dialogic
innovatie • interactie

Online identiteitsvaststelling en -verificatie

Onderzoek naar de technische mogelijkheden en risico's

Bij het aanvragen van een Nederlands identiteitsdocument geldt een verschijnings-plicht. Voor Nederlanders in het buitenland betekent dit dat zij naar een ambassade, consulaat of externe dienstverlener moeten reizen. Het vervangen van de fysieke verschijning door een 'online verschijning' of andere digitale variant van de daarbij uitgevoerde stappen, zou deze (soms lange) reis overbodig kunnen maken. In dit onderzoek verkennen we in hoeverre het aanvraag- en afgifteproces digitaal op afstand zou kunnen worden uitgevoerd. We brengen hiertoe de technische mogelijkheden en risico's in kaart voor het online vaststellen en verifiëren van de identiteit van Nederlandse burgers.

Ir. Tommy van der Vorst, dr. Tessel Blom, ir. ing. Reg Brennenraedts MBA

In opdracht van:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Publicatienummer
2022.017-2224 v1.5.521

Datum:
2 mei 2023

Inhoudsopgave

Met medewerking van: Valentyna Tsap MSc, Kaija Kirch MA, Hannes Krause MSc en Aivo Kalu PhD (Cybernetica).

Citeren als: Dialogic, Van der Vorst, T., Blom, T. & Brennenraedts, R. (2022). *Online identiteitsvaststelling en -verificatie. Onderzoek naar de technische mogelijkheden en risico's.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag.

Managementsamenvatting

Bij het aanvragen van een Nederlands identiteitsdocument geldt een verschijningsplicht. Voor Nederlanders in het buitenland betekent dit dat zij naar een ambassade, consulaat of externe dienstverlener moeten reizen. Het vervangen van de fysieke verschijning door een 'online verschijning' of andere digitale variant van de daarbij uitgevoerde stappen, zou deze (soms lange) reis overbodig kunnen maken. In dit onderzoek verkennen we in hoeverre het aanvraag- en afgifteproces digitaal op afstand zou kunnen worden uitgevoerd. We brengen hiertoe de technische mogelijkheden en risico's in kaart voor het online vaststellen en verifiëren van de identiteit van Nederlandse burgers.

Beantwoording onderzoeksvragen

Wat zijn de technische en procesmatige mogelijkheden en risico's voor overheidsorganisaties, voor digitale identiteitsvaststelling en -verificatie op afstand (zonder fysieke verschijning)?

Voor aanvragen waarbij de aanvrager geen geldig *bestaand* identiteitsmiddel kan overleggen, en derhalve identiteitsvaststelling dient plaats te vinden (waaronder eerste aanvragen), is een fysieke verschijning vooralsnog onmisbaar. Dit neemt uiteraard niet weg dat andere delen van het proces, zoals het overleggen van andere documenten, digitaal kunnen worden uitgevoerd. Voor aanvragen waarbij wel een bestaand geldig identiteitsmiddel beschikbaar is, zou een substantieel deel online op afstand moeten kunnen plaatsvinden.

De belangrijkste beperkende factor voor het volledig digitaal en op afstand brengen van dit proces is dat het op afstand afnemen van biometrie (technisch gezien, met de benodigde kwaliteit en betrouwbaarheid, en op dit moment) niet mogelijk is. Doordat afname van biometrie 'op afstand' in een niet-gecontroleerde omgeving plaatsvindt, blijft er fundamenteel meer ruimte voor manipulatie dan bij een fysieke verschijning in een sterker gecontroleerde omgeving. Ontwikkelingen op het vlak van vertrouwde eindgebruikersapparatuur maken wel dat er steeds meer technische garanties mogelijk zijn ten aanzien van de authenticiteit van verzamelde biometrie, maar deze technologieën zijn nog niet volwassen en nog niet algemeen beschikbaar in eindgebruikersapparaten zoals smartphones. Desondanks zien we mogelijkheden om het aanvraagproces zo in te richten dat het aantal keer dat een fysieke verschijning nodig is, te minimaliseren, en/of het moment hiervoor flexibeler te maken.

Vanuit het perspectief van fraude is de verwachting dat fraudeurs met name gebruik zullen maken van uitzonderingssituaties, en relatief minder van zwakheden in het reguliere aanvraagproces. Naast aandacht voor de betrouwbaarheid van de technische oplossingen 'op afstand' zal hier dan ook aandacht naar moeten uitgaan.

Wat betekent de (risico-)analyse voor het aanvraag- en uitgifteproces van paspoorten door Buitenlandse zaken en door gemeenten in Nederland?

Het *uitgeven* van een aangevraagd identiteitsmiddel gebeurt op dit moment al met enige regelmaat via aangetekende post of via koeriers (op risico en kosten van de aanvrager), in gevallen waar de aanvrager aangeeft dat niet van hen kan worden verwacht dat deze fysiek verschijnt. De koerier verifieert de identiteit van de ontvanger bij het uitgiftemoment van een Nederlandse identiteitskaart.

Het vervangen van de fysieke verschijning tijdens de *aanvraag* voor een digitaal proces op afstand is complexer. Een proces waarin biometrie op een eerder moment wordt ingenomen, kent beperkte toegevoegde waarde, omdat de 'houdbaarheidstermijn' van de biometrische

informatie nauwelijks langer is dan de maximale geldigheidstermijn van een identiteitsdocument. De bevindingen van dit onderzoek zien niet op de doelmatigheid, maar ondersteunen wel de conclusie dat beter nog even gewacht kan worden met het inslaan van deze richting tot de technologie volwassener is geworden. Technologische verbeteringen op het gebied van vingerafdrukscanners (met name 'touchless' sensoren) zouden deze optie in de toekomst aantrekkelijker kunnen maken. Gegeven het feit dat het gezicht bij veroudering minder 'stabiel' is dan de vingerafdruk zal de actualiteit van de pasfoto desondanks mogelijk een beperking kunnen blijven vormen voor de maximale houdbaarheidstermijn van eerder ingenomen biometrie.

Aanvullend spelen beperkingen vanuit de regelgeving, die één c.q. twee fysieke verschijningen vereisen bij aanvraag c.q. uitgifte van bepaalde identiteitsmiddelen, al is er op dit vlak (in verschillende mate voor paspoorten versus identiteitskaarten) wel enige ruimte (zolang aan de verplichtingen rondom opname van biometrie wordt voldaan).

Tot slot

Bij het digitaliseren van processen voor en rondom het aanvragen van identiteitsmiddelen (en wellicht overheidsprocessen in het algemeen) speelt dat de hoogste doeltreffendheid en doelmatigheid hoogstwaarschijnlijk kan worden behaald door (alleen) de meest voorkomende situaties digitaal te faciliteren. Bij digitalisering geldt in het algemeen dat er hoge initiële kosten zijn en (daarna) lage variabele kosten, terwijl in niet-digitale processen de vaste kosten lager zijn en de variabele hoger. Herhaalaanvragen voor identiteitsmiddelen komen het meest voor. Dit is dan ook de meest voor de hand liggende variant om te digitaliseren.

Voor alle andere soorten aanvragen, en om te kunnen omgaan met uitzonderingen, en om Nederlanders te accommoderen die geen gebruik kunnen of willen maken van een digitaal aanvraagproces, zal een niet-digitale route moeten blijven bestaan. Het invoeren van een digitaal proces vervangt de niet-digitale dienstverlening niet – deze blijft beschikbaar voor de minder digitaal vaardige aanvrager.

Aanbevelingen

We bevelen aan nader onderzoek uit te voeren naar de inzetbaarheid van technische innovaties op het gebied van biometrie-afname, waaronder met name de *touchless* vingerafdruksensoren. Daarnaast is nader inzicht wenselijk in de herbruikbaarheid/houdbaarheid van 'oude' pasfoto's. Tot slot achten we het zinvol de effectiviteit (kosten versus baten) van de bovenstaande optie in een business case uit te werken.

1 Introductie

1.1 Aanleiding

Voor allerlei formele en minder formele processen is het als individu nodig om je te identificeren. Hiervoor is een identiteitsmiddel nodig dat (typisch) wordt uitgegeven door Nederlandse gemeenten. Van een persoon die voor het eerst een identiteitsmiddel aanvraagt moet de identiteit, nationaliteit en verblijfstitel worden vastgesteld, voor de eerste keer (biometrische) gegevens worden afgenomen. Daarna kan het identiteitsmiddel worden geproduceerd. Naast deze identiteitsvaststelling is er ook sprake van identiteitsverificatie. Hiervan is onder andere sprake als iemand die al een identiteitsmiddel heeft (gehad) een nieuw middel aanvraagt. Op dat moment kunnen de oude biometrische gegevens vergeleken worden met de huidige. Op beide momenten kunnen daarnaast aanvullende controles plaatsvinden – bijvoorbeeld of de aanvrager gesignaleerd staat.

Op dit moment zijn de aanvraagprocessen vanuit perspectief van de aanvrager beperkt gedigitaliseerd. Een afspraak kan weliswaar online worden gemaakt, maar de aanvrager moet zich in veel gevallen toch fysiek begeven naar de innemer die verantwoordelijk is voor de aanvraag van de documenten (dat is veelal het kantoor van de gemeente). De reden hiervoor is (primair) Europese regelgeving, die stelt dat bij het afgeven van identiteitskaarten [1] en paspoorten [2, p. art. 28] een persoonlijke verschijning vereist is ('verschijningsplicht'). Afwijken van de verschijningsplicht is voor identiteitskaarten niet mogelijk. Voor paspoorten kan worden afgeweken van de verschijningsplicht indien '*dit niet van [de aanvrager] kan worden gevergd*', en '*op andere wijze voldoende zekerheid kan worden verkregen over de identiteit, de nationaliteit en de verblijfstitel van de aanvrager*' [2, pp. art 28, lid 3]. De Paspoortwet geeft geen verdere duiding bij het begrip 'persoonlijk verschijnen' – zo kan de vraag worden gesteld of een videoafspraak via internet wellicht ook als zodanig kan worden opgevat. Hoe dan ook zal aan de tweede hierboven genoemde voorwaarde moeten worden voldaan.

Vanuit verschillende hoeken is een vraag ontstaan naar (verdergaande) digitalisering van het aanvraagproces met daarbij ook identiteitsvaststelling en –verificatie. De casus die concrete aanleiding geeft tot dit onderzoek is die van Nederlanders in het buitenland, die in de huidige situatie één of twee keer naar een grensgemeente, ambassade of consulaat moeten reizen voor (bijvoorbeeld) het aanvragen van een paspoort. In een aantal gevallen is dit een behoorlijke reis, zeker wanneer bijvoorbeeld paspoorten voor kinderen moeten worden aangevraagd, welke ook persoonlijk moeten verschijnen. Daarnaast betreft dit onderzoek uiteraard ook de casus voor het aanvragen van identiteitsdocumenten door (ook nieuwe) Nederlanders bij Nederlandse gemeenten. In bredere zin speelt een beweging van digitalisering van overheidsdiensten waarbinnen het voor de hand ligt om te analyseren of een (tot nu toe) relatief 'fysiek' proces (zowel dat in het buitenland als in het binnenland) zou kunnen worden gedigitaliseerd.

Aanleiding voor het onderzoek was onder andere een motie die ingediend werd in de Tweede Kamer op 24 november 2021 (gevolgd door een aanpassing op 25 november). Deze ging over de nieuwe mogelijkheden voor digitalisering van producten en diensten voor

Nederlanders in het buitenland en over de volledige digitalisering van de consulaire documentenverstrekking.[1]

1.2 Doel van het onderzoek

Het onderzoek heeft als doel om technische mogelijkheden en risico's in kaart te brengen voor het online vaststellen en verifiëren van de identiteit van Nederlandse burgers. Het onderzoek draagt daarmee bij aan beleidsvorming op het gebied van online/digitale identiteitsvaststelling en identiteitsverificatie.

Het onderzoek bestaat daartoe uit twee delen. Het eerste deel richt zich op het verkennen van mogelijke technische oplossingen, en inschatting van de risico's daarbij, om betrouwbaar online tot identiteitsvaststelling te komen en op de technische mogelijkheden en risico's daarbij om betrouwbaar online de identiteit van betrokken persoon te verifiëren. Respectievelijk zijn er in deze cases nog geen of al wel referentiegegevens van de betrokken persoon bekend.

Het tweede deel richt zich op de vraag hoe deze gevonden oplossingen en risicomodellering toegepast kan worden op het proces van aanvraag en uitgifte van paspoorten door het ministerie van Buitenlandse Zaken voor Nederlanders in het buitenland, en van gemeenten in Nederland.

1.2.1 Onderzoeksvragen

De onderzoeksvragen van dit onderzoek zijn als volgt:

<u>Deel 1: Verkenning technische mogelijkheden en risico's daarvan</u>

I. Wat zijn de technische en procesmatige mogelijkheden voor overheidsorganisaties, zoals de gemeenten, om digitaal (zonder fysieke verschijning) de identiteit van persoon vast te stellen, dan wel verifiëren?

Ia. Hoe kunnen de volgende functionaliteiten gerealiseerd worden:

a. Betrouwbare en veilige communicatie met hun burgers op afstand (waarbij authenticiteit, integriteit, tijdigheid, vertrouwelijkheid en optioneel ook vrijwilligheid met hoge zekerheid zijn te garanderen).
b. Op afstand vaststellen, met medewerking van een burger, dat die burger leeft en vrijwillig handelt.
c. Op afstand vaststellen, met medewerking van de burger, welke persoonsgegevens bij de burger horen (naam, adres, geboortedatum, nationaliteit, verblijfsrecht, …)
d. Op afstand, met medewerking van de burger, actuele biometrische gegevens afnemen.
e. Op afstand, met medewerking van een burger, een identiteitsverificatie uitvoeren op basis van een door de overheid uitgegeven identiteitsmiddel.

Ib. Welke methoden van online identiteitsvaststelling en identiteitsverificatie zijn mogelijk?

Ic. Tot welk betrouwbaarheidsniveau kan een methode ingezet worden?

[1] Kamerstukken II 2021/2022, 35925, nr.54 en nr. 59

II. Welke risico's bestaan er bij online/ digitale identiteitsvaststelling en verificatie?

IIa. Welke risico's bestaan er aan de kant van de gebruikers? (bv. misleiding door deep fake, AI, …),

a. Autoriteit (personeel, kennis, …);
b. devices (camera´s, scanners, computer, smartphone, …);
c. Netwerk (onderscheppen van gegevens, cyberattack, …) en;
d. Referentiegegevens (identiteitsmiddelen, RFID-chip, basisregisters, biometrie).

IIb. Welke privacyrisico's bestaan er?

IIc. Welke maatregelen zijn mogelijk om risico's te voorkomen?

IId. Waarover (kennis, middelen, personeel) moet de autoriteit beschikken die de identiteitsvaststelling of identiteitsverificatie moet doen?

IIe. Welke maatregelen zijn mogelijk om risico's te voorkomen?

Deel 2: Toepassing van de gevonden (technische) mogelijkheden

III. Wat betekent de (risico-)analyse (antwoord op onderzoeksvragen I en II) voor het aanvraag- en uitgifteproces van paspoorten door Buitenlandse zaken en door gemeenten in Nederland?

IIIa. Kan hierbij gebruik worden gemaakt van digitale/ online identiteitsvaststelling en verificatie?

IIIb. Zo ja, wat dient er hiervoor aangepast te worden in dit proces?

1.3 Leeswijzer

In hoofdstuk 2 beschrijven allereerst de onderzoeksaanpak, waarin we definities geven voor diverse kernbegrippen en een analytisch kader schetsen. In hoofdstuk 3 gaan we nader in op het huidige aanvraagproces. Hierbij belichten we de aspecten die relevant zijn bij beoordeling van alternatieven 'op afstand'. In hoofdstuk 4 gaan we in op de technische oplossingen waarmee een aanvraagproces 'op afstand' zou kunnen worden gerealiseerd. In hoofdstuk 5 presenteren we tot slot onze bevindingen en conclusies en beantwoorden de onderzoeksvragen.

2 Onderzoeksaanpak

Ter beantwoording van de onderzoeksvragen is op hoofdlijnen de aanpak zoals hieronder weergegeven in Figuur 1 gevolgd.

Allereerst is een inventarisatie gemaakt van de aanvraagprocessen en diverse varianten daarvan, die relevant zijn voor dit onderzoek. Vervolgens is voor deze processen geanalyseerd hoe de 'vertrouwensketen' eruit ziet: welke stappen worden gezet om, met hoge mate van betrouwbaarheid en zekerheid over de identiteit van de aanvrager, een identiteitsdocument te verstrekken? Vervolgens inventariseren we technische oplossingen voor de stappen die op dit moment niet 'op afstand' (zonder fysiek contact) kunnen worden uitgevoerd. Tot slot analyseren we de geschiktheid van deze technische oplossingen om zo te bepalen welke stappen mogelijk 'op afstand' zouden kunnen worden uitgevoerd.

Figuur 1 Schematisch overzicht van het analytisch kader

2.1 Definities

2.1.1 Identiteit, de BRP, identiteitsvaststelling en identiteitsverificatie

Als er gesproken wordt over **identiteit** gaat het in deze context over de administratieve identiteiten in de relatie tussen persoon en overheid. Een (administratieve) identiteit is een set aan gegevens die horen bij één natuurlijk persoon en op basis van deze gegevens kunnen rechten en plichten ontleend worden. In de registratie van de overheid heeft de overheid het principe dat één persoon één identiteit heeft, waarbij een uniek identificerend nummer (BSN; burger service nummer) hoort.

Gegevens die de overheid bijhoudt over personen worden opgeslagen in de basisregistratie personen (BRP). In de BRP komen de gegevens van alle Nederlandse gemeentes samen. Ook mensen die korter dan vier maanden in Nederland zijn of niet-ingezeten Nederlanders staan in de BRP (ook wel RNI, de registratie van niet-ingezetenen). [3]

De **inschrijving in de BRP** gebeurt bijvoorbeeld na aangifte van de geboorte van een persoon of als een persoon naar Nederland verhuisd is en hier langer dan vier maanden gaat wonen. [4] De inschrijving in de BRP is een gevoelig proces omdat het leidt tot rechten en plichten. In Nederland zijn er echter (impliciete) checks aanwezig om frauduleuze inschrijvingen tegen te gaan. Bij bijvoorbeeld een inschrijving na een geboorte wordt verwacht dat een persoon zich meldt bij het consultatiebureau of op school wanneer het de leeftijd van

leerplicht bereikt. In het buitenland varieert de registratie en documentatie van dit soort levensgebeurtenisssen en zitten er ook grote verschillen in de betrouwbaarheid van het aangifteproces (bijvoorbeeld valse geboorteaktes die gekocht kunnen worden).

Bij **identiteitsvaststelling** wordt een natuurlijk persoon gekoppeld aan een identiteit. Identiteitsvaststelling gebeurt als een identiteit (nog) niet via een middel geverifieerd kan worden. Denk bijvoorbeeld aan een kind dat voor de eerste keer een **identiteitsmiddel** gaat aanvragen. Er is dan onderzoek nodig om een identiteitsclaim (iemand stelt bij een identiteit te horen) te verifiëren. Een eenmaal vastgestelde identiteit wordt vervolgens via biometrische gegevens duurzaam gekoppeld aan een persoon. Ook dit is een uiterst kwetsbaar proces. Ten eerste is het vaststellen van een identiteit zonder identiteitsmiddel fraudegevoelig omdat de BRP-inschrijving zelf alleen administratieve gegevens over een persoon bevat, en geen biometrische kenmerken. Daardoor zou in theorie iedereen die voldoet aan de kenmerken van de administratieve gegevens die beschikbaar zijn (bijv. leeftijd en geslacht) gekoppeld kunnen worden aan die identiteit.

Als er vervolgens een identiteitsmiddel is, dan kan er **identiteitsverificatie** plaatsvinden waarbij een identiteitsclaim geverifieerd wordt. Identiteitsverificatie vindt bijvoorbeeld plaats als, na het overleggen van een identiteitsmiddel, de biometrie geverifieerd wordt en daarmee de identiteit van de persoon gecontroleerd kan worden. Biometrische gegevens bevatten een set van eigenschappen van een persoon die voldoende uniek zijn om identificatie mogelijk te maken. In dit rapport zullen wij ons onder meer focussen op de technische oplossingen voor online identiteitsverificatie en of het mogelijk is om op afstand vast te stellen dat bepaalde biometrische kenmerken als vingerafdruk en gelaat bij een bepaalde (identiteit van een) persoon horen.

2.1.2 Het identiteitsmiddel

In Nederland bestaan er vijf wettelijke identiteitsmiddelen: Paspoort (incl. diplomatiek, dienstpaspoort etc.), Nederlandse identiteitskaart, rijbewijs, vreemdelingendocument en geprivilegieerd document. Het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) is beleidsverantwoordelijke voor paspoorten, identiteitskaarten en (toekomstige) elektronische identiteitsbewijzen. Het Ministerie van Buitenlandse Zaken (BZ) is de uitgevende instantie van paspoorten en identiteitskaarten in het buitenland, terwijl de gemeenten de uitgevende instantie zijn van rijbewijzen, paspoorten en identiteitskaarten in Nederland. [5] Een paspoort is een identiteitsmiddel dat de nationaliteit en identiteit aantoont, een Nederlandse identiteitskaart toont dit ook aan, maar kan alleen gebruikt worden voor verplaatsingen binnen de EU. Een (Europees) rijbewijs is ook een identiteitsmiddel, maar kan niet gebruikt worden om te reizen of voor identiteitsverificatie in het buitenland. Dit omdat er op het rijbewijs geen gegevens over verblijfsstatus en nationaliteit staan. [6]

Tabel 1 bevat ter illustratie de gegevens die op een Nederlands **reisdocument** (paspoort of identiteitskaart) staan en uit welke bron deze gegevens komen. Wanneer het gegeven niet in de BRP opgenomen is, moet de aanvrager het benodigde brondocument (bijvoorbeeld een geboorteakte, een huwelijksakte of een ander bewijsdocument) aanleveren. [7]

Tabel 1: Gegevens Nederlands reisdocument

Gegeven	Bron
Voornaam, achternaam of een namenreeks[2]	BRP of brondocument. Bij de voornaam of de achternaam kan een adellijke titel worden vermeld wanneer de aanvrager de titel draagt en prijs stelt op vermelding.
Wanneer de aanvrager er prijs op stelt, de naam van de partner	BRP of akte.
Geboortedatum	BRP of akte.
Geboorteplaats	BRP of akte.
Geslacht	BRP of akte.
Een uniek identificerend nummer, het BSN	BRP, wanneer de persoon niet bekend is in de BRP en er dus geen BSN bekend is, wordt er geen identificerend nummer in het paspoort vermeld.
Nationaliteit	BRP en bewijsdocumenten die bij nader onderzoek verzameld zijn.
Lengte	Bepalen bij het indienen van de aanvraag.
Handtekening	De handtekening wordt door de aanvrager op een kaartje gezet tijdens de aanvraag en vervolgens gedigitaliseerd.
Foto	De aanvrager levert een papieren foto in die voldoet aan een vastgestelde set acceptatiecriteria, de ´fotomatrix´ [8]. De foto wordt vervolgens gedigitaliseerd.
Vingerafdrukken	Tijdens de aanvraag worden met een elektronische vingerafdruklezer van (minimaal) twee vingers vingerafdrukken gemaakt.

