June 2004

[7] Hulsebosch, B. et al., Milestone M3.1: Inventory of strong identity assurance solutions and how they compare to a web of trust approach, https://www.terena.org/mail-archives/refeds/pdfc3Cedh8OFf.pdf, August 2014

[8] Jain, A.K., and Kumar, A., Biometric Recognition: An Overview, Second Generation Biometrics: The Ethical, Legal and Social Context, E. Mordini and D. Tzovaras (Eds.), pp. 49—79, Springer, 2012

[9] Jorgensen, Z. and Yu, T., On Mouse Dynamics as a Behavioral Biometric for Authentication, In Proc. ASIACCS '11, ACM, 2011

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

[11] Oostdijk M., et al., Step-up Authentication-as-a-Service, https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_step-up_authentication-as-a-service_architecture_and_procedures_final.pdf, November 2012

[12] Ortega-Garcia, J., Bigun, J., Reynolds, D., & Gonzalez-Rodriguez, J., Authentication gets personal with biometrics. *Signal Processing Magazine, IEEE*, *21*(2), 50-62, 2004

[13] Ratha, N.K., Connell, J.H., and Bolle, R.M., Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40(3), 2001

[14] Ross, Arun, Jain, Anil K., Multimodal Biometrics: An Overview, Proc. EUSIPCO12, 1221—1224, September 2004

[15] Sanjekar, P. S., & Patil, J. B., An Overview of Multimodal Biometrics, *Signal & Image Processing: An International Journal (SIPIJ) Vol. 4*, 2013

[16] Singh, Yogendra Narain and Singh, S. K., Evalutation of Electrocadriogram for Biometric Authentication, Journal of Information Security, Vol. 3, No. 1, 39—48, http://dx.doi.org/10.4236/jis.2012.31005, January 2012

[17] Spreeuwers, Luuk, Breaking the 99% barrier: optimisation of three-dimensional face recognition, IET Biometrics, 4(3) 169—178, http://dx.doi.org/10.1049/iet-bmt.2014.0017, September 2015

[18] Tuyls, Pim, Škorić, Boris, Kevenaar, Tom (Eds.), Security with Noisy Data, Springer, ISBN 978-1-84628-984-2, 2007