1 Introductie

Vanuit de expertgroep normenkaders Elektronische Toegangsdiensten (ETD) worden de betrouwbaarheidseisen onderzocht waaronder de eisen voor ‘registratie en verstrekking op afstand’ ten behoeve van authenticatiemiddelen op niveau Substantieel (LoA3) en Hoog (LoA3). Vanuit dit onderzoek zijn ondermeer de mechanismen bekeken zoals die zijn toegestaan in Duitsland ([BAFIN]) en in het Verenigd Koninkrijk [GPG45].

Het is niet eenvoudig om beheersdoelstellingen voor een ‘registratie en verstrekking op afstand’ proces te beschrijven. Deze complexiteit komt mede doordat de onderdelen binnen een dergelijk proces communicerende vaten zijn: een zwakheid in één onderdeel kan worden gemitigeerd met een versterking in een ander onderdeel.

Daarom is vanuit de expertgroep normenkaders gekozen om als eerste stap, concrete implementatie voorbeelden te beschrijven. Bij dergelijke voorbeelden worden dan concrete keuzen gemaakt die betrouwbaarheidsvoordelen opleveren die als ‘voldoende’ kunnen worden bestempeld. Dit levert direct soelaas voor authenticatiediensten en dienstverleners die snel aan de slag willen. Om vervolgens meer toegestane implementaties van ‘registratie en verstrekking op afstand’ toe te kunnen staan, kunnen als tweede stap betrouwbaarheidseisen worden geabstraheerd vanuit de opgestelde voorbeelden. Door hun rol zijn de voorbeelden tamelijk conservatief in acceptatie van risico’s en nemen zij feitelijk de vorm van een ‘good practice’ aan.

Deze ‘best practice’ beschrijft drie implementatie varianten van ‘registratie en verstrekking op afstand’. Het betreft alleen authenticatiemiddelen op LoA3 voor een natuurlijk persoon. In technische zin bestaan de varianten uit een authenticatie App (software) op een smartphone of tablet die *naast* het gebruikersplatform moet worden gebruikt, e.g. een laptop of PC. Zie Figuur 1. De keuze van een authenticatie App maakt een eenvoudige, betrouwbare integratie mogelijk tussen het registratie- en het middel verstrekking proces. Het verstrekking proces heeft daarbij geen fysiek karakter maar vindt ook ‘op afstand’ plaats.

De best practice beschrijft een basis variant en twee geavanceerdere varianten. De basis variant werkt met een foto van het WID document van de gebruiker en stelt weinig technische eisen aan de smartphone of tablet van de gebruiker. Beide geavanceerde varianten gaan uit van het uitlezen van de contactloze chip (RFID/NFC)[1] in het WID document van de gebruiker. Bij de eerste geavanceerde variant wordt verondersteld dat de smartphone/tablet waarop de App wordt geïnstalleerd NFC *enabled* is. Bij de tweede variant wordt verondersteld dat de gebruiker tijdelijk kan beschikken over een dergelijke smartphone/tablet waarop een *dedicated* UitleesApp wordt geïnstalleerd. De tweede variant stelt daarmee bijvoorbeeld in staat de App te registreren/activeren via NFC op een iPAD/iPhone (die niet NFC *enabled* zijn). Zie verder Sectie 2.1. Het idee van de uitleesApp is overigens van Gert Maneschijn van de RDW.

In algemene zin bieden de geavanceerdere processen meer zekerheid dan het basis proces en worden zij waarschijnlijk als gebruikersvriendelijker ervaren. Doordat niet iedereen kan beschikken over een NFC *enabled* telefoon, kunnen de geavanceerde processen echter niet dwingend worden voorgeschreven. Tot slot wordt opgemerkt dat het toegestaan is dat een authenticatiedienst slechts één van de drie varianten implementeert.

[1] Volgens http://www.statista.com/statistics/347315/nfc-enabled-phone-installed-base/ en http://www.statista.com/statistics/371889/smartphone-worldwide-installed-base/ is in 2016 ongeveer 50% en in 2017 ongeveer 60% van alle smartphones uitgerust met NFC.

Om zekerheid te krijgen dat de gebruiker zich optimaal bewust is van het feit dat hij een authenticatiemiddel aan het aanschaffen is, wordt als onderdeel van de authenticatie App installatie gebruik gemaakt van een zogenaamde Challenge-Response video. Zie Stap 23 in Sectie 2.2. Dit is een variant op een toegepast proces [BAFIN] in Duitsland, waarbij gebruik wordt gemaakt van een interactieve video sessie tussen de gebruiker en een medewerker van de authenticatiedienst. Bij de variant beschreven in dit document moet de gebruiker een videoboodschap inspreken die wordt opgenomen vanuit de App:

a. waarin hij aangeeft gebruik te willen maken van de authenticatiedienst (*wilsuiting*),
b. waaruit de authenticatie kan vaststellen dat de videoboodschap geen herhaling is van een eerdere registratie (*freshness*)
c. waarvan de authenticatiedienst kan vaststellen dat de videoboodschap is verbonden aan de specifieke App instantie (*device binding*).

Een concreet voorbeeld van bovenstaande is dat de App de gebruiker vraagt de volgende videoboodschap uit te spreken:

"Ik wil kunnen aanloggen via IdSupply en registreer mij onder nummer 1234"

hierbij is "IdSupply" een voorbeeld naam van een authenticatiedienst en realiseert het willekeurige getal aangegeven met "1234" de *freshness*. Door te kunnen vaststellen dat de videoboodschap is opgenomen vanuit de App wordt *device binding* gerealiseerd.

De Challenge-Response video is een nieuwe ontwikkeling waar het ETD stelsel nog geen ervaring mee heeft. Daarom worden voorlopig ook alternatieve mechanismen toegelaten. Het is daarbij essentieel dat deze mechanismen worden gestuurd vanuit en zijn verbonden aan de App installatie. Bij dergelijke alternatieve mechanismen moet de authenticatiedienst claimen en onderbouwen dat ze een vergelijkbare wilsuiting/freshness/device binding bieden.

Na afloop van de Idensys pilots en uiterlijk voor het einde van 2016 wordt deze practice geëvalueerd. Onderdeel van deze evaluatie is het nut/noodzaak van de Challenge-Response video en mogelijke alternatieven.

Leeswijzer

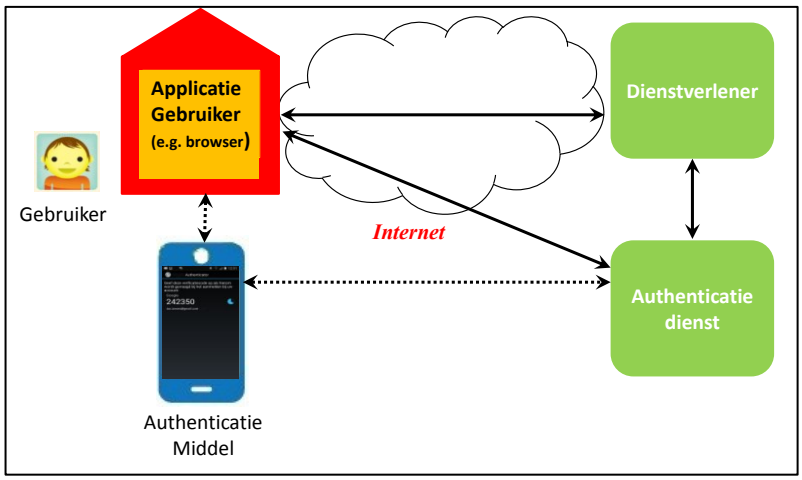
- In Sectie 2 staan de drie varianten van 'registratie en verstrekking op afstand' beschreven.
- In Sectie 3 wordt onderbouwd dat de voorbeelden conform zijn met het Normenkader Betrouwbaarheidsniveaus [NORMBN].
- Bijlagen A en B illustreren de iDEAL schermen die onderdeel uit maken van de voorbeelden.
- Bijlage C gaat in op de relatie met het WID document in het geval dat een gebruiker een gekozen, geregistreerde achternaam wil gebruiken bij de registratie.
- Bijlage D bevat een toelichting van de technische vereisten die worden gesteld in Sectie 2 aan het uitlezen van de WID document chip.
- Bijlage E beschrijft de belangrijkste risico's en mitigerende maatregelen.