In het vervolg van dit rapport zullen wij het hebben over *persoonsgegevens* en *biometrische gegevens*. Onder persoonsgegevens vallen de naam, geboortedatum, geboorteplaats, geslacht, BSN en nationaliteit van een persoon. De biometrische gegevens omvatten de foto en de vingerafdrukken en zijn persoonsgegevens die uniek zijn en op grond waarvan eenduidige identificatie van een persoon mogelijk is. [9]

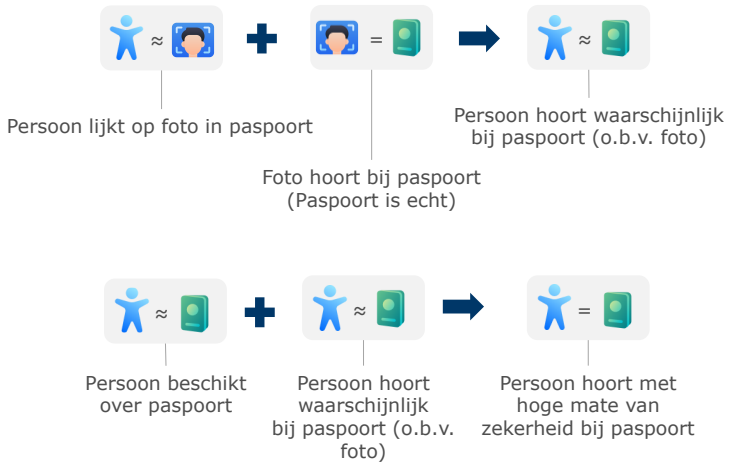
Behalve de vingerafdrukken, worden alle gegevens afgedrukt op het reisdocument zelf. Alle gegevens plus de vingerafdrukken worden daarnaast ook opgeslagen in een chip in het paspoort. Met een documentlezer kunnen alle gegevens die ook met het blote oog te zien zijn uitgelezen worden uit de chip. Alle instanties waar reisdocumenten met een chip worden aangevraagd kunnen het gedeelte van de chip waar de vingerafdruk is opgeslagen ook uitlezen, dit gaat dan om alle Nederlandse gemeenten, Nederlandse ambassades en consulaten en de uitgevende instanties in het Caribisch deel van het Koninkrijk. Voor het uitlezen van de vingerafdruk wordt een vinger op de vingerafdruklezer gelegd die de vingerafdruk

[2] Bij een namenreeks kan geen onderscheid worden gemaakt tussen de geslachtsnaam en de voornamen van een persoon. Dit wordt bijvoorbeeld gebruikt in: Afghanistan, Bangladesh, Egypte, Ethiopië, India, Indonesië, Irak, Democratische Republiek Congo, Nepal, Pakistan, Soedan, Somalië en Sri Lanka. (Minister van Justitie, 2010)

vergelijkt met de vingerafdruk die is opgeslagen. Andere instanties hebben een certificaat nodig voor toegang tot de vingerafdrukken in de chip. Deze certificaten worden verleend door de Nederlandse overheid.[3] [10]

2.2 De vertrouwensketen

Identiteitsverificatie kan worden beschreven als een proces waarin identiteitsclaims worden geverifieerd met identiteitsmiddelen, totdat voldoende zekerheid is ontstaan over de daadwerkelijke identiteit van een persoon. Onderstaande Figuur 2 toont hoe een vertrouwensketen schematisch kan worden weergegeven. Figuur 2 toont niet de gehele vertrouwensketen, maar dient slechts als voorbeeld van (een deel van) de vertrouwensketen. In theorie levert het valideren van een identiteitsclaim op basis van een identiteitsmiddel ofwel een positief, ofwel een negatieve uitkomst op (de persoon hoort wel/niet bij de geclaimde identiteit). In de praktijk is de uitkomst van een verificatie van een identiteitsclaim een bepaald zekerheidsniveau: de *kans* dat de persoon wel of niet hoort bij de geclaimde identiteit. Wanneer bijvoorbeeld een identiteitsmiddel met pasfoto wordt gebruikt, en de verificatie plaatsvindt aan de hand van de pasfoto, hangt de mate van zekerheid af van de mate van uniekheid van het gezicht en de gelijkenis met de pasfoto (en de mate waarin de persoon die de verificatie uitvoert een match van pasfoto's correct kan vaststellen).



Figuur 2. Schematische weergave van de vertrouwensketen bij identiteitsvaststelling/verificatie.

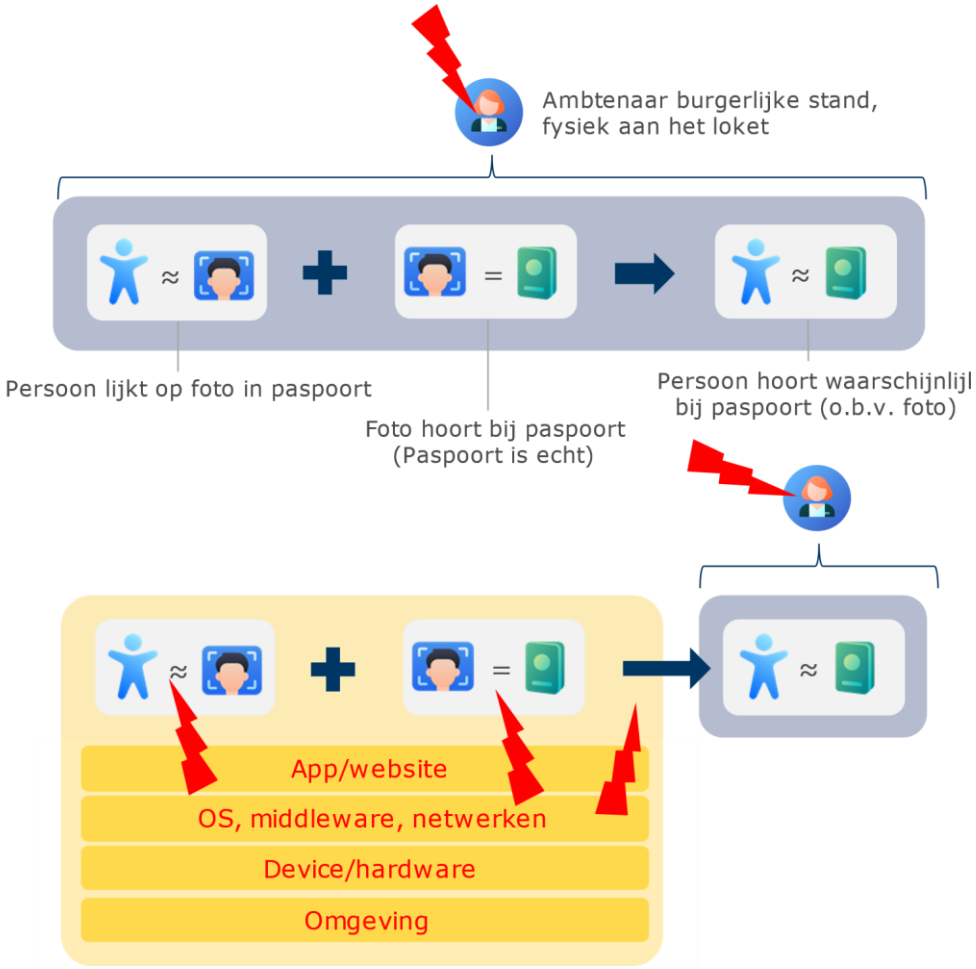
De vertrouwensketen kan worden weergegeven als een 'boomstructuur'. Bij bijvoorbeeld het verifiëren van identiteit op basis van de foto in een identiteitsmiddel dient niet alleen de gelijkenis tussen de persoon en de foto te worden geverifieerd, maar bijvoorbeeld ook de echtheid van het identiteitsmiddel (is de foto in het identiteitsmiddel niet gemanipuleerd?). Het controleren van de echtheid van een identiteitsmiddel gebeurt in de regel op basis van meerdere echtheidskenmerken (die opgeteld een bepaalde zekerheid van echtheid geven).

2.2.1 Omgeving

De fysieke *omgeving* waarbinnen de stappen in de vertrouwensketen worden uitgevoerd is bepalend voor de kwaliteit van de verificatie en daarmee de betrouwbaarheid van de keten. Wanneer bijvoorbeeld een controle van een vingerafdruk plaatsvindt op een stadskantoor,

[3] Er wordt gebruik gemaakt van een stelsel van certificaten (PKI). De Nederlandse overheid verstrekt certificaten aan andere Europese lidstaten. Deze lidstaten kunnen met deze certificaten organisaties machtigen (door specifiekere certificaten uit te geven).

dan kan met hoge mate van zekerheid worden voorkomen dat bijvoorbeeld de vingerafdruksensor wordt gemanipuleerd. Wanneer dezelfde controle op een locatie plaatsvindt met een lager niveau van controle over de fysieke omgeving is dit risico groter. In dit onderzoek is dan ook niet alleen van belang om vast te stellen welke stappen op welke manier op afstand worden uitgevoerd, maar ook in welke *omgeving* deze worden uitgevoerd. Figuur 3 toont dit schematisch. Deze laat zien dat als een controle van overeenkomst tussen een foto en een persoon digitaal wordt uitgevoerd er verschillende onzekerheden geïntroduceerd worden. Er zijn verschillende stappen in de keten (app, website, OS, middleware, netwerken, device, et cetera) waarover simpelweg geen of beperkte controle is. Hierdoor wordt het minder zeker of de persoon die achter de camera zit ook echt de persoon is die hij of zij claimt te zijn. Uiteraard kan, in het 'niet-digitale' proces, ook beïnvloeding plaatsvinden van de betrokken ambtenaren (integriteit).



Figuur 3 Invloed van de omgeving op stappen in de vertrouwensketen

2.3 Vereisten aan het aanvraagproces

Bepalend voor de invulling van het aanvraagproces zijn in beginsel de juridische kaders voor het aanvragen en uitgeven van paspoorten en identiteitskaarten (de Paspoortwet [2], Paspoortbesluit [11] en Paspoortuitvoeringsregeling [12]). [4] Daarnaast spelen Europese standaarden en vereisten ten aanzien van Europese identiteitsmiddelen, en wereldwijd diverse afspraken en standaarden ten aanzien van paspoorten en identiteitsmiddelen

[4] Op dit moment zijn deze ook van toepassing op uitgifte van Nederlandse identiteitskaarten.

(waaronder vanuit de ICAO). Deze juridische kaders vormen samen de uitgangspunten voor het *huidige* aanvraagproces. Het is echter denkbaar dat de juridische kaders uiteindelijk zouden moeten worden gewijzigd om een aanvraagproces mogelijk te maken dat volledig op afstand plaatsvindt. Zo is een belangrijke vraag in hoeverre op afstand kan worden voldaan aan de verschijningsplicht die in de juridische kaders wordt gesteld. Of het juridische begrip 'rekbaar' genoeg is om ook een digitale variant te accommoderen, of dat de kaders daarvoor gewijzigd zouden moeten worden, is een vraag voor juristen. In dit onderzoek pogen we allereerst de *mogelijkheden* te onderzoeken, waarna de (politieke) afweging kan worden gemaakt tot eventuele wijziging van de regelgeving.

Ter beantwoording van de onderzoeksvragen in het voorliggende onderzoek is in plaats daarvan gezocht naar een beoordelingskader op basis van de meer fundamentele waarden die onder de regelgeving liggen. Niet het feit dat de Paspoortwet een fysieke verschijning vereist, maar de vraag *waarom* deze verschijning noodzakelijk is, is voor dit onderzoek relevant. Afhankelijk van deze onderliggende redenen kan (beter) worden beoordeeld of een technische oplossing een volwaardig alternatief hiervoor zou kunnen zijn. We baseren het beoordelingskader in dit onderzoek op de gesprekken en sessies met experts die in dit onderzoek zijn gehouden, aangevuld met literatuurstudie. Tabel 2 toont de hieruit door ons geïdentificeerde meest relevante aspecten.

Tabel 2 Alfabetische lijst (niet-uitputtend) van relevante beoordelingsaspecten bij het aanvraagproces voor Nederlandse identiteitsmiddelen

Aspect	Toelichting
Actualiteit, juistheid, authenticiteit en niet-ambiguïteit biometrie (foto en vingerafdruk) in identiteitsmiddel	De foto en vingerafdruk die zijn opgenomen op en in een identiteitsmiddel worden gebruikt om (soms als onderdeel van de standaard werkwijze, en soms alleen als er twijfel bestaat) te controleren of een persoon hoort bij een identiteitsmiddel. Om op basis van biometrie een betrouwbare vergelijking te kunnen maken dienen de biometrische gegevens actueel te zijn. Onderzoek wijst uit dat de houdbaarheid van vingerafdrukken (maximumleeftijd van een 'oude' vingerafdruk waarmee een afgenomen vingerafdruk kan worden vergeleken) ongeveer elf jaar bedraagt. [13] Voor minderjarigen en ouderen is deze termijn mogelijk korter dan voor anderen. Voor minderjarigen (en in het bijzonder baby's) geldt daarnaast dat het gezicht zeer snel verandert. Uiteraard dient de biometrie te horen bij de aanvrager (juistheid), dient deze niet gemanipuleerd te zijn (authenticiteit) en dient deze in principe geen betrekking te hebben op meer dan één persoon (ambiguïteit). Van dit laatste is (bij pasfoto's) sprake bij *morphing* [14], maar (soms) ook bij eeneiige tweelingen.
Juistheid van identificatie	Het is gedurende het aanvraag- en uitgifteproces van belang dat de identificatie op een juiste manier gebeurt en de koppeling tussen persoon en identiteitsmiddel sterk is.

Aspect	Toelichting
Kwaliteit en betrouwbaarheid afgegeven identiteitsmiddelen	De kwaliteit van de identiteitsmiddelen die worden afgegeven moeten voldoen aan de geldende technische standaarden en internationale afspraken. Dat betekent onder andere dat de biometrische gegevens die in of op het identiteitsmiddel staan, van voldoende kwaliteit moeten zijn.
Privacy	Nederland slaat de vingerafdrukken die worden afgenomen ten behoeve van het aanvragen van een identiteitsmiddel niet centraal op. Afgegeven foto's worden wel centraal opgeslagen. Het centraal (gaan) opslaan van biometrische gegevens, en/of het vergroten van de mate waarin dit gebeurt (bijvoorbeeld door méér vingerafdrukken of een dieptescan van een gezicht op te slaan) kan een aantasting van de privacy van Nederlanders betekenen en leiden tot een politieke keuze.
Reputatie Nederlandse reisdocumenten	De bruikbaarheid van Nederlandse reisdocumenten in het buitenland staat of valt met de reputatie van deze reisdocumenten. Zou bijvoorbeeld bekend worden dat op grote schaal valse Nederlandse identiteitsdocumenten in omloop zouden zijn, dan zou dit het visumvrij reizen van Nederlanders in bepaalde landen kunnen bemoeilijken.
Signalering	Bij aanvragen van Nederlandse identiteitsmiddelen wordt gecontroleerd of een persoon gesignaleerd staat in bijvoorbeeld het Register Paspoortsignaleringen, waarin aangegeven wordt of de aanvrager een paspoort mág aanvragen.
Vaststellen in-leven-zijn	De overheid wil weten of de aanvrager nog in leven is, zeker wanneer bijvoorbeeld de AOW leeftijd is bereikt en er pensioen wordt uitgekeerd.
Vaststellen Nederlandse nationaliteit	Afhankelijk van het type aangevraagde identiteitsmiddel is het noodzakelijk om te kunnen vaststellen of de aanvrager beschikt over de Nederlandse nationaliteit. Op zichzelf zou identiteitsverificatie hiervoor voldoende moeten zijn: de persoon kan op dat moment immers worden opgezocht in de daarvoor ingerichte registers. In een aantal gevallen zal echter nader onderzoek moeten plaatsvinden.[5]
Verificatie vrijwilligheid van de aanvrager	Wanneer een aanvrager van een identiteitsmiddel de aanvraag niet vrijwillig doet (om het middel zelf te gebruiken), is er een grote kans dat het verstrekte middel onrechtmatig gebruikt gaat worden, en het bijvoorbeeld ter beschikking wordt gesteld van een derde (al dan niet tegen betaling).[6]

[5] Het is mogelijk dat dit naar verhouding vaker of minder vaak voorkomt binnen de groep Nederlanders die zich in het buitenland bevinden dan onder Nederlanders die zich in Nederland bevinden. Gegevens hierover zijn echter niet bekend bij de onderzoekers.

[6] Het is uiteraard denkbaar dat een identiteitsdocument ná afgifte in verkeerde handen komt (bijvoorbeeld door diefstal) en/of onrechtmatig wordt gebruikt. Dit valt buiten de scope van het aanvraagproces.

Aspect	Toelichting
	De vrijwilligheid van de aanvrager is echter lastig te verifieren in het huidige proces.
Uitvoerbaarheid	Het proces moet voor zowel de aanvrager als de innemende en uitgevende instantie uitvoerbaar zijn. De aanvrager moet het proces bijvoorbeeld kunnen doorlopen via een 'gewone' smartphone.

2.3.1 Fraude

Een aspect dat niet is genoemd in bovenstaande tabel, maar uiteraard wel relevant is in het onderzoek, is de mate waarin fraude tijdens het aanvraagproces wordt voorkomen. Fraude is, ons inziens, een overkoepelend begrip dat in de hierboven genoemde aspecten is verwerkt.

Identiteitsfraude en fraude met identiteitsdocumenten komt in verschillende vormen voor. Fraude op basis van vervalste of nagemaakte documenten valt buiten de afbakening van dit onderzoek: het gaat hier immers om het aanvraagproces dat in principe altijd leidt tot de verstrekking van een 'echt' document. Als het gaat om fraude met authentieke documenten, dan is onderscheid te maken tussen fraude door een derde, en fraude door de aanvrager zelf. [15] [16]

In het eerste geval gaat het om de vraag of de aanvrager *slachtoffer* wordt van fraude wanneer de aanvraag met succes zou worden afgerond. Uiteraard kan er ook na de aanvraag van een document fraude plaatsvinden – zo kunnen paspoorten worden gestolen ten behoeve van identiteitsfraude of vervalsing. In het kader van dit onderzoek gaat het dan ook om fraude met vooropgezet plan voor fraude tijdens de aanvraag. Omdat de aanvrager zelf niet de intentie heeft te frauderen moet er logischerwijs ook sprake zijn van *onvrijwilligheid* (verificatie van vrijwilligheid is daarom opgenomen als aspect). Er zou overigens ook sprake kunnen zijn van *onwetendheid* (denk bijvoorbeeld aan een hypothetisch scenario waarbij een aanvrager nietsvermoedend een paspoort zou aanvragen, maar waarbij in het aanvraagproces de pasfoto en het bezorgadres van het paspoort zou worden aangepast). Dit laatste hangt wat ons betreft vooral samen met de integriteit van het proces.

In het tweede geval gaat het om de vraag of de aanvrager zélf te goeder trouw handelt. We illustreren dit aan de hand van een aantal bekende vormen van fraude waarin de aanvrager zélf niet te goeder trouw handelt:

- Een fraudeur die een document aanvraagt ten behoeve van vervalsing (door bijvoorbeeld later in het authentieke document te proberen gegevens te wijzigen). De intentie van een paspoortgebruiker is nauwelijks te bepalen in het aanvraagproces (en kan uiteraard ook na de aanvraag wijzigen: een bezitter van een vijf jaar oud paspoort kan ook altijd nog besluiten dit te vervalsen). Dit valt buiten de afbakening van het onderzoek.
- Een fraudeur die een document aanvraagt namens iemand anders. Dit geval zou echter niet mogelijk moeten zijn als de identiteitsverificatie tijdens de aanvraag waterdicht is (en de referentiegegevens juist zijn – zie het volgende punt).
- Een fraudeur die een document aanvraagt met een gemanipuleerde foto, die het mogelijk maakt dat het document door meerdere personen zou kunnen worden gebruikt ('morphing' [14]). In dit geval is de verificatie van de foto met het gezicht van de aanvrager van belang. Dit is inbegrepen in het aspect "actualiteit en juistheid van biometrie".

2.3.2 Vergelijkingsniveau

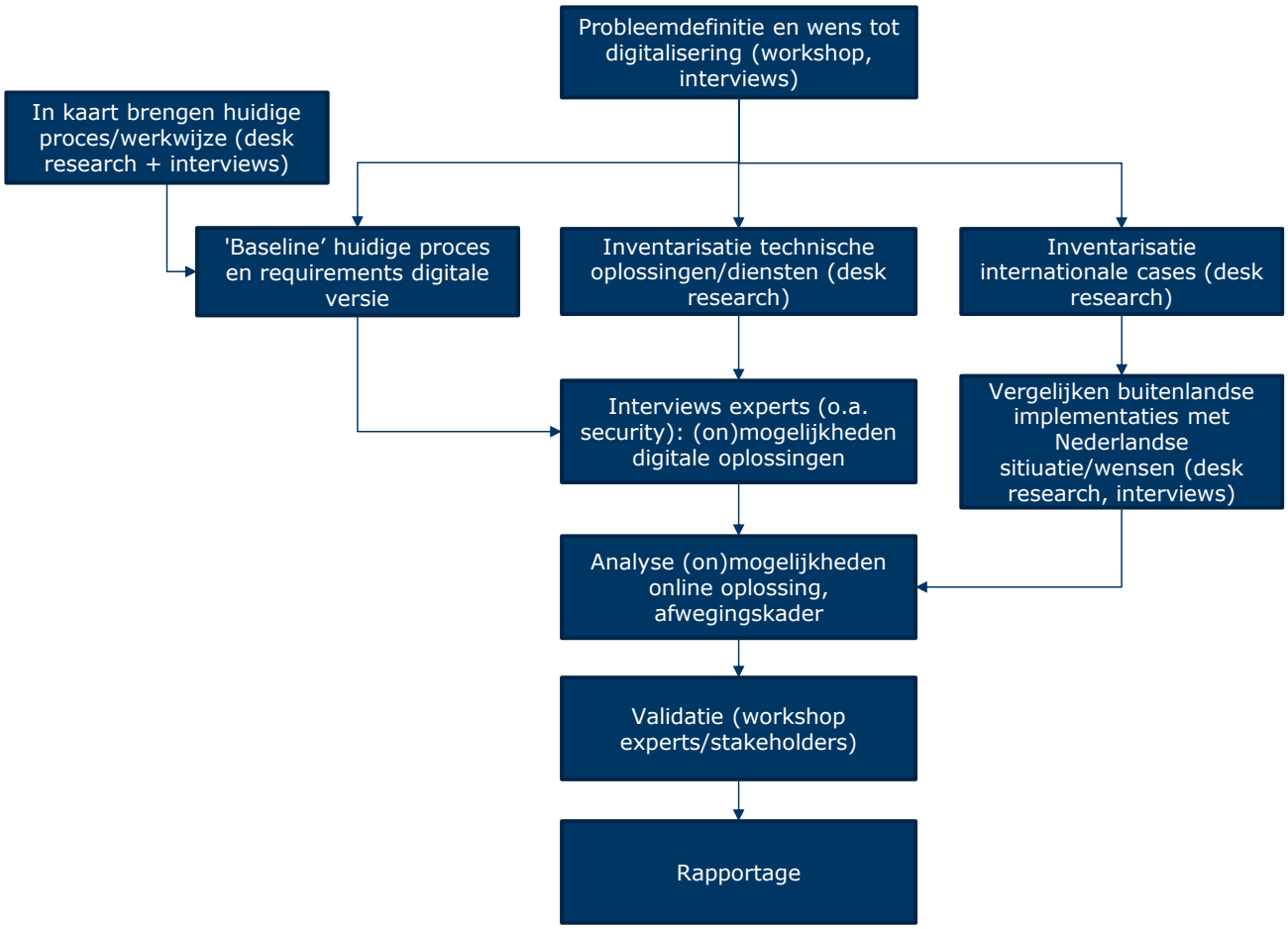
Voor veel van de hierboven genoemde aspecten geldt dat er geen 'hard' criterium is om vast te stellen dat aan het aspect wordt voldaan. Identiteitsverificatie is bijvoorbeeld idealiter in alle gevallen correct, maar in de praktijk is dat niet haalbaar. De vraag rijst wat het drempelniveau is waarboven een (deel)oplossing voldoet aan de hierboven genoemde aspecten.

Het huidige proces (waar we in hoofdstuk 3 in detail op ingaan) voor identiteitsmiddelen bij gemeenten in Nederland is niet 'waterdicht' tegen fraude. [17] Het is echter de vraag of het huidige proces, c.q. de opzet van het huidige systeem van identiteitsmiddelen als uitgangspunt zou moeten dienen. Het is zeer denkbaar dat een systeem op afstand andere zwakheden en vormen van fraude aantrekt dan het bestaande systeem. De uitgangspunten op basis waarvan het huidige proces is vormgegeven, zijn niet noodzakelijkerwijs op dezelfde manier van toepassing op het te ontwikkelen aanvraagproces op afstand.

2.4 Onderzoeksmethode

De onderzoeksvragen worden in dit onderzoek integraal bekeken. Dat wil zeggen dat we aan de hand van de set onderzoeksvragen als geheel hebben gezocht naar bronnen, die in sommige gevallen meerdere onderzoeksvragen/delen betroffen. We hebben daarnaast gebruik gemaakt van verschillende onderzoeksmethoden. Op basis van bureau- en literatuuronderzoek is een inventarisatie gemaakt van relevante documenten, zoals nationale en internationale wetgeving over identiteitsdocumenten, beleidsnota's, documentatie over middelen die worden gebruikt voor identiteitsvaststelling en -verificatie, en dergelijke. Daarnaast is via interviews met een breed palet aan experts specifiek voor deze casus relevante informatie verzameld.

