



RDW

Evaluatierapport pilot DigiD-RDA

DigiD versterkt met controle van het identiteitsbewijs

Doelstelling pilot DigiD versterkt met Remote Document Authentication (DigiD-RDA):

1. overheidsdienstverlening te ontsluiten die hogere betrouwbaarheid vereist;
2. snel een oplossing te bieden o.b.v. middelen die al breed beschikbaar zijn;
3. aan te tonen dat de oplossing technisch mogelijk is;
4. ervaring op te doen ten behoeve van het publieke eID-middel.

Opdrachtgever	Hans van Santen
Auteur	Herman Mulder
Versie	1.0
Versiedatum	23-05-2016



Versie informatie

Versie	Datum	Bijzonderheden	Auteur
0.1	17-05-2016	Interne notitie met inhoud ter 1e afstemming	Herman Mulder
0.2	18-05-2016	Revisie-opmerkingen op inhoud verwerkt	Herman Mulder
0.3	18-05-2016	Teksten externe notitie tbv commissie	Herman Mulder
0.4	19-05-2016	Eerste conceptrapport	Herman Mulder
0.5	19-05-2016	Samenvatting & review Logius verwerkt	Herman Mulder
0.6	19-05-2016	Vigerend i.v.m. laatste reviewopmerkingen	Herman Mulder
1.0	23-05-2016	Eindversie voor commissie Kuipers	Herman Mulder

Verzendlijst

Rol/ Functie	Naam	Versie
Reviewers RDW	Jetske ten Brug, Auke van der Meulen, Anke Meijer, Marije Stam	0.1, 0.3, 0.5, 1.0
Evaluatiecommissie	Commissie Kuipers	0.4, 0.5, 1.0
Directie RDW	Hans van Santen	0.5, 1.0
Ministerie van IenM	Petra de Roover	0.4, 0.6, 1.0
Logius	Nico van der Neut, Matthijs Claessen, Diepak Atwaroe, Winfried de Valk (cc)	0.4, 0.5, 1.0
BZK	Marc Gerrard (cc)	0.4, 0.5, 1.0



Inhoudsopgave

Samenvatting	4
1 Inleiding	5
2 Beschrijving Pilot	5
3 Werking RDA op hoofdlijn	6
4 Uitkomsten pilot gerelateerd aan de doelstellingen	9
5 Gebruikerservaringen.....	10
6 Betrouwbaarheid en veiligheid	11
7 Leerpunten & aanbevelingen RDW.....	13
8 Bijlagen	
Betrouwbaarheidsonderzoek van PWC naar RDA	
Privacy-impactanalyse uitgevoerd door PWC naar RDA	
Presentatie 11 april 2016 tijdens bezoek commissie aan Veendam	
Memo verschil publiek eID-middel op rijbewijs/NIK en RDA	

Samenvatting

Naast de pilots met Idensys, iDIN en publieke eID-middelen, loopt er een vierde pilot, waarbij tijdens het inloggen met een bestaand DigiD account het betrouwbaarheidsniveau wordt ‘opgewaardeerd’. Daarbij wordt aansluitend aan het inloggen met DigiD een extra controle uitgevoerd aan de hand van niet-zichtbare NFC¹-chips in bestaande paspoorten, identiteitskaarten en rijbewijzen. Deze techniek wordt Remote Document Authentication (RDA) genoemd.

Elk geldig paspoort en identiteitskaart (ook het oudste in omloop zijnde model), uitgereikt door een gemeente, heeft al een NFC-chip. En rijbewijzen afgegeven na 13 november 2014. Praktisch elke Nederlander die DigiD gebruikt heeft dus een ‘RDA geschikt’ identiteitsdocument.

Tijdens de pilot is aangetoond dat de RDA-techniek werkt, bestand is tegen aanvallers² en DigiD aan een hoger betrouwbaarheidsniveau³ kan helpen om bestaande en nieuwe diensten te ontsluiten. Zo hebben tijdens de pilot 430 unieke burgers RDA gebruikt om online een voertuig over te schrijven. Zonder RDA hadden burgers nog naar een kentekenloket moeten gaan. In juni start een pilot in de zorgsector met medicijngebruik. De pilot is pas sinds april 2016 onder een breder publiek aangeslagen op het moment dat er een nieuwe release is uitgebracht. Waarbij naast NFC-USB-kaartlezers ook NFC-smartphones kunnen worden gebruikt (nu nog beperkt tot Android-toestellen). Wij schatten in dat daardoor op dit moment tenminste 3 miljoen burgers een voertuig online zouden kunnen overschrijven. Met DigiD en een extra controle van de chip in hun identiteitsdocument via de NFC-antenne in hun Android smartphone.

Om Logius te ontlasten is de RDA-pilot technisch als een ‘add-on’ gebouwd: er hoefde niets in de DigiD-infrastructuur van Logius te worden aangepast. Via een bewerkersovereenkomst tussen Logius en RDW, die tot eind 2016 loopt, draait er bij de RDW een RDA-service. Om het gebruikersvriendelijker te maken voor een breder deel van de bevolking, is integratie in de DigiD-infrastructuur sterk aan te bevelen. In juni 2016 wordt de DigiD-app van Logius, die al in kleine kring is beproefd, onder een breder publiek beschikbaar gesteld. Het is de bedoeling dat die Q4 voor alle burgers beschikbaar komt. Op dit moment voert Logius een impactanalyse uit om de functionaliteit van de ‘RDA Lezer’-app te integreren in een toekomstige versie van de DigiD-app. In de impactanalyse worden tevens de aanbevelingen meegenomen ten aanzien van eIDAS ‘substantieel’, wat we burgers bieden die geen NFC-geschikte smartphone hebben (die kunnen desgewenst een losse USB-NFC-kaartlezer kopen), hoe de investering en exploitatiekosten beperkt kunnen worden gehouden en hoe het tijdpad voor deze integratie eruit ziet. De RDA-techniek komt met integratie in de DigiD app beschikbaar voor alle dienstverleners die al op DigiD zijn aangesloten.

Bij een positief besluit over doorontwikkeling binnen de Logius infrastructuur, worden op relatief korte termijn en tegen relatief beperkte investeringen en exploitatiekosten bereikt:

1. ontsluiting van overheidsdienstverlening die hogere betrouwbaarheid vereist,
2. een logisch groeipad o.b.v. middelen die al breed beschikbaar zijn,
3. het bieden van een oplossing die technisch relatief snel is te realiseren,
4. overbrugging naar en voorbereiding op de volgende generatie publiek eID-middel.

¹ NFC staat voor ‘near field communication’

² Penetratietesten door daarin gespecialiseerde, externe bureaus.

³ Drietal externe onderzoeken naar betrouwbaarheidsniveau, privacy (PIA) en gerichte risicoanalyse.

1 Inleiding

Naast de drie pilots Idensys, iDIN en publiek eID-middel op specimen rijbewijs en eNIK, loopt een vierde pilot waarbij tijdens het inloggen met DigiD een extra controle wordt uitgevoerd aan de hand van niet-zichtbare NFC-chips in bestaande paspoorten, identiteitskaarten en rijbewijzen. Deze controle wordt Remote Document Authentication (RDA) genoemd. Dit document beschrijft de ervaringen van deze pilot, ten behoeve van de besluitvorming van BZK en het Kabinetsvoorstel. De uitkomsten worden per doelstelling uitgewerkt. Zowel de gebruikerservaringen als de betrouwbaarheid en veiligheid zijn beschreven. Hierbij zijn zoveel mogelijk de vragen zoals TNO en Panteia die hebben gehanteerd, gevolgd.

2 Beschrijving Pilot

De doelstellingen van de pilot waren vierledig:

1. overheidsdienstverlening te ontsluiten die hogere betrouwbaarheid vereist;
2. snel een oplossing te bieden o.b.v. middelen⁴ die al breed beschikbaar zijn;
3. aan te tonen dat de oplossing technisch mogelijk is;
4. ervaring op te doen ten behoeve van het publieke eID-middel.

Door middel van RDA wordt aan het huidige DigiD een controle toegevoegd die het betrouwbaarheidsniveau verhoogt. Gerelateerd aan de doelstellingen van Idensys biedt deze versterking geen oplossing voor de afhankelijkheid van DigiD, maar biedt het wel een hoger niveau van betrouwbaarheid. Het kan desgewenst als een terugvaloptie c.q. alternatief dienen voor het geval dat een burger (bijvoorbeeld wegens vermissing) niet beschikt over een (nieuw) eID-middel. De doelstelling van de pilot is het beproeven van RDA als extra toegangscontrole voor dienstverleners die gebruik mogen maken van DigiD.

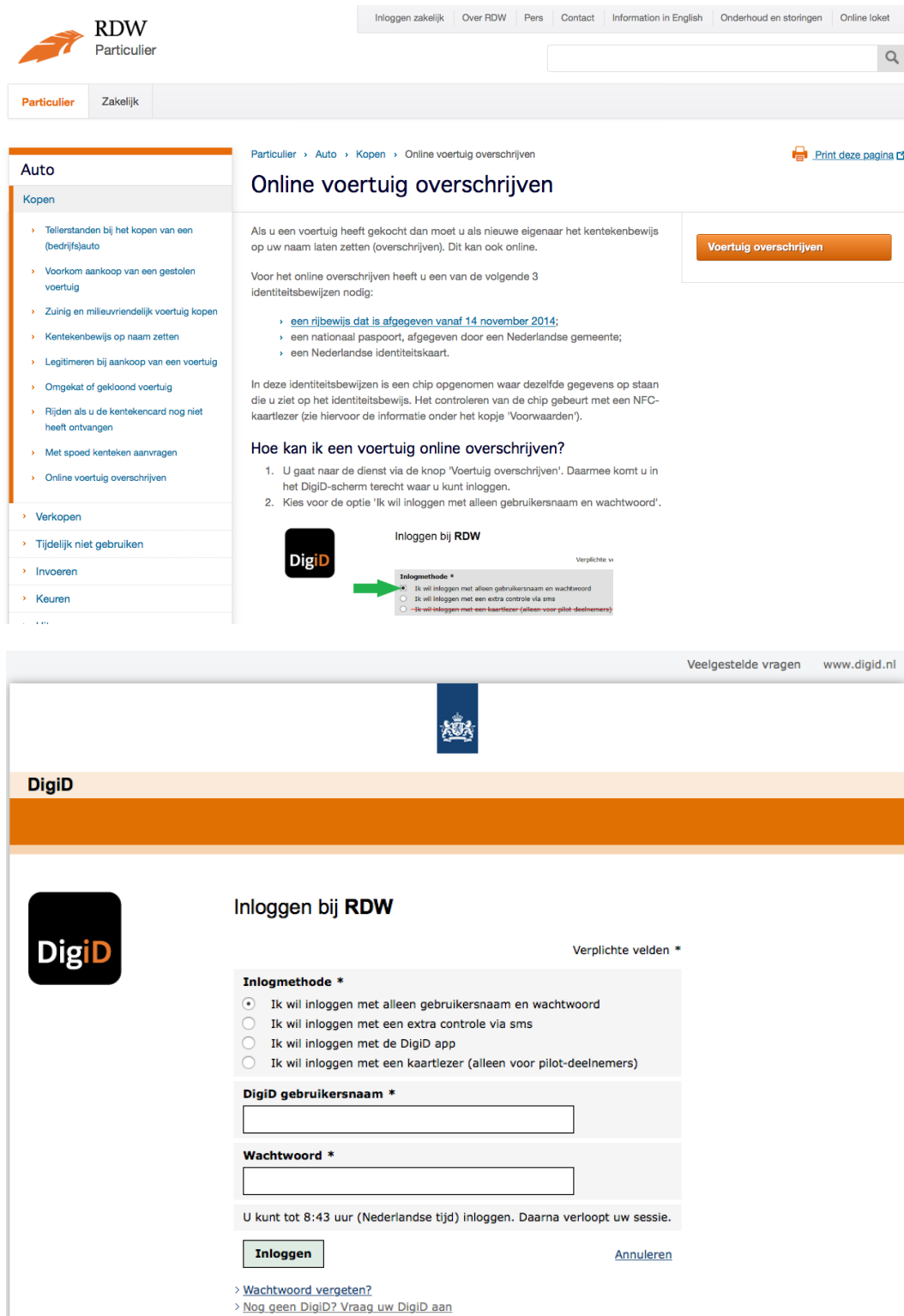
Logius hoefde voor de pilot niets in de infrastructuur aan te passen. De RDW host tijdelijk via een bewerkersovereenkomst met Logius een zogenaamde RDA service. De eerste dienst die in september 2015 achter RDA in productie beschikbaar is gekomen is de dienst “Online voertuig overschrijven”: een particulier kan een voertuig op zijn eigen naam zetten. In oktober 2015 is een tweede RDW-dienst ontsloten: “Mijn voertuigen bekijken”. Vervolgens is gewerkt aan ondersteuning van meer platforms (naast Windows ook Apple, variëteit aan browsers) en aan een app die de inzet van een smartphone als NFC-kaartlezer mogelijk maakt. In april 2016 is de app in de Google Play store opgenomen onder de naam ‘RDA Lezer’.

Diverse organisaties in het BSN-domein hebben laten weten de RDA-service ook te willen uitproberen, zodra een smartphone-app beschikbaar is. Andere organisaties zijn betrokken dan wel worden geconsulteerd bij een of meer componenten van de realisatie. Zoals BZK, Logius, RvIG, IenM, DUO, Belastingdienst, VZVZ, SURFnet en marktspecialisten. De ontwikkeling en het beheer van de RDA-service en de coördinatie van de pilots die met RDA worden gedaan, vallen tijdens de pilotfase (tot eind 2016) onder de aansturing van de RDW. Logius is vanaf het begin betrokken. Om bij positieve besluitvorming over voortzetting de overdracht zo snel mogelijk te kunnen realiseren. Tot die tijd wordt de samenwerking bestuurlijk geregeld via een bewerkersovereenkomst. Zodra voldoende ervaring is opgedaan is het aan de Minister van BZK om te bepalen of en hoe hij tot versterking van DigiD met de RDA-methodiek wil overgaan.

⁴ Onder breed beschikbare middelen worden naast paspoort, identiteitskaart en rijbewijs, ook smartphone, DigiD en bestaande koppelingen van overheidsdiensten aan DigiD bedoeld.

3 Werking RDA op hoofdlijn

In een websessie op bijvoorbeeld een PC of Mac wil een burger toegang tot een online overheidsdienst zoals 'Online voertuig overschrijven'. De dienst vraagt die burger dan eerst om in te loggen met zijn DigiD-account:



The screenshot shows the RDW website interface. At the top, there is a navigation bar with links: 'Inloggen zakelijk', 'Over RDW', 'Pers', 'Contact', 'Information in English', 'Onderhoud en storingen', and 'Online loket'. Below this is a search bar. The main content area is titled 'Online voertuig overschrijven' and includes a sidebar with a list of services under the 'Auto' category. The main text explains the process of online vehicle registration and lists the required documents. A 'Voertuig overschrijven' button is visible. Below the main text, there is a section titled 'Hoe kan ik een voertuig online overschrijven?' with two steps. A DigiD logo is shown next to the login instructions. The bottom part of the screenshot shows the DigiD login screen with the title 'Inloggen bij RDW' and a list of login methods. The login form includes fields for 'DigiD gebruikersnaam' and 'Wachtwoord', and a button to 'Inloggen'. There are also links for 'Wachtwoord vergeten?' and 'Nog geen DigiD? Vraag uw DigiD aan'.

RDW Particulier

Particulier > Auto > Kopen > Online voertuig overschrijven

Online voertuig overschrijven

Als u een voertuig heeft gekocht dan moet u als nieuwe eigenaar het kentekenbewijs op uw naam laten zetten (overschrijven). Dit kan ook online.

Voor het online overschrijven heeft u een van de volgende 3 identiteitsbewijzen nodig:

- > een rijbewijs dat is afgegeven vanaf 14 november 2014;
- > een nationaal paspoort, afgegeven door een Nederlandse gemeente;
- > een Nederlandse identiteitskaart.

In deze identiteitsbewijzen is een chip opgenomen waar dezelfde gegevens op staan die u ziet op het identiteitsbewijs. Het controleren van de chip gebeurt met een NFC-kaartlezer (zie hiervoor de informatie onder het kopje 'Voorwaarden').

Hoe kan ik een voertuig online overschrijven?

1. U gaat naar de dienst via de knop 'Voertuig overschrijven'. Daarmee komt u in het DigiD-scherm terecht waar u kunt inloggen.
2. Kies voor de optie 'Ik wil inloggen met alleen gebruikersnaam en wachtwoord'.

Inloggen bij RDW

Verplichte velden *

Inlogmethode *

- ☒ Ik wil inloggen met alleen gebruikersnaam en wachtwoord
- ☐ Ik wil inloggen met een extra controle via sms
- ☐ Ik wil inloggen met de DigiD app
- ☐ Ik wil inloggen met een kaartlezer (alleen voor pilot-deelnemers)

DigiD gebruikersnaam *

Wachtwoord *

U kunt tot 8:43 uur (Nederlandse tijd) inloggen. Daarna verloopt uw sessie.

Inloggen Annuleren

> Wachtwoord vergeten?

> Nog geen DigiD? Vraag uw DigiD aan

Hierna volgt een extra controle middels het hem door de overheid uitgereikte identiteitsbewijs:

[Veelgestelde vragen](#) www.digid.nl



DigiD



Inloggen met controle identiteitsbewijs

i Voor deze dienst is een controle van uw identiteitsbewijs vereist.

Verplichte velden *

Als extra controle gebruik ik mijn Nederlandse:*
☐ Identiteitskaart
☐ Paspoort
☒ Rijbewijs (afgegeven vanaf 14-11-2014)

Selecteer uw NFC-kaartlezer:*
☐ USB NFC-kaartlezer
☒ Smartphone met NFC

Door uw identiteitskaart, paspoort of rijbewijs op de NFC-kaartlezer te leggen of tegen de achterkant van uw smartphone met NFC aan te houden verleent u toestemming voor het vaststellen dat het document van u is en ook geldig. Daartoe worden van u uw BSN en geboortedatum verwerkt en van uw identiteitsdocument het nummer, de vervaldatum en de inhoudsinformatie.

Privacyverklaring
[Bekijk hier de privacyverklaring Controle Identiteitsbewijs](#)

[Annuleren](#)

Er verschijnt nu een QR-code in de websessie.

[Veelgestelde vragen](#) www.digid.nl



DigiD



Scan uw QR-code





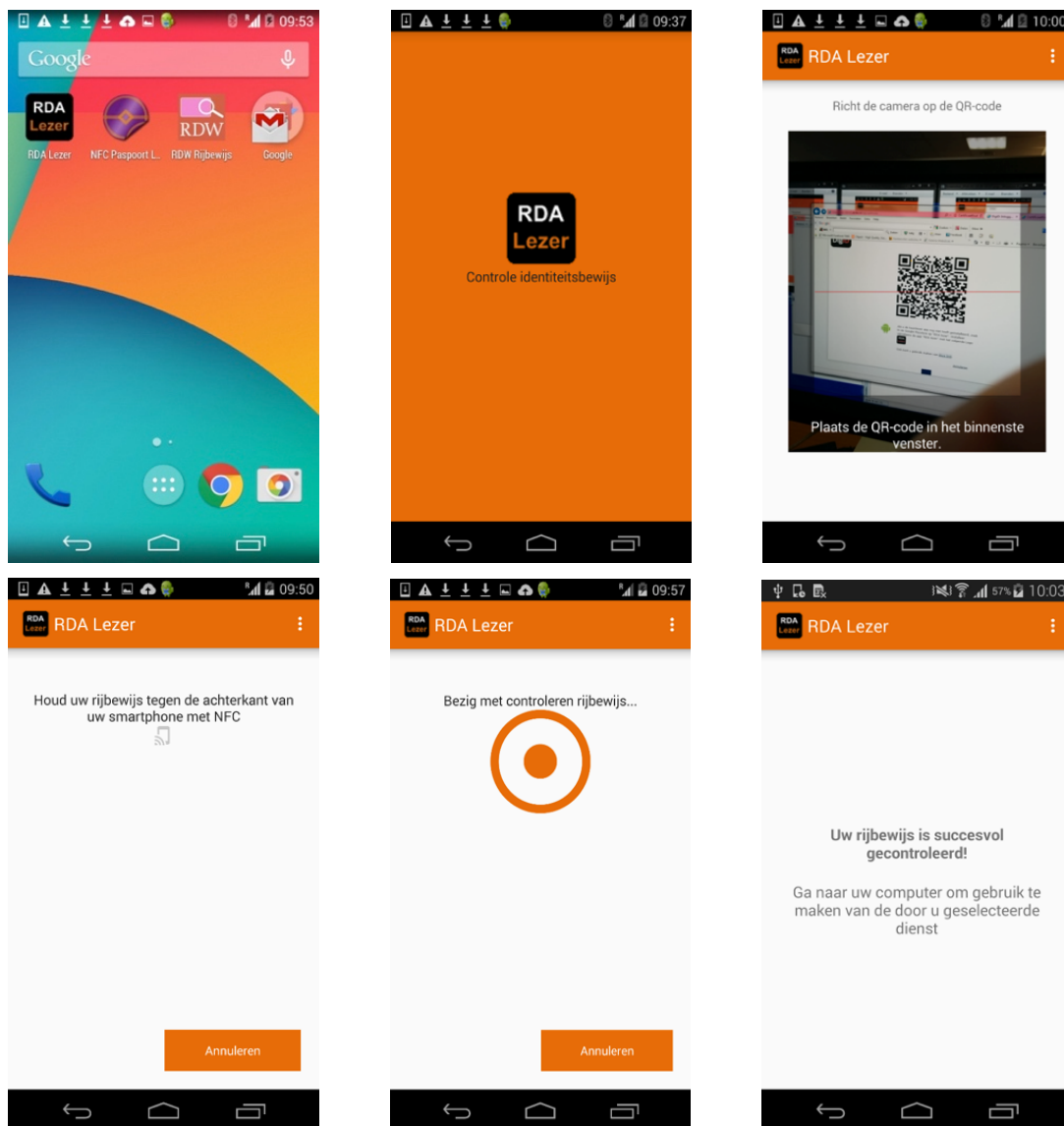
Als u de kaartlezer app nog niet heeft geïnstalleerd, zoek in de Google Playstore op "RDA lezer". Installeer vervolgens de app "RDA lezer" met het volgende Logo



Ook kunt u gebruik maken van [deze link naar de Google Playstore](#).

[Annuleren](#)

De camera in een NFC-Android-smartphone, waarop de 'RDA Lezer'-app uit de Google Play Store is geïnstalleerd, scant de QR-code. De app leidt de burger door de handelingen.



De authenticiteit en geldigheid van de chip in het tegen de telefoon gehouden identiteitsbewijs wordt gecheckt tegen overheidsregisters. Bij akkoord krijgt de burger toegang tot de dienst:



RDW

U bent ingelogd als: Herman Mulder

 Uittloggen

Voertuig online overschrijven

Invoeren aanvraag 	Akkoord	Betaling	Bevestiging
---	----------------	-----------------	--------------------

4 Uitkomsten pilot gerelateerd aan de doelstellingen

1. *Overheidsdienstverlening ontsluiten die hogere betrouwbaarheid vereist*
Tot en met 21 mei 2016 hebben 455 burgers succesvol met DigiD-RDA online een voertuig overgeschreven op hun naam (€ 9,91). Deze dienst had zonder RDA niet ‘live’ kunnen gaan, omdat het dan aan een voldoende betrouwbaar authenticatiemiddel had ontbroken, die binnen de huidige wet- en regelgeving past. Burgers vonden hun weg zonder publiciteitscampagne en zonder toezending van instructies. Daarmee spaarden ze de gang naar een kentekenloket (veelal postkantoor) uit. Het is gaan lopen sinds de RDW 7 april jl. een speciale ‘RDA Lezer’-app beschikbaar stelde voor Android-smartphones met Near Field Communication (NFC). De robuustheid tegen ‘aanvallers’ is vastgesteld middels penetratietesten door twee hierin gespecialiseerde bedrijven. Dat er voldaan is aan het benodigde betrouwbaarheidsniveau (STORK 3) is extern door PwC getoetst⁵. De belangrijkste aanbeveling van PwC om straks ook aan eIDAS-substantieel te voldoen is de inrichting van een 7x24 uur overheidservice om de vermissing van een identiteitsdocument te melden. Aan de andere drie aanbevelingen van PwC⁵ is inmiddels invulling gegeven.
2. *Snel een oplossing bieden o.b.v. middelen die al breed beschikbaar zijn*
Elke burger die een DigiD-account en een geldig paspoort of identiteitskaart heeft, kan RDA gebruiken. Ook het rijbewijs kan worden gebruikt, mits dat is afgegeven na 13 november 2014. Burgers hebben een Android smartphone nodig met NFC om de chip in zo’n identiteitsbewijs te laten controleren. Alleen Samsung bereikt met haar meest verkochte modellen in Nederland hiermee al ruim 2,7 miljoen burgers. Daar komen de aantallen van de andere Android-merken nog bovenop. Apple levert NFC mee sinds de iPhone 6(S)-serie en in modernere iPad’s en Applewatch, maar heeft de techniek nog niet ‘open’ gesteld voor toepassingen anders dan Apple Pay. Burgers die geen geschikt Android toestel hebben kunnen een losse USB-NFC-kaartlezer kopen en gebruiken. Bij eerste gebruik van een ‘RDA-dienst’ installeert zich daartoe na toestemming van de gebruiker vanzelf de benodigde functionaliteit in een internetbrowser.
3. *Aantonen dat de oplossing technisch mogelijk is*
De RDW heeft eerst als ‘proof of concept’ een basisoplossing beschikbaar gesteld. Gezien de veelheid aan platformen, operating systems, browsers en versies van dit alles is daarna besloten de oplossing door te ontwikkelen en deze op een marktoplossing te baseren. Te meer omdat daarmee direct ook de stap naar smartphones als ‘kaartlezer’ kon worden gemaakt. De gebruikerservaring is daarmee fors verbeterd. Randvoorwaardelijk voor de pilot was dat Logius in de DigiD-infrastructuur voor de RDA-pilot niets hoefde aan te passen. Om met RDA bij willekeurige overheidsdienst in te kunnen loggen is bij landelijke invoering nog wel een aanpassing aan de zijde van Logius in de DigiD-infrastructuur nodig. Ook raken nu nog ‘RDA-inloggers’ op de DigiD-pagina in verwarring. Na integratie van de RDA-service binnen de infrastructuur van Logius kan met RDA bij alle ruim 800 DigiD-diensten worden ingelogd zonder dat de betreffende overheidsdienst zelf iets heeft aan te passen. En wordt het voor burgers vanzelfsprekend wanneer het identiteitsbewijs ter extra controle moet worden aangeboden.

⁵ Zie de afzonderlijk beschikbaar gestelde rapportage betrouwbaarheidsniveau eIDAS en STORK voor DigiD in combinatie met RDA van PWC.

4. *Ervaring op te doen ten behoeve van het publieke eID-middel*

Ook bij het publieke eID-middel moet met een chip door middel van NFC-technologie worden gecommuniceerd. Zowel voor de overheid, als voor burgers, is het opdoen van ervaring met NFC-technologie belangrijk. Als overheid moeten we zicht hebben op de technisch benodigde en eventueel te verwerven componenten. Burgers willen bij vervanging van devices tijdig rekening kunnen houden met en gevoel kunnen krijgen bij wat dit voor hen betekent. De pilot met RDA leert een ieder veel.

5 Gebruikerservaringen

1. Grootste verschil qua pilotopzet met eID, iDIN en Idensys-pilots is dat burgers voor deelname aan de pilot niets vooraf hoeven aan te vragen of te activeren. RDA wordt geactiveerd en gebruikt op het moment dat een burger het écht nodig heeft. Zonder extra handelingen vooraf (behoudens download van de ‘RDA Lezer’-app). Met een concrete ‘noodzaak’ en ‘aanleiding’: het op zijn naam zetten van een voertuig. Dit verklaart ook waarom burgers noch vooraf een extra instructie kon worden toegestuurd, noch achteraf een evaluatielink. Personen die een voertuig hebben gekocht hebben namelijk de plicht onverwijld het voertuig op hun naam te zetten. Die gaan zich niet eerst voor een pilot aanmelden. Andersom ook: we kunnen burgers niet in het kader van een pilot vragen een voertuig aan te kopen en op hun naam te zetten.
2. Tot nog toe hebben 430 unieke burgers spontaan RDA gebruikt om een voertuig op hun naam te zetten. Het gebruik van de dienst is gaan lopen sinds 1,5 maand geleden de ‘RDA Lezer’-app is gelanceerd. Opvallend zijn de pieken in gebruik op zon- en feestdagen. Er zit een stijgende lijn in het gebruik. Op dit moment gemiddeld 14 geslaagde voertuigoverschrijvingen per dag met uitschieters boven de 20.
3. Omwille van privacy is op aangeven van de auditor de verwerking van burgergegevens tijdens inlogtransacties geminimaliseerd en daardoor niet bruikbaar voor evaluatiedoel-einden. Om toch wat gebruikerservaring te verkrijgen heeft de RDW aanvullend een oproep gedaan aan RDW-medewerkers om in te loggen met RDA. Door bij een tweede RDW-dienst eigen voertuiggegevens te raadplegen. Het aantal interne gebruikerservaringen (89 geïnteresseerden, 37 zijn begonnen de online enquête in te vullen, 29 hebben de enquête afgerond) is niet representatief. Mede doordat we ook spontane feedback van externe gebruikers kregen, valt er inhoudelijk wel voorzichtig enig beeld te geven qua ervaring:
 - a. In de regel verloopt de installatie van browserfunctionaliteit op een PC/Mac en de Android-app met de huidige RDA-release goed.
 - b. Wellicht omdat nog niet in elk rijbewijs een chip zit, wordt op dit moment vaker het paspoort gebruikt om in te loggen.
 - c. De huidige tekst op de DigiD-inlogpagina kan RDA-gebruikers momenteel op het verkeerde been zetten. De onderste keuze-optie “Ik wil inloggen met een kaartlezer (alleen voor pilotdeelnemers)” kan namelijk alleen worden gebruikt door pilotdeelnemers *eID*. Bij positief besluit over RDA lost Logius dit op bij de integratie van RDA in de eigen infrastructuur.
 - d. Gebruikers ervaren het inloggen met een extra controle op het identiteitsbewijs als veiliger dan met DigiD-basis en een redelijke tot zeer goede manier om in de toekomst in te loggen.
 - e. Er zijn wat kleinere storingen geweest. Door:
 - Het uitwisselen van zogenaamde ‘CRL-bestanden’ tussen RvIG en RDW (nieuwe ‘releases’ eens per kwartaal) gaat tijdens de pilot nog handmatig

waardoor 2x iets mis liep en er met bepaalde paspoorten en identiteitskaarten tijdelijk niet kon worden ingelogd.

- GBA-V heeft er een keer uitgelegd waardoor de check op geldigheid (en vermissing/intrekking) aangeboden paspoort en identiteitskaart niet mogelijk was. Tijdelijk kon men niet inloggen.
- Niet ondersteunde browserversies (in de aanloop, verholpen).
- Nieuwste Android-versie bleek niet te werken. Is verholpen.

6 Betrouwbaarheid en veiligheid

1. *Wordt voldaan aan de afgesproken eisen die verwoord staan in de gebruiksvoorwaarden van DigiD?* Meer dan dat: de gebruiksvoorwaarden zijn voor RDA aangevuld en aangescherpt om aan bevindingen te voldoen die uit de PIA naar voren kwamen.
2. *Voldoet de technische voorziening van Logius en RDW aan de BIR?* Extern onderzoek voor RDA loopt nog. Rapport wordt deze maand verwacht.
3. *Voldoen de ICT-componenten aan de gestelde technische veiligheidseisen en privacy-eisen?* Voor zowel de initiële als definitieve oplossingen zijn penetratietests uitgevoerd. Er is een PIA uitgevoerd door PwC⁶ waaruit aanbevelingen zijn gekomen. De aanbevelingen zijn als volgt opgepakt:
 - a. De privacyverklaring op de website van DigiD (bij Logius dus) is uitgebreid met RDA en rol RDW.
 - b. Op de RDW-inlogpagina staat nu een link naar de privacyverklaring zoals genoemd onder punt 3.a.
 - c. Privacygevoelige gegevens zijn verwijderd uit een aanvullende logging die werd gedaan om bij potentiële security-incidenten gericht actie te ondernemen.
 - d. Er is een bewaartermijn vastgesteld en gepubliceerd van de gegevens die worden verwerkt.
 - e. De gebruiker wordt inmiddels beter en vollediger geïnformeerd over zijn gegevens die worden verwerkt dan in de basisversie.
 - f. De gebruiker wordt inmiddels geïnformeerd over risico's. En maatregelen die hij zelf kan treffen om zijn identiteit tegen misbruik te beschermen.
 - g. Bij het ministerie van IenM loopt een verzoek tot aanvulling van het Reglement Rijbewijzen dat generiek borgt dat per 1/1/2017 Logius gegevens uit het rijbewijsregister kunnen worden verstrekt ten behoeve van haar authenticatie-taak binnen de overheid.
 - h. Er is een nieuw document gemaakt waarin alle koppelvlakken tussen systeemcomponenten bijeen zijn gebracht en welke gegevens tussen die componenten worden uitgewisseld zodat dit inzichtelijker is voor o.a. toezicht.
4. *In welke mate zijn dienstaanbieders en andere betrokkenen duidelijk geïnformeerd over het doel van de pilot, de gegevens en het gebruik tijdens de pilot?* Dienstaanbieders behoefden niet in de volle breedte te worden geïnformeerd omdat het vooralsnog RDW-eigen diensten betreft. Wel zijn dienstaanbieders via het DigiD-afnemersoverleg geïnformeerd en zijn geïnteresseerden uitgenodigd in een Klankbordgroep zitting te nemen. De Klankbordgroep is diverse malen bijeen geweest. Voor de RDA-pilot zijn primair burgers betrokkenen. De privacyverklaring van DigiD is aangevuld ten behoeve van de voor RDA te verwerken gegevens. De RDA-pagina heeft een link naar een uitgebreide 'Veelgestelde vragen' pagina. Met gebruikersvoorwaarden, hoe de controle werkt, pri-

⁶ Zie de afzonderlijk beschikbaar gestelde rapportage PIA DigiD met RDA van PwC

vacy-informatie, kaartlezers, smartphones, de software die zich in de browser installeert (SConnect), wat men zelf aan veiligheid kan doen etc.

5. *Zijn er issues opgetreden op het gebied van aansprakelijkheid bij de burger?* Nee. Bij de betreffende dienst zou dat hebben geleid tot een melding van een burger dat hij onterecht een voertuig op naam heeft gekregen. Die trekt direct aan de bel als hij onterecht een kentekencard thuis krijgt op zijn naam, een vrijwaringsbewijs in zijn berichtenbox krijgt, wegenbelasting moet gaan betalen of brieven over WA-verzekering, APK etc krijgt van een voertuig dat niet in zijn bezit is. En waarbij kennelijk zijn authenticatiemiddel zou zijn misbruikt. In het proces zitten dusdanig veel signaalfuncties dat misbruik snel naar boven komt. Tot op heden is geen enkel signaal dat daarop wijst.
6. *Wat is de performance van de techniek?* Er zijn geen klachten over de performance. RDA gedraagt zich volgens verwachtingspatroon gebruikers.
7. *Welke aandachtspunten zijn er bij de techniek?*
 - a. Burgers hebben in de regel nog geen USB-NFC-kaartlezers.
 - b. Deze kaartlezers werken niet op alle devices, zoals tablets.
 - c. Om deze kaartlezers met alle operating-system-browser-configuraties te laten werken is zogenaamde 'middleware' nodig. Omdat dit een vak apart blijkt heeft de RDW bij de laatste release daar een licentie op genomen.
 - d. Smartphones als kaartlezer inzetten zal veel sneller tot brede invoering leiden. Helaas is dit nu nog beperkt tot Android. Totdat Apple ook zijn NFC 'open' zet voor gebruik door derden.
 - e. Logius wil RDA primair inzetten om de DigiD-app die eraan komt op te waarderen naar een hoger betrouwbaarheidsniveau. Hiertoe wordt door Logius momenteel een impactanalyse uitgevoerd. Daarbij is een van de scenario's zo snel mogelijk de losse, tijdelijke RDW pilotvoorziening voor RDA zodanig 'om te leiden', dat het functioneel al een geïntegreerd geheel vormt met de rest van de DigiD-infrastructuur. Opdat RDA voor DigiD-'afnemers' (overheidsdiensten) zonder verdere inspanning beschikbaar is via het standaard DigiD-'koppelvlak'. En de gebruikerservaring voor burgers wordt geoptimaliseerd.
 - f. Als het volume van de RDA-transacties toeneemt (door toename van online voertuigoverschrijvingen hetzij ontsluiting van nieuwe overheidsdiensten), moet mogelijk de capaciteit van de service worden opgeschaald.

7 Leerpunten & aanbevelingen RDW

1. Zodra er duidelijkheid is over (toetsingswijze aan) het Nederlandse stelsel en normenkader als doorvertaling van eIDAS, wordt aanbevolen opnieuw te toetsen of aan alle normen kan worden voldaan. Op dit moment blijken verschillende normenkaders en interpretaties te circuleren die tot verschillende wegingen en conclusies van deskundigen leiden. En omdat geen van de bureaus is geaccrediteerd of aangewezen om het betrouwbaarheidsniveau (van bijvoorbeeld RDA) officieel namens of voor de Nederlandse overheid vast te mogen stellen, is onduidelijk welke aanbevelingen randvoorwaardelijk zijn.
2. Zet in op versterking van het huidige DigiD vanaf 2017 tot op STORK 3 / eIDAS ‘substantieel’ door de huidige RDA-oplossing verder te integreren binnen de DigiD-infrastructuur. In juni 2016 wordt de DigiD-app van Logius, die al in kleine kring is beproefd, onder een breder publiek beschikbaar gesteld. Het is de bedoeling dat die in het vierde kwartaal van 2016 voor alle burgers beschikbaar komt. Op dit moment voert Logius een impactanalyse uit om de functionaliteit van de ‘RDA Lezer’-app te integreren in een toekomstige versie van die DigiD-app. Waarmee de losse ‘RDA Lezer’-app kan komen te vervallen. Burgers die daar aan hechten kunnen dan zelf hun digitale identiteit al meer beschermen (bewustwording), zoals burgers nu ook vrijwillig er voor kunnen kiezen dat altijd de extra SMS-controle wordt uitgevoerd. En de overheid kan met bestaande infrastructuur en regelgeving alvast meer diensten online aan burgers beschikbaar stellen.
3. Richt binnen de overheid een 7x24 uur online voorziening in om bij vermissing, diefstal of misbruik een identiteitsdocument direct te blokkeren. Eerder was binnen de overheid StopID daartoe bedacht. Mogelijk kan een dergelijke functionaliteit in MijnOverheid worden ondergebracht.
4. Graag zouden we ook iOS (iPhone)-gebruikers willen bedienen. Apple is een half jaar geleden op de hoogte gesteld van onze wens. Wellicht helpt een gesprek op een ander niveau.
5. DigiD versterkt met RDA kan tegen relatief kleine investeringen en exploitatiekosten en zonder uitrol van nieuwe middelen vanaf 2017 landelijk de online dienstverlening in het publieke domein op een hoger betrouwbaarheidsniveau brengen. Waarmee zowel burgers als overheid ervaring opdoen met de inzet van wettelijke identiteitsdocumenten als publiek authenticatiemiddel. En tegelijkertijd naar het hoogste betrouwbaarheidsniveau doorgroeid kan worden door een eID-applet aan nieuw uit te reiken identiteitsdocumenten toe te voegen.
6. In 2016 pilots verder uitbouwen met onder andere de zorgsector. In juni start een pilot om het medicijngebruik van burgers met RDA te ontsluiten.



8 Bijlagen

Betrouwbaarheidsonderzoek van PWC naar RDA

Privacy-impactanalyse uitgevoerd door PWC naar RDA

Presentatie 11 april 2016 tijdens bezoek commissie aan Veendam

Memo verschil publiek eID-middel op rijbewijs/NIK en RDA