2 Voorbeelden 'Registratie en verstrekking op afstand'

2.1 Context

Een natuurlijk persoon beschikt over een smartphone of tablet en wil dit gebruiken als basis voor een authenticatie applicatie (App) naast een ander platform, e.g. een PC, laptop of andere tablet waarop zich een internet browser bevindt. Er is daarbij een duidelijke hardware scheiding voorzien tussen het gebruikersplatform en het authenticatiemiddel. Vergelijk Figuur 1. De

authenticatie applicatie (App) omvat geïntegreerde modules voor de registratie van de gebruiker, activatie (‘verstrekking’) en voor het uitvoeren van authenticaties.



Figuur 1: scheiding van gebruikersplatform en authenticatiemiddel

Er wordt minimaal verondersteld dat de smartphone/tablet van de gebruiker beschikt over een camera voor het nemen van ‘selfie’ foto’s en video’s alsmede het nemen van foto’s van WID documenten. Deze zaken zijn noodzakelijk voor de basisvariant van de ‘good practice’. De twee geavanceerde varianten van de ‘good practice’ veronderstellen verder dat:

- de gebruiker beschikt over een WID document met een RFID chip die ook beschikt over een mechanisme om zijn digitale echtheid aan te tonen.[2] Dit betreft onder meer alle geldige Nederlandse paspoorten, identiteitskaarten alsmede alle rijbewijzen die na 2 oktober 2014 zijn uitgegeven.
- de smartphone/tablet van de gebruiker is NFC enabled en stelt in staat om de WID document chip uit laten uitlezen *of* de gebruiker kan tijdelijk gebruik maken van een dergelijke smartphone/tablet voor het laten uitlezen van de WID document chip. Ondersteuning van de tweede variant betekent dat de authenticatiedienst naast de App ook een ‘WID document uitlees App’ ter beschikking moet stellen. Omdat daarbij gebruik kan worden gemaakt van andermans smartphone of tablet voorziet de opzet in Sectie 2.2 erin dat deze smartphone of tablet geen inzage krijgt of kan krijgen in de WID document gegevens. Dit is gebaseerd op toepassing van de *end-to-end* tunnels gespecificeerd in de WID standaarden, i.e. [ICAO], [ISO18013-3].

In Bijlage D worden de belangrijkste risico’s benoemd rond het registratie en verstrekking proces alsmede de gekozen mitigerende maatregelen. Een van de belangrijkste risico’s is daarbij dat het gebruikersplatform (typisch een internet browser) door een fraudeur is geïnfecteerd met malware waardoor de fraudeur activiteiten kan doen namens de gebruiker zonder dat de gebruiker hiervan op de hoogte is. Dit was in de jaren 2011 en 2012 een van de oorzaken dat binnen het internet bankieren van de Nederlandse banken fraude ontstond van 30 miljoen Euro.

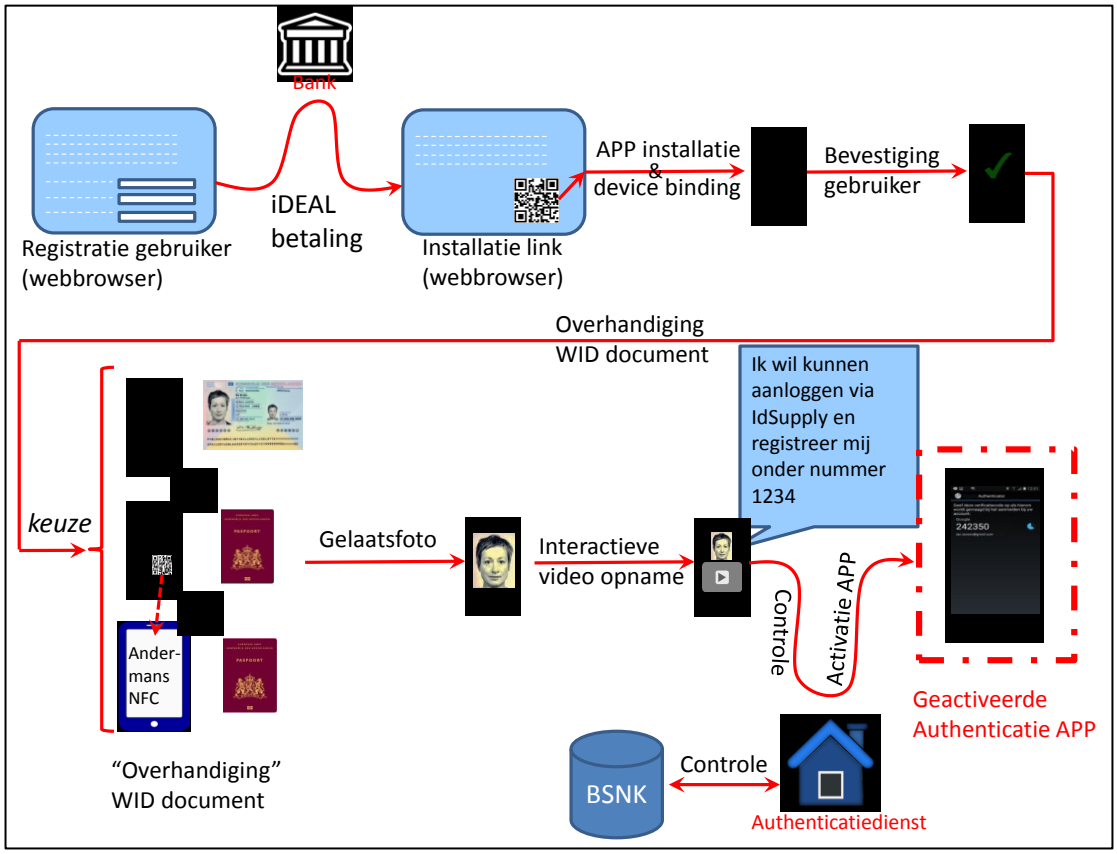
[2] Op de RFID chip van een paspoort of identiteit document, ook niet Nederlandse, bevinden zich in beginsel dezelfde gegevens van de houder die ook *op* het document staan. Deze gegevens zijn daarbij digitaal getekend door de uitgevende overheid. Alle Nederlandse RFID paspoort of identiteit document chips zijn uitgerust met anti-cloning mechanismen. Deze mechanismen staan bekend als Active Authentication (AA) of Chip Authentication (CA), zie [FRONTEX]. In het recente verleden beschikten paspoorten uit het Verenigd Koninkrijk niet over deze mechanismen.

Een fraudeur initieerde (of manipuleerde) daarbij betaaltransacties vanuit de browser zonder dat de gebruiker daarvan op de hoogte was.

2.2 Opzet en vereisten

Impliciete vereisten uit onderstaande stappen zijn aanvullend aan de vereisten voor een authenticatiedienst die LoA3 middelen uitgeeft.

1. De authenticatiedienst beschikt over gedocumenteerde procedures voor diens registratie- en verstrekking processen en traint zijn medewerkers hierin. De training omvat het verifiëren van de echtheid van WID documenten op basis van foto's en het vergelijken van een gelaatsfoto tegen een foto van een WID document. Specifieke aandacht moet daarbij zijn gegeven aan fotomanipulatie ('Photoshop'). Een medewerker mag het registratieproces niet uitvoeren zonder een succesvol afgeronde training.
2. De authenticatiedienst heeft een proces om periodiek, minimaal maandelijks, te toetsen of er geen *rogue* varianten van zijn Apps in de stores aanwezig zijn, i.e. Apps die zich proberen uit te geven voor die van de authenticatiedienst.
3. Alle onderstaand genoemde webpagina's worden verondersteld te zijn beveiligd via TLS in lijn met [NIST-TLS].
4. De authenticatiedienst is rechtstreeks verbonden als iDEAL *Merchant* aan zijn bank (hierna ook wel *acquiring bank* genoemd). Dit betekent aldus dat de authenticatiedienst niet verbonden is via een *payment service provider*. De *Merchant* naam van de authenticatiedienst die wordt getoond aan klanten tijdens het iDEAL protocol is een domeinnaam waar de gebruiker zich eenvoudig kan vervoegen in het geval van vragen. Een voorbeeld is registratie.authdienst.nl. Daarbij suggereert 'authdienst' de naam van de authenticatiedienst. Zie ook Bijlage A voor een nadere impressie. Bij aanroep van deze domeinnaam wordt een scherm getoond over het registratieproces alsmede een contactnummer in het geval van vragen.