Onderstaande Figuur 4 toont schematisch de stappen die zijn uitgevoerd om tot beantwoording van de onderzoeksvragen te komen.



Figuur 4 Schematisch overzicht onderzoeksmethode (stappen en volgordelijkheid daarvan)

Het onderzoek start breed, namelijk met drie stappen tegelijkertijd. We beginnen met het in kaart brengen van het huidige proces/werkwijze van het aanvraag- en uitgifteproces van identiteitsmiddelen in het binnenland en buitenland. Bij de aanvraag en uitgifte in het binnenland gaat dit om het proces wat zich afspeelt bij de gemeenten, bij de uitgifte van identiteitsmiddelen in het buitenland gaat dit om het proces dat valt onder het ministerie van Buitenlandse Zaken. De inventarisatie vindt plaats aan de hand van desk research en interviews met experts op het gebied van aanvraag en uitgifte van identiteitsmiddelen, identiteitsverificatie en -vaststelling. Denk hierbij aan medewerkers van de ministeries van Binnenlandse en Buitenlandse Zaken, de Rijksdienst voor Identiteitsgegevens (RvIG) en Dienst Wegverkeer (RDW). Zo kunnen we de huidige processen van identiteitsmiddelen in kaart brengen. Deze stap leidt uiteindelijk tot een 'baseline' van het huidige proces en vereisten (op hoofdlijnen) voor een hypothetische digitale versie 'op afstand'.

Parallel voeren we een eerste inventarisatie van technische oplossingen/diensten in de markt uit. Om er achter te komen welke digitale oplossingen er beschikbaar zijn voor identiteitsverificatie en -vaststelling of oplossingen die hieraan bij kunnen dragen, wordt desk research gedaan en gesproken met partijen die deze diensten aanbieden, of gebruik maken van deze diensten. Denk hierbij bijvoorbeeld aan commerciële aanbieders en de Nederlandse banken (verenigd in iDIN). Ook wordt gekeken naar hoe andere landen omgaan met de aanvraag en uitgifte van identiteitsmiddelen, en of zij een deel of het gehele proces online doen (inventarisatie internationale cases).

De voorgaande drie stappen komen samen in twee opvolgende stappen. De 'baseline' van het huidige proces en de gevonden technische oplossingen/diensten is voorgelegd aan

experts om erachter te komen wat de mogelijkheden en onmogelijkheden zijn van de digitale oplossingen. Op basis van de inventarisatie van de buitenlandse cases is een vergelijking gemaakt van de buitenlandse implementaties en de situatie in Nederland.

Vervolgens volgt de analyse van de (on)mogelijkheden voor online oplossingen. We gebruiken hierbij een afwegingskader. Dit afwegingskader is gevalideerd bij experts middels een (groeps)interview.

3 Huidig aanvraagproces

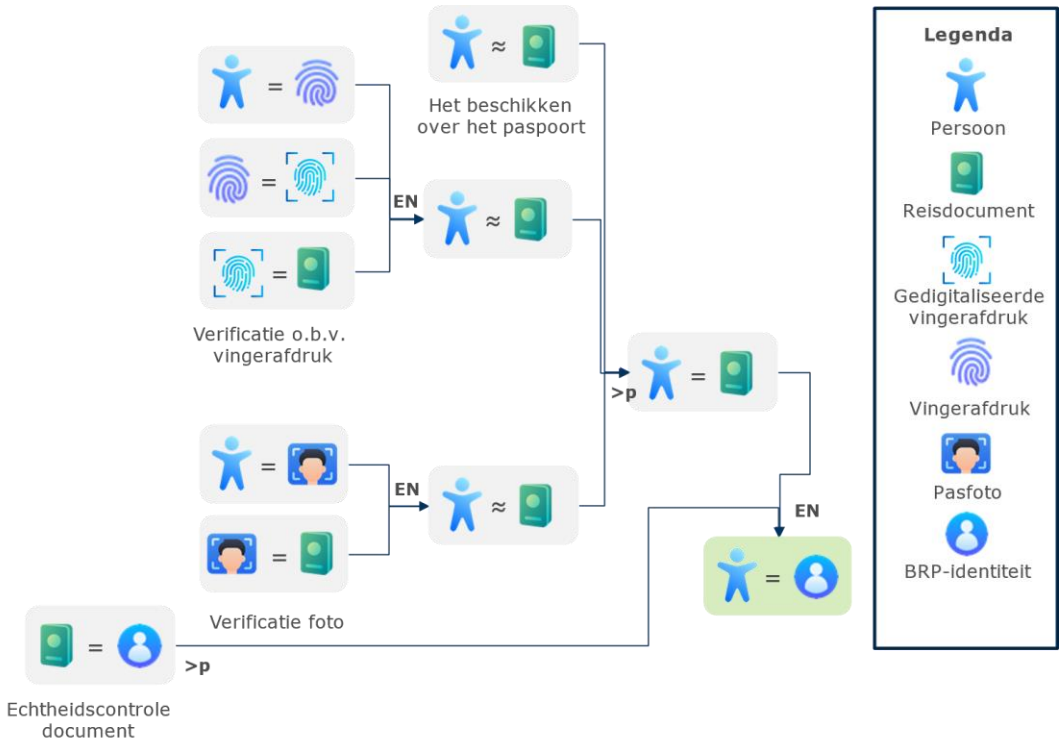
Om te kunnen beoordelen of (onderdelen van) het aanvraag- en uitgifteproces op een betrouwbare manier gedigitaliseerd kunnen worden is het van belang om eerst het huidige proces helder in kaart te brengen. Een identiteitsmiddel moet één keer voor de eerste keer aangevraagd worden. Sinds 2014 zijn Nederlandse paspoorten 10 jaar geldig. [2, p. art. 9 lid 1] Na de eerste aanvraag kunnen identiteitsmiddelen verlengd worden. Het normenkader wettelijke identiteitsmiddelen identificeert zes processtappen binnen het aanvraag- en uitgifteproces [5]:

1. Identiteitsverificatie van de aanvrager ten behoeve van de aanvraag
2. Verzamelen van relevantie biometrie van de aanvrager ten behoeve van de aanvraag (stap 1 en 2 samen: *inname*).
3. Beslismoment voor verstrekking van identiteitsdocument
4. Productie en personalisatie van het identiteitsmiddel (incl. de chip), gevolgd door ontvangst in de 'voorraad' (*inklaren*).
5. Uitgifte van het identiteitsmiddel (incl. identiteitsverificatie)
6. Intrekken en vervallen van het identiteitsmiddel en het registratieproces rond het identiteitsmiddel

3.1.1 Stap 1. Identiteitsverificatie van de aanvrager ten behoeve van de aanvraag

Bij de aanvraag voor een nieuw identiteitsmiddel vindt eerst een identiteitsverificatie van de aanvrager plaats. Deze verificatie wordt uitgevoerd door een *voor het innemen van een aanvraag gemachtigde (*hierna: *innemer*). De innemer kan een ambtenaar van een gemeente zijn, maar ook (in het buitenland) een externe dienstverlener.

In de figuur hieronder geven wij schematisch weer hoe de vertrouwensketen er uitziet. In deze figuur gaan we ervanuit dat de persoon, het document, de vingerafdruk, de foto en de identiteit in alle stappen gelijk blijft. Ook nemen we aan dat alle vergelijkingsstappen op betrouwbare wijze gebeuren.



Figuur 5: Vertrouwensketen bij het verifiëren van de identiteit van een aanvrager van een identiteitsmiddel

Bij identiteitsverificatie vindt eerst een echtheidscontrole plaats. Dit is onderaan in het schema weergegeven. Een Nederlands identiteitsmiddel bevat een aantal echtheidskenmerken [18] en het is aan de innemer in kwestie hoeveel en welke echtheidscontroles deze inzet om tot het benodigde betrouwbaarheidsniveau te komen. De persoonsgegevens in het identiteitsmiddel zijn gekoppeld aan een identiteit in de BRP. De identiteitsverificatie vindt vervolgens plaats via verschillende wegen. Ten eerste is het in bezit hebben van het identiteitsmiddel al indicatie dat de persoon bij de identiteit in het middel hoort: men gaat in het algemeen voorzichtig om met een identiteitsmiddel en draagt die niet zonder reden over aan een ander persoon. Vervolgens kan in de huidige werkwijze de innemer op verschillende manieren (al dan niet met behulp van apparatuur) verifiëren dat de persoon hoort bij de biometrische gegevens in het identiteitsmiddel. Bijvoorbeeld door middel van het checken van de vingerafdruk van de persoon met de vingerafdruk die is opgeslagen in het identiteitsmiddel (in de praktijk gebeurt dit niet of nauwelijks) of door de verschijning van de persoon en de foto die de persoon meeneemt te checken tegen de foto die is opgeslagen in het identiteitsmiddel. Een succesvolle combinatie van deze factoren leidt vervolgens tot het verbinden van de persoon aan het identiteitsmiddel met een zeker betrouwbaarheidsniveau. Hierdoor kan de natuurlijke persoon gekoppeld worden aan de identiteit uit de BRP. In deze keten is de kwaliteit van het uitgifteproces van het identiteitsmiddel niet meegenomen, net als de mate waarin de pasfoto en vingerafdruk uniek zijn. Deze beide factoren leiden tot een verandering in de zekerheid van het beschreven proces.

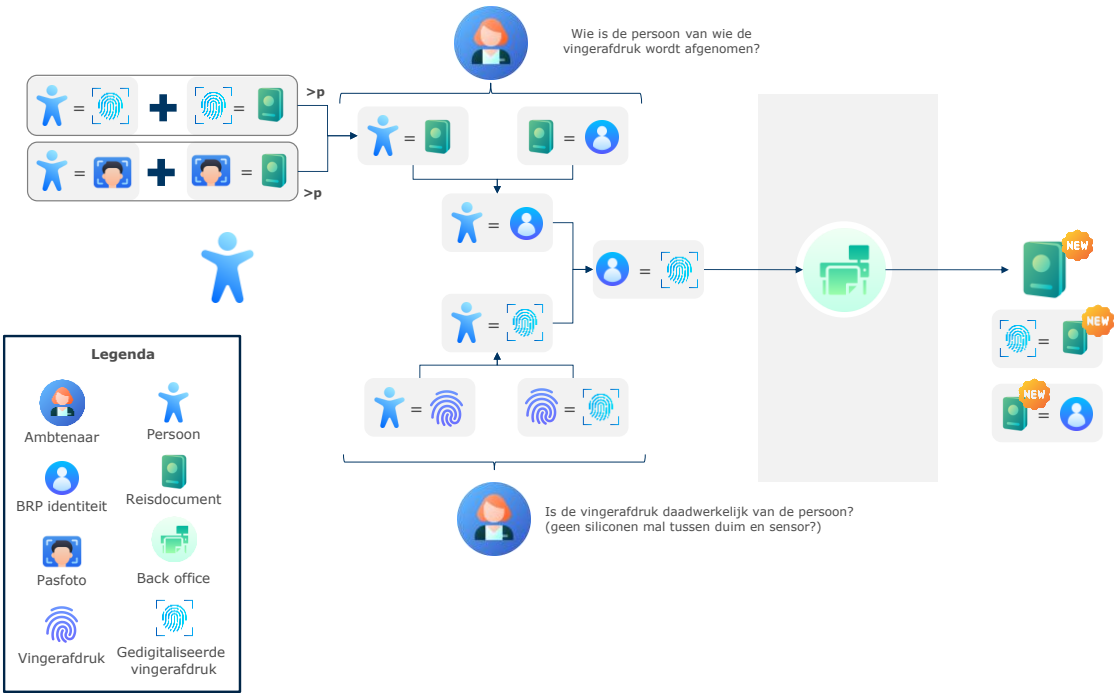
Naast de formele, gecodificeerde stappen die hierboven beschreven zijn, voeren de ambtenaren die betrokken zijn bewust of onbewust allerlei controles uit. Hun (getrainde) intuïtie zal bepalen in welke mate zij allerlei formele controles gaan uitvoeren. Voorbeeld: indien een aanvrager zijn eigen naam niet goed kan uitspreken, dan zal de innemer in functie direct onraad ruiken. Vervolgens zal de betrokken innemer in meer detail kijken naar de identificatie en wellicht aanvullende controles uitvoeren (zoals verificatie van vingerafdrukken). Dit lijkt wellicht niet zo relevant of evident, het is wel een fundamenteel verschil met digitale

systemen die een dergelijke intuïtie niet hebben. Een deel van deze 'intuïtieve' controles is uiteraard nog wel uitvoerbaar bij *gedeeltelijk* gedigitaliseerde oplossingen (bijvoorbeeld wanneer een videogesprek onderdeel uitmaakt van het aanvraagproces), al spelen daar nieuwe risico's, met name ten aanzien van *deep faking* (zie verderop).

3.1.2 Stap 2. Verzamelen van relevantie biometrie van de aanvrager ten behoeve van de aanvraag

Bij het aanvragen van een Nederlands paspoorten is op dit moment één verschijning vereist. Dit betekent concreet een fysieke ontmoeting met een innemer. Voor Europese identiteitskaarten zijn twee verschijningsmomenten voorgeschreven in de EU-wetgeving die van toepassing is op de identiteitskaarten en het daarop geplaatste digitale publieke identificatiemiddel. In de meeste gevallen (binnen Nederland) vindt een eerste verschijning veelal plaats bij het aanvragen van het identiteitsmiddel, en een eventuele tweede bij de uitgifte van het document.

Het verschijningsmoment heeft verschillende functies. Ten eerste voorkomt het vereisen van de fysieke ontmoeting diverse vormen van fraude (zo kan onder andere door de innemer worden vastgesteld dat de aanvrager daadwerkelijk een levend persoon is). Ten tweede wordt de identiteit geverifieerd zoals in de vorige stap is gedemonstreerd. Deze verificatie kan gebruik maken van de daadwerkelijke fysieke eigenschappen van de aanvrager. [5] De innemer heeft daarnaast de fysieke beschikking over eventuele bestaande identiteitsmiddelen, zodat alle mogelijke echtheidscontroles daarop kunnen worden uitgevoerd. Tijdens het eerste contactmoment wordt tot slot alle relevante biometrie verzameld ten behoeve van de aanvraag. Hieronder in Figuur 3 is weergegeven hoe dit proces op dit moment verloopt.



Figuur 6: Afname biometrie bij paspoort aanvraag

Eerst wordt (boven in het schema) de identiteitsverificatie van de vorige stap herhaald. Hier verifieert de innemer dat de persoon bij de vingerafdruk en de foto hoort en dat diezelfde vingerafdruk en foto overeenkomen met het gepresenteerde identiteitsmiddel. Als dat het geval is, dan kan met een bepaalde mate van zekerheid gezegd worden dat de persoon, met persoonsgegevens, bij de biometrische gegevens in het identiteitsmiddel hoort.

Voor een ongetraind persoon is het vaststellen dat een pasfoto behoort bij een persoon niet met voldoende zekerheid te doen. Ambtenaren die dit op regelmatige basis doen zijn hier vaak beter in dan ongetrainde personen.

Omdat het identiteitsmiddel gekoppeld is aan een identiteit, kan de persoon vervolgens gekoppeld worden aan die identiteit. Bij het verzamelen van de nieuwe biometrie, onder in het schema, staan de innemer, de vertrouwde apparatuur en het vertrouwde proces garant voor een correct verloop van dit proces. De innemer checkt of de vingerafdruk die op het apparaat geplaatst wordt ook daadwerkelijk van de persoon is (en of er bijvoorbeeld geen siliconen mal tussen zit), terwijl de apparatuur garandeert dat de uiteindelijk gedigitaliseerde vingerafdruk ook de vingerafdruk is die op het apparaat geplaatst werd. Door deze twee garanties kan dan met zekerheid gezegd worden dat de gedigitaliseerde vingerafdruk afkomstig is van de aanvrager. De verificatie stap koppelde eerder al een identiteit aan deze aanvrager en dus kan de nieuwe, gedigitaliseerde vingerafdruk gekoppeld worden aan een identiteit in de BRP. Voor de foto, handtekening en lengte vindt een soortgelijk proces plaats, waar de innemer checkt of de persoon hoort bij een factor (foto/handtekening/lengte) en vervolgens checkt of deze factor ook overeenkomt met de gedigitaliseerde versie.

Aanvragen zonder geldig 'oud' identiteitsmiddel

Wanneer de aanvrager geen 'oud', geldig identiteitsmiddel kan overleggen, moet de identiteit van de aanvrager op andere manieren worden vastgesteld. Dit kan op verschillende manieren plaatsvinden:

- Het opzoeken van informatie van eerdere aanvragen voor reis- en identiteitsdocumenten uit het gemeentelijke RAAS (indien nodig bij een andere gemeente). In het systeem zijn de oude aanvraagformulieren (met daarop diverse basisgegevens, een foto en handtekening) te vinden. De kwaliteit van de foto die op deze manier kan worden gevonden, is sterk wisselend, onder andere doordat de foto's veelal worden afgedrukt en daarna opnieuw worden gedigitaliseerd.
- Informatie uit de registers voor vreemdelingen, waarin onder andere basisgegevens en biometrie opgeslagen zijn.
- Andere bewijsstukken, waaronder geboorteaktes en buitenlandse paspoorten.

Van belang is dat de bovengenoemde methoden geen volledige zekerheid over de identiteit kunnen bieden. Voor de innemer en andere betrokkenen die de aanvraag in behandeling nemen zal een zo compleet mogelijk 'plaatje' moeten ontstaan van de identiteit, waarbij meerdere factoren worden gecombineerd en met elkaar moeten overeenstemmen.

Vaststellen Nederlandse nationaliteit

Voordat een paspoort kan worden afgegeven dient te worden vastgesteld of de aanvrager (nog) beschikt over de Nederlandse nationaliteit. Een Nederlander kan de Nederlandse nationaliteit verliezen wanneer deze vrijwillig een tweede of andere nationaliteit aanneemt en/of 13 jaar of langer buiten het Koninkrijk der Nederlanden of de EU woont met een dubbele nationaliteit, en het Nederlandse identiteitsmiddel niet tijdig verlengt. Een Nederlander kan ook zélf vrijwillig afstand doen van de Nederlandse nationaliteit. Automatisch verlies van de Nederlandse nationaliteit vindt nooit plaats voor personen die geen ándere nationaliteit hebben. [19] In het Nationaliteitenregister, dat wordt beheerd door de IND, worden alle wijzigingen aangaande de Nederlandse nationaliteit (op basis van onder andere afstandsverklaringen, verleningen, intrekkingen) geregistreerd. [20, p. art. 22 lid 1] Bij verlening van een identiteitsmiddel dient in dit register te worden gecontroleerd of de aanvrager het Nederlanderschap heeft verloren c.q. verleend heeft gekregen.

Paspoortsignaleringen

Aan sommige personen mag (tijdelijk) geen[7] paspoort worden verstrekt. Deze personen worden geregistreerd in het Register Paspoortsignaleringen (RPS), beheerd door RvIG. [21] Redenen voor opname in dit register kunnen onder andere zijn: meervoudige vermissing, het opzettelijk beschadigen van identiteitsmiddelen, (vermoeden van) fraude met identiteitsmiddelen, onttrekking van een opgelegde straf, faillissement, een publiekrechtelijke schuld, of vanwege een verzoek van de NCTV op grond van de nationale veiligheid.

Fraude

Fraudeurs zoeken (zonder hulp van een functionaris binnen het proces) de 'route met de minste weerstand'. Terwijl in de analyse het 'standaardproces' centraal staat is het vanuit het perspectief van de fraudeur niet evident dat zij via de standaardroute zullen proberen documenten aan te vragen. Dat zou immers vereisen dat bijvoorbeeld de controle op basis van de vingerafdrukken en/of pasfoto moet worden gemanipuleerd. In plaats daarvan is te verwachten dat fraudeurs liever een minder voorkomende procesroute volgen. Hiertoe zullen zij vanuit een uitzonderingssituatie proberen te starten, door bijvoorbeeld te beweren dat het eigen paspoort kwijt is geraakt. Als er wel hulp van binnenuit is, zou uiteraard via het gewone 'standaardproces' een frauduleus document kunnen worden bemachtigd.

3.1.3 Stap 3. Beslismoment voor verstrekking van identiteitsmiddel

Of de aanvraag voor een nieuw identiteitsmiddel gehonoreerd wordt, zou beslist moeten worden door een andere functionaris dan degene die het aanvraagproces overzien heeft (c.q. de innemer): het vier-ogen-principe. Dit om het besluit zo objectief mogelijk te houden en om intimidatie van ambtenaren te voorkomen.

3.1.4 Stap 4. Productie en personalisatie van het identiteitsmiddel (incl. de chip)

Voor het aanvraag- en uitgifteproces van paspoorten gebruiken de gemeenten een apart informatiesysteem genaamd het Reisdocumenten Aanvraag- en Archiefstation (RAAS). Iedere gemeente heeft zijn eigen RAAS en de gegevens worden alleen lokaal opgeslagen. [7]

Via het programma Verbeteren Reisdocumentenstelsel (VRS) wordt momenteel wel gewerkt aan een centraal systeem. In dit systeem moeten alle wereldwijde data van het RAAS worden overgeheveld, zodat digitaal inzage in aanvraaggegevens van andere uitgevende instanties mogelijk wordt. Ook moet in dit nieuwe systeem de signaleringscontrole automatisch uitgevoerd gaan worden. Uiteindelijk moet dit nieuwe systeem de RAAS'en volledig vervangen. [22]

Nu worden, na goedkeuring van de aanvraag, de gegevens uit de RAAS gebruikt om het paspoort en de chip te produceren. Het reisdocument zelf bevat alle persoonsgegevens en biometrische gegevens behalve de vingerafdruk, terwijl de chip alle leesbare gegevens plus de vingerafdruk bevat. Nadat alle data is geschreven naar en opgeslagen op de chip, wordt de chip 'vergrendeld'. Het is dan niet meer mogelijk om er extra informatie op te slaan. [23]

[7] Afwijking is onder zwaarwegende omstandigheden mogelijk (Rijksdienst voor Identiteitsgegevens, sd), maar beschouwen we in dit onderzoek als een zeldzame uitzondering.

3.1.5 Stap 5. Uitgifte van het identiteitsmiddel (incl. identiteitsverificatie)

Wanneer het identiteitsmiddel geproduceerd is kan het opgehaald worden bij de uitgifte-instantie of opgestuurd worden naar de aanvrager. Het uitgeven van een document mag (ook) worden gedaan door de innemer. In het buitenland gebeurt dit met enige regelmaat op kleinere locaties. Vanuit de wet- en regelgeving wordt slechts een functiescheiding opgelegd tussen *beheer* (van de gepersonaliseerde documenten) en uitgifte.[8] Bij de buitenlandse locaties is deze onverminderd van kracht: de beslissing om een document al dan niet uit te geven wordt in deze gevallen namelijk gemaakt door medewerkers in Den Haag, en niet door personeel op de buitenlandse locatie zélf.

Hoewel ophalen de norm is worden nieuwe documenten, met name in het buitenland, ook regelmatig opgestuurd naar de aanvrager. Dit gebeurt pas als het oude identiteitsmiddel ontvangen is (in het buitenland: op het consulaat of de ambassade of een externe dienstverlener). De aanvrager heeft hierbij een bezorgbedrijf gemachtigd en is zelf verantwoordelijk voor het vervoer van het identiteitsmiddel.

3.1.6 Stap 6. Intrekken en vervallen van het identiteitsmiddel en het registratieproces rond het identiteitsmiddel

Nadat het nieuwe identiteitsmiddel is opgehaald of verstuurd, wordt het oude identiteitsmiddel ongeldig gemaakt en worden de vingerafdrukken uit RAAS verwijderd. Voor het bewaren van de overige gegevens geldt een termijn van 16 jaar als het paspoort langer dan 5 jaar geldig is. [7]

3.2 Kwetsbaarheden huidige proces en mitigatie maatregelen

Op 8 juli 2022 rapporteerde de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer over de geconstateerde misstanden bij het verstrekken van paspoorten. [24] Het merendeel van deze misstanden betrof een afwijking in de procedure waarbij dezelfde ambtenaar verantwoordelijk was voor het 'inklaren' (ontvangen van een geproduceerd paspoort en deze toevoegen aan de 'voorraad') en het behandelen van de aanvraag van het paspoort. Dit gebeurde met name in gemeenten met minder dan 100.000 inwoners. Daarnaast werd geconstateerd dat in 181.500 gevallen een pasfoto die was afgekeurd door de programmatuur alsnog werd goedgekeurd door de ambtenaar, zonder dat deze daarbij een specifieke toelichting heeft opgegeven. Of deze afwijkingen hebben geleid tot frauduleuze uitgifte van identiteitsmiddelen is (nog) niet bekend. Er zijn echter wel tientallen gevallen bekend van onrechtmatig verkregen identiteitsbewijzen.

