Bureau ICT-toetsing
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2511 EA Den Haag

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties
t.a.v. de staatssecretaris, de heer drs. R.W. Knops
Postbus 20011
2500 EA Den Haag

Bureau ICT-toetsing
Muzenstraat 95
Den Haag
Postbus 20011
2500 EA Den Haag
www.bureauicttoetsing.nl

Contactpersoon
BIT@rijksoverheid.nl

Kenmerk
2020-0000376384

Uw kenmerk
2019-0000362528

Datum: 19 juni 2020
Betreft: Definitief BIT-advies programma VRS

Geachte heer Knops,

U heeft het Bureau ICT-toetsing (BIT) verzocht een toets uit te voeren op het programma Verbeteren Reisdocumentenstelsel (VRS). De opdrachtgever is de algemeen directeur van de Rijksdienst voor Identiteitsgegevens (RvIG). Hieronder vindt u een korte beschrijving van het programma. Daarna geven we de conclusie van de toets, onze analyse en adviezen. Wij concentreren ons hierbij op de belangrijkste risico's van het programma.

Nederlandse burgers reizen en identificeren zich met een paspoort of identiteitskaart. Deze kunnen worden aangevraagd bij een uitgevende instantie. Dit zijn gemeenten, Caribische gemeenten en landen, Buitenlandse Zaken (BZ) en de Koninklijke Marechaussee (KMar). Jaarlijks worden circa 3,5 miljoen paspoorten en identiteitskaarten uitgegeven.

Het reisdocumentenstelsel is in beheer bij RvIG. Het bestaat uit de volgende onderdelen:

- 500 decentrale Reisdocumenten Aanvraag- en Archiefstations (RAAS'en) bij uitgevende instanties. Hierin worden gegevens voor de aanvraag en uitgifte van reisdocumenten lokaal opgeslagen. Dit zijn ook biometrische gegevens: een gelaatsfoto, handtekening en, tijdelijk opgeslagen, vingerafdrukken. Leverancier ID&D verzorgt het technisch- en het applicatiebeheer van de RAAS'en en vervangt ze iedere vijf jaar. Ook is ID&D verantwoordelijk voor het productieproces van het fysieke reisdocument.
- Een centraal Basisregister Reisdocumenten met gegevens over vermiste, gestolen en van rechtswege vervallen reisdocumenten. De Dienst ICT Uitvoering (DICTU) van het ministerie van Economische Zaken en Klimaat verzorgt het technisch- en het applicatiebeheer van dit register.
- Een centraal Register paspoortsignaleringen met gegevens over personen aan wie een reisdocument geweigerd kan worden. Hiervan is het technisch- en het applicatiebeheer ook bij DICTU belegd.

Er bestaat echter geen volledige, centrale registratie van alle uitgegeven reisdocumenten, waardoor volgens RvIG en uitgevende instanties knelpunten zijn ontstaan. Zo is niet met 100 procent zekerheid aan te geven of een bepaald reisdocument wel in omloop mag zijn. Ook het controleren op mogelijke fraude zorgt voor veel telefoontjes en e-mailverkeer tussen uitgevende instanties die hiervoor elkaars aanvraaggegevens moeten inzien. Het BIT beschouwt deze

belangrijke knelpunten als een gegeven voor deze toets en heeft er geen onderzoek naar gedaan.

Het programma VRS heeft als opdracht de knelpunten in het huidige stelsel op te lossen en een nieuw fundament te leggen om in de toekomst identiteitsfraude te bestrijden en nieuwe dienstverlening voor de burger mogelijk te maken, zoals het online doorgeven van een vermist reisdocument. De aanpak van VRS richt zich op de realisatie van een centraal register als bron voor de reisdocumentengegevens en signaleringen, een apart centraal register voor biometrische gegevens en centrale toepassingen voor uitgevende respectievelijk signalerende instanties en burgers. Ook realiseert VRS functionaliteit (*services)* die betrokken partijen kunnen integreren in hun eigen systemen, zoals de reisdocumentenmodules van de burgerzakensystemen die zij van commerciële leveranciers betrekken. Met deze aanpak omvat VRS alle activiteiten die nodig zijn om het uitfaseren van de RAAS'en vóór de deadline van de volgende reguliere RAAS-vervanging (begin 2024) mogelijk te maken.