Figuur 2 overzicht registratie en verstrekking proces

Het registratie en verstrekking proces bestaat uit de volgende stappen die vereenvoudigd zijn weergegeven in bovenstaande Figuur 2:

5. De gebruiker start een internet browser op en vervoegt zich bij de website van de authenticatiedienst. De gebruiker is middels een TLS certificaat controle in staat vast te stellen dat hij van doen heeft met een ETD authenticatiedienst.

Registratie gebruiker

6. Bij de start van het registratieproces informeert de authenticatiedienst gebruikers proactief over zijn processen, de voorwaarden en de verplichtingen die gelden voor gebruikers. Dit omvat ook de verplichting van de gebruiker om de hardware scheiding tussen het gebruikersplatform en het authenticatiemiddel te eerbiedigen. Zie Figuur 1.
7. De gebruiker registreert zijn identiteit op de website. Dit omvat in ieder geval:
   - BSN,
   - voornamen,
   - geboortenaam,
   - geboortedatum,
   - geboorteplaats en
   - documentnummer van het later in het proces te gebruiken WID document en de verloopdatum van dit document.

   In het geval dat de gebruiker een gekozen, geregistreerde achternaam wil gebruiken bij de registratie dan moet de achternaam van de echtgenoot (e/v) of partner (p/v) ook vastgelegd worden. De authenticatiedienst informeert de gebruiker dat deze achternaam ook op het WID document moet zijn opgenomen dat later in het proces zal worden gebruikt. Zie Bijlage C.

8. De authenticatiedienst voert enkele vormcontroles uit op de verstrekte gegevens om proactief met type fouten van de gebruiker om te kunnen gaan. Dit omvat een controle op het verstrekte BSN controlegetal. Aanvullend moet de gebruiker ook contactgegevens verstrekken zoals een email adres, mobiel nummer, vast nummer of contact adres. Van minimaal één van deze contactgegevens moet de authenticatiedienst vaststellen dat het onder 'controle' van de gebruiker is. Bij een emailadres betekent dat bijvoorbeeld het sturen van een email naar het opgegeven emailadres waar de gebruiker op moet reageren.
9. Ter bevestiging van de verstrekte gegevens en de acceptatie de authenticatiedienst voorwaarden, wordt de gebruiker gevraagd een betaling van 0,01 eurocent te doen. *Noot: een betaling van een hoger bedrag, bijvoorbeeld een paar euro, biedt meer mogelijkheden voor social engineering.* De betaling is van het type iDEAL vanaf een betaalrekening waarvan de tenaamstelling overeenkomt met die opgeven door de gebruiker in Stap 7 van het proces.

iDEAL betaling

10. Conform het iDEAL protocol selecteert de gebruiker diens bank en start het iDEAL betaling proces. De authenticatiedienst vormt een betaalverzoek, ook wel iDEAL bericht B geheten, en stuurt dit naar zijn eigen bank. Zie [iDEAL]. Dit bericht bevat details rond het verzoek waar de belangrijkste genoemd zijn in onderstaande tabel.

Veld	Beschrijving	Lengte/Waarde
`description`	Omschrijving van de order	35 karakters alfanumeriek of vrije tekst
`purchaseID`	uniek orderkenmerk van *Merchant*	- 35 karakters alfanummeriek strikt, i.e. alleen letters en cijfers - Als spaties worden gebruikt, dan wordt volgens [iDEAL] de transactie niet geweigerd maar kunnen de spaties worden vervangen door een vraagteken of asterisk.
Merchant`ReturnURL`	terugkeer URL	512 karakters alfanumeriek of vrije tekst
`entranceCode`	unieke terugkeer code in URL waarmee de klant kan worden herkend	40 karakters alfanumeriek of vrije tekst
`amount`	Bedrag	
`currency`	Munteenheid (Euro)	

Specifiek zullen de twee velden `description` en `purchaseID` worden gebruikt voor het informeren van de gebruiker. Dit wordt onderstaand verder uitgelegd. Betreffende dit aspect is het belangrijk om de drie plaatsen te benoemen waar het iDEAL protocol minimaal verplicht deze velden aan de gebruiker te tonen:

- `description`:
  - bij het beginscherm bij de issuing bank en in het scherm dat de issuing bank de gebruiker toont bij de succesvolle afronding van de betaling, cf. Bijlage A
  - op het rekening afschrift van de gebruiker
- `purchaseID`
  - in het succesvolle afronding scherm dat de issuing bank de gebruiker toont bij de

succesvolle afronding van de betaling, cf. Bijlage B
- op het rekening afschrift van de gebruiker

Zie [CURRENCE]. Wij merken op dat sommige issuing banken het `purchaseID` ook tonen bij het beginscherm. Zie [BURGERS].

11. De authenticatiedienst waarschuwt de gebruiker over de ophanden zijnde registratie. Dit gebeurt door de gebruiker hierover te informeren middels het iDEAL veld `description` in het iDEAL *issuer* begin scherm. De informatie bevat naast een waarschuwing ook een unieke referentie naar de registratie. Zie Bijlage A. *Noot: idealiter zou men in dit veld ook een telefoonnummer van de authenticatiedienst willen plaatsen maar daar is helaas geen ruimte voor.* Een voorbeeld van een toegestaan `description` veld is (waarbij 'ABCDE' een uniek alfanummerieke referentie voorstelt):

Veld	Inhoud
`description`	`Let op: identiteit registratie ABCDE`
	`12345678901234567890123456789012345` `---------10--------20---------30---35`

12. De gebruiker is – in lijn met het iDEAL protocol – in staat het betalingsproces en daarmee de registratie af te breken.
13. De authenticatiedienst waarschuwt de gebruiker bij een succesvol afgeronde betaling. Dit gebeurt door de gebruiker hierover te informeren middels de iDEAL veld '`description`' (zie Stap 11) en het veld `purchaseID`. Het `purchaseID` verwijst de gebruiker naar een telefoonnummer dat gebeld kan worden in geval van twijfel of vragen. Een voorbeeld van een toegestaan `purchaseID` veld is:

Veld	Inhoud
`purchaseID`	`BIJ TWIJFEL OF VRAGEN BEL 08001111`
	`12345678901234567890123456789012345` `---------10--------20---------30---35`

Het iDEAL protocol voorziet er vanzelf in dat bij een succesvolle iDEAL betaling beide velden worden geplaatst op het dagafschrift van de gebruiker. Dit is met name relevant als de gebruiker het slachtoffer is geworden van 'social engineering' en de betaling weliswaar heeft uitgevoerd, maar zich niet bewust is geweest van de betekenis van de betaling.

14. Het systeem van de authenticatiedienst kan volgens het iDEAL protocol [iDEAL] een zogenaamd *merchant* status response bericht opvragen bij zijn (acquiring) bank. Dit bericht heet ook wel bericht F'. Dit bericht is digitaal getekend door de bank van de authenticatiedienst. De authenticatiedienst controleert allereerst de digitale handtekening van de bank. In het geval van een succesvolle betaling is het veld status gelijk aan "Succes". Als de betaling door de klant nog niet is afgerond, is de status "Open". In dit geval dient nogmaals een status response bericht te worden opgevraagd. Indien de status niet gelijk is aan "Succes" of "Open" dan dient het proces te worden afgebroken en moet de gebruiker van voren af aan beginnen. Bericht F' bevat ook de `purchaseID` en de `description` velden zoals die door de authenticatiedienst zijn aangeleverd voor de gebruiker en de authenticatiedienst moet controleren of deze overeenkomen. Het bericht F' bevat ook de tenaamstelling van de bankrekening in de vorm van het veld `Consumername`. In het geval van een natuurlijk persoon zijn dit de voorletters en de achternaam van de rekeninghouder. De rekening kan ook op meerdere namen staan ('en/of' rekening). In dat geval zijn de

voorletters en achternaam van de andere rekeninghouders ook opgenomen in bericht F'[3]. De authenticatiedienst controleert of de voorletters en achternaam precies overeenkomen met die opgegeven door de gebruiker bij Stap 7. Het bericht F' en het gebruikte verificatie certificaat worden bewaard door de authenticatiedienst als onderdeel van het dossier.