In de kamerbrief wordt een aantal oplossingen gepresenteerd om deze structurele problemen te verhelpen. [24] De maatregelen met relevantie voor het huidige onderzoek zijn:

1. Het programma **Verbeteren Reisdocumentenstelsel (VRS)**. VRS moet leiden tot twee centrale systemen, in plaats van de huidige, decentrale systemen op gemeente niveau. Dit moet de fout- en fraudegevoeligheid van het proces mitigeren.

2. **Modernisering Afname Biometrie**. Onderdeel van deze modernisering is het ter plekke afnemen van de pasfoto.[9] Hierdoor wordt het inleveren van een pasfoto op

[8] Zie Artikel 93 Paspoortuitvoeringsregeling Nederland 2001, lid 1 c, en Artikel 107 Paspoortuitvoeringsregeling Buitenland 2001, lid 1 c.

[9] Binnen Nederland wordt daarnaast onderzocht of erkende fotografen een rol kunnen (blijven) vervullen; in het buitenland is dit niet aan de orde.

papier (vaak een digitale foto die is afgedrukt) uitgefaseerd. Dit leidt naar verwachting tot een hogere kwaliteit van de foto en verlaagt de drempel voor een baliemedewerker om de foto af te keuren: er kan immers direct een nieuwe gemaakt worden.

3. **Aanpassing RAAS**. Binnen RAAS zal functiescheiding worden afgedwongen, waardoor de aanvraag en de uitgifte niet meer door eenzelfde persoon gedaan kunnen worden.

4 Technische oplossingen

In hoofdstuk 3 beschreven we de (voor dit onderzoek relevante) zes stappen in het huidige aanvraagproces. Deze stappen bestonden uit:

1. Identiteitsverificatie van de aanvrager ten behoeve van de aanvraag.
2. Verzamelen van relevante biometrie van de aanvrager ten behoeve van de aanvraag.
3. Beslismoment voor verstrekking van identiteitsmiddel. Hierbij wordt onder andere getoetst of de aanvrager beschikt over het Nederlanderschap, of de aanvrager gesignaleerd staat, et cetera.
4. Productie en personalisatie van het identiteitsmiddel (incl. de chip).
5. Uitgifte van het identiteitsmiddel (incl. de identiteitsverificatie).
6. Intrekken en vervallen van het identiteitsmiddel en het registratieproces rond het identiteitsmiddel.

Om dit proces vanuit perspectief van de aanvrager volledig op afstand te laten verlopen moeten in ieder geval de stappen 1, 2, 5 en 6 op afstand gedaan worden. Deze stappen bespreken we in het hoofdstuk hieronder. Voor stap 1 en 2 maken we onderscheid tussen een situatie waarin wel en waarin geen bestaand, geldig identiteitsmiddel beschikbaar is.

Stap 3 en stap 4 in het proces hoeven ten behoeve van dit doeleinde niet aangepast te worden (mits de aanvrager correct is geïdentificeerd) – deze vinden immers plaats in de 'backoffice' en vereisen geen interactie (specifiek geen verschijning) van de aanvrager. Bij stap 3 is uiteraard wel van belang dat wanneer de uitslag van de beslissing negatief is, er mogelijk een vervolgtraject start (wanneer bijvoorbeeld niet kan worden vastgesteld dat een persoon de Nederlandse nationaliteit bezit, zal deze persoon dit wellicht op een andere manieren kunnen aantonen). We gaan er van uit dat dit proces dan offline (fysiek) plaatsvindt.

4.1 Identiteitsverificatie op afstand met bestaand, geldig identiteitsmiddel

De eerste stap in het aanvraagproces van een identiteitsmiddel is de identiteitsverificatie van de aanvrager: *Bij welke identiteit in de BRP hoort de aanvrager?*[10] In het huidige proces heeft het de voorkeur om deze verificatie te doen op basis van een bestaand, geldig identiteitsmiddel. Als een geldig identiteitsmiddel niet beschikbaar is, dan zijn er (zoals in het vorige hoofdstuk beschreven) andere methoden beschikbaar. In de volgende paragraaf gaan we in op technische oplossingen die in situaties zouden kunnen worden ingezet waarbij géén bestaand (geldig) identiteitsmiddel voorhanden is.

In het huidige proces mét bestaand identiteitsmiddel verifieert de baliemedewerker de identiteit door een aantal stappen te doorlopen:

1. Beschikt de aanvrager over een identiteitsmiddel?
2. Is het identiteitsmiddel écht en geldig?
3. Komt het identiteitsmiddel overeen met de aanvragende persoon?
    a. In eerste instantie worden de basiskenmerken gecontroleerd.
    b. Als de basiskenmerken juist zijn wordt de foto vergeleken.

[10] Merk hierbij op dat het mogelijk is om wel een Nederlands paspoort te hebben, maar niet bent opgenomen in de BRP of RNI. Deze optie zien wij echter als een randgeval die wij hier buiten beschouwing zullen laten.

c. Bij twijfel kunnen de vingerafdrukken van de aanvrager worden vergeleken met de vingerafdruk die in het paspoort is opgeslagen.
d. Als er alsnog twijfel bestaat kunnen aanvullende technieken worden gebruikt, zoals het stellen van vragen, het opvragen van oude aanvragen voor identiteitsmiddelen, et cetera. We gaan er voor nu van uit dat deze uitzonderingen buiten het online proces vallen.

4. Welke identiteit (BRP) hoort bij de persoon en het identiteitsmiddel? Deze stap vindt plaats in de 'back office' en hoeft vanuit het perspectief van de aanvrager dus niet online te worden gebracht.

In deze paragraaf beschrijven we de technische oplossingen voor het op afstand (online) laten verlopen van de hierboven genoemde stappen.

4.1.1 Op afstand controleren of aanvrager over een écht en geldig identiteitsmiddel beschikt

In het reguliere aanvraagproces is het feit dat een aanvrager over een (mogelijk te vervangen) identiteitsmiddel beschikt een belangrijke aanwijzing voor de identiteit van de persoon. Het is uiteraard niet onmogelijk, maar zeker niet eenvoudig om andermans identiteitsmiddel te bemachtigen (waarbij dan uiteraard ook de biometrie en andere gegevens enigszins overeen zouden moeten komen). Om deze controle op afstand uit te voeren zien we een aantal mogelijkheden.

Technische oplossingen

Uitlezen van de MRZ

Een Nederlands identiteitsmiddel bevat een MRZ (Machine Readable Zone). Dit is een reeks letters en cijfers op het identiteitsmiddel, waarin gegevens opgenomen zijn die ook elders afgedrukt staan op het identiteitsmiddel, zoals de naam, geboortedatum, et cetera. [25] De MRZ bestaat uit twee of drie regels tekst onderaan het voorblad van een paspoort of de achterkant van een ID-kaart, en is internationaal gestandaardiseerd (zie Figuur 7). De MRZ is wereldwijd gestandaardiseerd door ICAO in 'document 9303' [26].

Het uitlezen geschiedt via een camera, op basis van OCR (Optical Character Recognition). Het lettertype dat gebruikt wordt voor de MRZ is zeer geschikt voor digitale herkenning en relatief lastig te manipuleren. In de MRZ zitten tevens een aantal controlegetallen waarmee berekend kan worden of de data in de MRZ correct is of dat de code aangepast is. Desondanks bieden deze controlegetallen geen garantie van integriteit: het controlegetal kan eenvoudig opnieuw worden berekend voor een aangepaste reeks gegevens. [27]

De MRZ-gegevens kunnen, vanwege het ontbreken van een methode om deze op afstand te authentiseren, hoogstens worden gebruikt om bijvoorbeeld een formulier met gegevens automatisch in te vullen. Het uitlezen van de MRZ via de camera van (bijvoorbeeld) een smartphone van de aanvrager biedt geen hoge mate van betrouwbaarheid. Hoogstens zouden algoritmes voor detectie van manipulatie van het beeld en visuele controles van overige echtheidskenmerken kunnen worden toegepast.

Betrouwbaarheid van eindgebruikersapparaten

Vanuit perspectief van digitale veiligheid zijn eindgebruikersapparaten in principe 'onvertrouwd'. Omdat een eindgebruiker fysieke toegang heeft tot een apparaat kan deze in principe zelf modificaties uitvoeren die op afstand niet te detecteren zijn. Er zijn inmiddels diverse technologieën beschikbaar waarmee de mate van vertrouwen in (eindgebruikers)apparaten echter desondanks sterk kan worden verhoogd.

Remote attestation

Middels **remote attestation** kan op afstand kan worden geverifieerd dat een apparaat bepaalde (ongewijzigde) software uitvoert. Een voorbeeld is de TPM-chip die in veel PC's aanwezig is – deze kan cryptografisch aantonen dat bepaalde systeemsoftware actief is. [28] Een meer geavanceerde implementatie is SGX voor Intel-processoren. Deze wordt onder andere gebruikt door Signal om aan gebruikers te kunnen aantonen dat de software die op de servers van Signal draait, een specifieke authentieke versie is, die geen 'achterdeur' bevat. [29] De technologie lijkt anno 2022 nog niet helemaal waterdicht; zo zijn er diverse zwakheden gevonden in Intel's implementatie van SGX (waaronder [30]).

Secure boot

Met **secure boot** kan worden gezorgd dat alleen een door de fabrikant ondertekend besturingssysteem kan worden opgestart op een apparaat [31]. Zo wordt bij recente iPhones gecontroleerd of de systeemsoftware is voorzien van een handtekening van Apple, en is het in theorie niet mogelijk om andere (of aangepaste) systeemsoftware te gebruiken. [32] Vergelijkbare beveiliging is te vinden op diverse Android-, macOS- en Windowsapparaten.

Secure boot is over het algemeen gebaseerd op controle van cryptografische handtekeningen die is 'ingebakken' in de processor van het apparaat. In het geval van de iPhone controleert deze onwijzigbare 'boot ROM' de handtekening van het besturingssysteem, en controleert het besturingssysteem vervolgens de handtekeningen (en toegangsrechten) van geïnstalleerde apps. Ondanks alle beveiligingen worden er nog regelmatig beveiligingslekken gevonden in iOS en Android (in het besturingssysteem en/of de onderliggende hardware) die aanpassing van de systeemsoftware mogelijk maken (een 'jailbreak' of 'root').

Hardware Security Modules (HSM)

Met **HSM's** (in consumentenapparatuur bekend als **TPM-chip** of **Secure Enclave** [33]) kunnen digitale sleutels veilig worden opgeslagen op eindgebruikersapparaten, waarbij het nagenoeg onmogelijk is deze te kopiëren. Dergelijke oplossingen zijn vergelijkbaar met de chip op bijvoorbeeld een betaalkaart, SIM-kaart of fysiek authenticatietoken [34].

Technisch gezien is dit op smartphones, tablets en laptops veelal geïmplementeerd middels een aparte chip of deel van een chip waarop afgeschermde software draait, en die alleen op specifieke manieren voor specifieke taken is te bereiken vanuit de applicatiesoftware. De HSM staat (veelal na controle van een pincode en/of biometrie) het gebruik van een cryptografische sleutel toe, voor bijvoorbeeld het ondertekenen van een digitaal bericht, maar voorkomt dat de geheime sleutel de HSM verlaat (deze kan dus niet worden gestolen). De HSM voorkomt daarnaast manipulatie door een lokale aanvaller (de chip is 'tamper proof' uitgevoerd, het aantal pogingen voor het invoeren van een onjuiste pincode is gelimiteerd, et cetera).

Secure hardware pairing

In sommige apparaten worden onderdelen voorzien van een cryptografische handtekening. De applicatieprocessor kan daarmee controleren of het aangesloten component authentiek en origineel is (de handtekening moet dan afkomstig zijn van de fabrikant) en/of het onderdeel verwisseld is. Dit wordt onder andere toegepast bij iPhones die zijn voorzien van een vingerafdruk- of gezichtsscanner. [35] [32] Manipulatie van de afbeelding die een gezichts- of vingerafdrukscanner maakt wordt daarmee een stuk ingewikkelder.

Figuur 7: Machine Readable Zone paspoort (bron afbeelding: [klippa.com])

NFC-chip (eMRTD)

In recente identiteitsmiddelen bevindt zich een chip die draadloos via NFC (Near-field Communication) kan worden benaderd. Een identiteitsmiddel met zo'n chip wordt ook wel een eMRTD (Electronic Machine Readable Travel Document) genoemd. Identiteitsmiddelen die zijn voorzien van een chip zijn te herkennen aan een specifiek logo (zie Figuur 8). De werking van eMRTD's is wereldwijd gestandaardiseerd door ICAO in een supplement op 'Document 9303' [26].

Figuur 8: NFC chips Nederlands paspoort en identiteitsbewijs (bron afbeelding: [privacy-web.nl])

De NFC-chip accepteert commando's die worden verzonden door een uitleesapparaat en stuurt in reactie gegevens terug. Via deze weg kan een willekeurige NFC-lezer de gegevens die ook zijn opgenomen in de MRZ (*Machine Readable Zone*) van een identiteitsmiddel uitlezen. Deze functionaliteit wordt op dit moment gebruikt door apps als de DigiD ID-check, waarmee een (zeer beperkte) controle van het identiteitsmiddel kan worden uitgevoerd. [36]

Om te voorkomen dat een identiteitsmiddel zonder medeweten van de houder wordt uitgelezen, zijn de niet-openbare gegevens (vanaf paspoorten met modelnummer eindigend op 6 of hoger, uitgegeven vanaf medio 2022 [37]) aanvullend beveiligd met een pincode. Deze pincode is (alleen) bekend bij de houder van het paspoort (deze wordt verstrekt bij afgifte van het paspoort).[11] Bij het uitlezen van een paspoort wordt de pincode gecontroleerd door de paspoortchip, die de gegevens alleen zal prijsgeven wanneer de juiste pincode is ingegeven. Het gehanteerde protocol is PACE (*Pasword Authenticated Connection Establishment*) [38].

Authenticatie van de gegevens op de chip

De gegevens die zijn opgeslagen op de chip van het identiteitsmiddel worden vergezeld van een digitale handtekening, die eveneens kan worden uitgelezen. Aan de hand van de digitale handtekening en de certificaten van de bevoegde autoriteiten kan worden gecontroleerd of de digitale handtekening klopt (en daarmee of ze authentiek zijn). De certificaten van de bevoegde autoriteiten hoeven technisch gezien niet geheim te zijn. [39] Figuur 9 toont het ondertekenen en verifiëren van gegevens in de paspoortchip.

[11] De standaard voorziet naast een pincode ook in een toegangscode die op de kaart zelf is afgedrukt (*Card Access Number*) en een sleutel die is afgeleid van de MRZ-inhoud.

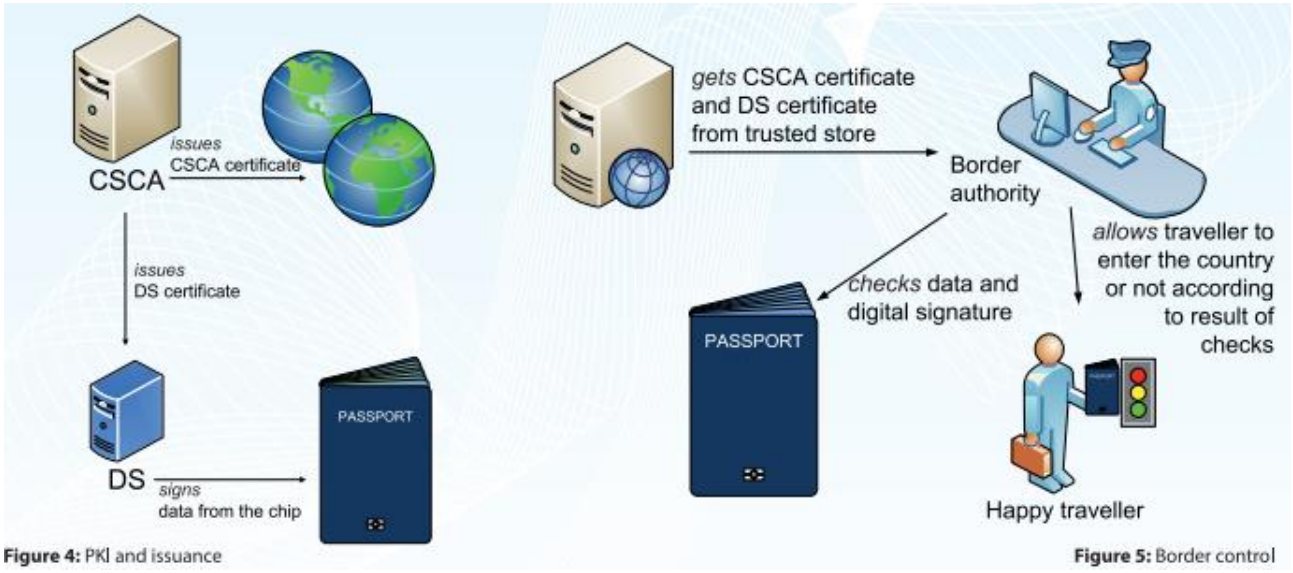


Figure 4: PKI and issuance

Figure 5: Border control

Figuur 9 Weergave van de wijze waarop gegevens in een eMRTD worden ondertekend (links) en worden uitgelezen (rechts) (bron afbeelding: [icao.int])

In Figuur 9 vindt een 'passieve' controle plaats: de grenswacht controleert op basis van controle van cryptografische handtekeningen of het certificaat in het reisdocument (uiteindelijk) is ondertekend door een 'vertrouwd' overheidscertificaat. Hiernaast is ook een 'actieve' controle denkbaar: hierbij legt (het controle-apparaat van) de grenswacht contact met de certificaatuitgever (Nederlandse overheid) om (aan de hand van het serienummer en/of de publieke sleutel van het certificaat) te controleren of het certificaat in het paspoort nog geldig is. Wanneer geen verbinding beschikbaar is, en/of het (vanuit privacy-oogpunt) niet wenselijk is dat de overheid op de hoogte is van alle controlemomenten, kan (ook) worden gewerkt met 'certificate revocation lists' (lijsten van ingetrokken certificaten) zoals ook toegepast voor TLS-certificaten. [40]

Bij het uitlezen van een eMRTD kunnen zich diverse uitzonderingen voordoen, zoals een chip die niet functioneert. In de ICAO-standaard wordt uitgewerkt hoe hiermee dient te worden omgegaan (Figuur 10). De stappen uit dit schema zouden in een scenario op afstand uiteraard allemaal moeten worden vertaald, waarbij een handmatige fysieke inspectie betekent dat het onlineproces staakt en moet worden teruggevallen op een persoonlijke verschijning.

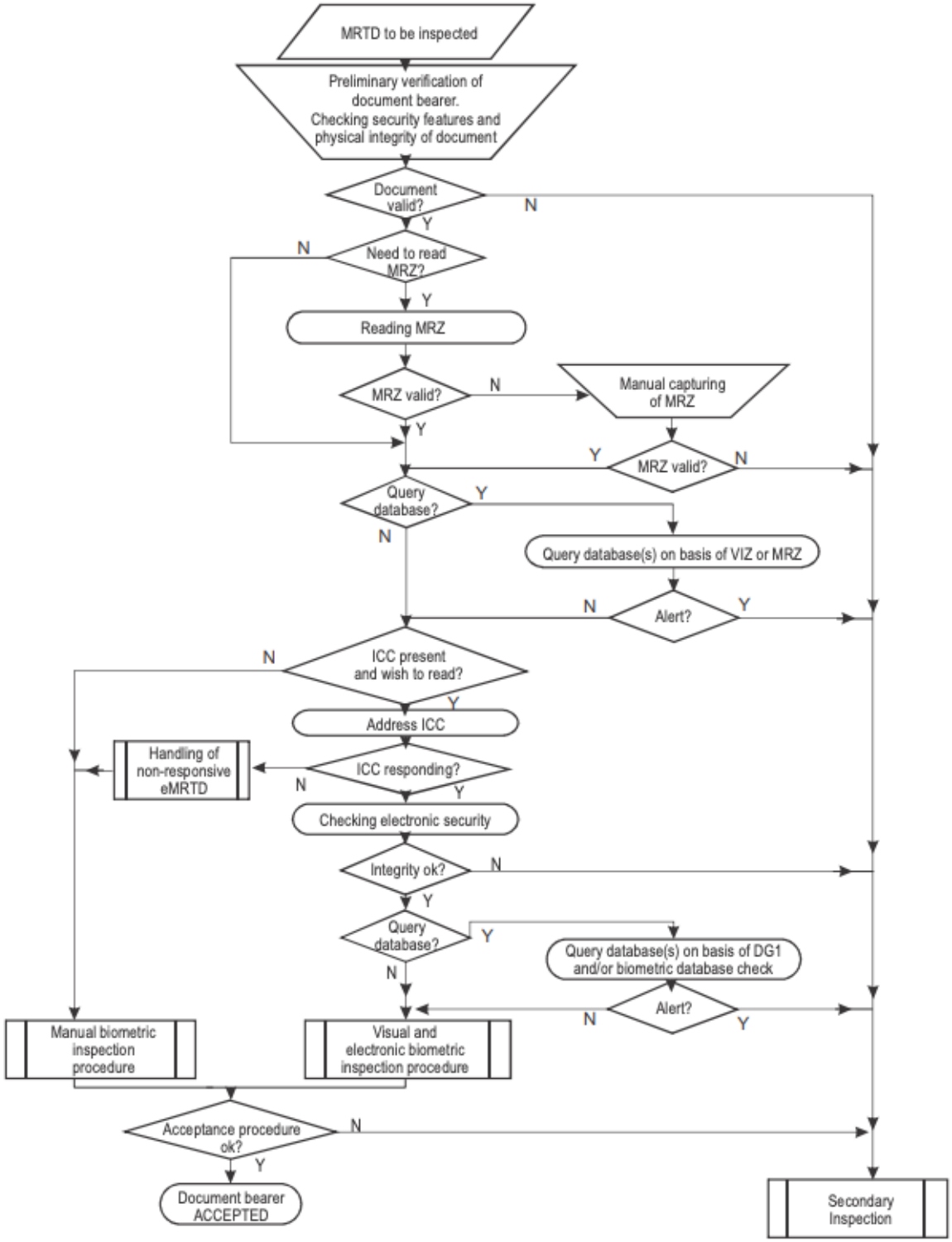


Figure A-2. eMRTD reading process

Figuur 10 Inspectieproces voor eMRTD's [41]

Op basis van het uitlezen van digitaal ondertekende gegevens uit de chip van een identiteitsmiddel via NFC kan met hoge betrouwbaarheid worden vastgesteld dat een aanvrager de beschikking heeft over een geldig identiteitsmiddel.

Door het uitlezen van de NFC-chip kan nog niet worden gewaarborgd dat de houder van het identiteitsmiddel hier toestemming voor heeft gegeven, tenzij wordt gewerkt met een additionele pincode (niet de CAN-code[12]) die alleen bij de houder bekend is (op basis van PACE en moderne identiteitsmiddelen). In dat geval kan hoogstens sprake zijn van dwang of van een lek in de geheimhouding (doordat er bijvoorbeeld iemand meekeek over de schouder).

Om dit proces op afstand plaats te kunnen laten vinden bij de aanvrager van een nieuw identiteitsmiddel is het een randvoorwaarde dat de aanvrager beschikt over een NFC-lezer voor het uitlezen van het huidige identiteitsmiddel. Een groot deel van de smartphones beschikt over een NFC-lezer; wereldwijd zouden er in 2018 ongeveer 2 miljard mobiele apparaten over NFC beschikken [42] van de in totaal ongeveer 12-13 miljard in datzelfde jaar. [43]. Daar komt bij dat Nederlanders over het algemeen over een moderne smartphone beschikken. In-store betalen met een mobiele telefoon, dat ook NFC-functionaliteit vereist, is in Nederland eveneens in opmars. [44]

Optisch controleren van het identiteitsmiddel

Een derde mogelijkheid is het 'optisch' controleren van het identiteitsmiddel. Hierbij wordt de aanvrager gevraagd het identiteitsmiddel te laten zien voor de camera. Op basis van de beelden zou de authenticiteit van het identiteitsmiddel kunnen worden gecontroleerd.