RvIG wil ICTU de bovengenoemde onderdelen laten ontwikkelen op een nieuw IT-platform en is daarvoor afhankelijk van het project 4V[1] dat RVIG samen met ODC-Noord en DICTU uitvoert. Het applicatiebeheer van de nieuw ontwikkelde onderdelen wordt bij DICTU belegd, maar RvIG neemt daar pas na een praktijkproef met ICTU, ODC-Noord en DICTU in september 2020 een besluit over.

Het programma is gestart op 1 april 2019 en bevindt zich in de realisatiefase. Het programma bestaat uit zeven projecten. Vier projecten richten zich op de realisatie en stapsgewijze implementatie van de beoogde toepassingen, registers en services. Drie andere projecten zijn ondersteunend en zorgen onder meer voor de invulling van de keuze voor de IT-leverancier, de aansturing van de IT-ontwikkeling en de datamigratie uit de bestaande RAAS'en naar de nieuwe registers. De programmakosten zijn ingeschat op circa € 46 miljoen, voor de periode 2019 tot en met 2024. Dit bedrag is exclusief een reservering van € 12 miljoen voor onvoorziene kosten.

De BIT-toets is uitgevoerd tussen oktober 2019 en begin februari 2020. De conclusie van onze toets luidt als volgt:

VRS kiest ervoor om een groot aantal ingrijpende veranderingen door te voeren in het systeemlandschap van het reisdocumentenstelsel. Hierdoor ontstaat een stapeling van risico's die het oplossen van knelpunten onzeker maakt. Daarbij leidt de gehanteerde aanpak onvoldoende tot resultaten en ontbreekt een gedegen uitwerking voor beveiliging en privacy. Wij verwachten hierdoor dat VRS belangrijke knelpunten later oplost dan nodig.

Wij adviseren het risicoprofiel te verlagen door de scope te beperken tot alleen de noodzakelijke activiteiten voor realisatie en ontsluiting van een centraal register van alle uitgegeven reisdocumenten en signaleringen. Focus hierbij op het sneller opleveren van resultaten en werk de kaders voor beveiliging en privacy uit. Door deze ingrepen kan VRS veel gerichter en met minder risico's een groot deel van de knelpunten oplossen. Overweeg om resterende activiteiten onder te brengen in een apart project en besluit over de voorzetting daarvan als er duidelijkheid is over de wetgeving voor biometrie en de te maken keuzes ten aanzien van leveranciers en technologie.

Wij lichten onze conclusie hieronder toe.

[1] 4V staat voor vervangen, verhuizen, vereenvoudigen en verhangen. Dit project realiseert een nieuw basisplatform voor alle RvIG-toepassingen.

VRS LOST BELANGRIJKE KNELPUNTEN LATER OP DAN NODIG

Datum
19 juni 2020

Kenmerk
2020-0000376384

Wij begrijpen dat VRS het reisdocumentenstelsel wil verbeteren en constateren dat er draagvlak is bij betrokken partijen voor het oplossen van belangrijke knelpunten. Juist dat tijdig doen komt echter in het geding, om drie redenen die we hieronder nader uitwerken.

A. Opeenstapeling risicovolle keuzes brengt oplossen knelpunten in gevaar

Op basis van de programmaopdracht om een nieuwe fundament voor de toekomst te leggen, kiest VRS ervoor om een groot aantal ingrijpende veranderingen door te voeren in het complexe systeemlandschap van het reisdocumentenstelsel. Omdat de veranderingen veelal tegelijkertijd worden doorgevoerd en sterk van elkaar afhankelijk zijn, ontstaat een stapeling van risico's. Dit brengt het andere deel van de programmaopdracht - het oplossen van de knelpunten - in gevaar.