Een iDEAL transactie is vrijwel real-time zodat een webshop vrijwel direct inzicht krijgt over de status van de betaling. Dit is onderscheidend met een reguliere (internet bankieren) betaling die pas een werkdag later kan binnenkomen bij de authenticatiedienst. De snelheid van dit proces bemoeilijkt ook de mogelijkheden voor fraude. Een ander onderscheid is dat de begunstigde naam bij iDEAL(Consumername) groter kan zijn (70 karakters) dan bij een reguliere betaling. Dit is met name bij "en/of" rekeningen een voordeel.

15. Bij een afronding van de vorige stappen wordt de gebruiker door diens bank naar de webpagina geleid gevormd door de `MerchantReturnURL` en de `entranceCode`. Bij een succesvolle afronding toont deze pagina nu een QR code die de gebruiker kan inscannen met de authenticatie App van de authenticatiedienst. De authenticatiedienst informeert de gebruiker hoe deze App bemachtigd kan worden in de Appstore. De informatie richting klanten (cf. Stap 6) omvat dat de klant alleen Apps uit de officiële Appstores mag betrekken.

App installatie en device binding

16. De gebruiker installeert de App (of had dat al eerder gedaan). De App bouwt een eenzijdige TLS verbinding met de authenticatiedienst op en vraagt de gebruiker om een vijf cijferige PIN code op te geven. De App vormt vervolgens een willekeurig publiek/privaat sleutelpaar in lijn met [NIST-KEY] en verstuurt het publieke gedeelte van het bovengenoemde publiek/privaat sleutelpaar in de vorm van een *self-signed* certificaat naar de authenticatiedienst. Vervolgens gebruikt de App dit certificaat om een tweezijdige versleutelde TLS verbinding op te bouwen met de authenticatiedienst. *Noot: de adequate bescherming van de private sleutel en geheime cryptografische sleutels in de App is cruciaal. Zie ook Sectie 2.3.*
17. De App registreert de volgende informatie bij de authenticatiedienst:
    - de PIN
    - Een Unique Device Identifier (UDID) van het platform waarop de App actief is. De meeste platformen hebben hier specifieke voorzieningen voor, maar bij gebrek daaraan kan bijvoorbeeld het MAC adres worden gebruikt van de WiFi interface of het IMEI nummer in het geval van een smartphone. *Noot: omdat dit mogelijk als persoonsgegeven kan worden bestempeld dient de authenticatiedienst duidelijk te maken aan de gebruiker dat deze gegevens worden vastgelegd.*
18. De PIN wordt na succesvolle overdracht door de App veilig gewist en niet lokaal opgeslagen. Deze opzet realiseert dat de App altijd een tweezijdige TLS tunnel kan opbouwen waarover de gebruiker zich *daarna* kan authenticeren bij de authenticatiedienst met de PIN. Daarbij wordt gerealiseerd dat slechts bij registratie de PIN en de UDID in klare taal naar de authenticatiedienst worden gestuurd. Zie Sectie 2.3 voor nadere *good practices* hieromtrent.

Het publiek/private sleutelpaar en UDID vormen de binding met het device, de PIN is de binding met de gebruiker.

[3] Sinds de introductie van SEPA (Single Euro Payments Area) in 2012 zijn financiële instellingen consequent de geboortenaam (of optioneel de geregistreerde achternaam) en voorletters gaan gebruiken zoals die voorkomt op het WID document waar men in het verleden ook de voorletter van de roepnaam kon gebruiken.

19. De App vormt een tweezijdige TLS tunnel met de authenticatiedienst. De App vraagt de gebruiker de QR code in te scannen, hierbij wordt de informatie uit Stappen 5-15 gekoppeld aan de registratie van de App bij Stappen 16-18.
20. De authenticatiedienst zoekt de informatie op die de klant in de Stap 7 heeft aangeleverd en verstrekt de volgende informatie aan de App:
    - BSN,
    - voornamen,
    - geboortenaam,
    - geboortedatum,
    - geboorteplaats,
    - eventueel opgegeven geregistreerde naam.

    Het WID documentnummer en de WID verloopdatum worden niet verstrekt aan de App.[4] De App toont deze informatie aan de gebruiker aangevuld met de vermelding dat een iDEAL transactie is uitgevoerd ter identificatie en het daarbij gebruikte bankrekening nummer. De App vraagt de gebruiker deze informatie te bevestigen.

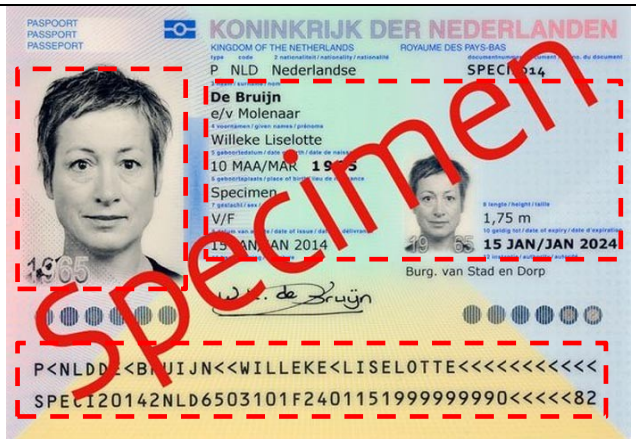
'Overhandigen' WID document

21. De App biedt de gebruiker nu drie mogelijkheden voor het 'overhandigen' van het WID document
    a. Maken van een foto via de App (Stap 21a),
    b. Uit laten lezen (NFC) van de WID document chip op afstand vanaf het eigen device (Stap 21b),
    c. Uit laten lezen (NFC) van de WID document chip op afstand vanaf andermans device (Stap 21c).

    Het ligt voor de hand dat de App probeert vast te stellen of het device beschikt over NFC alvorens de tweede optie voor te stellen. Als het device geen camera heeft dan stopt het proces.

Stap	Beschrijving
21a	De App vraagt en faciliteert de gebruiker om een foto te maken van zijn WID document met behulp van de camera aanwezig op het device. Daarbij biedt de App een positie raster waarmee de belangrijke onderdelen van het WID document door de gebruiker in geplaatst moeten worden. Zie Figuur 3. De App controleert tijdens het scannen/foto nemen of de Machine Readable Zone (MRZ) leesbaar is door de MRZ middels *Optical Character Reading* (OCR) te lezen en te controleren of de MRZ checksum klopt. De foto van het WID document moet van voldoende kwaliteit zijn om echtheidskenmerken te kunnen vaststellen en om de vergelijking met de gelaatsfoto uit de volgende stap te kunnen maken. Het feit dat de MRZ checksum klopt is daar een eerste indicatie voor.

[4] De reden hiervoor is tweeledig. Enerzijds zal het WID documentnummer en WID verloopdatum niet herkenbaar zijn voor de gebruiker. Anderzijds stellen deze gegevens de App in staat de WID document chip uit te lezen hetgeen niet de bedoeling is: het uitlezen gebeurt door de authenticatiedienst op afstand waarbij de App slechts fungeert als 'doorgeefluik' en de WID informatie alleen in versleutelde vorm voorbij ziet komen. Door het WID documentnummer en WID verloopdatum niet aan de App te verstrekken wordt daarmee ook een elementaire implementatiefout voorkomen waarbij de App de WID data leest en doorstuurt naar de authenticatiedienst.



Figuur 3: kader (in rood) voor het lezen/fotograferen WID documenten

22b

- De App vraagt en faciliteert de gebruiker om zijn WID document op afstand uit te laten lezen. In praktische zin betekent dit, dat de App de gebruiker instrueert zijn WID document in de buurt van de smartphone/tablet te houden. De gegevens verstrekt bij Stap 7 (WID documentnummer, WID document verloopdatum en geboortedatum) stellen de authenticatiedienst via de App in staat de WID document chip uit te lezen. De uitleesprotocollen[ICAO], [ISO18013-3] voorzien daarbij in end-to-end versleuteling: de App fungeert slechts als proxy en krijgt geen toegang tot deze gegevens.
- De authenticatiedienst voert, en in de aangegeven volgorde, de volgende activiteiten en controles uit (zie Bijlage D voor een toelichting):
  i. Opzetten van end-to-end tunnel tussen authenticatiedienst en WID document chip op basis van BAC, BAP of SAC.
  ii. Passive Authentication: controle van het Document Security Object (SOD) en publieke sleutels voor Authenticiteit controle van het document (volgende stap) middels controle van de aanwezige hashes in het SOD.
  iii. Authenticiteit controle van het document middels Active Authentication of Chip Authentication.
  iv. Lezen van houdergegevens en validatie van authenticiteit middels controle van de aanwezige hash in het SOD; dit omvat de gegevens die zijn verstrekt bij Stap 7.
  v. Lezen van gelaatsfoto(s) en validatie van authenticiteit middels controle van de aanwezige hash in het SOD

  In lijn met de proportionaliteit beginselen in de Wet bescherming persoonsgegevens mag de authenticatie dienst alleen die gegevens uitlezen die noodzakelijk zijn voor het registratieproces. Dit betekent bijvoorbeeld dat de authenticatiedienst bij het rijbewijs niet de categorie informatie of de scan van de ‘natte’ handtekening daarop mag lezen. Soms zijn er twee digitale gelaatsfoto’s aanwezig op een WID document. Als beide foto’s worden gebruikt binnen het controle proces en daarvoor noodzakelijk zijn, mogen beide foto’s worden gelezen.
- De controle genoemd onder punt b. omvat controle van de digitale handtekening tegen het *document signer* certificaat (veelal aanwezig in het SOD), de controle dat dit certificaat is uitgegeven door de root van de uitgevende nationale instantie (CSCA) en de controles dat de certificaten niet verlopen of ingetrokken zijn.
- Indien het WID document SAT of Chip Authentication ondersteunt moet één van beide worden gebruikt. Daarbij bestaat een sterke voorkeur voor SAT omdat dit de

	beste bescherming biedt. Het nadeel van SAT is dat het iets meer tijd kost en zo de gebruikerservaring mogelijk nadelig kan beïnvloeden.
22c	De App deelt de gebruiker mee dat en hoe hij binnen bepaalde termijn, e.g. een week, een UitleesApp moet installeren op een andere smartphone/tablet. Na afronding van de volgende stappen (Stap 23 etc.) sluit de App nogmaals af met deze mededeling alsmede met een QR code die vanaf de UitleesApp moet worden ingelezen. Zolang de UitleesApp niet succesvol is gebruikt blijft deze boodschap/QR code getoond worden door de App. Bij inscannen van deze QR-code vanaf de UitleesApp is de authenticatiedienst in staat om de registratiesessie te herkennen. De gebruiker wordt gevraagd het WID document te laten uitlezen door de UitleesApp zoals dat opgegeven bij registratie is in Stap 7. Het WID document kan daarbij gesloten blijven. De authenticatiedienst start de stappen aangegeven in Stap 22b. Indien het WID document SAT gebruikt moet dit worden toegepast door de UitleesApp tenzij dit tot zwaarwegende gebruikersproblemen leidt.

Maken gelaatsfoto

22. De App vraagt en faciliteert de gebruiker om een foto te maken van zijn gelaat met behulp van de camera aanwezig op de smartphone of tablet. De foto moet zo genomen zijn dat een vergelijking door een authenticatiedienst medewerker met de foto op het WID document optimaal mogelijk is. De App faciliteert dit door een raster te maken waar het hoofd van de gebruiker in moet passen.

Challenge-Response Video

23. De App toont de gebruiker een zinsnede uit een lijst van minimaal 1.000 mogelijkheden en vraagt de gebruiker deze zinsnede uit te spreken. Hiervan maakt de App een video opname. Feitelijk is dit een video *challenge-response* protocol. De beveiligingsdoelstellingen hiervan zijn dat a) de gebruiker een *wilsuiting* geeft rond de registratie, dat b) deze wilsuiting 'fresh' is, i.e. geen *replay* is van een eerdere wilsluiting en c) dat de videoboodschap is verbonden aan de App (*device binding*). Een voorbeeld is:

    "Ik wil kunnen aanloggen via IdSupply en registreer mij onder nummer 1234"

    hierbij is "IdSupply" een voorbeeld naam van een authenticatiedienst en realiseert het willekeurige getal aangegeven met "1234" de *freshness*.
24. De App stuurt beide genomen foto's en de videoboodschap naar de authenticatiedienst over de beveiligde verbinding.

Controle door authenticatiedienst

25. Een authenticatiedienst medewerker voert de volgende controles uit:
    - komt het document type- en nummer opgegeven bij Stap 7 overeen met dat op de foto van het WID document uit Stap 21?
    - is het document ten tijde van de registratie als gestolen of verloren opgegeven of is het document om andere redenen ongeldig is verklaard? Deze controle vindt plaats op basis van het document nummer.
    - correspondeert de foto van het WID document uit Stap 22 met een authentiek WID document?

- corresponderen de persoonsgegevens op het WID document uit Stap 22met die opgegeven bij Stap 7? In het geval een WID foto is aangeleverd (Stap 21a) dient de medewerker in te zoomen op de details van de persoonsgegevens op de foto en deze te inspecteren op beeld manipulatie (‘Photoshop').
- correspondeert de gelaatsfoto op het WID document uit Stap 21 met de gelaatsfoto genomen in Stap 22? Hierbij dient de medewerker in te zoomen op de details van deze gegevens op het WID document en deze te inspecteren op beeld manipulatie (‘Photoshop').
- correspondeert de gebruiker en omgeving in de videoboodschap uit Stap 23 met die op de foto in Stap 22?
- spreekt de gebruiker in de videoboodschap de gevraagde tekst uit getoond in Stap 23?

Als deze controles succesvol zijn, dan is de registratie van de persoon succesvol. In andere gevallen volgt een afwijzing.

26. In het geval van een afwijzing wist de authenticatiedienst hierna in iedere geval de foto’s en de videoboodschap verstrekt door de gebruiker. Hiervan mag worden afgeweken in het geval een vermoeden van fraude bestaat. In het geval van een succesvolle afronding van de controles archiveert de authenticatiedienst de WID foto. Daarbij wordt het BSN na maximaal 2 weken gewist van de WID foto. Ook wordt de gelaatsfoto en de videoboodschap na 2 weken gewist. De termijn van 2 weken stelt de organisatie in staat interne controle in te richten.

Controle BSN koppelregister

27. Het systeem van de authenticatiedienst doet een registratie verzoek bij het BSN koppelregister. Als onderdeel van de registratie zal de authenticatiedienst de geboortenaam, voorletters, geboortedatum en BSN van de gebruiker aanbieden bij het BSN Koppelregister van de overheid. Als de gebruiker aangeeft een geregistreerde naam te willen gebruiken zal additioneel de achternaam van de echtgenoot/partner worden aangeboden. De additionele levering van de echtgenoot/partner naam is een signaal aan het BSN Koppelregister dat de gebruiker een geregistreerde naam wil gebruiken. Registratie onder geboortenaam is altijd mogelijk, ook in geval dat de gebruiker een geregistreerde naam heeft.

Binnen het koppelregister vinden onder meer volgende drie controles op consistentie plaats waarmee extra zekerheid ontstaat over de registratie:

- *corresponderen de voorletters en geboortedatum vastgelegd bij het opgegeven BSN met de opgegeven voorletters en geboortedatum?*
- *correspondeert de geboortenaam vastgelegd bij het opgegeven BSN met de opgegeven geboortenaam en geboortedatum?*
- *indien gebruik wordt gemaakt van een geregistreerde naam: is er bij het opgegeven BSN sprake van een geregistreerde achternaam? Indien dit het geval is: correspondeert de verstrekte achternaam van echtgenoot/partner met de opgegeven geregistreerde achternaam van echtgenoot/partner? Zie Bijlage A.*

Verder wordt gecontroleerd of de persoon in kwestie niet overleden is. Als een van deze controles faalt wordt de registratie afgewezen door het BSN Koppelregister.

Activatie van de App

Indien alle voorgaande stappen succesvol zijn doorlopen volgt het verstrekking (‘activatie’) proces. Dit bestaat uit de volgende drie stappen:

28. Als de registratie bij het BSN Koppelregister succesvol is verlopen dan activeert het systeem van de authenticatiedienst de App voor gebruik als authenticatiemiddel.

29. Bij het eerste gebruik van de App na activatie door de authenticatiedienst vermeldt de App de activatie aan de gebruiker en wordt deze gevraagd dit te bevestigen. Deze bevestiging wordt gearchiveerd door de authenticatiedienst. Verder toont de App eenmalig een revocatiecode. Daarbij verwijst de App naar een locatie hoe de revocatiecode gebruikt moet worden. Verder geeft de App de gebruiker aan dat deze de revocatiecode zorgvuldig moet bewaren.
30. De gebruiker wordt ook geïnformeerd over de activatie van het middel via een van de gecontroleerde contactgegevens bij Stap 8.

2.3 Specifieke eisen aan de App en *good practices*

31. De controle van de iDEAL transactie in Stap 14 mag niet beïnvloedbaar zijn door de medewerker die de controles bij Stap 42 uitvoert. De iDEAL afhandeling bij de authenticatiedienst zal in de praktijk geautomatiseerd zijn.
32. De QR codes die worden gebruikt in de opzet moeten voldoende willekeurig zijn om succesvol raden te voorkomen; de raadkans moet kleiner dan 2^{-32} zijn.
33. Het is niet altijd eenvoudig om met een smartphone of tablet camera foto's te maken van een WID document die van voldoende kwaliteit en, met name, scherp zijn. Omdat de kwaliteit van de foto's en de video essentieel is voor de kwaliteit van het registratie proces moet de authenticatiedienst kunnen aantonen dat hieromtrent een succesvolle gebruikerstest heeft plaatsgevonden rond de belangrijkste platforms die worden ondersteund.
34. Een eenvoudige wijze om te zorgen dat de PIN en UDID alleen bij registratie hoeft te worden gestuurd naar de authenticatiedienst is als volgt. Bij Stap 17 wordt ook een willekeurige HMAC sleutel gegenereerd [HMAC] die wordt geregistreerd als onderdeel van Stap 17. Om te bewijzen dat de gebruiker de PIN weet en dat de UDID klopt, stuurt de authenticatiedienst na de realisatie van de tweezijdige TSL tunnel een random string S naar de App welke vervolgens een HMAC terugstuurt over de string S || PIN || UDID.
35. De QR code gepresenteerd in Stap 15 mag slechts beperkte tijd geldig blijven, maximaal een uur en mag slechts vanaf één IP adres leiden tot inzage van de geregistreerde gegevens. Na afronding van de stappen in Sectie 2.2, succesvol of niet, mag de QR niet meer kunnen worden gebruikt.
36. Bij het controleren van het server certificaat van de authenticatiedienst wordt geadviseerd dat de App niet vertrouwt op de truststore van het platform en zelfstandig controleert dat het server certificaat onder de PKI overheid root is afgegeven. Dit om te voorkomen dat de gebruiker middels social engineering wordt verleid *rogue* root certificaten toe te voegen aan de truststore van zijn device.
37. De App moet na bepaalde tijd van inactiviteit, maximaal 2 minuten, niet meer toegankelijk zijn en zich weer bij de authenticatiedienst aanmelden met ingave van de PIN op het toestel.
38. De App moet in staat zijn om de authenticiteit en integriteit van de QR codes die worden gebruikt te valideren. In praktische zin zou dit kunnen gebeuren door een HMAC waarde op te nemen in de QR codes afgeleid van de HMAC sleutel genoemd in het eerste punt.
39. De App moet maatregelen nemen om de integriteit en authenticiteit van de foto's en de videoboodschap te beschermen, zowel tijdens het proces van het nemen van de opnamen als tijdens de tijdelijke opslag in afwachting van het sturen naar de authenticatiedienst. Na afronding van het proces moet de App de foto's en de video veilig wissen conform [WIS] of vergelijkbaar. Bij opstarten van de App moet deze vaststellen of er nog foto's en video's aanwezig zijn uit eerdere sessies en deze dan alsnog wissen conform [WIS] of vergelijkbaar.
40. De App moet code *obfuscation* toepassen om zijn interne werking te beschermen.
41. De authenticatiedienst moet in zijn voorwaarden opnemen dat het fysieke platform waarop de applicatie actief is (typische een internet browser) niet hetzelfde mag zijn als het platform waarop de authenticatie App actief is. Geadviseerd wordt dat de authenticatiedienst ook technische maatregelen implementeert om hierop toe te zien.

42. Indien de authenticatiedienst de App ook wil gebruiken voor authenticatie bij dienstverleners buiten het ETD stelsel, dan moet de App bij elke authenticatie aan de gebruiker duidelijk maken of deze voor een dienstverlener is die binnen of buiten Idensys is gelegen.
43. De App houdt een gebruiker raadpleegbare log bij van alle registratie gebeurtenissen, hun tijdstip en de status van het resultaat.
44. Vooruitlopend op de nadere eisen voor een authenticatiemiddel op LoA3 is de volgende opzet toegestaan. Als onderdeel van de authenticatie bij de authenticatiedienst typt de gebruiker een gebruikersnaam in die bij het registratieproces is gekoppeld aan de gebruiker. De Authenticatiedienst zet daarop een willekeurig zescijferige code klaar voor deze App instantie. De App kan deze code ophalen en aan de gebruiker tonen na succesvolle ingave van de PIN door de gebruiker. De gebruiker typt deze code in, in het scherm van de authenticatiedienst.
45. Voor bescherming tegen man-in-the-browser aanvallen is het geadviseerde *good practice* dat de App ook de dienstverlener toont waarvoor de gebruiker geauthentiseerd wil worden.
46. De App van de authenticatiedienst moet met succes een penetratietest hebben doorstaan, waarbij de volgende zaken minimaal zijn onderzocht vanuit het perspectief van een *Moderate Attack potential* in de zin van [ISO18045], vergelijk ook [ImpReg]:
    - conformiteit met de beveiligingseisen geïmpliceerd in Sectie 2.2,
    - bescherming van het cryptografisch sleutelmateriaal, e.g. middels platform ondersteund Secure Storage of obfuscatie/white box crypto
    - bestandheid van de App tegen klonen middels aanvallen vanaf het internet,
    - de beveiligingswerking van de App wordt niet aangetast indien de webapplicatie van de gebruiker besmet is met man-in-the-browser malware.

    De penetratietester dient gecertificeerd te zijn tegen een gangbaar schema. Certified Ethical Hacker (CEH) van de EC-Council is een voorbeeld van een gangbare certificering.

3 Conformiteit met het Normenkader betrouwbaarheidsniveaus

In deze sectie zullen we niet de volledige conformiteit van de opzet beschreven in Sectie 2 met het Normenkader betrouwbaarheidsniveaus [NORMB] onderbouwen, maar slechts ingaan op een specifiek aandachtspunt, de verstrekking van een authenticatiemiddel:

- Bij de opzet beschreven in Sectie 2.2 is er geen sprake van een fysieke verstrekking van een middel. De activatie van de App in Stap 28 vult feitelijk de verstrekking in en deze is betrouwbaar gekoppeld aan de geregistreerde persoon. Hiermee wordt direct invulling gegeven aan de eis 10.2.2.1_15 uit [NORMD]: “If a credential is not delivered in person, then it SHALL be delivered using a secure channel and the entity or an authorized representative of the entity shall sign a receipt acknowledging receipt of the credential.” De ‘receipt’ is daarbij expliciet in Stap 28 genoemd.

4 Referenties

#	Document
[BAFIN]	Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin, Interpretation of section 6 (2) no. 2 of the GwG ("not personally present"), 2014. Beschikbaar op: http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/rs_1401_gw_verwaltungspraxis_vm_en.html. Alternatief kan worden gezocht bij Google met zoektermen: "III. Interpretation of section 6 (2) no. 2 of the GwG ("not personally present") site: bafin.de".
[Burgers]	Willem Burgers, Threesomes on the Internet – Investigating the security of the iDEAL payment System, November 2014. Zie http://www.ru.nl/publish/pages/769526/z-scriptie_willem_burgers.pdf.
[CURRENCE]	Email communicatie met Currence.
[FRONTEX]	Frontex, Operational and Technical security of Electronic Passports, 2011. Beschikbaar vanaf http://frontex.europa.eu.
[GPG45]	Cabinet Office, Guidance Identity proofing and verification of an individual, 3 November 2014. Beschikbaar op https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.
[ICAO-10]	ICAO, Machine Readable Travel Documents, part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), seventh edition, 2015. Beschikbaar vanaf http://www.icao.int.
[ICAO-11]	ICAO, Machine Readable Travel Documents, part 11: Security Mechanisms for MRTDs, seventh edition, 2015. Beschikbaar vanaf http://www.icao.int.
[iDEAL]	iDEAL Merchant Integratie Gids, Versie 3.3.1 (februari 2015), Rabobank. Zie https://www.rabobank.nl/images/ideal_merchant_integratie_gids_29696265.pdf.
[ImpReg]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015. Zie http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
[ISO18045]	ISO/IEC 18045, Information technology — Security techniques — Methodology for IT security evaluation, 2014. Beschikbaar vanaf http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.
[NIST-KEY]	Recommendation for Key Management – Part 1: General (Revision 3), NIST Special Publication 800-57, National Institute of Standards and Technology, juli 2012. Zie http://csrc.nist.gov/publications/PubsSPs.html.
[NIST-TLS]	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, NIST Special Publication 800-52 Revision 1, National Institute of Standards and Technology, april 2014. Zie http://csrc.nist.gov/publications/PubsSPs.html.
[ISO18013-3]	ISO, Information technology — Personal identification — ISO-compliant driving licence, ISO 18013, part 3, 2009.
[NORMD]	Eisen aan middelen, zie https://afsprakenstelsel.etoegang.nl/display/as/Eisen+aan+middelen
[WIS]	G.F. Hughes, D.M. Commins, and T. Coughlin, Disposal of disk and tape data by secure sanitization, IEEE Security and Privacy, Vol. 7, No. 4, (July/August

	2009), pp. 29-34.

A. Bijlage: iDEAL issuer begin scherm

B. Bijlage: iDEAL issuer afsluitscherm bij succesvolle transactie

C. Bijlage: Geregistreerde achternaam

Een persoon kan een gekozen achternaam bij de overheid (BPR) registeren, dit kan de achternaam van een echtgenoot of partner zijn of elk van de twee combinaties daarvan met de geboortenaam. Zie [JUSTIS]. In het WID document wordt het gebruik van een geregistreerde achternaam duidelijk doordat de achternaam van de echtgenoot of partner wordt bijgevoegd op het WID document voorafgegaan door de afkorting e/v (echtgenoot van) of p/v (partner van). Zie onderstaande voorbeelden (niet op relatieve schaal). Op welke wijze de persoon feitelijk geregistreerd staat bij BPR wordt evenwel niet duidelijk uit het WID document. Ter illustratie, de eerste persoon in Figuur 4 kan als officieel geregistreerde achternaam hebben: Willeke Liselotte Molenaar, Willeke Liselotte Molenaar-De Bruijn of als Willeke Liselotte De Bruijn-Molenaar. De vermelding ‘e/v’ in het WID document geeft aldus alleen aan dat er sprake is van een officieel geregistreerde achternaam maar niet welke.

Figuur 4: Voorbeelden WID documenten

D. Bijlage: Toelichting technische vereisten gesteld aan uitlezen van WID document chip

In deze bijlage wordt een toelichting gegeven op de stappen in Sectie 2.2 die het uitlezen van de WID document chip betreffen. Deze toelichting is gebaseerd op [Frontex], [ICAO-10], [ICAO-11] en [ISO18013-3].

D.1. Overzicht

Bij het uitlezen van een WID document chip (hierna: chip) noemt men de uitlezende partij veelal de *terminal*. In de opzet van Stap 22, heeft de authenticatiedienst de rol van de terminal; daarbij speelt de App slechts de rol van een proxy. Zodra de terminal een contactloze verbinding heeft opgebouwd met de chip, moet de terminal zich eerst authenticeren richting chip vooraleer gegevens kunnen worden gelezen van de chip. Als authenticatie moet de terminal bewijzen kennis te hebben van het WID documentnummer, de verloopdatum van het document en de geboortedatum van de houder. Hiervoor zijn twee protocollen gespecificeerd in [ICAO-11] en [Rijbewijs]. Dit zijn Basic Access Control (BAC) en Supplemental Acces Control (SAC). Daarbij wordt BAC in de context van het rijbewijs Basic Access Protection (BAP) genoemd en staat Supplemental Acces Control ook wel bekend onder de naam Password Authenticated Connection Establishment (PACE). SAT is een nieuwere en verbeterde vorm van BAC/BAP. Zie Sectie D.2 voor meer details.

Nadat de terminal toegang heeft gekregen tot de chip, kan deze de daarop aanwezige bestanden lezen. Bestanden heten datagroepen in de terminologie van de WID documenten. De eerste datagroep die de terminal moet lezen is het Document Security Object (SOD). Dit is een bestand dat digitaal getekend is door een zogenaamde *document signer*. Het is niet verplicht dat de SOD het certificaat van *document signer* bevat maar dat is meestal wel het geval. Dit is in ieder geval bij de Nederlandse WID documenten, waaronder het rijbewijs. Het *document signer* certificaat is op zijn beurt weer getekend door de root van de uitgevende nationale instantie. Deze root staat bekend als Country Signing Certificate Authority of CSCA en neemt de vorm aan van een *self-signed* certificaat. Het root certificaat moet betrouwbaar worden vergaard bij de uitgevende nationale instantie. In Nederland is dit voor reisdocumenten de Rijksdienst voor Identiteitsgegevens, onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Voor het rijbewijs is dat de RDW.

De eerste stap die de terminal moet doen is controleren of de SOD digitaal is getekend door de aanwezige *document signer* en dat deze is getekend door de CSCA. Vervolgens moet de terminal controleren of de certificaten niet zijn verlopen en dat zij niet zijn ingetrokken. Voor dat laatste moet de terminal een zogenaamde Certificate Revocation List downloaden bij de CSCA.

Door de controle van de SOD kan de terminal ook de authenticiteit van de andere datagroepen vaststellen. Deze zijn namelijk niet separaat getekend maar hun hashwaarde maakt deel uit van de SOD. Om de authenticiteit van een datagroep te controleren moet de terminal diens data lezen, daar een hash van uitrekenen en vervolgens vaststellen of deze in de SOD aanwezig is.

Voordat de terminal de datagroepen met persoonsgegevens en foto gaat lezen moet deze eerst nog vaststellen dat het WID document niet is gekloond. Een fraudeur zou immers alle genoemde datagroepen inclusief SOD kunnen kopiëren. Voor kloon detectie bestaan twee oplossingen: Active Authentication (AA) en Chip Authentication (CA). Beide zijn gebaseerd op een publiek/privaat sleutelpaar waarvan de publieke sleutel leesbaar aanwezig is in een bepaalde datagroep. De terminal leest de publieke sleutel en controleert de authenticiteit op bovenstaand

beschreven wijze. Bij AA stuurt de terminal een willekeurige boodschap naar de chip en vraagt de chip deze te tekenen. Met de publieke sleutel kan de terminal deze handtekening controleren en daarmee de authenticiteit van de chip vaststellen. CA werkt wat subtieler en lijkt op SAT: de terminal probeert een beveiligde tunnel op te zetten met behulp van de CA publieke sleutel. Dit is enigszins vergelijkbaar met het opzetten van een TLS sessie met een website. Het feit dat dit lukt, betekent ook dat de chip authentiek is. Een essentieel verschil tussen AA en CA is dat CA een nieuwe beveiligde tunnel opbouwt en AA niet. Qua rekenintensiteit zijn AA en CA vergelijkbaar. Als men CA combineert met BAC/BAP heeft dit het voordeel dat de BAC/BAP gebaseerde tunnel wordt vervangen door de CA gebaseerde tunnel. Anders dan de sterkte van de BAC/BAP tunnel is de sterkte van de CA tunnel wel in lijn met de gangbare normen. Zie Sectie D.2.

Als AA of CA succesvol zijn afgesloten, kan de terminal de relevante datagroepen met persoonsgegevens en de gelaatsfoto lezen en vervolgens de authenticiteit daarvan vaststellen op eerder beschreven wijze. Dat wil zeggen, na lezing van de datagroep moet de hash worden berekend en vergeleken met de versie aanwezig in de SOD.

D.2. Beveiligingskwaliteit van de WID document protocollen

De protocollen BAC/BAP zijn gebaseerd op een conventioneel three-pass-protocol gebaseerd op een gemeenschappelijke cryptografische sleutel afgeleid van de bovengenoemde drie gegevens: het WID documentnummer, de verloopdatum van het document en de geboortedatum van de houder. Nadat de chip vastgesteld heeft dat de terminal kennis heeft van deze gegevens wordt de afgeleide sleutel gebruikt voor een end-to-end tunnel tussen terminal en chip. Deze tunnel beschermt zowel de vertrouwelijkheid als authenticiteit van het verkeer.

Door deze opzet is de veiligheid van de BAC/BAP protocollen sterk afhankelijk van de onvoorspelbaarheid van deze drie gegevens. Een aanvaller die een BAC/BAP gebaseerde uitlees sessie kan onderscheppen zou middels het raden van deze drie gegevens (‘brute force) de sleutel kunnen bepalen en vervolgens de uitgelezen persoonsgegevens vergaren. Hoewel Nederlandse WID documenten specifieke aandacht aan deze kwestie hebben gegeven[5] kan gesteld worden dat de kwaliteit van de BAC/BAP sleutels niet de gangbare beveiligingsnorm van 128 bits halen, cf. [NIST-KEY]. In de opzet geschetst in Sectie 2.2 leest de authenticatiedienst de chip uit over een tweezijdige TLS verbinding tussen App en authenticatiedienst. De zwakheid van de BAC/BAP speelt daarbij dus alleen parten als de App niet vertrouwd kan worden, hetgeen daarmee al een afgeleid risico is.

Om zo min mogelijk afhankelijk te zijn van de App betrouwbaarheid moet, indien mogelijk, de BAC/BAP kwetsbaarheid worden gemitigeerd. Dit kan op twee manieren:

- De eerste manier bestaat uit het toepassen van Supplemental Acces Control (SAC) in plaats van BAC/BAP. Dit pakt de kwetsbaarheid in de kern aan. Bij SAC zetten zowel de terminal als de chip een veilig kanaal op mede op basis van de genoemde 3 gegevens. Daarna stellen terminal en chip vast dat ze ‘dezelfde’ tunnel hebben opgebouwd, hetgeen alleen het geval is als zij beide van dezelfde drie gegevens zijn uitgegaan. Uit een (on)succesvolle SAT gebaseerde uitlees sessie is het niet mogelijk om deze drie gegevens te brute-forcen. De enige mogelijke aanval is een actieve, waarbij een frauduleuze terminal alle mogelijkheden uitprobeert om succesvol een sessie met de chip op te zetten. Dit is in praktische zin niet

[5] Zie ook https://www.rijksoverheid.nl/documenten/kamerstukken/2007/04/10/antwoorden-op-kamervragen-over-biometrische-paspoorten .

mogelijk. Omdat SAC gebaseerd is op asymmetrische cryptografie (Diffie-Hellman) kost de toepassing hiervan substantieel meer tijd dan BAC/BAP dat symmetrisch van aard is.

- De tweede manier bestaat uit toepassen van Chip Authentication in plaats van Active Authentication. Dit vervangt immers de relatief zwakke BAC/BAP tunnel door de sterke CA tunnel. Een aanvaller kan dan in beginsel nog wel de drie gegevens achterhalen uit een onderschepte uitlees sessie tunnel maar daarin niet meer de uitgewisselde gegevens lezen. De aanvaller zou op een later moment met deze drie gegevens een nieuwe BAC/BAP tunnel opzetten en deze gegevens alsnog lezen. Maar omdat hiervoor de aanvaller contact moet kunnen maken met het WID document, is dit risico beperkt en in ieder geval beperkter dan de risico's rond het gebruik van BAC/BAP.

Bovenstaande twee punten zijn in Stap 21 vertaald in het vereiste om minimaal SAC of CA te gebruiken als deze aanwezig zijn.

E. Bijlage: Belangrijkste risico's en mitigerende maatregelen

#	Risico	Mitigatie
1.	De persoon is onvoldoende geïnformeerd over de voorwaarden van de authenticatiedienst waaronder zijn verplichtingen. Hierdoor kan deze onjuist met zijn authenticatiemiddel omgaan waardoor schade ontstaat.	• De persoon wordt op de hoogte gebracht over voorwaarden en verplichtingen en moet de persoon deze expliciet accepteren.
2.	Bij een mogelijke fraude kan de persoon niet tijdig worden bereikt door de authenticatiedienst.	• Dit is de grondslag van de minimale set van contactgegevens. Daarbij zal ook aandacht worden gegeven aan de correctheid van deze gegevens.
3.	De prospect gebruiker wordt niet onder eigen identiteit geregistreerd maar onder die van een andere persoon. Dit kan per ongeluk gebeuren (identiteit verwisseling) maar ook moedwillig (identiteit fraude).	• Ter voorkoming van identiteit verwisseling moeten de geregistreerde gegevens de persoon uniek vastleggen; dit is de grondslag van de minimale set persoonsgegevens. • Ter voorkoming van identiteit fraude moeten het WID document en de daarop geregistreerde gegevens gevalideerd worden door de authenticatiedienst. Essentieel daarbij is de vergelijking met de gelaatsfoto waarbij specifiek aandacht moeten worden besteed aan look-alike fraude. Hierbij presenteert een fraudeur een gestolen WID document van een persoon die op hem lijkt. • Het gebruik van de digitale foto van de WID document chip stelt de authenticatiedienst in staat de vergelijking beter uit te voeren. • De voorgeschreven iDEAL transactie beperkt de fraudeur in zijn look-alike mogelijkheden.
4.	De gebruiker wordt door een fraudeur middels *social engineering* verleid bepaalde zaken te doen niet wetende daarmee zichzelf te laten registreren bij een authenticatiedienst. Dit speelt bijvoorbeeld bij het gebruik van iDEAL ter identificatie: de gebruiker denkt bijvoorbeeld een prijsgunstige aankoop te doen in plaats van een identificatie.	• Binnen het gebruik van iDEAL is expliciete aandacht gegeven om de gebruiker te waarschuwen tegen *social engineering*. • De challenge-response video binnen de App context voorziet in het vragen van expliciet consent aan de gebruiker voor de registratie.
5.	Een medewerker van een authenticatiedienst voert een frauduleuze registratie en verstrekking uit en realiseert dat de App op naam van een gebruiker onder zijn controle komt.	• Het validatie proces door een medewerker kan pas worden gestart nadat het iDEAL proces succesvol is afgerond. Hier heeft de medewerker geen controle op. • Alle activiteiten gedurende het proces worden gelogd (generieke eis).
6.	De gebruikersomgeving is door een fraudeur voorzien van malware ('man-in-the-browser') die nadat de iDEAL	• De vereiste activiteiten binnen de App, met name de challenge-

	transactie succesvol is afgerond: • de App registratie/activatie overneemt en de gebruiker op een dwaalspoor zet, of • de gebruiker naar een *rogue* App leidt die tussen de echte App zit die de fraudeur heeft geïnstalleerd: de gebruiker voert binnen de rogue App alles uit wat de echte App vereist en na afronding beschikt de fraudeur over een App geregistreerd op de naam van de gebruiker.	response video, binden de App aan de gebruiker. • De authenticatiedienst is verplicht de Appstores te inspecteren op *rogue* Apps, i.e. Apps die suggeren afkomstig te zijn van de authenticatiedienst.
7.	Bij het uitlezen van de WID document chip via de UitleesApp op andermans device komen de digitale gegevens via deze App in verkeerde handen.	• De UitleesApp en in feite het device krijgt geen beschikking over deze gegevens omdat er een end-to-end tunnel wordt opgebouwd tussen authenticatiedienst en WID document.
8.	De App zou kunnen worden gecorrumpeerd of worden gekopieerd.	• In Sectie 2.3 wordt een aantal concrete eisen rond de App geformuleerd waaronder het uitvoeren van een penetratietest op de App door de authenticatiedienst.