Het verifiëren van de authenticiteit van een identiteitsmiddel zou kunnen worden gedaan door te kijken naar de echtheidskenmerken van het identiteitsmiddel, zoals hologrammen. Om manipulatie moeilijker te maken zou de aanvrager kunnen worden gevraagd het identiteitsmiddel op een bepaalde manier te bewegen. Daarnaast kan gebruik worden gemaakt van wisselende lichtomstandigheden, die kunnen worden gecreëerd door bepaalde patronen op het scherm van de aanvrager te laten zien. Op basis van *computer vision*-algoritmen kan dan, ondanks de grote variatie in condities en bijvoorbeeld camera-eigenschappen, worden bepaald hoe waarschijnlijk het is dat het identiteitsmiddel reageert als een 'echt' identiteitsmiddel.

Op zichzelf zijn camerabeelden fundamenteel gezien relatief eenvoudig te manipuleren. Naast 'analoge' manipulatie (trucage 'voor de camera') kan het vaak ook in het digitale domein: er zijn diverse softwarepakketten beschikbaar die een virtuele 'webcam' installeren op een computer, waarvan de beeldgegevens (zelfs live) zouden kunnen worden gemanipuleerd. [45] De eerder toegelichte technologieën op het gebied van *remote attestation* en *secure hardware pairing* kunnen hierbij mogelijk een rol spelen: deze kunnen voorkomen dat het camerabeeld/de gezichtsscan in het digitale domein wordt gemanipuleerd.

Net als het *deep faken* van gezichten zouden ook de echtheidskenmerken van een identiteitsmiddel kunnen worden gemanipuleerd. Het is relatief eenvoudig, op basis van technologieën die worden gebruikt en ontwikkeld voor *augmented reality*, om op een blanco document dat lijkt op een identiteitsmiddel een digitaal beeld te projecteren van een 'echt' identiteitsmiddel.

---

[12] *Card Access Number.* Dit nummer is afgedrukt op identiteitskaarten uitgegeven vanaf 4 januari 2021 en wordt gebruikt als wachtwoord om een veilige verbinding te kunnen opzetten tussen een inspectieapparaat en de chip in de kaart. (Raad voor Identiteitsgegevens, 2021) Het doel hiervan is om te voorkomen dat met de chip wordt verbonden zonder dat de houder van de kaart dit doorheeft (om verbinding te maken moet de voorkant van de kaart immers kunnen worden bekeken). Omdat de code is afgedrukt op de kaart kan deze niet dienen als aanwijzing dat de houder van de kaart aanwezig was c.q. toestemming geeft voor uitlezen van de gegevens.

Conclusie

De besproken methoden voor het verifiëren van de beschikking over, en echtheid van een identiteitsmiddel kennen ieder specifieke voor- en nadelen. Onderstaande Tabel 3 toont een vergelijking van de verschillende oplossingen op de diverse aspecten.

Tabel 3 Eigenschappen van technische oplossingen voor het controleren van de aanwezigheid en echtheid van een bestaand identiteitsdocument bij een aanvraag

Oplossing / Aspect	MRZ uitlezen via camera	NFC-chip uitlezen (eMRTD)	Optische controle via camera
Gegevens uitlezen voor automatisch invullen/opzoeken	Mogelijk	Mogelijk en betrouwbaar	Mogelijk
Echtheid identiteitsmiddel en authenticatie inhoud	Onbetrouwbaar	Betrouwbaar	Betrouwbaarheid afhankelijk van kwaliteit 'faking' versus kwaliteit 'fake-detectie'.
Aanwezigheid van aanvrager	Niet te controleren	Enigszins te controleren (indien PACE, code is alleen bekend bij aanvrager, en aanvrager draagt code niet over)	Enigszins te controleren
Vrijwilligheid van aanvrager	Niet te controleren	Enigszins te controleren (indien PACE en aanvrager kan weigeren de code af te geven)	Enigszins te controleren, met name indien interactief (opdrachten of gesprek)
Vereiste hard- en software	Smartphone/computer met camera	Smartphone/computer met camera en NFC-lezer	Smartphone/computer met camera

Op basis van Tabel 3 stellen we vast dat het uitlezen van de NFC-chip de meeste zekerheid biedt over de aanwezigheid van het identiteitsmiddel. Daarnaast geeft de digitale handtekening zekerheid over de inhoud van het identiteitsmiddel. Om deze oplossing te kunnen gebruiken heeft de aanvrager echter een apparaat nodig dat is voorzien van een geschikte NFC-lezer. Daarnaast biedt de methode beperkte garanties als het gaat om de aanwezigheid van de aanvrager zélf en de vrijwilligheid waarmee de aanvrager een aanvraag doet. De andere methoden werken op basis van camerabeelden – hiervoor geldt dat deze in theorie altijd te manipuleren zijn en dus nooit sprake zal zijn van volledige betrouwbaarheid.

Het combineren van methoden lijkt dan ook een voor de hand liggende oplossing. Wanneer een aanvrager gedurende een kort tijdsbestek vanaf dezelfde computer (binnen dezelfde aanvraagsessie) zowel geldige gegevens afkomstig uit een NFC-chip, als camerabeelden van het paspoort en de aanvrager, als camerabeelden van de MRZ kan produceren, is een hoge mate van betrouwbaarheid bereikt. Desondanks zal (net als in het huidige aanvraagproces) nooit sprake *kunnen* zijn van volledige zekerheid.

4.1.2 Overeenkomst tussen 'oud' identiteitsmiddel en aanvrager vaststellen op afstand op basis van foto en/of videogesprek

Wanneer bij een online aanvraag een bestaand identiteitsmiddel beschikbaar is, kan dit worden gebruikt voor identificatie. De vraag daarbij is hoe wordt gecontroleerd dat het identiteitsmiddel overeenkomt met de aanvrager. Aan de balie wordt dit bijvoorbeeld gedaan door de pasfoto en de persoonsgegevens te vergelijken met de uiterlijke kenmerken van de persoon. Daarnaast zou de baliemedewerker bijvoorbeeld ook nog de vingerafdruk uit de chip kunnen vergelijken met die van de persoon of verhelderende vragen stellen.

Dit proces van *stapelen* kan ook online gebeuren. Zo zou via een selfie check en liveness detection de pasfoto uit het oude identiteitsmiddel vergeleken kunnen worden met de aanvrager en door middel van videobellen verder controlerende vragen gesteld kunnen worden. Ook zijn er nog additionele mogelijkheden om de identiteit via andere wegen te verifiëren.

Selfie check

Komt de aanvrager overeen met de pasfoto op het identiteitsmiddel? Nadat de data uit de NFC-chip is gelezen kan een aanvrager gevraagd worden om een selfie te maken en te uploaden. Deze selfie kan dan vergeleken worden met de foto die opgeslagen is op de chip via face-matching algoritmes. Aanbieders van online verificatie-oplossingen zullen ten dele andere algoritmes implementeren, maar uit de vergelijking van de twee afbeeldingen zal een *similarity score* komen. Deze *similarity score* geeft aan in hoeverre de twee gezichten overeenkomen. Als de foto's van een hoge kwaliteit zijn, kunnen de foutmarges onder de 0,2% liggen. [46] Alternatief zouden de foto en de selfie ook nog door een baliemedewerker vergeleken kunnen worden.

Door de aanvrager te vragen om met het identiteitsmiddel op de foto te gaan, kan een hogere mate van zekerheid worden verkregen over de vraag of de aanvrager daadwerkelijk over het identiteitsmiddel beschikt, aanwezig is bij de aanvraag, en deze de aanvraag vrijwillig uitvoert. Op online fora als Reddit worden vergelijkbare methoden gebruikt om te verifiëren dat een foto van een persoon met toestemming van die persoon wordt gepost. [47] Ook van notarissen in Nederland is bekend dat zij in sommige gevallen gebruik maken van foto's van een persoon met een overeenkomst en een identiteitsmiddel voor het op afstand ondertekenen daarvan. Let wel dat deze methode kan worden omzeild middels 'deep fakes' (zie verderop).

Liveness detection

Liveness detection moet zogenaamde *spoofing attacks* tegengaan. Met spoofing attacks wordt getracht om met een replica een persoons unieke biometrie te imiteren. Deze spoofing attacks worden steeds geavanceerder en de liveness detection checks moeten dus continue blijven evolueren. Kwaadwillende personen kunnen bijvoorbeeld door middel van geavanceerde 2- of 3D maskers de aanvrager imiteren of door middel van *deep fakes*.

Deep fakes

Er zijn drie verschillende vormen van deep fakes die gebruikt kunnen worden, namelijk face swap, face sync en GAN-netwerken. [48] Face swap is een techniek waarmee je een gezicht op die van iemand anders plakt. Bij face sync wordt iemands gezicht gesynchroniseerd. Wat de maker met zijn gezicht doet, kan hij de ook een ander gezicht laten doen. GAN-netwerken leren hoe een gezicht eruitziet en genereren vervolgens kunstmatige gezichten. Er is open sourcesoftware beschikbaar waarmee real-time deep fakes kunnen worden gemaakt van een gezicht. [49]

Om deze deep fakes te detecteren kunnen geavanceerde gezichtherkenningsalgoritmes al voldoende zijn, maar er kunnen ook nog verdergaande checks gedaan worden. Een aantal voorbeelden uit de praktijk hiervan zijn (niet uitputtend): [50]

1. *Flashes.* De manier waarop het gezicht het licht reflecteert kan aantonen of het een echt gezicht is of bijvoorbeeld een masker.
2. *Pupillen en andere reflexen.* Het verwijden van de pupil in reactie op een fel licht kan een reflex zijn die bepaalde *spoofs* niet zullen hebben.
3. *Challenge-response.* Vragen of de aanvrager een dansje doet, kan knipperen of lachen kan aantonen dat het geen video-aanval is. Deze methode wordt bijvoorbeeld toegepast door datingapps. [51]

Uiteindelijk zal ten aanzien van 'deep fakes' en liveness detectie een kat-en-muisspel ontstaan tussen aanvaller en controleur. De algoritmes voor het genereren van *deep fakes* (*Generative Adversarial Networks*) zijn zelfs fundamenteel gebaseerd op dit principe. [52] Een genererend model wordt 'getrained' om een 'detector' (die 'fake' onderscheid van echte foto's) te omzeilen. Hoe beter de beschikbare technologie voor het detecteren van 'fakes', hoe beter in theorie de genererende modellen kortom kunnen worden gemaakt. Hetzelfde patroon is in bredere zin observeerbaar in het domein van digitale veiligheid. [53]

4.1.3 Overeenkomst tussen 'oud' identiteitsmiddel en aanvrager vaststellen op afstand op basis van vingerafdruk

Wanneer een identiteitsmiddel wordt verlengd en er twijfels bestaan over de identiteit van de aanvrager, kan gebruik worden gemaakt van het feit dat het te vervangen identiteitsmiddel biometrische gegevens bevat, opgeslagen op de chip die ingebouwd is in het identiteitsmiddel. Alle Nederlandse gemeenten, ambassades en consulaten en de uitgevende instanties in het Caribisch deel van het Koninkrijk beschikken over apparatuur om deze vingerafdruk uit te lezen uit het identiteitsmiddel via de daarin gebouwde chip. [10] De chip kan alleen worden uitgelezen door instanties die daarvoor geautoriseerd zijn. Nederland slaat geen (bij een identiteitsmiddel afgegeven) vingerafdrukken op in een centraal register. Dat maakt de in een identiteitsmiddel opgeslagen vingerafdruk de enige referentie waarmee eventueel identiteitsverificatie op basis van een vingerafdruk zou kunnen plaatsvinden.

Bij een online aanvraagproces zou de vingerafdruk in het te vervangen identiteitsmiddel kunnen worden gebruikt als referentie bij het vaststellen van de identiteit. De aanvrager geeft ter plekke een vingerafdruk af, die daarna kan worden vergeleken met de in het oude identiteitsmiddel opgeslagen vingerafdruk. Als er een overeenkomst is, geeft dit aanvullende zekerheid over de identiteit van de aanvrager. Daarnaast kan zo worden vastgesteld dat de nieuw aangeleverde biometrie voldoende lijkt op de oude biometrie. In theorie zou ook de oude biometrie kunnen worden 'hergebruikt' voor het nieuwe paspoort (bijvoorbeeld wanneer de vingerafdrukscanner van de aanvrager niet voldoet aan de eisen die aan de opgeslagen vingerafdruk worden gesteld, maar wel goed genoeg is om een vergelijking te maken, en om vast te stellen dat de vingerafdruk niet substantieel gewijzigd is), maar onderzoek van de Universiteit Twente heeft uitgewezen dat (voorlopig) biometrie slechts 11 jaar houdbaar is. [13]

Technische invulling

De vingerafdruk in een Nederlands identiteitsmiddel van de tweede generatie [54] wordt als 'digitale zwart-wit foto' opgeslagen. Hiervoor wordt gebruik gemaakt van het WSQ (Wavelet Scalar Quantization)-formaat. [55] Dit is een compressie-algoritme dat specifiek is ontworpen voor afbeeldingen van vingerafdrukken (het gebruiken van bekendere formaten, zoals JPEG, zou ertoe kunnen leiden dat essentiële details van de vingerafdruk onduidelijk

worden). Ondanks het feit dat het een specifiek formaat betreft wordt gebruik gemaakt van dezelfde principes als de meer gangbare compressieformaten. Technisch gezien moet een willekeurige softwareontwikkelaar in staat zijn om, op basis van de open standaard, vingerafdrukken te lezen uit en weg te schrijven naar het WSQ-formaat.

De WSQ-afbeelding van de vingerafdruk is opgeslagen in eMRTD's. Het uitlezen van gegevens uit deze chip is in het voorgaande reeds toegelicht. Om toegang te krijgen tot beschermde gegevens, zoals de vingerafdruk, is hierbij echter aanvullend wederzijdse authenticatie noodzakelijk. Met wederzijdse authenticatie wordt bedoeld dat zowel (1) de chip in het identiteitsmiddel vaststelt dat deze wordt uitgelezen door een geautoriseerde uitlezer, als (2) dat de uitlezende partij vaststelt dat de gegevens authentiek zijn (dat wil zeggen: de gegevens zijn door een bevoegde autoriteit in het identiteitsmiddel gezet en sindsdien niet meer gewijzigd).

Authenticatie van de uitlezer

Voordat de chip in het identiteitsmiddel beschermde gegevens zal verzenden aan een uitlezen wordt gecontroleerd of de uitlezer beschikking heeft over een zogenaamde digitale sleutel. Met een digitale sleutel kan een bericht worden 'ondertekend', zodanig dat de ontvanger kan vaststellen dat degene die het bericht ondertekende moet hebben beschikt over de (geheime) digitale sleutel. De technische uitdaging hierbij is dat de digitale sleutel te allen tijde geheim moet blijven: iedereen die over de sleutel beschikt zou immers willekeurige berichten kunnen ondertekenen. Daarnaast moet de digitale 'handtekening' zodanig zijn dat deze slechts één keer kan worden gebruikt (anders zou je met hetzelfde ondertekende bericht meerdere paspoorten kunnen uitlezen) en niet te manipuleren zijn.

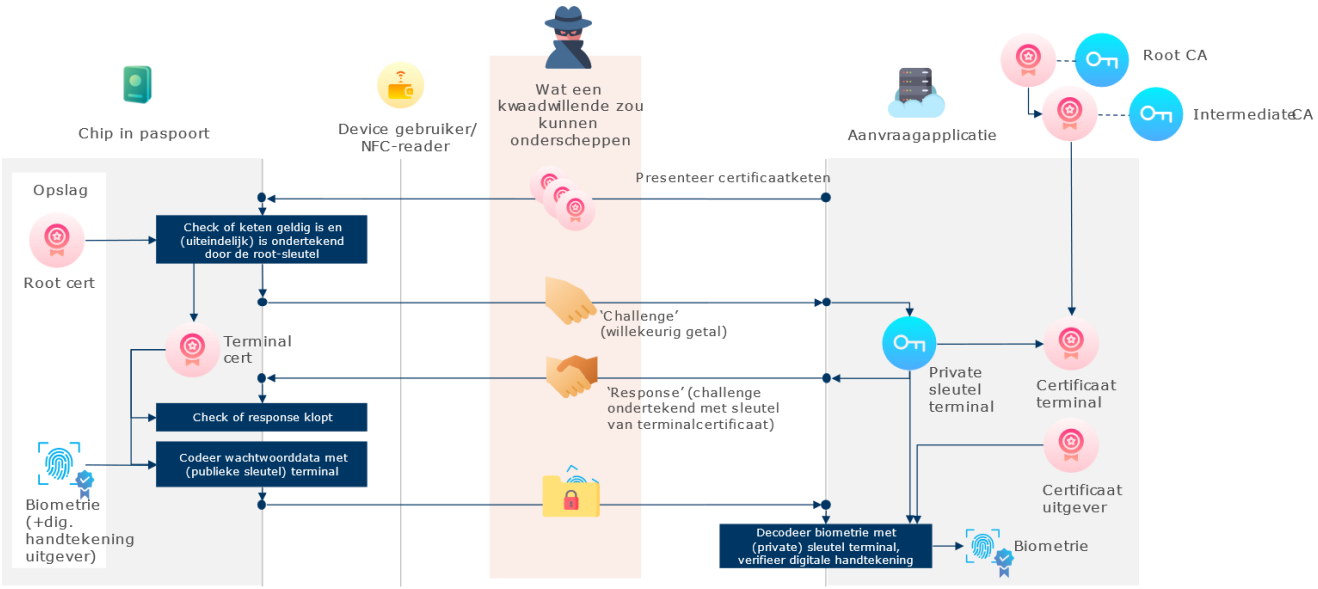
Omdat de communicatie tussen de uitlezer en de chip in principe af te luisteren is, zijn speciale protocollen ontwikkeld om deze garanties te kunnen bieden. De Nederlandse chips implementeren hiertoe een Duitse standaard (BSI-TR-03135, DOC9303 [38]). Deze standaard definieert een aantal protocollen, waaronder BAC (Basic Access Control) en EAC (Extended Access Control). Op hoofdlijnen werkt het uitlezen van gevoelige gegevens als volgt:

1. De aanvrager legt het identiteitsmiddel op een uitleesapparaat
2. Het uitleesapparaat genereert een verzoek tot uitlezen van de gevoelige gegevens en verstuurt dit commando draadloos naar de chip.
3. De paspoortchip geneert een 'challenge' (in feite een willekeurig getal) en verzendt dit draadloos naar het uitleesapparaat.
4. Het uitleesapparaat (c.q. een achterliggend systeem) genereert een 'response' door de challenge te 'ondertekenen' met de geheime digitale sleutel waarmee kan worden uitgelezen. De 'response' wordt verzonden naar de chip.[13]
5. De chip verifieert de 'response'. Als deze juist is, verstuurt het de gevraagde gegevens gecodeerd (middels het aangeboden digitale certificaat) naar het uitleesapparaat.

[13] In de praktijk is er niet één digitale sleutel, maar is er sprake van een hiërarchie van sleutels. Een hoofdsleutel wordt gebruikt om een groter aantal subsleutels te 'ondertekenen'. Een dergelijke 'subsleutel' kan een beperkte geldigheid hebben en bijvoorbeeld worden gedistribueerd aan geautoriseerde instanties. Mocht de sleutel toch in verkeerde handen vallen, dan is zo de impact beperkt. Om te kunnen verifiëren dat de gebruikte subsleutel geldig is, moet het uitleesapparaat een volledige 'certificatenhiërarchie' overleggen aan de paspoortchip. Dit is een serie van certificaten waarmee wordt aangetoond dat de gebruikte sleutel (uiteindelijk) is ondertekend door de hoofdsleutel. Het certificaat van de hoofdsleutel is ingeprogrammeerd in de paspoortchip.

6. Het uitleesapparaat (c.q. een achterliggend systeem) kan middels de geheime digitale sleutel de ontvangen gegevens decoderen.

In dit proces wordt verondersteld dat de communicatie tussen het uitleesapparaat en de chip kan worden afgeluisterd en eventueel zelfs verstoord. In de standaard is daarom geregeld dat bij authenticatie van de uitlezer er tevens een tijdelijke sleuteluitwisseling plaatsvindt, zodat gegevens die daarna worden overgebracht alleen door de geauthentiseerde uitlezer te decoderen zijn. [39, p. 17 'terminal authentication'] In principe is het zelfs niet vereist dat het uitleesapparaat wordt vertrouwd: alleen de chip en het systeem dat toegang heeft tot de digitale sleutel dienen volledig veilig te zijn. Vanwege deze eigenschappen is het denkbaar dat dit proces ook met grotere afstand tussen chip/uitleesapparaat enerzijds en een achterliggend systeem (met sleutel) anderzijds, bijvoorbeeld via internet, wordt uitgevoerd. Onderstaande afbeelding toont schematisch hoe dit zou kunnen werken.



Figuur 11 Schematisch overzicht van de manier waarop de vingerafdruk uit een paspoortchip mogelijk op afstand zou kunnen worden uitgelezen, op basis van de gebruikte technologie in recente paspoorten

Benodigde hard- en software

Om het hierboven geschetste proces te laten werken, dient de aanvrager de beschikking te hebben over een apparaat (smartphone, tablet) met een werkende internetverbinding en een NFC-lezer.

De NFC-lezer dient de gehanteerde protocollen (met name voor de onderliggende NFC-radiocommunicatie) te ondersteunen. Daarnaast dient op dit gebruikersapparaat een app (of wellicht website[14]) te worden geïnstalleerd en geopend. Vanuit de app dienen alle benodigde functies voor NFC-communicatie beschikbaar te zijn. De beschikbare softwarebibliotheken op iOS ondersteunen mogelijk niet alle vormen van NFC-toepassingen. [56]

[14] Er is een standaard in ontwikkeling (WebNFC) waarmee NFC-communicatie vanaf een website kan worden uitgevoerd. (W3C, 2022) Deze wordt echter nog niet door alle webbrowsers en -platforms ondersteund. (Can I Use, 2022) Daarnaast ondersteunt de standaard vooralsnog alleen het uitlezen en beschrijven van een specifiek type tag (NDEF).

Daarnaast moet het apparaat (als er ook een vergelijking dient te worden gemaakt tussen een actuele en de opgeslagen vingerafdruk) te beschikken over een vingerafdrukscanner. Zie hiervoor de bedenkingen in paragraaf 4.3.

Overwegingen

Centrale verwerking van vingerafdrukken ligt gevoelig – niet voor niets worden vingerafdrukken door Nederland niet centraal opgeslagen, maar uitsluitend in de chips in de identiteitsmiddelen.

Bij het uitlezen van de vingerafdruk van een identiteitsmiddel door een geautoriseerde uitlezer wordt de vingerafdruk overgedragen naar een ander systeem. Daarmee komt de vingerafdruk buiten de fysieke controle van de paspoorthouder. De aanvrager zal erop moeten vertrouwen dat de uitlezer (in principe onderdelen van Nederlandse overheid) de vingerafdruk goed behandelt en bijvoorbeeld niet langer opslaat dan nodig. Dit vertrouwen moet de houder van een identiteitsmiddel echter evengoed hebben wanneer de vingerafdruk wordt gecontroleerd via een uitleesapparaat op een stadskantoor (er zullen wellicht maatregelen zijn genomen zodat de authenticiteit en integriteit van het apparaat te controleren is, maar feit blijft dat de uitleescertificaten in handen zijn van de Nederlandse overheid; iedere uitleesactie berust fundamenteel op vertrouwen in de houder van deze digitale sleutels).

Een belangrijk ander probleem bij toepassing van deze methode is dat ook hier vrijwilligheid van de aanvrager niet kan worden gegarandeerd. De pincode bij modernere (op PACE-gebaseerde) chips biedt wel enige bescherming tegen uitlezen van het identiteitsmiddel tegen de wil van de houder in. Desondanks kan de houder uiteraard gedwongen worden de code af te geven.[15] Bij fysieke verschijning is dwang wellicht eenvoudiger te voorkomen.

4.2 Identificatie op afstand zonder 'oud' geldig identiteitsmiddel

Wanneer een aanvrager niet beschikt over een (geschikt en geldig) bestaand identiteitsmiddel dat kan worden gebruikt ter identificatie, of wanneer de hierboven beschreven methoden voor identificatie niet zouden kunnen worden toegepast, kan worden gewerkt met methoden die geen bestaand identiteitsmiddel vereisen.