Het gaat om de opeenstapeling van risico's als gevolg van deze keuzes:

- De keuze om biometrische gegevens niet langer decentraal in de RAAS'en op te slaan maar in een centraal register. Dit leidt af van het oplossen van een groot aantal knelpunten en zorgt voor onnodige tijdsdruk. Om een volgende reguliere RAAS-vervanging te voorkomen moet dit register vóór 2024 in gebruik zijn. Maar voor zo'n centraal biometrieregister is een wijziging van de paspoortwet noodzakelijk die, gezien de maatschappelijke en politieke gevoeligheid, naar onze verwachting niet tijdig is afgerond. Eerdere, minder gevoelige, wijzingen van de paspoortwet duurden ook langer en de benodigde juridische capaciteit ontbreekt vooralsnog.
- De keuze voor een fundament op basis van volledige nieuwbouw van twee registers, functionaliteit voor uitgevende instanties en zo'n 50 *services* is risicovol. Dit stelt namelijk hoge eisen aan RvIG en de beoogde IT-leveranciers, die bovendien nog beperkt ervaring hebben met een omvangrijk ontwikkeltraject voor maatwerksystemen in dit specifieke domein. Er zijn mogelijk veel minder risicovolle oplossingsrichtingen, zoals het moderniseren van de RAAS'en en de inzet van bestaande functionaliteit zoals bijvoorbeeld in de reisdocumentenmodules ter ondersteuning van het aanvraagproces bij onder andere grensgemeenten en KMar. Wij begrijpen niet waarom VRS deze alternatieven niet grondig heeft onderzocht.
- De keuze om leverancier ID&D te vervangen door drie IT-leveranciers binnen de overheid. Dit vergt meer aansturing door RvIG. Bovendien is het de vraag of de samenwerking met de beoogde IT-leveranciers wordt voortgezet; pas na de praktijkproef wordt hier in september 2020 een besluit over genomen terwijl VRS al in de realisatiefase zit. Daarbij heeft VRS geen alternatieve scenario's beschikbaar voor het geval de uitkomsten van deze proef negatief zijn.
- De keuze voor een IT-platform (*Platform-as-a-Service*) met containers en microservices is in deze context risicovol. Dit zijn concepten waar zowel de beoogde leveranciers als RvIG nu voor het eerst met VRS leerervaringen mee op gaan doen. Bovendien wordt het onderliggende basisplatform niet op tijd opgeleverd door het project 4V dat hiervoor verantwoordelijk is. Hierdoor loopt de eerste oplevering van VRS in september 2020 zeer waarschijnlijk vertraging op.
- De keuze voor de introductie van een agile werkwijze en de keuze voor uitbreiding van de bestaande beheerrol van RvIG. Dit zijn organisatie-veranderingen waar RvIG in de context van het complexe systeemlandschap van het reisdocumentenstelsel nog weinig ervaring mee heeft.

B. Gehanteerde aanpak leidt onvoldoende tot resultaten

Hoewel VRS bijna een jaar in de realisatiefase zit, komt het nog niet op stoom en heeft het al een aantal flinke bijstellingen in de aanpak moeten doen. Wij verwachten dat het programma gaat uitlopen in tijd en geld en mogelijk zelfs nooit van wal komt doordat de gehanteerde aanpak onvoldoende tot resultaten leidt:

