Inventarisatie van leeftijdsverificatiesystemen

Voor het aankopen van alcohol

Colofon

DATUM	20-07-2021
VERSIE	1.1
PROJECT REFERENTIE	P0327
VERTROUWELIJKHEID	Publiek
STATUS	Definitief
BEDRIJF	InnoValor Advies
AUTEUR(S)	Koen de Jong, Ines Duits, Marlies Rikken, Bob Hulsebosch

Inhoudsopgave

Managementsamenvatting

De verkoop via onlinekanalen neemt al jaren toe en is dankzij de coronacrisis nog verder versneld. Uit recent onderzoek blijkt echter dat de leeftijdsverificatie bij de aankoop van alcoholhoudende dranken op afstand te wensen overlaat. November 2020 is een wetswijziging van de Drank- en Horecawet in de Tweede Kamer behandeld. Deze is per 1 juli 2021 in werking getreden. Sinds die datum heeft de Drank- en Horecawet een nieuwe naam: Alcoholwet. Relevante wijzigingen zijn regels voor de verkoop op afstand (online of telefonisch) van alcoholhoudende dranken en de bijbehorende leeftijdsverificatie. Bij de bestelling van alcoholhoudende drank op afstand wordt vastgelegd hoe verkopers en aanbieders van alcohol op afstand (ofwel: de webwinkels) de leeftijdsgrens moet controleren. Hiervoor zal gebruik gemaakt worden van een leeftijdsverificatiesysteem.

Het doel van dit onderzoek is: ‘’*het in kaart brengen van digitale identificatiesystemen als onderdeel van het leeftijdsverificatiesysteem voor de verkoop van alcohol op afstand en het in algemene zin beschrijven van de effectiviteit, doelmatigheid en andere criteria, waaraan dergelijke systemen zouden moeten voldoen in het geval van verplichtstelling ervan.*”

Aanvullend is gevraagd om te onderzoeken in hoeverre deze systemen ook effectief zijn voor fysieke leeftijdsverificatie. In onderstaande paragrafen worden kort de belangrijkste bevindingen uit het rapport toegelicht aan de hand van de onderzoeksvragen.

Welke leeftijdsverificatiesystemen worden toegepast in Nederland?

Momenteel beperkt dit zich tot systemen waarbij de klant zelf moet aangeven 18 jaar of ouder te zijn. Een enkele partij doet daarnaast een pilot met iDIN. iDIN wordt ook voor andere leeftijdsgebonden diensten gebruikt. Het wordt bijvoorbeeld gebruikt bij online kansspelen, zoals de Nederlandse Loterij en Runnerz (paardenraces). Het aanbod van leeftijdsverificatiesystemen dat in de praktijk toegepast wordt is beperkt. Er zijn een aantal verschillende categorieën van systemen te onderscheiden die hier (in potentie) voor ingezet (kunnen) worden:

Categorie	Omschrijving
Zelf toegezegd	Eigen verklaring van de persoon zonder enige vorm van controle. Bijvoorbeeld: aanvinken ‘ik ben 18 jaar of ouder’.
Overheidsauthenticatie-oplossingen	Digitale oplossing uitgegeven door de overheid en gericht op het identificeren van consumenten bij overheidsinstanties of dienstverleners met een publieke taak.
Consumentenauthenticatie-oplossingen	Digitale oplossingen uitgegeven door een private partij en gericht op het identificeren van consumenten bij andere partijen, gebruikelijk een dienstverlener.
Betaaloplossingen	Oplossingen gericht op het doen van een (online) betaling.
Personal data wallets	Digitale oplossing die het mogelijk maakt voor het individu om veilig en onder eigen regie zijn of haar eigen persoonlijke data in te zien, op te halen en te delen. Ook Self-Sovereign Identity (SSI) oplossingen vallen hieronder.
Identificatie op afstand (IoA)	Oplossing gericht op het op afstand identificeren van een consument. De consument kan dit vanuit huis (of andere locatie naar voorkeur) doen en hoeft hiervoor niet naar een servicebalie te komen.

Deze categorieën van systemen zijn beoordeeld op de onderstaande criteria om de effectiviteit te bepalen. Voor detail toelichting per criteria zie ook Hoofdstuk 2: Succesfactoren.

- fraudebestendigheid en betrouwbaarheid
- beschikbaarheid en dekkingsgraad (gebruik onder Nederlanders)
- gebruiksgemak en begrijpbaarheid
- schaalbaarheid en flexibiliteit (toepasbaarheid in andere sectoren)

- kosten
- realisatietermijn
- toekomstbestendigheid
- vertrouwen en privacy
- draagvlak (onder verkopers en aanbieders van alcohol)

Wat is er bekend over de effectiviteit van de oplossingen?

De effectiviteit van de oplossingen waarbij de persoon **zelf toezegging** doet van de leeftijd is slecht, ze zijn namelijk onbetrouwbaar en daarmee niet toekomstbestendig. Wel scoren ze op alle andere criteria goed, ze zijn goedkoop, simpel en makkelijk. Dit is op het moment de huidige minimale oplossing die bij verkoop op afstand van alcohol ge-eist wordt. De lage effectiviteit is mede reden voor het aanpassen van de eisen.

De **betaaloplossingen** komen het best uit de bus op het gebied van gebruikersvriendelijkheid. Echter zijn niet alle middelen in deze categorie in de huidige vorm voldoende betrouwbaar voor leeftijdsverificatie. Dit geldt in het bijzonder voor PayPal, gezien er met een willekeurig email adres een PayPal account aangemaakt kan worden, zonder verdere identificatie. Het gebruik van een creditcard in combinatie met 3D Secure[1] is betrouwbaarder, naast bij de uitgifte van de creditcard een identificatieproces wordt doorlopen biedt dit een extra zekerheid. Het is echter nog steeds alleen een indirecte leeftijdsverificatie. Wanneer iDEAL een leeftijdsattribuut kan aanleveren of een leeftijdsverificatie kan uitvoeren zou dit een ideale combinatie zijn. Het duurt echter nog zeker tot na eind 2022 voordat iDEAL 2.0 geïmplementeerd wordt en er een mogelijke basis is om in leeftijdsverificatie te voorzien. Concreet heeft iDEAL leeftijdsverificatie nog niet op de roadmap.

Diverse webwinkels gaven aan dat hun voorkeur uitgaat naar een leeftijdsverificatiesysteem uitgegeven door de **overheid**. Deze verwachtingen vloeien voort uit het feit dat de overheid in fysieke context ook de middelen biedt voor leeftijdsverificatie door het uitgeven van identiteitsbewijzen. Het gebruik van DigiD levert echter ook het BSN op en is daarmee alleen inzetbaar voor overheidspartijen en partijen met een publieke taak. Technisch en juridisch is het niet realistisch dat het gebruik van DigiD als leeftijdsverificatiesysteem door private partijen in de komende paar jaar mogelijk wordt. Tevens kent DigiD een strikt audit regiem: aangesloten partijen dienen jaarlijks een beveiligingsaudit uit te laten voeren door een externe auditor en deze te delen met Logius. Veel kleine webwinkeliers zullen hier waarschijnlijk niet aan kunnen voldoen.

Het inzetten van **consumentenoplossingen** voor authenticatie (iDIN, itsme) lijkt op dit moment het meest realistisch. Consumentenoplossingen scoren gemiddeld positief op de verschillende eisen en randvoorwaarden en gaan ook nergens op onderuit. iDIN heeft een hoge dekkingsgraad en betrouwbaarheid. itsme biedt ook de mogelijkheid tot leeftijdsverificatie. Echter is de beschikbaarheid en dekkingsgraad momenteel een stuk lager, omdat itsme nog maar enkele maanden actief is op de Nederlandse markt.

Personal data wallets[2] zijn met name interessant wanneer we naar de toekomst kijken. Deze oplossingen bieden de belofte dat de gebruiker meer centraal gesteld wordt en zijn privacy beter geborgd wordt. De recente aankondiging van de Europese Commissie (EC) om lidstaten digital identity wallets uit te laten geven[3], geven deze oplossingen een extra zetje in de rug[4]. Op dit moment is deze categorie nog niet voldoende volwassen en is de dekkingsgraad van de verschillende oplossingen nog een probleem. Het tijdspad dat de EC voor ogen heeft en de snelheid van ontwikkelingen de afgelopen jaren, toont aan dat dit nog tenminste 3 jaar duurt.

Identificatie op afstand oplossingen zijn met name waardevol in processen waar een persoon voor de eerste keer geïdentificeerd moet worden. De identificatie kan met hoge zekerheid worden volbracht wanneer bijvoorbeeld een document wordt uitgelezen, in combinatie met biometrie. Echter moet de persoon veel

[1] 3D Secure is een extra authenticatiefactor voor creditcards. Naast de gegevens op de creditcard moet de gebruiker nog een extra goedkeuring geven, bijvoorbeeld door een wachtwoord en sms-code in te vullen of goedkeuring te geven in een bankieren-app.
[2] Dienst die het mogelijk maakt voor het individu om veilig zijn of haar eigen persoonlijke data in te zien, op te halen en te delen. Daarnaast maakt de operator het mogelijk om de uitwisseling van persoonlijke data met en tussen data aanbieders en afnemers te controleren.
[3] Zie ook: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663
[4] Zie ook: https://ibestuur.nl/podium/digitale-identiteit-als-nederlandse-troefkaart-in-europa

stappen doen om die identificatie uit te voeren. Daarnaast worden er vaak attributen opgehaald, die niet noodzakelijk zijn voor leeftijdsverificatie. In het geval van de leeftijdsverificatie voor aankoop van alcohol zijn deze middelen veelal te zwaar en onderbreken het aankoop proces te sterk.

In de **fraudetoets** zijn verschillende fraude scenario's geanalyseerd. Het risico op fraude is hoog als een volwassene een minderjarige vrijwillig helpt om alcohol te verkrijgen. Deze fraude is helaas lastig te voorkomen en is het handhaven lastig. Zwaardere vormen van fraude (als phishing) zijn onwaarschijnlijk in het geval van alcoholverkoop omdat de kosten niet opwegen tegen de baten. Andere fraude scenario's met een hoge waarschijnlijkheid in het geval van online leeftijdsverificatie, zoals het gebruik van een nep ID-document of het onvrijwillig gebruik van een identiteitsdocument van een ouder, zijn te mitigeren door bijvoorbeeld betere ID-verificatie software te gebruiken, bijvoorbeeld NFC, of een tweede factor voor authenticatie te gebruiken. Daarbij moet de afweging gemaakt worden of deze maatregelen opwegen tegen de andere succesfactoren, zoals privacy, dataminimalisatie, implementatie en gebruiksvriendelijkheid.

Een **alternatieve oplossingsrichting** is het inrichten van een 18+ account bij de webwinkel. Mits deze oplossing voldoet aan de eisen die het ministerie van Volksgezondheid, Welzijn en Sport (VWS) aan het leeftijdsverificatiesysteem stelt.

Dit zou er als volgt uit kunnen zien: bij het aanmaken van een account bij de webwinkel doorloopt de klant een verificatieproces (qua betrouwbaarheidsniveau vergelijkbaar aan eIDAS substantieel) waarbij wordt vastgesteld dat de persoon 18+ is. Bij elke online aankoop dient de klant in te loggen, met een authenticatie die typisch tweefactor is, op diens account waardoor de webwinkel weet hoe oud de klant is.

Het uitlenen van accounts is een voordehand liggende manier van fraude. Om deze tegen te gaan, is het nodig om aangemaakte accounts periodiek opnieuw te verifiëren. Bijvoorbeeld elke 30 à 90 dagen.

Deze oplossing zou kunnen voldoen aan artikel 20a van de Alcoholwet: *'het hanteren van een leeftijdsverificatiesysteem op het moment van aankoop'* en artikel 5.1 van de onderliggende AMVB dat stelt dat bij iedere aankoop en voor het sluiten van de verkoopovereenkomst de leeftijd wordt vastgesteld en dat hiervoor een actieve handeling van de klant is vereist. Mits het past binnen de additionele eisen. De klant moet immers voorafgaand aan de koop inloggen op diens 18+ account bij de webwinkel. Lagere kosten en gebruikersvriendelijkheid zijn de sterke punten van deze oplossing. Een dergelijke oplossing is door webwinkel Drankdozijn.nl geïmplementeerd (zie Bijlage E: Voorbeeld Drankdozijn).

Of dit voldoende is voor de leeftijdsverificatie volgens het Alcoholbesluit[5], zal mede afhankelijk zijn van de eisen die VWS aan het leeftijdsverificatiesysteem stelt. Daarnaast is bestellen als 'gast' in deze oplossing niet mogelijk, tenzij de webwinkel daarvoor een apart verificatieproces inricht.

Er zijn diverse oplossingen effectief genoeg om een leeftijdsverificatie uit te voeren, daarnaast zijn er diversen in ontwikkeling. Echter is de vraag naar deze oplossingen op dit moment laag, waardoor de dekkingsgraden over het algemeen ook nog laag zijn.

Hoe effectief zijn deze oplossingen voor fysieke leeftijdsverificatie?

Het gebruik van digitale middelen voor fysieke verificatie kan van toegevoegde waarde zijn wanneer de winkel of bezorgdienst de kwaliteit op basis van een wettelijk identificatiedocument (WID) in het kader van de wet op de identificatieplicht niet kan waarborgen. Bijvoorbeeld door de ruimte voor interpretatie in het huidige proces. Digitale middelen brengen één groot voordeel met zich mee: de mogelijkheid tot dataminimalisatie waardoor de privacy beter geborgd kan worden: digitale middelen kunnen ingericht worden om alleen een 18+-attribuut te ontsluiten, eventueel gecombineerd met een pasfoto. Door ook de pasfoto te tonen kan de persoon aantonen dat zij het middel ook daadwerkelijk bezit, wat de zekerheid vergroot en de kans op fraude verlaagd (holder verification[6]).

[5] https://www.rijksoverheid.nl/documenten/besluiten/2021/01/29/concept-ontwerpbesluit-houdende-regels-ter-uitvoering-van-de-alcoholwet-alcoholbesluit

[6] Zie Bijlage A: Begrippenlijst

Het WID blijft een legaal alternatief voor leeftijdsverificatie, naast de inzet van digitale systemen. Bezorgers en winkeliers mogen het WID niet weigeren. Dit betekent dat het wegnemen van die menselijke maat, niet volledig mogelijk is. Tenzij iedereen verplicht wordt een WID te tonen bij iedere aankoop of aanname van alcoholische drank. Iets wat op dit moment niet hoeft als iemand onmiskenbaar meerderjarig is. Om de verdere meerwaarde van digitale middelen voor fysieke leeftijdsverificatie te onderzoeken zijn additionele gebruikersonderzoeken en pilots nodig.

Welke eisen moeten we stellen aan oplossingen voor leeftijdsverificatie?

Er zijn verschillende criteria in kaart gebracht waaraan een systeem moet voldoen in het kader van leeftijdsverificatie, enkele welke als eisen kunnen worden gehanteerd door het ministerie van VWS en enkele welke als randvoorwaarde gelden voor succes.

Vanuit perspectief van **betrouwbaarheid** en fraudegevoeligheid kunnen er door VWS eisen gesteld worden aan een toekomstig leeftijdsverificatiesysteem. Een betrouwbaarheidsniveau dat overeenkomt met de eisen die de Europese eIDAS verordening voor niveau substantieel stelt is nodig voor leeftijdsverificatie bij de online verkoop van alcoholhoudende dranken. Dit laatste betekent dat er een substantiële mate van vertrouwen in iemands beweerde leeftijd is en wordt toegekend onder verwijzing naar technische controles, normen en procedures die tot doel hebben het risico op fraude of wijziging ervan te verkleinen. Een oplossing op niveau substantieel moet onder andere gebruik maken van tweefactor authenticatie. Daarnaast moet de oplossing zo ontworpen zijn dat verondersteld kan worden dat het identificatiemiddel slechts kan worden gebruikt door of onder controle van de persoon aan wie het toebehoort.

Daarnaast dienen er strenge eisen gesteld te worden op het gebied van **privacy, waaronder dataminimalisatie**. Uiteraard dienen oplossingen minimaal te voldoen aan de eisen die door de Algemene Verordening Gegevensbescherming (AVG) worden gesteld. Daarnaast, gezien de leeftijd bij iedere aankoop vastgesteld wordt, is het voldoende om alleen een 18+-attribuut uit te wisselen tussen het leeftijdsverificatiesysteem en de webwinkel. Een 18+-attribuut is een verklaring of iemand 18 jaar of ouder is, dat simpelweg met ja of nee beantwoord kan worden. In tegenstelling tot het delen van informatie over de exacte leeftijd of geboortedatum. Dit kan bijvoorbeeld worden omschreven als ‘bij vaststelling van de leeftijd worden niet meer gegevens gedeeld dan noodzakelijk om vast te stellen dat de koper meerderjarig is. Een 18+ verklaring volstaat.’

Een ander aspect van privacy is dat door één systeem te gebruiken, er al snel het risico ontstaat dat de uitgever van het systeem een ‘big-brother’ wordt die weet wie, waar en wanneer alcohol aanschaft. Dit risico kan worden verminderd door te eisen dat het systeem niet mag vastleggen met welke partij het attribuut gedeeld is. Dit kan gerealiseerd worden middels technische inrichting (privacy-by-design) of afspraken (de partij weet dit in principe wel, maar er wordt afgesproken dat er niet wordt opgeslagen dat er een verificatie heeft plaatsgevonden).

De criteria gebruiksgemak, schaalbaarheid, dekkingsgraad en toekomstbestendigheid zijn belangrijk voor webwinkels en slijters bij het beslissen om een systeem aan te schaffen, maar niet noodzakelijk om als specifieke eisen vast te leggen door VWS. Qua kosten zullen de webwinkels per leeftijdsverificatie transactiekosten moeten betalen, naar de kosten voor implementatie.

Tot slot is goede **handhaving** een randvoorwaarde die niet benoemd is in de criteria, maar door de geïnterviewde ondernemers wel als noodzakelijk wordt benoemd voor succes. Om het draagvlak onder ondernemers te behouden zal er gehandhaafd moeten worden op ondernemers die zich niet aan de nieuwe Alcoholwet houden. Met de NVWA (Nederlandse Voedsel- en Warenautoriteit) als centrale toezichthouder die over gemeentegrenzen heen kan opereren zal dit makkelijker zijn. Tevens heeft de NVWA sinds 1 juli 2021 meer instrumenten om de verkoop van alcohol op afstand te handhaven. Er zal minder nadruk komen op handhaving bij uitlevering, maar meer op de leeftijdsverificatie bij aankoop en de geborgde werkwijze.

Conclusie

Het is de vraag of het verstandig is om te wachten op de verdere doorontwikkeling van recent aangekondigde initiatieven zoals EU digital identity wallet en de in begin 2021 op nationaal niveau aangekondigde Digitale Bron

Identiteit (DBI)[7]. Om op korte termijn vooruitgang te creëren op het vlak van leeftijdsverificatie voor de aankoop van alcohol, is een pragmatische insteek geboden. Blijf niet wachten tot er één optimale oplossing is, die zal er waarschijnlijk nooit komen en vooral niet als er geen vraag naar is. Ga aan de slag met de oplossingen die er al wel zijn. Wijs deze eventueel aan maar sluit het inzetten van andere oplossingen niet uit.

Het vaststellen van eisen waar dergelijke leeftijdsverificatiesystemen aan moeten voldoen is dus wenselijk. Als onderdeel van de eisen moet minimaal een gewenst betrouwbaarheidsniveau opgenomen worden en eisen worden gesteld op het vlak privacy en dataminimalisatie. Hierbij lijkt het eIDAS betrouwbaarheidsniveau substantieel gewenst[8]. Bij het gebruik van een leeftijdsverificatiesysteem bij iedere aankoop is het voldoende om alleen een 18+-attribuut uit te wisselen. Het uitwisselen van leeftijd, geboortedatum of bijbehorende naam is niet nodig om de 18+-controle betrouwbaar uit te voeren.

Daarnaast is het van belang dat het ministerie van VWS duidelijk communiceert wanneer de sector betrouwbare oplossingen voor leeftijdsverificatie moet implementeren en welke extra handelingen dit betekent wanneer een persoon alcohol op afstand wil aankopen. Dit creëert duidelijkheid. Niet alleen voor de webwinkels, maar ook voor de leveranciers van oplossingen en burgers.

[7] De Digitale Bron Identiteit werd gepresenteerd in de kamerbrief Digitale Identiteit. Het is '*een door de overheid uitgegeven, erkende en in de wet- en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector*.' De DBI zal niet direct gebruikt kunnen worden om mee in te kunnen loggen bij andere partijen, maar een gezaghebbende bron waaruit andere authenticatieoplossingen (personal data wallets, consumentenoplossingen, etc.) betrouwbaar de identiteit kunnen ophalen.

[8] De eisen horende bij betrouwbaarheidsniveau substantieel zijn uitgewerkt in de eIDAS uitvoeringsverordening 2015/1502. Het omvat het verplicht gebruik van tweefactor authenticatie en eisen aan identificatie.

1 Inleiding

1.1 AANLEIDING

De verkoop via online kanalen neemt al jaren toe. Dankzij de coronacrisis is deze ontwikkeling nog verder versneld[9]. Dit geldt ook voor de verkoop door speciaalzaken zoals slijters. Uit recent onderzoek blijkt echter dat de leeftijdsverificatie bij online aankoop en thuisbezorging van alcoholhoudende dranken te wensen overlaat[10]. In slechts 8,8% van de gevallen werd 17-jarigen geweigerd als zij online alcohol probeerden aan te schaffen. Er is dus vraag naar betere oplossingen voor leeftijdsverificatie bij de aankoop van alcohol online. Zowel door het ingewikkelder te maken om als minderjarige online alcohol te kopen, als door de uitvoering van de leeftijdsverificatie beter te handhaven.

In november 2020 is een wetswijziging van de Drank- en Horecawet in de Tweede Kamer behandeld[11]. Deze wijziging is per 1 juli 2021 in werking getreden. Sinds die datum heeft de Drank- en Horecawet een nieuwe naam: Alcoholwet. Relevante wijzigingen zijn regels voor de verkoop op afstand (online of telefonisch) van alcoholhoudende dranken en de bijbehorende leeftijdsverificatie. De nieuwe regelgeving stelt dat de verkoper van alcoholhoudende drank (webwinkel) op afstand een werkwijze moet hanteren die waarborgt dat de alcoholhoudende drank slechts wordt afgeleverd op het adres van de geadresseerde of bij een distributiepunt en dat de leeftijd van degene die het pakket aanneemt ook wordt vastgesteld.

Bij de bestelling van alcoholhoudende drank op afstand wordt het verplicht voor de webwinkel om de leeftijdsgrens te controleren. Hiervoor zal gebruik gemaakt worden van een leeftijdsverificatiesysteem. De eisen voor dit leeftijdsverificatiesysteem worden bij Algemene Maatregelen van Bestuur bepaald[12]. Het leeftijdsverificatiesysteem zal in eerste instantie bestaan uit een leeftijdsvraag die bij iedere aankoop gesteld en beantwoord moet worden. Dit met als doel de koper bewust te maken van de aankoop van een leeftijdsgebonden product. Bij dit systeem is echter geen sprake van de controle op de correctheid van het antwoord op de leeftijdsvraag op moment van aankoop en is het dus mogelijk om als koper te liegen over de leeftijd. Wel zal de ontvanger bij aflevering nogmaals op leeftijd gecontroleerd moeten worden door de bezorger. Het verplichte leeftijdsverificatiesysteem beoogt minderjarige kopers te ontmoedigen om alcoholhoudende drank online of telefonisch te bestellen. Het huidige systeem met een vinkje of leeftijdsvraag is echter erg makkelijk om voor te liegen en laat ook te wensen over als het gaat om verificatie bij aflevering.

Het doel van dit onderzoek is om tot nadere criteria te komen voor een toekomstig leeftijdsverificatiesysteem dat kan worden ingezet door webwinkels om op een betrouwbare en eenduidige wijze de leeftijd van de koper op afstand te controleren op moment van aankoop. Om tot deze criteria te komen wordt in kaart gebracht welke digitale leeftijdsverificatiesystemen in Nederland (en daarbuiten) op de markt bestaan en in hoeverre deze systemen aan de criteria voldoen.

Het doel van het onderzoek kan daarmee als volgt worden samengevat tot: *"het in kaart brengen van digitale identificatiesystemen als onderdeel van het leeftijdsverificatiesysteem voor de verkoop van alcohol op afstand en het in algemene zin beschrijven van de effectiviteit, doelmatigheid en andere criteria, waaraan dergelijke systemen zouden moeten voldoen in het geval van verplichtstelling van dergelijke systemen."*

Om dit doel te behalen dienen enkele deelvragen beantwoord te worden:

- Welke leeftijdsverificatiesystemen worden toegepast in Nederland en wat is er bekend over hun effectiviteit in het voorkomen dat jongeren alcohol verkrijgen via verkoop op afstand?

[9] Zie https://www.cbs.nl/nl-nl/nieuws/2020/32/coronacrisis-jaagt-online-winkelen-aan-in-het-tweede-kwartaal
[10] kamerstuk 27565-177, zie https://zoek.officielebekendmakingen.nl/kst-27565-177.html
[11] Zie Kamerbrief Alcoholbesluit (https://www.rijksoverheid.nl/documenten/kamerstukken/2021/01/29/kamerbrief-ontwerpbesluit-houdende-regels-ter-uitvoering-van-de-alcoholwet-alcoholbesluit), Kamerstuk 35 337 (https://zoek.officielebekendmakingen.nl/kst-35337-3.html) en bijbehorende aankondiging in het Staatsblad 2021-26 (https://zoek.officielebekendmakingen.nl/stb-2021-26.html)
[12] Zie Artikel 20a.1 van de Alcoholwet.

Hierbij wordt ook gekeken naar leeftijdsverificatiesystemen in andere sectoren of die internationaal worden toegepast.

- Aan welke (andere) criteria zouden dergelijke systemen moeten voldoen in het kader van leeftijdsverificatie en in hoeverre kunnen de in omloop zijnde systemen op basis van de bestaande gegevens worden beschreven aan de hand van deze criteria?

- Welke belangrijke ontwikkelingen m.b.t. nieuwe leeftijdsverificatiesystemen zijn er gaande of in de nabije toekomst te verwachten?

- In hoeverre zijn de veelbelovende online oplossingen ook toepasbaar in een fysiek scenario?

1.2 PROCES VAN LEEFTIJDSVERIFICATIE

Er zijn twee momenten waarop de leeftijd van de persoon die alcohol aankoopt vastgesteld dient te worden: bij bestelling en bij aflevering. Deze twee momenten kunnen in verschillende situaties voorkomen:

	Scenario's	Bestellen (18+ check)	Betalen	Ontvangst (18+ check)
1	Online + Bezorgen	Online	Online	Huis
2	Online + Afhalen	Online	Online	Pakketpunt/Winkel
3	Online + Betalen bij ontvangst	Online	Pakketpunt/Winkel/Huis	Pakketpunt/Winkel/Huis
4	Fysieke aankoop	Winkel	Winkel	Winkel

- In scenario 1, 2 en 3 zijn er twee aparte momenten van leeftijdsverificatie: bij het bestellen en bij de aflevering (thuis, bij een pakketpunt of winkel).
- In scenario 4, aankoop van alcohol in een fysieke winkel, zijn bestelling en ontvangst gelijktijdig. Er is dan ook maar eenmalig, ter plekke, een leeftijdsverificatie noodzakelijk.

Deze scenario's worden meegenomen in de analyse van de mogelijkheden van de leeftijdsverificatiesystemen door te bepalen in hoeverre een systeem geschikt is voor leeftijdsverificatie online, bij ontvangst (in een winkel/pakketpunt of thuis) en in de winkel zelf (bijvoorbeeld bij een selfservice kassa).

1.3 AANPAK

Het onderzoek heeft een aantal fases doorlopen. Door experts in het onderzoeksteam is een eerste lijst aan criteria geformuleerd om de leeftijdsverificatiesystemen aan te toetsen. Deze lijst is gevalideerd met de begeleidingscommissie van het onderzoek (zie betrokken partijen hieronder) en gedurende het onderzoek verder aangescherpt (zie hoofdstuk 2 voor de beschrijving van de verschillende criteria). Vervolgens is een overzicht gemaakt van beschikbare leeftijdsverificatie systemen. Op basis van expertinput, eerdere onderzoeken en in afstemming met de begeleidingscommissie zijn een aantal categorieën van systemen opgesteld (zie hoofdstuk 3 voor de categorieën en beschrijvingen).

Na het vaststellen van de criteria en de beschikbare systemen, is door het onderzoeksteam een beoordeling gemaakt van de systemen. In deze beoordeling zijn de systemen getoetst en zijn diverse fraudetests van de systemen uitgevoerd. Om het draagvlak te toetsen is met een aantal stakeholders in het domein van alcoholverkoop en distributie gesproken. Deze gesprekken dienden daarnaast het doel om een beter inzicht te verkrijgen in het perspectief van de stakeholders op toekomstige ontwikkelingen op het vlak van identificatie en leeftijdsverificatie. De resultaten van deze analyse zijn te vinden in hoofdstuk 4, 5 en 6. De vragenlijst richting de stakeholders is te vinden in bijlage A.

Geïnterviewde stakeholders:

- Centraal Bureau Levensmiddelen (CBL)
- SlijtersUnie
- PostNL
- Thuisbezorgd
- Albert Heijn
- Afdeling Digitale Identiteit van Ministerie van Binnenlandse Zaken
- Nederlandse Voedsel- en Warenautoriteit (NVWA)
- Gall en Gall
- Whiskybase

De volgende partijen waren vertegenwoordigd in de begeleidingscommissie van het onderzoek:

- CBL
- SlijtersUnie
- Vereniging Drankhandel Nederland (VDN)
- SpiritsNL
- Koninklijke Vereniging Nederlandse Wijnhandelaren
- Nederlandse Brouwers
- Thuiswinkel.org
- NVWA
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Transport en Logistiek Nederland, Deelmarkt Koeriers- en Expresbedrijven (TLN, deelmarkt VKE)
- VNO NCW (Verbond van Nederlandse Ondernemingen – Nederlands Christelijk Werkgeversverbond)
- Logius[13]

1.4 LEESWIJZER

In deze rapportage worden een aantal specifieke en technische termen gebruikt die in het domein van digitale identiteiten gebruikelijk zijn. Denk aan termen als identificatie, authenticatie, toestemming, Decentralised Identifiers, Know Your Customer, etc. Met name in de uitleg van systemen (hoofdstuk 3), analyse van de systemen (hoofdstuk 4) en fraudescenario's (hoofdstuk 5) komen dergelijke termen terug. Voor de lezer die minder bekend is met het domein van digitale identiteiten is in ColofonBijlage A: Begrippenlijst een overzicht opgenomen waarin dergelijk begrippen kort worden toegelicht.

[13] Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Logius biedt voorzieningen en standaarden die alle overheidsorganisaties gebruiken in hun digitale dienstverlening, zoals bijvoorbeeld DigiD, MijnOverheid en Digipoort.

2 Succesfactoren

Om tot een succesvolle realisatie van oplossingen voor online leeftijdsverificatie te komen spelen diverse factoren een rol. Daarnaast moeten oplossingen voldoen aan diverse randvoorwaarden. Dit hoofdstuk beschrijft de succesfactoren en de randvoorwaarden waaraan de leeftijdsverificatiesystemen getoetst kunnen worden. Aan de hand van de analyse en interviews wordt in de conclusie advies gegeven over welke succesfactoren door VWS als eisen gesteld moeten worden en welke essentieel zijn voor succesvolle implementatie en voldoende draagvlak onder ondernemers.

2.1 SUCCESFACTOREN

Op basis van eerder onderzoek naar oplossingen voor leeftijdsverificatie[14] en interviews met stakeholders is duidelijk dat de volgende factoren een rol spelen bij oplossingen voor leeftijdsverificatie:

2.1.1 Fraudebestendigheid en betrouwbaarheid

Het moge duidelijk zijn dat de huidige oplossing waarbij de klant zelf moet aangeven of hij/zij ouder is dan 18 jaar veel te wensen over laat in termen van betrouwbaarheid. Meer zekerheid is gewenst voor de webwinkelier om te kunnen voldoen aan zijn wettelijke verantwoordelijkheden aangaande het verifiëren van de leeftijd van de klant: Welke zekerheid heeft de webwinkelier aangaande de betrouwbaarheid van de leeftijd van de klant? Ofwel, in hoeverre beperkt de oplossing de mogelijkheid voor het plegen van leeftijdsfraude? Hierbij speelt onder andere de vraag hoe makkelijk het is om eenmalig of juist herhaaldelijk leeftijdsfraude te plegen. Voor de uitgebreide fraudescenario's, zie hoofdstuk 5.

Eén van de belangrijke indicatoren om fraudebestendigheid in kaart te brengen is het betrouwbaarheidsniveau van een oplossing. Om de benodigde betrouwbaarheid voor online drankverkoop goed in te kunnen schatten, kan gebruik worden gemaakt van de handreiking die door Forum Standaardisatie is opgesteld.[15] Deze handreiking richt zich specifiek op het overheidsdomein, maar kan ook voor private dienstverlening als goed uitgangspunt worden beschouwd. De handreiking hanteert criteria zoals rechtsgevolgen en publieke belangen voor het inschatten van de voor een online dienst gewenste betrouwbaarheid van de identiteitsgegevens. Voor online drankverkoop is er een direct rechtsgevolg als de leeftijdsverificatie niet voldoende betrouwbaar wordt gedaan. Hiernaast is er kans op publieke onrust. Het wordt als maatschappelijk onwenselijk gezien als jongeren aan alcohol kunnen komen. Dit kan leiden tot klachten en berichten in de media en mogelijk zelfs Kamervragen in politiek Den Haag. Ook speelt het belang van de volksgezondheid, in het bijzonder die van jongeren mee. Dit wordt niet meegewogen in de handreiking, maar moet wel als een verzwarende factor beschouwd worden. Op basis hiervan is een substantieel betrouwbaarheidsniveau[16] over de leeftijd van de klant wenselijk. De specifieke eisen waar een identificatieoplossing op een bepaald betrouwbaarheidsniveau aan moet voldoen zijn vastgelegd in de eIDAS uitvoeringsverordening[17]. Een oplossing op niveau substantieel moet onder andere gebruik maken van twee-factor authenticatie. Daarnaast moet het zo ontworpen zijn dat verondersteld kan worden dat het identificatiemiddel slechts kan worden gebruikt door of onder controle van de persoon aan wie het toebehoort. Ook worden er eisen gesteld aan hoe de identiteit bij registratie betrouwbaar vastgesteld moet worden. Bijvoorbeeld op basis van een WID of door gebruik te maken van een middel dat minimaal op hetzelfde betrouwbaarheidsniveau zit.

In vergelijking met de huidige zelfverklaarde oplossing zijn dus striktere methoden voor verificatie nodig. Om te toetsen of een oplossing aan het gewenste betrouwbaarheidsniveau voldoet, kan gekeken worden naar de eisen zoals die in de eIDAS verordening en bijbehorende uitvoeringsverordening worden gesteld[18]. Deze eisen

[14] Online leeftijdsverificatie in Nederland – Marktverkenning, InnoPay (2013). Zie https://saferinternetcentre.nl/wp-content/uploads/2019/08/Online-leeftijdsverificatie-in-Nederland.pdf
[15] zie handreiking betrouwbaarheidsniveaus, https://www.forumstandaardisatie.nl/sites/default/files/BFS/4-basisinformatie/publicaties/fs-handreiking-betrouwbaarheidsniveus-v4_0.pdf
[16] Zoals beschreven in de eIDAS verordening (nr 910/2014)
[17] Uitvoeringsverordening 2015/1502, beschikbaar via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502
[18] Zie 16 en de eIDAS uitvoeringsverordening (nr 2015/1502)

worden ook als uitgangspunt gehanteerd in de wet Digitale Overheid die momenteel nog in behandeling is[19]. Deze wet maakt het mogelijk om private inlogmiddelen toe te laten tot het overheidsdomein, zodat burgers hiermee bij de overheid kunnen inloggen.

2.1.2 Beschikbaarheid en dekkingsgraad

Webwinkeliers zijn gebaat bij oplossingen die breed beschikbaar zijn in de Nederlandse samenleving en geen klanten uitsluiten als het aankomt op leeftijdsverificatie. Omdat de leeftijdsverificatie alleen plaats hoeft te vinden als de onderneming en de klant in Nederland gevestigd zijn, is het voldoende om te kijken naar de dekkingsgraad onder Nederlanders. De verwachting is dat ondernemers de voorkeur geven aan één oplossing met een hoge dekkingsgraad, in plaats van diverse oplossingen voor deelgroepen van klanten of voor specifieke processen. Een alternatief zou een systeem kunnen zijn waarin de gebruiker kan kiezen uit een leeftijdsverificatie-oplossing naar keuze, vergelijkbaar met hoe betaalproviders (Payment Service Provider) als Adyen en Mollie nu een betalingsplatform aanbieden. Bij dergelijke platformen kan de klant zelf kiezen uit de verschillende betaaloplossingen die door de winkelier geaccepteerd worden. Voor deze succesfactor wordt allereerst gekeken in hoeverre een oplossing al in gebruik is in de samenleving (dekkingsgraad). Daarna wordt er gekeken welk deel van de bevolking een oplossing zou kunnen aanvragen (beschikbaarheid).

2.1.3 Gebruiksgemak en begrijpbaarheid

Conversie is de sleutel voor de webwinkelier en dit wordt grotendeels bepaald door het gebruiksgemak van de oplossing. Klanten kunnen in het besteltraject afhaken als de oplossing te veel interactie vereist of als niet duidelijk uitlegbaar is waarom bepaalde handelingen moeten worden verricht. Dit is onwenselijk. Een toekomstige oplossing moet voor gebruikers met verschillende niveaus van ‘digivaardigheid’ begrijpelijk en toegankelijk zijn. Idealiter moet het doel zijn dat iedereen die online alcohol wil en mag kopen en dat nu kan, dat met het toevoegen van een leeftijdsverificatie nog steeds kan doen. Oplossingen dienen dus goed te begrijpen en gebruikersvriendelijk te zijn.

2.1.4 Schaalbaarheid en flexibiliteit

Belangrijk is dat de oplossing schaalt voor grote aantallen klanten. Biedt de oplossing mogelijkheden voor straight-through-processing van leeftijdsverificatie of zijn er handmatige handelingen vereist door de aanbieder van de oplossing? Handmatige stappen (denk bijvoorbeeld aan een medewerker die een identiteitsbewijs moet bekijken en goedkeuren) die bij iedere leeftijdsverificatie of authenticatie uitgevoerd moeten worden vertragen het proces en dit zal bovendien ten koste gaan van de schaalbaarheid. Handmatige stappen voor eenmalige identificatie om een middel uit te geven hebben minder grote impact. Zeker niet als de dekkingsgraad (2.1.2) al hoog is en weinig nieuwe gebruikers het middel hoeven aan te vragen.

Naast dat de oplossing schaalbaar moet zijn, kan het van meerwaarde zijn als de oplossing ook inzetbaar is voor andere toepassingen of in bredere context. Het wordt dan aantrekkelijker voor de klant om een oplossing te gebruiken. Kan de oplossing bijvoorbeeld ook online worden ingezet voor gamen gokken, bestellen van medicijnen of 18+ videocontent? Of is het mogelijk om de oplossing ook in een fysieke context in te zetten, zoals in de winkel of bij afleveringen van de bestelde producten? Dit komt tevens het gebruikersgemak ten goede.

2.1.5 Kosten

Het ligt in de lijn der verwachting dat de extra kosten voor leeftijdsverificatie doorberekend zullen worden aan de klant. Extra kosten voor het verifiëren van de leeftijd van de klant dienen zo laag mogelijk te zijn. Enerzijds omdat deze verificatie bij iedere transactie moet plaatsvinden. Anderzijds om een eerlijke concurrentiepositie te behouden ten opzichte van buitenlandse ondernemers die geen leeftijdsverificatie hoeven te doen. Naast de kosten per verificatie zijn er kosten gemoeid met het implementeren van de oplossing door de webwinkelier in de website en de achterliggende bestelsystemen. Deze dienen om te kunnen gaan met situaties waarin een verificatie vereist is en de uitkomsten van deze verificatie.

Bij de kosten moet rekening gehouden worden met de verschillen tussen de verschillende soorten verkopers van alcohol op afstand. Voor de lokale slijter met een kleine webwinkel kunnen hoge implementatiekosten een drempel opwerpen. Terwijl hij misschien wel bereid is iets meer per transactie te betalen. Grote webwinkels zullen hoge implementatiekosten over het algemeen beter kunnen dragen dan kleinere ondernemers.

[19] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/wet-digitale-overheid-in-het-kort

Tegelijkertijd zijn de marges per bestelling voor grotere webwinkels vaak kleiner[20] en zullen de kosten per transactie een grotere rol spelen. Aan het einde van het verhaal is de vraag: Zijn de totale kosten van de leeftijdsverificatie-oplossing aanvaardbaar voor zowel de kleinere als grotere webwinkelier?

2.1.6 Realisatietermijn

Het is wenselijk dat een gekozen oplossing snel gerealiseerd kan worden. Dit omdat de tijdelijke oplossing met een leeftijdsvinkje of geboortedatum onvoldoende betrouwbaarheid biedt. Er zijn een aantal randvoorwaarden die hier invloed op hebben. Bijvoorbeeld of de oplossing al volwassen genoeg is om direct gerealiseerd en geïmplementeerd te worden. Hiernaast speelt nog de vraag of de oplossing direct geschikt is voor leeftijdsverificatie. Mogelijk zijn hiervoor nog technische, juridische of organisatorische aanpassingen nodig. Als al deze punten meegenomen worden, moet het geheel optellen tot een realistische termijn waarin online leeftijdsverificatie mogelijk gaat zijn. Een harde termijn voor wanneer er strengere eisen vanuit VWS gesteld worden, moet nog officieel vastgesteld worden. Er wordt gestreefd naar een termijn van 2 jaar. Zodoende wordt voor de analyse in dit onderzoek een realisatietermijn van maximaal 2 jaar aangehouden.

2.1.7 Toekomstbestendigheid

Belangrijk is dat de oplossing niet alleen nu, maar ook in de toekomst beschikbaar is en blijft. Het is voor de ondernemer vervelend als hij om de twee jaar van oplossing moet wisselen. Dit schaadt tevens het gebruikersgemak en vertrouwen. Hiertoe moet overwogen worden hoe volwassen de sector of specifieke oplossing is. Is er een grote kans dat de oplossing op lange termijn beschikbaar en onderhouden blijft? Ook dient hierin meegenomen te worden hoe de markt, sector of oplossing zich naar verwachting zal ontwikkelen. Hierbij spelen naast organistische vraagstukken ook juridische en politieke uitdagingen. Wetgeving en politiek kunnen immers een specifieke categorie van oplossingen voor authenticatie en leeftijdsverificatie stimuleren, maar ook tot een halt roepen.

2.1.8 Vertrouwen en privacy

Een belangrijke voorwaarde vanuit het gebruikersperspectief is niet alleen dat de klant de oplossing gebruikersvriendelijk vindt, maar ook dat de klant het leeftijdsverificatiesysteem vertrouwt. Zonder vertrouwen zal de klant immers niet bereid zijn om zijn leeftijd te verifiëren en geen bestelling plaatsen, waardoor conversie daalt. Dit hangt samen met dat de klant begrijpt waarom hij zijn leeftijd moet laten zien, maar ook vertrouwen heeft in de specifiek gebruikte oplossing. Dit hangt onder andere af van het vertrouwen in de organisatie achter de oplossing. DigiD (vanuit de overheid) en iDEAL (vanuit de banken) zijn bijvoorbeeld erg sterke en bekende merken, waardoor deze snel vertrouwd zullen worden. Het introduceren van een centrale partij voor leeftijdsverificatie brengt ook het risico van een ‘big brother effect’ met zich mee. Waar bij het tonen van een WID alleen de webwinkel inzicht krijgt in het aantal aankopen, heeft bij een online leeftijdsverificatie met een digitaal middel de partij die de leeftijdsverificatie uitvoert hier ook inzicht in. Afhankelijk van de gekozen partij kan dit onwenselijk zijn.

Naast vertrouwen in de organisatie, is ook privacy van groot belang. Biedt de oplossing voldoende garanties om de privacy van de klant te waarborgen? Is de impact van de oplossing op de privacy van de klant niet te groot en proportioneel met het doel van de bestelling. Het inzetten van biometrie voor leeftijdsverificatie heeft bijvoorbeeld een grotere impact op de klant dan dit te doen via een betaaltransactie. Tot slot is het de vraag welke data de oplossing levert. Levert de oplossing een complete set aan data, enkel de geboortedatum van de klant aan of een verklaring dat deze ouder dan 18 jaar is? De laatste optie past binnen privacy-by-design en is vanuit het concept van dataminimalisatie zoals vastgelegd in de AVG ook de meest voor de hand liggende optie.

2.1.9 Draagvlak

Naast vertrouwen van de klant, moet voor daadwerkelijk succes ook de webwinkelier geloven in de oplossing. De vraag is dus welke oplossing de voorkeur geniet van de webwinkeliers zelf? Dit hangt grotendeels af van bovenstaande factoren, maar ook van het soort webwinkelier. Online slijters, slijters met een kleine webwinkel, supermarkten en maaltijdbezorgers zullen allen andere wensen hebben bij een dergelijk systeem. Het draagvlak is onder meer getoetst via verschillende interviews en via de feedback die vanuit de begeleidingscommissie verzameld werd.

[20] Zie bijvoorbeeld https://www.webwinkelsucces.nl/tips-betere-prijsstrategie-webwinkel/

3 Oplossingscategorieën

Online leeftijdsverificatie kan op verschillende manieren en vanuit verschillende bronnen en systemen worden uitgevoerd. Onderstaande paragrafen beschrijven de verschillende categorieën waarin deze oplossingen onderverdeeld kunnen worden. Zie ook bijlage A voor verdere toelichting van de specifieke begrippen die gebruikt worden in dit en opvolgende hoofdstukken. De categorieën worden geïllustreerd met specifieke voorbeelden van systemen door verschillende aanbieders. Dit hoofdstuk geeft antwoord op de eerste onderzoeksvraag:

Welke digitale leeftijdsverificatie- en identificatiesystemen worden toegepast in Nederland, wat is de werking (een beschrijving ervan)?

Onderstaande oplossingscategorieën zijn systemen die worden toegepast in Nederland voor identificatie en uitwisseling van attributen voor diverse toepassingen in diverse sectoren. Deze categorieën worden uitgebreid toegelicht in de volgende paragrafen. Een korte beschrijving van de verschillende categorieën wordt gegeven in Tabel 1.

Tabel 1 Korte omschrijving van de oplossingscategorieën

Categorie	Omschrijving **categorie**
Zelf toegezegd	Eigen verklaring van de persoon, bijvoorbeeld: ik ben 18 jaar of ouder.
Overheidsoplossingen	Digitale oplossing uitgegeven door de overheid en gericht op het identificeren van burgers bij overheidsinstanties of dienstverleners met een publieke taak.
Consumentenoplossingen	Digitale oplossingen uitgegeven door een private partij en gericht op het identificeren van consumenten bij andere partijen, gebruikelijk een dienstverlener.
Betaaloplossingen	Oplossingen gericht op het doen van een (online) betaling.
Personal data wallets	Digitale oplossing die het mogelijk maakt voor het individu om veilig en onder eigen regie zijn of haar eigen persoonlijke data in te zien, op te halen en te delen. Ook Self Sovereign Identity (SSI) oplossingen vallen hier onder.
Identificatie op afstand (IoA)	Oplossing gericht op het op afstand identificeren van een consument. De consument kan dit vanuit huis (of andere locatie naar voorkeur) doen en hoeft hiervoor niet naar een servicebalie te komen.

3.1 ZELF TOEGEZEGD

De zelf toegezegd categorie bevat oplossingen waarin een gebruiker zelf toezegt dat hij voldoet aan de 18+ eis (of een andere eis). Zelf toegezegd betekent dus dat een gebruiker, zonder verdere verificatie of controle, aangeeft dat hij voldoet aan de 18+ voorwaarde. Deze toezegging kan op verschillende manieren gedaan worden, door bijvoorbeeld de geboortedatum op te geven, maar ook door aan te geven ouder te zijn dan 18. Voorbeelden hiervan zijn een "vinkje" op een website of een gesproken bevestiging via telefoon of in persoon. Beide voorbeelden worden hieronder uitgewerkt.

De oplossingen in deze categorie vereisen geen ingewikkelde technische handelingen van de gebruiker of de website. De betrouwbaarheid van de oplossingen in deze categorie is slecht, omdat het makkelijk is om te liegen over de gevraagde data en er geen verificatie of controle plaatsvindt.

3.1.1 Vinkje “ik ben ouder dan 18” of geboortedatum invullen

Het vinkje is een simpele manier voor gebruikers om te bevestigen dat zij ouder zijn dan 18. Het vereist een minimale handeling waarbij de gebruiker het vinkje aanklikt, waarna het door kan gaan op de website of met de bestelling. In sommige gevallen wordt de gebruiker gevraagd om een geboortedatum boven de 18 in te vullen.

Daarbij is deze manier van bevestigen van een attribuut of het geven van toestemming vergelijkbaar met vinkjes die ook veel online gebruikt worden, zoals “ik ga akkoord met de cookie voorwaarde” en “ik heb de

privacy regelementen gelezen". De wettelijke basis van deze toestemming vinkjes komt vanuit de AVG (Algemene Verordening Gegevensbescherming), waarin staat dat toestemming gevraagd moet worden "[…] in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden."

3.1.2 Toezegging via telefoon

De telefonische oplossing waarbij de gebruiker zijn leeftijd doorgeeft via de telefoon wordt bijvoorbeeld bij banken of andere bel diensten gebruikt. Daarbij kan een "Bent u ouder dan 18" vraag gecombineerd worden met dat de klant gevraagd wordt om zich te identificeren door het beantwoorden van een aantal persoonlijke vragen (naam, geboortedatum, adres, postcode, etc.). Deze oplossing wordt niet gecontroleerd of geverifieerd behalve aan de hand van een gesproken bevestiging.

Om betrouwbaardere authenticatie via de telefoon te kunnen doen, kunnen ook diepgaandere vragen zoals de meisjesnaam van je moeder gesteld worden. Deze informatie moet dan al wel eerder vastgelegd zijn en de klant moet dus al in een eerder stadium een keer geïdentificeerd zijn. Voor betrouwbare authenticatie is het van belang dat dergelijke informatie niet publiek beschikbaar is.

3.2 OVERHEIDSOPLOSSINGEN

Overheidsauthenticatieoplossingen, kortweg overheidsoplossingen, zijn middelen die uitgegeven worden door de overheid. De bestaande overheidsmiddelen kunnen alleen gebruikt worden binnen het overheidsdomein en bij organisaties met een publieke taak. Bestaande middelen zijn DigiD en Europese middelen die toegelaten zijn binnen het eIDAS stelsel. Hiernaast doet BZK momenteel onderzoek naar een nog te ontwikkelen Digitale Bronidentiteit. Hiermee moet het mogelijk worden om een door de overheid uitgegeven set identiteitsgegevens, de bronidentiteit, in te laden in identiteitsoplossingen, bijvoorbeeld consumentenoplossingen of personal data wallets, die ook buiten het overheidsdomein te gebruiken zijn. De Rijksdienst voor Identiteitsgegevens (RvIG) is bezig met een vID, een digitale versie van een identiteitsbewijs in de vorm van een app op een smartphone.

3.2.1 DigiD

DigiD is het authenticatiemiddel voor burgers om in te loggen bij overheidsdiensten en bij organisaties met een publieke taak. DigiD mag alleen door een organisatie gebruikt worden als hier een wettelijke basis voor is, zoals vastgelegd in de WABB[21] – Wet algemene bepalingen BSN. Momenteel kan het daarom niet gebruikt worden voor private dienstverlening. DigiD geeft niet automatisch iemands leeftijd terug. Bij inloggen met DigiD ontvangt de dienstverlener het BSN van de gebruiker die inlogt. Eventuele andere gegevens, zoals naam en leeftijd, dienen apart opgehaald te worden. Bijvoorbeeld uit de BRP (Basisregistratie Personen). Met ruim 18,3 miljoen accounts is de dekkingsgraad van DigiD hoog[22]. Wat betreft vertrouwen door gebruikers is DigiD ook een erg sterk merk.

3.2.2 Digitale Bronidentiteit

Begin 2021 werd het concept van de Digitale Bronidentiteit (DBI) gepresenteerd in de kamerbrief 'visiebrief digitale identiteit'[23]. De DBI zal in tegenstelling tot DigiD geen authenticatiemiddel worden, maar zal de mogelijkheid bieden om een set geverifieerde identiteitsgegevens bij de overheid op te halen. De burger kan deze gegevens vervolgens zelfstandig gebruiken en delen. De gegevens zouden bijvoorbeeld in een PDM-oplossing – wallet – geladen kunnen worden. Hierna kan de gebruiker deze onder eigen regie met andere partijen delen. Het concept DBI is momenteel nog in de verkennende fase. Naar verwachting zullen in 2022 de eerste pilots gedraaid worden met de DBI. Hoe snel de ontwikkelingen zullen gaan rondom de DBI zal onder meer afhangen van de politieke urgentie die de DBI krijgt van het nieuwe kabinet. Er mag echter vanuit gegaan worden dat het nog enkele jaren zal duren voordat een DBI breed beschikbaar komt.

3.2.3 vID

Een vID (virtueel ID) is een digitale versie van een identiteitsbewijs. Het identiteitsbewijs wordt in digitale vorm beschikbaar gemaakt in de vorm van een app. Afhankelijk van de gekozen richting kan een vID in fysieke context, online context of in beide contexten gebruikt worden. Het concept van vID is niet uitsluitend

[21] https://wetten.overheid.nl/BWBR0022428/2018-06-13
[22] Cijfers over DigiD in 2020: https://magazines.logius.nl/logiusjaarverslag/2020/01/4-logius-diensten-het-jaar-in-cijfers
[23] Zie https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/11/kamerbrief-over-visie-digitale-identiteit

Nederlands. Meerdere landen werken aan vergelijkbare concepten. In Denemarken is eind 2020 bijvoorbeeld een digitaal rijbewijs geïntroduceerd[24]. In Nederland werkt de RvIG aan de ontwikkeling van een vID die zowel fysiek als online te gebruiken is[25]. Online leeftijdsverificatie wordt hierbij expliciet als één van de use-cases genoemd. In 2019 en 2020 zijn verschillende gebruikersonderzoeken en pilots gedaan. Momenteel wordt gewerkt aan het programma van eisen voor een Nederlandse vID. Het is echter nog onduidelijk of er daadwerkelijk een Nederlandse vID komt en zo ja op welke termijn deze er moet zijn.

3.3 CONSUMENTENOPLOSSINGEN

Consumentenauthenticatieoplossingen, kortweg consumentenoplossingen, hebben de mogelijkheid gebruikers te authentiseren en identificeren binnen het consumentendomein. Ze voorzien in gegevensuitwisseling ten behoeve van de online authenticatie van de gebruiker en diens autorisaties (machtigingen) voor toegang tot online diensten. Veel van de oplossingen in de markt bieden tegenwoordig een federatieve identiteit. Federatief betekent dat je met één en hetzelfde authenticatiemiddel, namelijk een online identiteit bij een identiteitsprovider, bij verschillende partijen kunt inloggen. Denk hierbij aan iDIN (sectie 3.3.1), waarmee de gebruiker bij verschillende dienstverleners kan inloggen met de inlogmethode van de bank. Ook behoren oplossingen waarbij je met verschillende identiteitsproviders kunt inloggen bij één of meerdere diensten tot de mogelijkheden.

Consumentenoplossingen kunnen door verschillende partijen worden aangeboden. Waar bij iDIN de bank identiteit gebruikt wordt, gebruikt itsme (sectie 3.3.2) voor Nederlanders bijvoorbeeld het identiteitsdocument van de gebruiker en Mobile Connect[26] gebruikt gegevens die voor de telecomsector bekend zijn. De betrouwbaarheid van de gegevens hangt hierdoor sterk af van de bronidentiteit. Elk ontsluiten gegevens zoals naam en geboortedatum welke gebruikt kunnen worden om gebruikers te identificeren en daarbij de 18+ check te doen.

Het komt ook voor dat een personal data wallet (zie 3.5) een consumentenoplossing gebruikt als data bron. Zo wordt data vanuit iDIN opgehaald door IRMA en Schluss.

3.3.1 iDIN

iDIN[27] is een oplossing die is ontstaan vanuit een samenwerking van de Nederlandse banken voor de consumenten. Bij iDIN loggen gebruikers in via hun eigen bank, om vervolgens via iDIN geauthentiseerd te worden naar een andere dienst. Het iDIN account is dus direct gekoppeld aan het persoonlijke bank account van de gebruiker. De gegevens die door iDIN ontsloten worden, zijn betrouwbaar door de strenge KYC (Know Your Customer) eisen die aan de banken gesteld worden in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme[28]. Banken hebben op een eerder moment de identiteit van de gebruiker betrouwbaar vastgesteld door een wettelijk identificatiedocument (WID) te controleren, fysiek of met behulp van identificatie op afstand (IoA) technologie. iDIN is beschikbaar voor de meeste mensen met een Nederlands bank account. Bedrijven kunnen iDIN als inlog methode gebruiken om gebruikers te laten inloggen en deze uniek te identificeren. De kosten van het inloggen met iDIN verschillen per aanbieder maar zijn beschikbaar vanaf 13 cent[29]. Het betrouwbaarheidsniveau van iDIN is substantieel.[30] Het koppelvlak om met iDIN te werken bestaat al, daarbij bieden verschillende partijen ondersteuning in het implementatietraject.

3.3.2 itsme

itsme[31] is een Belgische variant van DigiD, die Belgische burgers een online uniek nummer geeft, welke beschikbaar is voor alle consumenten en sectoren (niet overheid alleen). itsme identificeert gebruikers met de Belgische identiteitskaart of via een bank, waarna gebruikers de app kunnen gebruiken om op verschillende plekken hun identiteit te laten zien. Sinds kort is itsme ook in Nederland actief. Nederlandse gebruikers kunnen

[24] https://www.thelocal.dk/20201124/denmark-introduces-digital-driving-licence/
[25] https://www.rvig.nl/digitale-identiteit/digitaal-identiteitsbewijs
[26] https://mobileconnect.io/
[27] iDIN, https://www.idin.nl/
[28] Wet ter voorkoming van witwassen en financieren van terrorisme, zie https://wetten.overheid.nl/BWBR0024282/2021-07-01.
[29] Zie bijvoorbeeld https://bluem.nl/identificeren/
[30] https://www.idin.nl/cms/files/Productleaflet-iDIN.pdf
[31] itsme. https://www.itsme.be/

een itsme aanmaken met een Nederlands identiteitsdocument dat NFC ondersteunt[32]. Hierbij maakt itsme gebruik van Identifcatie op Afstand technologie (zie sectie 3.6). itsme is van oorsprong een authenticatievoorziening, maar biedt ook functionaliteiten om andere attributen uit te wisselen.

itsme kan voor bedrijven al voor 61 cent per gebruiker per jaar gebruikt worden[33], waarmee het bedrijf via itsme toegang krijgt tot een geverifieerd ID. Daarbij zijn er initiële kosten aan verbonden (à 1500 euro) en is er mogelijkheid tot maintenance en support voor 250 euro per maand extra.

3.3.3 Mobile Connect

Mobile Connect[34] is een voorbeeld van een samenwerking binnen de telecomsector om consumenten te authentiseren, waarbij persoonsgegevens, zoals geboortedatum, gebruikt en gedeeld kunnen worden. Deze zouden gebruikt kunnen worden voor leeftijdsverificatie. Verschillende internationale telecombedrijven zijn hierop aangesloten of gebruiken Mobile Connect om gebruikers te authentiseren. Mobile Connect biedt twee verschillende niveaus van online authenticatie, met één of twee factoren. De data afnemers (welke bijvoorbeeld een slijterij zou kunnen zijn) kan hiermee gebruikers authentiseren. Mobile Connect wordt momenteel voornamelijk door KPN en haar dochterondernemers ondersteund[35]. Voordeel is dat Mobile Connect een internationaal concept is en daardoor ook in andere landen beschikbaar is.

3.4 BETAALOPLOSSINGEN

Betaaloplossingen bestaan in veel verschillende vormen. Denk aan iDEAL, PayPal, Apple Pay, creditcards en Klara. In de fysieke context wordt er hiernaast vaak cash of met pin betaald. De oplossingen verschillen sterk van elkaar, onder andere in gebruik en betrouwbaarheid. Aan betaaloplossingen worden strenge Know Your Customer (KYC) eisen gesteld. Hierdoor hebben ze de identiteit van de gebruiker betrouwbaar vastgesteld. Betaaloplossingen zijn echter niet ontwikkeld als identificatie- of authenticatieoplossing. Ze zijn ook niet primair ontwikkeld om een leeftijdsverificatie uit te voeren. Een aantal van de oplossingen, zoals een creditcard, zijn alleen te verkrijgen voor mensen van 18 jaar en ouder. Zodoende kan uit dergelijke middelen wel een leeftijd afgeleid worden van de eigenaar van de betaaloplossing.

3.4.1 iDEAL

iDEAL is de betaaloplossing van verschillende Nederlandse banken. Als een gebruiker iDEAL aanklikt als betaalmethode, moet hij eerst de bank selecteren waarmee hij wil betalen. Vervolgens logt de klant bij zijn eigen bank in en bevestigt de betaling. Omdat veel Nederlanders over internetbankieren beschikken, kunnen ze ook gebruik maken van iDEAL. De dekkingsgraad van iDEAL is zeer hoog, 99% van de online shoppers gebruikt het betaalmiddel[36]. iDEAL deelt alleen betaalgegevens, maar geen leeftijdsgegevens bij een betaling. Het broertje iDIN is wel ontwikkeld om identiteitsgegevens te delen, maar hier kan dan weer niet mee betaald worden. Een integratie waarmee een iDIN-verificatie en iDEAL-betaling in één sessie gedaan kan worden bestaat momenteel nog niet.

3.4.2 Creditcard

Creditcards zijn geschikt om zowel online als fysiek in de winkel mee te betalen. Om een creditcard aan te vragen moet de gebruiker minimaal 18 jaar zijn. De uitgever van de creditcard dient dit te controleren. Creditcards worden lang niet overal geaccepteerd waar gepind kan worden. Ook niet alle webwinkels accepteren creditcards als betaalmiddel. Om online te betalen zijn de naam, het creditcardnummer, verloopdatum en CVC code nodig. Deze gegevens zijn allemaal op het pasje gedrukt. Iemand die de creditcard (onbedoeld) in handen krijgt, kan er hierdoor makkelijk mee betalen. Dit is een mogelijk risico voor fraude in de context van leeftijdsverificatie. Om het online betalen met creditcard betrouwbaarder te maken, kan gebruik gemaakt worden van 3D Secure[37]. Hierbij moet met een extra authenticatiefactor, bijvoorbeeld goedkeuring in

[32] Voor meer informatie, zie https://support.itsme.be/hc/nl/articles/360060551074-Hoe-kan-ik-mijn-itsme-account-aanmaken-met-een-Nederlandse-eID-of-paspoort-
[33] Zie https://business.itsme.be/nl
[34] https://mobileconnect.io/
[35] Zie https://www.mijnmobileconnect.nl/
[36] https://www.ideal.nl/15jaar/
[37] Ook bekend onder de namen Verified by Visa en Mastercard SecureCode. Zie ook https://en.wikipedia.org/wiki/3-D_Secure

de app van de bank, de online betaling goedgekeurd worden. Het gebruik van 3D Secure verlaagt voor de ondernemer tevens het risico op chargebacks, het terug moeten betalen van een eerder ontvangen betaling.

3.4.3 PayPal

PayPal is een online betaalplatform. Om met PayPal te kunnen betalen, kun je of saldo aan een account toevoegen of direct een betaalrekening of creditcard koppelen. Hiermee kan vervolgens betaald worden in verschillende webwinkels. Naast de gebruikelijke klantreis waarbij de klant eerst zijn NAW-gegevens invult en daarna betaalt, biedt PayPal ook Express Checkout. Hierbij hoeft de klant niet eerst apart de NAW-gegevens in te vullen, maar worden deze met de betaling van PayPal meegestuurd. De leeftijd van een klant is echter geen onderdeel van de gegevens die PayPal verstuurt. Een PayPal-account is officieel alleen aan te vragen vanaf 18 jaar. Een uitgebreide KYC-procedure vindt echter niet altijd direct bij aanmaken van het account plaats.

3.5 PERSONAL DATA WALLETS

Een relatief nieuwe ontwikkeling is het gebruik van mobiele 'wallets' van waaruit de gebruiker gecontroleerd data kan verstrekken aan dienstverleners. Deze ontwikkeling wordt ook wel Personal Data Management (PDM) of Self-Sovereign Identity (SSI) genoemd[38]. PDM gaat over toegang, gebruik, correctie en delen van persoonlijke data, onder regie van het individu. De gegevens zijn beveiligd en digitaal ondertekend, waardoor de ontvangende partij de echtheid ervan kan controleren. In PDM staat de gebruiker centraal en heeft deze controle over het delen van zijn persoonlijke data. In de basis omvat PDM vier rollen: de persoon, de data afnemer, de data aanbieder en de wallet. De persoon bepaalt welke gegevens uit welke bron met welke afnemer worden gedeeld. Uitgangspunt daarbij is dat de gegevens bij de gezaghebbende, vertrouwde bron staan: de data aanbieder. De data aanbieder, ofwel data leverancier, beschikt over persoonlijke gegevens van de persoon en maakt het mogelijk deze te delen. De data afnemer kan, met toestemming van de persoon, de gegevens ophalen bij de databron en deze verwerken. Data afnemers zijn typische dienstenleveranciers die gegevens van de klant nodig hebben voor hun dienstverlening, maar ook de klant optimaal willen bedienen.

In het geval van leeftijdsverificatie zal de slijterij of online webwinkel dan ook de rol van data afnemer nemen. Personal data wallets laten gebruikers hun persoonlijke data ophalen en delen met verschillende partijen. Ze kunnen allerlei verschillende type data ontsluiten, zoals naam en geboortedatum. Deze categorie bevat een aantal oplossingen die op het eerste oog erg geschikt lijken voor leeftijdsverificatie, met name omdat leeftijdsattributen door diverse operators ontsloten worden, vaak in de vorm van een "18+" attribuut. Deze attributen kunnen op verschillende manieren ingeladen worden in de wallet. IRMA ontvangt de gegevens door met DigiD in te loggen ondersteund door een aantal gemeentes (die de BRP gegevens doorgeven). Datakeeper haalt de gegevens op uit een WID.

Er is een grote hoeveelheid aan aanbieders van persoonlijke apps waarin een gebruiker zijn data zelf opslaat, bijvoorbeeld op een mobiele telefoon. Enkele voorbeelden van dergelijke wallets zijn IRMA[39], Schluss[40], Ockto[41], Digi.me[42], Financieel Paspoort[43], Datakeeper[44] en Buddy Payment[45]. Ter illustratie beschrijven we twee bekende wallets.

3.5.1 IRMA

IRMA[46] (I share my Attributes) is een mobiele app die gericht is op het delen van attributen. Alleen de attributen die nodig zijn hoeven te worden gedeeld. Zo bevat IRMA ook het 18+- attribuut welke gedeeld kan worden zonder de exacte geboortedatum te hoeven delen. Hierdoor is de privacy voor de gebruiker hoog. Ook de veiligheid is goed geborgd, omdat de gebruiker deze attributen alleen op zijn eigen telefoon opslaat. IRMA

[38] Voor meer informatie over PDM en een recent overzicht van het Nederlands PDM overzicht, zie ook '*PDM landschap 2020 – Regie op gegevens in Nederland*' – Innovalor, 2020. Beschikbaar via https://innovalor.nl/digitaal-vertrouwen/persoonlijk-datamanagement
[39] https://privacybydesign.foundation/irma/
[40] https://schluss.org/nl/
[41] https://www.ockto.nl/
[42] https://digi.me/
[43] https://financieelpaspoort.nl/
[44] https://datakeeper.nl/
[45] https://buddypayment.nl/
[46] https://privacybydesign.foundation/irma/

en andere partijen hebben hier zonder consent van de gebruiker geen toegang toe. Voor de gebruiker is toegang tot de app is vergrendeld met een PIN-code. De attributen die ingeladen worden door IRMA kunnen van verschillende bronnen komen, zoals iDIN en BRP, via de gemeente Nijmegen. Een webwinkel kan zelf kiezen welke bronnen hij vertrouwt. De betrouwbaarheid van de attributen ligt dicht bij de betrouwbaarheid van de bron. Zo is voor het ophalen van de gegevens uit de BRP een inlog met DigiD vereist.

3.5.2 Datakeeper

Datakeeper[47] (voorheen IDA) is een PDM oplossing die ontwikkeld is vanuit de innovatie afdeling van de Rabobank. De Datakeeper app is een wallet die gebruik maakt van blockchain technologie om te verifiëren dat data inderdaad is uitgegeven door de databron. Datakeeper wordt op dit moment ingezet bij test cases rondom auto verhuur en corona back-to-live events. Op dit moment is het mogelijk om gegevens in te laden met behulp van het uitlezen van NFC en Optical Character Recognition (OCR) (zie sectie 3.6). De app is op dit moment gratis voor gebruikers.

3.6 IDENTIFICEREN OP AFSTAND (IOA)

Identificeren op Afstand (IoA) bestaat uit oplossingen die speciaal ontwikkeld zijn om mensen op afstand te identificeren. Dergelijke oplossingen worden onder andere gebruikt bij het aanvragen van een creditcard of het openen van een bankrekening. Zoals de naam doet vermoeden onderscheiden deze oplossingen zich van andere oplossingen omdat er identificatie plaats vindt in plaats van authenticatie[48]. Bij andere categorieën is de identiteit in een eerder stadium al vastgesteld. Bij meerdere oplossingen in de andere categorieën gebeurt deze identificatie met behulp van IoA-oplossingen. Omdat bij IoA de identiteit nog vastgesteld moet worden, kosten deze oplossingen vaak meer tijd voor de gebruiker dan authenticatieoplossingen. Ook zijn ze vaak prijziger in gebruik voor de ondernemer.

Er bestaan verschillende IoA oplossingen, die afhankelijk van de gekozen methode in betrouwbaarheid verschillen. Om een hoger betrouwbaarheidsniveau te realiseren worden dergelijke oplossingen vaak gecombineerd met biometrie. Methodes die voor IoA gebruikt worden zijn onder andere telefonisch, door te video bellen, door een foto te maken van het identiteitsdocument of door het document uit te lezen via NFC. De laatste twee methodes worden vaak uitgebreid met gezichtsherkenning. Zo kan bewezen worden dat je niet alleen het document in bezit hebt, maar dat je ook de eigenaar van het document bent. Dit wordt ook wel holder verification genoemd. Voor alle IoA subcategorieën zijn er verschillende leveranciers. Ze bieden op hoofdlijnen vaak dezelfde functionaliteit, maar verschillen wel in kwaliteit en betrouwbaarheid. Omdat het aanbod groot is, gaan we onderstaand alleen in op de verschillende subcategorieën van IoA.

3.6.1 Biometrie

Biometrische (persoons)gegevens zijn gegevens die iets zeggen over een fysiek of gedragskenmerk van een persoon, denk hierbij aan gezicht, ogen of vingerafdruk maar ook aan handschrift en de manier van spreken. Biometrische identificatie oplossingen worden vaak gebruikt in combinatie met andere oplossingen om iemands identiteit te bepalen. Hierbij wordt een al bekend biometrisch kenmerk (template) vergeleken met hetzelfde kenmerk wat op dat moment waargenomen wordt. Een voorbeeld van zo'n combinatie is een foto van een identiteitsbewijs met het maken van een selfie, om vervolgens te analyseren of het gezicht van de selfie en de foto op het identiteitsbewijs een en dezelfde persoon zijn.
Een andere richting is het gebruiken van biometrische sensors (op basis van vingerafdruk of gezicht) als authenticatiemechanisme om een smartphone of app op de smartphone te ontgrendelen. Het vervangt in dat geval een pincode die de gebruiker moet onthouden en dient dus als authenticatiefactor.

3.6.2 Foto van het identiteitsdocument (OCR)

Deze oplossing staat in de volksmond ook wel bekend als het 'kopietje paspoort'. Waar deze vroeger vaak per mail opgestuurd moest worden, zijn er tegenwoordig ook speciale applicaties voor beschikbaar. De gegevens van het identiteitsdocument worden vaak met behulp van Optical Character Recognition (OCR) van het document gehaald. In sommige gevallen worden de gegevens gecontroleerd of in zijn geheel overgenomen door een medewerker. Afhankelijk van de gekozen oplossing worden de echtheidskenmerken op een identiteitsdocument gecontroleerd. Dit gebeurt al dan niet automatisch. De kwaliteit van de foto's laat regelmatig te wensen over. Hierdoor is het lastig om de gegevens goed over te nemen en goed te controleren

[47] https://datakeeper.nl/
[48] Voor verschil tussen identificatie en authenticatie, zie Bijlage A: Begrippenlijst

op de echtheidskenmerken. Soms moet de klant hierdoor het proces nogmaals doorlopen. Tevens vereist het proces vaak handmatige controle door een medewerker van de leverancier van de oplossing.
Om zeker te zijn dat het identiteitsdocument bij de persoon hoort die het proces doorloopt, wordt er vaak gebruik gemaakt van biometrie. Een selfie van de persoon wordt vergeleken met de pasfoto op het identiteitsdocument.

3.6.3 Uitlezen identiteitsdocument via NFC

Nederlandse en vele internationale identiteitsdocumenten worden tegenwoordig uitgegeven met een chip. Op deze chip staat dezelfde informatie als op het identiteitsdocument. Deze informatie is digitaal ondertekend, waardoor het praktisch onmogelijk is om de informatie op de chip te vervalsen. Door de chip van het identiteitsdocument uit te lezen, wordt de kans op fouten in de uitgelezen gegevens nihil. Er is in dit proces dan ook geen controle door personeel van de leverancier nodig, waardoor de oplossing beter schaalt. Randvoorwaarde is dat de gebruiker over een identiteitsdocument en een NFC-lezer beschikt. Bij de meeste moderne smartphones is dit echter het geval.[49]

Ook deze methode van IoA wordt vaak gecombineerd met biometrie. Een pasfoto in kleur en van hoge kwaliteit staat ook opgeslagen op de chip. Hierdoor is identiteitsverificatie met behulp van een selfie goed te combineren met deze oplossing.

3.6.4 Videobellen

Bij deze oplossing start de klant een videogesprek met de aanbieder van de IoA oplossing. Tijdens een dergelijke sessie moet de gebruiker normaliter zijn identiteitsdocument dicht bij de camera houden, zodat de informatie goed te lezen is en het document op echtheidskenmerken gecontroleerd kan worden. Hierna moet de gebruiker het document naast zijn gezicht houden, zodat gecontroleerd kan worden of hij de rechtmatige eigenaar is van het document. In sommige gevallen moet de gebruiker een video opnemen, die nadien handmatig gecontroleerd wordt. In de meeste gevallen moet hij echter een afspraak maken waarbij live een videosessie wordt gedaan en de controle plaats vindt. De gebruiker moet hier eerst een afspraak voor maken. Hiernaast is de oplossing slecht schaalbaar, omdat er altijd een medewerker handmatig de identiteitscontrole moet doen.

3.7 ANDERE SECTOREN EN INTERNATIONALE INITIATIEVEN

De discussie over leeftijdsverificatie bij diensten op afstand beperkt zich niet tot alcoholverkoop en ook niet tot de Nederlandse grens. Ook bij andere diensten waarbij in fysieke context een leeftijdsverificatie gebruikelijk of wettelijk verplicht is, ontstaat een sterkere roep om leeftijdsverificatie in de online context. Denk hierbij onder andere bij online loterijen en kansspelen, medicijnverkoop, tabaksverkoop, messenverkoop en de verkoop van 18+ content. Op veel plekken waar een leeftijds- of identiteitsverificatie wenselijk is, maar het gebruik van DigiD niet toegestaan is, wordt iDIN gebruikt (o.a. Nederlandse Loterij[50], Marktplaats[51], Bureau Kredietregistratie[52]). Waar (in de online context) een identiteitsverificatie op een hoger betrouwbaarheidsniveau nodig is, wordt gebruik gemaakt van identificatie op afstand technologie. Denk hierbij aan het openen van een bankaccount. Naast de ontwikkelingen in Nederland ontstaan ook in het buitenland initiatieven voor online leeftijdsverificatie. Onderstaand worden de meest relevante Nederlandse en internationale initiatieven benoemt.

3.7.1 Kansspelen en loterijen

Per 1 april 2021 is de wet Kansspelen op Afstand (KoA) in werking getreden. Deze wet reguleert het aanbod van online kansspelen op de Nederlandse markt en maakt het mogelijk om deze legaal aan te bieden op de Nederlandse markt. De kansspelen die onder deze wet vallen zijn casinospellen, weddenschappen op sportwedstrijden en weddenschappen op paardenrennen[53]. Partijen die dergelijke spellen aan willen bieden moeten een vergunning aanvragen bij de Kansspelautoriteit (KSA). De eisen voor de identiteitsverificatie onder de wet KoA gaan verder dan alleen een leeftijdsverificatie, maar zijn slechts minimaal uitgewerkt. Dit omdat

[49] *InnoValor Advies is een zelfstandig onderdeel van InnoValor. InnoValor heeft een technologie genaamd ReadID dat NFC-gebaseerde mobile identiteitsdocument verificatie implementeert en levert aan onder andere banken en wallets.*
[50] https://www.nederlandseloterij.nl/speel-bewust
[51] https://help.marktplaats.nl/s/article/aanmelden-voor-betaalverzoeken-met-ideal-via-marktplaats
[52] https://www.bkr.nl/veelgestelde-vragen/inloggen-mijn-bkr/wat-is-idin/
[53] https://kansspelautoriteit.nl/wet-koa/voorbereiden/

partijen die een vergunning krijgen voor KoA ook moeten voldoen aan de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). In deze wet worden strenge eisen gesteld aan de identiteitsverificatie. Deze worden uitgewerkt in de leidraad Wwft van de KSA[54]. Volgens de eisen die uit de Wwft volgen moeten niet alleen naam en geboortedatum, maar ook aard, nummer, datum en plaats van uitgifte van een geldig identiteitsdocument worden vastgelegd. Dit betekent dat veel consumentenoplossingen zoals iDIN niet voldoende zijn. In plaats hiervan zal er een kopie van een WID geüpload moeten worden of van andere IoA (zie sectie 3.6) oplossingen gebruik gemaakt moeten worden.
Om te controleren of de gegevens die door de gebruiker opgegeven worden kloppen, moet de kansspelaanbieder een aantal identiteitsgegevens inclusief BSN van de gebruiker opsturen naar de KSA. De KSA controleert aan de hand van het BSN in het BRP of de opgegeven gegevens kloppen. Dit koppelt de KSA terug aan de kansspelaanbieder, waarna de KSA de identiteitsgegevens weer verwijderd.

Een aantal partijen, waaronder grote spelers zoals Unibet[55], die op dit moment nog geen vergunning heeft om in Nederland KoA aan te bieden, maakt momenteel gebruik van iDIN om de leeftijd en andere identiteitsgegevens te verifiëren. Ook de Nederlandse Loterij maakt voor de online verkoop van loten voor verschillende loterijen gebruik van iDIN om de leeftijd van de consument te verifiëren. De Nederlandse Loterij valt niet onder de strengere eisen van de Wwft, waardoor een iDIN verificatie hier voldoende is.

3.7.2 Tabaksverkoop

Ook in de tabaks- en rookwarenwet worden eisen gesteld aan de leeftijdsverificatie[56]. De eisen die in de tabakswet worden gesteld lijken zeer op de eisen die in de Alcoholwet gesteld worden. Het is verplicht om bij aflevering of uitgifte de leeftijd te controleren. Ook kunnen er bij algemene maatregelen van bestuur eisen gesteld worden aan de leeftijdsverificatie op moment van aankoop. Momenteel is de eis hier een zelfverklaarde leeftijdsvraag.

3.7.3 Messenverkoop

Recentelijk is er een nieuwe discussie ontstaan over de verkoop aan en het bezit onder jongeren van messen. Dit naar aanleiding van een toenemend aantal steekpartijen waar jongeren bij betrokken zijn. Het kabinet is voornemens om strengere eisen te stellen aan het bezit van messen onder jongeren en de verkoop van (legale) messen aan jongeren onder de 18 jaar zelfs helemaal te verbieden[57]. Het kabinet is voornemens om ook de online verkoop van messen aan minderjarigen tegen te gaan. Dit zal betekenen dat ook hier met een leeftijdsverificatiesysteem gewerkt zal moeten worden. In het actieplan Wapens en Jongeren[58] wordt hierover het volgende geschreven: *"In de verkenning van de mogelijkheden om online verkoop van wapens aan minderjarigen tegen te gaan, zal het invoeren van de voorwaarde om bij de bestelling van een mes een kopie van het ID-bewijs via KopieID te sturen betrokken worden."* Er zijn hier dus nog geen definitieve eisen voor de leeftijdsverificatie. Maar naar aanleiding van het actieplan lijkt ook hier een kopie van een WID of andere vorm van identificatie op afstand voor de hand te liggen.

3.7.4 Age Check Certification Scheme UK

In het Verenigd Koninkrijk bestaat het Age Check Certification Scheme[59] als onafhankelijke certificering voor leeftijdsverificatiediensten, zowel in de fysieke als in de digitale context. Voor online diensten worden zogenaamde Age Check providers gecertificeerd[60]. Dit gebeurt op basis van het door de British Standards Institute (BSI) opgestelde raamwerk PAS 1296:2018 ('*Online age checking. Provision and use of online age check services. Code of Practice*'). Momenteel wordt op basis van dit raamwerk ook gewerkt aan een ISO standaard, waarvan eind 2021 de eerste conceptversie verwacht wordt[61]. Oplossingen onder de Age Check Certification Scheme gebruiken bijvoorbeeld identificatie op afstand of bieden een smartphone app aan waarmee de leeftijd bewezen kan worden.

[54] Beschikbaar via https://kansspelautoriteit.nl/wet-koa/regels-leidraden/leidraad-wwft/
[55] https://www.unibet.eu/registration
[56] Zie artikel 9 van de Tabaks- en rookwarenwet, https://wetten.overheid.nl/BWBR0004302/2021-07-01
[57] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5196290/verbod-op-messen-jongeren-de-maak-en-strengre
[58] https://www.rijksoverheid.nl/documenten/rapporten/2020/11/11/tk-bijlage-actieplan-wapens-en-jongeren
[59] https://www.accscheme.com/about
[60] https://www.accscheme.com/services/age-assurance/age-verification/age-determination
[61] https://avpassociation.com/standards-for-age-verification/

3.7.5 Systembolaget - BankID

In een aantal Scandinavische landen wordt alcohol alleen via staatswinkels verkocht, ook online. In Zweden is het mogelijk om alcohol online te bestellen via de webshop van de staatswinkel Systembolaget. Hierbij moet de klant een account aanmaken. Zonder account is het niet mogelijk om alcohol te bestellen. Daarnaast moet er bij elke aankoop betaald worden met BankID[62], een Scandinavisch betaal- en identificatiemiddel. Gelijktijdig met de betaling kan ook de leeftijdsverificatie uitgevoerd worden.

[62] https://www.bankid.com/en

4 Toetsing van categorieën

Dit hoofdstuk beantwoordt het tweede deel van de eerste onderzoeksvraag: "*... en wat is er bekend over hun (leeftijdsverificatiesystemen) effectiviteit in termen van naleving en hun doelmatigheid (voorkomen dat jongeren alcohol of andere leeftijdsgebonden producten en diensten kunnen bestellen en verkrijgen via verkoop op afstand)?*" De oplossingen zoals omschreven in hoofdstuk 3 worden per categorie geanalyseerd, waarbij enkele systemen per categorie onder de loop worden genomen als illustratie.

4.1 ZELF TOEGEZEGD

Bij zelf toegezegd geeft de gebruiker zelf aan 18+ te zijn of niet. Dit is direct de grootste negatieve factor voor zelf toegezegde oplossingen. De betrouwbaarheid is zeer laag en het is makkelijk om te frauderen. De gebruiker hoeft immers alleen te liegen over zijn leeftijd. Daarentegen is het gebruiksgemak en begrijpbaarheid erg hoog, omdat het voor mensen erg makkelijk te gebruiken is. Er is geen technische kennis nodig en het kost weinig tijd. Er hoeft bijvoorbeeld niet nog een keer extra ingelogd te worden of via een app een authenticatie gestart te worden. In Tabel 2 wordt een overzicht gegeven van hoe deze categorie scoort op de succesfactoren zoals beschreven in hoofdstuk 2. De tabellen zijn indicatief en de score moet geïnterpreteerd worden als relatief ten opzichte van de andere oplossingen en categorieën. Onderstaand wordt een uitgebreidere toelichting van de score gegeven. Voor een overzicht van alle tabellen tezamen, Zie Bijlage D: Analysetabellen.

Tabel 2 Indicatie van score op succesfactoren voor zelf toegezegd

Criteria	Zelf toegezegd	Vinkje	Telefonisch
Fraudebestendigheid en betrouwbaarheid	--	--	--
Beschikbaarheid en dekkingsgraad	++	++	++
Gebruiksgemak en begrijpbaarheid	++	++	++
Schaalbaarheid en flexibiliteit	++	++	--
Kosten	++	++	--
Realisatietermijn	++	++	++
Toekomtbestendigheid	--	--	--
Privacy en vertrouwen	++	++	++

Oplossingen waarbij de gebruiker zijn leeftijd zelf toezegt zijn relatief goedkoop. Er zijn voornamelijk implementatiekosten, maar de kosten per verificatie zijn daarna nihil.

De privacy hangt af van de gekozen oplossing. Sommige partijen vragen om de geboortedatum in plaats van een statement of iemand ouder dan 18 is. Dit biedt niet meer betrouwbaarheid, het is immers net zo makkelijk om over te liegen. Het is daarnaast onnodig onvriendelijk vanuit privacy perspectief.

Door de lage betrouwbaarheid zijn oplossingen waarbij de gebruiker zelf een toezegging doet niet toekomstbestendig. Dit is ook waarom VWS alternatieven onderzoekt.

4.1.1 Vinkje

Zoals alle oplossingen in deze categorie is het 18+-vinkje niet betrouwbaar. Gebruikers kunnen hier makkelijk over liegen, maar kunnen ook makkelijk op ja klikken zonder te lezen. Zo blijkt uit onderzoek dat mensen de "privacy statement van websites" gewoon accepteren zonder te lezen[63]. Daar tegenover staat dat deze oplossing misschien wel de makkelijkste en snelste oplossing is om te implementeren. Ook zijn de kosten per transactie verwaarloosbaar.

4.1.2 Bellen

Bij bellen zegt de klant zijn leeftijd telefonisch toe. Hierdoor zijn de kosten hoger en de schaalbaarheid slecht. De betrouwbaarheid wordt er nauwelijks hoger van, omdat aan de telefoon (zonder controlevragen) de leeftijd slecht geverifieerd kan worden. Als er gebruik gemaakt wordt van diepgaandere controlevragen (zoals de meisjesnaam van je moeder), wordt de betrouwbaarheid wel hoger. Deze oplossing kan gezien worden als

[63] https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2465&context=law_and_economics

authenticatie op afstand, omdat de identiteit en de te vragen gegevens al eerder vastgesteld moeten zijn. De betrouwbaarheid hangt af van hoe ingewikkeld het is om de antwoorden te achterhalen. Voor een familielid zal dit relatief makkelijk zijn.

Ook bellen is dus ongeschikt en het biedt nauwelijks tot geen meerwaarde ten opzichte van een andere vorm van een leeftijdsvraag.

4.2 CONSUMENTENOPLOSSINGEN

Consumentenoplossingen worden op dit moment gebruikt om consumenten te authentiseren binnen het consumenten domein. Van oorsprong gebruiken deze oplossingen een combinatie van gebruikersnaam en wachtwoord, aangevuld met een tweede factor (denk aan een code via een SMS of app). Tegenwoordig zien we ook steeds meer oplossingen die gebruik maken van een app of hardware-token die beveiligd is met een pincode. Maar er bestaan ook andere vormen zoals het gebruik van een online certificaat, welke een online website of systeem herkent en aan de hand daarvan de consument kan herkennen. In Tabel 3 wordt een indicatie gegeven van hoe deze categorie scoort op de succesfactoren. De score moet geïnterpreteerd worden als relatief ten opzichte van de andere oplossingen en categorieën.

De fraudebestendigheid en betrouwbaarheid zijn over het algemeen hoog, zoals bij iDIN waarbij de koppeling is gemaakt met de bank accounts, welke goed beveiligd zijn. Hierbij helpen ook de strenge KYC (Know Your Customer) eisen die aan banken gesteld worden. Tevens wordt er vaak een duidelijke indicatie gegeven van het betrouwbaarheidsniveau van de oplossing volgens de eIDAS-richtlijnen.

De consumentenoplossingen zijn gemaakt voor consumenten en zijn daardoor beschikbaar voor een significant deel van Nederland (en soms ook daarbuiten). De kosten van consumentenoplossingen variëren per oplossing. Interessant is dat we hier niet alleen pay-per-use, maar ook pay-per-user oplossingen zien.

Een uitdaging van consumentenoplossingen is dat de gebruikers verspreid zijn over verschillende platformen. Het risico is dat er verstrooiing plaats kan vinden doordat elke website een andere oplossing gebruikt, waardoor de gebruiker een groot aantal verschillende apps of accounts moet installeren, instellen en gebruiken. Dit komt de dekkingsgraad niet ten goede. Aan de ander kant is te verwachten dat veel webwinkels een oplossing zullen kiezen met een hoge dekkingsgraad. De kans is anders groot dat de klant anders naar een andere winkel gaat.

Als consumentenoplossingen als categorie volwassener worden, ontstaan er mogelijk service providers die verschillende (consumenten)oplossingen naast elkaar gaan aanbieden. Vergelijkbaar met betaalproviders die verschillende betaaloplossingen aanbieden.

Consumentenoplossingen komen niet bij iedere eis op de eerste plaats, maar scoren over de breedte zeer goed. De categorie gaat ook op geen van de gestelde eisen onderuit.

Tabel 3 Indicatie van score op succesfactoren voor consumentenoplossingen.

Criteria	Consumenten	Itsme	iDIN
Fraudebestendigheid en betrouwbaarheid	++	++	++
Beschikbaarheid en dekkingsgraad	+	-	++
Gebruiksgemak en begrijpbaarheid	+	+	+
Schaalbaarheid en flexibiliteit	++	++	++
Kosten	++	+	+
Realisatietermijn	++	+	++
Toekomtbestendigheid	++	+/-	++
Privacy en vertrouwen	+	+/-	++

4.2.1 iDIN

De fraudebestendigheid van iDIN is hoog, omdat deze gekoppeld is aan persoonlijke bank accounts, welke mensen niet zomaar eenmalig of structureel zullen uitlenen of delen met derden. De dekkingsgraad van iDIN is

zeer hoog. Er kunnen zo'n 13 miljoen Nederlanders gebruik van maken[64]. iDIN is niet bij alle banken beschikbaar, maar wel bij de grote 4: ABN AMRO, ING, Rabobank en Volksbank (met merken zoals ASN Bank, RegioBank en SNS). Ook mensen met een rekening bij bunq kunnen iDIN gebruiken. Hiermee is de dekkingsgraad lager dan voor iDEAL, maar bijzonder hoog voor een consumentenoplossing. iDIN is sterk gelieerd aan iDEAL en wordt al op meerdere plekken in de praktijk ingezet. Onder andere voor leeftijdsverificatie voor kansspelen bij de Nederlandse Loterij[65] en Runnerz[66] (paardenraces), maar ook bij identiteitsverificatie door onder andere Marktplaats[67]. In 2020 werd iDIN 7,5 miljoen keer gebruikt voor online identificatie, inloggen of leeftijdsverificatie.

Eén van de voordelen is dat iDIN de mogelijkheid biedt om alleen een 18+-attribuut uit te wisselen. Tijdens één van de interviews werd als nadeel genoemd dat de mogelijkheden om iDIN direct te integreren via platformen als Shopify en Magento momenteel nog beperkt zijn. Aan de andere kant is er door online slijters al getest met de inzet van iDIN voor online leeftijdsverificatie[68] en lijken de eerste resultaten daar positief.

4.2.2 itsme

itsme is één van de Belgische nationale eID oplossingen. Het is eIDAS genotificeerd op betrouwbaarheidsniveau hoog. Sinds kort is itsme ook beschikbaar voor Nederlanders. Het aantal plekken waar itsme in Nederland ingezet kan worden is nog beperkt. Het aantal Nederlandse gebruikers zal zodoende ook laag zijn. Wel staat er een pilot met een aantal Nederlandse gemeentes op de planning. Bijzonder is dat itsme een pay-per-user model kent (vanaf €0,61 per gebruiker per jaar[69]). Deze methode kan goedkoper uitpakken dan iDIN als klanten regelmatig terugkeren bij de webwinkel.

4.3 OVERHEIDSOPLOSSINGEN

Overheidsoplossingen zijn (digitale) middelen die uitgegeven worden door de overheid. Bestaande middelen kunnen alleen gebruikt worden binnen het overheidsdomein en bij organisaties met een publieke taak. Bestaande middelen zijn DigiD en Europese middelen die toegelaten zijn binnen het eIDAS stelsel. Hiernaast doet BZK momenteel onderzoek naar een nog te ontwikkelen Digitale Bronidentiteit. Hierbij moet het ook mogelijk worden om het middel in het private domein te gebruiken.

Omdat deze categorie uit een volwassen oplossing en nog te ontwikkelen concepten bestaat, worden deze apart van elkaar uitgebreid uitgelicht. In Tabel 4 wordt een indicatie gegeven van hoe deze categorie scoort op de succesfactoren. De score moet geïnterpreteerd worden als relatief ten opzichte van de andere oplossingen en categorieën.

Tabel 4 Indicatie van score op succesfactoren voor overheidsoplossingen

Criteria	Overheid	DigiD
Fraudebestendigheid en betrouwbaarheid	++	++
Beschikbaarheid en dekkingsgraad	++	++
Gebruiksgemak en begrijpbaarheid	+	++
Schaalbaarheid en flexibiliteit	++	++
Kosten	++	++
Realisatietermijn	--	--
Toekomtbestendigheid	++	++
Privacy en vertrouwen	+/-	+/-

[64] Zie jaarverslag Currence (merkeigenaar van o.a. iDIN en iDEAL) over 2020: https://www.currence.nl/wp-uploads/2021/05/Currence-Jaarverslag-2020.pdf
[65] zie https://www.nederlandseloterij.nl/speel-bewust
[66] https://runnerz.nl/watisidin
[67] Zie https://help.marktplaats.nl/s/article/aanmelden-voor-betaalverzoeken-met-ideal-via-marktplaats
[68] Zie https://www.idin.nl/actueel/drankdozijn-blij-met-idin-leeftijdsverificatie/
[69] Zie https://business.itsme.be/nl

4.3.1 DigiD

DigiD is het authenticatiemiddel om als burger bij de overheid in te loggen. DigiD is op verschillende betruwbaarheidsniveaus beschikbaar. Er kan gekozen worden alleen middelen toe te staan die op een hoog genoeg betrouwbaarheidsniveau zitten.

DigiD is in principe voor alle inwoners van Nederland beschikbaar. Met 18,3 miljoen actieve accounts is de dekkingsgraad zeer hoog. Nederlanders zijn gewend om DigiD te gebruiken om bij de overheid in te loggen. Het gebruik van DigiD wekt vertrouwen, omdat mensen het associëren met veilig zaken doen met de overheid. Dit vertrouwen reflecteert ook in het draagvlak onder ondernemers. Ondernemers zien graag een overheidsmiddel voor online leeftijdsverificatie. Meerdere geïnterviewden redeneren dat omdat de overheid verantwoordelijk is voor identiteitsdocumenten in het fysieke domein, zij dit ook zou moeten zijn in online context.

Het is echter zeer de vraag of DigiD hiervoor het geschikte middel is. Allereerst is het gebruik van DigiD momenteel alleen toegestaan voor overheidsorganisaties en organisaties met een publieke taak. Dit is zo vastgelegd in de wet ABB[70]. Het ligt niet in de lijn der verwachting dat dit op korte termijn aangepast zal worden. En zelfs al mocht het nieuwe kabinet dit besluiten, zal dit niet op zeer korte termijn gerealiseerd kunnen worden. Daarnaast zal de wetgeving aangepast moeten worden, maar er kan ook gerekend worden op bezwaar vanuit commerciële identiteitsproviders. Dit omdat het gebruik van DigiD in het private domein een marktverstorende werking kan hebben. Een ander probleem is dat DigiD na inloggen het BSN terugkoppelt. Dit betekent dat andere identiteitsgegevens dus eerst nog apart opgehaald moeten worden, bijvoorbeeld uit de Basisregistratie Personen (BRP). Om leeftijdsgegevens terug te geven zal DigiD hiervoor aanzienlijk aangepast moeten worden. Tevens kent DigiD een strikt audit regiem: aangesloten partijen dienen jaarlijks een beveiligingsaudit uit te laten voeren door een externe auditor en deze te delen met Logius[71]. Veel kleine webwinkeliers zullen hier waarschijnlijk niet aan kunnen voldoen.

Daarnaast heeft de overheid zich in het verleden niet altijd als een betrouwbare partner getoond op het gebied van digitale identiteiten. De pilot rondom inloggen met Idensys en iDIN bij de overheid werd eind 2018 beëindigd. Dit ter voorbereiding van de aanbesteding voor private diensten onder de wet Digitale Overheid[72]. De wet Digitale Overheid heeft als doel dat burgers en bedrijven veilig en betrouwbaar bij de overheid kunnen inloggen. Het biedt ook de ruimte om private inlogmiddelen toe te laten, zodat burgers hiermee bij de overheid kunnen inloggen. Ruim drie jaar na de eerste indiening van de wet Digitale Overheid in de Tweede Kamer is deze wet echter nog niet aangenomen en is het dus tot op heden nog niet mogelijk om met consumentenoplossingen bij de overheid in te loggen.

Tot slot zou het gebruik van DigiD betekenen dat de overheid (specifiek Logius) ziet wie waar, wanneer en hoe vaak online alcohol koopt. Iets wat in een aantal Scandinavische landen als normaal ervaren wordt, maar vanuit Nederlands standpunt vanuit privacy als onwenselijk wordt gezien. Een vergelijkbare methode wordt wel toegepast bij kansspelen. Hierbij dient de kansspelaanbieder de identiteitsgegevens ter verificatie aan te bieden aan de kansspelautoriteit (zie hoofdstuk 3.7.1). Deze kansspelen vallen echter onder de Wwft, waardoor aanzienlijk strengere eisen aan de identiteitscontrole worden gesteld. Het gaat hiernaast om een eenmalige verificatie in plaats van een leeftijdsverificatie bij iedere aankoop.

Met bovenstaande praktische bezwaren in het achterhoofd, lijkt het niet realistisch dat DigiD op korte termijn geschikt gemaakt kan worden voor online leeftijdsverificatie.

4.3.2 Digitale Bronidentiteit

Begin 2021 werd het concept van de Digitale Bronidentiteit (DBI) gepresenteerd in de kamerbrief ‘visiebrief digitale identiteit’[73]. De DBI zal in tegenstelling tot DigiD geen authenticatiemiddel worden, maar zal de mogelijkheid bieden om een set geverifieerde identiteitsgegevens bij de overheid op te halen. Het is nog erg onduidelijk hoe de DBI er precies uit gaat zien. Het ligt niet in de lijn der verwachting dat webwinkels direct

[70] Wet algemene bepalingen Burgerservicenummer, zie https://wetten.overheid.nl/BWBR0022428/2018-07-28

[71] Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Logius biedt voorzieningen en standaarden die alle overheidsorganisaties gebruiken in hun digitale dienstverlening, zoals bijvoorbeeld DigiD, MijnOverheid en Digipoort.

[72] Meer informatie over de wet Digitale Overheid, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/wet-digitale-overheid-in-het-kort/

[73] Zie https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/11/kamerbrief-over-visie-digitale-identiteit

kunnen aansluiten op de DBI. Hiermee is de DBI zelf direct ongeschikt voor online leeftijdsverificatie. Het kan wel de basis bieden voor online leeftijdsverificatie. Waarschijnlijk zullen PDM-oplossingen of consumentenoplossingen de gegevens uit de DBI kunnen gebruiken als betrouwbare identiteitsgegevens.

Naar verwachting zullen in 2022 de eerste pilots gedraaid worden met de DBI. Hoe snel de ontwikkelingen zullen gaan rondom de DBI zal onder meer afhangen van de politieke urgentie die de DBI krijgt van het nieuwe kabinet. Er mag echter vanuit gegaan worden dat het na de eerste pilots nog enkele jaren zal duren voordat een DBI breed beschikbaar komt.

4.3.3 vID

In Nederland werkt de RvIG (Rijksdienst voor Identiteitsgegevens) aan de ontwikkeling van een vID, een digitale versie van een identiteitsbewijs, die zowel in fysieke als online context te gebruiken is[74]. In 2019 en 2020 zijn verschillende gebruikersonderzoeken en pilots gedaan. Momenteel wordt gewerkt aan het programma van eisen voor een Nederlandse vID. Hoe een toekomstig vID er dus daadwerkelijk uit zou zien is nog onduidelijk. In potentie zou een vID goed geschikt zijn voor online leeftijdsverificatie. Het wordt door RvIG als één van de potentiële use-cases benoemd. Naast dat de exacte invulling onduidelijk is, is het überhaupt onduidelijk of er daadwerkelijk een Nederlandse vID komt en zo ja op welke termijn deze er moet zijn. Omdat de vID nog niet bestaat is een uitgebreide toets aan de criteria niet mogelijk.

4.4 BETAALOPLOSSINGEN

Betaaloplossingen bestaan in veel verschillende vormen. Denk aan iDEAL vanuit de banken, PayPal, Apple Pay en creditcards. Deze oplossingen verschillen sterk van elkaar en daarmee is er ook een sterk verschil in hoeverre ze aan de gestelde eisen voldoen. Waarin deze oplossingen wel overeenkomen is dat ze allen een erg groot gebruikersgemak hebben. Echter zijn ze niet ontworpen als middel voor identificatie of authenticatie. Bij iDEAL is het op dit moment onmogelijk om de leeftijd te verifiëren. Bij oplossingen als creditcards kan dit alleen indirect. Creditcards zijn namelijk alleen aan te vragen door volwassenen van 18 jaar en ouder. In Tabel 5 wordt een indicatie gegeven van hoe deze categorie scoort op de succesfactoren. De score moet geïnterpreteerd worden als relatief ten opzichte van de andere oplossingen en categorieën.

Tabel 5 Indicatie van score op succesfactoren voor betaaloplossingen.

Criteria	Betalen	iDeal	Creditcard	Paypal
Fraudebestendigheid en betrouwbaarheid	++	++	--	--
Beschikbaarheid en dekkingsgraad	++	++	+/-	+
Gebruiksgemak en begrijpbaarheid	++	++	+	++
Schaalbaarheid en flexibiliteit	++	+	+	+
Kosten	++	++	++	+
Realisatietermijn	--	--	+	-
Toekomtbestendigheid	++	++	+	++
Privacy en vertrouwen	+/-	++	+	++

Kijkend naar betrouwbaarheid en fraudebestendigheid zien we direct grote verschillen. Bij de meeste betaaloplossingen is de identiteit van de gebruiker op een hoog betrouwbaarheidsniveau vastgesteld. De fraudebestendigheid wisselt echter. Bij iDEAL moet je toegang hebben tot iemands online bankierenomgeving. Bij een creditcard staat alle informatie al op de kaart zelf en is het in handen krijgen van de creditcard voldoende om er mee te betalen. Door de introductie van 3D Secure[75], een extra authenticatiefactor, wordt dit risico wel beperkt.

Positief is dat de beschikbaarheid en dekkingsgraad van de betaaloplossingen bij elkaar hoog zijn. Bijkomend voordeel is dat verschillende betaaloplossingen door solution providers op één platform naast elkaar aangeboden worden. Hierdoor kan de klant zelf het middel van zijn voorkeur kiezen. Dit komt tevens het

[74] https://www.rvig.nl/digitale-identiteit/digitaal-identiteitsbewijs
[75] https://www.internetkassa.nu/3d-secure/

gebruikersgemak en het vertrouwen ten goede. Het gebruikersgemak en begrijpbaarheid zijn ook hoog, omdat personen er al gebruik van maken.

De kosten voor een betaling zijn relatief laag ten opzichte van een leeftijdsverificatie. Daarnaast is de sector volwassen, goed gereguleerd en toekomstbestendig. Betalen zullen we immers altijd blijven doen. Ook bieden betaaloplossingen een mooie manier van dataminimalisatie. Doordat de leeftijd, bijvoorbeeld bij een creditcard, afgeleid wordt uit het bezit van de oplossing, wordt er niet onnodig extra informatie uitgewisseld.

Het grootste pijnpunt voor deze categorie blijft dat één van de meest gebruikte oplossingen, iDEAL, geen leeftijdsattribuut levert of anderszins een mogelijkheid biedt om de leeftijd te verifiëren. Ook is het de vraag of de afgeleide leeftijdsverificatie voor andere oplossingen als betrouwbaar genoeg beschouwd kan worden.

4.4.1 iDEAL

iDEAL is een betaaloplossing van de Nederlandse banken. Veel Nederlanders beschikken al over de mogelijkheid om iDEAL te gebruiken, omdat het een middel is om bij de eigen bank online te kunnen bankieren. iDEAL scoort op bijna alle punten erg goed. Het enige pijnpunt is dat iDEAL niet ontworpen is om identiteitsgegevens uit te wisselen. Het broertje iDIN (zie 4.2.1) is hier wel voor geschikt. Momenteel wordt gewerkt aan iDEAL 2.0. Hierbij wordt iDEAL Snel bestellen geïmplementeerd. Bij easy check-out deelt de bank direct het verzendadres met de webwinkel, waardoor het check-out en betaalproces soepeler wordt. Hiermee wordt ook de basis gelegd om een betaling met leeftijdsverificatie mogelijk te maken. iDEAL 2.0 wordt naar verwachting begin 2022 gelanceerd en zal dan aan het einde van 2022 door alle betrokken partijen geïmplementeerd zijn. Hiermee staat de deur op een kier om iDEAL te gebruiken voor online leeftijdsverificatie. iDEAL met leeftijdsverificatie staat echter nog niet concreet op de roadmap en zal dus ook niet voor begin 2023 gelanceerd worden.

4.4.2 Creditcard

Net zoals een bank wordt aan een creditcardmaatschappij hoge eisen gesteld op het gebied van KYC (Know Your Customer). Bij uitgifte is de identiteit van de klant dus op een hoog betrouwbaarheidsniveau vastgesteld. Aan de andere kant is het relatief makkelijk om met een creditcard fraude te plegen. Meestal zijn de gegevens die op de creditcard staan genoeg om een online betaling te doen. Hiermee is het voor een jongere die een creditcard in handen krijgt relatief makkelijk om een online bestelling te doen. Dit hoeft tevens niet direct opgemerkt te worden, omdat bestellingen via creditcards niet direct afbetaald hoeven te worden. Deze vorm van fraude kan eenvoudig worden voorkomen door bij een creditcard betaling ook het gebruik van 3D Secure af te dwingen. Hierbij moet de klant nog een extra authenticatiestap uitvoeren, bijvoorbeeld het invoeren van een wachtwoord of door de betaling goed te keuren in de bankieren-app. Dit verlaagt voor de ondernemer tevens het risico op chargebacks, het terug moeten betalen van een eerder ontvangen betaling.

Lang niet iedereen in Nederland beschikt over een creditcard. Het is zodoende onwenselijk om een creditcard als enige optie in te zetten. In combinatie met andere leeftijdsverificatie- of betaaloplossingen waarbij de klant zelf kan kiezen, zoals dit bij betalingen nu ook al vaak gebeurt, is dit geen probleem.

Een mogelijk bezwaar is dat er met betaling met een creditcard geen directe leeftijdsverificatie gedaan kan worden. De leeftijd wordt indirect afgeleid, omdat een creditcard alleen aan te vragen is door meerderjarigen. Los van dit mogelijke bezwaar lijkt een betaling met creditcard en 3D secure wel een hoog genoeg betrouwbaarheidsniveau te bieden voor online leeftijdsverificatie.

4.4.3 PayPal

PayPal is een betaalmiddel waarbij de gebruiker een account aanmaakt waarmee betaald kan worden. Aan dit account kan vervolgens een creditcard of bankrekening gekoppeld worden. Ook kan er saldo op het account gezet worden met een iDEAL-betaling of een overschrijving.

Officieel moet je meerderjarig zijn voor het aanmaken van een PayPal-account[76]. Er wordt echter niet altijd een identiteitscontrole gedaan bij het aanmaken van een account. Vaak gebeurt dit pas als er grotere bedragen worden betaald of ontvangen met het account. Dit maakt de leeftijdsclaim net zo betrouwbaar als een

[76] Zie gebruikersvoorwaarden, https://www.paypal.com/nl/webapps/mpp/ua/useragreement-full

zelfverklaarde leeftijdsclaim. Dit in combinatie met dat hier net zoals bij een creditcard alleen een afgeleide leeftijdsverificatie gedaan kan worden, maakt het in dit geval ongeschikt voor online leeftijdsverificatie.

4.5 PERSONAL DATA WALLETS

Privacy en regie op eigen gegevens zijn belangrijke drijfveren van het personal data wallets. De gebruiker heeft controle over wat er gedeeld wordt en houdt regie over zijn data. Ook dataminimalisatie krijgt hierbij veel aandacht. Het is vaak mogelijk om enkel het “ik ben ouder dan 18” attribuut te delen of bijvoorbeeld enkel de woonplaats, waardoor niet meer data dan nodig gedeeld wordt. De wallets verschillen in de technische details, maar werken via dezelfde rolverdeling: de gebruiker staat centraal en kan zijn data ophalen bij de data bron, om deze vervolgens onder consent te delen met de data afnemer. In Tabel 6 wordt een indicatie gegeven van hoe deze categorie scoort op de succesfactoren. De score moet geïnterpreteerd worden als relatief ten opzichte van de andere oplossingen en categorieën.

Tabel 6 Indicatie van score op succesfactoren voor Personal Data Wallets

Criteria	Wallets	IRMA	IDA
Fraudebestendigheid en betrouwbaarheid	+/-	+/-	+/-
Beschikbaarheid en dekkingsgraad	--	-	-
Gebruiksgemak en begrijpbaarheid	+	+	+
Schaalbaarheid en flexibiliteit	++	++	++
Kosten	+	+	+
Realisatietermijn	-	+/-	+/-
Toekomtbestendigheid	+	+	+
Privacy en vertrouwen	+/-	+/-	+/-

Attributen worden in wallets ingeladen door deze bij andere partijen op te halen (bijvoorbeeld via iDIN of uit de BRP). De betrouwbaarheid van deze attributen hangt daardoor sterk af van het authenticatiemechanisme dat gebruikt is om de attributen uit de bron op te halen. Er bestaat nog onduidelijkheid over de betrouwbaarheidsniveaus die aan de wallets gehangen kunnen worden. Het kan zo zijn dat het betrouwbaarheidsniveau van de wallet zelf lager is als de betrouwbaarheid van het attribuut bij inladen. Bij ontsluiten van het attribuut zal de betrouwbaarheid dan niet hoger zijn dan het betrouwbaarheidsniveau van de wallet.

Daarbij is het mogelijk om attributen van iemand anders eenmalig in te laden in een PDM-oplossing (zie sectie 5.7). Deze kunnen vervolgens op meerdere plekken en voor een langere tijd hergebruikt worden. De drempel om dit te doen is laag, omdat het veld onvolwassen is. Het aantal plekken waar PDM-oplossingen gebruikt kunnen worden is nog beperkt. De drempel voor het uitlenen van attributen is laag, omdat het attribuut (op dit moment) in weinig andere processen gebruikt kan worden, hiermee is er minder risico op verder misbruik door de minderjarige. Veel oplossingen binden dergelijke data niet hard aan één persoon. Bij sommige oplossingen kan een persoon zelfs data van verschillende personen bezitten. Zie de uitgebreide analyse van de fraudemogelijkheden in hoofdstuk 5.

De bekendheid en dekkingsgraad van wallets zijn nog beperkt. Een aantal apps is momenteel alleen inzetbaar in processen op uitnodiging van de data-afnemer. Voorbeelden hiervan zijn de apps Schluss en Ockto. Een aantal use-cases met personal data wallets hebben hun meerwaarde al wel bewezen (waaronder voor hypotheken en financiële dienstverlening). Waar een aantal wallets op specifieke sectoren of use-cases focust, zijn er ook generieke PDM-oplossingen, zoals IRMA en IDA. Dergelijke wallets zijn ook inzetbaar in een andere context. De wallets zijn nog relatief onbekend. Onbekend maakt onbemind, waardoor het vertrouwen van consumenten in wallets nog relatief laag is.

Een van de principes van PDM is dat de gebruiker zelf kan kiezen voor een wallet. Idealiter zou een webwinkel dus meerdere oplossingen naast elkaar aanbieden. Zolang wallets nog niet interoperabel of gestandaardiseerd zijn, zal iedere wallet apart aangesloten moeten worden door de webwinkel. Dit zal extra kosten met zich meebrengen. Andersom bestaat het risico op versnippering als iedere webwinkel met een aparte wallet samenwerkt, waardoor de gebruiker meerdere wallets moet installeren.

Technisch zijn de oplossingen goed schaalbaar, flexibel en is er geen handmatige handeling nodig vanuit de oplossing bij identiteitsverificatie. Sommige oplossingen zijn open source en andere oplossingen gebruiken open standaarden. Daarbij bieden enkele oplossingen de mogelijkheid tot technische ondersteuning bij implementatie en problemen.

Deze categorie aan oplossingen is nog niet volwassen genoeg om op korte termijn ingezet te kunnen worden voor leeftijdsverificatie bij alcoholverkoop. Ontwikkelingen zoals de Digitale Bron Identiteit (zie 3.2.2) en de EU digital wallet[77] zouden wel een stimulans kunnen geven aan deze categorie. Het is dus nog afwachten hoe de categorie zich als geheel ontwikkelt. Losstaande oplossingen kunnen wel voor leeftijdsverificatie ingezet worden, maar hebben nog zeer beperkte dekkingsgraad.

4.5.1 IRMA

IRMA is één van de bekendere en relatief volwassenere PDM-oplossingen in Nederland. IRMA is een generieke wallet met een sterke identiteitscomponent. Voordeel van IRMA is dat het via een aantal Nederlandse gemeentes toegang krijgt tot het BRP. Hierdoor kunnen betrouwbare identiteits- en leeftijdsgegevens opgehaald worden. IRMA biedt hierbij de mogelijkheid om 18+ attributen uit te wisselen. De fraudebestendigheid van de attributen is discutabel. Het is mogelijk om attributen, waaronder het “18+” attribuut, van bijvoorbeeld een oudere broer of zus in te laden in de app en deze vervolgens te gebruiken. Als er alleen een leeftijdsattribuut uitgewisseld wordt, kan de webwinkel dit niet controleren. Om dit probleem enigszins te ondervangen, kan bij IRMA momenteel maar één set identiteitsattributen vanuit het BRP ingeladen worden.

IRMA wordt al op verschillende plekken in de praktijk ingezet. Momenteel loopt er bijvoorbeeld een pilot waarbij men met IRMA bij de gemeente Amsterdam kan inloggen. Ook is het mogelijk om met IRMA bij Ivido in te loggen. Ivido is een persoonlijke gezondheidsomgeving (PGO) erkend onder het afsprakenstelsel MedMij[78], wat ervoor moet zorgen dat mensen gemakkelijker (digitaal) toegang kunnen krijgen tot hun gezondheidsgegevens.

IRMA werd ontwikkeld door de Radboud Universiteit, maar wordt tegenwoordig beheerd door SIDN. Hiermee heeft IRMA een stabiele onderliggende organisatie. Bij IRMA betaalt de databron voor het aanleveren van gegevens. De vraag is of dit model erg duurzaam is, maar het is wel gunstig voor de webwinkelier die gegevens wil ontvangen. Overigens is het wel zo dat er voor kwaliteitsgarantie (op het gebied van beschikbaarheid) en ondersteuning wel vergoedingen gevraagd kunnen worden aan de data-afnemer.

4.5.2 Datakeeper

Datakeeper (voorheen IDA) is een wallet opgericht in oktober 2020 en ontwikkeld door Rabobank. Datakeeper maakt gebruik van W3C standaarden, voor Verifiable Credentials (VC) en Distributed Identities (DID) [79], waarmee het in potentie interoperabel is met andere SSI-oplossingen die dezelfde W3C-standaarden gebruiken. Momenteel wordt de identiteit ingeladen aan de hand van IoA-oplossingen met NFC en biometrie (zie 3.6.3). Hiermee kan de identiteit op een betrouwbare manier ingeladen worden. Nadeel is dat Datakeeper pas recent gelanceerd is en de dekkingsgraad hierdoor nog laag is. Er worden inmiddels wel de eerste projecten mee gedaan. Zo is Datakeeper ingezet voor het tonen van een attribuut van een negatieve testuitslag bij een aantal van de Fieldlab evenementen. Verder is het aantal use-cases waarbij Datakeeper wordt ingezet beperkt. Dit is echter niet vreemd gezien het korte bestaan van Datakeeper.

Op dit moment ondersteunt Datakeeper de use-case voor leeftijdsverificatie nog niet. In theorie is Datakeeper wel geschikt voor online leeftijdsverificatie. Met IoA op basis van NFC en biometrie wordt de identiteit ingeladen. De geboortedatum is dus één van de attributen die standaard in de wallet aanwezig is.

4.6 IDENTIFICEREN OP AFSTAND

Identificeren op Afstand (IoA) bestaat uit oplossingen die speciaal ontwikkeld zijn om mensen op afstand te identificeren. Dergelijke oplossingen worden momenteel onder andere gebruikt bij het aanvragen van een

[77] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663
[78] https://www.medmij.nl/
[79] Voor VC en DID, zie begrippenlijst

creditcard of het openen van een bankrekening. Zoals de naam doet vermoeden onderscheiden deze oplossingen zich van andere oplossingen omdat er identificatie plaats vindt in plaats van authenticatie.

De oplossingen in deze categorie verschillen op een aantal punten sterk van elkaar. Daarom zullen de verschillende oplossingen binnen deze categorie naast algemeen ook nog uitgebreid per item uitgelicht worden. In Tabel 7 wordt een indicatie gegeven van hoe deze categorie scoort op de succesfactoren. De score moet geïnterpreteerd worden als relatief ten opzichte van de andere oplossingen en categorieën.

Tabel 7 Indicatie van score op succesfactoren voor Identificeren op Afstand

Criteria	ID op Afstand	Video bellen +	OCR	OCR + b
Fraudebestendigheid en betrouwbaarheid	+/-	-	--	+
Beschikbaarheid en dekkingsgraad	+	++	++	++
Gebruiksgemak en begrijpbaarheid	-	-	+/-	-
Schaalbaarheid en flexibiliteit	-	--	+/-	+/-
Kosten	--	--	-	--
Realisatietermijn	++	++	++	++
Toekomtbestendigheid	+	+/-	--	-
Privacy en vertrouwen	+/-	-	-	-

Criteria	NFC	NFC + b
Fraudebestendigheid en betrouwbaarheid	+/-	++
Beschikbaarheid en dekkingsgraad	+	+
Gebruiksgemak en begrijpbaarheid	-	--
Schaalbaarheid en flexibiliteit	++	++
Kosten	--	--
Realisatietermijn	++	++
Toekomtbestendigheid	+	++
Privacy en vertrouwen	-	-

Eén van de grootste verschillen ontstaat rondom betrouwbaarheid en fraudegevoeligheid. Oplossingen die geen gebruik maken van biometrie scoren hier bijzonder slecht op. Dit omdat ze alleen een documentverificatie doen, maar geen holder verification. Door biometrie te gebruiken, vaak in een vorm van gezichtsherkenning, kan gecontroleerd worden of het document bij de gebruiker hoort. Een goede vorm van liveness-detectie[80] is belangrijk om fraudebestendig te zijn. Goed ingezet kan met IoA inclusief biometrie een zeer hoge betrouwbaarheid behaald worden.

De voordelen van identificatie op afstand zijn dat er vaak alleen een mobiele telefoon of ander apparaat met camera voor nodig is. Voor sommige oplossingen moet het apparaat tevens over NFC beschikken, maar dit is bij veel moderne smartphones geen probleem. Ook is de realisatietermijn geen bezwaar. Er zijn al veel spelers op de markt van identificatie op afstand. Dekkingsgraad speelt geen grote rol, omdat de gebruiker überhaupt nog geïdentificeerd moet worden.

Hiermee zijn wel praktisch alle voordelen van identificatie op afstand benoemd. Het gebruiksgemak laat te wensen over. Voor een proces dat bij iedere aankoop uitgevoerd moet worden kost het de gebruiker veel tijd. Hiernaast is het niet privacy vriendelijk zowel voor de klant als de webwinkelier. Er worden hierbij relatief veel persoonsgegevens verwerkt. Het zal dus lastig aan de gebruiker uit te leggen zijn waarom bij iedere aankoop IoA uitgevoerd zou moeten worden. Bovendien, dient de webwinkelier door gebruik van biometrie extra beveiligingsmaatregelen te treffen om de persoonsgegevens conform de AVG te verwerken.

Daar komt bij dat sommige oplossingen slecht schalen, omdat er een handmatige actie vereist is door de aanbieder van IoA. Bij de NFC-gebaseerde oplossingen is dit niet het geval. De kosten per identificatie zijn relatief hoog voor een leeftijdsverificatie.

[80] Zie begrippenlijst

Identificatie op afstand is hiermee ongeschikt voor het vaststellen van de leeftijd bij iedere aankoop. Het is hiervoor een veel te zwaar middel. Voor het eenmalig betrouwbaar vaststellen van iemands identiteit is het daarentegen wel een goede optie. Om een account eenmalig of periodiek te upgraden zou het bijvoorbeeld wel geschikt zijn. De nota van toelichting bij de nieuwe Alcoholwet is echter duidelijk over dat de leeftijdsverificatie voor iedere aankoop moet plaats vinden.

4.6.1 Videobellen (inclusief biometrie)

Videobellen is een geschikte manier om iemand betrouwbaar op afstand te kunnen identificeren. De klant moet hierbij zijn identiteitsdocument tonen en er wordt direct gecontroleerd of hij de rechtmatige eigenaar van het document is. Een apparaat met camera is als gebruiker voldoende om van deze oplossing gebruik te maken. Nadeel is dat de oplossing slecht schaalt. Er moet altijd een medewerker de beelden controleren. Hierdoor zijn de kosten van deze oplossing ook hoog voor online leeftijdsverificatie.

4.6.2 OCR

Optical Character Recognition[81] (OCR) is in de basis te vergelijken met het alom bekende 'koptietje paspoort'. De betrouwbaarheid is erg afhankelijk van de kwaliteit van de gebruikte afbeelding van het paspoort. Omdat er gebruik gemaakt wordt van een afbeelding is het lastig om de echtheidskenmerken van het identiteitsdocument te controleren. Afhankelijk van de gekozen aanbieder is er niet per sé een medewerker nodig voor IoA, maar kan dit ook automatisch. Hierbij geldt wel dat de oplossingen die geheel automatisch werken, vaak minder betrouwbaar zijn. Zonder biometrie is het daarnaast lastig te controleren of het gepresenteerde identiteitsdocument hoort bij degene die de bestelling plaatst.

4.6.3 OCR + biometrie

OCR inclusief biometrie werkt in de basis hetzelfde als OCR. Er is echter nog een extra stap waarbij de gebruiker een selfie moet maken. Hierbij wordt vergeleken of de selfie overeenkomt met de pasfoto op het identiteitsdocument. Op deze manier kan gecontroleerd worden of degene die het proces doorloopt ook eigenaar is van het identiteitsdocument. Of dit goed lukt is zeer afhankelijk van de kwaliteit van de foto van het identiteitsdocument. Hiernaast is het belangrijk dat er goede liveness detectie gedaan wordt.

Nadeel van OCR + biometrie is dat het een dure oplossing is. De kosten voor OCR op een hoog betrouwbaarheidsniveau zijn gebruikelijk hoger dan bij NFC + biometrie. Ook is de oplossing niet bijzonder gebruikersvriendelijk voor het doel wat het dient, online leeftijdsverificatie.

4.6.4 NFC

Veel moderne identiteitsbewijzen beschikken over een chip die met NFC[82]-technologie uitgelezen kan worden. Op de chip staat dezelfde informatie als op het identiteitsbewijs, maar dan in digitaal formaat. Voordeel van informatie uitlezen via NFC is dat de kans op fouten bij het uitlezen van de identiteitsgegevens geminimaliseerd wordt, en het fraudebestendig is, omdat de informatie digitaal ondertekend is. Hiermee is het gebruik van NFC beter geschikt dan OCR. Wel is een vereiste dat de klant beschikt over een apparaat met NFC. Dit is echter geen probleem voor hedendaagse smartphones.

Zonder biometrie is deze oplossing ook beperkt fraudebestendig, omdat er geen holder verification mogelijk is.

4.6.5 NFC + biometrie

NFC inclusief biometrie werkt hetzelfde als NFC. Hierbij wordt nog een extra stap genomen, waarbij de gebruiker een selfie neemt. Hierdoor is te controleren of de klant ook de rechtmatige eigenaar is van het identiteitsdocument. Omdat op de chip van het identiteitsdocument ook een hoge kwaliteit pasfoto staat, is de betrouwbaarheid van de gezichtsherkenning betrouwbaarder dan bij OCR inclusief biometrie.

Ook hier blijft echter gelden dat de kosten hoog zijn. Daarnaast kost het de gebruiker relatief veel tijd. Hierdoor is het niet gebruiksvriendelijk genoeg om bij iedere aankoop uit te moeten voeren.

[81] Voor een uitgebreide uitleg over OCR, zie begrippenlijst.
[82] Zie begrippenlijst

5 Fraudescenario's

In dit hoofdstuk worden de meest waarschijnlijke scenario's om fraude te plegen bij het verifiëren van leeftijd benoemd. Sinds de coronacrisis is er een sterkte toename van cyber criminaliteit[83]. Daarbij is het online risico op fraude groter dan fysiek in de winkel, omdat online fraude anoniemer en beter schaalbaar is. De focus ligt op de online fraude scenario's, maar er zal ook gekeken worden naar de fysieke context.

Per scenario wordt aangegeven voor welke oplossingscategorieën ze van toepassing zijn, wat de implicaties zijn voor leeftijdsverificatie, een korte risicoanalyse gedaan aan de hand van moeite (benodigde tijd en moeilijkheidsgraad), kosten en waarschijnlijkheid. Zowel de fysieke als digitale context is hierin meegenomen en een mogelijke oplossingsrichting is geschetst om het risico te verkleinen. De afweging of het verkleinen van de fraude kans, door middel van bepaalde middelen, opweegt tegen andere factoren, zoals privacy en gebruiksvriendelijkheid, is niet meegenomen in dit hoofdstuk, maar wordt in hoofdstuk 4 behandeld.

Elk scenario focust op het onrechtmatig verkrijgen van alcohol, door een minderjarig persoon. Hierbij probeert de minderjarige een fles sterke drank te kopen van 50 euro. De moeite en de kosten van elk scenario worden weggezet tegen dit bedrag. Twee weken moeite of 300 euro kosten zijn in verhouding erg hoog om deze fles drank van 50 euro te bemachtigen en maken de waarschijnlijkheid van het scenario laag.

De volgende scenario's zijn geanalyseerd:

- Volwassene helpt vrijwillig om fraude te plegen
- Fraude bij zelf toegezegde leeftijdsverificatie
- Gemanipuleerd identiteitsdocument
- Gestolen identiteitsdocument ouder
- Phishing e-mail
- Social engineering aanval
- Inladen andermans attribuut
- Gebruik andermans account
- Gebruik gestolen telefoon + pincode

Deze negen scenario's zijn niet allesomvattend maar geven wel inzicht in de waarschijnlijke mogelijkheden tot fraude. De scenario's en wegingen worden in onderstaande paragrafen toegelicht.

5.1 VOLWASSENE HELPT VRIJWILLIG OM FRAUDE TE PLEGEN

Het kan voorkomen dat een minderjarige geholpen wordt door een volwassene om fraude te plegen. De reden van een volwassene om te helpen zou bijvoorbeeld kunnen zijn dat hij het onterecht vindt dat een minderjarige geen alcohol mag kopen of drinken[84]. Ook kan het voorkomen dat de minderjarige optrekt met meerderjarige vrienden, die hem willen helpen om er bijvoorbeeld "bij te horen".

Voor leeftijdsverificatie is dit scenario van toepassing op elke categorie. Denk aan het vrijwillig inladen van PDM attributen in de wallet van de minderjarige, toegang geven tot de overheids of consumentenoplossingen (zoals het delen van een account van DigiD of iDIN) aan de minderjarige, gebruiken van een betaaloplossing door de minderjarige, of het doorlopen van een identificeren op afstand methode voor de minderjarige.

Vrijwillig helpen met fraude plegen kan ook voorkomen in de fysieke context. Het simpelste voorbeeld is bijvoorbeeld dat een volwassene een fles alcohol koopt voor de minderjarige. Maar ook het gebruik van een ID

[83] https://www.politie.nl/nieuws/2021/januari/22/08-minder-overvallen-woningbraken-en-straatroven-maar-meer-cybercrime.html
[84] https://www.alcoholinfo.nl/opvoeding/jongeren-zijn-strafbaar-als-ze-alcohol-drinken-of-kopen

kaart van een oudere broer of zus is mogelijk. Als de twee broers/zussen erg op elkaar lijken, is het voor een winkelier moeilijk te onderscheiden.

Het voorkomen of detecteren van deze 'vrijwillige hulp' fraude, is erg lastig, zowel digitaal als fysiek. Om deze vrijwillige hulp minder aantrekkelijk te maken wordt het doorgeven van alcohol door een volwassene aan een minderjarige in de publieke ruimte in de nieuwe Alcoholwet strafbaar gesteld[85]. Daarnaast is het belangrijk om te beseffen dat wanneer iemand vrijwillig helpt, deze volwassene ook gewoon alcohol kan kopen, geven en schenken aan een minderjarige. Bij fysieke verkoop aan een volwassene is het relatief lastig om te weten of deze het voor een minderjarige koopt. Een winkelier zou er voor kunnen kiezen om dit aan alle of een deel van de klanten te vragen, met een controle vraag.

In de digitale en fysieke context zou bij de verkoop extra benadrukt kunnen worden dat alcohol alleen bedoeld is voor volwassenen, zo wordt er vaak al gebruikt gemaakt van NIX<18[86], dat aandacht vraagt voor de leeftijdsgrens van alcoholverkoop en gebruik. Het gaat dan echter om bewustzijn en niet om een mitigerende maatregel.

Risico inschatting

- Categorie: Alle
- Moeite: Laag, maar in fysieke context Midden: omdat een volwassene mee moet of ID moet uitlenen.
- Kosten: Laag
- Waarschijnlijkheid in het geval van alcoholverkoop: Hoog

Mitigerende maatregel: Het voorkomen van fraude met behulp van een vrijwillig helpende volwassene is lastig. Het is volgens de nieuwe Alcoholwet verboden om een minderjarige alcohol door te geven (weder verstrekking) in openbare ruimtes, maar in huiselijke kringen is dit lastig te voorkomen.

5.2 FRAUDE MET ZELF TOEGEZEGD

Doordat er bij de zelf toegezegde oplossingen geen enkele of amper verificatie plaatsvindt is het makkelijk om te frauderen bij deze oplossingen. In het voorbeeld van alcohol verkoop kan de minderjarige gewoon liegen over de leeftijd, of indien nodig de leeftijd van een ouder noemen, om zo de leeftijdsverificatie voor de gek te houden en alcohol te kunnen kopen.

Het liegen over de leeftijd wordt in de fysieke context bemoeilijkt. Supermarkten gebruiken de eigen richtlijn om iedereen onder de 25 te vragen om zich te legitimeren. Een minderjarige moet zich dan voordoen als een 25+ persoon, om op deze manier niet zijn legitimatie te hoeven tonen.

Risico inschatting

- Categorie: zelf toegezegd, personal data wallets
- Moeite: Laag, als liegen de minderjarige geen moeite kost.
- Kosten: Laag
- Waarschijnlijkheid in het geval van alcoholverkoop: Hoog, fysieke context: midden

Mitigerende maatregel: De makkelijkste manier om deze fraude te voorkomen is om zelf toegezegde methodes niet te gebruiken voor leeftijdsverificatie.

[85] Artikel 45a, https://zoek.officielebekendmakingen.nl/stb-2021-26.html
[86] https://www.nix18.nl

5.3 GEMANIPULEERD IDENTITEITSDOCUMENT

Er zijn verschillende manieren om een nep ID kaart te maken. Het kan een simpele fotokopie zijn van een echt document[87], tot een plastic kopie, en zelfs een deepfake gemanipuleerde video van een identiteitsdocument. Op internet zijn verschillende voorbeelden[88] en tutorial te vinden om zo'n nepdocument te maken.

Voor het scenario binnen leeftijdsverificatie gaan we uit van een kopie, op glimmend fotopapier, van het echte document van de minderjarige waar digitaal de geboortedatum is gemanipuleerd voordat hij geprint is. De minderjarige maakt een nep ID kaart en deelt deze tijdens het leeftijdsverificatie proces waarbij alleen het laten zien van een identiteitsbewijs genoeg is (Identificeren op Afstand of het gebruik van een betaaloplossing, beide zonder biometrie). Afhankelijk van de methode waarop het identiteitsdocument wordt geverifieerd is er een groter risico op fraude bij de leeftijdsverificatie.

Een fotokopie komt niet door de Identificeren op afstand NFC-methode heen, omdat de kopie geen chip heeft. Voor de identificeren op afstand OCR-methodes bestaat er wel een grote kans dat zulke kopieën worden doorgelaten, omdat het detecteren van deze fotokopieën vaak moeilijk is voor de OCR-methodes. Ook betaaloplossingen die de OCR gebruiken om het identiteitsdocument te verifiëren, als ze hierom vragen wanneer er een account gemaakt wordt, zijn hiervoor kwetsbaar.

In een videogesprek is het erg afhankelijk van de kwaliteit van de video en de persoon die de leeftijd verifieert aan de andere kant van de lijn. In de digitale context kan het gebruik van vervalste identiteitsdocumenten alleen voorkomen worden door een betrouwbare methode te gebruiken om deze te verifiëren. Ook holder verification kan de zekerheid verhogen, zoals het maken van een gezichtsscan met liveness detectie, of het controleren van de betaalgegevens van de koper en zijn identiteitsdocument. Dit voegt wel weer een extra stap toe voor de gebruiker, waardoor dit minder gebruiksvriendelijk is.

In de fysieke context kunnen bovengenoemd methodes zoals NFC, OCR en een gezichtsscan ook toegepast worden. Daarbij is het gebruik van een fotokopie makkelijker te detecteren, Bij het vasthouden van het document is al meteen duidelijk dat het om een papieren versie gaat. Echter kunnen documenten, bijvoorbeeld vanwege 'social distancing', in hoesjes of vanuit de hand van de klant worden aangeboden. Het goed controleren van de echtheidskenmerken van een document en het trainen van mensen om dit te doen, blijft daarom erg belangrijk.

Dit scenario raakt vooral het identificeren op afstand. Identificatie op afstand wordt echter ook gebruikt voor het onboarden van klanten (eerste keer aanmaken van een digitale identiteit, vaak uitgevoerd ten behoeve van een specifiek proces) in verschillende digitale oplossingen. Daarmee raakt dit scenario indirect ook de categorieën betaaloplossingen, personal data wallets, consumentenoplossingen. Als er tijdens het onboarden met IoA fraude is gepleegd vertaalt dit zich door naar de andere oplossingen.

Risico inschatting

- Categorie: IoA (indirect: betaaloplossingen, personal data wallets, consumentenoplossingen)
- Moeite: Midden, gebruik van foto bewerking software om het document goed te manipuleren.
- Kosten: Midden, gebruik van goede printer en kwaliteit papier
- Waarschijnlijkheid in het geval van alcoholverkoop: Midden

Mitigerende maatregel: De kans op fraude met een nepdocument kan verkleind worden door het gebruik van NFC, in plaats van OCR, omdat het namaken van een chip aanzienlijk meer kosten en moeite is dan het maken van een fotokopie. Daarbij kan holder verification in de vorm van een gezichtsscan (met zogenoemde liveness detectie) bijdragen aan de fraudebestendigheid. In praktijk zien we dat veel van deze oplossingen al een combinatie van deze stappen gebruiken. Ook omdat dit voor het verkrijgen van een hoog genoeg betrouwbaarheidsniveau noodzakelijk is

[87] https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/fraude-voorkomen-met-kopie-id-bewijs
[88] https://www.npo3.nl/vals-id-knippen-plakken-aflakken-en-door-naar-halt

5.4 ‘GESTOLEN’ IDENTITEITSDOCUMENT VAN OUDER

Een gestolen of verloren identiteitsdocument is nog steeds een geldig document, omdat deze aan alle kenmerken voldoet en zelfs de chip nog correct werkt. Echter is het document niet meer in het bezit van de rechtmatige eigenaar.

Voor het aankopen van alcohol kan een minderjarige een identiteitsdocument van een van zijn ouders gebruiken om daarmee de leeftijdsverificatie via Identificeren op Afstand voor de gek te houden of het aanmaken van bijvoorbeeld een PayPal betaalrekening. Een alternatief, waarin een minderjarige een document steelt, heeft hogere rechtelijke gevolgen en kost meer moeite en laten we daarom buiten beschouwing. Voor een kind is het makkelijk het document van een ouder te gebruiken (onvrijwillig te lenen, ofwel tijdelijk te stelen) omdat ze in hetzelfde huis wonen en deze documenten niet altijd veilig opgeborgen zijn.

Het risico op fraude is afhankelijk van de verificatie methode. Als enkel het identiteitsdocument wordt gebruikt en geverifieerd, bijvoorbeeld via Identificeren op afstand met NFC of OCR, of bij het openen van een betaalrekening, dan wordt er alleen gekeken of het document echt is, niet of het document ook bij de (minderjarige) persoon hoort die hem aanbiedt.

Het risico op misbruik kan worden verkleind door holder verification om de identiteit te verifiëren, zoals een biometrische gezichtsscan of het verifiëren of de betaalgegevens overeenkomen met de details van het identiteitsdocument. Door het uitvoeren van een scan kan vastgesteld worden of de persoon die het document vasthoudt ook bij het document hoort.

In de fysieke context is het makkelijker om deze manier van fraude te detecteren omdat men kan zien dat een minderjarige het identiteitsdocument van een van zijn ouders gebruikt doordat de foto niet klopt en de leeftijd sterk afwijkt.

Dit scenario raakt vooral de identificeren op afstand, maar net als in 5.3 al genoemd, wordt IoA gebruikt voor de onboarding van klanten in verschillende online systemen. Daarmee raakt dit scenario indirect ook de categorieën betaaloplossingen, personal data wallets, consumentenoplossingen. Als er tijdens onboarding met de IoA fraude is gepleegd vertaalt dit zich door naar de andere oplossingen.

Risico inschatting

- Categorie: IoA, (indirect: betaaloplossingen, personal data wallets, consumentenoplossingen)
- Moeite: laag
- Kosten: laag
- Waarschijnlijkheid in het geval van alcoholverkoop: Hoog

Mitigerende maatregel: De kans op fraude met een ‘gestolen’ (ofwel: onvrijwillig geleend) document kan verkleind worden door het toevoegen van een gezichtsscan (met zogenoemde liveness detectie) als tweede stap. In de praktijk zien we dat veel van deze oplossingen al een combinatie van deze stappen gebruiken. Ook omdat dit voor het verkrijgen van een hoog genoeg betrouwbaarheidsniveau noodzakelijk is.

5.5 PHISHING E-MAILS

Phishing e-mails zijn e-mails die lijken te komen van een betrouwbare instantie, maar dat niet zijn. In de e-mail wordt de ontvanger gevraagd in te loggen met bijvoorbeeld DigiD en iDIN, of een betaling te doen met bijvoorbeeld zijn bankrekening, PayPal of creditcard. Vaak wordt in deze e-mails ingespeeld op het gevoel van urgentie, waardoor mensen snel willen of moeten reageren. Denk hierbij aan een e-mail voor een vergeten factuur die per direct betaald moet worden anders krijg je een boete of het bericht dat je betaalpas gehackt is en daarom geblokkeerd is en dat je snel en veilig een nieuwe moet aanvragen via de bijgevoegde link. Er zijn voorbeelden bekend van phishing e-mails van onder andere iDIN[89], DigiD[90], PayPal[91] en creditcards[92]. Zie ook Figuur 1 voor een voorbeeld van een dergelijke e-mail.

Figuur 1. Voorbeeld van een recente DigiD phising e-mail.

In het geval van leeftijdsverificatie zou het kunnen voorkomen dat een meerderjarige een (phishing) e-mail krijgt waarin wordt gevraagd om de leeftijd te verifiëren en een “boete” te betalen. De minderjarige, de afzender van de mail, kan hiermee het bestelproces van alcohol (beide leeftijdsverificatie en betaling) afronden, of toegang krijgen tot de gegevens van accounts waarbij hij vervolgens zelf dit proces kan afronden.

Phishing e-mails spelen ook een rol in de fysieke wereld. Zo kan het ook voorkomen dat klanten gevraagd worden om hun gegevens via papieren brieven waarin gevraagd wordt om hun inlog gegevens, zoals bijvoorbeeld gebeurde bij de bank ING[93]. De succesvolle phishing mails en brieven zijn goed nagemaakte e-mails met een vertrouwd beeldmerk, waardoor ze slecht te onderscheiden zijn van de echte brieven en mensen er gemakkelijker intrappen en hun gegevens delen.

Om het risico te verkleinen wijzen eigenlijk alle oplossingen hun gebruikers op het bestaan van deze mails en brieven. Ook wordt er benadrukt door de meeste oplossingen dat zij nooit een link in een e-mail of SMS zullen gebruiken en nooit zullen vragen om inlog gegevens van de gebruiker. Zo meldt de website van DigiD: “Let op, er staat nooit een link in een e-mail of sms van DigiD”[94].

Risico inschatting

- Categorie: personal data wallets, consumentenoplossingen, overheidsoplossingen, betaaloplossingen, IoA
- Moeite: Hoog, het bouwen van een (realistische) valse website of e-mail kost veel tijd.
- Kosten: Laag.
- Waarschijnlijkheid in het geval van alcoholverkoop: Laag, deze aanval kost veel moeite en vraagt daarbij specifieke kennis om dit systeem te bouwen, ten opzichte van de mogelijke winst (een fles alcohol).

Mitigerende maatregel: De waarschijnlijkheid van deze aanval is erg laag in het geval van alcohol verkoop, waardoor een mitigerende maatregel uit verhouding is. Daarnaast is het verkleinen van de kans op fraude door middel van phishing e-mails lastig. Maatregelen focussen zich op gebruikers bekend maken met het bestaan en

[89] https://www.idin.nl/actueel/valse-mail-idin/
[90] https://opgelicht.avrotros.nl/alerts/artikel/valse-mail-van-digid-uw-digid-account-dient-geverifieerd-te-worden/
[91] https://opgelicht.avrotros.nl/alerts/artikel/pas-op-er-gaat-veel-paypal-phishingmail-rond/
[92] https://www.icscards.nl/klantenservice/veiligheid/zo-herkent-en-meldt-u-phishing
[93] https://opgelicht.avrotros.nl/alerts/artikel/klant-van-ing-kijk-uit-voor-phishing-oplichters-sturen-valse-brieven-namens-de-bank/
[94] https://www.digid.nl/veiligheid/phishing/

de risico's van deze e-mails. In praktijk zien we ook dat onder andere DigiD en de Nederlandse banken druk bezig zijn met het bewustmaken van hun gebruikers voor phishing e-mails.

5.6 SOCIAL ENGINEERING AANVAL

Een social engineering aanval is erop gericht om een persoon voor de gek te houden. Deze aanvallen focussen op de sociale kant van de mens, door ze voor te liegen, te verleiden of af te leiden. Een phishing aanval, zie ook het scenario phishing aanval, is een specifieke vorm van een social engineering aanval.

Bij de leeftijdsverificatie zou het bijvoorbeeld kunnen voorkomen dat een minderjarige een onwetende meerderjarige overtuigt om de online leeftijdsverificatie te doen om alcohol te kopen voor hem. Reden die de minderjarige hiervoor kan opgeven is bijvoorbeeld dat hij een cadeau voor vader- of moederdag wil kopen, of dat hij online medicijnen moet bestellen voor een zieke ouder. Ook zou in dit scenario inlog gegevens kunnen worden verkregen van een volwassene, zie ook scenario 5.8.

Het risico op deze fraude wordt verkleind doordat erop bijna alle online webwinkels expliciet wordt samengevat, wat er is gekocht en waar het naartoe verzonden wordt.

In de fysieke context resulteert deze aanval in een variatie op het in scenario 5.1 geschetste "een volwassene helpt een minderjarige vrijwillig".

Risico inschatting

- Categorie: personal data wallets, consumentenoplossingen, overheidsoplossingen, betaaloplossingen, IoA
- Moeite: Hoog
- Kosten: Laag
- Waarschijnlijkheid in het geval van alcoholverkoop: Laag

Mitigerende maatregel: de waarschijnlijkheid van deze aanval is laag in het geval van alcohol verkoop, waardoor geen harde mitigerende maatregel nodig is. Daarnaast is het verkleinen van de kans op fraude door middel van een social engineering aanval lastig, maar focust de aanpak zich op gebruikers bewust maken gegevens nooit te delen en ze bekend te maken met het bestaan en de risico's van deze aanvallen. In de praktijk zijn onder andere banken bezig met deze bewustwording met zinnen als: "wij vragen je nooit om je pincode en ook niet naar andere inloggegevens."

5.7 INLADEN ANDERMANS ATTRIBUTEN

Veel personal data wallets binden de data attributen die worden ingeladen in een wallet niet aan een persoon of identiteit. Het is hierdoor mogelijk om andermans attributen in te laden, te bezitten en deze vervolgens te delen alsof deze van jou zijn. Voor leeftijdsverificatie zou dat betekenen dat een minderjarig persoon in zijn wallet het attribuut van iemand die 18+ is inlaadt (bijvoorbeeld een oudere broer of zus). Vervolgens gebruikt de minderjarige dit attribuut om te delen bij het kopen van alcohol.

Doordat attributen die eenmaal ingeladen zijn langere tijd beschikbaar blijven, is het ook makkelijk om structureel iemand anders z'n leeftijd te gebruiken. Nadat de leeftijd van oudere broer of zus is ingeladen, kan deze langere tijd gebruikt worden voor bijvoorbeeld de aankoop van alcohol.

In zowel de fysieke als digitale context zal de winkel iemand vragen om zijn "18+" attribuut te delen, omdat deze niet gekoppeld is aan bijvoorbeeld andere attributen waarmee de identiteit kan worden bepaald, kan niet worden nagegaan of het "18+" attribuut ook daadwerkelijk bij de koper hoort. Om dit risico te verkleinen zou de winkel kunnen vragen om nog een ander attribuut, wat gekoppeld is aan het 18+ attribuut. Belangrijk is wel dat dit attribuut ook echt gekoppeld is aan het "18+" attribuut, wat in veel wallets nog niet het geval is omdat dit vanuit een privacy oogpunt weer meer data vrijgeeft dan nodig. In de digitale context kan het "18+" attribuut bijvoorbeeld gecombineerd worden met het naam attribuut, welke bij bestelling en/of ontvangst gecontroleerd wordt met de ontvangende partij. Dit is echter niet verplicht onder de Alcoholwet. In de fysieke context zou het "18+" attribuut bijvoorbeeld gecombineerd kunnen worden met een foto, welke gecontroleerd

kan worden met degene die de telefoon vast heeft. Echter met het delen van meer attributen heeft de gebruiker minder privacy en is er minder dataminimalisatie.

Risico inschatting

- Categorie: personal data wallets
- Moeite: Laag, het kost weinig moeite om dit scenario uit te voeren: je moet enkel een volwassene overhalen om (eenmalig) te helpen
- Kosten: Laag
- Waarschijnlijkheid in het geval van alcoholverkoop: Hoog

Mitigerende maatregel: De kans op fraude door middel van het inladen van andermans attribuut is te verkleinen door naast het 18+ attribuut, ook een ander attribuut te ontsluiten, zoals naam of foto, welke vervolgens ook gecheckt wordt met de naam van de bestelling. In praktijk zien we dit nog niet overal gebeuren, omdat het landschap van personal data wallets nog in ontwikkeling is. Privacy en dataminimalisatie spelen hier ook een rol, deze zijn belangrijk voor veel personal data wallets.

5.8 GEBRUIK ANDERMANS ACCOUNT

De toegang tot andermans account kan op verschillende manieren verkregen worden, bijvoorbeeld door een phishing mail, social engineering attack of het stelen van de data. Dit account kan vervolgens misbruikt worden.

De minderjarige krijgt toegang tot het account van een meerderjarige op bijvoorbeeld DigiD of iDIN. Het gebruik van andermans account zou om verschillende manieren kunnen gebeuren, denk hierbij aan stiekem gebruik van het account van een ouder, bijvoorbeeld omdat de ouder digibeet is of de taal niet goed beheerst. Benadrukt moet worden dat het hier gaat om randgevallen, ook omdat deze accounts niet zomaar uitgeleend worden.

Het impliciet gebruik van andermans account wordt bemoeilijkt door het gebruik van een tweede authenticatiefactor, wat betekent dat de minderjarige ook toegang moet hebben tot deze factor om de online alcohol verkoop af te ronden. Gebruik van een tweede factor is een eis voor betrouwbaarheid niveau substantieel. In praktijk wordt deze tweede factor bij veel oplossingen al toegepast. Als de minderjarige toegang heeft tot het account en de tweede factor, dan kan deze ook gebruikt worden in de fysieke context.

Om fraude te voorkomen moet er gebruik worden gemaakt van een tweede factor. Ook een bevestigende mail, waarin de volwassene op de hoogte wordt gesteld van het gebruik van het account is een oplossing, vooral als er ook een snelle manier wordt aangeboden om fraude te melden. Daarnaast is ook oplettendheid van de accountbezitter gewenst en als deze fraude wordt gedetecteerd deze meteen te melden en het account te laten blokkeren.

Risico inschatting

- Categorie: Consumentenoplossingen, overheidsoplossingen, betaalmiddel
- Moeite: Laag
- Kosten: Laag
- Waarschijnlijkheid in het geval van alcoholverkoop: Midden

Mitigerende maatregel: De kans op fraude door middel van het gebruik van andermans account is te verkleinen door het toevoegen van een tweede factor, welke ook vereist is voor een betrouwbaarheidsniveau substantieel. In praktijk gebruiken veel online oplossingen deze tweede factor al.

5.9 GEBRUIK VAN GESTOLEN TELEFOON + PINCODE

Een gestolen telefoon in combinatie met de correcte pincode kan gebruikt worden om fraude te plegen. Een dief zou over de schouder van de gebruiker kunnen meekijken als deze zijn PIN intoetst en vervolgens het toestel kunnen ontvreemden.

In dit scenario zou de minderjarige het telefoontoestel van een meerderjarige kunnen gebruiken om daarmee de leeftijdsverificatie bij de online alcohol verkoop af te ronden. Dit kan als de telefoon bijvoorbeeld gekoppeld is aan een personal data wallet, overheid/consumentenoplossingen of betaaloplossing.

Deze aanval is lastig te detecteren, de minderjarige heeft namelijk toegang tot alle gegevens in de telefoon, zoals de DigiD app, de betaal app en dus de tweede factor (zoals uitgelegd in sectie 5.8). Oplettendheid van de telefoonhouder en de bezitter van de accounts is dan ook nodig. Het is mogelijkheid om de bank accounts, attributen in een wallet en authenticatie middelen te blokkeren wanneer men weet dat deze gestolen of gelekt zijn. Hetzelfde geldt voor een goede en snelle manier van het resetten van PIN codes en wachtwoorden. Het is dan ook aan de volwassene om deze stappen direct te ondernemen wanneer hij of zij erachter komt dat de telefoon gestolen is of fraude is gepleegd met een van de accounts.

Afhankelijk van de oplossing is deze methode toepaspaar in de fysieke context. Voor personal data wallets is het bijvoorbeeld mogelijk om het “18+” attribuut te laten zien op de telefoon, zie ook scenario “inladen andermans attributen”. Het gebruik van (leeftijd) geverifieerd betaalmiddel of authenticatie oplossing is ook mogelijk.

Risico inschatting

- Categorie: personal data wallets, consumentenoplossingen, overheidsoplossingen, betaaloplossing
- Moeite: Hoog, er moet iets gestolen worden en de PIN-code moet onderschept worden
- Kosten: Laag, stelen kost niets
- Waarschijnlijkheid in het geval van alcoholverkoop: Laag

Mitigerende maatregel: De waarschijnlijkheid op dit scenario in het geval van alcohol verkoop is klein. Het verkleinen van de kans op fraude door middel van het gebruik van andermans telefoon is lastig, omdat de minderjarige toegang heeft tot alles (dus ook de tweede factor). Het is aan de meerderjarige accounthouder om zijn account goed in de gaten te houden en bij onraad accounts te blokkeren en wachtwoorden te resetten.

5.10 CONCLUSIE

De risico inschatting van elk scenario’s en de getroffen categorieën zijn weergegeven in Figuur 2.

			Waarschijnlijkheid bij	Getroffen categorie					
Scenario titel	Moeite	Kosten	leeftijdsverificatie	PDW	CO	OO	BO	IoA	Zelf
Volwassene helpt vrijwillig om fraude te plegen	Laag	Laag	Hoog	●	●	●	●	●	●
Fraude met zelftoegezegd	Laag	Laag	Hoog	●					●
Gemanipuleerde identiteitsdocument	Midden	Midden	Midden	○	○		○	●	
Gestolen identiteitsdocument van ouder	Laag	Laag	Hoog	○	○		○	●	
Phishing email	Hoog	Laag	Laag	●	●	●	●	●	
Social engineering aanval	Hoog	Laag	Laag	●	●	●	●	●	
Inladen andermans attributen	Laag	Laag	Hoog	●					
Gebruik andermans account	Laag	Laag	Midden		●	●	●		
Gebruik gestolen telefoon + pincode	Hoog	Laag	Laag	●	●	●	●		

●	Direct
○	Indirect
	n.v.t.

Figuur 2. Een overzicht van de verschillende fraude scenario’s. Per scenario zijn de score van de risicoanalyse weergegeven (door middel van laag, midden of hoog) en de getroffen categorie aangegeven (met een rondje). De risicoanalyse bestaat uit moeite, kosten en waarschijnlijkheid op een schaal van laag, midden en hoog.

In het algemeen zijn bijna alle categorieën gevoelig voor een of meerdere fraudescenario’s. Echter kosten een aantal van deze fraudescenario’s buiten proportioneel veel moeite of geld, die niet opwegen tegen de te behalen winst (namelijk een fles alcohol), waardoor hun waarschijnlijkheid laag is bij online alcoholverkoop. Dit is het geval voor phishing e-mails, social engineer aanvallen en het gebruik van een gestolen telefoon + pincode.

Daarentegen heeft het “vrijwillig helpende volwassene” scenario een hoge waarschijnlijkheid, waar geen grote mitigerende maatregelen tegen genomen kunnen worden. Voor de minderjarige is het een makkelijk uit te voeren scenario en als er eenmaal een volwassene meehelpt, hebben de mitigerende maatregelen bij de andere scenario’s geen effect. Het is in de Alcoholwet verboden om een minderjarige alcohol te geven in

openbare ruimtes, maar in huiselijke kringen kan dit nog steeds voorkomen. Het is echter geen “nieuw” fraude scenario voor leeftijdsverificatie, omdat dit in de fysieke context ook al kan voorkomen.

Ook fraude met “zelf toegezegde” leeftijdsverklaringen zijn niet te voorkomen. De mitigerende maatregel is hier simpel: gebruik deze oplossingen niet voor online leeftijdsverificatie.

Andere scenario’s die waarschijnlijk zijn bij online leeftijdsverificatie, zijn wel te mitigeren. Voor fraude met nepdocumenten geldt dat het gebruik van NFC methode meer fraude voorkomt dan OCR methode. Daarbij kan het toevoegen van een tweede factor, bijvoorbeeld een gezichtsscan (met zogenoemde liveness detectie), bijdragen aan de fraudebestendigheid. Daarbij is een tweede factor bij online authenticatie ook een eis voor betrouwbaarheidsniveau substantieel. Een gezichtsscan als tweede factor kan ook de fraude kans bij een ‘gestolen’ (ofwel: onvrijwillig geleend) document verkleinen. De kans op fraude door middel van het inladen van andermans attribuut is te verkleinen door naast het 18+ attribuut, ook een ander attribuut te ontsluiten, zoals naam of foto. Echter worden hierdoor andere succesfactoren zoals dataminimalisatie en privacy weer minder belangrijk geacht.

5.11 SAMENVATTING FRAUDESCENARIO’S

Samengevat concluderen we dat het voor leeftijdsverificatie afgeraden wordt om oplossingen met zelf toegezegd leeftijdsverklaringen te gebruiken. Daarbij is er, naast een verbod in de Alcoholwet, technisch niet altijd een oplossing tegen een fraudescenario met een vrijwillig helpende volwassene. Echter voor de meeste fraudescenario’s kan de kans op fraude bij online leeftijdsverificatie worden verkleind met mitigerende maatregelen, zoals het eisen van een tweede factor bij authenticatie en campagnes om bewustzijn te verhogen. Wel moet de afweging gemaakt worden of deze maatregelen opwegen tegen de andere succesfactoren, zoals privacy, dataminimalisatie, implementatie en gebruiksvriendelijkheid, zoals benoemd in hoofdstuk 2. Zeker als de waarschijnlijkheid van een fraudescenario klein is.

6 Toetsen fysieke verificatie

In dit onderzoek wordt voornamelijk gefocust op middelen voor online leeftijdsverificatie. Een aantal partijen heeft echter ook interesse geuit om deze digitale middelen in fysieke context in te kunnen zetten. Het gegeven argument is dat ze hiermee de kwaliteit van de leeftijdsverificatie beter kunnen borgen. Hierbij hanteren deze partijen het uitgangspunt dat bij iedere persoon een leeftijdsverificatie uitgevoerd moet worden. Ook als deze persoon overduidelijk meerderjarig is, en de leeftijdsverificatie aan de hand van een WID volgens de wet dus niet nodig is. Dit zorgt er namelijk voor dat er geen ruimte meer is voor interpretatie van de medewerker. Hij kan ook niet in verlegenheid gebracht worden door te vragen om de leeftijd te mogen controleren. Dit speelt onder andere bij de bezorging van pakketten.

Momenteel mag een leeftijdsverificatie in fysieke context alleen gebeuren aan de hand van een WID (wettelijk identificatiemiddel). De winkelier moet in staat zijn om de echtheid van het WID te controleren en moet de persoon betrouwbaar kunnen identificeren aan de hand van het getoonde WID. Dit vereist enige kennis en training van medewerkers en mogelijk apparatuur.

In onderstaande analyse onderzoeken we hoe de verschillende oplossingen zich staande houden in fysieke context. Belangrijk is dat er in fysieke context ook verschillende use-cases mogelijk zijn, zoals:

- ***Bezorging van pakket aan de deur***: Na de online aankoop wordt het pakket door de webwinkel via een bezorgdienst opgestuurd. Het pakket met alcoholhoudende drank wordt aan de deur bezorgd. De webwinkel heeft aangegeven dat voor dit pakket leeftijdsverificatie nodig is. De bezorger stelt aan de deur vast of iemand voldoende oud is om het pakket aan te mogen nemen.

- ***Uitgifte van pakket bij pakketpunt***: Na de online aankoop wordt het pakket door de webwinkelier via een bezorgdienst opgestuurd. Het pakket wordt bij een afhaalpunt bezorgd. De klant komt op een zelfgekozen tijdstip naar het pakketpunt om het pakket op te halen. Voordat het pakket uitgegeven wordt, wordt door veel bezorgdiensten eerst nog de identiteit gecontroleerd. In principe biedt dit bij een pakket waarvoor de leeftijd geverifieerd moet worden direct de mogelijkheid om dit te doen.

- ***Verkoop van alcohol in de winkel***: Bij aankoop in de winkel verzamelt de klant gebruikelijk zelf zijn producten voordat hij hiermee langs de kassa loopt. Voordat bij de kassa de aankoop gedaan wordt, wordt eerst de leeftijd geverifieerd. Omdat het moment van aankoop en uitgifte samenvallen is er maar één keer een leeftijdsverificatie nodig. In potentie zou een use-case met een digitaal middel in fysieke context ook bij (zelfscan/onbemande) kassa's van meerwaarde kunnen zijn. Er is dan geen ruimte meer voor interpretatie en er is geen interactie met een medewerker meer nodig.

Van bovenstaande scenario's liggen de eerste twee scenario's in het verlengde van de online verkoop van alcoholhoudende dranken. Het derde scenario staat hier los van. In alle drie de scenario's vindt leeftijdsverificatie nu plaats aan de hand van een WID. Dit scenario zal voor onderstaande analyse per categorie ook als vergelijkingsmateriaal gebruikt worden. De verschillende oplossingscategorieën zullen verder aan dezelfde eisen getoetst worden als in de online context. Omdat de score op een aantal eisen niet verandert ten opzichte van de online context worden ze in dit hoofdstuk niet verder besproken. Het gaat hier om de eisen beschikbaarheid en dekkingsgraad, schaalbaarheid en flexibiliteit en toekomstbestendigheid. Het draagvlak onder ondernemers wordt besproken bij de uitkomsten van de interviews (hoofdstuk 7). Ook de eis fraudebestendigheid en betrouwbaarheid verandert nauwelijks in de fysieke context, maar aangezien dit één van de belangrijkste eisen is, is hij toch in de vergelijking meegenomen. In

Tabel 8 worden de verschillende categorieën ten opzichte van de eisen gewogen. Een verdere toelichting is te vinden in de verschillende paragrafen van dit hoofdstuk.

Tabel 8: Indicatie van score van de categorieën in fysieke context

Eis / Categorie	PDM	Consument	Overheid	Betalen	IoA	Zelf-toegezegd	WID
Fraudebestendigheid en betrouwbaarheid	+/-	++	++	+/-	+/-	--	+
Gebruiksgemak en begrijpbaarheid	-	+/-	+	+	--	++	++
Kosten	-	-	+/-	+	--	++	++
Realisatietermijn	-	+	--	+/-	++	++	++
Privacy en veiligheid	+	+/-	+/-	++	-	++	+

6.1 PERSONAL DATA WALLETS

Personal data wallets maken het mogelijk om attributen te delen. In de fysieke context zijn er verschillende richtingen denkbaar. Het is mogelijk dat de gebruiker een 18+-attribuut deelt door een QR-code te tonen die de winkelier kan scannen. Het kan ook andersom door de gebruiker een QR-code te laten scannen en een attribuut te laten delen. Ook in de fysieke context is het een uitdaging om een harde koppeling te maken tussen attribuut en de identiteit van de gebruiker. Bij een normaal identiteitsbewijs gebeurt dit aan de hand van de pasfoto. Eventueel zou een dergelijke foto ook getoond kunnen worden door de wallet. Als foto en leeftijd aan elkaar gekoppeld zijn, biedt dit voldoende betrouwbaarheid, maar wordt er minimaal informatie gedeeld. Er hoeft in ieder geval niet alle informatie die op het WID staat getoond te worden. Het is dus mogelijk om personal data wallets als privacy vriendelijke oplossing te gebruiken in de fysieke context. De zorg over het inladen van andermans identiteit blijft echter ook in fysieke context bestaan.

De kosten om personal data wallets te implementeren voor leeftijdsverificatie is afhankelijk van de huidige situatie van de bezorger of locatie. Als de winkelier een QR-code moet scannen, is er apparatuur nodig om dit te doen. In het geval van bezorging zijn de bezorgers vaak al uitgerust met scanners. In de winkel is dit minder waarschijnlijk en zouden kassasystemen hierop ingericht moeten worden. Of er moeten aparte scanners aangekocht worden. Zeker in verhouding met het WID brengt dit een stijging in kosten met zich mee.

Gezien de volwassenheid en adoptie van personal data wallets nog beperkt zijn is het echter niet realistisch om dergelijke oplossingen op korte termijn al in fysieke context toe te passen.

6.2 CONSUMENTENOPLOSSINGEN

Consumentenoplossingen zijn speciaal ontwikkeld om iemands identiteit online op een hoog betrouwbaarheidsniveau vast te kunnen stellen. Online wordt een proces normaliter geïnitieerd door als gebruiker een QR-code te scannen met de authenticatieoplossing. Voor iDIN zijn er echter ook een aantal oplossingen die gebruik maken van een hardware token. Deze moet dus wel bij de hand zijn op het moment dat de leeftijdsverificatie uitgevoerd moet worden. Dit is niet triviaal op het moment dat je bij een pakketpunt of in de winkel staat. Hiermee daalt het gebruikersgemak van iDIN in de fysieke context ook sterk.

Voordeel is dat veel oplossingen de mogelijkheid bieden een 18+-attribuut te delen, wat de privacy van de gebruiker ten goede komt. De betrouwbaarheid blijft ook in fysieke context hoog. Zeker bij iDIN waar een harde koppeling is gemaakt met het bankaccount, waardoor het minder aantrekkelijk is het authenticatiemiddel uit te lenen. De implementatiekosten voor leeftijdsverificatie met consumentenoplossingen zullen hoger liggen dan de controle van een WID. Tevens zal het meer tijd kosten, zeker als de klant nog niet gewend is aan een dergelijk proces.

Desondanks lijken consumentenoplossingen ook geschikt voor toepassing in de praktijk. Op moment van schrijven heeft PostNL leeftijdsverificatie aan de deur op basis van iDIN geïmplementeerd (tot 1 juli). In eerste instantie werd de pilot gestart waarbij het de bedoeling was dat er primair van IDIN gebruik werd gemaakt[95]. Na herziening vanwege verplichte acceptatie van het WID als identificatiemiddel, is besloten beide methodes te gebruiken tijdens de pilot. Daarbij was reguliere identificatie het alternatief op het gebruik van IDIN. De eerste resultaten van deze pilot lijken positief. Echter is het digitaal identificeren aan de deur ook nieuw voor mensen en gewenning aan een dergelijke oplossing kost tijd.

[95] https://www.postnl.nl/ontvangen/pakket-ontvangen/bezorging-pakketten/leeftijdscheck-aan-de-deur/

6.3 OVERHEIDSOPLOSSINGEN

Een aantal partijen ziet graag dat de overheid naast de verantwoordelijkheid voor de uitgifte van identiteitsdocumenten ook verantwoordelijkheid neemt in het digitale domein. DigiD focust zich voorlopig echter nog op het overheidsdomein en organisaties met een publieke taak. Ook levert DigiD standaard het BSN terug in plaats van de leeftijd. Deze bezwaren uit de digitale context gelden net zo goed in de fysieke context.

Hiernaast is het niet direct duidelijk hoe de userflow er uit zou zien bij het gebruik van DigiD voor fysieke leeftijdsverificatie. Voor de hand ligt dat de gebruiker een QR-code scant met de DigiD-app. Momenteel wordt er bij de DigiD app gebruik gemaakt van een koppelcode, die een dergelijk proces in de war schopt.

Tot slot kost ook de DigiD leeftijdsverificatie waarschijnlijk meer tijd dan het controleren van een WID en is het kostenmodel onduidelijk. In theorie kan DigiD gebruikt worden voor leeftijdsverificatie in fysieke context. Met bovenstaande bezwaren is het op korte termijn echter geen realistische optie.

In de toekomst zijn er mogelijkheden denkbaar rondom concepten zoals de Digitale Bronidentiteiten of vID (een digitaal identiteitsbewijs dat in een app getoond kan worden). Het is echter niet te verwachten dat dergelijke opties gedurende 2021 of 2022 wijdverspreid beschikbaar en bruikbaar zullen zijn.

6.4 BETAALOPLOSSINGEN

Een aantal van de eerder geïntroduceerde betaaloplossingen zijn speciaal ontwikkeld voor gebruik in online context. Denk hierbij aan PayPal en iDEAL. Tijdens de coronacrisis heeft iDEAL in combinatie met betaalverzoeken echter ook bewezen geschikt te zijn in de fysieke context. Bij PayPal ligt het gebruik in fysieke context minder voor de hand. Creditcards zijn juist ontwikkeld voor gebruik in fysieke context, waarna later ook opties zijn ontstaan om deze online te gebruiken.

iDEAL en creditcards zijn in potentie geschikt voor gebruik bij fysieke leeftijdsverificatie. Hier moeten echter wel de kanttekeningen zoals beschreven in hoofdstuk 4 in acht genomen worden. iDEAL biedt momenteel nog geen betaling met leeftijdsverificatie aan. Bij de creditcard is de fraudegevoeligheid hoger. Daarnaast worden lang niet overal in Nederland creditcards geaccepteerd.

Nog steeds worden betalingen in de winkel ook met cash of met pinpas betaald. Deze betaaloplossingen bieden geen mogelijkheid voor leeftijdsverificatie. Een betaalmiddel is meestal niet geschikt voor gebruik bij bezorging of afhalen bij een pakketpunt. De bestelling wordt dan immers gebruikelijk via een andere weg betaald. In fysieke context bieden betaaloplossingen daarmee geen duidelijke meerwaarde ten opzichte van andere leeftijdsverificatiesystemen. Dit omdat bij veel van de betalingen of het aannemen van een pakket alsnog een extra stap gedaan zal moeten worden voor de leeftijdsverificatie.

6.5 IDENTIFICATIE OP AFSTAND

Bij identificatie op afstand wordt nu altijd de identiteit aan de hand van een identiteitsbewijs vastgesteld. Er worden vergelijkbare handelingen verricht zoals deze ook nu al bij fysieke controle uitgevoerd worden (zie hoofdstuk 2). De processen die ingericht dienen te worden voor IoA kosten relatief veel tijd en zijn prijzig. Tevens biedt IoA in de basis geen mogelijkheden voor dataminimalisatie.

Wel zijn er een aantal alternatieven speciaal voor fysieke context geweest. Enkele stakeholders benoemden het systeem AgeViewer[96], waarbij een medewerker op afstand iemands leeftijd verifieert, als alternatief. Dit initiatief is gestopt omdat het niet voldoende voet aan de grond kon krijgen. Ook zijn er kassasystemen beschikbaar waarbij de kassamedewerker bijvoorbeeld de leeftijd moet invullen. Dit gaat echter altijd op basis van een WID.

Identificatie op afstand biedt beperkt voordelen ten opzichte van de huidige fysieke controle, en heeft enkele nadelen. Het is dus minder geschikt voor fysieke leeftijdsverificatie dan andere oplossingen.

[96] Zie https://nos.nl/artikel/2166550-jumbo-wint-rechtszaak-van-leeftijdscontrolesysteem-ageviewers

6.6 ZELF TOEGEZEGD

Net zoals bij online leeftijdsverificatie biedt zelf toegezegd in de fysieke context te weinig betrouwbaarheid. De persoon kan gemakkelijk liegen over de leeftijd. Zeker als hij of zij er meerderjarig uitziet.

Bij bezorging, uitgifte of fysieke verkoop krijgt de klant de alcohol daadwerkelijk in handen. Hier is een betrouwbare leeftijdsverificatie dus van belang. Zelf toegezegd is dus ongeschikt voor leeftijdsverificatie.

6.7 UITDAGINGEN VOOR FYSIEKE LEEFTIJDSVERIFICATIE

In potentie zijn een aantal van de oplossingen voor online leeftijdsverificatie ook in fysieke context in te zetten. Er moet echter goed nagedacht worden over de meerwaarde die dit biedt ten opzichte van het controleren van een WID. Veel van de oplossingen zullen de gebruiker meer tijd kosten. Wel biedt het mogelijkheden voor dataminimalisatie, omdat niet alle informatie die op een WID vermeld staat met digitale middelen ontsloten moet worden. In een aantal gevallen is het voldoende om alleen een 18+-attribuut te delen.

Over alle categorieën heen zijn er een aantal vragen die boven komen drijven voor het gebruik bij leeftijdsverificatie in fysieke context. Allereerst is de vraag of alle middelen die online geaccepteerd worden ook fysiek geaccepteerd moeten worden. Gaat het hierbij om een verplichting waarbij de winkelier alle middelen moet accepteren, zoals nu met het WID het geval is, of mag de winkelier kiezen welke middelen hij accepteert? De eerste optie zou betekenen dat de winkelier veel verschillende opties moet gaan accepteren. Dit zal zorgen voor een laag draagvlak onder ondernemers. Bij de tweede optie ontstaat het risico dat de klant bij iedere winkel een ander middel kan of moet gebruiken. Dit zorgt voor verwarring bij de klant en een lage gebruikersvriendelijkheid.

Vervolgens is het de vraag of een winkelier het gebruik van één specifiek digitaal middel mag afdwingen of dat een WID nog steeds geaccepteerd moet worden. Bij fysieke koop en aflevering moet het WID in ieder geval altijd geaccepteerd worden, ook als er een digitaal alternatief aangeboden wordt. Daarnaast zal een digitaal middel afdwingen in de fysieke context de gebruikersvriendelijkheid nog verder doen dalen. Dit zou ook de inclusiviteit schaden. Een gedeelte van de mensen geeft de voorkeur om fysiek aankopen te doen en zou op deze manier alsnog tot een digitaal middel gedwongen worden. Mogelijk zijn ze zelf niet in staat om een dergelijk digitaal middel te gebruiken.

Het inzetten van een digitaal middel in fysieke context roept vragen op over de gebruikerservaring en meerwaarde voor de gebruiker. Die is voor een aantal oplossingen nog onduidelijk. Voor de meeste oplossingen is het inzetten van een digitaal middel voor de gebruiker niet makkelijker dan een WID tonen. Het meest voor de hand liggend zijn de oplossingen waarbij de gebruiker gebruik kan maken van een app. Enerzijds omdat dit voor de meest logische user flow zorgt, anderzijds omdat veel mensen niet meer zonder telefoon de deur uit gaan. Een aantal oplossingen zoals iDIN en iDEAL vereisen het gebruik van een hardware token (in zowel fysieke als online context). Het kan niet van de gebruiker verwacht worden dat hij deze standaard bij de hand heeft.

Ook vanuit de winkelier of pakketbezorger zijn er een aantal bezwaren denkbaar. Allereerst zullen de kosten voor een digitaal middel over het algemeen hoger zijn. Voor de leeftijdsverificatie moet namelijk betaald worden terwijl het controleren van een WID in de basis geen extra kosten met zich meebrengt. Het draagvlak onder ondernemers zal onder meer afhankelijk zijn van in hoeverre digitale leeftijdsverificatiemiddelen afgedwongen worden.

Ook vanuit betrouwbaarheid en fraudegevoeligheid zijn er kanttekeningen te plaatsen bij het gebruik van digitale identiteiten in fysieke context. De koppeling tussen de leeftijd en identiteit is minder sterk dan bij een WID, waarbij pasfoto en geboortedatum op hetzelfde document staan. Het zal dus sneller opvallen als iemand een WID van een ander gebruikt ten opzichte van een digitaal middel van een ander. Al is de vraag of dit niet meer moeite kost dan een meerderjarige vriend, kennis of familielid naar de winkel te sturen om de alcohol te kopen of aan te nemen.

Om antwoorden te vinden op bovenstaande vragen en te onderzoeken of het gebruik van digitale middelen in de fysieke wereld meerwaarde biedt, is gebruikersonderzoek nodig.

6.8 SAMENVATTING FYSIEK

De voordelen van het gebruik van digitale middelen in de fysieke context zijn beperkt. Tevens zijn er een aantal punten die verdere aandacht behoeven. Bijvoorbeeld of de winkelier alle geaccepteerde digitale middelen die voldoen aan de eisen voor leeftijdsverificatie moet accepteren of zelf mag kiezen welke hij gebruikt. Digitale middelen brengen wel één groot voordeel met zich mee: de mogelijkheid tot dataminimalisatie waardoor de privacy beter geborgd kan worden. Met een digitaal middel is het mogelijk alleen een 18+-attribuut te ontsluiten, eventueel gecombineerd met een pasfoto. Het gebruik van digitale middelen in fysieke context is van toegevoegde waarde als de winkel of bezorgdienst de kwaliteit van fysieke leeftijdsverificatie op basis van een WID niet kan waarborgen. Het neemt in ieder geval de menselijke maat en daarmee ruimte voor interpretatie weg uit het proces. Deze kwaliteitsborging zou echter ook gerealiseerd moeten kunnen worden door iedereen verplicht een WID te laten tonen bij iedere aankoop of aanname van alcoholische drank. Iets wat volgens de Alcoholwet niet hoeft als de klant onmiskenbaar meerderjarig is. De oplossingen die op moment van schrijven in aanmerking komen om fysiek in te zetten is het inzetten van iDIN met QR-code scan.

Er is (gebruikers)onderzoek nodig om te bepalen of en welke manier van fysieke verificatie het beste werkt. Testomgevingen waarbij zowel webwinkels, als bezorgers als NVWA betrokken zijn, lijken hiervoor wenselijk. Daarnaast is communicatie richting de consument vanuit bijvoorbeeld NIX>18 over nieuwe vormen van identificeren aan de deur nodig om bereidheid en begrip te vergroten.

7 Discussie en conclusie

In dit onderzoek is gekeken naar de mogelijkheden voor leeftijdsverificatie bij de online verkoop van alcoholische dranken. Dit in het kader van de nieuwe Alcoholwet waar strengere eisen gesteld worden rondom de online verkoop van alcoholische dranken. In dit hoofdstuk worden de verschillende onderzoeksvragen bondig beantwoord en wordt afgesloten met een discussie over mogelijke oplossingsrichtingen.

7.1 HUIDIGE OPLOSSINGEN

Welke systemen voor leeftijdsverificatie worden reeds toegepast? Momenteel beperkt dit zich tot systemen waarbij de klant zelf moet aangeven 18 jaar of ouder te zijn. Een enkele partij doet daarnaast een pilot met iDIN. iDIN wordt ook voor andere leeftijdsgebonden diensten gebruikt. Het wordt bijvoorbeeld gebruikt bij online kansspelen. Denk hierbij aan de Nederlandse Loterij[97] en Runnerz[98] (paardenraces). Andere partijen zoals Marktplaats, Bureau Kredietregistratie (BKR) en AEGON gebruiken iDIN tevens voor identiteitsverificatie.

Het aanbod van leeftijdsverificatiesystemen dat in de praktijk toegepast wordt is beperkt. In vergelijking met een vergelijkbaar onderzoek uit 2013[99] is er in dit opzicht weinig veranderd. De belangrijkste vooruitgang is de introductie van iDIN. In de tussentijd is de samenleving steeds verder gedigitaliseerd en zijn er nieuwe mogelijkheden voor digitale identificatie en leeftijdsverificatie, echter blijft het gebruik ervan achter. De vraag is of hier een duidelijke reden voor aan te wijzen is. Wat in ieder geval meespeelt is het kip-ei probleem: Zolang er geen vraag en nog geen noodzaak is, zal de inzet van diensten voor leeftijdsverificatie in de alcoholverkoop tevens beperkt blijven. Inmiddels wordt bij steeds meer diensten waarbij in de fysieke context een leeftijdscontrole noodzakelijk is ook online deze controle wettelijk vastgelegd. Hierdoor zal de markt voor online leeftijdsverificatie naar verwachting meegroeien.

Wat is bekend over de effectiviteit van beschikbare systemen? De uitkomsten van de effectiviteitsanalyse zijn samen te vatten in onderstaand overzicht. De scores zijn indicatief en ook relatief voor de oplossingen ten opzichte van elkaar. In hoofdstuk 4 is de toelichting per systeem te lezen. In onderstaande paragrafen schetsen we de meest voor de hand liggende oplossingsrichtingen gebaseerd op de bevindingen.

Criteria	Zelf toegezegd	ID op Afstand	PDM	Betalen	Consumenten auth	Overheidsauth
Fraudebestendigheid en betrouwbaarheid	--	+/-	+/-	++	++	++
Beschikbaarheid en dekkingsgraad	++	+	--	++	+	++
Gebruiksgemak en begrijpbaarheid	++	-	-	++	+	++
Schaalbaarheid en flexibiliteit	++	-	++	++	++	++
Kosten	++	--	+/-	++	++	++
Realisatietermijn	++	++	-	--	++	--
Toekomtbestendigheid	--	+/-	+/-	++	++	++
Privacy en vertrouwen	++	+/-	++	+/-	+/-	+/-

7.1.1 Zelf toegezegd

De effectiviteit van de 'systemen' waarbij de persoon **zelf toezegging** doet van de leeftijd is slecht, ze zijn namelijk onbetrouwbaar en daarmee niet toekomstbestendig. Wel scoren ze op alle andere criteria goed, ze zijn goedkoop, simpel en makkelijk. Dit is op het moment de huidige minimale oplossing die ge-eist wordt in de Alcoholwet. De lage effectiviteit is mede reden voor het aanpassen van de eisen.

7.1.2 Betaaloplossingen

De betaaloplossingen komen het best uit de bus op het gebied van gebruikersvriendelijkheid. Echter zijn niet alle middelen in deze categorie in de huidige vorm voldoende betrouwbaar voor leeftijdsverificatie. Dit geldt in het bijzonder voor PayPal, gezien er met een willekeurig email adres een PayPal account aangemaakt kan

[97] Zie https://www.nederlandseloterij.nl/speel-bewust
[98] Runnerz richt zich op paardenraces, zie https://runnerz.nl/watisidin
[99] Online leeftijdsverificatie in Nederland – Marktonderzoek, InnoPay (2013)

worden, zonder verdere identificatie. Het gebruik van een creditcard in combinatie met 3D Secure[100] is betrouwbaarder, naast bij de uitgifte van de creditcard een identificatieproces wordt doorlopen biedt dit een extra zekerheid. Het is echter nog steeds alleen een indirecte leeftijdsverificatie. Wanneer iDEAL een leeftijdsattribuut kan aanleveren of een leeftijdsverificatie kan uitvoeren zou dit een ideale combinatie zijn. Het duurt echter nog zeker tot na eind 2022 voordat iDEAL 2.0 geïmplementeerd wordt en er een mogelijke basis is om in leeftijdsverificatie te voorzien. Concreet heeft iDEAL leeftijdsverificatie nog niet op de roadmap.

7.1.3 Overheidsoplossingen

Diverse partijen gaven aan dat als ze mogen kiezen, hun voorkeur uitgaat naar een leeftijdsverificatiesysteem uitgegeven door de overheid. Een aantal gaat hierin nog een stap verder door de verwachting uit te spreken dat de overheid dit daadwerkelijk gaat regelen. Deze verwachtingen vloeien voort uit het feit dat de overheid in fysieke context ook de middelen biedt voor leeftijdsverificatie door het uitgeven van identiteitsbewijzen. Ze verwachten ook dat het gebruik van een overheidsoplossing voor het meeste vertrouwen onder consumenten zorgt. Praktisch gezien ligt het niet voor de hand dat de ondernemers zelf aan zullen sluiten op DigiD, de huidige overheidsoplossing. Dit is momenteel expliciet verboden onder de WABB. Bovendien biedt DigiD op dit moment niet de mogelijkheid tot leeftijdsverificatie, omdat het alleen het BSN teruggeeft. Het is niet de verwachting dat andere relevante concepten zoals de Digitale Bronidentiteit (DBI) of de vID eerder gerealiseerd zullen zijn.

Een alternatief scenario zou kunnen zijn dat een overheidspartij (uitvoerder) een koppeling aan gaat bieden waar webwinkels die online alcohol verkopen op kunnen aansluiten. De klant zou via een uitvoerder bij DigiD kunnen inloggen, waarna deze de leeftijdscheck uitvoert en terugkoppelt aan de webwinkel. Dit lijkt voor de webwinkel een gunstig scenario. Het introduceert echter één centrale overheidspartij die van alle Nederlanders weet waar zij alcohol (proberen te) kopen. Naast praktische bezwaren, is dit dus vanuit privacy oogpunt ook erg onwenselijk. Waar dit in Scandinavische landen de norm is, is dit in de Nederlandse context moeilijk te verantwoorden.

7.1.4 Consumentenoplossingen

Het inzetten van consumentenoplossingen lijkt op dit moment het meest realistische scenario. iDIN scoort gemiddeld positief op de verschillende eisen en randvoorwaarden en gaat ook nergens op onderuit. itsme biedt nu ook de mogelijkheid tot leeftijdsverificatie. Echter is de beschikbaarheid en dekkingsgraad momenteel een stuk lager, omdat itsme nog maar enkele maanden actief is op de Nederlandse markt. Voordeel is dat veel consumentenoplossingen de mogelijkheid bieden een 18+-attribuut te delen, wat de privacy van de gebruiker ten goede komt. De betrouwbaarheid blijft ook in fysieke context hoog. Zeker bij iDIN waar een harde koppeling is gemaakt met het bankaccount, waardoor het minder aantrekkelijk is het authenticatiemiddel uit te lenen.

7.1.5 Personal data wallets

Als gekeken wordt naar belangrijke ontwikkelingen met betrekking op leeftijdsverificatiesystemen dan vallen vooral personal data wallets op. Deze oplossingen bieden de belofte dat de gebruiker meer centraal gesteld wordt en zijn privacy beter geborgd wordt. De recente aankondiging van de Europese Commissie (EC) om lidstaten digital identity wallets uit te laten geven[101], geven deze oplossingen een extra zetje in de rug[102]. Op dit moment is deze categorie nog niet voldoende volwassen en is de dekkingsgraad van de verschillende oplossingen echter nog een probleem. Het tijdspad dat de EC voor ogen heeft en de snelheid van ontwikkelingen de afgelopen jaren, toont aan dat dit nog tenminste 3 jaar duurt.

7.1.6 Identificatie op afstand

IoA oplossingen zijn met name waardevol in processen waar een persoon voor de eerste keer geïdentificeerd moet worden. De identificatie kan met hoge zekerheid worden volbracht wanneer bijvoorbeeld een document wordt uitgelezen, in combinatie met biometrie. Echter moet de persoon veel stappen doen om die identificatie uit te voeren. Daarnaast worden er attributen opgehaald, die niet noodzakelijk zijn voor leeftijdsverificatie. In

[100] 3D Secure is een extra authenticatiefactor voor creditcards. Naast de gegevens op de creditcard moet de gebruiker nog een extra goedkeuring geven, bijvoorbeeld door een wachtwoord en sms-code in te vullen of goedkeuring te geven in een bankieren-app.
[101] Zie ook: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663
[102] Zie ook: https://ibestuur.nl/podium/digitale-identiteit-als-nederlandse-troefkaart-in-europa

het geval van de leeftijdsverificatie voor aankoop van alcohol zijn deze middelen dan ook te zwaar en onderbreken het aankoop proces te sterk.

7.1.7 Fraudetoets

In de fraudetoets zijn verschillende fraudescenario's geanalyseerd. Het risico op fraude is hoog als een volwassene een minderjarige vrijwillig helpt om alcohol te verkrijgen. Deze fraude is helaas lastig te voorkomen en zelfs al is het verboden in de Alcoholwet, is het handhaven lastig. Zwaardere vormen van fraude (als phishing) zijn onwaarschijnlijk in het geval van alcoholverkoop omdat de kosten niet opwegen tot de baten. Andere fraudescenario's met een hoge waarschijnlijkheid in het geval van online leeftijdsverificatie, zoals het gebruik van een nep ID-document of het onvrijwillig gebruik van een identiteitsdocument van een ouder, zijn te mitigeren door bijvoorbeeld betere ID-verificatie software te gebruiken, bijvoorbeeld NFC, of een tweede factor te gebruiken. Daarbij moet de afweging gemaakt worden of deze maatregelen opwegen tegen de andere succesfactoren, zoals privacy, dataminimalisatie, implementatie en gebruiksvriendelijkheid.

7.1.8 18+ accounts

Een **alternatieve oplossingsrichting** is het inrichten van een 18+ account bij de webwinkel. Mits deze oplossing voldoet aan de eisen die VWS aan het leeftijdsverificatiesysteem stelt.

Dit zou er als volgt uit kunnen zien: bij het aanmaken van een account bij de webwinkel doorloopt de klant een verificatieproces (qua betrouwbaarheidsniveau vergelijkbaar aan eIDAS substantieel) waarbij wordt vastgesteld dat de persoon 18+ is. Bij elke online aankoop dient de klant in te loggen, met een authenticatie die typisch tweefactor is, op diens account waardoor de webwinkel weet hoe oud de klant is.

Het uitlenen van accounts is een voordehand liggende manier van fraude. Om deze tegen te gaan, is het nodig om aangemaakte accounts periodiek opnieuw te verifiëren. Bijvoorbeeld elke 30 à 90 dagen.

Deze oplossing zou kunnen voldoen aan artikel 20a van de Alcoholwet: *'het hanteren van een leeftijdsverificatiesysteem op het moment van aankoop'* en artikel 5.1 van de onderliggende AMVB dat stelt dat bij iedere aankoop en voor het sluiten van de verkoopovereenkomst de leeftijd wordt vastgesteld en dat hiervoor een actieve handeling van de klant is vereist. Mits het past binnen de additionele eisen. De klant moet immers voorafgaand aan de koop inloggen op diens 18+ account bij de webwinkel. Lagere kosten en gebruikersvriendelijkheid zijn de sterke punten van deze oplossing. Een dergelijke oplossing is door webwinkel Drankdozijn.nl geïmplementeerd (zie Bijlage E).

7.1.9 Fysieke context

In hoeverre zijn de veelbelovende online oplossingen ook toepasbaar in een fysiek scenario? Een beperkt aantal partijen toont interesse voor het inzetten van digitale middelen voor leeftijdsverificatie in fysieke context. Tot 1 juli voerde PostNL een pilot uit met iDIN. Daarbij was reguliere identificatie het alternatief op het gebruik van IDIN. De eerste resultaten van deze pilot lijken positief. Als groot voordeel wordt genoemd dat een verificatiesysteem de ruimte voor interpretatie van de medewerker wegneemt en zodoende de kwaliteit van de leeftijdsverificatie beter geborgd kan worden. Echter is het digitaal identificeren aan de deur ook nieuw voor mensen en gewenning aan een dergelijke oplossing kost tijd. IDIN is ook inzetbaar in de winkel zelf, bij de kassa of de selfservice balie.

Het gebruik van digitale middelen in fysieke context roept echter ook een aantal vragen op. Moet de leeftijdsverificatie met een digitaal middel ook uitgevoerd worden als iemand overduidelijk meerderjarig is? En mag het gebruik van een digitaal middel door de winkelier of bezorger afgedwongen worden. Onder de huidige Alcoholwet is het antwoord op deze vragen nee. Daarmee lijkt het belangrijkste genoemde voordeel (het wegnemen van ruimte voor interpretatie door de medewerker) te vervallen. Daarnaast is het de vraag of een bezorger of winkelier alle digitale middelen die op grond van de eisen in de algemene maatregel van bestuur toegelaten worden, verplicht moet accepteren. Als dit het geval is zal het ten koste gaan van het draagvlak onder ondernemers. Mag iedere winkelier zelf kiezen welke oplossingen hij accepteert zal dit voor verwarring leiden onder consumenten.

Al met al lijkt het gebruik van het WID in de fysieke context simpelweg praktischer. Het is goedkoper en gebruikersvriendelijker. Hiernaast is de dekkingsgraad van WID erg hoog. Voordelen van digitale middelen zijn

naast het wegnemen van ruimte voor menselijke interpretatie de mogelijkheden voor dataminimalisatie door alleen een 18+-attribuut te delen. Om de verdere meerwaarde van digitale middelen voor leeftijdsverificatie in fysieke context te onderzoeken zijn in ieder geval gebruikersonderzoeken en pilots nodig. Testomgevingen waarbij zowel webwinkels, als bezorgers als de NVWA betrokken zijn, lijken hiervoor wenselijk. Daarnaast is communicatie richting de consument vanuit bijvoorbeeld NIX>18 over nieuwe vormen van identificeren aan de deur nodig om bereidheid en begrip te vergroten.

7.2 CRITERIA

Aan welke criteria moeten systemen voor leeftijdsverificatie voldoen? Er zijn verschillende criteria in kaart gebracht. Een aantal van deze criteria zullen gehanteerd moeten worden als eisen waar dergelijke systemen aan moeten voldoen. Andere zijn randvoorwaardelijk om voor voldoende draagvlak onder ondernemers te zorgen, het vertrouwen van consumenten te borgen en zo online leeftijdsverificatie succesvol te maken.

Vanuit perspectief van **betrouwbaarheid en fraudegevoeligheid** zullen er eisen gesteld moeten worden aan een toekomstig leeftijdsverificatiesysteem. Hiervoor kan het best naar de eIDAS betrouwbaarheidsniveaus gekeken worden. Om fraude bij leeftijdsverificatie tegen te gaan bij de online verkoop van alcoholhoudende dranken is een dienst met een betrouwbaarheidsniveau vergelijkbaar met eIDAS substantieel nodig[103]. De specifieke eisen waar een identificatieoplossing op betrouwbaarheidsniveau substantieel aan moet voldoen zijn vastgelegd in de eIDAS uitvoeringsverordening[104]. Een oplossing op niveau substantieel moet onder andere gebruik maken van tweefactor authenticatie. Daarnaast moet het de oplossing zo ontworpen zijn dat verondersteld kan worden dat het identificatiemiddel slechts kan worden gebruikt door of onder controle van de persoon aan wie het toebehoort. Ook worden er eisen gesteld aan hoe de identiteit bij registratie betrouwbaar vastgesteld moet worden. Bijvoorbeeld op basis van een WID of door gebruik te maken van een middel dat minimaal op hetzelfde betrouwbaarheidsniveau zit. Deze eisen bieden de toezichthouder een kader om oplossingen tegen af te zetten.

Daarnaast dienen er strenge eisen gesteld te worden op het gebied van **privacy, waaronder dataminimalisatie**. Uiteraard dienen oplossingen minimaal te voldoen aan de eisen die door de AVG worden gesteld. Daarnaast, gezien de leeftijd bij iedere aankoop vastgesteld wordt, is het voldoende om alleen een 18+-attribuut uit te wisselen tussen het leeftijdsverificatiesysteem en de webwinkel. Een 18+-attribuut is een verklaring of iemand 18 jaar of ouder is, dat simpelweg met ja of nee beantwoord kan worden. In tegenstelling tot het delen van informatie over de exacte leeftijd of geboortedatum. Dit kan bijvoorbeeld worden omschreven als ‘bij vaststelling van de leeftijd worden niet meer gegevens gedeeld dan noodzakelijk om vast te stellen dat de koper meerderjarig is. Een 18+ verklaring volstaat.’

Een ander aspect van privacy is dat door één systeem te gebruiken, er al snel het risico ontstaat dat de uitgever van het systeem een ‘big-brother’ wordt die weet wie, waar en wanneer alcohol aanschaft. Dit risico kan worden verminderd door te eisen dat het systeem niet mag vastleggen met welke partij het attribuut gedeeld is. Dit kan gerealiseerd worden middels technische inrichting (privacy-by-design) of afspraken (de partij weet dit in principe wel, maar er wordt afgesproken dat er niet wordt opgeslagen dat er een verificatie heeft plaatsgevonden).

Een aantal van de criteria zijn wel belangrijk voor webwinkels bij het beslissen om een systeem aan te schaffen, maar niet noodzakelijk om als specifieke eisen vast te leggen door het ministerie van VWS. Tenzij het ministerie van VWS besluit zelf specifieke systemen aan te wijzen. Dit geldt voor **gebruiksgemak, schaalbaarheid, dekkingsgraad en toekomstbestendigheid**. Deze criteria zijn relevant om te beoordelen of een oplossing op korte en lange termijn werkbaar is. Vanuit de interviews onder ondernemers komt bijvoorbeeld naar voren dat gebruikersvriendelijkheid hoog moet zijn. Voor webwinkels is conversie namelijk zeer belangrijk. De userflow moet zo min mogelijk verstoord worden. Idealiter zou de leeftijdsverificatie onderdeel zijn van het betaalproces. Andere oplossingen zijn altijd minder gebruikersvriendelijk. Overigens komt deze

[103] Op basis van de handreiking betrouwbaarheidsniveaus van Forum Standaardisatie, beschikbaar via https://www.forumstandaardisatie.nl/publicaties
[104] Uitvoeringsverordening 2015/1502, beschikbaar via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502

klantvriendelijkheid ook bij een leeftijdsverificatie in fysieke context in het geding. Om 18+ verificatie effectief uit te voeren is een verstoring van de userflow in beide contexten onontkoombaar.

Kosten zijn minder belangrijk als criteria vast te leggen. Webwinkels verwachten (en zijn bereid) om per verificatie een fee te moeten betalen. Dit is een bekende methode die ook gebruikt wordt voor het afhandelen van betalingen. Dit zal betekenen dat online aanschaf van alcohol iets duurder wordt voor de klant. De kosten moeten wel realistisch en uitlegbaar zijn.

Tot slot is goede **handhaving** een randvoorwaarde die niet benoemd is in de criteria, maar wel noodzakelijk voor succes. Bevraagde partijen hebber er begrip voor dat er een vorm van online leeftijdsverificatie nodig is, er moet echter wel een eerlijk speelveld zijn. Onder de oude Drank- en Horecawet was handhaving van de verkoop van alcohol op afstand lokaal georganiseerd. Verkoop van alcohol op afstand gaat echter over gemeentegrenzen heen. Hiernaast was toezicht bij de uitlevering (aan de voordeur) niet goed uitvoerbaar, omdat gemeentes geen zicht hebben op waar en wanneer bezorgd wordt. Hierdoor werd er door de gemeentes nauwelijks op gehandhaafd en werd er nauwelijks opgetreden tegen partijen die zich niet aan de regels hielden bij de verkoop van alcohol op afstand. Om het **draagvlak** onder ondernemers te behouden zal er gehandhaafd moeten worden op ondernemers die zich niet aan de nieuwe Alcoholwet houden. Met de NVWA als centrale toezichthouder die over gemeentegrenzen heen kan opereren zal dit makkelijker zijn. Tevens heeft de NVWA per 1 juli 2021 meer instrumenten om de verkoop van alcohol op afstand te handhaven. Er zal minder nadruk komen op handhaving bij uitlevering, maar meer op de leeftijdsverificatie bij aankoop en de geborgde werkwijze.

Hiernaast wordt door ondernemers verwacht dat het gebruik van een toekomstig leeftijdsverificatiesysteem vragen of zelfs weerstand op zal roepen bij consumenten. Een publiekscampagne vanuit de overheid, bijvoorbeeld vanuit NIX18, over het invoeren van het leeftijdsverificatiesysteem wordt daarom als een essentiële succesfactor gezien om het begrip bij de consument te waarborgen. Dit is nodig om te zorgen dat de consument bereid is om de leeftijdsverificatie uit te voeren.

7.3 TOEKOMSTPERSPECTIEF

Het is de vraag of het verstandig is om te wachten op de verdere doorontwikkeling van initiatieven als de Digitale Bron Identiteit en de EU digital identity wallet. Gezien de geringe voortgang sinds het rapport over leeftijdsverificatie uit 2013, kan het nog lang wachten zijn tot de ideale oplossing gerealiseerd is.

Om op korte termijn vooruitgang te creëren op het vlak van leeftijdsverificatie voor de aankoop van alcohol, is een pragmatische insteek geboden. Blijf niet wachten tot er één optimale oplossing is, die zal er waarschijnlijk nooit komen en vooral niet als er geen vraag naar is. Ga aan de slag met de oplossingen die er al wel zijn. Wijs deze eventueel aan maar sluit het inzetten van andere oplossingen niet uit. Het vaststellen van eisen waar dergelijke leeftijdsverificatiesystemen aan moeten voldoen is dus wenselijk. Als onderdeel van de eisen moet minimaal het vereiste betrouwbaarheidsniveau opgenomen worden en eisen worden gesteld op het vlak privacy inclusief dataminimalisatie.

Daarnaast is het van belang dat het ministerie van VWS duidelijk communiceert wanneer de sector betrouwbare oplossingen voor leeftijdsverificatie moet implementeren en welke extra handelingen dit betekent wanneer een persoon online alcohol wil aankopen. Dit creëert duidelijkheid. Niet alleen voor de webwinkels, maar ook voor de leveranciers van oplossingen en burgers.

8 Bijlage A: Begrippenlijst

Begrip	Uitleg
18+ attribuut	Een 18+-attribuut is een verklaring of iemand 18 jaar of ouder is, dat simpelweg met ja of nee beantwoord kan worden. Er wordt hierbij geen informatie over de exacte leeftijd of geboortedatum onthuld.
Anoniem (of: geanonimiseerd)	Niet traceerbaar naar de persoon.
Attribuut	Een attribuut is een digitale verklaring dat iemand iets is of bezit. Denk hierbij aan een naam attribuut die iemands volledige naam bevat.
Authenticatie	Authenticatie is de techniek waarmee een systeem kan vaststellen wie een gebruiker is (https://www.ncsc.nl/onderwerpen/authenticatie). Dit gebeurt met behulp van één of meerdere authenticatiefactoren. Denk bijvoorbeeld aan een gebruikersnaam en wachtwoord. Om een gebruiker te authentiseren moet hij/zij in een eerder stadium al een keer geïdentificeerd zijn.
Authenticatiefactor	Bij authenticatie worden vaak twee factor authenticatie gebruikt. Authenticatie factoren kunnen zijn: iets wat iemand bezit (bijvoorbeeld een identiteitsdocument of een telefoon met een speciale app), iets wat iemand weet (bijvoorbeeld een wachtwoord of code) en iets wat iemand is (bijvoorbeeld een gezicht of vingerafdruk).
Autoritatieve bron	Gezaghebbende, erkende bron van gevalideerde (persoons)gegevens.
Big brother	Het big brother begrip wordt gebruikt om aan te geven dat een organisatie of persoon vergaand toezicht heeft op het (digitale) leven van iemand.
Blockchain	Een specifieke implementatie van een distributed ledger technologie, waarin data in blokken in een ketting vorm op een ledger gezet worden, waardoor ze hun chronologische volgorde houden.
BRP	Het Basisregistratie Personen (BRP) bevat persoonsgegevens van inwoners van Nederland en personen die Nederland hebben verlaten. De gemeentes houden deze informatie bij in het BRP.
Consent	Het geven van geïnformeerde toestemming. Zie ook het begrip toestemming.
Data aanbieder	Verzameld en verwerkt persoonlijke data die de andere partijen (data afnemers) mogelijk willen inzien of gebruiken om een dienst aan te bieden.
Data afnemer	Partij die data in wil zien of gebruiken van een of meerdere data aanbieders om een dienst aan te bieden. Bijvoorbeeld een webwinkel.
Decentralized Identifiers (DID)	Een Decentralized Identifier (DID) is een digitaal adres waar naar verwezen kan worden (bijvoorbeeld een URL zoals www.rijksoverheid.nl) die een belangrijke rol speelt in het decentrale internet. DIDs worden vaak gebruikt bij SSI oplossingen (maar zijn hiervoor geen vereiste). Vaak wordt er gerefereerd aan de W3C documentatie voor DIDs, zie ook https://www.w3.org/TR/did-core/
Digitale bronidentiteit (DBI)	Zie sectie 4.3.2.
eIDAS	eIDAS is een Europese verordening en staat voor 'Electronic Identities And Trust Services'. De Europese lidstaten hebben met eIDAS afspraken gemaakt om dezelfde betrouwbaarheidsniveaus, begrippen en onderlinge digitale infrastructuur te gebruiken. Onder de eIDAS-verordening is het mogelijk om met een nationale digitale identiteit in te loggen bij digitale diensten in een andere lidstaat.

Holder verification	Holder verification is het verifiëren dat degene die bijvoorbeeld een identiteitsdocument aanbiedt, ook de rechtmatige eigenaar van dat identiteitsdocument is. Bijvoorbeeld door te controleren of de pasfoto op het identiteitsdocument overeenkomt met de persoon die het document aanbiedt. Holder verification kan uitgevoerd worden als onderdeel van identificatie.
Identificatie	Identificatie is het vaststellen van de identiteit. Gebruikelijk vindt tijdens identificatie ook verificatie plaats om te controleren of de geclaimde identiteit klopt. Bijvoorbeeld in de vorm van holder verification.
Identificeren op Afstand (IoA)	Oplossing gericht op het op afstand identificeren van een consument. Zie ook sectie 3.6.
Identiteitsprovider	Een identiteitsprovider (IdP) is een partij die gebruikers identificeert en vervolgens de digitale identiteiten van gebruikers beheert. Een IdP levert een authenticatiedienst aan data-afnemers (bijv. een webwinkel). Een gebruiker kan door zich te authentiseren bij de IdP toegang krijgen tot de dienst van data-afnemer. Hij identificeert zich op die manier bij de data-afnemer. Voorbeelden zijn inloggen met Digid, iDIN, IRMA en Google.
Interoperabiliteit	Digitale systemen zijn interoperabel als ze kunnen samenwerken of kunnen communiceren zonder problemen en beperkingen.
Know-Your-Costumer (KYC)	Know-Your-Costumer (KYC), ofwel ken je klant, is een term die wordt gebruikt om aan te geven dat bedrijven bekend zijn met welke klanten er van hun systeem gebruik maken (bijvoorbeeld door middel van identificatie). KYC speelt een belangrijke rol bij de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).
Leeftijdsverificatie	Het controleren dat degene die een bestelling wil plaatsen de benodigde leeftijd heeft bereikt. Bijvoorbeeld door een leeftijdsvraag te stellen of de leeftijd op te vragen bij een identiteitsprovider.
Liveness detectie	Het detecteren van of iemand ‘live’ aanwezig is en dat er geen gebruik gemaakt wordt van bijvoorbeeld een foto of een masker.
NFC	Bij Near Field Communication (NFC) is het mogelijk om op korte afstand, maximaal enkele centimeters, contactloos een chip of apparaat uit te lezen of er mee te communiceren. Naast het gebruik in identiteitsbewijzen wordt het ook gebruikt voor contactloos betalen en reizen met de OV-chipkaart. Ook veel moderne smartphones ondersteunen NFC, waardoor er bijvoorbeeld tegenwoordig met een smartphone contactloos betaald kan worden.
OCR	Met Optical Character Recognition (OCR) is het mogelijk om geautomatiseerd karakters, letters en cijfers op een foto te herkennen. Dit wordt onder andere gebruikt bij identiteitsdocumenten, maar wordt ook toegepast door bijvoorbeeld Google Maps om nummerborden van auto's onzichtbaar te maken.
Open source	Open Source computersoftware is software die onder een licentie is vrijgegeven waardoor iedereen de software kan bekijken, aanpassen en delen.
Open standaarden	Een open standaard is een standaard die publiek toegankelijk is. Hierdoor kan iedereen de standaard gebruiken en toepassen. Er zijn bijvoorbeeld veel open standaarden beschikbaar om het "internetten" en e-mailen mogelijk te maken.
Personal data wallet	Dienst die het mogelijk maakt voor het individu om veilig zijn of haar eigen persoonlijke data in te zien, op te halen en te delen. Daarnaast maakt de operator het mogelijk om de uitwisseling van persoonlijke data met en tussen data aanbieders en afnemers te controleren.

Persoon	Natuurlijk persoon. Binnen context van PDM: degene die regie op zijn of haar gegevens wil voeren.
Persoonlijk Data Management (PDM)	Het concept rond het duurzaam beheren en onderhouden van persoonlijke data. Zie ook sectie 3.5.
Self Sovereign Identity (SSI)	Self-sovereign identity (SSI) is een vorm van personal datamanagement (PDM) waarin de gebruiker geheel de controle heeft. In de standaard architectuur van SSI haalt de gebruiker zelf zijn data op bij een data aanbieder (bijvoorbeeld DigiD of Google) en slaat deze zelf op (op bijvoorbeeld zijn mobiel of zijn eigen cloud). De gebruiker kan er vervolgens voor kiezen zijn data, of slechts een deel daarvan, te delen met andere partijen (data afnemer). De data aanbieder is op dat moment niet meer betrokken en toch kan de data afnemer zekerzijn van de echtheid van de data. Zie ook hoofdstuk 4.6.
Toestemming	Twee van de eisen die de AVG stelt aan 'toestemming' zijn dat deze 'geïnformeerd' en 'specifiek' gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat men kan laten zien op basis van welke informatie de betrokken persoon de toestemming heeft gegeven. Het is dus onvoldoende om alleen de toestemming zelf vast te leggen.
Verifiable Credentials (VC)	Verifiable credentials (VC) zijn digitale gegevens, die geverifieerd kunnen worden doordat ze van digitale echtheidskenmerken zijn voorzien. VCs worden vaak gebruikt bij SSI oplossingen (maar zijn hiervoor geen vereiste). Vaak wordt er gerefereerd aan de W3C documentatie voor VCs, zie ook https://www.w3.org/TR/vc-data-model/
WID	Een Wettelijk identificatiedocument (WID) is een origineel en geldig identiteitsbewijs, zoals paspoort, identiteitsbewijs, rijbewijs of een vreemdelingsdocument zoals vastgelegd in de Wet op de identificatieplicht.

9 Bijlage B: Vragenlijst stakeholders

Huidige situatie:

- Hebben jullie processen voor leeftijdsverificatie?
    - Online op moment van aankoop (18+ vinkje vs. geboortedatum)?
    - Bij bezorging?
    - Wat zijn de ervaringen met dit systeem?

Ideale oplossing:

- Hebben jullie overwogen hoe jullie systeem er in de toekomst uit zou moeten zien?
- Hoe staan jullie tegenover de toekomstige oplossing waarbij voor elke aankoop de leeftijd vastgesteld moet worden?
- Geven jullie de voorkeur aan één oplossing die door veel mensen gebruikt kan worden of een solution provider die meerdere oplossingen voor jullie aanbiedt? (Denk aan online betaling waarbij persoon zelf de betaalmethode selecteert)

Fraudebestendigheid en betrouwbaarheid

- In hoeverre is fraudebestendigheid voor jullie van belang?
- Voldoen jullie bij voorkeur aan wat (wettelijk) minimaal noodzakelijk is? Of zijn er extra maatregelen die jullie zelf willen treffen?

Beschikbaarheid en dekkingsgraad:

- Is jullie organisatie bereid om een oplossing mee te ontwikkelen als dit nodig zou zijn? (meedoen in pilot e.d.)
- Geven jullie de voorkeur aan inkopen van een bestaande oplossing?
- Voorkeur voor zelf integreren of via digital identity service provider/integrator?
- Hoe groot moet de groep Nederlanders ongeveer zijn die een oplossing gebruikt voordat jullie overwegen de oplossing in te zetten?

Gebruiksgemak en begrijpbaarheid:

- Belang van adoptie onder gebruikers?
    - Gebruikers kunnen het direct gebruiken
    - Gebruikers moeten eenmalig registreren
- Hoe belangrijk is het voor jullie dat het een oplossing is die al (grotendeels) bekend is onder Nederlanders?

Schaalbaarheid en flexibiliteit:

- Hoe belangrijk is het dat een oplossing door veel gebruikers gebruikt kan worden?
- Hoe belangrijk is het voor jullie dat de oplossing grote volumes aankan?
- Is het voor jullie belangrijk dat de oplossing ook in andere context ingezet kan worden? (Bijv. zowel fysiek als online, of in andere processen waar 18+ verificatie een rol speelt.)

Kosten

- Wat zouden de kosten ongeveer mogen zijn?
    - Voor de implementatie?
    - Per verificatie/aankoop?
- Voorkeur voor kostenmodel? (i.e. Pay-per-use, vs pay-per-user, subscription)

Realisatietermijn

- Staat het implementeren van een nieuwe oplossing al op jullie roadmap?
    - Hoe snel moet een oplossing te integreren zijn?
- Zien jullie wettelijke belemmeringen?

Privacy en veiligheid:

- Welke gegevens willen jullie ontvangen?
- Geven jullie de voorkeur aan geboortedatum of een 18+ bevestiging en naam?

Zijn er nog andere factoren belangrijk bij de overweging van de inzet van een leeftijdsverificatiesysteem? (Top 3?)

Zijn jullie bekend met/wat is jullie mening t.o.v. bestaande oplossingen?

- Overheidsoplossingen
- Bankenoplossing
- SSI met afgeleid attribuut
- Identiteit-afsprakenstelsel (zoals eHerkenning of middelen toegelaten onder wetDO)
- Certificering (bijvoorbeeld bepaald eIDAS betrouwbaarheidsniveau, of speciale certificering voor oplossingen die gebruikt mogen worden voor leeftijdsverificatie).

10 Bijlage C: Uitkomsten interviews

Gedurende de sessies met de begeleidingscommissie en de interviews met stakeholders kwamen diverse thema's naar boven. Deze thema's waren niet allen direct gerelateerd waren aan de criteria zoals geformuleerd in de beoordeling van de verschillende identificatie systemen, maar wel relevant voor webwinkels en wetgever bij de implementatie van de Alcoholwet. Onderstaande paragrafen vatten de belangrijkste discussies samen.

10.1 18+ ACCOUNT

Een veelgehoorde wens van de stakeholders was de mogelijkheid om een 'geverifieerde account' toe te staan. De propositie is om klanten een account te laten aanmaken bij de webwinkel. Deze account kan vervolgens een '18+ account' worden, door de klant zich eenmalig te laten identificeren. Vervolgens kan de klant door in te loggen in de account aankopen doen. De redenering van de webwinkels is dat dit het makkelijker maakt om herhaald aankopen te doen en goedkoper is.

De keerzijde van een 18+ account is het risico dat een account eenmalig wordt geverifieerd door iemand van 18+, en de jongere vervolgens alsnog alcohol kan bestellen. Daarnaast kan dit mogelijk een 'handel' in 18+ accounts stimuleren. Daarnaast vereist de nieuwe wetgeving simpelweg dat de verificatie per aankoop plaatsvindt. Niet eenmalig per webwinkel of winkel.

Ter vergelijking: in Zweden en Noorwegen moet de klant ook een account aanmaken. Zonder account is het niet mogelijk om Alcohol te bestellen. Het verschil in deze landen is dat er bij elke aankoop betaald moet worden met BankID, een betaalmiddel waar ook leeftijdsverificatie mee uitgevoerd wordt. Daarnaast wordt alcoholverkoop door de overheid verzorgd.

10.2 BUSINESSMODEL

Het antwoord op de vraag welk businessmodel de voorkeur heeft was vrij eenduidig. Webwinkels verwachten (en zijn bereid) om per verificatie een kleine fee te moeten betalen. Dit is een bekende methode die ook gebruikt wordt voor betalingen. Deze fee zal ook in dit geval doorberekend worden aan de klant. Wat betekent dat het online bestellen van alcohol duurder zal worden voor de eindklant.

Er is verschil in bereidheid om nieuwe systemen te piloten en implementeren. Voor marktpartijen met grotere budgetten is dit een mogelijkheid. Echter heeft het zeker voor individuele slijters de voorkeur om een 'off-the-shelf' oplossing in te kopen, zoals dit ook mogelijk is voor betaalmiddelen. Het aanbod aan off-the-shelf oplossingen is nog beperkt. Dit maakt het duur om leeftijdsverificatie simpel te implementeren.

10.3 INTERNATIONALE VERKOOP

Een thema dat vragen oproept bij de stakeholders is verkoop aan internationale klanten. Zo'n 10 tot 15 procent van de inkomsten komen vanuit buitenlandse bestellingen. In hoeverre gelden de lokale of internationale regels als het gaat om identificatie? Hiervoor verwijzen we naar de verordening Geoblocking vanuit de Europese Commissie. Het basisprincipe van de verordening luidt:

'Een handelaar past geen verschillende algemene toegangsvoorwaarden tot zijn goederen of diensten toe om redenen die verband houden met de nationaliteit, de verblijfplaats of de plaats van vestiging van de klant.'

Deze verordening doet vermoeden dat internationale kopers ook moeten voldoen aan een 18+ check. Echter wordt in de nieuwe wetswijziging gesteld dat deze geldt voor:

'*verkoop op afstand waarbij een verkoopovereenkomst wordt afgesloten tussen degene die bedrijfsmatig of anders dan om niet alcoholhoudende drank verkoopt en een particulier die zich beiden in Nederland bevinden'.*

Dit zal in praktijk betekenen dat het verkrijgen van alcohol in Nederland via webwinkel voor kopers in het buitenland makkelijker is dan voor kopers in Nederland. Andersom geldt ook dat het makkelijker zal worden

om drank te bestellen bij een buitenlandse webwinkel dan bij een Nederlandse. Om te kijken of dit geen te groot marktverstorend effect heeft, heeft VWS al een nulmeting laten uitvoeren[105].

Een aantal van de geïnterviewden gaf aan dat een gedeelte van hun klanten bestaat uit buitenlanders die zich voor kortere of langere tijd in Nederland bevinden. De zorg bestaat dat als er een leeftijdsverificatiesysteem gekozen wordt dat alleen beschikbaar is voor Nederlanders, deze groep klanten buiten de boot zal vallen.

Internationaal opererende partijen geven sowieso aan de voorkeur een leeftijdsverificatiesysteem dat grens overstijgend inzetbaar is. Dit hoeft overigens niet specifiek één middel te zijn, maar mag ook een service provider zijn die verschillende systemen via één platform naast elkaar aanbiedt en waarbij de consument de oplossing van zijn of haar voorkeur kan kiezen.

10.4 TOEKOMSTBESTENDIGHEID

Een ander belangrijk thema voor de stakeholder is toekomstbestendigheid. Er is een zorg dat wanneer systemen in 2021 geïmplementeerd moeten worden, er mogelijk nog een keer kosten gemaakt moeten worden in de nabije toekomst. Met name zodra er op nieuwe mogelijkheden voor verificatie ontstaan. Hierbij wordt met name verwezen naar de Digitale Bronidentiteit en vID die in ontwikkeling zijn binnen de overheid. Niet alleen de ontwikkeling van oplossingen door de overheid is roept zorgen op. Stakeholders vragen zich ook af wat de impact is van de ontwikkeling van een 18+ verificatie door een grotere marktpartij, die mogelijk de markt aan ID-oplossingen zou overnemen.

10.5 DRAAGVLAK

Vanuit de interviews onder ondernemers komt bijvoorbeeld naar voren dat gebruikersvriendelijkheid hoog moet zijn. Voor webwinkels in conversie namelijk zeer belangrijk. De userflow moet zo min mogelijk verstoord worden. Idealiter zou de leeftijdsverificatie onderdeel zijn van het betaalproces.

Wanneer we naar het brede draagvlak voor leeftijdsverificatie systemen vragen, geven de partijen aan voorkeur te hebben dat er één middel wordt voorgeschreven. Daarbij wordt voorkeur uitgesproken voor een overheidsmiddel. Daarnaast wordt ook de voorkeur gegeven aan een betaalmiddel waar ook leeftijd mee geverifieerd kan worden, gezien de klant dan niet uit het bestelproces wordt gehaald. Het (verplicht) moeten werken met een breder scala aan mogelijke middelen heeft minder voorkeur. Zeker in de situatie waar deze allen verplicht geaccepteerd moet worden.

Beide opties, inzetten van een overheidsmiddel en het inzetten van een betaalmiddel met verificatie, zijn in Nederland op dit moment echter geen mogelijkheid. DigiD mag niet door private organisaties ingezet worden. Betaalmiddelen hebben (op dit moment) nog beperkt de mogelijkheid om een 18+ attribuut te leveren.

Tot slot geeft een aantal partijen aan dat het ook belangrijk is dat de overheid duidelijk achter de wet gaat staan. Allereerst wordt aangegeven dat handhaving van de nieuwe wet belangrijk is. Zo zijn er naar verluid momenteel meerdere online drankhandels die officieel geen slijtersvergunning hebben en daarmee tussen de regels in opereren. De leeftijdsverificatie brengt extra kosten met zich mee voor de webwinkel en heeft mogelijk een negatief effect op de conversie. Om een eerlijk speelveld te behouden is het belangrijk dat alle partijen daadwerkelijk de leeftijdsverificatie uitvoeren. Om te zorgen dat dit gebeurt roepen meerdere partijen op tot goede handhaving.

Hiernaast wordt door ondernemers verwacht dat het gebruik van een toekomstig leeftijdsverificatiesysteem vragen of zelfs weerstand op zal roepen bij consumenten. Een publiekscampagne vanuit de overheid, bijvoorbeeld vanuit NIX18, over het invoeren van het leeftijdsverificatiesysteem wordt daarom als een essentiële succesfactor gezien.

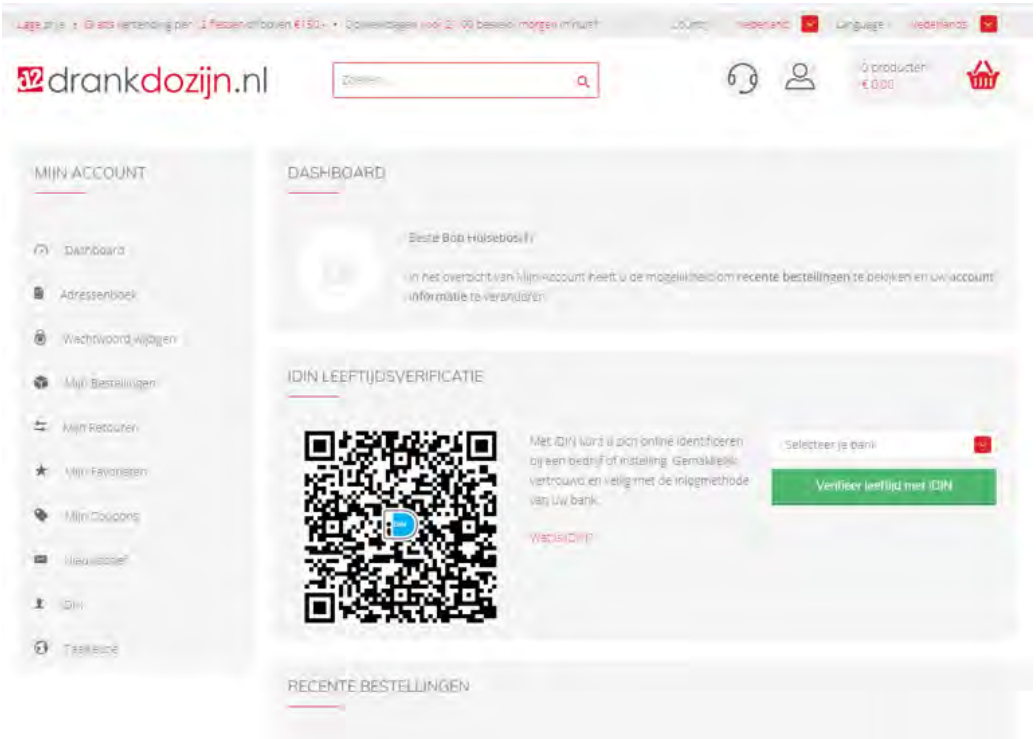
[105] 'Alcoholverkoop op afstand – onderzoeksverslag' – Ecorys i.o.v. VWS (2020), beschikbaar via https://www.ecorys.com/sites/default/files/2021-05/alcohol-verkoop-op-afstand.pdf

11 Bijlage D: Analysetabellen

Criteria	Zelf toegezegd	ID op Afstand	PDM	Betalen	Consumenten auth	Overheidsauth
Fraudebestendigheid en betrouwbaarheid	--	+/-	+/-	++	++	++
Beschikbaarheid en dekkingsgraad	++	+	--	++	+	++
Gebruiksgemak en begrijpbaarheid	++	-	+	++	+	+
Schaalbaarheid en flexibiliteit	++	-	++	++	++	++
Kosten	++	--	+	++	++	++
Realisatietermijn	++	++	-	--	++	--
Toekomtbestendigheid	--	+	+	++	++	++
Privacy en vertrouwen	++	+/-	+/-	+/-	+	+/-
Criteria	**Zelf toegezegd**	**Vinkje**	**Telefonisch**			
Fraudebestendigheid en betrouwbaarheid	--	--	--			
Beschikbaarheid en dekkingsgraad	++	++	++			
Gebruiksgemak en begrijpbaarheid	++	++	++			
Schaalbaarheid en flexibiliteit	++	++	--			
Kosten	++	++	--			
Realisatietermijn	++	++	++			
Toekomtbestendigheid	--	--	--			
Privacy en vertrouwen	++	++	++			
Criteria	**Wallets**	**IRMA**	**IDA**			
Fraudebestendigheid en betrouwbaarheid	+/-	+/-	+/-			
Beschikbaarheid en dekkingsgraad	--	-	-			
Gebruiksgemak en begrijpbaarheid	+	+	+			
Schaalbaarheid en flexibiliteit	++	++	++			
Kosten	+	+	+			
Realisatietermijn	-	+/-	+/-			
Toekomtbestendigheid	+	+	+			
Privacy en vertrouwen	+/-	+/-	+/-			
Criteria	**ID op Afstand**	**Video bellen +**	**OCR**	**OCR + b**	**NFC**	**NFC + b**
Fraudebestendigheid en betrouwbaarheid	+/-	-	--	+	+/-	++
Beschikbaarheid en dekkingsgraad	+	++	++	++	+	+
Gebruiksgemak en begrijpbaarheid	-	-	+/-	-	-	--
Schaalbaarheid en flexibiliteit	-	--	+/-	+/-	++	++
Kosten	--	--	-	--	--	--
Realisatietermijn	++	++	++	++	++	++
Toekomtbestendigheid	+	+/-	--	-	+	++
Privacy en vertrouwen	+/-	-	-	-	-	-
Criteria	**Betalen**	**iDeal**	**Creditcard**	**Paypal**		
Fraudebestendigheid en betrouwbaarheid	++	++	--	--		
Beschikbaarheid en dekkingsgraad	++	++	+/-	+		
Gebruiksgemak en begrijpbaarheid	++	++	+	++		
Schaalbaarheid en flexibiliteit	++	+	+	+		
Kosten	++	++	++	+		
Realisatietermijn	--	--	+	-		
Toekomtbestendigheid	++	++	+	++		
Privacy en vertrouwen	+/-	++	+	++		
Criteria	**Consumenten**	**Itsme**	**iDIN**			
Fraudebestendigheid en betrouwbaarheid	++	++	++			
Beschikbaarheid en dekkingsgraad	+	-	++			
Gebruiksgemak en begrijpbaarheid	+	+	+			
Schaalbaarheid en flexibiliteit	++	++	++			
Kosten	++	+	+			
Realisatietermijn	++	+	++			
Toekomtbestendigheid	++	+/-	++			
Privacy en vertrouwen	+	+/-	++			
Criteria	**Overheid**	**DigiD**				
Fraudebestendigheid en betrouwbaarheid	++	++				
Beschikbaarheid en dekkingsgraad	++	++				
Gebruiksgemak en begrijpbaarheid	+	++				
Schaalbaarheid en flexibiliteit	++	++				
Kosten	++	++				
Realisatietermijn	--	--				
Toekomtbestendigheid	++	++				
Privacy en vertrouwen	+/-	+/-				

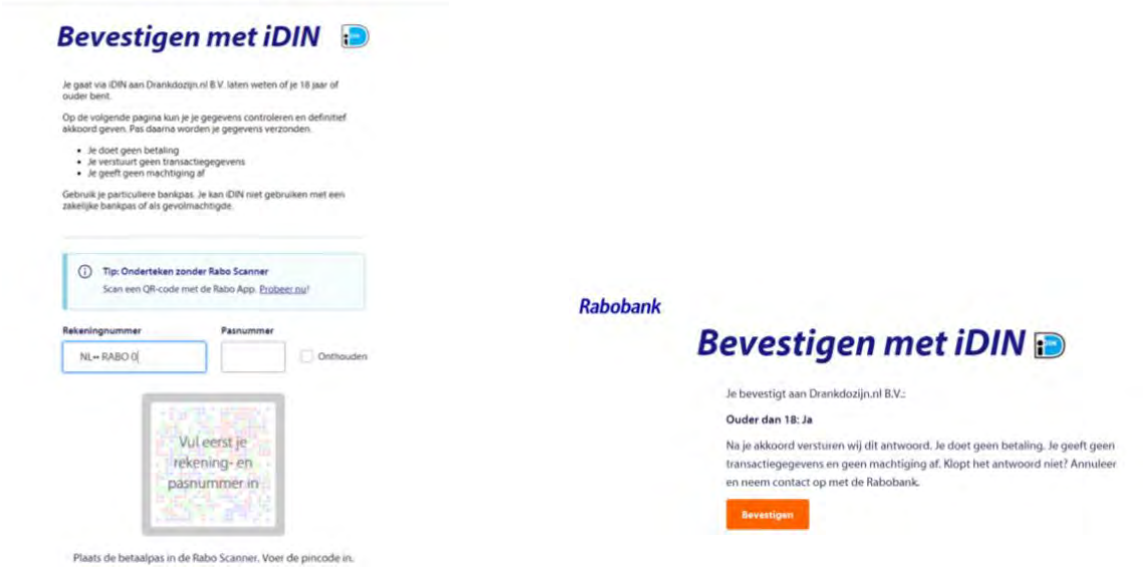
12 Bijlage E: Voorbeeld Drankdozijn

De inzetbaarheid van de verschillende oplossingen voor leeftijdsverificatie kan op manieren. De eenvoudigste manier is de verificatie plaats te laten vinden direct voorafgaand aan of tijdens de betaling. Het nadeel van deze manier is dat een derde partij bij iedere online aanschaf de leeftijd van de klant controleert. Dit is niet heel gebruikersvriendelijk en brengt kosten met zich mee. Een andere use-case betreft de klant een account te laten aanmaken bij de webwinkel en tijdens dat proces eenmalig een leeftijdsverificatie uit te voeren. De webwinkel weet vervolgens zodra de klant inlogt om een aankoop te doen of deze ouder dan 18 jaar is. Lagere kosten en gebruikersvriendelijkheid zijn de sterke punten van deze use-case. Bestellen als 'gast' is hierdoor echter niet meer mogelijk, tenzij daarvoor een aparte verificatie wordt uitgevoerd. Een dergelijke oplossing is door webwinkel Drankdozijn.nl geïmplementeerd. Nadat de klant is ingelogd kan met iDIN het account worden opgewaardeerd met een leeftijdsverificatie (zie Figuur 1).



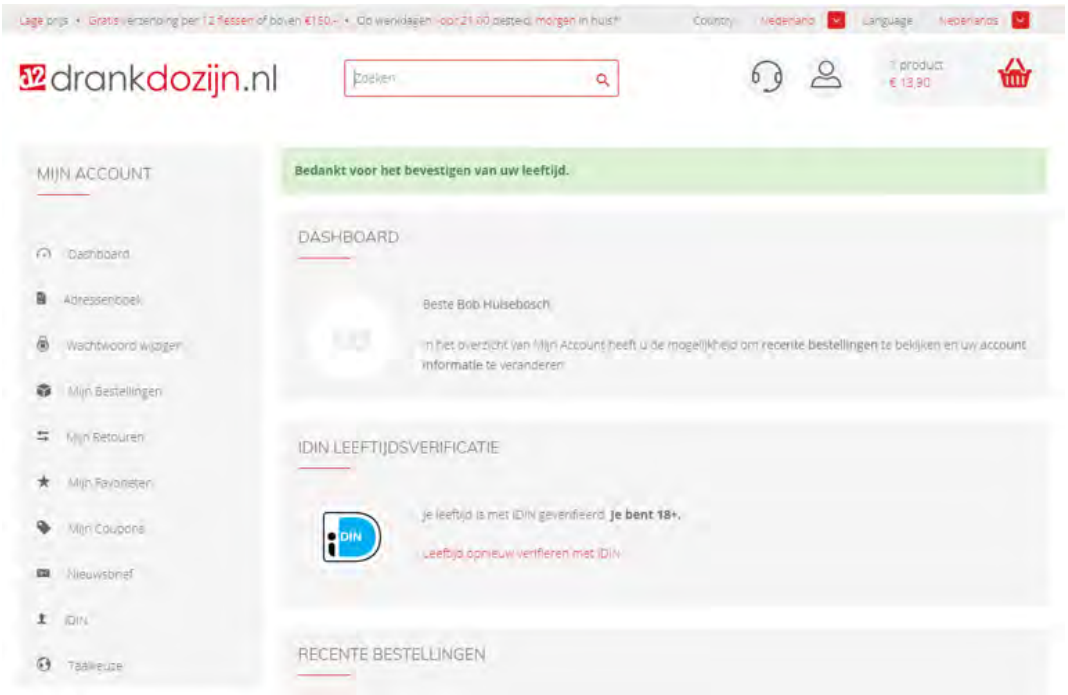
Figuur 1: Opwaarderen van een account met iDIN leeftijdsverificatie.

Voor de iDIN-sessie dient selecteer de klant zijn bank en voert een bankauthenticatie uit (zie Figuur 2). Conform de AVG vraagt iDIN toestemming aan de klant om leeftijdsgegevens te mogen delen met Drankdozijn.nl.



Figuur 2: Leeftijd bevestigen met iDIN.

Vervolgens ziet de klant in de mijn-omgeving van Drankdozijn.nl dat zijn/haar leeftijd is gecontroleerd (54).



Figuur 3: Account met geverifieerde leeftijd.

Vervolgens kan de klant alcohol bestellen en afrekenen.