Merk op dat deze methoden ook kunnen worden toegepast wanneer de aanvrager wél over een geldig identiteitsmiddel beschikt, en in dat kader relevant kunnen zijn bij het vergroten van de zekerheid van identificatie ('stapelen' van factoren).

Er zijn diverse manieren waarop een aanvrager zich online zou kunnen identificeren zonder (geldig) bestaand identiteitsmiddel. Online identificatie met een hoog niveau van betrouwbaarheid is immers voor veel diensten, zoals bijvoorbeeld online bankieren en toegang tot overheidsdiensten, al uitgewerkt en in gebruik. In deze paragraaf bespreken we enkele voor de hand liggende methoden.

---

[15] Een oplossing hiervoor zou *plausible deniability* kunnen zijn. Hierbij krijgt de houder de beschikking over twee pincodes, die allebei ogenschijnlijk (voor derden) op dezelfde manier werken. Een van beide codes is daarbij bedoeld voor een reguliere aanvraag, de andere voor een aanvraag die onder dwang plaatsvindt. Alleen aan de ontvangende kant is duidelijk welke code is gebruikt, en kan zo worden gesignaleerd dat een aanvraag onder dwang plaatsvond. De precieze implementatie hiervan komt echter erg nauw. Zo kan een persoon onder druk worden gezet om *beide* codes af te geven. Daarnaast is het onthouden van meerdere codes over de geldigheidstermijn van een paspoort (tien jaar) geen sinecure. Het effect zou uiteraard teniet worden gedaan als de codes worden opgeschreven.

4.2.1 Technische oplossingen voor online identificatie op afstand

Videobellen met aanvrager

Kan de aanvrager antwoord geven op vragen die ze zouden moeten kunnen beantwoorden? Zijn de kenmerken van de locatie waarin de aanvrager zich bevindt als verwacht? De innemer in kwestie zou op kenmerken kunnen letten zoals of de hoeveelheid daglicht klopt met het tijdstip op een bepaalde plek. Deze identificatiemethode zou het proces aan de balie tot op zekere hoogte kunnen spiegelen en wordt al toegepast bij het verstrekken van een DigiD op afstand.

Vooraf uitgewisselde sleutel

Een laatste mogelijkheid om op afstand de identiteit van een aanvrager vast te stellen, is het vooraf uitwisselen van een 'sleutel'. Een aanvrager zou, wanneer deze in Nederland is, zich kunnen identificeren bij een vertrouwde partij (denk bijvoorbeeld aan de gemeente, marechaussee of politie), en een wachtwoord kunnen achterlaten. Wanneer vervolgens dit wachtwoord wordt ingevoerd bij een aanvraag, bestaat er enige zekerheid over de identiteit van de aanvrager. In plaats van een wachtwoord zou kunnen worden gewerkt met digitale sleutels en/of 'ondertekende QR-codes' (zoals gebruikt op het Europese coronabewijs) – zodoende zou centraal zelfs niets hoeven te worden opgeslagen over de aanvrager.

Identiteitsmiddelen die kunnen worden 'gestapeld'

Er zijn diverse digitale identiteitsmiddelen die kunnen worden gebruikt om de betrouwbaarheid van identificatie te verhogen. Op zichzelf geven ze veelal geen volledige uitsluitsel over de identiteit van een persoon, maar de combinatie van verschillende middelen maakt de onderbouwing van een identiteitsverificatie wel sterker. Door meerdere middelen te combineren wordt het fraudeurs lastiger gemaakt: zij zullen immers controle moeten zien te krijgen over alle benodigde middelen.

Banken (iDIN)

iDIN is een voorbeeld van een verificatie-oplossing waarbij een aanvrager zich via de login methode van een bank kan identificeren. [57] Het idee achter deze verificatiemethode is dat banken bij het afsluiten van een rekening de identiteit van de aanvrager verifiëren via een bestaand identiteitsmiddel. Door vervolgens online in te loggen bij de bank kan de aanvrager aantonen in ieder geval toegang te hebben tot de bankrekening en waarschijnlijk de identiteit van de eigenaar te hebben (mensen geven over het algemeen niet snel hun inloggegevens af en de systemen van de Nederlandse banken kennen een hoge mate van beveiliging).

DigiD

Net als bankgegevens, geven mensen ook niet snel hun DigiD gegevens af. Ook dit zijn gegevens waar gebruik van gemaakt zouden kunnen worden. Als een aanvrager kan inloggen met zijn/haar DigiD, draagt dit bij aan de waarschijnlijkheid dat het daadwerkelijk om de persoon zelf gaat. Bovendien kan er bij DigiD gebruik worden gemaakt van two factor authentication (2FA). Via een app of sms krijgen mensen tijdens het inlogproces een code toegestuurd die ze moeten doorgeven. Dit zorgt voor een extra laag beveiliging; mensen moeten namelijk over hun eigen telefoon bezitten om dit te kunnen doen.

Overige digitale identiteiten

Naast digitale identiteiten waarvoor onderliggend een verificatie heeft plaatsgevonden kunnen ook andere, minder harde digitale identiteiten worden aangewend. Het feit dat een aanvrager zich kan authentiseren met één of meerdere sociale media-accounts zou een (extra) indicatie van identiteit kunnen zijn.

'Anekdotische' identificatie / overige factoren

In aanvulling op 'harde' identiteitsverificatie kan aanvullend worden gewerkt met meer anekdotisch bewijs en 'aanvullende factoren'. Hierbij bedoelen we dat een aanvrager demonstreert dat deze bepaalde handelingen kan uitvoeren die eenvoudig zouden moeten zijn als de identiteit van de persoon klopt, maar meer moeite kosten voor een fraudeur. Hoe meer van deze handelingen kunnen worden uitgevoerd, hoe zekerder de identiteit van de aanvrager is (vanwege het feit dat een fraudeur steeds meer moeite zou moeten doen om al deze handelingen te kunnen reproduceren). Denk bijvoorbeeld aan de volgende handelingen (Tabel 4). Hoewel de onderliggende verificatie hierbij in sommige gevallen overlapt met eerder genoemde bronnen, maakt het feit dat een handeling op een bepaald moment en met specifieke kenmerken wordt gevraagd het fraudeurs lastiger.

Tabel 4 Vormen van 'anekdotisch bewijs' en de asymmetrie tussen de gevraagde handeling en de handeling die een fraudeur zou moeten doen

Handeling	Handeling voor fraudeur
Het kunnen inloggen op een sociale media-account en het daar kunnen achterlaten van een willekeurige code.	Accountgegevens zien te bemachtigen voor het account. Dergelijke gegevens worden op het dark web verhandeld of zouden bijvoorbeeld kunnen worden bemachtigd via een phishingaanval.
Het kunnen doen van een bankoverschrijving met symbolisch bedrag vanaf een bankrekening met een bepaalde naam.	Het bemachtigen van de inloggegevens van de bank of (wellicht eenvoudiger) een vorm van phishing/social engineering toepassen.
Het kunnen overleggen van een willekeurige code die per SMS is verstuurd naar een telefoonnummer waarvan bekend is dat deze behoort/behoorde tot de aanvrager.	SIM-card swapping, spoofing, hacking, social engineering [58] en/of het stelen van de telefoon.
Het kunnen beantwoorden van specifieke vragen over de historie van een persoon (bijvoorbeeld gegevens over genoten opleiding, burgerlijke staat, et cetera, zoals beschikbaar op mijnoverheid.nl)	Accountgegevens voor mijnoverheid.nl (DigID) bemachtigen, sociale engineering, recherchewerk.

4.2.2 Conclusie

Onderstaande Tabel 5 toont de belangrijkste eigenschappen van de verschillende methoden voor betrouwbare identiteitsverificatie van een aanvrager op afstand, zonder gebruik te maken van een bestaand en geldig identiteitsmiddel.

Tabel 5 Methoden voor online identificatie zonder bestaand en geldig identiteitsmiddel

Methode	Identiteit gebaseerd op	Beschermd met
iDIN	Persoonlijke verificatie op basis van identiteitsmiddel door bank voor nieuwe klanten	Bankpas en pincode, fraudedetectie banken
DigiD	Eenmalige registratie, verificatie van woonadres	Inloggegevens en 2FA
Videobellen	Stellen van persoonlijke vragen waarop de persoon snel en accuraat antwoord zou moeten weten.	Deepfakedetectie, beoordelen snelheid antwoorden, combinatie met de andere identificatiefactoren.
Vooraf uitgewisselde sleutel	Identificatie met verschijning in Nederland bij vertrouwde instantie	Digitale sleutel (hebben) en/of wachtwoord (weten)
Anekdotische identificatie	Het demonstreren van een bepaalde specifieke handeling die voor de te identificeren persoon eenvoudig is, maar voor een fraudeur lastig.	De moeite die een fraudeur zou moeten doen om de handeling te voltooien, combinatie van handelingen.

Bij de selectie van een online identificatiemethode speelt primair de vraag of het gewenste niveau van betrouwbaarheid wordt gehaald. DigiD en iDIN zijn methoden die een hoge betrouwbaarheid kunnen bieden. Een aandachtspunt is dat aan deze identificatiemethoden (uiteindelijk) een identiteitsmiddel ten grondslag ligt. Daarnaast is het bij beide methoden mogelijk om (ondanks dat dat niet de bedoeling is) namens iemand anders in te loggen (bij iDIN kan dit wanneer iemand beschikt over de bankpas en pincode van iemand anders, bij DigiD zijn een gebruikersnaam, wachtwoord en voor de hogere niveaus de smartphone benodigd).

Om het fraudeurs moeilijker te maken zouden de identificatiemethoden (in gevallen waarin twijfel bestaat over de identiteit eventueel risicogestuurd) kunnen worden 'gestapeld'. Een fraudeur moet dan meerdere middelen verzamelen om namens iemand anders een aanvraag te kunnen doen. Een combinatie van 'sterke' identificatiemethoden zou kunnen worden gecombineerd met 'zwakkere'; in extremo zou zelfs het feit dat iemand kan inloggen op bijvoorbeeld een studentenaccount of sociale media aanvullend 'anekdotisch bewijs' geven ter ondersteuning en extra beveiliging van het inloggen. Deze accounts staan nergens officieel geregistreerd als horende bij een persoon en zijn ook overdraagbaar, maar maken wel dat een fraudeur nog meer stappen moet doorlopen om succesvol te zijn.

4.3 Afgifte van biometrie op afstand

Een belangrijke stap bij het aanvragen van een identiteitsmiddel is het afgeven van actuele biometrie. Bij een online aanvraag moet deze biometrie uiteraard ook worden afgenomen, en moet daarnaast zeker worden gesteld dat de biometrie ook *juist* is (dat wil zeggen: overeen komt met de feitelijke biologische eigenschappen van de aanvrager).

4.3.1 Biometrie afgeven via een smartphone

Handtekening

Voor het vergaren van een nieuwe handtekening ten behoeve van de aanvraag bestaan programma's. Bijvoorbeeld het in Apple's besturingssysteem ingebouwde Preview kan een

blanco papier waarop de aanvrager een handtekening heeft gezet en voor de camera heeft gehouden digitaliseren. [59]

Vingerafdruk afgeven via een smartphone

Veel smartphones beschikken tegenwoordig over een vingerafdrukscanner, maar deze is veelal niet vanuit een app of website uit te lezen. [35] Deze toegang wordt geblokkeerd, om te voorkomen dat malafide applicaties de vingerafdruk van de gebruiker kunnen stelen. In theorie zou de fabrikant toegang voor deze specifieke toepassing kunnen openen, maar gezien de beveiligingsimplicaties (en de vraag of dat dan ook voor oudere modellen en versies zal gebeuren) ligt dit niet voor de hand. De onlangs ingevoerde Europese *Digital Markets Act* zou er echter voor kunnen zorgen dat smartphonefabrikanten de toegang tot hardware, waaronder in ieder geval de NFC-lezer, maar wellicht ook de vingerafdrukscanner, moeten vergroten voor derde partijen. [60]

De vingerafdrukscanners op smartphones zijn daarnaast primair bedoeld om het apparaat te beveiligen. Het is goed mogelijk dat de vingerafdrukscanners op smartphones hiervoor niet alle kenmerken van een vingerafdruk controleren, maar slechts een deel daarvan, en/of dit met een lagere kwaliteit doen.

In algemene zin geldt dat bij het gebruik van niet-vertrouwde apparaten om vingerafdrukken af te nemen, het niet (goed) te garanderen is of de vingerafdruk zoals de sensor deze registreert, ook daadwerkelijk de vingerafdruk is die het aanvraagsysteem uiteindelijk ontvangt. Malafide software zou zich in theorie tussen de vingerafdrukscanner en de applicatie kunnen nestelen, en de vingerafdruk (die de applicatie via het besturingssysteem uit de sensor ontvangt) kunnen wijzigen. Het zou ook mogelijk zijn voor malafide software om al eerder in te haken en de gehele scanner na te bootsen, waardoor er ook een andere gedigitaliseerde vingerafdruk opgestuurd zou kunnen worden.

Daarnaast geldt dat er geen controle mogelijk is van wat er precies op de sensor wordt aangeboden. Bij het in persoon afgeven van biometrie kan een innemer controleren of de sensor niet is gemanipuleerd en of daadwerkelijk de vinger van de verschenen persoon op de sensor wordt aangeboden. Bij het afnemen van pasfoto's kan met diverse aanvullende controles (zie hieronder) grotere zekerheid worden verkregen dat er geen manipulatie plaatsvindt, maar bij vingerafdrukken is dit minder goed mogelijk (de vingerafdruksensor meet alleen wat er op de vingerafdruksensor wordt aangeboden, en daarbij is minder ruimte voor variatie dan bij een fotocamera).

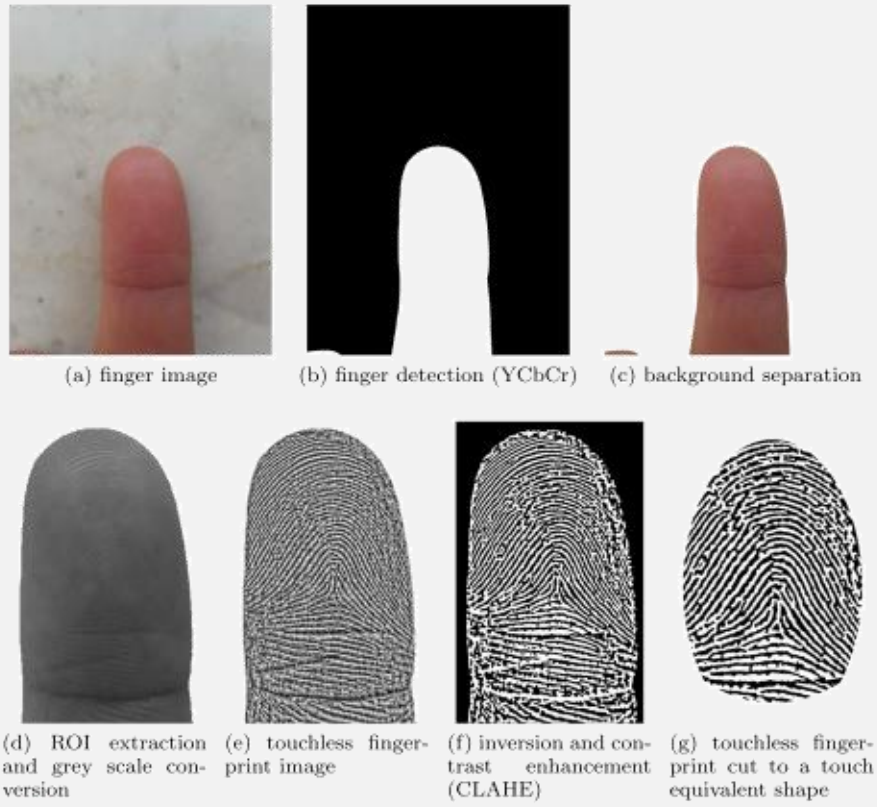
Touchless vingerafdruksensoren

Een ontwikkeling die in dit kader relevant is om te noemen, is die van zogeheten *touchless* vingerafdruksensoren. Bij traditionele (*touch*) vingerafdruksensoren is het nodig de vinger op een plaat te plaatsen. Bij *touchless* sensoren wordt gebruik gemaakt van een camera, waarbij de vinger 'in de vrije lucht' wordt gefotografeerd.

(a) touch-based fingerprint (b) touchless fingerprint image

Fig. 3 Two impressions of the same finger: **a** touch-based fingerprint acquired with a Crossmatch Guardian 200; **b** touchless fingerprint image captured with a Samsung Galaxy S8. Both images are manually cut to represent only the fingerprint area

Figuur 12 De ruwe opname van een vingerafdruk met (links) een touch-based sensor en (rechts) een touchless sensor (in dit geval een reguliere smartphonecamera). [61]



(a) finger image (b) finger detection (YCbCr) (c) background separation

(d) ROI extraction and grey scale conversion (e) touchless fingerprint image (f) inversion and contrast enhancement (CLAHE) (g) touchless fingerprint cut to a touch equivalent shape

Fig. 4 Touchless preprocessing workflow. Example of a touchless preprocessing workflow based on a finger image manually taken by a Samsung Galaxy S8

Figuur 13 Verwerking van een camera-opname van een vingerafdruk tot een bruikbare afbeelding van de vingerafdruk [61]

Figuur 12 toont het verschil in de ruwe afbeelding van de vingerafdruk die beide methoden opleveren (in dit voorbeeld is de 'touchless sensor' simpelweg de camera van een Samsung-smartphone). Het camerabeeld van een vingerafdruk kan met beeldverwerkingalgoritmen worden getransformeerd tot een afbeelding van de

vingerafdruk die voor vergelijking geschikt is (zie Figuur 13). Daarmee zou de vingerafdruk in theorie ook vergelijkbaar moeten zijn met opnames van een *touch*-sensor. . De variatie in de ruwe afbeeldingen is bij *touchless* sensoren een stuk groter dan bij touch-sensoren (zo varieert de afstand van de vinger tot de camera, zijn er vervormingen als gevolg van de gebruikte cameralenzen, is het contract van de 'groeven' laag, et cetera). De goede en betrouwbare werking van *touchless* sensoren staat of valt daarmee met de beeldverwerking. Daar staat tegenover dat *touchless* sensoren méér of andere informatie zouden kunnen verzamelen dan een *touch*-sensor (bijvoorbeeld door de vingerafdruk uit verschillende hoeken te fotograferen, en/of door te werken met geavanceerdere camera's). Een andere route is het toepassen van 'multi-biometrics' waarbij meerdere vingerafdrukken worden gecombineerd.

Bij toepassing van *touchless* vingerafdruksensoren worden tot slot ook algoritmes voor fraudepreventie belangrijker (zo moet, net als bij het afnemen van een gelaatsfoto, worden vastgesteld dat het gezicht c.q. de vingerafdruk op de foto daadwerkelijk van de aanvrager is - een scherpe foto van iemands duim is immers eenvoudiger te verkrijgen dan een *touch*-foto van de vingerafdruk op de duim, en het is niet de bedoeling dat met zo'n foto een paspoortaanvraag kan worden voltooid).

Foto van het gelaat

Vrijwel alle hedendaagse smartphones en laptops zijn voorzien van een camera. Hoewel de kwaliteit ervan sterk varieert zou het mogelijk moeten zijn om met deze middelen een foto te maken die voldoet aan de eisen (de fotomatrix: [8]). Met behulp van beeldherkenning kan de gebruiker worden geassisteerd bij het maken van de juiste foto.

Net als bij het afgeven van vingerafdrukken en het verifiëren van de foto (ten opzichte van een oud identiteitsmiddel) speelt dat de foto niet zonder meer kan worden vertrouwd. Het is triviaal om een foto te manipuleren. Allerlei filters die op foto's worden toegepast zijn hier een uitstekend voorbeeld van. Een smartphone-app zou tot op zekere hoogte kunnen controleren of de foto rechtstreeks met de smartphonecamera is gemaakt (zie eerdere toelichting bij vertrouwde eindgebruikersapparatuur).

Een tweede risico dat speelt is *morphing*. Bij het aanvragen van identiteitsmiddelen is in het verleden gebleken dat fraudeurs foto's van twee personen samenvoegen. De aanvraag wordt gedaan door de eerste persoon, maar de foto lijkt voldoende op de tweede persoon om deze met het identiteitsmiddel te kunnen laten reizen. Omdat bij het op afstand insturen van een foto geen vergelijking kan worden gemaakt met de fysieke verschijning van de aanvrager, is dit risico groter (bij een fysieke verschijning kunnen immers details worden 'gezien' die niet goed op de foto zichtbaar zijn als gevolg van morphing, maar dat wel zouden moeten zijn; dit is niet mogelijk wanneer de aanvrager volledige controle heeft gehad over het fotomateriaal dat bij de aanvraag en eerder is aangeleverd).

Morphing in het huidige proces

Het huidige proces is (ook) kwetsbaar voor morphing, omdat de foto vrijwel nooit op moment van verschijning, maar vooraf wordt gemaakt, en dus gemanipuleerd kan zijn. Door de foto's wel op moment van verschijning te maken (*live enrolment*) kan dit worden gemitigeerd. [62] Onderzoek van RvIG naar live enrolment geeft, naast mitigatie van *morphing*, een aantal andere redenen om *live enrolment* uit te rollen. Zo zou de kwaliteit van de opgenomen pasfoto beter zijn, tot tijdsbesparing leiden en eenvoudiger zijn voor de aanvrager. Bij live enrolment op afstand bestaat een risico op manipulatie van de beelden (zie elders de bespreking over deep faketechnologie). Tenzij er een hoge mate van authenticatie van de gebruikte camera, en/of betrouwbare detectie van manipulatie wordt toegepast (voor zover mogelijk) is de mitigatie door toepassing van live enrolment op afstand, vanuit perspectief van morphing, beperkt (het biedt niet dezelfde zekerheden, maar werpt wel een aanvullende drempel op voor manipulatie).

Mogelijkerwijs kunnen deze risico's worden gemitigeerd door méér foto's af te nemen en (net als bij de eerder besproken verificatiestap) te werken met opdrachten en lichtinval. Dit maakt het manipuleren van het fotomateriaal in ieder geval lastiger. Daarnaast zijn sommige smartphones voorzien van gezichtsscanners die ook de *vorm* van een gezicht (op basis van diepte) kunnen meten. In tegenstelling tot de vingerafdrukscanner is deze vanuit een applicatie op Apple-telefoons wél te benaderen. [63] Die data zou kunnen dienen als aanvullende biometrie, maar bijvoorbeeld ook om nadere controle uit te voeren op een ingestuurde pasfoto (een fraudeur zou dan zowel de dieptegegevens als de foto moeten manipuleren, wat uiteraard complexer is).

Lengte

Het meten van de lengte van een persoon is wellicht mogelijk op basis van camerabeelden, al dan niet in combinatie met andere sensoren in een smartphone. Bij volwassenen verandert de lengte in principe echter nauwelijks. Na een succesvolle identiteitsverificatie zou de lengte uit het oude identiteitsmiddel daarom kunnen worden overgenomen uit het bestaande identiteitsmiddel (zie 4.1.1).

De lengte zou uiteraard kunnen worden geverifieerd, maar de vraag is of dat veel toegevoegde zekerheid biedt: de 'juiste' lengte is immers leesbaar op het identiteitsmiddel (dit in tegenstelling tot bijvoorbeeld de vingerafdruk) en een fraudeur weet dan ook exact welke waarde de verificatie zou moeten opleveren.

4.3.2 Vingerafdruk afgeven bij een vertrouwde (derde) partij

Voor het aanvragen van een paspoort in het buitenland kunnen Nederlanders in sommige landen terecht bij derde partijen. [64] Dit zijn externe dienstverleners die voor meerdere landen paspoort- en visumaanvragen innemen. Deze dienstverleners voeren identiteitsverificatie uit, nemen de nodige biometrie in of af en sturen de aanvraag naar een Nederlandse backoffice voor verwerking.