- De zeven projecten van VRS kunnen niet zelfstandig tot implementeerbare resultaten komen. Projecten moeten samen tot een ontwerp van te bouwen software zien te komen. Eén van de projecten treedt daarbij op als interne opdrachtnemer voor alle IT-behoeften van de andere projecten. Het is onduidelijk wie welke rol heeft in de aansturing van de IT-leveranciers binnen de beoogde agile aanpak. In de plannen werken tot 50 personen tegelijk binnen deze onduidelijke structuur; wij zien niet hoe dit effectief kan gaan werken.
- De planning van VRS biedt onvoldoende houvast voor de beheersing van de softwareontwikkeling. De planning omvat zo'n 20 opleveringen waarvan de minimaal gewenste inhoud onduidelijk is. Zelfs voor de eerste oplevering in september 2020 is nog niet vastgesteld welke concrete functionaliteit minimaal moet zijn gerealiseerd. Dat geldt bijvoorbeeld voor identiteits- en toegangsbeheer, logging en de functionaliteit voor uitgevende instanties. Ook is er een groot aantal afhankelijkheden tussen de opleveringen geïdentificeerd maar deze zijn nog onvoldoende inhoudelijk uitgewerkt.
- VRS verwacht dat de recente koerswijziging (de keuze voor nieuwbouw in plaats van hergebruik) binnen de bestaande planning opgelost kan worden. De keuze om het centrale register nieuw te bouwen – in plaats van het recent gerealiseerde centrale register voor de elektronische Nederlandse Identiteitskaart (eNIK) te hergebruiken – leidt tot extra complexiteit in het reisdocumentenstelsel, doordat nieuwe koppelingen en synchronisaties moeten worden gerealiseerd, en beheer- en regietaken worden uitgebreid. Wij verwachten dat het ondervangen van deze extra complexiteit wel tot uitloop zal leiden.
- VRS schat de benodigde tijd voor de aanpassingen en implementatie bij uitgevende instanties en informatie-afnemers van reisdocumentengegevens te optimistisch in. In totaal worden circa 1000 partijen geraakt; zij hebben nog geen concreet beeld wat de veranderingen voor hen betekenen. Ruim tien externe leveranciers moeten hun pakketten aanpassen en 600 overeenkomsten tussen RvIG en haar afnemers moeten opnieuw worden afgesloten. Dit is niet binnen een paar maanden geregeld.

C. Gedegen uitwerking beveiliging en privacy ontbreekt

Gezien de gevoeligheid van reisdocumentgegevens is een adequate uitwerking van de informatiebeveiliging en privacybescherming essentieel. Dit moet in ontwerpen worden uitgewerkt (*by design*) voor de start van de realisatie. Die uitwerking ontbreekt echter vooralsnog:

- Er is geen volledige inventarisatie gedaan van het niveau van informatiebeveiliging en privacybescherming in het huidige stelsel (RAAS). Daardoor bestaat er geen meetlat voor het bepalen van het noodzakelijke beveiligings- en privacyniveau van het nieuwe stelsel.
- De uitgangspunten van VRS voor beveiliging en privacybescherming zijn niet uitgewerkt. Zo heeft RvIG nu geen toegang tot biometrische gegevens in de RAAS'en. VRS weet nog niet of ze dit uitgangspunt ook gaat hanteren in het nieuwe reisdocumentenstelsel. Ook beoogt VRS een 'pseudonieme koppeling[2]'

[2] Pseudonimiseren is een privacy-verhogende maatregel waarbij identificerende gegevens niet meer rechtstreeks aan een individu zijn te relateren.

tussen de opslag van biometrische gegevens en andere registers te realiseren. Of dit een voldoende beveiligingsniveau oplevert is vooralsnog onduidelijk.
- Authenticatie en autorisatie zijn nog onvoldoende uitgekristalliseerd. Het gaat daarbij niet alleen om vervanging van de huidige (op smartcard gebaseerde) functionaliteit van de accordering van reisdocumentaanvragen in het RAAS middels een elektronische handtekening. Het gaat ook om nieuwe authenticatiefunctionaliteit waarmee uitgevende instanties elkaar inzage kunnen geven in de pasfoto's van hun reisdocumentenaanvragen.
- Het is onduidelijk hoe VRS invulling gaat geven aan de hogere eisen op het gebied van beschikbaarheid en 'robuustheid' die de centralisatie van het reisdocumentenstelsel met zich meebrengt om zo goed mogelijk te voorkomen dat er *single points of failure* ontstaan. Voor een aantal uitgevende instanties, zoals de KMar, moet het namelijk mogelijk zijn om in alle omstandigheden noodpaspoorten uit te kunnen geven.

ADVIES: ZORG DAT VRS EERST BELANGRIJKE KNELPUNTEN OPLOST

Wij denken dat VRS veel gerichter en met minder risico's de belangrijke knelpunten in het reisdocumentenstel kan oplossen. Wij adviseren daarom om de scope van het programma te herzien. Pas daarbij tevens de aanpak aan om de slaagkans te vergroten en zorg dat de kaders voor beveiliging en privacy zijn uitgewerkt.

Plaats de resterende activiteiten in een afzonderlijk project en besluit over de voorzetting daarvan als er duidelijkheid is over de wetgeving voor biometrie en de te maken keuzes ten aanzien van leveranciers en technologie.

Onze adviezen werken we hieronder in meer detail uit.

1. Beperk de scope van VRS

Wij adviseren om het risicoprofiel te reduceren door de scope van VRS te beperken tot alleen de noodzakelijke activiteiten voor het realiseren en ontsluiten van een centraal register van uitgegeven reisdocumenten en signaleringen. Daartoe raden we aan om de volgende activiteiten op te pakken:
- Gebruik de praktijkproef met de beoogde leveranciers voor het toetsen van de haalbaarheid van een nieuw te bouwen centraal register en voor het bepalen van de minimale functionaliteit voor de ontsluiting ervan. Toets hierbij ook de haalbaarheid van de keuze om dit register naast het bestaande eNIK-register te positioneren, waardoor er extra koppelingen en synchronisaties tussen de registers nodig zijn.
- Overweeg de huidige leverancier ID&D te betrekken bij de uitwerking van de oplossingsrichting en mogelijke alternatieve oplossingen. Dat kan mogelijk vertraging voorkomen indien de uitkomst van de praktijkproef negatief uitvalt en de koppeling met de systemen bij ID&D vergemakkelijken.
- Start met het beoogde basisplatform van 4V en de beschikbare ontwikkelomgeving van ICTU en bouw dit in kleine stappen uit op basis van technologie die zich heeft bewezen.
- Start na afloop van de praktijkproef, indien besloten kan worden om de samenwerking met de beoogde leveranciers te continueren, met het geleidelijk vullen en ontsluiten van het centrale register. Zorg dat de gegevens van álle uitgevende instanties erin komen en dat de gehele levenscyclus van een reisdocument wordt afgedekt.

Pas op basis van deze scope de plannen en begroting van VRS aan.

2. Zorg dat de aanpak leidt tot snel implementeerbare resultaten

Wij adviseren om in de huidige aanpak de volgende wijzigingen door te voeren zodat het programma veel beter in staat is om concrete, implementeerbare resultaten op te leveren:

- Deel VRS op in onafhankelijke projecten die zelfstandig releases kunnen opleveren en implementeren en hiervoor de hele verantwoordelijkheid dragen. Sluit hierbij aan op de agile ontwikkelaanpak die ICTU hanteert.
- Definieer concreet welke functionaliteit minimaal nodig is voor een centraal register voor uitgegeven reisdocumenten en signaleringen. Deel deze scope op in periodiek op te leveren releases en bepaal welke knelpunten daarmee worden opgelost. Bepaal gedetailleerd wat de inhoud van de eerstvolgende release is.
- Werk het realisatietraject uit. Stel met de IT-leveranciers een realistische planning op en zorg dat de extra complexiteit, veroorzaakt door de recente koerswijziging (nieuwbouw centrale register in plaats van doorontwikkeling eNIK-register), hierin goed wordt verwerkt.
- Werk een transitiestrategie uit. Maak hierin voor elk moment duidelijk welke gegevens in welk register leidend zijn en welk kwaliteitsniveau die gegevens bij elke stap hebben. Maak deze informatie breed bekend in het stelsel.
- Werk de implementatie uit. Ga op basis van een impactanalyse na welke wijzigingen bij de uitgevende instanties en informatie-afnemers moeten worden doorgevoerd. Stel samen met de betrokken partijen een realistische planning op en doe een aantal proefimplementaties om de haalbaarheid te beproeven.

3. Zorg voor een gedegen uitwerking van beveiliging en privacy

Wij adviseren om het programma zo snel mogelijk gedegen kaders voor beveiliging, privacy en beschikbaarheid uit te laten werken, als volgt:

- Formuleer concrete beveiligingsdoelstellingen voor VRS, mede op basis van *best practices* voor het beheer van reisdocumenten[3]. Stem die af met betrokken partijen. Inventariseer hiertoe met leverancier ID&D het huidige niveau van beveiliging en ga na wat daarvan in de beoogde centrale opzet gehandhaafd of aangescherpt moet worden. Wees hierbij alert op nieuwe risico's in de beoogde centrale opzet, zoals dat RvIG (biometrische) gegevens kan inzien en dat uitgevende instanties toegang hebben tot elkaars gegevens.
- Werk maatregelen uit voor de authenticatie- en signeerbehoefte binnen het beoogde centrale stelsel. Ga daarbij na hoe de huidige smartcard-gebaseerde signeerfunctionaliteit in de RAAS'en dusdanig in een centrale opzet kan worden vormgegeven dat aan de beveiligingsdoelstellingen wordt voldaan.
- Werk maatregelen uit om de gewenste robuustheid en beschikbaarheid binnen het centrale stelsel te realiseren. Geef daarbij specifiek aandacht aan uitgevende instanties die altijd (nood)paspoorten moeten kunnen uitgeven.
- Werk maatregelen uit voor de cryptografische versleuteling van gegevens in het beoogde centrale biometrie register (als de wetgeving voor biometrie wordt goedgekeurd). Maak daarbij traceerbaar wanneer RvIG toegang heeft verkregen tot de gegevens, bijvoorbeeld door de verplichte inzet van een Hardware Security Module. Maak hierbij onderscheid tussen opvraagbare (gelaatsfoto, handtekening) en niet-opvraagbare, tijdelijk opgeslagen, gegevens (vingerafdrukken).

[3] Zie *Guide for Assessing Security of Handling and Issuance of Travel Documents,* https://www.icao.int/. Deze gids is van de VN-organisatie die niet alleen de technische specificaties van reisdocumenten beheert maar ook aanbevelingen doet voor de beveiliging en het beheer van de levenscyclus ervan.

4. Plaats de resterende activiteiten in een afzonderlijk project

Datum
19 juni 2020

Kenmerk
2020-0000376384

Wij geven RvIG in overweging om de resterende activiteiten, die niet tot de in aanbeveling 1 beperkte scope behoren, op een later moment onder te brengen in een apart project. Dit betreft de realisatie van een centraal register voor biometrie, de realisatie van een centrale toepassing voor het aanvraagproces voor uitgevende instanties en toepassingen voor signalerende instanties en burgers.

Voordat deze activiteiten kunnen worden voortgezet in een afzonderlijk project, adviseren we om eerst de dan nog niet opgeloste knelpunten in kaart te brengen en de ernst en de omvang ervan te kwantificeren. Ga op basis van deze analyse na welke scenario's in aanmerking komen voor het oplossen van deze knelpunten en het uitfaseren van de RAAS'en. Tegelijkertijd kunnen de wetgeving en alternatieve oplossingen voor centrale opslag van biometrische gegevens worden onderzocht en uitgewerkt. Onderzoek in die tijd tevens of de inzet van bestaande functionaliteit zoals bijvoorbeeld in reisdocumentenmodules haalbaar is voor de uitgevende instanties die hier nu nog geen gebruik van maken.

***

Tot slot danken wij alle geïnterviewden voor hun medewerking en openheid bij deze toets. Wij hopen u met dit advies aanknopingspunten te hebben gegeven voor het vervolg van VRS.

Met de meeste hoogachting,
namens het Bureau ICT-toetsing,

Sander van Amerongen
wnd. Hoofd BIT