4.3.3 Biometrie op afstand afgeven, en bij uitgifte controleren

Een variant is dat biometrie op afstand wordt afgenomen bij de aanvraag (op een van de manieren elders beschreven in dit rapport zonder verschijning), maar nog niet gecontroleerd wordt. De controle zou dan plaats kunnen vinden bij het uitgiftemoment, waarvoor dan een verschijning vereist is. Bij deze invulling wordt de verschijningsplicht dus in stand gehouden. Deze oplossing biedt dan ook niet direct voordelen ten opzichte van een proces met de

verschijning bij aanvraag (tenzij verschijnen op het aanvraagmoment een specifieke aanvrager om wat voor reden dan ook minder goed uitkomt dan het uitgiftemoment). Deze werkwijze verhoogt daarentegen mogelijk de kans dat er documenten in omloop raken met onjuiste biometrie, omdat deze immers wel al worden geproduceerd (naast diefstal kan de uitgever in dit scenario sterk onder druk worden gezet). Het zou daarom meer voor de hand liggen om dat verschijningsmoment bij de aanvraag plaats te laten vinden, zodat de biometrie direct gecontroleerd kan worden.

4.3.4 Afgeven van biometrie op een eerder moment

Als het afgeven van nieuwe biometrie (en dan met name de vingerafdruk) gedaan moet worden in een gecontroleerde omgeving met betrouwbare apparatuur, dan zou een mogelijkheid zijn om het voor de aanvrager mogelijk te maken om diens vingerafdrukken af te geven op locaties waar dit wel het geval is, maar op een moment dat zelf te kiezen is voor de aanvrager. Dit houdt in dat de aanvrager zijn vingerafdrukken in kan leveren als die 'toevallig' in de buurt is van een (grens)gemeente of een ambassade/consulaat. Wanneer het tijd is voor het vernieuwen van een paspoort kan de aanvrager dan een beroep doen op deze eerder afgegeven biometrie.

De oplossingsrichting waarin biometrie al in een eerder stadium wordt afgegeven, is reeds onderzocht en voorlopig als minder kansrijk bestempeld ten opzichte van andere mogelijke innovaties. [65] Uit onderzoek volgt dat, met de huidige technologie, de houdbaarheid van biometrie (en dan met name de vingerafdrukken) maximaal circa 11 jaar is. [13] Aangezien dit slechts één jaar meer is dan de houdbaarheid van het identiteitsmiddel zelf, zou dit leiden tot een dermate kleine meerwaarde dat besloten is voorlopig niet verder te gaan langs deze route. Technologische verbeteringen op het gebied van vingerafdrukscanners zouden deze optie in de toekomst wel aantrekkelijker kunnen maken - het patroon van de vingerafdruk zelf verandert nauwelijks over de jaren, het maken van een betrouwbare scan hiervan (die bruikbaar blijft terwijl de kenmerken van de vingerhuid veranderen met leeftijd) vormt de beperking. Daarnaast speelt dat gezichtskenmerken veranderen door de tijd heen. Er zal in de toekomst dan ook onderzocht moeten worden hoelang een ('oude') pasfoto nog gebruikt kan worden voor identiteitsverificatie om deze route zinvol te laten zijn. De Kamerbrief stelt in conclusie dat *"het nu realiseren van deze innovatie aanzienlijke technische en financiële consequenties heeft"* en dat om die reden op andere innovaties wordt ingezet.

4.4 Uitgifte van het identiteitsmiddel op afstand

Het uitgeven van identiteitsmiddelen vereist een verschijning, waarbij opnieuw de identiteit van de aanvrager (afhaler) wordt gecontroleerd.

Identiteitsmiddelen die in het buitenland zijn aangevraagd worden verstuurd naar de innemende ambassade, consulaat of externe dienstverlener. De aanvrager moet vervolgens daar het identiteitsmiddel persoonlijk ophalen, tenzij deze heeft aangegeven dat dit niet van hem of haar kan worden verwacht. Bij een grote reisafstand of beperkte mobiliteit kan het identiteitsmiddel in dat geval worden opgestuurd. Opsturen kan alleen indien dit veilig kan plaatsvinden, en is voor risico en rekening van de aanvrager. [64] Ook gemeenten in Nederland bezorgen onder bepaalde omstandigheden identiteitsmiddelen (bijvoorbeeld de gemeente Rotterdam [66]).

4.4.1 Alternatieven

Echte alternatieven voor het op afstand (zonder reisafstand voor de aanvrager) uitgeven van een identiteitsmiddel zijn er niet, althans zonder daarbij een derde partij te vertrouwen. Een

digitale versie van het identiteitsmiddel zou uiteraard eenvoudiger digitaal kunnen worden uitgegeven.

4.5 Intrekken van het oude identiteitsmiddel op afstand

Een belangrijke reden voor het vereisen van een fysieke verschijning bij het afhalen van een aangevraagd identiteitsmiddel is dat het oude identiteitsmiddel kan worden gecontroleerd en ingenomen of ongeldig kan worden gemaakt. Dit laatste gebeurt veelal door het identiteitsmiddel te perforeren.

Wanneer er geen sprake is van een fysieke verschijning zal het identiteitsmiddel op een andere manier moeten worden ingenomen. Denkbare routes zijn:

1. Het door de koerier laten innemen (of onklaar maken) van het oude identiteitsmiddel. Hierbij zou de koerier moeten verifiëren dat het identiteitsmiddel het juiste identiteitsmiddel is (en daarnaast ook juist moeten handelen indien het oude identiteitsmiddel bijvoorbeeld niet kan worden overhandigd).
2. De aanvrager verstuurt het oude identiteitsmiddel op naar de uitgifte-instantie. Na ontvangst van het oude identiteitsmiddel wordt het nieuwe identiteitsmiddel opgestuurd. Dit zou dan uiteraard veilig moeten plaatsvinden. Dit betekent wel dat de aanvrager tijdelijk geen identiteitsmiddel heeft. Deze methode wordt in het buitenland al succesvol toegepast.
3. Het bij de aanvraag inleveren van het oude identiteitsmiddel. Dit heeft als nadeel dat de aanvrager tijdelijk zonder identiteitsmiddel kan komen te zitten. Een verklaring dat een aanvraag in behandeling is kan hierbij enigszins uitkomst bieden, maar brengt ook weer nieuwe vragen en risico's met zich mee.

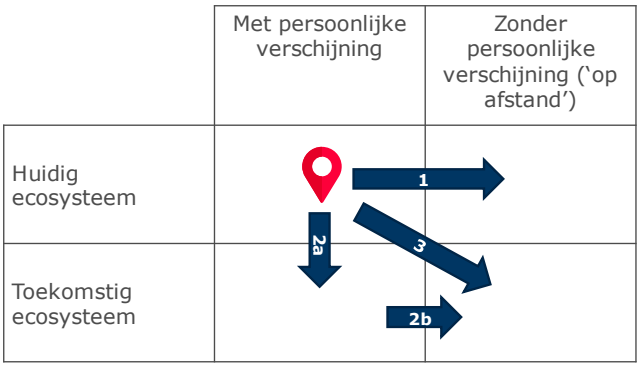
4.6 Aansluiting bij het ecosysteem

Relevant voor de analyse is, naast de kenmerken van de technische (deel)oplossing(en), de positionering van een mogelijk nieuw te ontwikkelen proces ten opzichte van enerzijds het bestaande ecosysteem (geheel van regelgeving, technische standaarden en afspraken), en anderzijds het 'toekomstige ecosysteem'. Op verschillende vlakken vinden ontwikkelingen plaats aangaande identiteitsmiddelen, met name op gebied van digitalisering. In de Verenigde Staten wordt bijvoorbeeld in een aantal staten een digitaal paspoort en/of rijbewijs op smartphones uitgerold. [67] In onder andere Estland gaan stemmen op om werk te maken van digitale identiteiten. [68] Op Europees niveau wordt de eIDAS-verordening geïmplementeerd, die er (uiteindelijk) toe moet leiden dat Europees erkende inlogmiddelen van Europese burgers en organisaties door lidstaten wederzijds worden herkend en geaccepteerd. [69] Daarnaast wordt voortbouwend op de eerdere eIDAS-verordening (in de herziening) nagedacht over een "Digital Identity Wallet" waarmee digitale identiteiten kunnen worden bewaard en gebruikt. [70] De vraag kan worden gesteld of een toekomstig aanvraagproces dat grotendeels online verloopt, niet direct zou moeten worden ingericht op deze toekomstige digitale identiteiten en bijbehorende digitale identiteitsmiddelen.

Het lijkt daarom voor de hand te liggen om een nieuw proces voor het op afstand aanvragen van identiteitsmiddelen te ontwikkelen als 'digitale versie' van het huidige proces. Voor ieder van de stappen in het huidige proces zouden (op basis van de vertrouwensketen) digitale alternatieven kunnen worden gezocht.

Onderstaande Figuur 14 toont schematisch de hierboven besproken noties. De rode markering duidt de huidige situatie aan: het huidige ecosysteem met daarbinnen een aanvraagproces waarin een persoonlijke verschijning noodzakelijk is. De blauwe pijlen stellen mogelijke ontwikkelroutes voor:

1. Het ontwikkelen van een variant ‘op afstand’ van het huidige proces op basis van het huidige ecosysteem;
2. Het afwachten van ontwikkelingen in het huidige ecosysteem tot een toekomstig ecosysteem, en vervolgens (2b) het ontwikkelen van een aanvraagproces op afstand in het toekomstige ecosysteem;
3. Het ontwikkelen van een systeem voor aanvragen op afstand in een toekomstig ecosysteem.



Figuur 14 Positionering en beoordeling van een toekomstig proces voor het aanvragen van reis- en identiteitsdocumenten 'op afstand'

De eerste route ligt hierbij op het eerste gezicht het meest voor de hand. De ontwikkelingen in het ecosysteem staan nog in de kinderschoenen en zijn nog onzeker. Daar staat tegenover dat de nieuwe digitale technologieën mogelijk beter aansluiten bij een aanvraagproces ‘op afstand’, en dat zo alvast wordt voorbereid op de toekomstige situatie.

5 Beantwoording onderzoeksvragen

In dit hoofdstuk beschrijven we onze bevindingen en geven we antwoord op de onderzoeksvragen.

5.1 Onderzoeksvraag I en II

> ***I. Wat zijn de technische en procesmatige mogelijkheden voor overheidsorganisaties, zoals de gemeenten, om digitaal (zonder fysieke verschijning) de identiteit van persoon vast te stellen, dan wel verifiëren?***
>
> ***II. Welke risico's bestaan er bij online/ digitale identiteitsvaststelling en verificatie?***

Met het *vaststellen* van de identiteit van een persoon bedoelen we het koppelen van een identiteit aan een natuurlijk persoon, zonder dat daarbij een identiteitsmiddel beschikbaar is. Is er een identiteitsmiddel beschikbaar, dan kan de identiteit op basis daarvan worden geverifieerd en spreken we van *identiteitsverificatie*. In het aanvraagproces voor een identiteitsmiddel is ofwel identiteitsvaststelling, ofwel identiteitsverificatie nodig.

Hieronder gaan we allereerst in op identiteitsvaststelling, en vervolgens op identiteitsverificatie op afstand. Daarna bespreken we de mogelijkheden voor het op afstand afnemen van biometrie. We bespreken daarbij de beide onderzoeksvragen gezamenlijk, omdat de antwoorden op onderzoeksvraag II (risico's) sterk samenhangen met de specifieke mogelijkheid (onderzoeksvraag I).

5.1.1 Identiteitsvaststelling op afstand

Een fysieke verschijning biedt fundamenteel gezien meer mogelijkheden dan een proces dat op afstand wordt uitgevoerd. Alle digitale middelen zijn bij een fysieke verschijning immers nog steeds in te zetten, maar bij een fysieke verschijning is aanvullend een hoge mate van controle van apparatuur en omgeving mogelijk. Daarnaast kan fysieke verificatie plaatsvinden van digitaal verzamelde gegevens, waarmee scenario's van manipulatie (waaronder 'deep fakes', 'morphing', et cetera) in geheel kunnen worden uitgesloten.

Uit gesprekken met (voormalige) baliemedewerkers valt daarnaast op dat, naast de formele procedures, ook de intuïtie van baliemedewerkers en het 'menselijk beoordelen van het gehele plaatje' een belangrijk onderdeel van het aanvraagproces van identiteitsmiddelen vormt. Het is denkbaar (maar in dit onderzoek nadrukkelijk niet geverifieerd) dat baliemedewerkers op basis van de extra informatie die een fysieke verschijning oplevert beter in staat zouden kunnen zijn pogingen tot fraude en bijvoorbeeld onvrijwilligheid van de aanvrager op te merken. Daar staat tegenover dat dit sterk afhankelijk is van de betreffende ambtenaren, en er waarschijnlijk variatie zal zijn in de kwaliteit. Hoe dan ook zal de mensenkennis van ambtenaren 'aan de balie' zeer beperkt kunnen worden vertaald naar een digitaal proces. Daar staat wellicht tegenover dat gewerkt kan worden met algoritmes en fraudevoorspellende modellen, waarin andere omgevingsfactoren kunnen worden meegenomen.

We concluderen dat het vaststellen van de identiteit van een individu fundamenteel gezien zeer lastig op afstand is uit te voeren, omdat er geen biometrische gegevens beschikbaar zijn. Zonder biometrische gegevens kunnen methoden voor identiteitsverificatie op afstand niet worden toegepast. In deze gevallen is in het huidige proces 'aan de balie' overigens ook

al sprake van een hoge mate van complexiteit en maatwerk. Zo wordt, afhankelijk van de situatie, mogelijk gebruik gemaakt van een verscheidenheid aan bewijsstukken en andere identiteitsaanwijzingen. Denk hierbij bijvoorbeeld aan geboorteaktes uit andere landen. Vanwege de verscheidenheid van deze bewijsstukken, en de menselijke beoordeling van het geheel aan bewijsstukken die nodig is om tot identiteitsvaststelling te komen, zijn deze gevallen niet (goed) op afstand te verwerken.

5.1.2 Identiteitsverificatie op afstand

In algemene zin zien we dat er voor identiteitsverificatie op internet legio betrouwbare technieken bestaan. Dit is in hoge mate te danken aan de ontwikkeling van e-commerce, online bankieren en online overheidsdienstverlening in de afgelopen decennia. Op basis van goede cryptografische principes kan met hoge mate van zekerheid worden vastgesteld dat een aanvrager in bezit is van een bepaalde 'geheime sleutel' (zoals een pincode, wachtwoord of digitale sleutel ingebed in een chip). Aanvullend kunnen diverse controles worden uitgevoerd die het met name fraudeurs moeilijker zouden maken (denk aan het nabellen van een aanvrager op een bij de overheid bekend telefoonnummer, SMS-verificatie, verificatie per brief op bekend huisadres, et cetera).

Het Nederlandse DigiD biedt een sterk online identiteitsmiddel. De Europese eIDAS-verordening maakt dat dergelijke middelen binnen Europa uitwisselbaar worden en zal de verdere adoptie ervan mogelijk verder vergroten. De vraag of en welk niveau eIDAS-middelen volstaat voor het aanvragen van een identiteitsmiddel, is in het onderzoek onbeantwoord gebleven.

Een principe dat bij online identiteitsverificatie veelal wordt toegepast is 'stapelen', waarbij verschillende 'factoren' tezamen leiden tot een drempelwaarde voor betrouwbare identiteitsverificatie. Naast bestaande, hoogwaardige identiteitsmiddelen kan daarbij worden gedacht aan het aanvullend verifiëren van de identiteit door middel van identificatie via banken (iDIN of bijvoorbeeld het overmaken van een symbolisch bedrag) of door het inloggen op sociale media-accounts. Deze middelen geven vrijwel geen aanvullende gegevens over de identiteit van de aanvrager, maar maken het een fraudeur vele malen lastiger: deze moet dan immers controle zien te krijgen over alle factoren.

Naast het 'stapelen' van factoren kan in online context sterk risico-gestuurd worden gewerkt. Waar bij een fysieke verschijning omgevingsfactoren beschikbaar zijn en worden meegenomen, zoals hierboven toegelicht, zijn er in de 'digitale omgeving' evengoed diverse factoren beschikbaar. Denk bijvoorbeeld aan informatie over het IP-adres vanaf waar een aanvraag wordt gedaan en het tijdstip.

De complexiteit bij online identiteitsverificatie zit niet zozeer in deze stap in de vertrouwensketen, maar in het verifiëren dat het middel waarmee wordt geïdentificeerd (in feite de drager van de 'geheime sleutel') in handen is van de juiste persoon. In een proces met fysieke verschijning kan hiervoor gebruik worden gemaakt van de koppeling tussen de (centraal of in een identiteitsmiddel opgeslagen) biometrie en de feitelijke biometrie. Bij biometrie kan gedacht worden aan de vingerafdruk, het gezicht (pasfoto), maar ook 'eenvoudigere' kenmerken zoals lengte, leeftijd en de mate waarin iemand de Nederlandse taal machtig is. Daarnaast zien we in de praktijk ook minder 'harde' methoden toegepast worden: denk bijvoorbeeld aan het stellen van vragen als "welke rivier stroomt er door Maastricht?" als de persoon volgens de bekende gegevens tien jaar lang in Maastricht heeft gewoond.

Het op afstand verifiëren van het feit dat een aanvrager beschikt over een specifiek identiteitsmiddel, zoals een Nederlands paspoort, Europese identiteitskaart of een rijbewijs, is technisch gezien betrouwbaar mogelijk wanneer het een recent uitgegeven identiteitsmiddel

betreft. Hiervoor heeft de eindgebruiker in principe genoeg aan een (mobiel) apparaat met NFC-lezer. Het feit dat modernere documenten daarbij een pincode vereisen maakt dat er grotere zekerheid is dat het de houder van het document is die zich identificeert.

Identiteitsverificatie op afstand middels opgeslagen biometrie

Op basis van biometrische kenmerken die ofwel zijn opgeslagen in het bestaande identiteitsmiddel, ofwel centraal zijn geregistreerd, kan aanvullende verificatie plaatsvinden van biometrische eigenschappen van de aanvrager. Het eenvoudigst is dit op basis van pasfoto's, omdat deze in principe centraal beschikbaar zijn, en het 'afgeven' van een actuele pasfoto middels bijvoorbeeld een selfiecamera (zie echter verderop de kanttekeningen onder 'biometrie op afstand afnemen').

Voor vingerafdrukken ligt de situatie anders. Allereerst is het afnemen van een actuele vingerafdruk niet altijd goed mogelijk (zie eveneens verderop). Aanvullend speelt dat vingerafdrukken niet centraal worden opgeslagen. De vingerafdruk wordt, nadat deze is afgegeven bij de aanvraag, opgeslagen op de chip in een Nederlands paspoort of identiteitskaart. De vingerafdruk kan draadloos worden uitgelezen via NFC door eenieder die beschikt over het daarvoor nodige digitale certificaat (en, afhankelijk van het model identiteitsmiddel, een pincode die in principe alleen bij de houder van het identiteitsmiddel bekend is). Het is tot slot niet zeker of de kwaliteit van de vingerafdrukken die op de chip zijn opgeslagen, voldoende is voor betrouwbare verificatie.

Doordat de afname van de 'actuele' biometrie 'op afstand' niet in een gecontroleerde omgeving plaatsvindt, blijft er fundamenteel meer ruimte voor manipulatie dan bij een fysieke verschijning (wederom kunnen alle methoden die bij een fysieke verschijning worden toegepast ook digitaal worden ingezet, en zijn er aanvullend methoden voor digitale manipulatie).

5.1.3 Biometrie op afstand afnemen

Voor het uitgeven van Nederlandse reisdocumenten is het opnemen van persoonsgegevens als leeftijd, geslacht en lengte en afnemen van biometrie vereist. Op hoofdlijnen gaat het om biometrische gegevens als gelaat (pasfoto) en vingerafdrukken. Bij een herhaalaanvraag of andere aanvraag waarbij er een ander (geldig) identiteitsmiddel beschikbaar is gaan we ervan uit dat de persoonsgegevens en de pasfoto aan overheidszijde beschikbaar zijn. De persoonsgegevens hoeven in dat geval niet te worden afgenomen (de geboortedatum wijzigt immers in principe niet), of er kan worden volstaan met informatie die de aanvrager zelf opgeeft (lengte en geslacht). De pasfoto en vingerafdruk zijn de twee biometrische kenmerken die bij iedere aanvraag moeten worden 'bijgewerkt' en uiteraard op dat moment overeen moeten komen met de feitelijke eigenschappen van de aanvrager.

Pasfoto's

Voor wat betreft het afnemen van pasfoto's zien we technisch diverse mogelijkheden. Anno 2022 beschikken de meeste Nederlanders over een smartphone met een selfiecamera. Met deze camera's kunnen relatief hoogwaardige foto's worden gemaakt. Middels beeldherkenningsalgoritmes kan vervolgens gedurende het proces al automatisch worden vastgesteld of een gemaakte foto voldoet aan de kwaliteitseisen en de Fotomatrix.

Zoals eerder opgemerkt speelt ook hier de vraag of de foto die het systeem uiteindelijk ontvangt, daadwerkelijk hoort bij de aanvrager. In het geval van foto's kan daarbij gebruik worden gemaakt van diverse methoden om de betrouwbaarheid van de foto te verhogen. Zo kan de aanvrager worden gevraagd meerdere foto's in te sturen, al dan niet op basis van een 'challenge response'-methodiek waarbij bepaalde poses moeten worden aangenomen. Dit maakt het voor een fraudeur lastiger om het benodigde fotomateriaal te verzamelen en

daarnaast is het (op korte termijn) 'faken' van dergelijke foto's lastiger (maar niet onmogelijk).

Een ander veel toegepast principe is dat de aanvrager wordt gevraagd om, naast zijn gezicht, ook het huidige identiteitsmiddel of een specifieke code zichtbaar in beeld te houden. Uiteraard kunnen ook deze foto's door een fraudeur middels manipulatie worden gemaakt (er zijn bijvoorbeeld beeldalgoritmes die een foto van een paspoort zouden kunnen 'overlayen' op de plaats van een blanco boekje dat door de persoon op de foto wordt vastgehouden en bewogen). Door hierbij eisen te stellen aan de resolutie, of bijvoorbeeld het aantal foto's (of zelfs te vragen een video-opname te maken) kan meer informatie worden verkregen en kan eerder worden vastgesteld of een beeldopname gemanipuleerd is of niet. In aanvulling op pasfoto's kan tot slot gebruik worden gemaakt van dieptecamera's op recentere telefoons.

Vingerafdrukken

In principe is een opname van een vingerafdruk niet meer dan een foto van een vinger – zij het gemaakt op een glasplaat, zodat het profiel op de vinger goed zichtbaar is (nieuwere vingerafdrukscanners werken op basis van geavanceerdere methoden waarbij de diepte nauwkeuriger wordt gemeten). Ten opzichte van het afnemen van een pasfoto zien we hierbij echter twee complicaties.

Allereerst is de kans dat een aanvrager de beschikking heeft over een *bruikbare* vingerafdrukscanner veel kleiner dan dat deze over een selfiecamera beschikt. Hoewel veel smartphones tegenwoordig met een vingerafdrukscanner zijn uitgerust, zijn deze in de meeste gevallen (in ieder geval bij Apple-telefoons, goed voor ongeveer de helft van het marktaandeel) niet uit te lezen is door applicaties. De reden hiervoor is om te voorkomen dat malafide applicaties die zich op de smartphone van de gebruiker weten te nestelen, niet zomaar de vingerafdruk kunnen 'stelen'. Vingerafdrukscanners op smartphones zijn daarnaast ontworpen voor verificatie ten opzichte van één bekende vingerafdruk (al dan niet op basis van een subset van de kenmerken daarvan), en niet voor het vastleggen van een zo gedetailleerd mogelijke afbeelding van een gehele vingerafdruk. Voor de Apple-telefoons geldt overigens ook nog dat bij de nieuwere modellen de vingerafdrukscanner is ingeruild voor gezichtsherkenning op basis van een dieptecamera.

Een tweede complicatie is dat de hierboven genoemde aanvullende verificatiemethoden, zoals het naast het gezicht tonen van een code of identiteitsmiddel op camera, bij vingerafdrukken niet toepasbaar zijn. Dit maakt het lastiger om vast te stellen of de vingerafdruk die wordt aangeboden daadwerkelijk bij de aanvrager hoort.

Doordat afname van biometrie 'op afstand' niet in een gecontroleerde omgeving plaatsvindt, blijft er fundamenteel meer ruimte voor manipulatie dan bij een fysieke verschijning (wederom kunnen alle methoden die bij een fysieke verschijning worden toegepast ook digitaal worden ingezet, en zijn er aanvullend methoden voor digitale manipulatie). Ontwikkelingen op het vlak van vertrouwde eindgebruikersapparatuur maken dat er steeds meer technische garanties mogelijk zijn ten aanzien van de authenticiteit van verzamelde biometrie.

Hergebruik van eerder afgenomen biometrie

Uit bovenstaande volgt dat het op afstand afnemen van biometrie met de benodigde betrouwbaarheid en kwaliteit technisch gezien lastig is. Een alternatief voor het opnieuw (op afstand) afnemen van biometrie zou het hergebruiken van bestaande biometrische gegevens kunnen zijn.

Hergebruik van biometrische gegevens is alleen mogelijk als de biometrie nog actueel is – biometrische kenmerken veranderen immers door de jaren heen (hierover verderop meer).

Wanneer er nog bruikbare biometrische gegevens centraal zijn opgeslagen, zou het voldoende kunnen zijn om de aanvrager te identificeren. De eerder afgenomen biometrie zou daarbij mogelijk zelfs betrouwbaarder kunnen zijn dan eventueel nieuw afgenomen biometrie. Voor vingerafdrukken speelt dat deze niet centraal zijn opgeslagen. Desondanks kunnen deze in theorie veilig en versleuteld uit een modern paspoort gelezen worden.

5.2 Onderzoeksvraag III

III. Wat betekent de (risico-)analyse voor het aanvraag- en uitgifteproces van paspoorten door Buitenlandse zaken en door gemeenten in Nederland?

De casus die aanleiding vormt voor dit onderzoek is de Nederlander in het buitenland die voor het aanvragen van een identiteitsmiddel moet reizen naar een ambassade, consulaat of externe dienstverlener, die zich mogelijk op grote reisafstand bevindt. Voor Nederlandse gemeenten speelt deze reisafstand (absoluut gezien) in mindere mate, al zal ook een aanvrager in Nederland eveneens meestal liever *niet* dan *wel* afreizen naar een gemeentekantoor. Het vervangen van de fysieke verschijning door een 'online verschijning' of andere digitale variant van de daarbij uitgevoerde stappen, zou de reis overbodig kunnen maken.

Allereerst gaan we in op de mogelijkheden om de resterende stappen die in het huidige proces bij de fysieke verschijning plaatsvinden 'op afstand' uit te voeren. Verderop beschouwen we mogelijkheden om dit proces anders in te richten.

Het huidige proces 'op afstand' uitvoeren'

Hoe zouden de stappen in het huidige aanvraagproces die op dit moment een fysieke verschijning vereisen, op afstand (online) kunnen worden uitgevoerd?

Zoals al eerder opgemerkt stellen we vast dat voor aanvragen waarbij de aanvrager geen geldig bestaand identiteitsmiddel kan overleggen (en dus een vorm van identiteitsvaststelling moet plaatsvinden), een fysieke verschijning onmisbaar is. Dit betekent dat voor eerste aanvragen (bijvoorbeeld voor kinderen van Nederlanders in het buitenland) de reis nodig blijft. Uiteraard neemt dit niet weg dat grote delen van het proces digitaal zouden kunnen worden voorbereid, door bijvoorbeeld alvast de nodige informatie aan te leveren, documenten te scannen, et cetera.

Kijken we naar de subset van aanvragen waarbij een bestaand geldig identiteitsmiddel beschikbaar is, dan is onze conclusie dat een substantieel deel daarvan op afstand zou moeten kunnen plaatsvinden. De belangrijkste beperkende factor lijkt daarbij te zijn dat biometrie op afstand afnemen (bij de benodigde kwaliteit en betrouwbaarheid technisch gezien, op dit moment) niet mogelijk is, en eerder afgegeven en opgeslagen biometrie een beperkte 'houdbaarheidstermijn' heeft (zodanig dat de biometrie nauwelijks langer kan worden bewaard dan de maximale geldigheidstermijn van een identiteitsdocument, waarmee de toegevoegde waarde van een vooraanvraag zeer beperkt is). Met name bij minderjarigen en bij ouderen veranderen de kenmerken zodanig dat afname van biometrie met hoge kwaliteit eens in de tien jaar noodzakelijk zal zijn.

Aanvullend spelen beperkingen vanuit de regelgeving, die één c.q. twee fysieke verschijningen vereisen bij aanvraag- en uitgifte van bepaalde identiteitsmiddelen. De regelgeving biedt hiervoor (in verschillende mate voor paspoorten versus Europese identiteitskaarten) wel

enige ruimte. Het uitgeven van het identiteitsmiddel gebeurt op dit moment al 'op afstand' via speciaal daarvoor gecontracteerde koeriers (op risico en kosten van de aanvrager).[16]

De vraag is in hoeverre de casus van de Nederlander in het buitenland wordt verbeterd, als een fysieke verschijning voor een aanvraag bij een ambassade, consulaat, externe dienstverlener of overheidsinstantie in Nederland noodzakelijk blijft, en dit daarnaast nog altijd het geval zal blijven voor eerste aanvragen (en andere situaties waarbij geen bestaand identiteitsmiddel voorhanden is, zoals verlies of diefstal). Op deze vraag geeft dit onderzoek geen antwoord. Wel is onderzocht in hoeverre een andere invulling van het proces mogelijk zou kunnen zijn.

Een nieuw proces 'op afstand'

Uit bovenstaande wordt duidelijk dat, zolang er bij de Nederlandse overheid actuele en bruikbare biometrische gegevens beschikbaar zijn van een aanvrager, en de identiteit van de aanvrager met hoge mate van betrouwbaarheid kan worden geverifieerd, een aanvraag in principe volledig 'op afstand' zou kunnen worden uitgevoerd. We stellen echter ook vast dat het op afstand afnemen van biometrie met de benodigde kwaliteit en betrouwbaarheid technisch gezien niet mogelijk is. Ontwikkelingen op het vlak van vertrouwde eindgebruikersapparatuur maken wel dat er steeds meer technische garanties mogelijk zijn ten aanzien van de authenticiteit van verzamelde biometrie, maar deze technologieën zijn nog niet wijdverspreid. Desondanks zien we mogelijkheden om het aanvraagproces zo in te richten dat het aantal keer dat een fysieke verschijning nodig is, te minimaliseren, en/of het moment hiervoor flexibeler te maken.

Er zou een proces kunnen worden ingericht waarbij Nederlanders die dat willen, eens in de vijf tot tien jaar, op een moment dat hen uitkomt, biometrische gegevens afgeven bij een Nederlandse overheidsinstantie (gemeente, ambassade, consulaat, of bijvoorbeeld een balie op Schiphol) of een externe dienstverlener. De oplossingsrichting waarin biometrie al in een eerder stadium wordt afgegeven, is echter reeds onderzocht en voorlopig als minder kansrijk bestempeld ten opzichte van andere mogelijke innovaties. [65] Uit onderzoek volgt dat, met de huidige technologie, de houdbaarheid van biometrie (en dan met name de vingerafdrukken) maximaal circa 11 jaar is. [13] Aangezien dit slechts één jaar meer is dan de houdbaarheid van het identiteitsmiddel zelf, zou dit leiden tot een dermate kleine meerwaarde dat besloten is voorlopig niet verder te gaan langs deze route. In een recente Kamerbrief stelt de staatssecretaris van Binnenlandse Zaken hierover in conclusie dat *"het nu realiseren van deze innovatie aanzienlijke technische en financiële consequenties heeft"* en dat om die reden op andere innovaties wordt ingezet.

De bevindingen van dit onderzoek zien niet op de doelmatigheid, maar ondersteunen wel de conclusie dat beter nog even gewacht kan worden met het inslaan van deze richting tot de technologie volwassener is geworden. Technologische verbeteringen op het gebied van vingerafdrukscanners zouden deze optie in de toekomst aantrekkelijker kunnen maken. Het patroon van de vingerafdruk zelf verandert namelijk nauwelijks over de jaren, maar juist het maken van een betrouwbare scan hiervan (die bruikbaar blijft terwijl de kenmerken van de vingerhuid veranderen met leeftijd) vormt de beperking. Met *touchless* sensoren en bijbehorende algoritmen zou een hogere kwaliteit en daarmee langere houdbaarheid mogelijk kunnen zijn. Wel dient men dan bij zowel bij de afname van de biometrie als bij controle beschikking te hebben over een dergelijke *touchless* sensor, hetgeen nu nog niet aan de

[16] Het is overigens niet altijd zo dat het vereiste tweede verschijningsmoment voor Europese identiteitskaarten in de praktijk altijd plaatsvindt. In het buitenland worden, uitsluitend in schrijnende gevallen, identiteitskaarten uitgereikt per aangetekende post.

orde is. Daarnaast speelt dat gezichtskenmerken veranderen door de tijd heen. Er zal in de toekomst dan ook onderzocht moeten worden hoelang een ('oude') pasfoto nog gebruikt kan worden voor identiteitsverificatie om deze route zinvol te laten zijn.

Tot slot

Bij het digitaliseren van processen voor en rondom het aanvragen van identiteitsmiddelen (en wellicht overheidsprocessen in het algemeen) speelt dat de hoogste doeltreffendheid en doelmatigheid hoogstwaarschijnlijk kan worden behaald door (alleen) de meest voorkomende situaties digitaal te faciliteren. Bij digitalisering geldt in het algemeen dat er hoge initiële kosten zijn en (daarna) lage variabele kosten, terwijl in niet-digitale processen de vaste kosten lager zijn en de variabele hoger. Het digitaliseren van de 'long tail' van uitzonderingsgevallen leidt tot een hoge mate van complexiteit in de digitale processen (en dus hogere initiële kosten voor ontwikkeling). De totale kosten kunnen ondanks hoge variabele kosten in een niet-digitaal proces uiteindelijk lager uitvallen, vanwege het kleine aantal.

In de context van het aanvragen van identiteitsmiddelen is de meest voorkomende aanvraagvariant, en daarmee de voor de hand liggende variant om te digitaliseren, de herhaalaanvraag ('verlenging' van een bijna verlopen identiteitsdocument) waarbij de aanvrager beschikt over een geldig en betrouwbaar geacht identiteitsmiddel.

Voor alle andere soorten aanvragen, alsook de herhaalaanvragen waarbinnen een uitzondering optreedt (bijvoorbeeld onvoldoende zekerheid bij identiteitsverificatie) zal een niet-digitale route moeten (blijven) bestaan. Een andere reden om het huidige aanvraagproces te laten voortbestaan is ten behoeve van de Nederlanders die geen gebruik kunnen of willen maken van het digitale aanvraagproces.

Vanuit het perspectief van fraude is de verwachting dat fraudeurs met name gebruik zullen maken van uitzonderingssituaties, en relatief minder van zwakheden in de vertrouwensketen van de 'meest voorkomende' variant van het aanvraagproces. Een fraudeur zal, kort gezegd, eerder aangeven dat zijn paspoort kwijt is, dan dat deze een paspoort zal namaken en overhandigen bij een aanvraag.

Als de digitale route voor een groot deel van de aanvragen van Nederlanders in het buitenland goed werkt, dan kan dit betekenen dat ambassades en consulaten de schaal van hun werkzaamheden op het gebied van aanvragen verkleinen ('minder balies openhouden'). Daarnaast kan het betekenen dat de oplossingen die nu buiten de ambassades zijn gerealiseerd (de externe dienstverleners waar een aanvraag kan worden gestart) niet meer kosteneffectief blijken. Het invoeren van een digitaal proces is kortom additioneel, maar kan voor de minder digitaal vaardige aanvrager daardoor toch leiden tot verslechtering van de dienstverlening.

Aanbevelingen

We bevelen aan nader onderzoek uit te voeren naar de inzetbaarheid van technische innovaties op het gebied van biometrie-afname, waaronder met name de *touchless* sensoren. Daarnaast is nader inzicht wenselijk in de herbruikbaarheid/houdbaarheid van 'oude' pasfoto's. Tot slot achten we het zinvol de doelmatigheid van digitalisering van het aanvraagproces (al dan niet voor een deel van de aanvragen) en het effect op de niet-digitale dienstverlening (in het buitenland) te verkennen.

Verwijzingen

[1] Europese Parlement en de Raad (2019). *Verordening (EU) 2019/1157 betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten afgegeven aan burgers van de Unie en hun familieleden die hun recht van vrij verkeer uitoefenen* [eur-lex.europa.eu] vol. 62,

[2] (2021). *Paspoortwet* [wetten.overheid.nl]

[3] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2020). *Wat is de Basisregistratie Personen* [www.rijksoverheid.nl]

[4] Gemeente Den Haag. *1e inschrijving BRP voor Nederlanders uit het buitenland (u heeft nog geen BSN)* [www.denhaag.nl]

[5] identiteitsmiddelen, W.n. N. (2021). *Normenkader Nederlandse wettelijke identiteitsmiddelen*

[6] Rijksoverheid (2022). *Met welke identiteitsbewijzen kan ik mij identificeren?* [www.rijksoverheid.nl]

[7] PBLQ (2019). *Internationaal onderzoek naar innovaties in het aanvraag- en uitgifteproces voor paspoorten* [zoek.officielebekendmakingen.nl]

[8] Rijksdienst voor Identiteitsgegevens (2020). *Fotomatrix model 2020* [www.rijksoverheid.nl] Den Haag,

[9] Autoriteit Persoonsgegevens. *Biometrie* [autoriteitpersoonsgegevens.nl]

[10] Rijksoverheid. *Wat is een elektronisch reisdocument en welke gegevens staan op de chip hierin?* [www.rijksoverheid.nl]

[11] (2021). *Paspoortbesluit* [wetten.overheid.nl]

[12] (2022). *Paspoortuitvoeringsregeling Nederland 2001* [wetten.overheid.nl]

[13] de Wit, F., and Spreeuwers, L. (2020). *Houdbaarheid en hergebruik biometrie* [kennisopenbaarbestuur.nl] Enschede: Universiteit Twente.

[14] Raad voor Identiteitsgegevens (2020). *Photomorphing: een nieuw fenomeen* [magazines.rvig.nl]

[15] Interpol. *Identity and travel document fraud. The different types of document fraud* [www.interpol.int]

[16] Secure Identity Alliance (2021). *Passport Fraud Trends and Ways to Combat Them. Public version* [secureidentityalliance.org]

[17] Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (2022). *Brief regering. Aankondiging van maatregelen ter voorkoming van identiteitsfraude* [www.tweedekamer.nl]

[18] Raad voor Identiteitsgegevens (2021). *Kenmerken Nederlandse paspoorten* [www.rvig.nl] Den Haag,

[19] Rijksoverheid (2022). *Nederlandse nationaliteit verliezen* [www.rijksoverheid.nl]

[20] (2022). *Rijkswet op het Nederlanderschap* [wetten.overheid.nl]

[21] Rijksdienst voor Identiteitsgegevens. *Register paspoortsignaleringen* [www.rvig.nl]

[22] Identiteitsgegevens, R.v. (2022). *Belangrijkste wijzigingen reisdocumentenstelsel* [www.rvig.nl]

[23] ICAO (2021). *Doc 9303. Machine Readable Travel Documents. Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)* [www.icao.int] Quebec, Canada,

[24] De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, D.e. K. (2022). *Aankondiging van maatregelen ter voorkoming van identiteitsfraude* [www.rijksoverheid.nl] Den Haag,

[25] ScanID (2015). *Het uitlezen van de MRZ op identiteitsdocumenten* [www.scanid.nl]

[26] ICAO (2021). *Machine Readable Travel Documents, eight edition. Part 3: Specifications common to all MRTDs* [www.icao.int]

[27] PlanetCalc. *ICAO MRZ Check Digit* [planetcalc.com]

[28]IBM (2021). *Remote attestation of system software* [www.ibm.com]

[29]Signal.org (2017). *Technology preview: Private contact discovery for Signal* [signal.org]

[30]Murdock, K., Oswald, D., Garcia, F.D., Bulck, J.v., Gruss, D., and Piessens, F. (2020). *Plundervolt: Software-based Fault Injection Attacks against Intel SGX* [www.computer.org]

[31]Microsoft (2021). *Windows 11 and Secure Boot* [support.microsoft.com]

[32]Apple (2022). *Apple Platform Security* [help.apple.com]

[33]Apple (2021). *Secure Enclave* [support.apple.com]

[34]Yubico. *Authentication standards* [www.yubico.com]

[35]Apple (2022). *About Touch ID advanced security technology* [support.apple.com]

[36]DigiD. *Inlogmethodes - identiteitskaart* [www.digid.nl]

[37]Rijksdienst voor Identiteitsgegevens (2022). *Uitlezen chip op het paspoort en de Nederlandse identiteitskaart binnenkort uitsluitend via PACE-protocol* [www.rvig.nl]

[38]Bundesamt für Sicherheit in der Informationstechnik (2021). *BSI TR-03135 Machine Authentication of MRTDs for Public Sector Applications, version 2.4* [www.bsi.bund.de]

[39]Bundesamt für Sicherheit in der Informationstechnik (2015). *TR-03110-1. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 1. eMRTDs with BAC/PACEv2 AND EACv1. Version 2.20* [www.bsi.bund.de]

[40]SSLCertificaten.nl. *Certificate Revocation List (CRL)* [www.sslcertificaten.nl]

[41]ICAO (2021). *Machine Readable Travel Documents, eigth edition. Part 9: Deployment of biometric identification and electronic storage of data in MRTDs* [www.icao.int] ICAO.

[42]Statista (2018). *Number of NFC-enabled mobile devices worldwide from 2012 to 2018* [www.statista.com]

[43]Statista (2022). *Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)** [www.statista.com]

[44]Betaalvereniging Nederland, De Nederlandsche Bank (2022). *Voorkeur voor contactloos betalen neemt toe* [www.betaalvereniging.nl]

[45]OBS (2022). *Open Broadcaster Software. OBS Studio* []

[46]Grother, P., Ngan, M., and Hanaoka, K. (2018). *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* [docs.house.gov] NIST.

[47]Reddit (2016). *Rule Reminder: The Verification Sign* [www.reddit.com]

[48]AVROTROS (2019). *Wat is deepfake en hoe herken je het?* [opgelicht.avrotros.nl]

[49]GitHub (2022). *iperov/DeepFaceLive* [github.com]

[50]Thales (2020). *Liveness in biometrics: spoofing attacks and detection* [www.thalesgroup.com]

[51]Tinder (2022). *Photo Verification FAQs* [www.help.tinder.com]

[52]Browniee, J. (2019). *A Gentle Introduction to Generative Adversarial Networks (GANs* [machinelearningmastery.com]

[53]Instituut, R., Munnichs, G., Kouw, M., Kool, L., van der Vorst, T., Veldman, J., Hermanussen, L., Brennenraedts, R., Wein, B., and Willems, R. (2017). *Een nooit gelopen race: Over cyberdreiging en versterking van weerbaarheid* [www.rathenau.nl]

[54]Wikipedia (2022). *Nederlands biometrisch paspoort* [nl.wikipedia.org]

[55]Federal Bureau of Investigation (2010). *WSQ Gray-scale fingerprint image compression specification, version 3.1* [fbibiospecs.fbi.gov] Clarksburg, WV,

[56]Apple (2022). *Core NFC Framework* [developer.apple.com]

[57]iDIN (2022). *Hoe werkt het?* [www.idin.nl]

[58]Bunn, C. (2021). *Why Using SMS Authentication for 2FA Is Not Secure* [securityboulevard.com]

[59]Apple. *Een pdf-formulier invullen en ondertekenen in Voorvertoning op de Mac* [support.apple.com]

[60]Phillips, T. (2022). *European Parliament passes law that requires Apple to open up its NFC chip* [www.nfcw.com]

[61]Priesnitz, J., Rathgeb, C., Buchmann, N., Busch, C., and Margraf, M. (2021). *An overview of touchless 2D fingerprint recognition* [jivp-eurasipjournals.springeropen.com]

[62]Raad voor Identiteitsgegevens (2020). *Onderzoek Live Enrolment* [www.rvig.nl]

[63]Apple (2022). *Capturing Photos with Depth* [developer.apple.com]

[64]Rijksoverheid (2022). *Waar kan ik een paspoort of ID-kaart aanvragen als ik in het buitenland woon?* [www.rijksoverheid.nl]

[65]Koninkrijksrelaties, S.v. B. Z. e. (2020). *Brief regering. Onderzoeken innovaties dienstverlening paspoorten.* [www.rijksoverheid.nl]

[66]Gemeente Rotterdam. *Bezorgen documenten* [www.rotterdam.nl]

[67]Apple (2021). *Apple announces first states signed up to adopt driver's licenses and state IDs in Apple Wallet* [www.apple.com]

[68]Trommel, S. (2021). *Regeringsadviseur Estland: 'Begin met een digitale identiteit'* [ibestuur.nl]

[69]Europese Parlement en de Raad (2014). *Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG* [eur-lex.europa.eu] Brussel, pp. 73-114.

[70]Europese Commissie (2021). *Commission Recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework* [digital-strategy.ec.europa.eu] Brussel,

[71]ReadID (2020). *Overview security mechanisms in ePassports* [www.readid.com]

[72]Tweede Kamer der Staten-Generaal (2019). *Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden* [zoek.officielebekendmakingen.nl] Vols. Vergaderjaar 2019-2020, Den Haag,

[73]Rijksoverheid. *Hoe maak ik met de KopieID-app een veilige kopie van mijn identiteitsbewijs?* [www.rijksoverheid.nl]

[74]Department of Foreign Affairs Ireland. *Applicant Photo Guidelines* [www.dfa.ie]

[75]NOS. *Vingerafdruk in paspoort wordt nooit gecontroleerd* [nos.nl]

[76]Publicatieblad van de Europese Unie (13 december 2004). *VERORDENING (EG) Nr. 2252/2004 VAN DE RAAD*

[77]W3C (2022). *Draft Community Group Report 18 July 2022* [w3c.github.io] W3C.

[78]Can I Use (2022). *Can I Use WebNFC* [caniuse.com]

[79]Chang, R. (2022). *Americans Will Soon Be Able to Renew Passports Online* [www.cntraveler.com] Condé Nast.

[80]Minister van Justitie (2010). *Besluit van de Minister van Justitie van 17 maart 2010, nummer WBN 2010/1, houdende wijziging van de Handleiding voor de toepassing van de Rijkswet op het Nederlanderschap 2003* [zoek.officielebekendmakingen.nl]

[81]Intel. *Intel Software Guard Extensions (SGX)* [www.intel.com]

[82]Raad voor Identiteitsgegevens (2021). *Kenmerken Nederlandse identiteitskaart* [www.rvig.nl]

Bijlage 1. Overzicht interviewrespondenten

Tabel 6. Overzicht interviewrespondenten

Organisatie	Functie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Beleidsmedewerker
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Beleidsmedewerker
Ministerie van Buitenlandse Zaken	Beleidsmedewerker
Rijksdienst voor Identiteitsgegevens	Implementatiemanager
Rijksdienst voor Identiteitsgegevens	Adviseur
Dienst Wegverkeer	Adviseur Expertisecentrum
iDIN	Product Consultant
Evidos	Product Consultant
SK ID	Compliance and Security

Bijlage 2. Overzicht deelnemers groepssessies

Tijdens het onderzoek zijn groepssessies georganiseerd. Doel van de sessies was het verzamelen van inzichten en het valideren en aanscherpen van bevindingen ten aanzien van de onderzoeksvragen. De conclusies in dit rapport zijn gebaseerd op, maar komen niet noodzakelijkerwijs volledig overeen met de standpunten van de individuele betrokken personen en organisaties. Wij danken alle deelnemers voor hun waardevolle bijdragen.

Tabel 7: Overzicht deelnemers groepssessies

Organisatie	Functie
Sessie fraude-experts	
Politie - Afdeling Vreemdelingen Identificatie en Mensenhandel	Operationeel Specialist
Expertisecentrum Identiteitsfraude en Documenten	Beleidsmedewerker
Expertisecentrum Identiteitsfraude en Documenten	Beleidsmedewerker
Ministerie van Buitenlandse Zaken	Beleidsmedewerker
Gemeente Amsterdam	Medewerker Team Identiteitsfraude
Sessie met stakeholders	
Nederlandse Vereniging voor Burgerzaken	Directielid
Ministerie van Infrastructuur en Waterstaat	Beleidsmedewerker
Nederlandse Vereniging voor Burgerzaken	Strategisch adviseur
Ministerie van Buitenlandse Zaken	Beleidsmedewerker
Rijksdienst voor Identiteitsgegevens (RvIG)	Adviseur
Rijksdienst voor Identiteitsgegevens (RvIG)	Teamcoördinator
Rijksdienst voor Identiteitsgegevens (RvIG)	Adviseur
Ministerie van Buitenlandse Zaken	Beleidsmedewerker

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl