Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

PSA Verbeteren Reisdocumenten Stelsel (VRS)

Werken onder architectuur

Datum	08-11-2019
Versie	1.14
Status	Ter vaststelling
Inlichtingen bij	Architectuurberaad VRS

Versie informatie

Versie	Datum	omschrijving	Auteur
0.1	20-07-2018	Initiële opzet	5.1, 2 onder e
0.2	14-11-2018	Initiële vulling van principes en aanpassing hoofdstukindeling	5.1, 2 onder e 5.1, 2 onder e
0.3	30-11-2018	Aanvullingen nav doelenboom, splitsing eindbeeld/toekomstvisie, algehele aanvullingen en invulling principes	5.1, 2 onder e
0.4	23-12-2018	Wijzigingen nav QA en architect overleggen	5.1, 2 onder e 5.1, 2 onder e
0.5	10-2-2019	Wijzigingen nav review ronde met programmateamleden en verdere uitwerking	5.1, 2 onder e
0.9	22-2-2019	Review commentaar verwerkt. Voorgelegd in bredere (externe) review	5.1, 2 onder e 5.1, 2 onder e
0.91	18-03-2019	Tekstuele review verwerkt	5.1, 2 onder e
0.92	12-04-2019	Review commentaar verwerkt n.a.v. bredere reviewvraag	5.1, 2 onder e
0.93	17-04-2019	Review commentaar verwerkt n.a.v. bredere reviewvraag	5.1, 2 onder e
1.0	25-04-2019	Redactie en vaststelling d.d. 23-04-2019 in DT RvIG verwerkt	5.1, 2 onder e
1.1	11-10-2019	Eerste update van de PSA. Inhoudelijk vooral detaillering datamodel, statusmodel, API / URI strategie, toegangs-beveiliging, match met NORA-principes.	5.1, 2 onder e
1.14	08-11-2019	Aanvullingen programmateam en QA verwerkt.	5.1, 2 onder e

Verzendlijst

Versie	Datum	omschrijving
0.1	3-12-2018	Basisdocument doorgestuurd voor verdere invulling door de architecten
0.4	21-12-2018	Aanvullingen gevraagd aan programmateam en QA
0.5	10-2-2019	Review voor programmateam alvorens er een brede review plaatsvindt.
0.9	22-2-2019	Voorgelegd in bredere (externe) review
0.93	17-04-2019	DT RvIG en reviewers uit bredere (externe) review
1.0	24-04-2019	Besluitvormingsdossier Stas
1.1	11-10-2019	Review programmateam inclusief QA
1.14	08-11-2019	RvIG Architectuuroverleg

Reviewers

Versie	Naam	Bedrijf/Functie

Referenties

Nr	Titel	Auteur	Versie	Datum
[1]	Producten- en Dienstencatalogus Kennisweb	5.1.2.e		
[2]	NORA 3.0 katern strategie	ICTU	3.0	19 augustus 2009
[3]	RvIG referentie architectuur	RvIG	1.2	9 januari 2017
[4]				
[5]				
[6]				
[7]				
[8]				

Inhoud

Inhoud 4

1 Inleiding 7

1.1 Het programma VRS 7

1.2 Toekomstvisie 7

1.3 Toelichting voor de lezer 8

2 Eindbeeld VRS 10

3 Business Architectuur 19

3.1 Inleiding 19

3.2 Klantervaringen 19

3.3 Hoofdprocesoverstijgende zaken 22

3.4 Aanvraag en uitgifte 31
3.4.1 Algemeen 31

3.5 Statusbeheer 37
3.5.1 Richtinggevende uitspraken 37
3.5.2 Statusmodel reisdocument 39

3.6 Signaleringenbeheer 42

3.7 Informatieverstrekking 45

3.8 Gebruik 46

4 Informatie Architectuur 48

4.1 Applicaties 53
4.1.1 Afbakening en applicatiecomponenten 53
4.1.2 Beleidslijnen, richtlijnen, standaarden 59
4.1.3 Analyse en ontwerp 61
4.1.4 Applicatie kwaliteitseisen 62

4.2 Gegevens 63
4.2.1 Informatiemodellering 63
4.2.2 Algemene uitgangspunten en kaders 65
4.2.3 Verklaring aan de hand van domeinen 66
4.2.4 Beleidslijnen, richtlijnen, standaarden 76

5 Technische architectuur 79

5.1 De techniek van het boekje/ID kaart 80
5.1.1 Afbakening 80

5.2 Fysieke apparatuur 80
5.2.1 Afbakening 80
5.2.2 Beleidslijnen, richtlijnen, standaarden 81

5.3 Platform 81
5.3.1 Afbakening 81
5.3.2 Aansluiten op de Nederlandse API strategie 85

5.3.3 Aansluiten op de Nederlandse URI strategie 86
5.3.4 Beleidslijnen, richtlijnen, standaarden 87

5.4 Netwerk 88
5.4.1 Afbakening 88
5.4.2 Beleidslijnen, richtlijnen, standaarden 88

6 Informatiebeveiliging 90

6.1 Informatiebeveiliging 90

6.2 Logische toegangsbeveiliging 92
6.2.1 Definities 92
6.2.2 Lagen in de toegangsbeveiliging 92
6.2.3 Toegang van interactieve gebruikers tot applicaties 93
6.2.4 Toegang van applicaties tot API's 94
6.2.5 Toegang tot kritische resources / data 95

6.3 Privacy 95
6.3.1 Verantwoordelijkheid 95
6.3.2 Legitiem doel en doelbinding 96
6.3.3 Doelbinding 96
6.3.4 Delen van gegevens met derden 96
6.3.5 Principes privacy-by-design 96
6.3.6 Dataretentie 96
6.3.7 Dataminimalisatie wordt toegepast bij alle persoonsgegevens. 96
6.3.8 Maak onherleidbaar 97
6.3.9 Informeren 97
6.3.10 Scheid 97
6.3.11 Abstraheer 98
6.3.12 Toon aan 98
6.3.13 Gegevensexport 98

7 Beheer 99

7.1 Informatievoorzieningenbeheer 99

7.2 Applicatiebeheer 99

7.3 Beheervoorzieningen 100
7.3.1 Digitale Werkruimtevoorzieningen 100
7.3.2 Managementvoorzieningen voor beheer RvIG 101

8 Programma overstijgende ontwerpkeuzen 102

8.1 Keuze service gerichte architectuur 102

9 Architectuurgovernance binnen VRS 104

9.1 Doelen van de architectuurgovernance in VRS 104

9.2 Relevante architectuur- en ontwerpobjecten 104

9.3 Organisatie architectuurgovernance, ontwerpautoriteit 105

9.4 Vastgestelde en uit te werken ontwerpkeuzes 106

Bijlage 1: Actuele knelpunten 107

Bijlage 2: Toekomstvisie 108

1.1 Externe maatschappelijke trends 108
1.2 Ontwikkelingen in wetgeving en beleid: 108
1.3 Overige ontwikkelingen 109
1.4 Veranderdoelen voor het reisdocumentenstelsel 109
1.5 VRS als fundament voor de veranderingen 111
1.6 Na VRS 111
1.7 Ten slotte 113

Bijlage 3: Begrippenlijst 114

Bijlage 4: Openstaande punten 115

Bijlage 5: Overzicht componenten Reisdocumenten 116

Bijlage 6: Overzicht deelproducten VRS 117

Bijlage 7: overzicht van Business Services 118

Bijlage 8: Eisen functionaliteit datamigratie v05.docx 119

Bijlage 9: Architectuurafwijkingen 120

Afwijking 1 – Reisdocumenten diensten via internet toegankelijk 120

Bijlage 10: Inzicht in uitvoering van NORA principes 122

1 Inleiding

1.1 Het programma VRS

VRS verbetert een aantal businessprocessen alsmede de informatievoorziening rondom het aanvragen, uitgeven en gebruiken van reisdocumenten waarbij de vorming van een samenhangende kernregistratie (voor houders, eventuele signaleringen, (reis)documenten, de aanvragen voor die documenten en documentstatussen) centraal staat.

Tevens voorziet VRS in een flexibelere informatievoorziening waarmee het stelsel ook voorbereid is om toekomstige stappen te zetten als:

- Mogelijke uitgifte van alternatieve documenten en virtuele documenten;
- Mogelijkheid voor andere inrichting van aanvraag- en uitgifteprocessen;
- Mogelijke alternatieve verdelingen tussen frontoffice en lokale en centrale backoffices;
- Betere fraudepreventie, - detectie en -bestrijding.

Het gaat hierbij steeds om verbeteringen die in de toekomst – na afronding van VRS - mogelijk worden. De feitelijke toepassing hiervan is echter in alle gevallen nog onderhevig aan beleidsvorming en, in de meeste gevallen, ook noodzakelijke aanpassingen in wet- en regelgeving.

VRS wordt verder steeds gerealiseerd met inachtneming van de toekomstvisie reisdocumenten, zodat ook op die andere onderdelen toekomstvastheid is geborgd. Zie hiervoor ook de volgende paragraaf. Het bewaken van deze toekomstvastheid is één van de doelen van de architectuurgovernance in het programma, zie hoofdstuk 9.

1.2 Toekomstvisie

Alvorens over te gaan tot de beschrijving van de eigenlijke programmastartarchitectuur heeft het programma VRS een toekomstvisie ontwikkeld op het *reisdocumentenstelsel* en de positie daarbinnen.

Het reisdocumentenstelsel is daarbij gedefinieerd als het geheel van actoren, processen en systemen dat tot doel heeft betrouwbare reisdocumenten – in analoge of digitale vorm - aan te vragen, te produceren en te personaliseren, uit te geven, te beheren, te verifiëren en anderszins te gebruiken.

De toekomstvisie dient om duidelijk te krijgen op welke punten VRS 'funderend' zou moeten zijn. VRS dient er immers voor een flexibel en toekomstvast fundament op te leveren, waarmee mogelijk is het reisdocumentenstelsel te ontwikkelen op de middellange termijn (5-10 jaar). Het is van belang voor VRS, om een helder beeld te hebben wat voor toekomstige ontwikkelingen VRS dient voor te bereiden. Voorbereiding in de zin van: 'Welke flexibiliteit en toekomstvastheid bouwen we nu al in?' En: 'Welke toekomstige ontwikkelingen willen we in ieder geval niet blokkeren?'.

De toekomstvisie is beschreven in bijlage 1. Hierin zijn veranderdoelen geformuleerd. Deze worden beredeneerd vanuit externe maatschappelijke trends, ontwikkelingen in onder meer wetgeving en beleid, alsmede vanuit de wens om een aantal knelpunten weg te nemen. De toekomstvisie bevat de doelen, waarvan RvIG verwacht dat deze op enig moment op de middellange

termijn (5-10 jaar) gaan leiden tot concrete veranderingen. Zulks uiteraard onder voorbehoud van beleidsvorming op die punten.

1.3 Toelichting voor de lezer

Dit document bevat de programmastartarchitectuur (PSA) voor het programma Verbeteren Reisdocumentenstelsel (VRS).

Deze PSA wordt gemaakt om te waarborgen dat nieuwe ontwikkelingen en veranderingen zoals RvIG die beoogt voor het reisdocumentenstelsel in samenhang worden gerealiseerd en passen binnen gewenste kaders. Met de PSA en de bijbehorende governance daarop kan VRS een programma zijn dat enerzijds concrete resultaten realiseert binnen de scope van het programma, maar ook voldoende basis legt voor verdere (toekomstige) verbeteringen van het reisdocumentenstelsel.

Om reden van het funderende karakter van het VRS programma, is ook een toekomstvisie beschreven. Dit is een werkbeeld dat RvIG hanteert over de gewenste toekomstige situatie. VRS implementeert deze toekomstvisie dus maar ten dele. Voor de overige ontwikkelingen treft VRS wel voorbereidingen of en werpt er tenminste geen blokkades voor op.

Deze PSA moet niet verward worden met de meer gebruikelijke *project*startarchitecturen. VRS kent diverse projecten en in elk van die projecten zal er sprake zijn van één of meer architectuur- en/of ontwerpproducten. Denk bijvoorbeeld aan procesontwerpen, use cases, nader uitgewerkte informatiemodellen, user stories, solution architectures. De detaillering wordt dus aangetroffen in de diverse projecten, de programmastartarchitectuur geeft echter wel de richting en kaders, waarbinnen de projecten zich dienen te begeven.

In deze programmastartarchitectuur zijn daarom de volgende richtinggevende en kaderende zaken opgenomen:

- De eerdergenoemde toekomstvisie;
- Het beoogde eindbeeld dat door het programma VRS wordt gerealiseerd, is aan de hand van een doelenboom beschreven;
- Richtinggevende uitspraken op de Business, Informatie en Techniek, lagen, alsmede op het gebied van Beveiliging en Privacy en Beheer.

In het programmaplan, dat parallel is ontwikkeld aan deze PSA zijn de verschillende projecten en hun respectievelijke resultaten beschreven, met inbegrip van richtinggevende uitspraken die vanuit het programma aan de projecten worden meegegeven.

Aanvullend zijn er enkele modellen opgenomen in deze programmastartarchitectuur, die richting geven aan de concrete invulling door de verschillende projecten:

- Een integraal datamodel op hoofdlijnen.
- Een eerste versie van een lijst business services[1]. Dit zijn services die vanuit de reisdocumentenomgeving ter beschikking worden gesteld aan frontofficeapplicaties van ketenpartners en/of webportalen.

Ten slotte is een hoofdstuk specifiek over de architectuursturing in het programma VRS opgenomen. Dit is met name gedaan omdat er nog veel architectuur- en ontwerpproducten in VRS ontwikkeld zullen worden, waarop architectuurgovernance gewenst is. In dit hoofdstuk worden tevens de architectuur- en ontwerpproducten benoemd.

De gele vlakken in de PSA geven die onderwerpen aan waarop 'beweging' zit. Wezenlijke wijzigingen, aanvullingen of onderwerpen waarop nog discussie loopt. Om redenen van leesbaarheid is ervoor gekozen om geen versie met renvoyering te verspreiden.

[1] *De* oplossing voor VRS is gebaseerd op een service oriented architectuur, waarbij we kiezen voor een microservice benadering. We spreken in deze architectuur over *informatieservices* en *business services*. Informatieservices zijn aanroepbare technische diensten, die een afgebakende functie vervullen zoals het antwoord geven op een zoekopdracht of het registreren van een gegeven. De business service is een business concept. Het zijn die (gezamenlijke) informatievoorzieningsdiensten, die een business proces(stap) ondersteunen. Ze leveren in de context van deze architectuur toegevoegde waarde aan eindgebruikers in het reisdocumentenstelsel via frontofficeapplicaties of portalen.

2 Eindbeeld VRS

Het programma VRS legt de basis voor de verbetering van het reisdocumentenstelsel. VRS kent hiervoor een aantal algemene doelen:

- Een betrouwbaar reisdocument;
- Betrouwbare identiteitsverificatie en informatie;
- Toekomstvast en flexibel stelsel.

Allereerst is daar het doel van een betrouwbaar reisdocument. Daarbij wordt meestal gedacht aan een document dat niet of zeer moeilijk is te vervalsen. Op dit gebied onderneemt VRS echter geen acties. Wel verbetert VRS zowel een aantal businessprocessen rondom het aanvragen, uitgeven en gebruiken van reisdocumenten zodat reisdocumenten, voorzien van precies de juiste gegevens, in handen komen van de juiste personen, die bovendien recht hebben op een reisdocument.

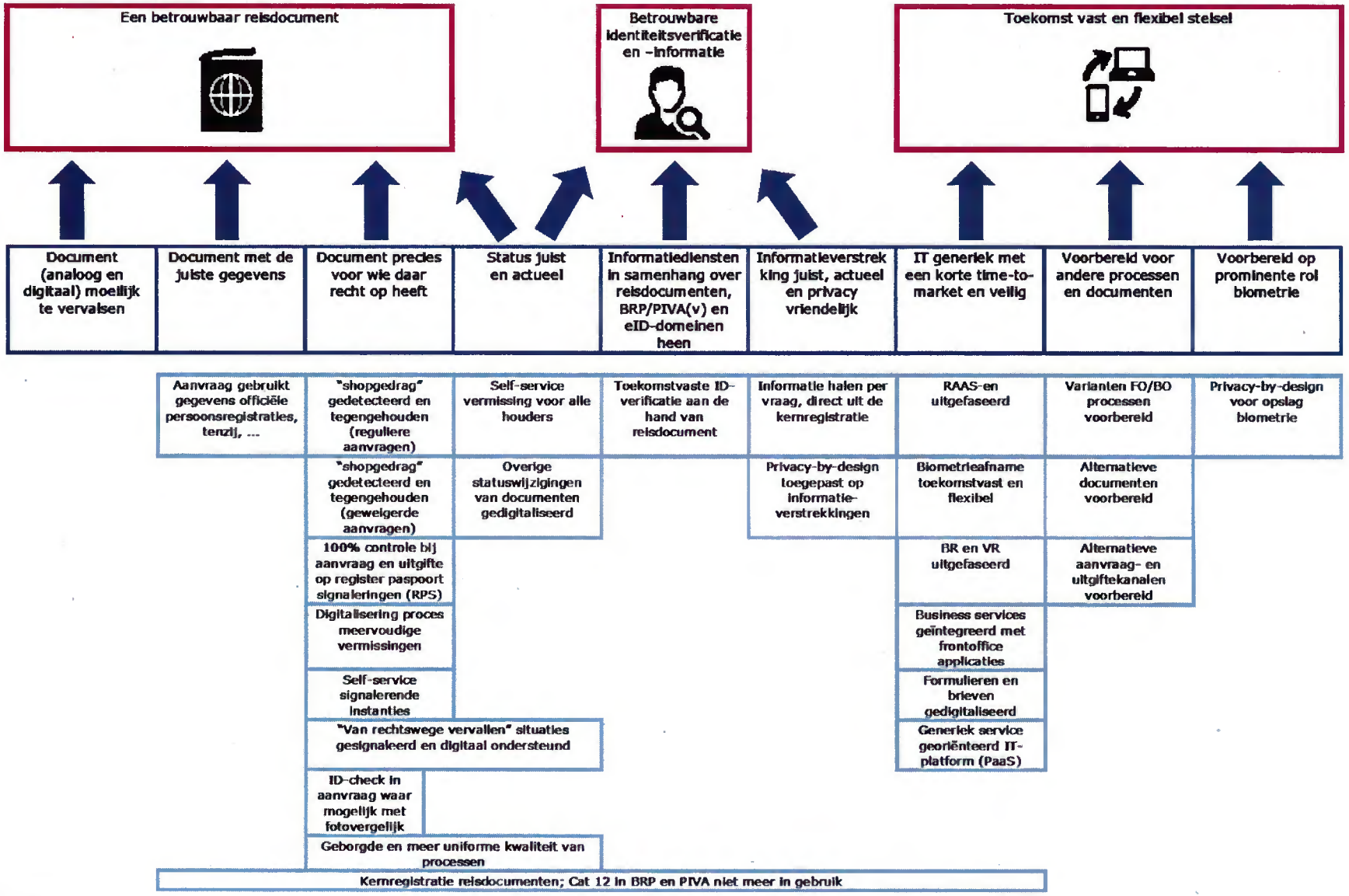
Ten tweede wordt ook de informatieverstrekking wezenlijk verbeterd, met juistere en actuelere informatie, die bovendien op een manier wordt verstrekt, die in lijn is met de AVG en de daarin vervatte privacy-by-design uitgangspunten. Ook worden de diensten voor identiteitsverificatie verbeterd; binnen VRS gaat het dan steeds om identiteitsverificatie aan de hand van een reisdocument. Om zowel de businessprocessen als de informatieverstrekking wezenlijk te verbeteren worden gegevens technisch in één kernregistratie gecentraliseerd. Overigens blijft daarbij de verantwoordelijkheid voor het aanvraag- en uitgifteproces gewoon bij de uitgevende instanties te liggen.

Ten slotte worden ook de ICT-systemen gemoderniseerd en gecentraliseerd, ter vervanging van de bestaande decentrale systemen. Met een flexibeler opgezette informatievoorziening is het stelsel ook voorbereid om toekomstige stappen sneller en goedkoper te realiseren.

Hiermee worden vervolgstappen zoals voorzien in de toekomstvisie wezenlijk makkelijker te realiseren dan thans het geval is. Denk bijvoorbeeld aan het verbeteren van de dienstverlening aan de burger of aan varianten van het aanvraag- en uitgifteprocessen of aan toekomstige stappen in de fraudepreventie, -detectie en -bestrijding. Deze laatste voorbeelden van verbeteringen zijn dus geen doelen van VRS, VRS legt hiervoor slechts het fundament. Ook zijn het onderwerpen waarvoor eerst nog beleidsbeslissingen nodig zijn en in een aanzienlijk aantal gevallen zal er ook wet- en regelgeving aangepast moeten worden.

Om deze algemene doelen in programmaverband te realiseren, zijn voor VRS een aantal operationele doelen gedefinieerd. Deze zijn SMART[2] te definiëren. De operationele doelen dragen bij aan de gedefinieerde algemene doelen. In het programma worden activiteiten ontplooid om de operationele doelen te realiseren. Hieronder is het doelenoverzicht van VRS weergegeven. In de tekst onder deze figuur lichten we daarbij de operationele doelen puntsgewijs toe.

[2] *SMART: Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden*



Figuur 1 Doelen

Hieronder zijn de operationele doelen puntsgewijs toegelicht:

1. Aanvraag gebruikt gegevens officiële persoonsregistraties, tenzij ...
   In het aanvraagproces wordt zoveel mogelijk gebruik gemaakt van de gegevens uit persoonsregistraties, in casu de BRP, PIVA, PIVA-v. Deze gegevens worden gebruikt om de documenten correct op naam te zetten. Afwijkingen van de officiële persoonsregistraties blijven mogelijk en zijn ter beoordeling van de uitgevende instanties, echter wel onder registratie van de reden van de afwijking. Waar terugmelding naar officiële persoonsregistraties aan de orde is, is deze voorzien in het proces van de uitgevende instantie. NB Wanneer een bestaande documenthouder niet in een persoonsregistratie voorkomt, worden gegevens uit de eerdere aanvraag gebruikt. Gegeven de centralisatie van deze gegevens is dit goed mogelijk. Verder blijven er altijd situaties over dat er sprake is van een eerste aanvraag en dat de persoon nergens is geregistreerd. Dit doet echter niets af aan het bovenstaande.
2. 'Shopgedrag' gedetecteerd en tegengehouden. Een langlopende wens van uitgevende instanties is om 'shopgedrag' van burgers te kunnen detecteren en tegen te gaan. Dit valt uiteen in twee gevallen:
   a. Burgers vragen meerdere documenten aan, mogelijk met onrechtmatige handelingen in gedachten.
   b. Burgers die op een aanvraag geen document hebben gekregen proberen op andere plaatsen een aanvraag te doen, in de hoop een uitgevende instantie te treffen die een voor hun positieve beslissing neemt.

   Beide gevallen worden in het eindbeeld gedetecteerd.
   Ad a. Hierdoor kan in de eerste casus voorkomen worden dat een burger in het bezit komt van meerdere reisdocumenten. Bij de aanvraag kan de burger worden gewaarschuwd en bij de uitgifte kan de uitgevende instantie tevens op de hoogte worden gesteld dat er een (recent) uitgegeven reisdocument is dat (aanvullend) aan het verkeer dient te worden onttrokken.
   Ad b. In de tweede casus worden beslissingen van uitgevende instanties in relatie tot een aanvraag geregistreerd. Denk hierbij aan weigeringen of opgelegde beperkingen, al dan niet naar aanleiding van een signalering. Met deze gegevens omtrent eerdere beslissingen op aanvragen kunnen actuele uitgevende instanties hun besluit beter geïnformeerd nemen. Hiertoe wordt een aanvraag in de kernregistratie geregistreerd zodra er sprake is van een geïdentificeerd persoon die aangeeft een reisdocument te willen verkrijgen van een uitgevende instantie. Alle beoordelingsactiviteiten van uitgevende instanties vinden plaats in het kader van een aanvraag en worden geregistreerd. Er wordt bijvoorbeeld niet gecontroleerd op een signalering zonder de aanwezigheid van een (geregistreerde) aanvraag.
3. 100% controle bij aanvraag en uitgifte op register paspoort signaleringen (RPS).
   In alle aanvragen wordt gecontroleerd of de aanvrager is gesignaleerd in RPS. Alle uitgevende instanties beschikken in hun frontoffice-processen over actuele signaleringen, doordat ze inzage hebben in het RPS. Inzage in RPS is alleen mogelijk indien er sprake is van een aanvraag of een inhouding en is zodanig ingericht dat niet meer gegevens worden verstrekt dan noodzakelijk in de fase van het reisdocumentenproces. In eerste instantie betreft dit alleen een hit/no hit bevraging of een persoon voorkomt in RPS zonder mededeling van signaleringsgrond. Pas bij een hit worden nadere gegevens verstrekt. Als back-up voorziening of bij wijze van extra controle zijn de actuele signaleringen ook beschikbaar in de backoffice processen van uitgevende instanties. Het proces van de

controle op en opvolging van de signalering is gedigitaliseerd. De uitkomst van dit proces wordt bovendien vastgelegd (datgeen wat nu met het C6 formulier wordt gecommuniceerd).

4. Digitalisering proces meervoudige vermissingen.
   Een zaak voor een meervoudige vermissing start zodra er sprake is van een nieuwe vermissing binnen de gestelde termijn. Bij het starten van een zaak worden automatisch al die gegevens bijeengebracht langs digitale weg die relevant zijn voor de beoordeling, zodat beoordeling door uitvoeringsjuristen in één gang mogelijk is. Daarbij kunnen ook gegevens ingewonnen worden van de burger, al dan niet via de digitale weg (verklaring van de burger, aangifte bij politie). In het verdere proces wordt de afstemming tussen uitgevende instantie en RvIG ook gedigitaliseerd. Deze digitalisering omvat overigens geen geautomatiseerde besluitvorming.
5. Self-service signalerende instanties.
   Formulierenstromen en briefwisseling tussen RvIG en signalerende instanties worden vervangen door functies op een self-service portaal en/of business services, zulks voor het gehele koninkrijk. Signalerende instanties dragen via dit portaal of via daarvoor gecreëerde business services zorg voor de ordentelijke administratie van 'hun' signaleringen. In het systeem wordt wat betreft signaleringsverzoeken, opslag en raadpleging van gegevens en terugmelding van beslissingen rekening gehouden met het feit dat de signaleringen vanuit de Caribische landen de wettelijke verantwoordelijkheid zijn van de Gouverneurs en dat de Gouverneurs in die gevallen dezelfde rol hebben als de Minister van BZK. Dit betekent dat er in het systeem vier signaleringsdomeinen moeten worden onderscheiden.
   De wettelijk beschreven marginale toets die Minister van BZK, in casu RvIG in Europees NL en de Gouverneurs in de Caribische landen uitvoeren op signaleringen, blijft eveneens ongewijzigd. Ook brieven om burgers te attenderen op hun signalering, bestaan nog steeds, hoewel een deel van die correspondentie via MijnOverheid is komen te lopen.
6. "Van rechtswege vervallen" situaties gesignaleerd en digitaal ondersteund.
   In sommige situaties komt een reisdocument van rechtswege te vervallen. Denk aan overlijden en naamswijzigingen, wijziging BSN, wijziging nationaliteit, wijziging verblijfsstatus en correctie geboortedatum. Deze situaties worden in eerste instantie veelal geadministreerd vanuit het beheer op de Burgerlijke Stand en/of de BRP. Dit operationele doel behelst een signalering vanuit deze administratieve verwerkingen naar autoriteiten, belast met de uitvoering van de Paspoortwet.
   Dit implementeren we bij gemeenten primair via de burgerzakenapplicaties. Leveranciers van de burgerzakenapplicaties bouwen hierin functies in om een reisdocument als vervallen te administreren in de kernregistratie in casu het Basisregister, in die gevallen dat de medewerker in kwestie dat van toepassing acht in het kader van de uitvoering van de Paspoortwet. Naast functies in de burgerzakenapplicaties voor het laten vervallen wordt voorzien in een portaaloplossing voor bijzondere omstandigheden waarvoor de burgerzakenapplicaties geen ondersteuning bieden of niet aanwezig zijn.
7. ID-check in aanvraag waar mogelijk met fotovergelijk.
   In de aanvraag wordt de identiteit van de aanvrager steeds op een deugdelijke wijze gecontroleerd. In die gevallen dat er sprake is van een eerdere aanvraag, wordt er bij de identiteitsverificatie altijd ook een vergelijking gedaan met de gezichtsopname uit de eerdere aanvraag of aanvragen. Hiertoe heeft de actuele uitgevende instantie beschikking over

die gezichtsopnames, alsmede de resultaten van een geautomatiseerde fotovergelijking.

8. Self-service vermissing voor alle houders.
   Alle houders van reisdocumenten hebben on-line voorzieningen waarmee ze hun document als vermist kunnen melden, onafhankelijk van de aanvraag van een nieuw document. De eerder gedefinieerde StopID-dienst maakt dit centraal mogelijk, wellicht via MijnOverheid.nl.
   Gemeentes hebben eerder al decentrale voorzieningen voor het on-line melden van vermissingen gerealiseerd. RvIG coördineert de co-existentie van de decentrale oplossingen en Stop-ID, zodat het on-line melden van vermissingen op een uniforme wijze wordt uitgevoerd ongeacht de aanbieder van de on-line mogelijkheid om de vermissing te melden. Het betrouwbaarheidsniveau van de authenticatie voor het melden van vermissingen is eIDAS Substantieel. Er zijn geen voorzieningen voor het on-line melden van een vermissing van een document, anders dan door de documenthouder zelf.
9. Overige statuswijzigingen van documenten gedigitaliseerd.
   Uitgevende instanties hebben voorzieningen waarmee ze statuswijzigingen van documenten kunnen doorvoeren, niet alleen de gevallen waarin een document vervalt van rechtswege (doel 6). De statuswijziging wordt direct doorgevoerd door die instantie die constateert dat een statuswijziging aan de orde is (dus niet per definitie de oorspronkelijke uitgevende instantie). Daarnaast kunnen ingevolge het wetsvoorstel invoering eID en uitbreiding basisregister reisdocumenten straks bij of krachtens Amvrb ook andere overheidsorganen worden aangewezen om statuswijzigingen door te geven.
10. Toekomstvaste ID-verificatie aan de hand van reisdocument.
    Er zijn vanouds partijen die een zwaarwegend belang hebben om een goede identiteitsverificatie te doen aan de hand van een reisdocument. Vele partijen bevragen daarbij het Verificatieregister (VR), via voorzieningen van hun koepelorganisatie.
    In de nieuwe situatie wordt de bevraging uitgebreid met informatie waarmee duidelijk wordt welke partij voor welk doel de identiteit verifieert aan de hand van het reisdocument.
11. Kernregistratie reisdocumenten; Cat 12 in BRP en PIVA niet meer in gebruik.
    De kernregistratie is een technische voorziening waarmee de gegevensopslag voor BR, VR en RPS (zoals bij en krachtens de Paspoortwet beschreven) wordt gerealiseerd. Daarnaast worden in de kernregistratie de voor de aanvraag en uitgifte benodigde gegevens opgeslagen (aanvraag zelf, administratieve gegevens over de aanvraag, gezichtsopname, handtekening en (tijdelijk) vingerafdruk).
    De categorie 12 gegevens in de BRP en PIVA zijn uitgefaseerd. Bevragingen van de cat12 gegevens zijn vervangen door bevragingen van of leveringen vanuit de kernregistratie reisdocumenten.
    De kernregistratie heeft ten opzichte van de bestaande losse systemen een versterkte informationele samenhang. Ze hanteren één logisch gegevensmodel en verwijzingen tussen de verschillende registers zijn eenvoudig mogelijk. Daarmee gaat de kernregistratie, ontsloten via een aantal informatieservices, zich logisch als één database gedragen. Een centrale kernregistratie zoals hier beschreven leidt tot beter bijgehouden en actuele gegevens, wat direct tot betere beslissingen leidt in de processen die van deze gegevens gebruikmaken, zoals het aanvraagproces. Daarbij wordt de kernregistratie wel zodanig ingericht dat de wettelijke verantwoordelijkheden en bevoegdheden ten aanzien van de verschillende registraties die hiermee zijn geïmplementeerd

volledig in stand blijven en er in de kernregistratie geen sprake zal zijn van processen die leiden tot geautomatiseerde besluitvorming.

12. Informatie halen per vraag, direct uit de kernregistratie.
    Informatieverstrekking is opnieuw ingericht, waarbij de informatie zoveel mogelijk per vraag actueel uit de kernregistratie reisdocumenten wordt opgehaald. Tussenliggende informatieproducten en kopiebestanden zijn (waar mogelijk) uitgefaseerd.
13. Privacy-by-design toegepast op informatieverstrekkingen.
    De komst van een kernregistratie, waarin de gegevens van het reisdocumentenstelsel worden opgeslagen, heeft er ook voor gezorgd dat informatieverstrekking anders gaat verlopen. De wettelijke grondslagen voor informatieverstrekkingen en de onderkende doelen staan op zich los van de technologische veranderingen. Echter, sommige doelen van partijen aan wie informatie wordt verstrekt zijn wel met minder gegevens te realiseren. In lijn met het beginsel van privacy-by-design zijn de informatieverstrekkingen daarom tegen het licht gehouden. Vragen zijn gesteld zoals:
    - Wat zijn de minimale gegevens die een afnemer nodig heeft voor een bepaald doel?
    - Kan een (huidige) verstrekking van bijvoorbeeld een bestand worden vervangen door een gerichte online bevraging?
    - Is het mogelijk het doel te bereiken met een hit/no-hit systematiek?

    De informatieverstrekking blijft uiteraard geautoriseerd en geprotocolleerd plaatsvinden. Evenals nu het geval is, zijn deze verstrekkingen opvraagbaar voor de burger (uitzondering inlichtingen- en opsporingsdiensten).
14. RAAS-en uitgefaseerd.
    De bij aanvang van het programma bestaande RAAS-en zijn nog één keer vervangen. Gedurende het programma zijn de RAAS-en vervangen door nieuw ontwikkelde functionaliteit.
    De hiervoor ontwikkelde business services zijn in de frontoffice toepassingen zoals RDM[3] geïntegreerd.
    Het aanvraagproces, zowel front-als backoffice, is via een webportaal aangeboden. De backoffice functies zullen uitsluitend via een webportaal beschikbaar komen.
15. Biometrieafname toekomstvast en flexibel.
    In de eerste periode van VRS zijn de huidige aanvraagstations in bedrijf, waarbij de gebruikte biometrische middelen alsmede het proces rondom het aanvraagstation (kaartje met aanvraag-id, foto en handtekening[4]) gelijk is gebleven. Er wordt echter rekening gehouden met ontwikkelingen als live enrollment. Er is voldaan aan eisen omtrent veiligheid en gebruikersvriendelijkheid, waarbij het beveiligingsconcept van het oorspronkelijke Aanvraagstation (AS) is geëvalueerd en mogelijk ook op een andere wijze technisch vormgegeven.
16. BR en VR uitgefaseerd.
    Het huidige in gebruik zijnde BR en VR zijn vervangen door bevraging van de kernregistraties reisdocumenten. De oorspronkelijk via het Verificatieregister (VR) aangeboden documentverificatieservice is door een toekomstvast alternatief vervangen, zie doel 10.

---

[3] RDM is de reisdocumentenmodule, waarmee gemeentelijke medewerkers de aanvraag van een reisdocument kunnen starten. RDM bestaat in verschillende varianten en wordt geleverd als onderdeel van de burgerzakensoftware door de gemeentelijke softwareleveranciers.

[4] In het kader van VRS wordt de verwerking van de gezichtsopname, de handtekening en (tijdelijk) de vingerafdruk voorzien. Dit wordt in dit document aangeduid als 'biometrie'. Er is discussie mogelijk of een handtekening wel een biometrisch gegeven is. Niettemin wordt het behandeld als ware het een biometrisch kenmerk met de bijbehorende voorzorgen.

17. Business services geïntegreerd met frontoffice applicaties.
    Ontwikkelde business services worden daadwerkelijk gebruikt, zowel in nieuw ontwikkelde portalen als in bestaande frontoffice applicaties zoals de reisdocumentenmodule (RDM).
    Achtergrond: Het programma voorziet in het ontwikkelen van business services en onderliggende informatie services. Het gaat er om dat deze services ook daadwerkelijk worden gebruikt in de diverse front-office applicaties. Denk bijvoorbeeld aan het integreren in RDM van een service voor het uitvoeren van een signaleringscontrole.
18. Formulieren en brieven gedigitaliseerd.
    De verschillende formulieren en brieven tussen de verschillende actoren zijn waar mogelijk vervangen door digitale faciliteiten. Voor signaleringenbeheer is dit al beschreven in doel 5. Alle operationele papierstromen in het aanvraag- en uitgifteproces zijn geheel gedigitaliseerd, met uitzondering van het C1 formulier bij de aanvraag van een vreemdelingenpaspoort. Formulieren rondom statusbeheer komen te vervallen omdat uitgevende instanties direct muteren op de kernregistraties.
    De verstrekking van informatie door de burger omtrent een vermissing (Verklaring vermissing, C2 formulier) is zowel on-line direct door de burger, of via een papieren formulier bij een uitgevende instantie mogelijk. In alle gevallen wordt de informatie rondom vermissingen centraal digitaal ter beschikking gesteld, waar mogelijk in de vorm van gestructureerde gegevens (bijlagen zoals scans van aangiftes worden niet als gestructureerde gegevens opgeslagen, de essentie van de inhoud van de aangifte wèl).
    De beschreven digitalisering impliceert dat in een aantal gevallen de 'natte handtekening' is komen te vervallen of door een elektronische ondertekening is vervangen, afhankelijk van de precieze situatie.
    De hierboven beschreven digitalisering houdt geen geautomatiseerde beslissingen met rechtsgevolgen voor de burger in.
19. Generiek servicegeoriënteerd IT-platform (Platform-as-a-Service, PaaS).
    Er is een generieke IT gerealiseerd, waar de informatievoorziening voor het reisdocumentenstelsel op is gerealiseerd. Dit maakt gebruikt van een PaaS bovenop een IaaS (Infrastructuur-as-a-Service). De doelstelling is dat er voor 'standaard' IT maximaal gebruik wordt gemaakt van het aanbod in de markt en van de schaalvoordelen die cloud-ontwikkelingen in de markt bieden, rekening houdend met de specifieke eisen op het gebied van security en privacy (De beoogde functionaliteit van het platform is elders in de PSA beschreven).
20. Varianten FO/BO-processen voorbereid.
    De taken (waaronder controles) in het aanvraag- en uitgifteproces zijn in hoge mate geüniformeerd, als opstap naar een uniforme proceskwaliteit. Tegelijkertijd is het technisch mogelijk geworden om die taken op verschillen plaatsen in het proces te leggen. De software voor de aanvraag- en uitgifteketen per uitvoeringsinstantie is daartoe configureerbaar gemaakt zodat taken aan de daarin betrokken organisatie-eenheden zijn toe te wijzen.
    Zodoende wordt het technisch mogelijk om verschillende operationele varianten van het aanvraag- en uitgifteproces te ondersteunen met dezelfde software.
    Van deze ingebouwde variatiemogelijkheden wordt binnen VRS geen gebruik gemaakt. Het feitelijk invoeren van dergelijke variatie is afhankelijk van nog te maken beleidskeuzen en voor sommige verschuivingen van taken zijn ook wetswijzigingen noodzakelijk.

21. Geborgde en meer uniforme kwaliteit van processen.
    De kwaliteit van het reisdocumentenstelsel is geborgd, waarbij wordt toegezien op de kwaliteit van zowel het aanvraag- en uitgifteproces, statusbeheer als signaleringenbeheer. De input voor de wijze van kwaliteitsborging komt uit het in oktober 2019 verwachte advies Toekomstbestendigheid kwaliteitsverbetering en toezicht. Een deel van de te borgen kwaliteitsnormen komt bovendien uit het in ontwikkeling zijnde Normenkader Nederlandse Identiteitsmiddelen.
    De wettelijk vastgelegde toezichtstaak die ziet op de kwaliteit van het reisdocumentenstelsel is bij RvIG belegd. VRS geeft, in samenwerking met het betreffende organisatiedeel van RvIG, handen en voeten aan kwaliteitsverhogende maatregelen en metingen. Kwaliteitsverhogende maatregelen zijn gelegen in het afdwingen van een aantal controles en het zorgen voor een uniforme uitvoering van die processen en ondersteuning van de controles in die processen. Zoals gezegd betreft dit dus niet uitsluitend het aanvraagproces, maar ook de uitgifte, statusbeheer en signaleringenbeheer. Uitgangspunt daarbij is dat RvIG de gehele keten 'van klant tot klant' overziet. Als onderdeel van het overzien van de gehele keten werkt VRS in afstemming met de relevante actoren een systematiek van kwaliteitsmetingen en -rapportages uit die in de nieuwe systemen worden gerealiseerd. Een en ander laat de wettelijke verantwoordelijkheden van de met de uitvoering van de Paspoortwet belaste autoriteiten onverlet.
22. Alternatieve documenten voorbereid.
    Er wordt geëxperimenteerd met verschillende alternatieve digitale 'documenten' en wijzes van identificeren, zoals vID (virtual ID), SSI (Self Sovereign Identity) en KTDI (Known Traveler Digital Identity). Om deze te ondersteunen wordt er in de architectuur rekening gehouden met de mogelijke komst van deze alternatieve 'documenten'. Concreet betekent dat dat er een notie van 'afgeleid document' in het gegevensmodel is opgenomen en dat statuswijzigingen in het 'hoofddocument' effect kunnen hebben op afgeleide documenten. Tevens betekent het dat we onderkennen dat er een specifiek aanvraag- en uitgifteproces is te verwachten.
    Het gaat in het bovenstaande om een beperkte technische voorbereiding, zonder wezenlijk te investeren in te realiseren functionaliteit of in te kopen technische faciliteiten. De feitelijke toepassing van alternatieve documenten is afhankelijk van nog te nemen beleidsbeslissingen en zullen waarschijnlijk ook wetswijzigingen met zich meebrengen.
23. Alternatieve aanvraag- en uitgiftekanalen voorbereid.
    In de toekomst worden aanvullende aanvraag- en uitgiftekanalen verwacht. Denk bijvoorbeeld aan plaatsonafhankelijk aanvragen of het online starten van een aanvraag. Hiermee wordt rekening gehouden door het mogelijk te maken dat een aanvraag wordt gestart via het ene kanaal en wordt afgemaakt via een ander kanaal en hier zaakmanagement als funderende techniek te gebruiken. Daarbij kan worden gekoppeld aan de systemen van andere partijen in de aanvraag- en uitgifteketens. Denk hierbij aan systemen van externe dienstverleners die ingezet worden door uitgevende instanties of aan externe logistieke dienstverleners die voor de uitgifte van reisdocumenten worden ingezet. Uitgangspunt is dat RvIG zicht op het ketenproces houdt en kan controleren of er aan de kwaliteitseisen wordt voldaan. De feitelijke toepassing van alternatieve aanvraag- en uitgiftekanalen is afhankelijk van nog te nemen beleidsbeslissingen en zullen dan ook wetswijzigingen met zich meebrengen.

24. Privacy-by-design voor opslag biometrie.
    Biometrie is in het kader van het reisdocumentenstelsel steeds de gezichtsopname, de handtekening en tijdelijk (tussen aanvraag en uitgifte) vingerafdrukken. De opslag van de gezichtsopname, handtekening en (tijdelijk) de vingerafdruk vindt plaats in een apart onderdeel van de kernregistratie (in het verleden ook aangeduid met ROB).
    Om de gegevens in dit onderdeel van de kernregistratie te beschermen tegen ongeoorloofde toegang en datalekken is een aantal concrete maatregelen genomen:
    - In dit onderdeel zelf zijn de gegevens opgenomen aan de hand van een pseudoniem. Er wordt geen direct of indirect identificerend nummer zoals een BSN, houdernummer, documentnummer of aanvraagnummer gehanteerd. Bij onverhoopt verlies van of ongeautoriseerde toegang tot de database heeft men alleen de beschikking over een groot aantal niet te relateren foto's en handtekeningen.
    - Het relateren van een aanvraagnummer (en daarmee indirect een houder) aan de biometrische gegevens is weliswaar mogelijk, maar is slechts mogelijk vanuit de context van een aanvraag dan wel een informatieverzoek dat door de uitgevende instantie, in overeenstemming met de regelgeving, is goedgekeurd.
    - Het omzetten van een aanvraagnummer naar de pseudoniemen in dit onderdeel is een extra beveiligde functie die met een hardware security module of iets vergelijkbaars wordt ondersteund.
    - Dit onderdeel zelf is uitgevoerd op een 'gehard' systeem, dat een minimaal 'aanvalsoppervlak' biedt.

3 Business Architectuur

3.1 Inleiding

In dit hoofdstuk wordt op hoofdlijnen vastgelegd wat de architectuurkaders en –richting zijn van het programma VRS op het gebied van producten en diensten, processen en organisatie.

Daarbij wordt uitgegaan van 2 productsoorten en 5 *hoofdprocessen*.

De (business) producten zijn:

- De verschillende reisdocumenten. (Weliswaar levert de uitgevende instantie dit product aan de burger, maar de Minister van BZK stelt hiervoor de normen en doet deze producten voortbrengen door een leverancier.)
- Identiteitsverificatie

De *hoofdprocessen* zijn:

Afkorting	Hoofdproces	Uitspraken in paragraaf
AU	Aanvraag- en uitgifte van een reisdocument	3.4
STABEH	Statusbeheer	3.5
SIGBEH	Signaleringenbeheer	3.6
INFO	Informatieverstrekking	3.7
GEBR	Gebruik van reisdocumenten	3.8

Richtinggevende uitspraken zijn hieronder per hoofdproces en de daarin te onderkennen deelprocessen beschreven, naast enkele algemene, hoofdprocesoverstijgende, uitspraken.

Gekozen is om in deze programmastartarchitectuur nog geen volledige procesbeschrijvingen op te nemen. Wel wordt er middels richtinggevende uitspraken richting gegeven aan en kaders gesteld voor de te ontwerpen hoofdprocessen. De processen zullen daarbij als onderdeel van de businessprojecten in het programma nader worden uitgewerkt.

Naast richtinggevende uitspraken zijn hieronder ter toelichting een aantal klantreizen om duidelijk te maken hoe het reisdocumentenstelsel in de toekomst gaat werken.

3.2 Klantervaringen

Wat merken de 'klanten' van het reisdocumentenstel nu van VRS? Wie zijn die klanten trouwens?

Bij 'klant' komt onmiddellijk het beeld op van de burger, die een reisdocument aanvraagt of gebruikt. Maar de groep klanten is veel breder. Het gaat ook om medewerkers van uitgevende instanties, signalerende instanties, de vele organisaties die identiteitsverificatie doen aan de hand van een reisdocument.

En ook: opsporingsinstanties die – gelukkig bij uitzondering – gegevens nodig hebben over de identiteit van burgers, inclusief een foto.

Wat verandert er zoal voor deze klanten? Hieronder zijn enkele casussen beschreven.

1. Aanvraag van een reisdocument

Myra werkt op de afdeling Burgerzaken bij de gemeente AA en Hunze en zij verzorgt aanvragen en uitgeven van reisdocumenten. Dhr. Velema uit Rolde komt langs voor een nieuw paspoort, omdat zijn paspoort oude binnenkort verloopt.

Myra klikt aan dat het gaat om een nieuwe paspoortaanvraag en haalt het oude paspoort door de lezer. Het systeem doet een aantal dingen:

- Achter de schermen wordt gecontroleerd of het oude paspoort inderdaad geldig is.
- Myra ziet meteen dat dhr. Velema naast dit oude paspoort ook een identiteitskaart van vorig jaar in zijn bezit heeft.
- Het systeem toont een duidelijke foto van de identiteitskaart van dhr. Velema aan de hand waarmee het eenvoudig is om te zien dat ze inderdaad dhr. Velema voor zich heeft staan.

Myra pakt een kaartje voor het aanvraagstation, voert het nummer daarop in in de aanvraagapplicatie. Ze plakt de pasfoto die ze zojuist heeft ontvangen erop en vraagt dhr Velema in het vakje te tekenen. Ze scant het kaartje op het aanvraagstation. Vervolgens neemt ze met de scanner op de balie de vingerafdrukken van dhr. Velema af. Ze krijgt de gescande foto te zien en ook de fotovergeijkingssoftware bevestigt dat de nieuwe foto goed overeenkomt met de eerdere foto van dhr. Velema.

Als dat allemaal gelukt is, wordt er betaald voor de aanvraag. Dan wordt nog gecontroleerd of er geen paspoortsignalering uitstaat voor dhr. Velema. Dat blijkt gelukkig niet het geval te zijn. Na de backoffice controle gaat de aanvraag door voor personalisatie.

Een paar dagen later wordt een pakketje reisdocumenten ontvangen van de leverancier. Ze worden gecontroleerd en ingescand. Ook het paspoort van dhr. Velema zit er tussen. Als dhr. Velema een paar dagen later zijn paspoort komt ophalen wordt de uitreiking afhandeld door Yvonne, de collega van Myra, in verband met functiescheiding. Zodra er twee of meer medewerkers voor 'regulier' werk beschikbaar zijn, dwingt het systeem functiescheiding af. Nu wordt er nog een keer een identiteitscontrole gedaan aan de hand van het nieuwe paspoort en wordt er nogmaals een controle gedaan op de signaleringen. Het oude paspoort wordt ontwaard en meer Velema krijgt het – met gaten – weer mee naar huis. Yvonne registreert dat in het systeem. Het oude paspoort is daarmee een souvenir voor dhr. Velema geworden.

2. Signaleringenbeheer

Jaap werkt bij DUO. Als onderdeel van zijn werkzaamheden zorgt hij er ook voor dat daarvoor in aanmerking komende personen met een grote problematische studieschuld worden aangemeld voor een signalering in het Register paspoortsignaleringen. Die worden dan nog wel gecontroleerd door RvIg, voordat het actieve signaleringen worden.
Recent is de werkwijze fors veranderd. Vroeger was dat een proces met veel papier en bellen. De signaleringsverzoeken worden ingevoerd in een portaal

van RvIG, waar Jaap met eHerkenning op inlogt. Ook worden geregeld exports van de van DUO afkomstige signaleringen uit dat systeem gemaakt en door DUO gecontroleerd op actualiteit. Jaap kan zelf ook eenvoudig signaleringen laten vervallen of verlengen in dat portaal.
Contacten omtrent de signalering tussen DUO, RvIG en een eventuele uitgevende instantie worden bovendien in het portaal mogelijk gemaakt, zodat alle betrokken partijen goed op de hoogte blijven.

3. Gesignaleerde persoon vraagt paspoort aan bij grensgemeente

Mieke behandelt grensgemeente-aanvragen van reisdocumenten bij Den Haag.

Dhr. Talpa heeft zich 3 jaar geleden uit laten schrijven bij zijn gemeente, omdat hij zich ging vestigen in het buitenland. Zijn huidige woonplaats is onbekend. Dhr. Talpa heeft diverse problematische schulden bij overheidsinstanties, die hij niet aflost en waar hij geen afbetalingsregeling op heeft getroffen. Dhr. Talpa is onvindbaar voor deze instanties.

Op enig moment meldt dhr. Talpa zich in Den Haag voor een nieuw paspoort. Mieke behandelt zijn aanvraag. Hij identificeert zich met zijn oude paspoort. De aanvraag verloopt aanvankelijk regulier. Nadat de aanvraag echter in behandeling is genomen, blijkt dat er twee signaleringen voor dhr. Talpa zijn opgenomen in het Register paspoortsignaleringen.

Mieke geeft aan dat zij voornemens is de aanvraag te weigeren en overlegt de gegevens omtrent de 2 signaleringen aan dhr. Talpa. Dhr. Talpa protesteert nog wat om Mieke over te halen 'niet zo moeilijk te doen'. Mieke geeft aan dat zij wel direct een nieuwe aanvraag kan aanmaken voor een identiteitskaart. Dhr. Talpa is het er niet mee eens maar vertrekt, terwijl hij krachttermen uitslaat. Mieke registreert een weigering in het systeem met redenen.

De volgende dag meldt dhr. Talpa zich in Breda, om ook hier een paspoort aan te vragen. Nu blijkt uit het systeem al snel dat dhr. Talpa het gisteren al in Den Haag heeft geprobeerd. De gegevens van de weigering worden opgevraagd. Omdat er niets aan de situatie is veranderd wordt dhr. Talpa ook hier geweigerd.

4. Parallelle aanvragen

Piet werkt in Breda en hij voert daar geregeld het grensgemeenteproces uit. Mw. Animo is enkele jaren geleden geemigreerd naar Indonesie en ze is nu op vakantie in Nederland. Ze vraagt bij de gemeente Breda een nieuw paspoort aan. Piet behandelt haar aanvraag.

Maar bij het registreren van haar aanvraag wordt geconstateerd dat ze 2 dagen eerder ook in Den Haag een aanvraag heeft gedaan. Piet vertelt dat hij de aanvraag verder niet gaat behandelen en verwijst mw. Animo terug naar Den Haag. Het feit dat mw. Animo dit heeft geprobeerd, wordt echter wel geregistreerd.

5. Paspoort gestolen op vakantie

Mw. Willems is op vakantie bij haar dochter in de Verenigde Staten en wordt bestolen. Ook haar paspoort is bij de gestolen spullen. Ze meldt zich op een Nederlandse post om een nieuw reisdocument te verkrijgen. Omdat er nog

even tijd is, kan een vervangend normaal paspoort worden aangevraagd. Ze heeft geen scan van haar oude paspoort gemaakt. Dat blijkt geen probleem te zijn, het systeem op de post geeft direct inzicht in de gegevens van het oude paspoort en de daarop aanwezige foto. Ook kan het oude paspoort direct in het systeem op 'ongeldig' worden gezet, zodat daarvan geen misbruik meer kan worden gemaakt. Dat hoeft niet meer door de gemeente van mw. Willems te worden gedaan.
Wel moet mevrouw Willems nog een formulier 'Verklaring vermissing' invullen en samen met een kopie van de aangifte van de diefstal inleveren. Ze doet dat ter plekke.

Het nieuwe paspoort wordt voor een redelijke vergoeding zelfs bezorgd op het adres van haar dochter.

6. Reisdocument vermist en gemeld met StopID

Dhr. Pieterse wordt op zakenreis in Parijs bestolen en raakt zijn paspoort kwijt. Gelukkig heeft hij zijn mobiel nog wel. Hij gaat naar de StopID website en meldt - na het inloggen met zijn DigiD app – direct het paspoort als gestolen. Vervolgens gaat hij naar de politie om aangifte te doen.
Gelukkig is het in Frankrijk, dus hij reist terug naar huis zonder een nooddocument aan te vragen.
Bij zijn gemeente meldt hij zich om een nieuw paspoort aan te vragen. Daar kan men eenvoudig constateren dat zijn oude document gestolen is, maar ook constateren dat hij nog een aangifte moet inscannen en insturen. Daar wordt hij op gewezen.

7. Opvragen foto door de politie

Dhr. Janse werkt bij de politie aan een zaak. De politie heeft op deze zaak onder meer behoefte aan een foto van burger. Waar dat vroeger een bezoekje aan een gemeente betekende, is dat nu beter geregeld. Dhr. Janse maakt in zijn backoffice een digitaal verzoek aan voor de gegevens van deze burger. Dit verzoek wordt richting RvIG 'geschoten' en vandaar gerouteerd naar de gemeente Arnhem waar deze persoon vorig jaar een paspoort heeft gekregen. Bij de gemeente Arnhem beoordeelt men het verzoek.

Na goedkeuring van het verzoek door de gemeente Arnhem worrden de gegevens van deze burger, inclusief de foto in een bericht verzameld en op veilige wijze teruggestuurd.

3.3 Hoofdprocesoverstijgende zaken

De volgende richtinggevende uitspraken worden gehanteerd, die de onderkende ketendiensten overstijgen.

B-ALG-01	RvIG is regisseur van de hoofdprocessen a) aanvraag en uitgifte, b) statusbeheer, c) signaleringenbeheer en informatieverstrekking.
Statement	Binnen de hoofdprocessen voor aanvraag en uitgifte, statusbeheer en signaleringen zijn meerdere ketenpartners actief. Deze ketenpartners zijn verantwoordelijk voor onderdelen in deze ketens, wat veelal is vastgelegd als wettelijke taak.

	RvIG is (keten)regisseur voor deze hoofdprocessen. Dit houdt het volgende in: - Ontwerp van het hoofdproces; - Bepalen van verplichte technische inrichtingseisen aan de keten zoals standaarden en verplicht gebruik van bepaalde technische faciliteiten; - Bepalen van de gemeenschappelijke normen voor de keten, bijvoorbeeld aangaande de kwaliteit, tijdigheid en beveiliging; - Het bewaken van deze normen; - Afleggen van verantwoording over de werking van de keten; - Coördinatie van incidenten; - Coördinatie van fraudedetectie en -preventie.
Rationale	RvIG wil, uit de aard van haar bijgestelde missie, regie voeren over de identiteitsketen(s). Dat impliceert dat RvIG ook regie voert over de genoemde hoofdprocessen. Dit is in lijn met de wettelijke rol als toezichthouder.
Implicaties	Een van de belangrijkste consequenties is dat RvIG, meer dan in het verleden het geval was: - Kan bepalen wat voor kwaliteitsborgende maatregelen, technisch of procedureel, in het proces worden ingebouwd (controlestappen in het aanvraagproces bijvoorbeeld); - Zicht heeft op deze hoofdprocessen, in de zin dat we kritische kwaliteitsaspecten kunnen meten. Geaggregeerd spreken dan vooral over management informatie. Informatie over individuele gevallen levert 'leergevallen' op die door RvIG ter bespreking met ketenpartners geagendeerd kunnen worden.

B-ALG-02	**We werken zaakgericht in het reisdocumentenstelsel.**
Statement	Binnen het reisdocumentenstelsel wordt zaakgericht gewerkt. Een zaak wordt gedefinieerd als samenhangende hoeveelheid werk met een gedefinieerde aanleiding en een gedefinieerd resultaat, waarvan de kwaliteit en doorlooptijd moet worden bewaakt. Zaakgericht werken omvat: - Bewaken van de informatiestroom van een zaak. - Bewaken van de voortgang van een zaak. - Delen van de voortgang van een zaak met alle belanghebbenden. Zaakgericht werken is in het reisdocumentenstelsel alleen van toepassing als: - Het werk verdeeld is over meerdere stappen en meerdere actoren; - Het wenselijk is de voortgang te bewaken; - Het wenselijk is de kwaliteit te bewaken; - Het resultaat terug te koppelen en/of te delen Een zaak eindigt bij de actor waarmee die zaak start. Een aanvraag eindigt met de (bevestigde) uitgifte van een document. Een signaleringsverzoek start bij de signalerende instantie en eindigt met een terugkoppeling aan die signalerende instantie. Een melding van de burger eindigt met een bevestiging van de verwerking van die melding aan die burger. Et cetera.

	Binnen het reisdocumentenstelsel kennen we diverse varianten van zaakgericht werken: 1. Een zaak die geheel binnen RvIG wordt afgehandeld. Hierbij krijgt de medewerker een systeem met interactieve ondersteuning voor de afhandeling van een zaak, c.q. het uitvoeren van een concrete stap in een zaak. Managers krijgen faciliteiten om werk toe te wijzen, voortgang van de werkvoorraad te bewaken etc. 2. Een zaak die over verschillende actoren in de keten loopt. Hierin is onderscheid te maken in a) Die gevallen waarbij de ketenpartner gebruikt maakt van een portaal dat in het kader van VRS wordt gerealiseerd. In die gevallen lijkt de ondersteuning sterk op variant 1; b) Die gevallen waarbij de ketenpartner gebruik maakt van eigen systemen. In dit geval zal de zaak waarschijnlijk starten en stoppen bij de ketenpartner. Het systeem van de ketenpartner signaleert dat starten en stoppen alsmede overige relevante statusovergangen van de zaak met het zaaksysteem van RvIG / VRS. Hiermee kan RvIG de overall keten bewaken en aldus de kwaliteit van de hoofdprocessen beheersen.
Rationale	De toepassing van zaakgericht werken en de bijbehorende informatievoorziening biedt wezenlijke voordelen voor de bewaking van kwaliteit en voortgang. In de geautomatiseerde ondersteuning van zaken zijn er bovendien aanvullende mogelijkheden die binnen bereik komen. In het kader van het reisdocumentenstelsel zijn dan relevant: - Kwaliteitsbewaking: zijn alle vereiste controles wel verricht? - Flexibel kunnen inrichten van een workflow ter afhandeling van een zaak over organisaties c.q. organisatiedelen heen. Het wordt eenvoudiger om verschillende procesvarianten voor een bepaald zaaktype te ondersteunen. - Een aanvraag wordt gestart via het ene kanaal (bijvoorbeeld online), maar uiteindelijk afgemaakt via een ander kanaal (bijvoorbeeld aan de balie) - Verschuiven van werk tussen medewerkers in eenzelfde organisatie of organisatiedeel, bijvoorbeeld in verband met specifiek noodzakelijke kennis en kunde. - Inroepen van 'meekijk' hulp in de behandeling door een (andere) specialist (onder verantwoordelijkheid van de aangewezen behandelaar). Bovengenoemde mogelijkheden zijn al relevant voor de scope van VRS, zij het dat niet alle bovenstaande mogelijkheden per definitie door VRS geboden gaan worden. Na VRS kan het zaakgericht werken grotere verschuivingen van taken mogelijk maken. Denk dan bijvoorbeeld aan het desgewenst (na beleidsvorming) verschuiven naar een regionale of centrale backoffice van bepaalde controlewerkzaamheden.
Implicaties	- Zaakgericht werken leidt er toe dat kwaliteit en voortgang heel transparant worden, wat voor de dienstverlening een groot voordeel is. - Zaakgericht werken wordt meestal als een cultuurverandering ervaren. Medewerkers worden ingeroosterd om een bepaald deel van hun tijd zaken af te handelen. Daarbinnen gelden dan normen voor kwaliteit en productietempo.

B-ALG-03	De hoofdprocessen a) aanvraag en uitgifte, b) statusbeheer en c) signaleringenbeheer alsmede d) informatieverstrekking hebben een uniforme en geborgde kwaliteit.
Statement	Een belangrijk onderdeel van de regie op genoemde hoofdprocessen is het streven naar een *uniforme kwaliteit* van die hoofdprocessen, ongeacht de organisaties die bij het uitvoeren van dat hoofdproces betrokken zijn. RvIG hanteert hiervoor een kwaliteitsmanagementsysteem.
Rationale	RvIG wenst een bepaalde kwaliteit van haar business-producten zoals bovenstaand te kunnen bieden. Het bieden van een betrouwbaar reis-/identiteitsdocument en betrouwbare identiteitsverificatie zijn belangrijke doelen. In de huidige situatie komen er nog aanzienlijke kwaliteitsverschillen voor in de kwaliteit van de hoofdprocessen, afhankelijk van de uitvoerder van die hoofdprocessen. Dit doet af aan de kwaliteit van het reisdocument / identiteitsverificatie. Hierop gerichte verbetering is dus wenselijk. Concrete acties zijn: - Uniformeren van de hoofdprocessen, geborgd door de informatiesystemen en services; - Hanteren van een kwaliteitsmanagementsysteem. Hiermee geven we bovendien nadere invulling aan het principe uit de RvIG referentiearchitectuur *B3-BEH-05, Gelijkmatige kwaliteit totale keten*, wat op zijn beurt weer is afgeleid uit de NORA-principes. De wijze van kwaliteitsborging – momenteel wordt er gebruik gemaakt van een zelfevaluatie – wordt momenteel geëvalueerd. In oktober 2019 wordt een advies hierover verwacht: Toekomstbestendigheid kwaliteitsverbetering en toezicht. Het kwaliteitsmanagementsysteem zal met de aanbevelingen uit dit advies rekening houden. Een deel van de te borgen kwaliteitsnormen heeft betrekking op de aanvraag- en uitgifteproces voor reis- en identiteitsdocumenten alsmede die documenten zelf. Deze zullen dienen te passen binnen het ontwikkeling zijnde Normenkader Nederlandse Identiteitsmiddelen.
Implicaties	RvIG hanteert voor het borgen van de kwaliteit een kwaliteitsmanagementsysteem, dat wil zeggen een samenhangend geheel van alle activiteiten die erop zijn gericht om de processen conform een vastgestelde kwaliteit te laten verlopen en producten van een vastgestelde kwaliteit voort te brengen. Dat impliceert: - Voor de hoofdprocessen (en eventueel de voortgebrachte business producten) worden de kwaliteitsnormen en wijze van meting van die normen voorgeschreven. (het 'wat'). - Deels worden bepaalde werkwijzen en standaarden ter uitvoering en ondersteuning verplicht. - Ook gebruik van bepaalde (IT) techniek kan verplicht zijn. - De bereikte kwaliteit worden gemeten. Afwijkingen van de norm worden besproken en afspraken worden gemaakt om de gewenste kwaliteit alsnog te bereiken. RvIG neemt hierin het voortouw.

	- De feitelijk gerealiseerde kwaliteit is transparant voor alle partijen in het reisdocumentenstelsel. - Kwaliteitsissues die meerdere ketenpartijen raken worden in een passend overleg met betreffende ketenpartijen besproken.

B-ALG-04	**Ketenpartners krijgen (beperkte) vrijheid van inrichting van het proces, passend binnen de kaders die RvIG formuleert vanuit de uniforme kwaliteit.**
Statement	We bieden, binnen de hoofdprocessen aanvraag en uitgifte, statusbeheer en signaleringenbeheer, de ketenpartners de mogelijkheid hun procesinrichting zelf te regelen, met behoud van kwaliteit en veiligheid. Tegelijkertijd wordt deze vrijheid ook beperkt door de techniek. We geven alleen vrijheid op die punten waar we voorzien dat daar behoefte aan bestaat op korte of lange termijn.
Rationale	We zien dat met name uitgevende instanties het aanvraag- en uitgifteproces al enigermate verschillend uitvoeren. Denk bijvoorbeeld aan de variaties bij Buitenlandse Zaken en KMar. In het signaleringenbeheer is het ook de te verwachten dat er (meer subtiele) variaties zullen optreden. Tegelijkertijd willen we over de verschillende ketenpartners heen een gelijkmatige kwaliteit kunnen garanderen. NB De uitspraak is minder nieuw dan het wellicht lijkt: we hebben nu immers ook al een zekere vrijheid per uitgevende instantie, wat nu leidt tot verschillende RAAS-en.
Implicaties	RvIG maakt een standaard indeling van het aanvraagproces, waarin verplicht een aantal controles worden uitgevoerd. Door die controles verplicht te maken en die meer te uniformeren, zal het aanvraagproces naar verwachting een meer uniforme kwaliteit krijgen. Zie B-AU-01. De vrijheid van procesinrichting zal voor het aanvraagproces zich beperken tot een variabele volgorde van voorgeschreven controles vanuit de eigen applicaties (bijvoorbeeld RDM), en het ondersteunen met een aanvraagportaal van een beperkt aantal (ordegrootte 6-8) varianten. Dat laatste kan vergeleken worden met de ondersteuning van meerdere RAAS-configuraties. Uitgangspunt is dus te onderkennen dat uitgevende instanties verschillend zijn, maar enigszins een rem te zetten op het aantal te ondersteunen varianten. In het algemeen zal RvIG meer inzetten op een toezichthoudende en controlerende taak voor wat betreft het voldoen aan de gestelde kaders, dan op het technisch 'dichtregelen' (door bijvoorbeeld slechts één procesvariant te ondersteunen). Zulks in lijn met het bieden van services die in eigen applicaties gebruikt kunnen worden.

B-ALG-05	Informatiebeveiliging in hoofdprocessen wordt waar mogelijk als kwaliteitsafspraak ingeregeld, om de ketenpartners flexibiliteit in procesinvulling te bieden.
Statement	Beveiligingseisen worden gesteld conform het BZK en aanvullend het RvIG IB-beveiligingsbeleid, mede op basis van een risicoanalyse. Om meer flexibiliteit in het proces mogelijk te maken met behoud van het niveau van beveiliging, wordt een aantal beveiligingseisen met name opgelegd aan ketenpartners, die daar vervolgens op verschillende wijze invulling aan kunnen geven.
Rationale	Dit is een verbijzondering van B-ALG-04.
Implicaties	Informatiebeveiliging van de RAAS-en als zodanig wordt vervangen door andere concepten, zoals de beveiliging van de centrale ICT-systemen.

B-ALG-06	Formulieren en brieven worden gedigitaliseerd.
Statement	De verschillende formulieren en brieven tussen de verschillende actoren zijn waar mogelijk vervangen door digitale faciliteiten.
Rationale	Formulierstromen zijn ongewenst. De verwerking ervan is arbeidsintensief, foutgevoelig en leidt tot ongewenste vertraging. Met centralisatie van de gegevenshuishouding met betrekking tot reisdocumenten is er bovendien nauwelijks meer een noodzaak om formulieren te hanteren (voor de belangrijkste processen). Burgers verwachten tegenwoordig te kunnen kiezen hoe zij worden aangeschreven door de overheid: langs de papieren weg, of via Mijn Overheid.
Implicaties	De verandering gepreciseerd (zie ook de operationele doelen): - Signalerende instanties voeren hun signaleringsverzoeken direct in een portaal in. - Alle operationele papierstromen in het aanvraag- en uitgifteproces zijn geheel gedigitaliseerd, met uitzondering van het C1 formulier bij de aanvraag van een vreemdelingenpaspoort. - Formulieren rondom statusbeheer komen te vervallen omdat uitgevende instanties direct muteren op de kernregistratie. - De verstrekking van informatie door de burger omtrent een vermissing (Verklaring vermissing, C2 formulier) is zowel on-line direct door de burger, of via een papieren formulier bij een uitgevende instantie mogelijk. In alle gevallen wordt de informatie rondom vermissingen centraal digitaal ter beschikking gesteld, waar mogelijk in de vorm van gestructureerde gegevens (bijlagen zoals scans van aangiftes worden niet als gestructureerde gegevens opgeslagen, de essentie van de inhoud van de aangifte wèl). - Brieven aan burgers blijven bestaan. Er zal rekening worden gehouden met de voorkeur van burgers om correspondentie via MijnOverheid te ontvangen. - Brieven aan de burger die nu door de uitgevende instantie worden gestuurd blijven in de toekomst ook door de uitgevende instantie worden verstuurd, bijvoorbeeld brieven ter notificatie van het binnenkort verlopen van een reisdocument. Die ontvangt hiervoor desgewenst een mailmerge bestand vanuit RvIG.

	De beschreven digitalisering impliceert dat in een aantal gevallen de 'natte handtekening' is komen te vervallen of door een elektronische ondertekening.

B-ALG-07	Kernregistratie reisdocumenten. Eenmalige registratie, meervoudig gebruik voor gegevens omtrent reisdocumenten.
Statement	De kernregistratie is een technisch gecentraliseerde voorziening waarmee de enkelvoudige gegevensopslag voor BR, VR en RPS (zoals bij en krachtens de Paspoortwet beschreven) wordt gerealiseerd. Daarnaast worden in de kernregistratie de voor de aanvraag en uitgifte benodigde gegevens opgeslagen (aanvraag zelf, administratieve gegevens over de aanvraag, gezichtsopname, handtekening en (tijdelijk) vingerafdruk). Deze gegevens worden decentraal beheerd door uitgevende instanties. De regels die met betrekking tot verstrekking van deze gegevens worden gesteld, zijn onveranderd in lijn met de verantwoordelijkheid van de uitgevende instantie. Aanvullend worden deze gegevens door uitgevende instanties ook aan RvIG ter beschikking gesteld, om regie te voeren over het hoofdproces aanvraag en uitgifte. De kernregistratie wordt door alle ketenpartners direct gebruikt, in plaats van afgeleide bestanden. (Zie ook operationeel doel 11.)
Rationale	Versnippering van de gegevens omtrent reisdocumenten, zoals momenteel het geval is, leidt tot lagere kwaliteit, actualiteit en volledigheid van die gegevens dan mogelijk en gewenst. Dergelijke lagere actualiteit en kwaliteit wordt ook gezien bij het gebruik van kopiebestanden. Ook kunnen informatieverstrekkingen eenvoudig meer uniform worden ingericht, waar dit nu nog een decentrale verantwoordelijkheid betreft en de feitelijke levering niet gestandaardiseerd is. Gekozen is voor een (landelijke) kernregistratie en niet voor een basisregistratie, aangezien de match met de 12 criteria voor een basisregistratie onvoldoende is.
Implicaties	Het vormen van een kernregistratie heeft een aantal consequenties, in de zin 'wat moet ervoor geregeld worden om te komen tot een goedwerkende kernregistratie' - Ontsluiting van bestaande systemen met gegevens. De gegevens zijn nu op verschillende plaatsen opgeslagen. In CORI, in RAAS-en, in het oude BR, in RPS. RAAS-en en het oude BR komen te vervallen en de gegevens worden gemigreerd. De gegevens in CORI alsmede RPS, als systemen die blijven bestaan, worden via een informatieservice-'stekker' beschikbaar gesteld, zodat daar door gebruikers van de kernregistratie gebruik kan worden gemaakt; - De informationele samenhang van de verschillende databases, die samen de kernregistratie vormen, dient te worden versterkt. Hiermee worden verwijzingen eenvoudig mogelijk en wordt (referentiële) integriteit bewaakt. Dit als tegenstelling ten opzichte van de huidige losse relatie die tussen de gegevens in de verschillende systemen bestaan; - Als onderdeel van het versterken van deze informationele samenhang van de verschillende registraties wordt er één virtuele

	registratie gemaakt van alle burgers die we kennen in relatie tot het reisdocumentenstelsel. Waar mogelijk wordt dit gerealiseerd door verwijzing naar bestaande registraties. - Hoge beschikbaarheid van de kernregistratie en de (netwerk)ontsluiting. Omdat ketenpartners zoals uitgevende instanties en verifiërende instanties direct bediend gaan worden vanuit de kernregistratie en kopie-bestanden afgeschaft zijn, zijn netwerkverbindingen met een (zeer) hoge beschikbaarheid cruciaal. - De categorie 12 gegevens verdwijnen uit de BRP en PIVA. Zie B-ALG-08

B-ALG-08	**Uitfasering categorie 12 BRP en PIVA**
Statement	De keuze voor een kernregistratie reisdocumenten impliceert de uitfasering van de categorie 12 gegevens uit de BRP. Dit vindt noodzakelijkerwijs gefaseerd plaats.
Rationale	Een consequentie van B-ALG-07 is dat er geen plaats meer is voor de registratie omtrent reisdocumenten in de BRP. Die registratie in de BRP kent toch al een aantal problemen, met name a) de handmatige verwerking van gegevens omtrent signaleringen die via een 'vrij bericht' en kwaliteitsmonitor worden aangeleverd en b) het feit dat alleen van ingezetenen een deugdelijke administratie van die reisdocumentengegevens wordt bijgehouden. Deze problemen komen te vervallen bij de invoering van de kernregistratie reisdocumenten.
Implicaties	Met de vorming van een kernregistratie reisdocumenten komt het gebruik van categorie 12 gegevens in de BRP en PIVA's ten einde. Afgestemd is dat dit in grote lijnen als volgt zal plaatsvinden: - Gebruikers/afnemers van de categorie 12 gegevens zullen worden aangesloten op de nieuwe kernregistratie en de hierop gebouwde informatieverstrekking. Uiteraard voor zover ze aangeven van deze informatievoorziening gebruik te willen maken. Omdat dit verstrekkingen zijn uit (juridisch gezien) het Basisregister, zullen deze partijen hiervoor nieuw geautoriseerd moeten worden krachtens de Paspoortwet. - Met uitzondering van 12.36.10 Dit element in categorie 12 geeft de signalering weer. Om dit te vervanngen moet er een verstrekking uit de nieuwe kernregistratie plaatsvinden (RPS) (=wetswijziging) - Voor het beheer van de status van reisdocumenten worden voorzieningen aangeboden, die direct op de kernregistratie werken en uitgevende instanties, alsmede andere autoriteiten die bevoegd zijn sommige statuswijzigingen door te voeren, gaan hiervan gebruik maken - Nadat de kernregistratie de volledige en actuele gegevens omtrent reisdocumenten en signalering bevat en partijen informatie hieruit verstrekt krijgen, worden de categorie 12 gegevens (en de verstrekking daarvan) feitelijk overbodig. Administratie en beheer van die categorie 12 gegevens kan dan komen te vervallen. Een wetswijziging voor de Wet BRP is hiervoor nodig. Wetswijzigingen zijn ook voor de PIVA's aan de orde.

	- Bovengenoemde wetswijzigingen aan de kant van de BRP en PIVA, vallen buiten de scope van VRS. Uiteraard worden de wijzigingen wel in nauwe afstemming doorgevoerd en gecommuniceerd.

3.4 Aanvraag en uitgifte

3.4.1 Algemeen

Het aanvraag- en uitgifteproces bestaat op het hoogste beschouwingsniveau uit de volgende *deelprocessen*:

- Aanvragen
- Beoordelen
- Produceren en personaliseren
- Distribueren
- Uitgeven (synoniem met uitreiken)

Deelprocessen zijn samengesteld uit *processtappen*. De procesontwerpen worden opgeleverd als onderdeel van het project Aanvraag en uitgifte en statusbeheer. Processtappen bestaan uit *activiteiten* en worden ondersteund door *business services*.

B-AU-01	**Hoge, welbepaalde kwaliteit van aanvraag en uitgifteproces**
Statement	Het aanvraag- en uitgifteproces is van een uniforme kwaliteit, ongeacht de specifieke omstandigheden van de uitgevende instantie en diens eventuele dienstverleners (zoals bezorgdiensten). Dezelfde controles in het aanvraag- en uitgifteproces vinden altijd plaats, op een kwalitatief vergelijkbare wijze.
Rationale	Zie B-ALG-03
Implicaties	- Een lijst controles is af te werken, als onderdeel van de hoofdproces aanvraag en uitgifte. Deze controles worden waar mogelijk technisch afgedwongen. - Binnen het deelproces produceren en personaliseren hebben we geen controles, slechts het eindresultaat (het gepersonaliseerde reisdocument) is aan controles onderhevig. - Afhankelijk van de uitvoeringskwaliteit van bepaalde organisaties of organisatiedelen kunnen aanvullende controles worden ingelast, om de beoogde kwaliteit te realiseren. De workflow is dus flexibel te configureren, afhankelijk van bij de aanvraag en uitgifte betrokken partijen. - Voor de te bereiken kwaliteit van het aanvraag- en uitgifteproces wordt een kwaliteitsmanagementsysteem opgezet. Een norm wordt daarbinnen nog vastgesteld alsmede een methode om de realisatie ten opzichte van die norm te meten.

B-AU-02	Volledige en gedigitaliseerde controle op RPS-signaleringen in aanvraagproces
Statement	In het aanvraagproces wordt in alle gevallen gecontroleerd op RPS-signaleringen. RvIG krijgt inzicht in het raadplegen van die signaleringen en de wijze waarop de uitgevende instantie hiermee omgaat.. Binnen de context van een aanvraag kan de behandelend medewerker ook de reden opvragen voor een signalering. Bij de uitgifte wordt nogmaals gecontroleerd op een eventuele RPS-signalering.
Rationale	Zie betreffende operationele doel. Dit is gewenst om een hoge en uniforme kwaliteit zeker te stellen.
Implicaties	- In het aanvraag- en uitgifteproces dient deze controle plaats te vinden. Dit wordt zoveel mogelijk geautomatiseerd. - Bij de aanwezigheid van een signalering dient te worden aangegeven hoe de uitgevende instantie hiermee omgaat. Dit wordt vastgelegd in de kernregistratie. Deze gegevens dienen voor RvIG om de kwaliteit van het proces aanvraag en uitgifte te beheersen. Deze gegevens of een samenvatting hiervan kunnen ook verstrekt worden aan actuele uitgevende instanties in het kader van het voorkomen van shopgedrag (operationeel doel 2).

B-AU-03	Uitgevende instantie kan de reden voor een RPS-signalering digitaal raadplegen binnen de context van een aanvraag
Statement	Binnen de context van een aanvraag kan de behandelend medewerker ook de reden opvragen voor een RPS-signalering, zulks op verzoek van de aanvrager. Zodoende kan die medewerker aan de aanvrager laten weten met welke instantie die contact dient op te nemen.
Rationale	Momenteel wordt informatie over signaleringen verstrekt via menselijke tussenkomst bij RvIG. In dit contact wordt de rechtmatigheid van het verzoek ook wordt getoetst. Er is echter geen reden waarom dit niet ook digitaal zou kunnen, mits de gegevens slechts selectief beschikbaar worden gesteld in de relevante gevallen. Door te regelen dat deze RPS-signaleringen alleen raadpleegbaar zijn binnen de context van een aanvraag is de privacy goed geregeld.
Implicaties	Het opvragen van de RPS-signaleringsinformatie verloopt in 2 separate acties: - Het opvragen of er bij de aanvrager van een reisdocument een RPS-signalering aanwezig is; - Het opvragen van de signalerende instantie en contactgegevens van die signalerende instantie en (eventueel, nog te beslissen) een indicatie van de signaleringsgrond. - Informatie over RPS-signaleringen wordt beperkter beschikbaar. De informatie wordt niet in gemeentelijke systemen meer opgeslagen en op termijn ook niet meer via categorie 12 BRP. Het raadplegen van RPS wordt in praktische zin geregeld door RvIG. RvIG kan informatie over signaleren aan de burger ter beschikking stellen onder voorwaarden van afdoende beveiliging en een afdoende niveau van authenticatie (DigiD Substantieel).

B-AU-04	Uitgevende instanties hebben zicht op 'hun' aanvragen en in behandeling zijnde documenten tot het moment van uitgifte
Statement	Uitgevende instanties hebben zicht op de aanvragen die via hen lopen cq liepen, alsmede de status van die aanvragen en de organisatie of

	het organisatiedeel waar deze in behandeling is. Ook hebben uitgevende instanties zicht op de documenten die ze in behandeling hebben en de plaats waar die documenten zich bevinden, zulks ter invulling van hun eigen verantwoordelijkheid ten aanzien van die documenten. Uitgevende instanties hebben die informatie waarmee zij in control zijn over het aanvraag- en uitgifteproces
Rationale	Uitgevende instanties zijn verantwoordelijk voor de afhandeling van een concrete aanvraag en het uit te geven document. Als zodanig dienen zij zicht te hebben op de status van concrete aanvragen en de status van documenten die nog niet aan de aanvrager zijn uitgegeven.
Implicaties	- Tussen organisaties en organisatiedelen in de keten vindt overdracht plaats, impliciet of expliciet, zodat het voor alle ketenpartners ondubbelzinnig vast staat wie de aanvraag of het document in behandeling heeft. - De uitgevende instantie kan eenvoudig vaststellen of er aanvragen of documenten ongewenst lang blijven 'hangen'. - Tevens hebben uitgevende instanties inzage in managementinformatie die ze voor hun doeleinden nodig hebben: realisatiecijfers, planning, kwaliteitsbewaking zijn dan relevante doeleinden.

B-AU-05	**Flexibele invulling frontoffice en backoffice voorbereid**
Statement	De processtappen van het aanvraag- en uitgifteproces zijn flexibel in te richten in de deelprocessen die de onderscheiden organisaties of organisatiedelen uitvoeren.
Rationale	Een specifieke vorm van flexibele inrichting van processen betreft het aanvraag- en uitgifteproces. Met name bestaat de wens om het aanvraag- en uitgifteproces flexibeler in te richten. Deels vanuit het feit dat we ook al een aantal varianten van dit proces kennen. Deels willen we mogelijkheden creëren zodat er in de toekomst ook nieuwe varianten mogelijk zijn. Denk concreet aan controles die, afhankelijk van de uitgevende instanties, op verschillende plaatsen kunnen voorkomen. Denk ook aan verschillende inrichtingen van frontoffice en backoffice taken (meer of juist minder kennisintensieve frontoffices) en mogelijke samenwerkingsverbanden in de backoffice.
Implicaties	• De *processtappen* in het aanvraag- en uitgifteproces zijn expliciet vastgesteld. Deze processtappen zijn voor alle uitgevende instanties gelijk, het zijn de bouwblokken waarmee het aanvraag- en uitgifteproces wordt opgebouwd. • Processtappen worden aaneengeregen tot het *deelproces*. Een deelproces wordt uitgevoerd door 1 organisatie of organisatiedeel. • Een kwaliteits- en controlestrategie is bepaald per uitgevende instantie om aanvragen van de vereiste kwaliteit op te leveren (de kwaliteit dient uniform te zijn over uitgevende instanties, het 'hoe' kan verschillen afhankelijk van uitgevende instanties en dit 'hoe' ligt vast in de kwaliteits- en controlestrategie). Deze kwaliteits- en controlestrategie is bepalend voor de vormgeving van de deelprocessen Aanvragen, Beoordelen en deels ook Uitgeven.

	• Op het moment dat een zaak van het type 'Aanvraag' wordt aangemaakt, wordt ook het proces bepaald voor het afhandelen van deze zaak. • Afhankelijk van de uitgevende instantie alsmede het type reisdocument is het overige proces te bepalen. Dan is duidelijk welke processtappen er in de verschillende deelprocessen worden uitgevoerd en welke deelprocessen door welke organisaties / organisatiedelen worden uitgevoerd. • Bovenstaande realiseren we door dit in de software configureerbaar te maken.

B-AU-06	**Vroegtijdig registreren aanvraag, detectie parallel lopende aanvragen, geen beoordelingen of controles buiten de aanvraag**
Statement	Binnen het deelproces Aanvragen wordt een aanvraag geregistreerd zodra bekend is: 1) de aannemelijke identiteit van de aanvrager en 2) het soort document dat aanvrager wenst aan te vragen en 3) bij welke uitgevende instantie de aanvrager dat doet. Alle beoordelingsactiviteiten (bijvoorbeeld op een RPS-signalering), zijn geregistreerde stappen als onderdeel van de aanvraag. Gegevens over parallel lopende of recente aanvragen en hun uitkomst zijn beschikbaar voor de actuele uitgevende instantie, zulks conform operationeel doel 2a. Deze worden gecontroleerd tijdens de deelprocessen aanvragen en uitgeven.
Rationale	Het is een programmadoel om het shopgedrag van burgers te voorkomen. Dit doel wordt reeds voor een deel bereikt door op lopende aanvragen alsmede recent afgewezen aanvragen te controleren gedurende het aanvraagproces. Dit komt overeen met operationeel doel 2a en 2b respectievelijk,
Implicaties	De werkwijze voor een aanvraag wordt werkelijk veranderd, door het vroegtijdig registreren van een aanvraag en doordat beoordelingsactiviteiten alleen binnen de context van een aanvraag moeten plaatsvinden. De meeste impact is te verwachten bij BZ, de Caribische landen en grensgemeenten.

B-AU-07	**Toekomstvaste en flexibele procesinrichting en techniek voor afname biometrie**
Statement	Biometrie-afname wordt flexibel vormgegeven. We constateren dat er veel beweging zit in de wijze waarop de afname van biometrische kenmerken in de toekomst mogelijk wordt vormgegeven. In VRS wordt hierop inspeelt door in de inrichting van processen en services rekening gehouden met beleidsontwikkelingen op de onderwerpen. Smaken die wellicht plaats zouden kunnen vinden, waar VRS rekening mee houdt: • Het starten van biometrieafname via een biometrisch randapparaat (kiosk, scanner etc.); • Het starten van biometrieafname op basis van een centraal geproduceerd signaal. • Gescheiden aanlevering van foto, handtekening en vingerafdrukken (nu reeds met de MVA aan de orde) op verschillende momenten in het proces;

	• Ontkoppelen van de biometrieafname van een actuele aanvraag; • Eventueel aanleveren van foto's via vertrouwde derde partijen • Live capture in verschillende varianten (in gemeentehuis, via vertrouwde derde);
Rationale	Op het gebied van biometrie zien we vele ontwikkelingen en behoeftes die zich ook doorontwikkelen. Het doel is om toekomstvast te zijn ook op dit gebied. Tegelijkertijd is het ook niet de bedoeling om alle smaken van biometrieafname binnen de scope van VRS ook uit te werken.
Implicaties	- De implicaties liggen primair in de procesinrichting en de vormgeving van business services binnen VRS. - Secondair kan het wenselijk zijn om het AS in de komende releases op de gerealiseerde services en processen aan te passen.

B-AU-08	**Biometrie-afname is in het proces gekoppeld aan identiteitsverificatie.**
Statement	Afname van biometrische kenmerken wordt in het proces steeds vergezeld van een identiteitsverificatie van de hoge betrouwbaarheid, waarbij van eventuele eerder vastgelegde biometrische kenmerken gebruik wordt gemaakt.
Rationale	Van biometrische kenmerken moet eenduidig zijn bij welke persoon deze horen. Daarom wordt er een steeds een koppeling met een goede identiteitsverificatie zodat het altijd mogelijk is eenduidig vast te stellen dat biometrische kenmerken behoren bij een bepaalde persoon.
Implicaties	De koppeling met de identiteit van de houder dient geen onderdeel te zijn van de opslag van de biometrische gegevens, zie B-AU-09.

B-AU-09	**Biometrische gegevens worden gepseudonimiseerd en technisch separaat opgeslagen**
Statement	Opslag van biometrische gegevens vindt plaats in een apart systeem, waarin de gegevens pseudoniem zijn opgeslagen. Het systeem wordt technisch zwaarder beveiligd.
Rationale	Van biometrische kenmerken moet eenduidig zijn bij welke persoon deze horen. Herleidbaarheid is derhalve noodzakelijk. Voorkomen dient echter te worden dat biometrische gegevens ook eenvoudig zijn te koppelen aan de persoon, buiten een context waarin er ook een legitiem doel voor is, vandaar een opname op pseudoniemen.
Implicaties	De implicaties zijn reeds gegeven in operationeel doel 24. Om de gegevens in dit onderdeel van de kernregistratie te beschermen tegen ongeoorloofde toegang en datalekken is een aantal concrete maatregelen genomen: - In dit onderdeel zelf zijn de gegevens opgenomen aan de hand van een pseudoniem. Er wordt geen direct of indirect identificerend nummer zoals een BSN, houdernummer, documentnummer of aanvraagnummer gehanteerd. Bij onverhoopt verlies van of ongeautoriseerde toegang tot de database heeft men alleen de beschikking over een groot aantal niet te relateren foto's en handtekeningen. - Het relateren van een aanvraagnummer (en daarmee indirect een houder) aan de biometrische gegevens is weliswaar mogelijk, maar is slechts mogelijk vanuit de context van een aanvraag dan

	wel een informatieverzoek dat door de uitgevende instantie, in overeenstemming met de regelgeving, is goedgekeurd. - Het omzetten van een aanvraagnummer naar de pseudoniemen in dit onderdeel is een extra beveiligde functie die met een hardware security module of iets vergelijkbaars wordt ondersteund. - Dit onderdeel zelf is uitgevoerd op een 'gehard' systeem, dat een minimaal 'aanvalsoppervlak' biedt. Bovenstaande kan gevolgen hebben voor de mate waarin gebruik gemaakt kan worden van IaaS / PaaS faciliteiten. Mogelijk moeten voor adequate scheiding aanvullende maatregelen worden genomen zoals het gebruik van fysieke gescheiden en niet gevirtualiseerde machines. Gebruik van pseudonimiseren levert overigens wel het probleem op dat het de-pseudonimiseren een 'afgeschermde functie' dient te zijn, die alleen onder bepaalde omstandigheden toegankelijk is. Met name wordt hiervan gebruik gemaakt bij het opvragen van gezichtsopnames ten behoeve van de uitgevende instanties in het aanvraag- en uitgifteproces.

B-AU-10	**In de aanvraag wordt altijd vergeleken met de foto's van eerdere aanvragen**
Statement	Bij wijze van extra controle wordt in de uitgifte (indien aanwezig) gecontroleerd tegen de foto's uit eerdere aanvragen. Vooralsnog wordt hiervoor een geautomatiseerde vergelijking uitgevoerd, waarvan de resultaten ter beschikking worden gesteld van de uitgevende instanties. De uitgevende instanties voeren zelf de vergelijking uit, ondersteund door deze geautomatiseerde vergelijking. Uitgevende instanties ontvangen hiervoor zelf ook de foto's.
Rationale	Om de integriteit van het aanvraagproces te versterken, wordt als onderdeel van het aanvraagproces deze controle opgenomen.
Implicaties	De werkwijze van uitgevende instanties komt te veranderen.

B-AU-11	**Volwaardige ondersteuning en registratie nooddocumenten**
Statement	Aanvraag- en uitgifte van nooddocumenten, evenals (status)registratie, geschiedt op gelijkwaardige wijze aan andere reisdocumenten.
Rationale	In lijn met de gestelde doelstellingen wordt voor de uitgifte van nooddocumenten eenzelfde registratie- en kwaliteiten gesteld om misbruik en onterechte uitgifte te voorkomen.
Implicaties	▪ Decentrale personalisatie wordt ondersteund. ▪ T.a.v. noodprocedures en continuïteit is het ook mogelijk om zonder gebruikmaking van centrale applicaties nooddocumenten te personaliseren, waarbij wél wordt afgedwongen dat deze met terugwerkende kracht worden geregistreerd. ▪ De informatievoorziening en kwaliteitseisen t.a.v. voorraadbeheer wordt verbeterd. ▪ Informatie m.b.t. nooddocumenten worden net als andere documenten geregistreerd in de kernregistratie en via services waar nodig beschikbaar gesteld.

3.5 Statusbeheer

3.5.1 Richtinggevende uitspraken

B-STATBEH-01	Statussen van documenten worden bijgehouden in de kernregistratie (onderdeel Basisregister) onder de verantwoordelijkheid van de minister van BZK, i.c. RvIG
Statement	Een brede groep autoriteiten kan de statussen van reisdocumenten wijzigen na het moment van uitreiking. De minister van BZK, i.c. RvIG, is verantwoordelijk voor het voeren van een betrouwbare administratie van deze statussen, als onderdeel van de verantwoordelijkheid voor het Basisregister, zoals beschreven in de Paspoortwet. In dat verband schrijft de minister de werkwijze voor, voor het ordentelijk administreren van statuswijzigingen en de 'events' die daaraan ten grondslag liggen.
Rationale	Door één authentieke bron te hanteren voor reisdocumenten kunnen statuswijzigingen ook eenvoudig door andere autoriteiten worden doorgevoerd. Een autoriteit die feitelijk kennis verkrijgt over een relevante gebeurtenis met een reisdocument kan deze dus direct administreren. Om onnodig handelen en onnodig verkeer tussen uitgevende instanties onderling uit te bannen, is deze verandering doorgevoerd. Denk bij het bovenstaande bijvoorbeeld aan het melden van een diefstal of vermissing en de daarmee samenhangende statuswijziging.
Implicaties	- In de regelgeving zijn de verantwoordelijkheden vast te leggen rondom het registreren van events en het aan de hand daarvan wijzigen van statussen. Mogelijk worden hierbij de principes van zaakgericht werken gehanteerd. - De processen rondom de statuswijzigingen worden (opnieuw) ontworpen, opdat de kwaliteit afdoende geborgd is. - Zowel de gebeurtenissen die leiden tot statuswijzigingen en de statuswijzigingen zelf worden vastgelegd. - Mogelijk voert RvIG een toets uit op ingevoerde events en doorgevoerde statuswijzigingen. - De formulierenstroom in verband met statuswijzigingen komt te vervallen voor de reguliere gevallen. De overige formulierenstroom wordt door een digitale tegenhanger vervangen.

B-STATBEH-02	De status van sommige reisdocumenten wordt niet beheerd door een brede groep autoriteiten, maar een specifieke autoriteit.
Statement	In B-STATBEH-01 wordt een brede autorisatie beschreven voor het administreren van events en het doorvoeren van statuswijzigingen. Op deze brede autorisatie is een aantal uitzonderingen: diplomatieke paspoorten, dienstpaspoorten, paspoorten van leden van het Koninklijk Huis.

Rationale	Het bestaan van bepaalde reisdocumenten dan wel de gegevens van die reisdocumenten is gevoelige informatie. Daarom dient informatie omtrent die documenten slechts in beperkte kring toegankelijk te zijn. Zo dient ook de administratie van events en het doorvoeren van statuswijzigingen voorbehouden te zijn voor een select aantal autoriteiten en medewerkers van die autoriteiten.
Implicaties	- Zoals aangegeven zijn er uitzonderingen op de brede autorisatie. In dergelijke gevallen is de oorspronkelijke uitgevende instantie naast RvIG als enige geautoriseerd om de status te wijzigen. - Het feit dat sommige documenten een uitzonderingsstatus hebben, betekent niet dat ze in een aparte registratie zijn opgenomen. De afscheiding is uitsluitend logisch binnen de kernregistratie.

B-STATBEH-03	**Alle documenthouders kunnen online een vermissing melden van zijn/haar document.**
Statement	De burger meldt een vermissing bij voorkeur online, via het Internet (Stop-ID). Opgave van vermissing en de bijbehorende statuswijziging kan tevens via uitgevende instanties plaatsvinden. Melding van vermissing kan eveneens nog steeds bij de balie plaatsvinden.
Rationale	Het is van belang dat vermissing tijdig wordt gemeld. Dat geldt voor de houder, maar het is ook een algemeen belang. De online werkwijze maakt dit mogelijk. Deze online werkwijze zullen we in de toekomst vaker gaan zien bij de gemeente die het document heeft uitgegeven (autonome ontwikkeling, los van VRS). Door tevens in sommige gevallen de vermissing via andere uitgevende instanties af te kunnen handelen zijn de voorwaarde voor tijdige melding ingevuld.
Implicaties	- Voldoende niveau van authenticatie van de burger (DigiD Substantieel, op korte termijn DigiD Midden) om denial-of-service aanvallen tegen te gaan en de burger dus ook te beschermen. - Documenthouders vullen on-line ook direct een verklaring over de vermissing (huidige C2-formulier). De mogelijkheid om relevante bijlages (scan aangifte politie e.d.) te uploaden op dat moment of later, wordt tevens geboden. - Het C2 formulier blijft bestaan voor de balie-situaties. - De on-line mogelijkheid om een vermissing te melden staat open voor de houder zelf. In specifieke machtigingen wordt niet voorzien, hiervoor zal het invullen van een C2 te prefereren zijn. - Gemeentes bieden nu ook al in toenemende mate ook een on-line mogelijkheid om een vermissing te melden. RvIG neemt de coördinatie op zich om deze oplossing af te stemmen op de oplossing die in VRS geboden zal gaan worden.

B-STATBEH-04	**De status van afgeleide digitale documenten volgen het (analoge) 'parent' reisdocument.**
Statement	We onderkennen reisdocumenten en afgeleide digitale 'reisdocumenten' of identiteitsdocumenten. De status van een afgeleid document wordt aangepast bij een statuswijziging van het 'parent' reisdocument. Met name geldt dat als een 'parent' document komt te vervallen of wordt ingetrokken, dat dan ook geldt voor de afgeleide digitale documenten.

	Omgekeerd geldt niet dat de intrekking van een afgeleid digitaal document leidt tot een statuswijziging van het 'parent document.
Rationale	Er wordt geëxperimenteerd met nieuwe vormen van digitale identiteiten zoals vID en SSI. Ook vindt er voor virtuele ID's standaardisatie plaats in ICAO-context. Daarin is voorzien dat er een notie van 'afgeleide' virtuele identiteit is.
Implicaties	- In het gegevensmodel is de notie van 'afgeleid document' op te voeren. Ook dient het systeem te zijn voorbereid om dergelijke afleidingsrelaties te leggen. - Statuswijzigingen van een 'parent' document dienen een trigger te vormen om de status van een afgeleid document te wijzigen. - Ook al zijn vID, SSI en KTDI projecten die niet onder de vlag van VRS worden uitgevoerd, maakt het hier beschreven principe het wel mogelijk om de status van deze virtuele identiteiten op een efficiente manier te beheren, waarmee VRS ook al op de toekomst is voorbereid.

3.5.2 Statusmodel reisdocument

Hieronder wordt een concept statusmodel gepresenteerd voor reisdocumenten. Dit is het resultaat van een analyse van bestaande statussen, een analyse van de huidige juridische situatie. Daarbij is er naar gestreefd om een eenvoudig inzichtelijk model te creëren, dat echter recht doet aan de verschillende soorten gebeurtenissen, de zogenaamde events. De gehanteerde terminologie voor statussen is nog een eerste voorstel.

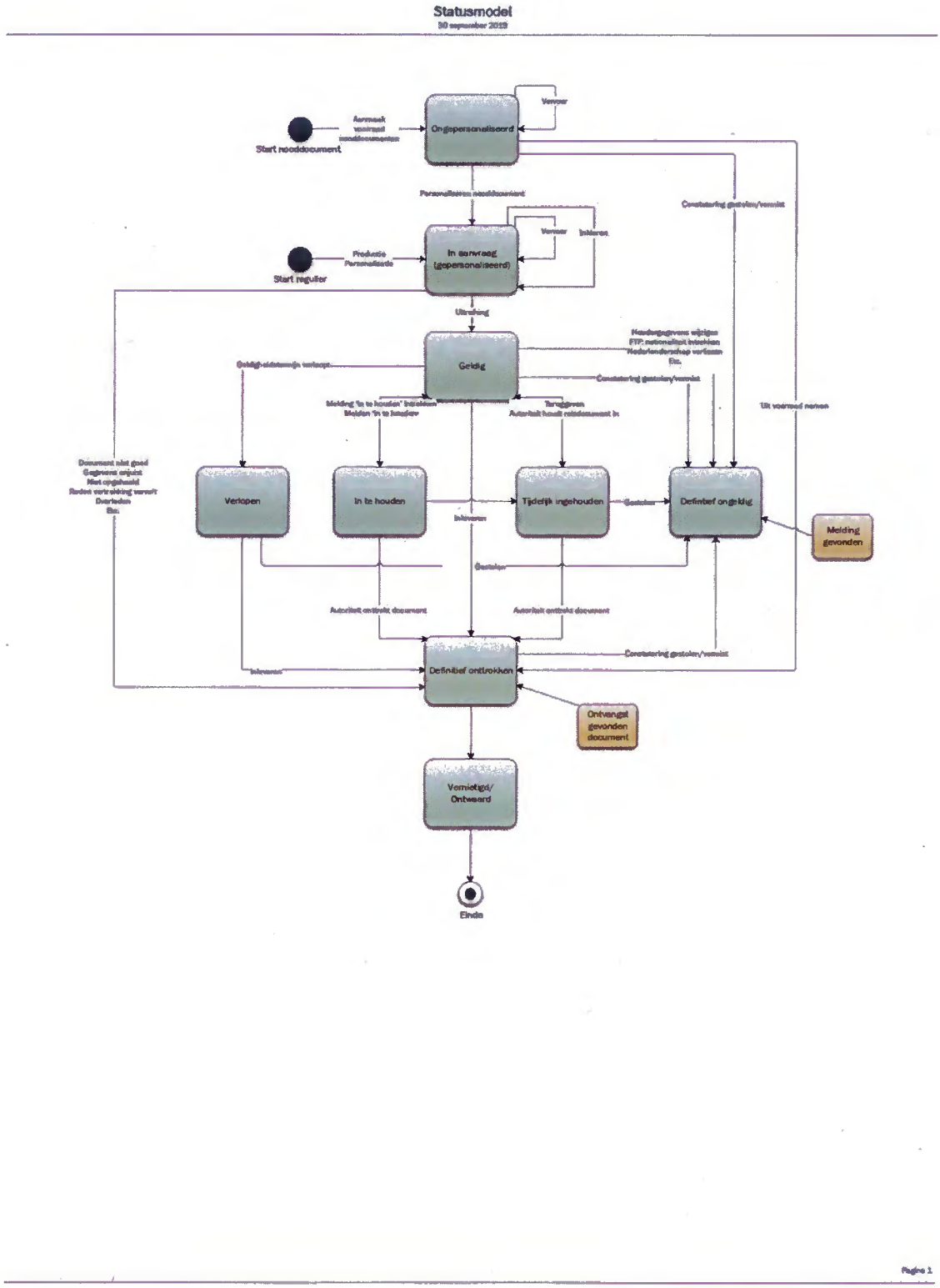
Uitgangspunten voor het statusmodel zijn:

1. Met een status bedoelen we een relevante toestand, die het handelen van een autoriteit mede bepaalt, of het handelen van een organisatie die vertrouwt op de identificerende functie van het reisdocument.
2. De precieze gebeurtenis, aanleiding of reden is geen status, maar leggen we wel vast als 'event'. Een event is bijvoorbeeld 'houder overleden' of 'houdergegevens gewijzigd'.
3. Events registreren we ook in de historie van een document, zodat details beschikbaar zijn wanneer dat nodig is. Bijvoorbeeld bij doorlevering aan de politie speelt dat niet alleen de status relevant is, maar ook de in de events vastgelegde details.
4. Een event zal zijn eigen proceslogica hebben, deze is geen onderdeel van dit model.
5. De status zal (naar we nu verwachten) wel voldoende informatie bieden voor documentverificatie zoals we die nu kennen.
6. Het model onderscheidt nooddocumenten waarbij er ongepersonaliseerde voorraad is en reguliere documenten die in een klap geproduceerd en gepersonaliseerd worden.
7. Het model onderkent het reguliere verlopen van een document (geldigheidsdatum is overschreden) en eventueel de speciale behandeling die daaraan wordt gegeven. Een verlopen document kan na einde geldigheid ook nog verloren of gestolen raken. In dat geval gaat het document naar 'definitief ongeldig'.
8. Het model maakt geen onderscheid meer tussen 'nette redenen waarom het document van rechtswege vervalt' en gevallen dat het document gestolen / vermist is. Daarmee komen ook de 'nette gevallen' in de documentverificatie op 'rood licht'. Dit is ook wat we

willen; we willen immers ook niet dat er gebruik wordt gemaakt van die documenten in die omstandigheid.

9. Wel kan er eventueel voor gekozen worden om niet alle gevallen ook op lijsten van derden (internationale signaleringslijsten bv) op te nemen.
10. Het model onderkent de mogelijkheid dat een autoriteit het voornemen heeft om te gaan inhouden, maar dat om redenen van rechtszekerheid van de burger nog niet doet. Dit is een in beginsel herstelbare status. Een autoriteit kan op basis hiervan besluiten om in te houden en met de autoriteit die het voornemen heeft geregistreerd in overleg te treden. Het kan tot een al dan niet tijdelijke inhouding leiden.
11. Aan het einde van de levenscyclus kan een document definitief worden onttrokken door een autoriteit. Hierna kan nog slechts vernietiging of ontwaarding volgen, of het document moet onverhoopt gestolen worden bij die partij of gedurende een transport naar een vernietigingsfaciliteit. Vanwege de laatste mogelijkheid is er daar sprake van aparte statussen.
12. Het vinden van een document door een organisatie is nu gesplitst in 2 events: de melding van een (enigermate betrouwbare) partij en de daadwerkelijke ontvangst van een reisdocument door een autoriteit. Idee is ook dat de melding van enigermate betrouwbare partijen reeds tot het definitief ongeldig maken kan leiden.
13. Inhouding is als term voorbehouden aan het fysiek onttrekken aan de circulatie van een document. Het document is dan dus niet ter beschikking van de houder.
14. Documenten kunnen lange tijd blijven 'hangen' in een bepaalde status. Er is geen termijn voor het afvoeren bedacht, de wettelijke bewaartermijn voor de registratie van het document wordt gehanteerd.
15. Aanname is dat eventuele gebruiksbeperkingen van een reisdocument apart geregistreerd, beheerd en gecommuniceerd gaan worden.
16. Documentverificatie zou 'groen licht' kunnen geven voor 'geldig'. Over 'in te houden' en 'verlopen' (de laatste wellicht met een tijdsbeperking) is inbreng van inzichten welkom.

Het statusmodel is weergegeven in de onderstaande figuur.



Figuur 2 Statusmodel

3.6 Signaleringenbeheer

B-SIGBEH-01	RPS-signaleringen maken deel uit van de kernregistratie reisdocumenten.
Statement	Het Register paspoortsignalering is onderdeel van de kernregistratie reisdocumenten. De juridische verantwoordelijkheden van de Minister van BZK alsmede de Gouverneurs zijn hierin vormgegeven.
Rationale	We willen toe naar de notie van een kernregistratie. Logischerwijs hoort het Register paspoortsignaleringen daar ook bij.
Implicaties	- RPS-signaleringen worden slechts gedaan op personen die bekend zijn in persoonsregistraties danwel die bekend zijn als houder van een reisdocument. - Indien een signaleringsverzoek wordt gedaan op personen buiten bovengenoemde doelgroep, dan dient de signalerende instantie het recht op een Nederlands reisdocument van die persoon aan te tonen. - Personen kunnen in afwijking van bovenstaande dus ook uitsluitend worden geregistreerd in verband met een signalering. Als ze bij beeindiging van de signalering nog steeds niet anderszins geregistreerd zijn, dan wordt hun registratie op dat moment ook terstond beëindigd. - Omwille van de versterking van de informationele samenhang van de kernregistratie worden gedurende VRS stappen gezet tot nadere integratie. Allereerst op de registratie van personen ten behoeve van het reisdocumentenstelsel, wat virtueel één registratie van personen wordt. - De signalering van documenten wordt op termijn onderdeel van het statusbeheer van reisdocumenten. Hiervoor is de status 'in te houden' toegevoegd.

B-SIGBEH-02	De verantwoordelijkheden voor RPS-signaleringen blijven ongewijzigd
Statement	RvIG blijft verantwoordelijk voor het beheer van RPS en de daarin geadministreerde signaleringen. Hoewel in SIGBEH-03 is aangegeven dat signalerende instanties hierin een actievere rol krijgen, blijven de verantwoordelijkheden ongewijzigd. Daar hoort bij dat er een marginale toets wordt uitgevoerd op de signaleringsverzoeken. Daar hoort ook bij dat RvIG de kwaliteit (inclusief actualiteit) van de signaleringen actief bewaakt. RvIG gaat dit doen middels een kwaliteitssysteem.
Rationale	Er zijn redenen om het systeem van RPS-signaleringen aan te passen aangezien het proces inefficiënt is met veel papierwerk. Belangrijke verbeteringen zijn echter al te realiseren binnen het kader van de huidige verantwoordelijkheden, dus dit is een passende stap voor VRS.
Implicaties	Invoeren van een kwaliteitssysteem.

B-SIGBEH-03	Signalerende instanties voeren het beheer over 'hun' signaleringen in de kernregistratie reisdocumenten via self-service.
Statement	Signalerende instanties kunnen hun signaleringsverzoeken in een self-service portaal invoeren. Hierin wordt dit als zaak afgehandeld. De volgende processtap is de marginale toets.

	Op 'hun' bestaande signaleringen dient de signalerende instantie beheer te voeren, om zeker te stellen dat de signalering in stand blijft voor de juiste periode. In het self-service portaal wordt 3 maanden voor het verloop van de 2-jaars termijn een zaak aangemaakt voor de signalerende instantie om te bepalen of de signalering nog in stand moet blijven. Signalerende instanties krijgen tevens middelen om rapportages te genereren.
Rationale	Het huidige signaleringenbeheer is arbeidsintensief, tijdrovend en foutgevoelig. Dat wordt hiermee ondervangen.
Implicaties	- Gegeven het grote aantal signalerende instanties is goede authenticatie en autorisatie van medewerkers van signalerende instanties een aandachtspunt. Vanuit die optiek wordt voorgesorteerd om dit via eHerkenning te doen, zodat signalerende instanties zelf het beheer over de authenticatie en autorisatie van medewerkers kunnen voeren. - Het betrouwbaarheidsniveau voor de authenticatie dient nog nader te worden bepaald, vooralsnog wordt gedacht aan EH3. - Met de keuze voor eHerkenning ligt het voor hand om het self-service portaal via Internet ter beschikking te stellen.

B-SIGBEH-04	**Brieven en formulieren omtrent signaleringen komen te vervallen.**
Statement	Brieven en formulieren omtrent signaleringen komen te vervallen. De uitzondering hierop vormen de brieven richting de burger over het feit dat deze gesignaleerd staat.
Rationale	Bij het digitaliseren kunnen brieven en formulieren eenvoudig door self-service handelingen worden vervangen. Voor de communicatie aan deze doelgroep is dat echter niet het geval, zodat de kennisgevingen per brief nog zullen blijven bestaan. Voor communicatie met de burger is echter een meer proactieve vorm gewenst om de signalering onder zijn aandacht te brengen.
Implicaties	- Het ondertekeningsvereiste van de brief aan de burger wordt omgezet naar de digitale situatie op een nog nader af te stemmen wijze. - Alternatieve vormen van informatieverstrekking naar de burger over diens signalering zijn nog onderwerp van onderzoek

B-SIGBEH-05	**Het behandelproces voor 24b signalering wordt gedigitaliseerd. Zaakgericht werken is van toepassing.**
Statement	Het behandelproces voor 24b signaleringen (meervoudige vermissingen, oneigenlijk gebruik) wordt gedigitaliseerd.
Rationale	Het proces rondom meervoudige vermissingen24b signaleringen is arbeidsintensief en bevat in de huidige vorm veel stappen met weinig of geen toegevoegde waarde (digitaal naar papier naar digitaal conversies bijvoorbeeld). Eenduidige besluitvorming over uitgevende instanties heen is bovendien gewenst, zodat een volledige vastlegging van de situatie, het advies en het uiteindelijk besluit gewenst is.

	Bovengenoemde kenmerken zijn typisch voor een situatie dat zaakgericht werken nuttig en nodig is. Dit wordt hier dan ook toegepast.
Implicaties	- Bij een aanvraag of anderszins wordt (geautomatiseerd) geconstateerd dat er sprake is van een dusdanig aantal vermissingen of in het ongerede geraakt zijn van een reisdocument in de afgelopen jaren, dat een paspoort wellicht te weigeren zou zijn. - Op dit moment wordt er een zaak aangemaakt om te beoordelen of er sprake is van verwijtbaarheid bij een of meer van deze vermissingen. De zaakmanager is dus ook altijd de signalerende instantie. - Aan deze zaak automatisch de documentatie omtrent eerdere vermissingen wordt toegevoegd (denk aan kopie-aangiftes van diefstal, verklaringen v.d. houder) - De burger waar nodig wordt uitgenodigd langs digitale weg het dossier aan te vullen - De zaakmanager van deze zaak is: o Indien er sprake is van een aanvraag waarbinnen de vermissing wordt geconstateerd: de actuele uitgevende instantie. o Indien er geen sprake is van een aanvraag: de actuele autoriteit van inschrijving. o Indien er geen autoriteit van inschrijving is: RvIG - De zaak kan door de zaakmanager overgedragen worden aan RvIG (huidige praktijk vanuit een aantal gemeenten). - De zaakmanager kan ook advies vragen aan RvIG - De uiteindelijke beslissing van de zaakmanager / signalerende instantie wordt vastgelegd, waarbij tevens wordt vastgelegd wat de onderbouwing van de beslissing is.

B-SIGBEH-06	**Signaleringen uit de kernregistratie worden doorgeleverd aan OPS**
Statement	Ten behoeve van bij wet aangewezen opsporingsinstanties kunnen signaleringen uit het register paspoortsignaleringen worden doorgeleverd aan OPS. Buiten de digitalisering van het aanleveringsproces richting deze opsporingsinstanties, worden geen wezenlijke veranderingen in deze aanleveringen voorzien.
Rationale	Er is geen aanleiding om de huidige werkwijze wezenlijk te veranderen. On-line raadpleging is bovendien geen optie, omdat OPS als bestand wordt gedistribueerd.
Implicaties	Nader te bepalen implicaties van gestructureerde digitale aanlevering. Zie ook B-INFO-03.

3.7 Informatieverstrekking

B-INFO-01	Directe bevraging kernregistratie 'op maat'
Statement	Bestaande informatieproducten en -verstrekkingen worden waar mogelijk vervangen door directe online bevraging van de kernregistratie reisdocumenten.
Rationale	Directe bevraging heeft een hogere actualiteit. Bovendien worden niet meer gegevens verstrekt dan strikt noodzakelijk.
Implicaties	- Preciezer dan nu moeten de use cases van de bevragende organisaties in kaart worden gebracht - Omdat het gaat om online bevraging, dienen de authenticatie en autorisatie van het bevragende systeem en de bevragende medewerker sluitend te worden geregeld. - De bevragende organisatie is verantwoordelijk voor het intern autoriseren van haar medewerkers voor de verschillende soorten bevragingen.

B-INFO-02	Privacy-by-design
Statement	Informatieverstrekkingen uit de kernregistratie worden (op basis van de Paspoortwet) ontworpen op basis van de principes van privacy-by-design
Rationale	De principes van privacy-by-design zijn verplicht vanuit de Algemene Verordening Gegevensbescherming. Ook de informatieverstrekkingen in en vanuit het reisdocumentenstelsel zijn hieraan gehouden, aangezien de AVG algemeen geldend is.
Implicaties	- De rechtsgrond voor informatieverstrekkingen (vanuit de Paspoortwet) zal per casus beoordeeld moeten worden - Idem voor het doel voor de informatieverstrekking - De proportionaliteit is van geval tot geval nieuw te beoordelen, mede op basis van het gegeven van een direct bevraagbare kernregistratie reisdocumenten - In het ontwerp dienen eisen omtrent dataminimalisatie alsmede mogelijkheden voor privacybeschermende maatregelen als pseudonimisatie te worden meegenomen

B-INFO-03	Weerkerende informatieverstrekkingen vinden geautomatiseerd en zonder menselijke tussenkomst plaats
Statement	Weerkerende informatieverstrekkingen aan derde partijen (zoals het opsporingsregister van politie) worden geautomatiseerd en de verstrekkingen vinden langs digitale weg plaats. In die gevallen stappen we af van informatiestromen o.b.v. documenten/formulieren en menselijk contact.
Rationale	Vanuit efficiencyoverwegingen zijn geautomatiseerde koppelingen te prefereren. Bovendien vermijdt dit menselijke fouten.
Implicaties	- Specificatie en bouw van een koppeling is noodzakelijk. - Weerkerende informatieverstrekkingen zijn op voorwaarde van een positieve autorisatiebeslissing - Ad hoc vragen zijn niet te voorzien als geautomatiseerde koppeling. Dit blijft mensenwerk.

B-INFO-04	Identiteitsverificatie wordt als on-line service ingericht. Vooralsnog betreft het uitsluitend identiteitsverificatie aan de hand van een reisdocument.
Statement	Door niet het document centraal te stellen, maar identiteitsverificatie als dienst, wordt een maatschappelijke meerwaarde geleverd. Bepaald wordt bij welke vormen van dienstverlening een identiteitsverificatie aan de hand van een reisdocument dient plaats te vinden.
Rationale	Identiteitsverificatie is een belangrijk maatschappelijk product / dienst. RvIG onderneemt nu in pilots stappen om dit terrein te betreden met initiatieven als SSI en (in mindere mate) vID. VRS onderneemt daarom stappen om beter te begrijpen wat het betekent om diensten op het gebied van identiteitsverificatie te leveren en wat het betekent om zich hierop voor te bereiden. Binnen het VRS programma wordt identiteitsverificatie aan de hand van een reisdocument uitgewerkt als opvolger van (de bevraging van) het VR. Zie operationeel doel 10.
Implicaties	- Deze vormen van identiteitsverificatie zijn thans niet zo benoemd in de wet- of regelgeving. - De behoefte zal derhalve dienen te worden geïnventariseerd en beleidsvorming hierop moet plaatsvinden - Bovendien is aanpassing van het Paspoortbesluit te verwachten voor sommige van bovengenoemde use cases

B-INFO-05	Aanvragen door en verstrekken foto's aan opsporingsinstanties loopt via een centraal koppelpunt
Statement	Aanvragen en verstrekken van fotomateriaal aan opsporingsinstanties wordt technisch gecentraliseerd, maar blijft onder de verantwoordelijkheid van de uitgevende instantie.
Rationale	Foto's worden in het huidige proces verzameld als onderdeel van het aanvraagproces. Uitgevende instanties blijven echter verantwoordelijk en beheerder van deze gegevens. Uitgevende instanties blijven dan ook verantwoordelijk voor de verstrekking van foto's aan opsporingsinstanties. Het huidige proces voor het aanvragen en leveren van die foto's is echter matig geregeld (met uitdraaien uit RAAS en versturen).
Implicaties	- Het aanvragen en leveren van foto's verloopt elektronisch via een centraal koppelpunt (API Gateway); - Aanvragen en verstrekken gebeurt via beveiligde verbindingen, waarbij de authenticatie van de aanvrager technisch geregeld is; - Een aanvraag komt als verzoek bij de backoffice van de uitgevende instantie, alwaar het verzoek wordt beoordeeld en afgehandeld.

3.8 Gebruik

B-GEBR-01	RvIG heeft zicht op het (gepseudonimiseerd) gebruik van reisdocumenten
Statement	RvIG verkrijgt gegevens waar een reisdocument daadwerkelijk wordt gebruikt voor identiteitsverificatie. Dit beperkt zich vooralsnog tot het vastleggen van gegevens over de situatie dat er identiteitsverificatie aan de hand van een reisdocument plaatsvindt

	Doel van deze verkrijging is om a) ná het programma VRS de burger te kunnen informeren omtrent identiteitsverificatie aan de hand van diens reisdocument waarmee de burger 'in regie' komt en b) het detecteren van 'verdachte' gebruikspatronen.
Rationale	Momenteel autoriseert RvIG afnemers van het verificatieregister. Er is echter geen sprake van operationeel zicht op het gebruik. Om beter toe te kunnen zien dat verificatieverzoeken uitsluitend bekende partijen en geautoriseerde doelen betreft, worden deze gegevens meegegeven bij een bevraging. Op termijn kunnen (afhankelijk van toekomstige vastlegging) gegevens worden gebruikt om pseudoniem onderzoek te doen naar 'verdachte' gebruikspatronen. Zulks analoog aan de werking van het misbruikregister zoals dat door Logius wordt ontwikkeld voor eID.
Implicaties	- De meest voor de hand liggende uitwerking is dat gebruikers van het verificatieregister worden gemigreerd naar een specifieke service vanuit de kernregistratie reisdocumenten. - Aparte organisaties die gebruik maken van deze service worden apart geautoriseerd en zijn geauthenticeerd, tot op het niveau van de organisatie of gedetailleerder. - Het proces dat deze service gebruikt wordt bij aanroep van de service geïdentificeerd. - Om te vermijden dat er een 'privacy hotspot' ontstaat, waarmee RvIG zicht zou krijgen op de alle identiteitsverificaties die Nederlanders doen aan de hand van hun reisdocument, vindt de duurzame opslag van deze gegevens uitsluitend gepseudonimiseerd plaats. Terugvertaling naar een 'real world' identiteit is vooralsnog niet mogelijk en op termijn uitsluitend als er vermoedens van misbruik zijn. Een en ander afhankelijk van toekomstige beleidsontwikkeling.

4 Informatie Architectuur

In dit hoofdstuk wordt op hoofdlijnen vastgelegd wat de informatiearchitectuur is van het programma VRS binnen het reisdocumentenstelsel. Het betreft de relatie van de processen tot de in die processen impliciete gegevensverwerkingen, alsmede de gegevens, de applicaties en services waarmee die gegevensverwerkingen worden ondersteund. Daarmee betreft het zowel de geautomatiseerde als de niet geautomatiseerde gegevensverwerking.

In meer detail worden gegevens, applicaties en services in beeld gebracht. Ook de berichten die zorgen voor informatie uitwisseling, zijn onderdeel van de informatiearchitectuur.

Op conceptueel niveau kan de opzet van de informatiearchitectuur worden beschreven als een servicegerichte (of ook wel service georiënteerde) architectuur waarbij zoveel mogelijk informatie via generieke (micro)services worden aangeboden aan primaire processen, door integratie in applicatie(componenten).

Een business principe is dat er recht dient te worden gedaan aan de diversiteit van verschillende ketenpartners en hun huidige (en toekomstige) systemen. Met andere woorden: we erkennen een variëteit aan verschillende verschijningsvormen van processen bij ketenpartners (zoals verschillen in uitvoering met betrekking tot aanvraag en uitgifte van reisdocumenten).

Die variëteit kan ondersteund worden door (functionaliteit in) eigen applicaties (zoals bijvoorbeeld de reisdocumentenmodules bij gemeenten of domein specifieke applicaties bij Identiteit verifiërende instanties) ofwel (toekomstige) applicaties die gefaciliteerd zullen worden door RvIG (zoals een Reisdocumenten Aanvraag Portaal of een Portaal Signaleringenbeheer).

Al deze applicaties (zowel de 'eigen' applicaties van de ketenpartners, als de applicaties die RvIG beschikbaar stelt) doen via functionaliteiten c.q. gebruikerinteracties (beschreven in verschillende 'use cases') een beroep op door RvIG en middels een serviceplatform beschikbaar gestelde business- en informatieservices.

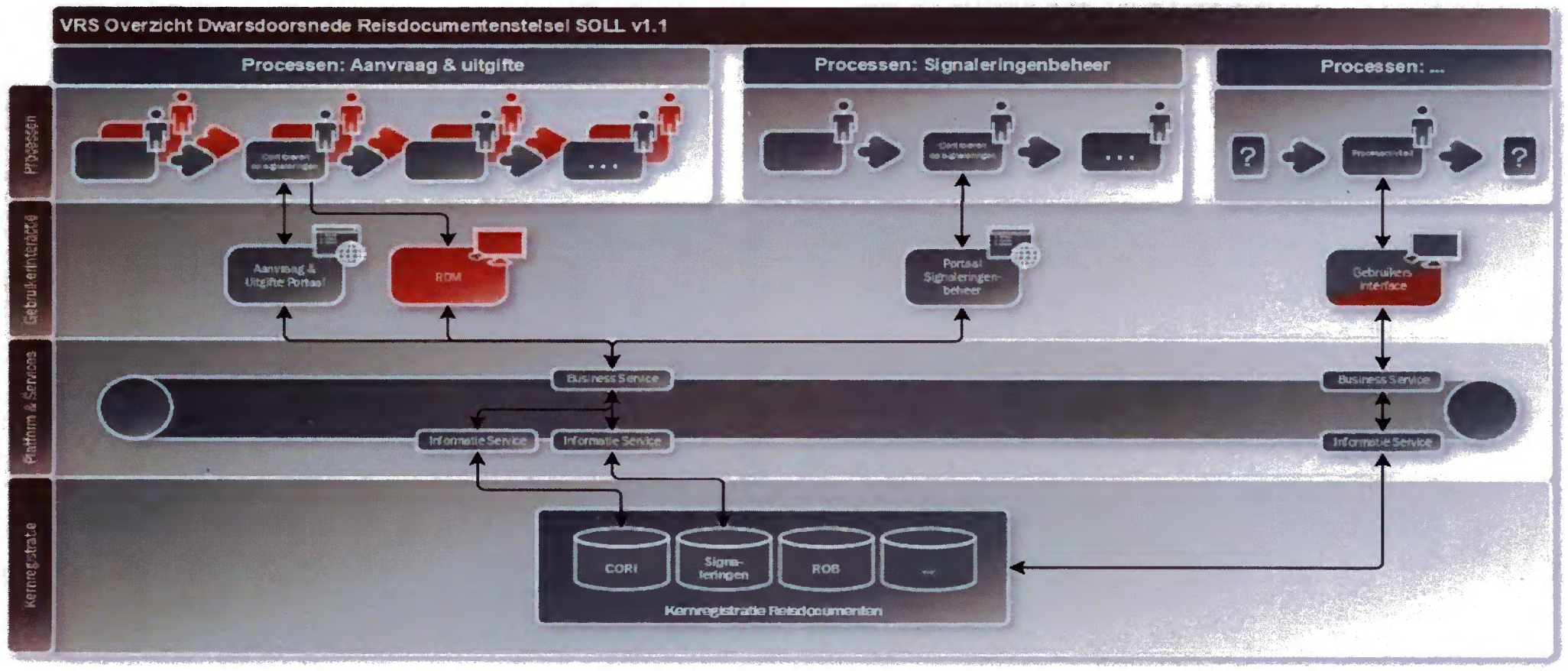
Het serviceplatform verwerkt de verzoeken via verschillende informatieservices richting de kernregistratie reisdocumenten en andere authentieke bronnen (zoals de basisregistratie personen), om vervolgens een antwoord terug te leveren aan de applicatie die van de betreffende services gebruik maakt.
Waar processen van ketenpartners en RvIG verschillen en ondersteund worden door middel van verschillende applicaties, zien we dat de benodigde onderliggende services en gegevens tamelijk uniform van aard zijn.

Door het stelsel servicegericht op te zetten komen we tegemoet aan de doelstellingen om informatie specifieker, vraaggerichter, flexibeler en privacy vriendelijker beschikbaar te stellen. Bovendien wordt het mogelijk om de informatievoorziening aan verschillende ketenpartners te uniformeren en standaardiseren, waarbij verschillende verschijningsvormen van informatiestromen en leveringen (zoals nu vaak het geval is) komen te vervallen.

Bovenstaande is uiteraard alleen mogelijk omdat de hoofdprocessen zoals aangeduid in hoofdstuk 3 op hoofdlijnen NIET afhankelijk zijn van de identiteit en inrichtingskeuzen van de organisatie in kwestie. De verantwoordelijkheden en wettelijke kaders zijn immers voor alle organisaties van een bepaald type (uitgevende instanties, signalerende instanties, ..) gelijk. Ook de processen staan op hoofdlijnen vast.

De procesvrijheid van de organisaties is er derhalve een binnen kaders. Wel zijn er bijvoorbeeld in het aanvraag- en uitgifteproces enige variaties mogelijk, zoals bepaalde verschuivingen in de volgorde van controles. Door een uitgekiende ontleding in services kan er aan die variatiemogelijkheden ondersteuning worden geboden.

We geven hieronder een voorbeeld:



Figuur 3: Visualisatie dwarsdoorsnede

Een van de activiteitein in het aanvraag- en uitgifteproces betreft de activiteit 'controleren op RPS signaleringen' (e.g. het toetsen of een persoon/aanvrager op dit moment een paspoortsignalering heeft) bekijken. Sommige uitgevende instanties willen deze controle uitvoeren door middel van een eigen applicatie (RDM). Andere uitgevende instanties zijn hierin afhankelijk van een portal van RvIG waarin deze dienst wordt geboden. Het ligt dus voor de hand om de activiteit 'controle op RPS signaleringen' te ondersteunen met een of meer informatieservices.

Naast de toepassing in het aanvraag- en uitgifte proces is dergelijke functionaliteit ook nodig in processen omtrent signaleringenbeheer. Het ligt voor de hand dat ook daar van diezelfde informatieservices gebruik wordt gemaakt. We merken op dat dit echter een ander doel betreft en ook andere ketenpartners die hiervan gebruik maken. Ook zullen de applicaties die signaleringbeheer ondersteunen wezenlijk andere zijn dan die voor aanvraag- en uitgifte.

Wat beide processen en groepen applicaties gemeen hebben is dat ze alle afhankelijk zijn van kwalitatief hoogwaardige gegevens omtrent signaleringen, waarvan de authentieke bron zich bevindt in de Kernregistratie reisdocumenten. Om tegemoet te komen aan de verschillende situaties, wordt een generieke business service 'signaleringcontrole' ontwikkeld die, via informatieservices, wordt ontsloten via het service platform (bijvoorbeeld een API) naar zowel een RDM applicatie als een toekomstig Aanvraag- en uitgifte Portaal voor de uitgevende instanties. Voor de signalerende instanties zal een apart portaal worden gemaakt.

Voor alle verschillende contexten waarin de service wordt gebruikt (verschillende processen en systemen) geldt een uniforme set aan (bedrijfs)regels (zoals autorisaties, benodigde input etc.), zodat toekomstige wijzigingen in beleid, wetgeving of informatiehuishouding direct via de uniforme services kunnen worden aangepast en/of bijgewerkt, waarbij de nieuwe situatie direct voor alle gebruikers van de service hetzelfde is.

De voorgestelde informatiearchitectuur kent de volgende grondslagen:

- Het kunnen vervullen van de voorgestelde regisseursfunctie in verschillende ketenprocessen betekent dat RvIG de hoeder van data en gegevens is. In de mate waarin zijn rol hier de gelegenheid toe biedt, draagt RvIG zorg voor kwalitatief hoogwaardige data en gegevens.
- RvIG is naast regisseur ook facilitator aan verschillende ketenpartners en stakeholders in termen van het beschikbaar stellen van noodzakelijke informatiediensten en applicaties. Dit betekent dat RvIG niet alleen wil voorschrijven, maar ook tegemoet wenst te komen aan de verschillende werkwijzen en belangen van de verschillende organisaties.
- Als ketenregisseur is, omwille van bewaking van de kwaliteit en het bewerkstelligen van doorlopende procesverbetering, gedetailleerd zicht op de keten noodzakelijk. Hiervoor is veel gedetailleerde operationele informatie noodzakelijk, die wezenlijk verder gaat dan louter de gegevens van de aanvraag en de gegevens omtrent het reisdocument.
  Deze operationele informatie dient als input voor een kwaliteitsmanagementsysteem, waarmee RvIG de kwaliteit op basis

van een (vooraf overeengekomen norm) beheerst, in samenwerking met de ketenpartners.
NB We merken op dat de benodigde informatie ook gedetailleerder is dan vooraf gedefinieerde management informatie of performance-indicators. Ervaringen uit andere branches leert immers dat het hebben van veel detailinformatie kan leiden tot niet van tevoren bedachte conclusies over knelpunten etc.

- Waar er behoefte is aan veel detailinformatie over het proces ten behoeve van analyse en procesverbetering, is het onwenselijk dat deze informatie gevoelige persoonsgegevens bevat. Een juiste ontkoppeling tussen beide soorten gegevens is dus essentieel.

Deze grondslagen hebben geleid tot enkele concrete besluiten met betrekking tot de informatiearchitectuur.

Bovenaan staat de keuze om alle gegevens voor het reisdocumentenstelsel in 1 kernregistratie samen te laten komen. Een kernregistratie zal weliswaar uit meerdere databases bestaan, maar de informationele samenhang en integriteit van gegevens en relaties wordt over de gehele kernregistratie geborgd. Op termijn betekent dit een aantal aantal aanpassingen aan de verschillende databases. Het betekent ook 1 centraal Master Data Management voor het gehele reisdocumentenstelsel.

De voordelen van deze aanpak zijn evident. Door een kernregistratie in te richten kan RvIG:

- adequater voldoen aan de informatiebehoefte van ketenpartners;
- beter inspelen op (toekomstige) wensen op het gebied van managementinformatie, fraudepreventie- en opsporing;
- de kwaliteit van gegevens beter monitoren en verbeteren.

Overigens is er gekozen om voor het reisdocumentenstelsel een Kernregistratie in te richten en er niet te streven naar een volwaardige Basisregistratie. Reisdocumentengegevens vormen kort gezegd geen basisgegeven voor een groot aantal andere overheidsprocessen. Ook de match met de 12 eisen van basisregistraties[5] is zodanig dat er geèn aanleiding is om te streven naar een Basisregistratie.

Consequenties van het hanteren van een kernregistratie zijn:

- Zoveel mogelijk wordt er rechtstreeks in de authentieke bron geregistreerd (eenmalige opslag, meervoudig gebruik). Deze is daarmee actueler.
- Zo min mogelijk gegevens worden gekopieerd en zoveel mogelijk aan de bron wordt bevraagd.
- In deze opzet is geen plaats meer voor de huidige rol van de BRP ten behoeve van gegevensopslag met betrekking tot reisdocumenten en signaleringen (met de komst van verschillende services zal uiteindelijk cat. 12 overbodig worden of zelfs een last vormen).

Op dit moment worden de reisdocument gegevens gefragmenteerd opgeslagen in verschillende registers op verschillende plekken bij verschillende leveranciers. Middels de servicegerichte architectuur kunnen deze gegevens logisch vanuit één centraal punt (het serviceplatform) worden ontsloten, ook al blijft het beheer van deze gegevens in veel gevallen

[5] *Zie: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/gegevens/naar-een-gegevenslandschap/themas/twaalf-eisen-stelsel-van-basisregistraties/*

onderdeel van de instantie of ketenpartner die hier verantwoordelijk voor is (zie voor een duidelijkere beschrijving paragraaf 4.2).

Voor de technische datamodellen (de database inrichting) zijn de leveranciers verantwoordelijk. Voor het conceptuele en logische gegevensmodel, alsmede de business rules is RvIG verantwoordelijk.

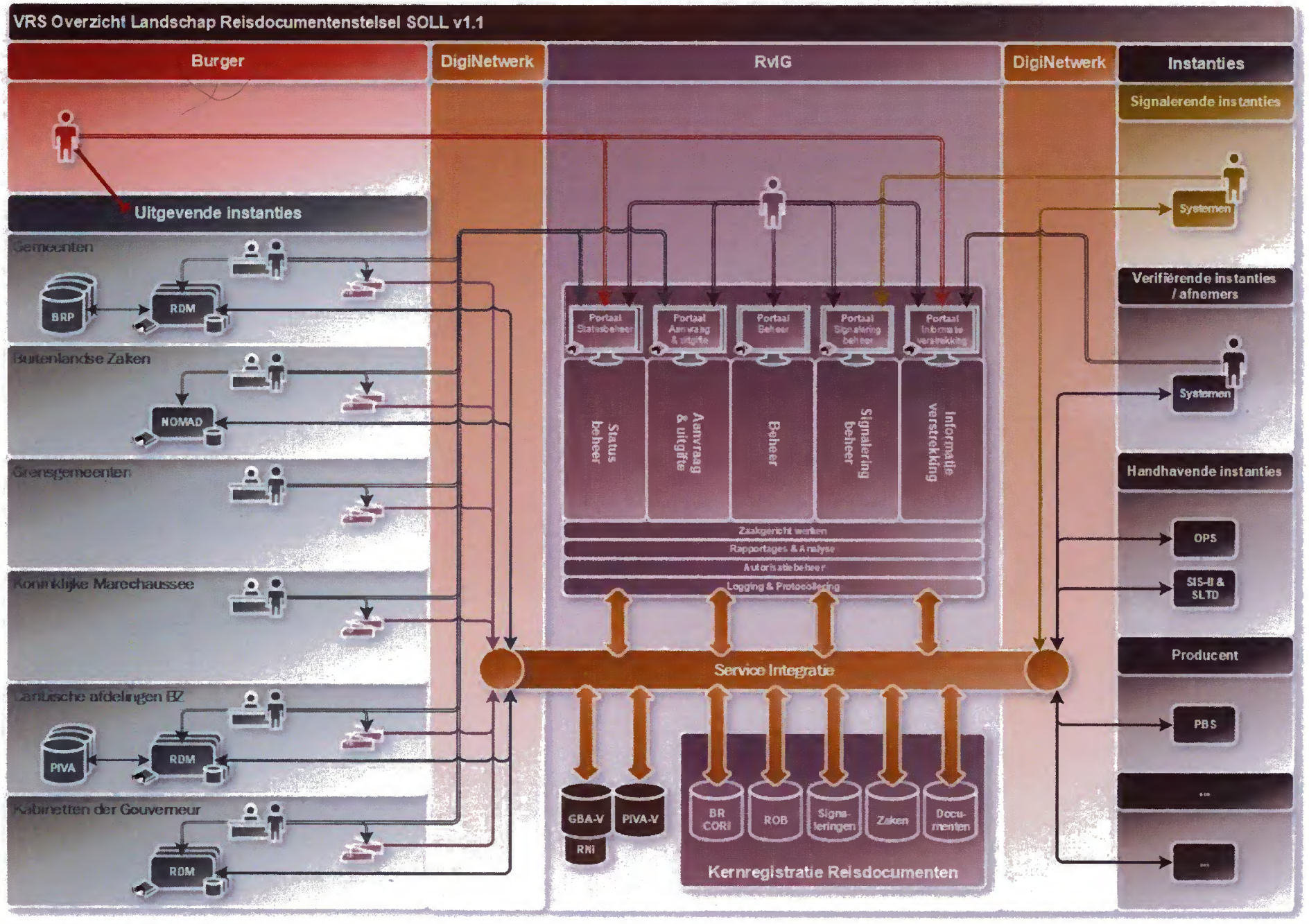
Voor de realisatie van de kernregistratie zoals hierboven beschreven is een reeks aanpassingen aan bestaande databases en systemen noodzakelijk. Een reeks niet limitatieve opsomming:

- Het creeren van een virtuele registratie voor personen die we kennen in relatie tot het reisdocumentenstelsel. Het gaat hierbij om 1 registratie, waarbij de bulk van de personen echter in de BRP of PIVA's voorkomen of alleen als houder van een reisdocument. Waar mogelijk wordt een persoon uitsluitend als referentie opgenomen. Dit impliceert ook een aantal wijzigingen in de bestaande reisdocument applicaties.
- Het signaleren van reisdocumenten verhuist naar het beheer van status van reisdocumenten.
- Er worden CRUD (create, read, update en delete) 'stekkers' op de huidige databases gemaakt om de gegevens via het services platform te kunnen ontsluiten. Hiervoor is er wel een goed beeld nodig van welke type bevragingen er op die databases in de huidige situatie worden gedaan. In de nieuwe opzet wordt dit geregeld via business- en informatieservices.
- Een reeks van wijzigingen is nodig om de verschillende systemen meer in samenhang te laten werken.

4.1 Applicaties

4.1.1 Afbakening en applicatiecomponenten

In de bijlage is een overzicht toegevoegd van de verschillende applicatiecomponenten die worden gerealiseerd/aangepast binnen het programma VRS. Daarnaast wordt op de volgende pagina een conceptuele weergave van het beoogde stelsel gepresenteerd, waarvan de verschillende componenten vervolgens worden toegelicht.



Figuur 4 VRS Architectuurvisualisatie

Kernregistratie Reisdocumenten
In lijn met de verschillende doelstellingen en kaders zoals eerder beschreven, wordt de totstandkoming van een volwaardige kernregistratie Reisdocumenten beoogd. Deze kernregistratie, die effectief bestaat uit een op informatie niveau geïntegreerde set aan registers, bevat alle relevante gegevens met betrekking tot het stelsel en zal gelden als de primaire authentieke bron van reisdocument gerelateerde gegevens. Via het later te omschrijven integratie platform kunnen de gegevens worden aangepast of ontsloten via business processen, diens ondersteunende applicaties en daarin geïntegreerde business services. Onderdeel van deze kernregistratie zijn:

- CORI/BR – Een centrale opslag voor informatieobjecten betreffende het aanvraag- en uitgifte domein (exclusief biometrie), het statusbeheer domein (statusregistratie van fysieke en digitale documenten en de bijbehorende meldingsgegevens) en het reisdocument domein (gegevens over de reisdocumenten zelf). CORI is 'loosely coupled' aan de BRP, om de integratie te kunnen leggen met de authentieke bron voor persoonsinformatie.
- ROB/biometrie – Een centrale opslagmogelijkheid voor informatieobjecten betreffende biometrie, aanpasbaar/raadpleegbaar/opvraagbaar onder strikte condities. Afhankelijk van voortschrijdend inzicht met betrekking tot beleid en wetgeving wordt het register aangepast om aan (toekomstige) eisen en functionele behoefte te kunnen voldoen. (Onderdelen van) biometrische informatie is gekoppeld of 'loosely coupled' aan informatie in CORI, maar met adequate en eventueel afwijkende beveiligings- en anonimiseringsmaatregelen).
- Het signaleringsregister (louter de database, waar paspoortsignaleringen en een referentie naar natuurlijke personen centraal staan) zien we als onderdeel van de kernregistratie maar zal losjes gekoppeld (loosely coupled) worden ingericht t.o.v. CORI (waar documenten en houders centraal staan).
- Informatieobjecten betreffende zaakgegevens en documenten[6] (DMS), 'loosely coupled' aan de bovenstaande registers. Indien bedrijfsprocessen vragen om nieuwe oplossingen betreffende documenten en zaakgegevens, zullen deze via een nader te ontwerpen oplossing worden geïntegreerd (loosely coupled) in de kernregistratie. Realisatie zal uitwijzen of de noodzaak voor database oplossingen in de front-end overeind blijft of dat met de mogelijkheid om procesgerelateerde zaakgegevens op te slaan deze noodzaak kan komen te vervallen.
- Mogelijk ontstaan in de toekomst wensen voor additionele gegevensopslag, bijv. een geanonimiseerde/gepseudonimiseerde data warehouse voor onderzoek, analyse en fraudedetectie.

Het doel van de loosely coupled bronnen is om één logische en authentieke bron (ofwel kernregistratie) te ontwikkelen. Uiteindelijk moet het tot één fysieke kernregistratie leiden maar dat is een operatie die langer dan het programma VRS in beslag zal nemen. Aanpasbaarheid en dynamisch beheer zijn hierbij sleutelwoorden: anders dan het creëren van een gefragmenteerd informatiestelsel van verschillende registers op verschillende locaties en in

[6] *Bedrijfsanalyse en analyse beleid/wetgeving zal uitwijzen om welke documenten het in potentie kan gaan. Te denken valt aan documenten die op dit moment reeds onder beheer van RvIG worden opgeslagen (zoals verschillende C-formulieren, mochten deze niet gedigitaliseerd kunnen worden), maar daarnaast zijn documenten omtrent signaleringenbeheer, dossiervoering, statusbeheer niet ondenkbaar. Hoewel het te vroeg is om een definitief uitsluitsel te geven, is een toekomstbestendige voorziening die kan omgaan met nieuwe wensen/eisen de doelstelling.*

beheer bij verschillende partijen/leveranciers, is het de doelstelling om naar een flexibel en wendbare kernregistratie te bewegen waarbij toekomstige aanpassingen als norm i.p.v. uitzondering worden verondersteld.

Ondersteuning van aanvraag- en uitgifte
In het aanvraag -en uitgifte domein hebben we te maken met verschillende applicaties die varianten van het aanvraag- en uitgifteproces ondersteunen. Op hoofdlijnen is het aanvraag- en uitgifte proces uniform, maar er bestaan verschillen in werkwijze en prioriteiten (veelal op basis van verschillen in doelgroepen/aanvragers en benodigd onderzoek), volgordelijkheid van procesactiviteiten en verschillende mogelijkheden in gebruikte brongegevens. Met de nieuwe architectuur en te ontwikkelen applicatiecomponenten beogen we recht te doen aan deze diversiteit zonder de processen fundamenteel aan te passen, maar tegelijkertijd uniformiteit te faciliteren en bewerkstelligen en flexibiliteit en keuzemogelijkheden te ondersteunen. Daarnaast is het van belang om te benoemen dat we met name de onderliggen informatievoorziening (e.g. het beroep wat gedaan wordt op (externe) registraties) willen uniformeren en gelijkwaardig willen aanbieden middels business- en informatieservices.

Concreet betekent dit het volgende:

- Een eerste prioriteit komt voort uit de noodzakelijke vervanging van de (front- en backoffice) functionaliteit van het RAAS. Teneinde het RAAS te kunnen uitfaseren wordt daarom de realisatie van een Reisdocumenten aanvraag portaal beoogd, ter ondersteuning van het aanvraag- en uitgifte proces.
- Het nieuwe portaal wordt via het service integratie platform gekoppeld aan de kernregistratie reisdocumenten, zodat via uniforme services gegevens kunnen worden aangeleverd en verkregen. Enerzijds betekent dit dat gegevens betreffende een aanvraag via services worden toegevoegd, gewijzigd en opgehaald aan/in/uit de kernregistratie. Anderzijds wordt het gebruik van externe (controle)gegevens, zoals een controle op paspoortsignaleringen, via services aan de applicatiefuncties van het portaal beschikbaar gesteld.
- De te realiseren business- en informatieservices worden ook beschikbaar gesteld voor integratie in 'eigen' applicaties van ketenpartners, op basis van nader te analyseren behoeften en eisen/wensen. Op deze manier wordt het mogelijk om, ook al worden onderdelen van het aanvraag- en uitgifteproces bij verschillende instanties in verschillende applicaties uitgevoerd, een uniformiteit in het gebruik en registratie van gegevens richting te kernregistratie bewerkstelligd.

Er wordt voor ondersteuning van het aanvraag- en uitgifte proces voorzien in een breed scala van services, waarvan een (niet limitatieve en uit te breiden) opsomming zich bevindt in de bijlage.

Ondersteuning voor statusbeheer
Business services ten behoeve van statusbeheer zullen worden gerealiseerd en beschikbaar gesteld. Uitgangpunt hierbij is het actueel kunnen ontvangen en verwerken van signalen omtrent de status van reisdocumenten. De services zullen n.a.v. een procesinventarisatie worden verdeeld over frontoffice of backoffice handeling, afhankelijk van de specifieke situatie en applicatieondersteuning bij verschillende ketenpartners en (meldende) instanties. Doelstelling is dan ook om de diversiteit aan methoden van melden (zoals nu gebeurd via onder andere de BRP, formulieren, doorverwijzingen

naar andere instanties) te uniformeren en toekomstige mogelijkheden (zoals het rechtstreeks kunnen melden van een statuswijziging door de houder) mogelijk te maken. Zo kan eenzelfde service voor het melden van een vermissing mogelijk worden geïntegreerd in de reisdocumentenmodule bij gemeenten, het aanvraag- en uitgifteportaal wat wordt beheerd door RvIG of bijvoorbeeld MijnOverheid voor de burger (analyse gaat uitwijzen waar een dergelijke aanroep van de service gewenst is).

In deze systematiek zal de rol van het huidige BR, de formulierenverwerking met betrekking tot statusbeheer en de proces en signalerende functie van GBA/cat. 12 komen te vervallen.

Ondersteuning voor signaleringenbeheer
We onderscheiden bij signaleringenbeheer twee type processen die binnen het VRS programma zullen worden herontworpen en waarvan de applicatieondersteuning wordt veranderd:

1. Het beheren van signaleringen door signalerende instanties. Waar signaleringen (zowel totstandkomingen als wijzigingen of beëindigingen) nu veelal middels fomulierenverkeer worden bewerkstelligd en kampt met inefficiëntie, wordt de totstandkoming van een signaleringebeheer portaal beoogd zodat signalerende instanties de mogelijkheid krijgen om direct mutaties door te voeren (met inachtneming van de controlerende en toetsende functie van RvIG). Indien mogelijk wordt de benodigde dossiervoering hier ook ondergebracht.
2. Het zelf kunnen opvoeren, toetsen en beheren van meervoudige vermissingen, beschadiging of misbruik en de daaropvolgende paspoortsignalering (artikel 24b). Dit is een proces wat in veel gevallen door RvIG wordt uitgevoerd en waar veel (efficiëntie)verbeteringen mogelijk zijn. Hiervoor is aanvullend op eerdere diensten ook een document managementsysteem nodig en een koppeling op het zaakmanagementsysteem.

Op de applicatiecomponenten voor 'signaleringenbeheer' en de te ontsluiten services zijn de hierna te beschrijven generieke componenten voor autorisatiebeheer, rapportage en analyse, zaakgericht werken en logging en protocollering van toepassing.

Informatievoorziening/verstrekking
In de maatschappij zijn een groot aantal organisaties en ketenpartners afhankelijk van actuele en kwalitatief hoogwaardige gegevens met betrekking tot reisdocumenten en andere onderdelen van de kernregistratie, bijvoorbeeld voor identiteitsverificatie. Door de gefragmenteerde opzet kent deze informatieverstrekking op dit moment een grote diversiteit aan (technische en functionele) varianten. Door deze verschillende vormen van informatieverstrekking onder generieke architectuur te brengen kunnen deze centraal (uniform) worden aangeboden richting de buitenwereld. Voorbeelden van externe services zijn levering aan het Schengen informatiesysteem (SIS II), het nationaal opsporingsysteem (OPS), Interpol's Stolen and Lost Travel Documents (SLTD), het verificatieregister (VR) en de huidige informatieverstrekking aan (publieke) organisaties op basis van GBA-V.

Van belang is om te onderkennen dat hoewel de gegevens centraal worden opgeslagen en ontsloten, de verantwoordelijkheid voor het beheer (toevoegen, wijzigen etc.) en het eigendom conform huidige wet- en regelgeving bij de huidige instanties blijft. Conform B-ALG-07 ontstaat dan

ook de noodzaak dat hoewel informatieverstrekkingen vanuit een centraal punt worden georganiseerd en ontsloten, de verantwoordelijke instantie (lees: uitgevende instantie die de gegevens initieel heeft geregistreerd) toestemming dient te geven voor ontsluiten van inhoudelijke informatie richting een andere instantie.

Service integratie platform
Een service integratie platform gaat voorzien in de informatiebehoefte van de verschillende applicatiecomponenten (intern/centraal) en gegevensbehoefte van externe instanties. Het platform maakt hierbij gebruik van gegevens uit de kernregistratie Reisdocumenten en de basisregistraties personen (GBA-V, PIVA-V en PIVA's). Doelstelling is om alle informatiestromen met behulp van in via het platform beschikbaar gestelde generieke business- en informatieservices (zie hoofdstuk 'gegevensuitwisseling') te digitaliseren, uniformeren, raadpleegbaar te maken en beschikbaar te stellen.

De toegevoegde waarde van het service platform is dat er één uniforme toegang is waarop met verschillende technieken er orkestratie kan plaatsvinden welke informatie er aan welke partij wordt geleverd. Integraal onderdeel van de bus zijn identificatie, authenticatie, autorisatiebeheer, rapportage en analyse, logging en protocollering en transformatie van verschillende protocollen.
Op het platform zijn tenminste aangesloten:

- Kernregistratie Reisdocumenten
- Applicatie voor aanvraag- en uitgifte en statusbeheer
- Applicatie voor signaleringenbeheer
- (Eigen) systemen voor aanvraag- en uitgifte bij uitgevende instanties, zoals RDM (gemeenten en Caribische instanties) of NOMAD (Buitenlandse Zaken).
- Systemen van de producerende en personaliserende organisatie, waaronder ook decentrale personalisatiesystemen voor bijvoorbeeld nooddocumenten.
- Systemen van verifiërende instanties (huidige VR afnemers)
- Systemen van handhavende instanties (SIS-II, OPS)
- Systemen van instanties die behoefte hebben aan informatie omtrent reisdocumenten (de huidige afnemers van in BRP aanwezige gegevens omtrent reisdocumenten).

Beheer
Beheerfuncties voor functioneel- en applicatiebeheer in het stelsel worden generiek opgezet en toegankelijk gemaakt voor medewerkers van RvIG (of onder regie van RvIG uitbesteed). Beheerfunctionaliteiten zijn in deze van toepassing op de verschillende te realiseren applicaties- en portalen en regie over de business services die via het platform worden ontsloten. Te denken valt aan de mogelijkheid tot het inrichten en aanpassen van parameters, masterdata management op uitgiftepunten, type documenten en het delegeren van het wijzigen van deze basisgegevens, het inrichten en beheren van autorisatie(profielen), workflow-aspecten, inzicht in en mogelijkheid tot afhandeling van fouten etc. Hierbij is het uitgangspunt dat formulieren hiervoor digitaal worden aangeboden (zogenaamde e-formulieren).

Zaakmanagement
Concepten van zaakgericht werken zullen binnen de generieke architectuuropzet als uitgangpunt worden genomen. Procesmatige onderdelen zoals werktoewijzing, statusovergangen, het beheer van doorlooptijden, eigenaarschap, documentregistratie en dossiervoering zullen over de reeds

beschreven domeinonderdelen middels concepten van zaakgericht werken worden geregistreerd, beheerd en ontsloten. De specifieke (applicatieve) invulling wordt in de toekomst nader bekeken, alsmede de noodzakelijkheid voor zaakmanagement over de keten indien meerdere zaaksystemen betrokken zijn. We voorzien in berichtuitwisseling tussen zaaksystemen waarbij regie kan worden gevoerd m.b.t. informatie over (lopende) zaken en diens afhandeling.

Rapportage en analye
Functionaliteiten voor rapportage en analyse worden voorzien. Daarbij is het van belang om flexibel rapportages in te richten en te produceren, bijvoorbeeld ten behoeve van inzicht in lopende processen, aantallen documenten in relatie tot status, berichten en foutsituaties.

4.1.2 Beleidslijnen, richtlijnen, standaarden

I1-ALG-01 **Akkoord**	**Softwareontwikkeling volgens beproefde methodieken**
Statement	Softwareontwikkeling dient volgens beproefde methodieken te verlopen.
Rationale	Ontwikkelprocessen zijn gedefinieerd, transparant en kwalitatief goed. Hierbij is inzicht en beheersing van het ontwikkelproces.
Implicaties	Dit komt tot uiting in inzicht van de ontwikkelpartij(en) in o.a. ▪ Actueel inzicht in aantal opgeloste en openstaande fouten in de diverse software 'builds'. ▪ Inzicht in code kwaliteit, security kwetsbaarheden en code smells. ▪ Beschreven ontwikkelproces met beschreven deliverables. ▪ Automatische toetsing tegen richtlijnen. ▪ Offreren op basis van functiepunten en uren per functiepunt. ▪ Inzichtelijke inhoudelijke rapportage over ontwikkelproces en mijlpalen. ▪ Inrichting van softwareontwikkelstraat met continuous integration / continuous delivery ten behoeve van de ontwikkeling van webapplicaties (op diverse portals) en mobiele apps.

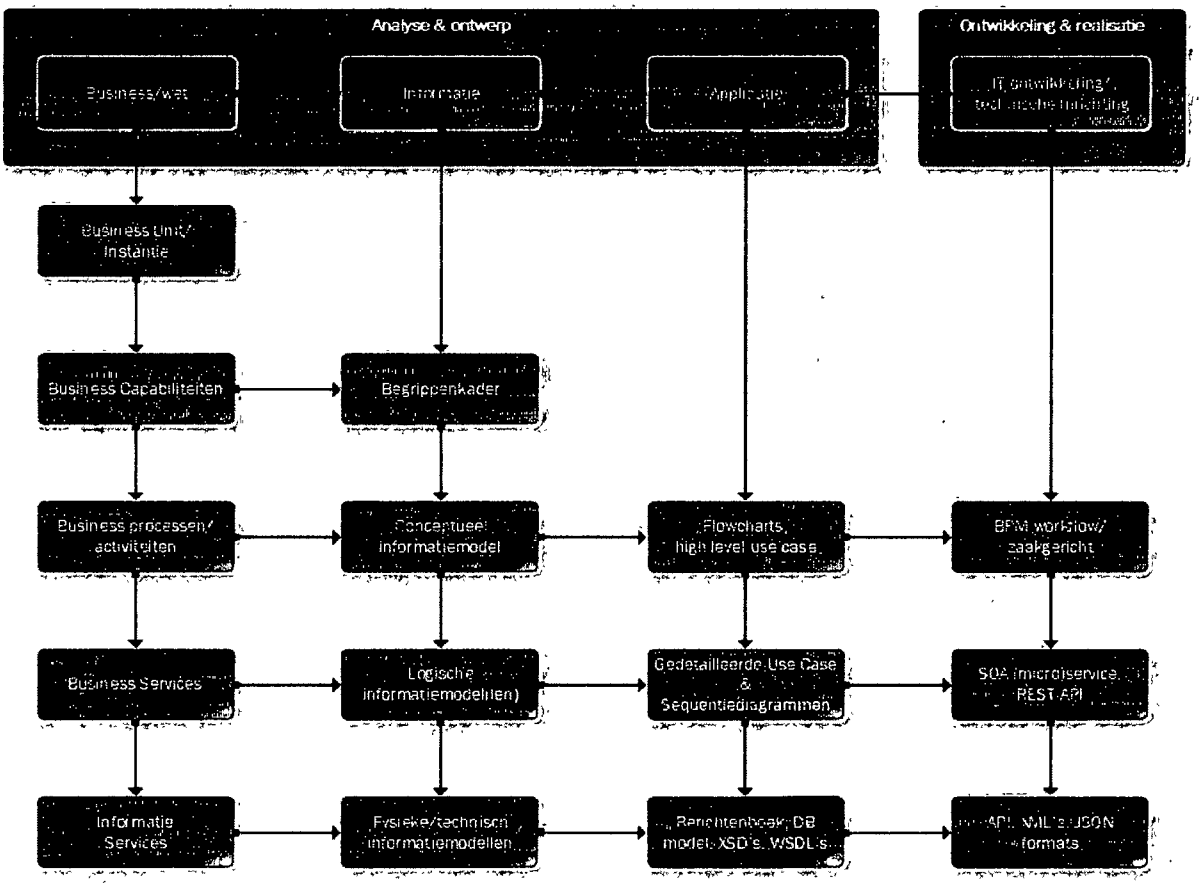
I1-ALG-02 **Akkoord**	**Scheiding tussen applicatielagen**
Statement	Logische scheiding tussen applicatielagen.
Rationale	Het is mogelijk om applicatieonderdelen die zich binnen een bepaalde applicatielaag (presentatie, verwerking, data) bevinden, aan te passen, zonder dat de functionaliteit van de andere lagen moet worden aangepast (conform het concept van 'microservices'. Een uitzondering vormt de situatie waarin wezenlijk nieuwe informatie aan de interface wordt toegevoegd, bijvoorbeeld een nieuwe rubriek dat in de presentatielaag moet worden ingewonnen en in de verwerkingslaag moet worden toegepast.
Implicaties	▪ Aanpassingen in de technologie c.q. ICT-producten waarop een laag is gebaseerd (bijvoorbeeld client/server wordt web-based, een flat file wordt DBMS) zijn nimmer aanleiding om andere lagen aan te passen. ▪ Bij scheiding van lagen moeten er afspraken worden gemaakt over welke lagen de statussen over een proces bijhouden. Zo zijn de zaaktypen altijd statefull en is de harde infrastructuurlaag stateless (IAAS - Infrastructure as a Service). Voor de uitwisseling van berichten wordt zo veel mogelijk gebruik gemaakt van asynchrone berichtgeving.

I1-ALG-03 Akkoord	Kwaliteit logging
Statement	Bepaalde applicatielogs dienen voor één jaar bewaard te worden. De logging dient voldoende verklarend te zijn.
Rationale	Goede logging biedt een leidraad in het traceren van de herkomst van een probleem. Het is daarom essentieel dat logging de juiste informatie bevat.
Implicaties	▪ Opnemen van tijdstempels, herkomst (zoals object en/of methode welke de log betreft) en overige nuttige informatie in de logging. ▪ Iedere log heeft zijn eigen unieke identificatie van de logging. ▪ Standaardopmaak van de logging, zodat de log later eenvoudig door een automatisch proces te bewerken is. ▪ Persoonsgegevens worden niet in logging opgenomen; slechts een sleutel of verwijzing.

I1-ALG-04 Akkoord	Authenticatie en autorisatie wordt gestandaardiseerd ingericht en moet compatible zijn met andere systeemcomponenten teneinde te streven naar een Single Sign-On
Statement	Omgevingen zijn gebruikersvriendelijk; het aantal inlogacties wordt geminimaliseerd.
Rationale	Authenticatie en autorisatie wordt gestandaardiseerd ingericht en moet compatible zijn met andere systeemcomponenten teneinde te streven naar een Single Sign-On. De aangeboden applicaties en systemen moeten SSO faciliteren in hun oplossing over de Infrastructuur en de Applicatieve kant heen. Het doel van RvIG is om een beheerder éénmaal in te laten loggen en daarna zonder verdere aanmelding te kunnen laten werken.
Implicaties	▪ Infrastructuren, diensten en applicaties moeten gestandaardiseerd zijn zodat ze aan kunnen sluiten op de methoden van SSO die gehanteerd wordt. ▪ Toegang voor gebruik van Infrastructuur, diensten en Applicaties is alleen mogelijk na vaststelling van de identiteit en de juiste autorisaties. ▪ Vanuit beveiligingsbeleid, bijv. door verschillen in dataclassificatie, kan van dit principe afgeweken worden.
Kwaliteits-kenmerken	▪ Verantwoording, Integriteit, Efficiëntie

I1-ALG-05 Akkoord	'Gebruiker centraal' bij software ontwikkeling
Statement	Servicegerichtheid en gebruikersvriendelijkheid met gebruiker als uitgangspunt dienen centraal te staan bij het ontwerp en ontwikkeling van applicatiecomponenten.
Rationale	Ontwerp en ontwikkeling van software is aantoonbaar met de gebruiker als uitgangspunt ontwikkeld.
Implicaties	▪ Producten worden volgens beproefde ontwerpdisciplines (UX design, interaction design) ontworpen, gericht op het creëren van producten en diensten die nuttig, bruikbaar en betekenisvol zijn voor de mensen die ze gebruiken. ▪ Daadwerkelijke gebruikers fungeren als testers en leveren input.

4.1.3 Analyse en ontwerp



Figuur 5. Visualisatie ontwerp- en analyseproducten

Bovenstaande weergave geeft schematisch weer hoe de applicatiecomponenten en benodigde beoogde ontwerpdocumenten en analyseproducten zich tot elkaar verhouden. Centraal hierin staat de notie van 'business services', die de grondslag vormen voor het stelsel en de te realiseren informatievoorziening.

Onder een business service verstaan we: 'een herkenbare brok werk'. Deze definitie is bewust breed, omdat er enige mate van subjectiviteit bestaat met betrekking tot de granulariteit (lees: de mate van afbakening of 'grootte' van een service). De volgende aspecten dienen in ogenschouw te worden genomen bij het formuleren van een adequate set aan business services:

0. Naam en doelstelling: Een herkenbare naam en een herkenbaar doel voor de organisatie of ketenpartner. Het doel wordt meestal uitgedrukt in termen van de bedrijfsfunctie die ermee gerealiseerd wordt. Een brok werk is pas gereed als het betreffende doel is bereikt. Als sprake is van verschillende bedrijfsfuncties worden aparte business services onderkend.
1. Het (bedrijfs)activiteitenaspect: De activiteiten die worden ondersteund of uitgevoerd. Er wordt gestreefd naar generiek bruikbare business services. De basis hiervoor vormt een traditioneel procesontwerp (het 'generiek behandel proces'), waarin gezocht is naar gelijksoortige processen voor de behandeling van alle soorten werk van de organisatie. Bij activiteiten die heel specifiek voor één werksoort gelden, wordt een aparte business service

onderkend. Het uitgangspunt is om geen vaste flow te hanteren: welke business services moeten worden uitgevoerd, is afhankelijk van de context van de zaak en kan op elk willekeurig moment opnieuw bepaald worden. Ook dit beïnvloedt de afbakening van business services.

2. Het organisatieaspect: De rol binnen de organisatie of keten die de activiteiten mag uitvoeren. Medewerkers met de betreffende rol zien de business services die zij mogen uitvoeren, daadwerkelijk ook terug op hun scherm, in de vorm van een behandelplan met behandeltaken die zij mogen uitvoeren voor de betreffende zaak. Als sprake is van ongeveer hetzelfde werk voor twee verschillende rollen, dan worden aparte business services onderkend.
3. Het informatieaspect: De informatie die nodig is om het brok werk te starten en de informatie die is vastgelegd als het doel van het werk is bereikt. Ook pre- en postcondities worden vastgelegd, met name de precondities (onder welke voorwaarden kan dit brok werk starten en op een juiste manier uitgevoerd worden) hebben invloed op het afbakenen van business services.
4. Het kennisaspect: De kennis die nodig is om de activiteiten uit te voeren of te ondersteunen. Deze kennis wordt deels geautomatiseerd ondersteund in de vorm van rules en een rule engine, maar kan ook in de vorm van intelligente ondersteuning worden aangeboden aan de medewerker. Het uitgangspunt is dat het systeem zou moeten kunnen werken op basis van de kennis en competentie van de medewerker, daardoor overlapt dit aspect wat betreft afbakening van business services met het organisatieaspect.
5. Het applicatieaspect: De applicatieve ondersteuning die wordt gerealiseerd met de gekozen standaardpakketten. Een business service valt uiteen in (herbruikbare) systeemfuncties, die in het applicatieaspect worden gerealiseerd in de vorm van bijvoorbeeld scherm en datastructuur. Er wordt met standaardpakketten gewerkt; wat er 'out-of-the-box' mogelijk is, bepaalt dus mede de afbakening van business services.
6. Het technologieaspect: De infrastructurele componenten die nodig zijn om de business service uit te voeren. Naast de gebruikelijke computerhardware of netwerken zijn er specifieke technische voorzieningen, zoals een aanvraagstation. Ook het technologieaspect kan leiden tot besluiten een aparte business service te onderkennen.

Bij verdere uitwerking en keuze van inrichting zal het ontwerp van services en andere ontwerpproducten nader gestalte krijgen.

4.1.4 Applicatie kwaliteitseisen

Invulling vanuit Quint2/ISO9126. Aangezien er wordt voortgeborduurd op de invullingen van het Basisregister/CORI nemen we die criteria als uitgangspunt en dienen de criteria in de projecten te worden getoetst c.q. qua capaciteit te worden uitgebreid.

08. Non functionals v2_1.docx

4.2 Gegevens

4.2.1 Informatiemodellering

In paragraaf 4.1.3 is reeds gevisualiseerd weergegeven hoe wordt omgegaan met informatiemodellering, waarbij een lagenmodel wordt gehanteerd om de informatiearchitectuur inzichtelijk te maken. Het programma VRS raakt vrijwel alle informatieobjecten in het reisdocumentenstelsel.

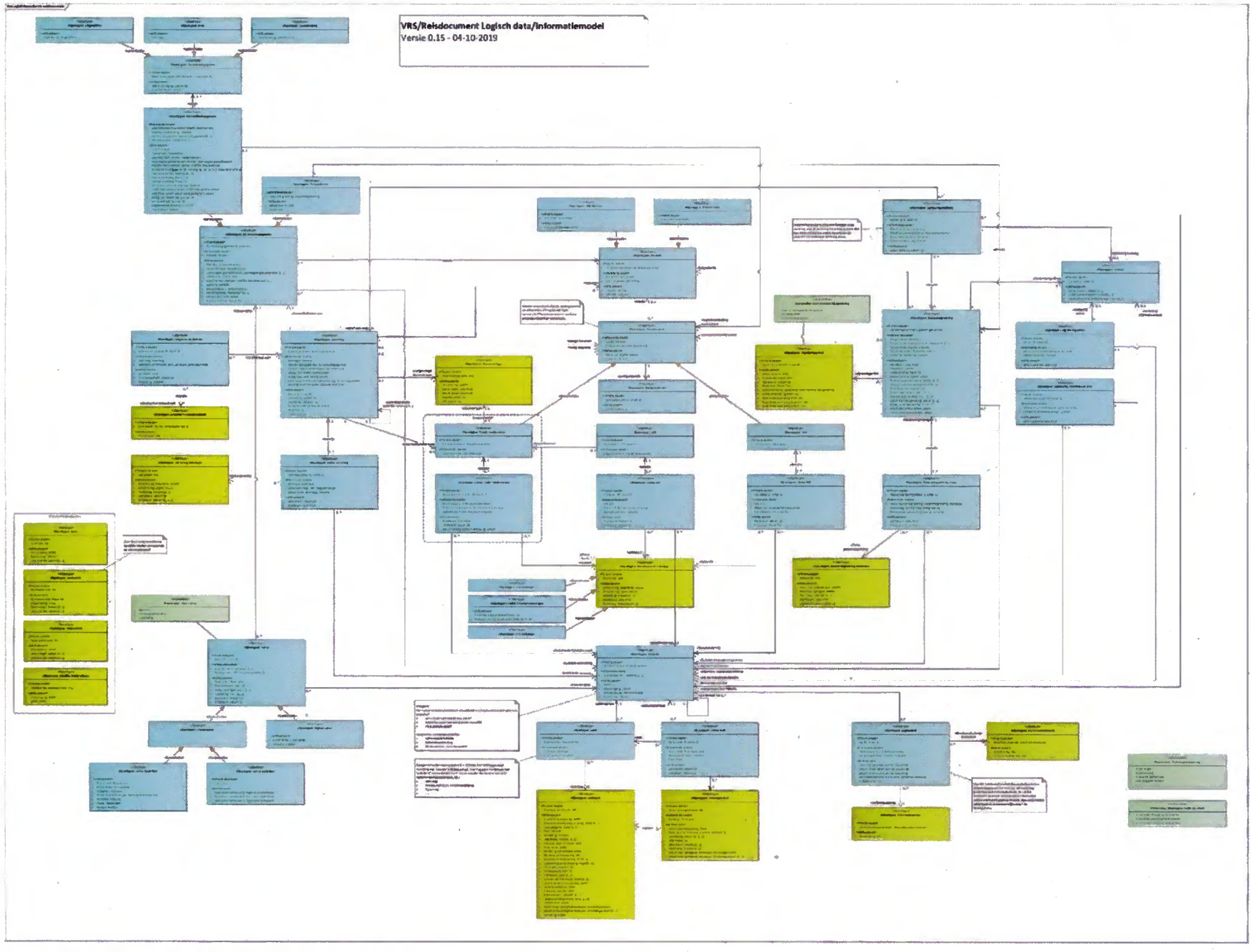
T.a.v. informatiearchitectuur en gegevensopslag worden een aantal veranderingen beoogd met betrekking tot processen, informatiestromen- en uitwisselingen, applicaties/registers en IT-infrastructuur. Om de creatie van een dergelijk informatie gedreven stelsel gedegen en toekomstbestendig op te zetten, is het van belang de opslag van informatie zodanig vorm te geven dat deze goed aansluit bij de (fysieke) werkelijkheid. Vandaar dat in dit hoofdstuk een logisch datamodel worden gepresenteerd om zo een 'model-driven' architectuur van het stelsel te bewerkstelligen. Het datamodel dient verschillende doelen:

- Een uniform kader voor communicatie en afstemming, door uniforme definities te geven voor in het stelsel relevante informatieobjecten.
- Het dient als blauwdruk voor applicatiecomponenten èn diens databases. De kernregistratie dient primair conform het model te worden gerealiseerd. Procesapplicaties kunnen de informatiemodellering idealiter volgen of dienen tenminste hiernaar vertaalbaar te zijn.
- Het model dient als canoniek model voor de te realiseren services en informatie-uitwisseling. Dit wil zeggen dat hoewel de specifieke datamodellering (fysiek) van applicaties kan afwijken er altijd ten behoeve van de uniforme uitwisseling vertaald dient te worden naar de objecten ineht model.

Het datamodel zelf is waar mogelijk gebaseerd op standaarden en normeringen (principes), met het oog op verbetering van de kwaliteit en integriteit van gegevensopslag. Op basis van de verschillende informatieobjecten in domeinen is het mogelijk een aantal richtinggevende uitspraken en doelstellingen te formuleren inzake de informatiearchitectuur en informatiestromen, eigenaarschap en visie op mutatiebeleid. De in het business onderdeel geformuleerde doelstellingen van het programma worden hiermee ondersteund/bewerkstelligd.

Op de volgende pagina is een weergave van het model te vinden. Voor een grotere weergave, open het onderstaande bestand. Het volledige model inclusief metagegevens en definities is op te vragen bij het programmateam (Sparx EA .eap file).

Logisch datamodel
VRS Reisdocumenten



Figuur 6 Logisch datamodel Reisdocumenten, versie 0.15

4.2.2 Algemene uitgangspunten en kaders

Het logisch informatiemodel is aan een aantal generieke uitgangspunten en kaders onderhevig.

- Als methodiek is een aangepaste UML methodiek genaamd MIM[7] toegepast. Het metamodel is ingelezen in Sparx EA, wat het mogelijk maakt om volgens de MIM standaard voor informatiemodellering het model vorm te geven en gegevens over objecten etc. vast te leggen.
- Uitgangspunt (tot op heden) is de creatie van één integraal model voor het gehele reisdocumentenstelsel. Vanuit dit model kunnen vervolgens, indien opportuun en mogelijk, domeinmodellen gegenereerd worden die betrekking hebben op bijvoorbeeld een business- of informatieservice.
- Centraal in het model staan objecttypen en diens attribuutsoorten. Attribuutsoorten zijn gelabeld als attribuutsoort, primaire sleutel of refererende sleutel.
- Het model bestaat uit een collectie van objecttypen en diens relaties. Objecttypen zijn geel gemarkeerd indien ze te classificeren zijn als beheerbare stam/ondersteunende objecten.
- Hoewel de granulariteit van beoogde informatie (micro-) services nog moet worden bepaald en gedurende doorontwikkeling zal worden verdiept, hanteren we het uitgangspunt dat één informatieservice idealiter op maximaal één of slechts enkele objecten/tabellen mutaties kan uitvoeren. Het aantal te raken tabellen beperken maakt is gunstig voor de onafhankelijkheid en wendbaarheid, maar is complexer om te realiseren.
- Uniformiteit staat centraal in het model. Objecten worden met het oog op normalisatie en objectgericht modelleren zoveel mogelijk onafhankelijk beschreven.
- Objecten die in beginsel vergelijkbaar zijn, worden maar één keer opgenomen (waar mogelijk met een generalisatie/specialisatie). Indien verschillen in populatie bestaan zoeken we dus naar één generieke methode van registreren. Voorbeeld: statustypen van verschillende type reisdocumenten kennen in principe voor een groot deel dezelfde attributen. Ze zijn daarom met behulp van een generalisatie opgenomen.
- Objecten worden niet (potentieel) dubbel opgenomen, maar waar mogelijk middels een verwijzing. Voorbeeld: we registreren niet een autoriteit verstrekking bij een aanvraag, maar leggen een verwijzing naar een instantie van het type autoriteit verstrekking.
- Het model dient zowel recht te doen aan het verleden als voorbereid te zijn op de toekomst. Dit betekent concreet dat gegevens die nu worden vastgelegd in huidige systemen op zijn minst na vertaling/mapping een plek moeten kunnen krijgen in het nieuwe model.

[7] *MIM: Metamodel voor informatiemodellering. Zie Link.*

- Wanneer we verwachten dat de veranderingen met betrekking tot gegevens in de toekomst mogelijk zijn, dienen deze beheerbaar te worden gemaakt. Voorbeeld: statussen worden niet in een (harde, niet wijzigbare) enumeratie ondergebracht, maar in een beheerbare stamtabel. Zo kunnen statussen die niet meer relevant zijn in het stelsel worden uitgefaseerd, terwijl historie bewaard blijft. Om een status toe te voegen is geen aanpassing in de database benodigd: dit behoort tot de mogelijkheden van een (functioneel) beheerder.
- Uitgangspunt is dat data in actieve tabellen blijven en van daaruit worden geschoond aan de hand van bewaartermijn (dus géén archieftabellen/stagingtabellen, zoals in de huidige registers vaak wel het geval is). Redenen om te werken met (geconsolideerde) archieftabellen vanuit oogpunt van opslagcapaciteit zijn er niet meer, en de database blijft qua aantallen objecten/tabellen eenvoudiger door historie in de reguliere tabellen te onderhouden.
- Het vraagstuk om te werken met een 'insert only' principe staat nog open. Mogelijk wordt de keuze gemaakt om mutaties in bestaande regels niet toe te staan, wat automatisch betekent dat veranderingen in de werkelijkheid altijd nieuwe regels/instanties tot gevolg hebben. Het voordeel hiervan is dat de integriteit van de database beter gewaarborgd wordt en het mogelijk wordt de database 'naar een bepaald tijdstip' terug te brengen. 'Tijdreizen' wordt hiermee (eenvoudiger) mogelijk.

4.2.3 Verklaring aan de hand van domeinen

In dit onderdeel van de PSA zal per af te bakenen domein/onderdeel van het datamodel een verklaring worden gegeven van de generieke opzet en specifieke keuzes. In het daadwerkelijke model zijn definities en kenmerken van objecten en diens attributen te vinden, zoals herkomst, verwijzing naar externe referenties etc. Met betrekking tot een aantal onderwerpen geven deze beschrijvingen echter niet voldoende onderbouwing om de keuzes ten aanzien van het model te onderbouwen.

Domein 'Personen en persoonsgegevens'
In het reisdocumentenstelsel worden persoonsgegevens (lees: een digitale representatie van een natuurlijk persoon en diens attribuutgegevens) op dit moment op verschillende plekken geregistreerd en beheerd. De BRP en PIVA's worden hierbij reeds als authentieke bron worden beschouwd. Door de fragmentatie van het stelsel, diens registers en (analoge) informatiestromen en systemen is een situatie ontstaan waarbij veel van deze persoonsgegevens worden gekopieerd en gearchiveerd. Dit brengt onherroepelijk vraagstukken met zich mee t.a.v. het bijhouden/bijwerken van deze gegevens bij wijzigingen in de authentieke bron, wat dan ook niet altijd/niet op tijd/niet volledig gebeurt.

In het programma VRS wordt een situatie beoogd waar we zo min mogelijk persoonsgegevens 'kopiëren'. Waar mogelijk wordt vanuit de nieuw op te zetten onderdelen van de kernregistratie en processystemen direct een beroep gedaan op de authentieke basisregistraties personen, door gebruik te maken van unieke sleutels (BSN, A-nummer en/of unieke sleutel ten behoeve van het reisdocumentenstelsel). We scheiden in deze de definities van een 'natuurlijk persoon' en de meer specialistische voorkomens (veelal momentopnames van gegevens) van deze persoon in het reisdocumentenstelsel. Ook is het een doelstelling om met betrekking tot de

primaire processen in het reisdocumentenstelsel altijd gebruik te maken van gegevens uit de basisregistraties (bijv. ten behoeve van het starten van een aanvraag) en deze digitaal middels services beschikbaar te stellen.

Bovenstaande kwesties en uitdagingen worden gevat in de volgende uitspraken:

- In principe zijn de basisregistraties personen (BRP en PIVA) de authentieke bron van persoonsgegevens en diens historie. Echter, deze registraties bevatten niet de gehele populatie van voor het reisdocumenten van belang zijnde personen[8] (in verschillende vormen, zoals aanvrager of gesignaleerde).
- De persoonsgegevens die op een document belanden, zijn een momentopname van de gegevens van een persoon. De gegevens van de persoon kunnen daarna wijzigen, maar het document (en dus de gegevens die daarop staan) blijft gelijk. De daadwerkelijk gepersonaliseerde gegevens dienen eenvoudig terug te vinden te zijn. Soms dienen services een beroep te doen op de gegevens van de persoon op dit moment, soms op de gegevens op het moment van … (vul in: momentopname in proces/functie).
- Het reisdocumentenstelsel wil reisdocument-relevante gegevens beheren, maar nadrukkelijk géén persoonsregistratie worden.
- Persoonsgegevens worden als resultaat van verschillende processen vastgelegd. Externe 'informatievragers' zijn veelal geïnteresseerd in de meeste recente momentopname-gegevens.

Rekening houdend met bovenstaande zijn de volgende keuzes gemaakt:

- Waar mogelijk heeft het Logisch ontwerp GBA als standaard gediend voor de specifieke keuzes t.a.v. datavelden en definities.
- Een voor het reisdocumentenstelsel relevant persoon krijgt een uniek ID binnen het object 'Persoon'. Dit object heeft daarnaast attributen om de koppeling met BRP/PIVA te bewerkstelligen. Dit is dan ook de externe verwijzing naar de authentieke bron van persoonsgegevens.
- Aan een persoon kunnen via het object 'RD persoonsgegevens' momentopnames van een set generieke persoonsgegevens worden gekoppeld. Zo heeft een object persoon 'een op veel' relatie hebben met 'RD persoonsgegevens'.
- Op dit moment beschouwen we 'personalisatiegegevens' en 'gesignaleerde persoon' als verbijzonderingen (specialisaties) van het object 'RD persoonsgegevens', elk met eigen relevante attributen. Op deze manier is het mogelijk de signalering te relateren aan een persoon met een basisregistratie personen verwijzing (wiens gegevens kunnen wijzigen in de tijd), maar ook aan een 'momentopname' van gegevens bij totstandkoming van de signalering (e.g. voor personen zonder verwijzing naar een basisregistratie personen. In de toekomst kan het aantal specialisaties worden uitgebreid.
- Een instantie/voorkomen van 'RD persoonsgegevens' van de specialisatie 'Personalisatiegegevens' bevat uitsluitend gegevens die gegevens die daadwerkelijk op het reisdocument worden gepersonaliseerd. Nadrukkelijk géén gegevens met betrekking tot de aanvraag (proces).

[8] *Een BRP of PIVA registratie is niet rand voorwaardelijk voor de aanvraag van een reisdocument. Er zijn veel personen die wél een reisdocument bezitten maar niet in de BRP of PIVA staan.*

- 'RD persoonsgegevens' (inclusief specialisatie) is bewust apart gemodelleerd ten opzichte van het object 'aanvraag'. Dit wijkt af van bestaande registraties: daar werden de gegevens m.b.t. personalisatie veelal als attributen van een aanvraag gezien. De scheiding wordt gemodelleerd omdat:
    - Ze mogelijk nu of in de toekomst aan een ander beveiliging/archieftermijn/NTB regime moeten voldoen.
    - De generieke gegevens (mogelijk) ook voor andere doeleinden moeten kunnen worden gebruikt (bijvoorbeeld een nieuwe aanvraag).

Bovenstaande modellering heeft de volgende voordelen:

- Mogelijkheden voor hergebruik van gegevens zijn geoptimaliseerd.
- Door uniforme registratie (i.c.m. reden/doelbinding/procescontext) kunnen bedrijfsregels worden opgesteld die de toegang en specifieke toestemming van (her)gebruik van gegevens nauwkeurig en spaarzaam worden ingeregeld.
- Gegevens van personen die géén registratie in de basisregistratie hebben, kunnen adequaat a.d.h.v. momentopnames worden vastgelegd, zonder dat direct de noodzaak bestaat om deze ook bij te houden/bij te werken zonder 'nieuw reisdocumenten gerelateerd proces'.
- Indien identiteitsfraude – aanvragen onder verschillende namen – wordt ontdekt, kunnen de gegevens op een juiste manier worden vastgelegd: 2 instanties van 'Persoon' kunnen worden gekoppeld waarbij de 'RD persoonsgegevens' instanties allemaal gekoppeld worden aan 'persoon'.
- Deze vorm van registratie maakt het bijzonder eenvoudig om te controleren of een bepaalde set persoonsgegevens voorkomt in het register (bijvoorbeeld voor de uitvoering van hit/no hit toetsingen), waarbij niet alleen naar de gegevens in hetzelfde domein wordt gekeken. Als voorbeeld: voor de registratie van een 'paspoortsignalering' kan (indien wenselijk) gebruik gemaakt worden van gegevens die verkregen zijn in de context van een eerdere 'aanvraag'. Op dit moment zijn deze domeinen gescheiden, waardoor fouten op de loer liggen.

Domein 'Reisdocumenten'
Met het vervallen van BRP Cat. 12 en de totstandkoming van een door RvIG beheerd (positief) register van reisdocumenten komt, in tegenstelling tot aanvraaggegevens en biometrie, de eindverantwoordelijkheid van de registratie van reisdocumenten, diens status en de kwaliteit van deze gegevens bij RvIG te liggen (hoewel dit reeds het geval was met betrekking tot het huidige basisregister). Initiële registratie van een reisdocument komt tot stand door de gebeurtenis 'verstrekken'. Veranderingen vinden daarna overwegend plaats door middel van statuswijzigingsverzoeken van uitgevende instanties, maar in de toekomst ook op basis van meldingen door de houder.

Enkele concrete uitspraken:

- Voorzien wordt in een adequate registratie van alle typen (fysieke) reisdocumenten, dus ook Laisser Passers en nooddocumenten (deze worden in het bijzonder genoemd omdat deze op dit moment geen registratie in een basisregistratie kennen).
- Gegevens over reisdocumenten worden in samenhang met andere informatieobjecten opgeslagen, zodat deze te relateren zijn aan een persoon of aanvraag.

- Binnen het reisdocument domein wordt de bijhouding van gegevens van andersoortige (reis)documenten voorzien. Denk hierbij aan eID, VID en mogelijk andere vormen van (digitale) reisdocumenten waarvoor in de toekomst gegevens dienen te worden bijgehouden. De kernregistratie en de opzet van services dienen hier reeds rekening mee te houden.
- Het primair identificerend attribuut is het documentnummer.

De volgende keuzes zijn gemaakt t.a.v. de registratie van reisdocumenten en diens gegevens:

- Centraal staat het objecttype 'reisdocument' met slechts een beperkte set gegevens en een verwijzing naar de houder (in de vorm van objecttype 'persoon').
- Er is gekozen voor een specialisatie t.a.v. verschillende soorten reisdocumenten zoals een 'fysiek document' en (mogelijke) toekomstige soorten zoals 'VID'. De specialisaties kennen een eigen set aan attribuuttypen (relevante gegevens voor de specialisatie). Op deze manier zijn in de toekomst nieuwe documentsoorten toe te voegen als specialisatie. Voor nu is alleen VID als andersoortig reisdocument in het model toegevoegd met een lichtere kleurindicatie, om aan te geven dat het optioneel is.
- De 'aan een document te relateren gegevens' die te beschouwen zijn als persoonsgegevens (lees in praktische zin: personalisatiegegevens) worden niet als attribuut bij een document geregistreerd, maar in een instantie van het objecttype 'RD persoonsgegevens' van het discriminator type 'personalisatiegegevens'. Op deze manier worden persoonsgegevens onafhankelijk beheerd en zijn deze te relateren aan zowel de betreffende aanvraag als het daadwerkelijk gepersonaliseerde reisdocument.
- eID is niet als documentsoort toegevoegd, maar als 'afgeleid document'. Daarbij wordt een eID document altijd aan een dragerdocument gekoppeld, waarbij het een eID object instantie een refererende sleutel heeft naar een fysiek document als 'dragerdocument'. Op deze manier zijn in de toekomst nieuwe documenten die een ander document als 'drager' kennen toe te voegen.
- Elk document (dus óók eID of 'gedragen document') kent een bijbehorende objecttype 'status', waarin de status van het document en diens historie wordt bijgehouden. In fysieke termen wordt er bij iedere statusovergang een nieuwe 'statusregel' aangemaakt. Daarmee is de gehele levenslijn van een document beschikbaar.
- Een stamtabel 'documenttype' wordt gebruikt als beheerbaar objecttype waarmee het documenttype van een 'fysiek document' kan worden vastgelegd (zoals nu ook gebruikelijk in de huidige systemen zoals RAAS of CORI/BR). Voor de andere documentsoorten voorzien we nu nog géén 'type attribuut'. Indien dit wel wenselijk is, zijn er twee mogelijkheden:
    - Er wordt per documentsoort een stamtabel met documenttypen gecreëerd.
    - Er wordt een specialisatie toegepast op de 'documenttype' stamtabel, waarbij we specialisaties creëren naar documenttypen die relevant zijn voor een specifieke documentsoort. In deze opzet zijn 'fysiek document' en 'VID' dus documentsoorten en de verschillende varianten van een 'fysiek document' (zoals een dienstenpaspoort of vreemdelingendocument) documenttypen.

- De totstandkoming van een stamtabel 'reisdocument statustype' met een specialisatie naar verschillende documentsoorten inclusief gedragen documenten maakt het beheer van statustypen mogelijk. Statustypen worden voorzien van een start- en mogelijk einddatum. Op deze manier kunnen statustypen in de toekomst worden uit gefaseerd, kunnen nieuwe statustypen worden toegevoegd. Bovendien kan historie met betrekking tot statustypen en statusregels worden gemigreerd zónder 'vervuiling' in de toekomst (immers, statustypen die voor de migratie van belang zijn maar vandaag de dag niet meer worden gebruikt kunnen een einddatum krijgen).
- Elke statusregel (instantie van status) krijgt een refererende sleutel naar een instantie, welke voor nu 'statushouder' genoemd is. Met andere woorden: de instantie die een nieuwe status meldt is ook direct de statushouder.
- Een objecttype 'configuratie info' is toegevoegd aan het model, met een relatie richting reisdocument. Hier kunnen configuratiegegevens die betrekking hebben op het reisdocument worden geregistreerd.

Domein ´Aanvragen´
De totstandkoming van de kernregistratie reisdocumenten beoogd een uniforme en enkelvoudige opslag van gegevens (zowel inhoudelijk als proces gerelateerd) omtrent aanvragen. De huidige decentrale opzet van verschillende RAAS systemen en diens archiveringsfunctie met betrekking tot aanvragen komt te vervallen. Aanvraaggegevens worden rechtstreeks in de kernregistratie geregistreerd, beheerd en waar nodig in informatieservices beschikbaar gesteld richting (andere) behoevende ketendiensten. Dit onder stricte condities en randvoorwaarden.

- Door de centralisering van aanvraaggegevens wordt het mogelijk om deze gegevens uniform en direct aan de verschillende uitgevende instanties beschikbaar te stellen en bevraagbaar te maken, weliswaar onder strikte condities. De aanvraaggegevens blijven echter onder regie/verantwoordelijkheid/eigendom van de uitgevende instantie in kwestie, dus een oplossing voor toestemming m.b.t. het gebruik van deze gegevens is benodigd. Dit voorkomt onnodige kopieën en (onveilige) overdracht van informatie via andere methoden zoals e-mail.
- De lokale (en arbeidsintensieve) back-up werkwijze van de verschillende RAAS registers komt te vervallen.
- Door de aanvraaggegevens uniform en centraal op te slaan ontstaan mogelijkheden voor andersoortig gebruik in de toekomst, zoals het finaliseren van een aanvraag bij een andere uitgevende instantie.

De volgende keuzes zijn gemaakt t.a.v. de registratie van aanvragen en diens gegevens in het logisch datamodel:

- Centraal staat het objecttype ´aanvraag´ met diens attribuuttypen. Er is nadrukkelijk voor gekozen om de attributen te beperken tot gegevens die alleen voor de aanvraag relevant zijn en niet gepersonaliseerd worden (deze zijn namelijk reeds ondergebracht in de specialisatie van ´RD persoonsgegevens´: 'personalisatiegegevens').
- Het objecttype aanvraag kent verschillende relaties (via refererende sleutels) naar andere objecttypen.

- Statusregistratie en het beheer van statustypen van aanvragen is gelijkwaardig opgezet aan de methodiek bij reisdocumenten. Van een aanvraag wordt de status bijgehouden in een apart objecttype, inclusief verwijzing naar instantie als statushouder. Dit biedt o.a. mogelijkheden om in de toekomst een aanvraag (met betrekking tot status in het proces) over te dragen aan een andere instantie (denk bijvoorbeeld aan de situatie waarin de afgifte wordt verzorgd door een andere instantie of een onderdeel van het proces wordt uitgevoerd door een centrale backoffice of controle-autoriteit). Daarnaast is er een stamtabel waarin de verschillende statustypen kunnen worden beheerd.
- Een aanvraag wordt altijd gekoppeld aan een objecttype 'personalisatiegegevens', die de gegevens bevat die daadwerkelijk zullen worden gepersonaliseerd op het document.
- Een toevoeging t.a.v. de huidige opzet van het stelsel is een objecttype 'uitgevoerde controle' met 'standaard controleactiviteit' als bijbehorende stamtabel. Dit maakt het mogelijk om te registreren dat bepaalde controles t.a.v. de aanvraag zijn uitgevoerd en op welke manier (bijvoorbeeld 'handmatig' of via een automatisch aangeroepen informatieservice). Het biedt bovendien mogelijkheden om in de toekomst kwaliteitscriteria te toetsen aan het aanvraagproces of de uitvoering van controles 'af te dwingen'.

Domein 'Paspoortsignaleringen'
Informatie omtrent paspoortsignaleringen wordt gedurende het programma integraal onderdeel van de kernregistratie reisdocumenten en via generieke informatie- en business services ontsloten richting relevante processen en applicaties.

- Signaleringscontrole ten behoeve van het aanvraagproces wordt op basis van actuele gegevens digitaal en generiek beschikbaar gesteld. De huidige vorm van gegevensleveringen aan uitgevende instanties komt daarmee te vervallen. Dit komt de handhaving en het acteren op signaleringen sterk ten goede en is nodig om de eerder beschreven doelstellingen te bereiken.
- Functies ten behoeve van het beheren van signaleringen worden voor zover mogelijk direct aan de signalerende instanties beschikbaar gesteld. Hiermee wordt de huidige document intensieve en inefficiënte werkwijze geoptimaliseerd.
- Het huidige datamodel van RPS bevat gekopieerde persoonsgegevens, welke moeten worden gesynchroniseerd met basisregistraties personen. Uitgangspunt is dat het kopieren van persoonsgegevens komt te vervallen, doordat gelijkwaardig aan eerder gestelde uitgangspunten er een directe link wordt gevormd tussen een signalering en een natuurlijk persoon. RPS zal dan echt onderdeel van de kernregistratie moeten worden om deze wijziging goed te faciliteren.
- Door signaleringen integraal onderdeel te maken van de kernregistratie wordt voorzien dat de adeqaute registratie (en daarmee controle op) van controles, beslissingen en andere aan het aanvraagproces gerelateerde handelingen m.b.t. signaleringen sterk verbeterd wordt. Op dit moment wordt hier niets over vastgelegd, maar is er wel de behoefte om meer grip te krijgen.

De volgende keuzes zijn gemaakt t.a.v. de registratie van paspoortsignaleringen en andere gerelateerde objecttypen en diens gegevens:

- De modellering van paspoortsignaleringen, adviezen en informatieverzoeken is grotendeels in stand gehouden in vergelijking met RPS.
- Het objecttype paspoortsignalering bevat geen persoonsgegevens maar is gekoppeld aan 'persoon' en 'RD persoonsgegevens', specialisatie 'gesignaleerde' om de koppeling te kunnen leggen met de persoon in kwestie. Op deze manier is het mogelijk de signalering te relateren aan een persoon met een basisregistratie personen verwijzing (wiens gegevens kunnen wijzigen in de tijd), maar ook aan een 'momentopname' van gegevens bij totstandkoming van de signalering (e.g. voor personen zonder verwijzing naar een basisregistratie personen.
- Het objecttype 'contact' is gecreëerd om op een uniforme methode contactgegevens bij een signalering, advies of informatieverzoek te kunnen registreren én te hergebruiken. Er is, omwille van het feit dat het relevant is om de contactgegevens t.b.v. één specifiek contactmoment te kunnen registreren, voor gekozen om dit niet bij 'instantie' en 'adres' vast te leggen.
- Een paspoortsignalering kan verschillende statussen verkrijgen, die geregistreerd kunnen worden met behulp van objecttype 'paspoortsignalering status'. Gelijkwaardig aan reisdocumenten en aanvragen, wordt gebruik gemaakt van een stamtabel voor statustypen en wordt een statusregel altijd gekoppeld aan een instantie.

Domein 'adressen'
In de huidige gegevensregistratie van het stelsel reisdocumenten worden adresgegevens op veel verschillende (en niet uniforme) locaties en manieren vastgelegd. Er is geen eenduidige registratie. In de nieuwe kernregistratie wordt hier wel in voorzien.

De volgende keuzes zijn gemaakt t.a.v. de registratie van adressen:

- Er is één uniform objecttype voor adressen gecreëerd. Een adres kan gekoppeld worden aan een instantie of een 'RD persoonsgegevens' via een refererende sleutel.
- Onder de attributen van het generieke objecttype adres zijn o.a. enkele toelichtingsvelden en herkomst geplaatst. Ook kent een adres altijd een registratiedatum. Zo kan, indien wenselijk, altijd het 'laatst bekende' adres van een object ('RD persoonsgegevens' ofwel 'instantie') worden bepaald. Dit biedt veel mogelijkheden t.a.v. informatieverstrekking van adressen. Bedrijfsregels kunnen worden toegepast om limitatie toe te passen op het soort adres (e.g. vanuit welke context een adres verkregen kan/mag worden).
- Adres wordt gespecialiseerd naar 'fysiek' adres en 'digitaal adres', elk met bijbehorende attributen.
- 'Fysiek adres' kent een specialisatie naar 'Adres Nederland' en 'Adres buitenland', zodat adressen waar mogelijk gestructureerd kunnen worden opgeslagen (in tegensteling tot adresregistratie in de huidige systemen, waar regelmatig zowel binnenlandse als buitenlandse adressen met vrije tekstregels zijn geregistreerd).

Domein 'instanties'
Instanties (lees: de registratie van organisaties/afdelingen/afnemers) kent in het huidige stelsel een gefragmenteerde opzet. Binnen het programma beogen

we deze te uniformeren ten behoeve van primaire taken, maar ook ten behoeve van autorisatie en logging.

De volgende keuzes zijn gemaakt t.a.v. de registratie van instanties:

- Het objecttype 'instantie' wordt als objecttype veronderstelt voor alle instanties die we erkennen in het reisdocumenten stelsel. Bij het objecttype zijn relevante attributen toegevoegd, gebaseerd op de gegevens die op dit moment worden vastgelegd in de huidige systemen.
- Een instantie als objecttype wordt in zéér veel objecttypen in het stelsel als refererende sleutel toegepast. Zo kan een instantie worden geduid als 'autoriteit verstrekking bij een aanvraag', 'statushouder bij signalering' of 'locatiehouder bij adres'.
- Een instantie kan onderdeel van een andere instantie zijn (bijvoorbeeld een afdeling als onderdeel van een overkoepelende instantie).

Domein 'biometrische gegevens'

Op dit moment worden biometrische gegevens decentraal opgeslagen in de verschillende RAAS registers. Vingerafdrukken worden na afloop van de aanvraag/uitreiking verwijderd (of na niet uitreiking bij overlijden of na drie maanden niet uitgereikt), terwijl foto's en handtekeningen gearchiveerd worden.

Doelstelling is om een centrale voorziening binnen de kernregistratie te creëren van waaruit biometrische gegevens kunnen worden ontsloten onder strikte condities van de context waarbinnen deze dienen te worden gebruikt (waarbij verschillende regels zullen gelden voor de verschillende voorkomens van biometrie, zoals foto's of vingerafdrukken). Voor de opslag van de vingerafdrukken blijft gelden dat deze na productie van het document of bij vervallen van het document worden verwijderd. De gegevens blijven onder verantwoordelijkheid en eigendom vallen van de uitgevende instantie. De centrale opslag ondersteunt een aantal (toekomstige) functies en mogelijkheden, zoals het toepassen van fotovergelijking, voorbereiding op een betere kwaliteit van foto's en het (eventueel) beter organiseren van een bevragingsfunctie voor handhavende instanties. Dit laatste vindt nu ad-hoc plaats waarbij gegevens per uitgevende instantie onder verschillende voorwaarden vaak onveilig beschikbaar worden gesteld en zonder uniform centraal beleid (afhankelijk van uitgevende instantie).

Enkele uitgangspunten hierbij:

- Biometrie wordt centraal opgeslagen en beheerd, waarbij protocollering van bewaartermijnen, anonimiseringsoverwegingen (e.g. het zo opslaan van biometrie dat deze slechts indirect te herleiden is tot een natuurlijk persoon) en autorisatie/toegang structureel kan worden ingebed en centraal georganiseerd. Het beheer/mutatierecht en eigendom blijft echter bij de uitgevende instantie.
- Biometrie wordt (beveiligd) niet direct gekoppeld aan een natuurlijk persoon (en indirect aan een aanvraag). Een uniek nummer zal worden toegekend aan de individuele biometrische kenmerken zodat de privacy wordt geborgd. Dit is een wezenlijk verschil met de huidige situatie/werkwijze. Het proces van bijvoorbeeld identiteitsverificatie zou dan als volgt kunnen lopen: opzoeken burger in kernregistratie, zien welk document c.q. welke aanvraag de meest recente biometrie bevat, daar staat een verwijzing naar de unieke nummers van de biometrie en van daaruit de foto ophalen voor een vergelijking of anderszins.

- Om de biometrische gegevens centraal te kunnen opslaan is er een wetstraject opgestart. Er zal echter geen wijziging aan de biometrische gegevens worden gedaan. Zodoende blijven vingerafdrukken slechts tijdelijk en ten gunste van een aanvraag (en dus de plaatsing op de chip) opgeslagen. Wel wordt voorzien in de opslag van metadata m.b.t. biometrie (bijvoorbeeld datum/tijdstip van afname, locatie, gebruikte apparatuur en eventuele afwijkingen m.b.t. afname).

Met betrekking tot de logische gegevensmodellering zijn de volgende keuzes zijn gemaakt:

- Een objecttype 'biometrisch gegeven' kan via een refererende sleutel worden gekoppeld aan een RD persoon van het discriminatortype 'personalisatiegegevens'. Dit is per definitie een momentopname en direct te relateren aan een specifieke aanvraag, wat de intrinsieke doelbindingsrelatie goed aantoonbaar maakt.
- 'biometrisch gegeven' kent een specialisatie naar 'vingerafdruk', 'foto' en 'handtekening'. Door deze werkwijze te kiezen ontstaat er ruimte om (indien gewenst) het aantal specialisaties in de toekomst uit te breiden.
- Het logisch model zegt in essentie niets over de fysieke locatie of scheiding van data m.b.t. de opslag van biometrische gegevens. Met andere woorden: de opzet zoals gepresenteerd in het model laat onverlet dat ervoor gekozen kan worden de daadwerkelijke biometrische gegevens fysiek gescheiden onder te brengen. Daardoor kan de toegang en autorisaties ook fysiek gescheiden worden en dat je bijvoorbeeld de "koppeling" tussen beiden kan beveiligen. Uiteindelijk moet er wél een koppeling te maken zijn met de personalisatiegegevens van een aanvraag.

Domein 'zaakgericht werken'
Zaakgerichte registratie wordt binnen het programma gezien als een middel om op een adequaat abstractieniveau harmonisatie over processen, behandeltermijnen, statussen, archivering en andere generieke concepten te bewerkstelligen. Zoals reeds eerder gesteld hebben instanties tot in bepaalde mate inrichtingsvrijheid ten aanzien van processen en applicatiecomponenten, maar dient er tegelijkertijd een uniform kader te zijn waarbinnen dit gebeurt of wordt toegestaan. Door middel van het vastleggen van belangrijke mijlpalen (proces cq statusovergang) wordt sturing op processen mogelijk. Niet in de laatste plaats om gegevens (en daarmee ook de uitwisseling) interpreteerbaar te maken.

Het domein van 'zaakgericht werken' is nog aan verschillende keuzes/opties onderhevig. In het logisch datamodel ervoor gekozen om gegevens met betrekking tot zaakgericht werken al wel te modelleren, maar slechts in beperkt. De volgende keuzes zijn gemaakt t.a.v. de registratie van zaakgegevens:

- De objecttypen met betrekking tot zaakgericht werken (e.g. 'zaak', 'zaaktype', 'status zaak' en 'statustype zaak') zijn direct overgenomen uit de VNG standaard voor zaakgericht werken, StUF-ZKN.
- Er is voor gekozen te starten met het modelleren van deze essentiële objecttypen. Mogelijk kan dit worden uitgebreid met de andere objecttypen conform de standaard, zoals verschillende stamtabellen en een zaaktypecatalogus.

- Een 'zaak' en 'zaakstatus' hebben altijd een refererende sleutel naar een 'instantie' (als zaakeigenaar of statushouder zaak).
- Er is voor gekozen om de koppeling naar mogelijke 'zaakobjecten' (lees in praktische zin: het onderwerp van de zaak) nog niet direct te modelleren gezien de complexiteit en leesbaarheid van het model. In essentie kan een zaak in het reisdocumentenstelsel betrekking hebben op een aanvraag, persoon, paspoortsignalering of reisdocument, maar het is niet ondenkbaar dat er meer zaakobjecten kunnen worden gedefinieerd. Voorstel is dan ook om dit stapsgewijs aan te pakken en relaties naar zaakobjecten te modelleren wanneer er een eerste zaaktype wordt vastgesteld.
- Vanuit het primair proces worden business services aangeroepen die leiden tot statuswijzigingen van de zaak (mijlpalen). De zaak kent hierbij een 'hoger aggregatieniveau' dan het proces of individuele systemen (zoals een aanvraag).
- De mijlpalen zijn communiceerbaar naar de buitenwereld (eventueel ook de burger, indien zaaktype voor hem/haar relevant).
- De mogelijkheid bestaat om functionaliteit omtrent workflow, kwaliteitscriteria, operationele en tactische managementinformatie voor uitgevende instanties te ontwerpen vanuit het concept zaakgericht werken.

Logging
In de kernregistratie en procesapplicaties dient logging uniform te worden ondersteund en ingeregeld. In het model zijn op dit moment een aantal vormen van logging opgenomen, al zijn er ook nog keuzes te maken gedurende het verloop van het programma. Doel is om een basis te leggen waarin er langzaam gegroeid kan worden richting Business Activity Monitoring, waarbij snel inzichtelijk gemaakt wordt hoe de primaire processen lopen.

- Een objecttype logbestand kan worden beschouwd als de primaire vorm van functionele logging t.a.v. de aanroep van (informatie)services (die 'raadpleeg' danwel Create/Update/Delete acties tot gevolg kunnen hebben). Elk 'event' wordt zodoende gelogd met een verwijzing naar de betreffende gestandaardiseerde informatieservice en andere gegevens zoals een berichtresultaatcode.

Additionele onderwerpen en uitbreidingen
Naast bovenstaande domeinen behoeven een aantal andere zaken verduidelijking:

- Waar mogelijk wordt gewerkt met stam/referentietabellen die verwijzen naar externe bronnen. Zo lijkt het zinvol en opportuun om gebruik te maken van de Landelijke tabellen (BRP) voor ´land´, ´gemeente´, ´nationaliteit´ en ´adellijke titel/predicaat´.
- Voor de registratie van (een verwijzing naar) documenten worden verschillende opties overwogen.
- Statusregistratie maakt integraal onderdeel uit van de kernregistratie en is toekomstbestendig opgezet door te werken met (uitbreidbare) statustypen. Dit met betrekking tot aanvragen, zaken, signaleringen en reisdocumenten).

- Voorrraadbeheer en nooddocumenten registratie is door een adequate opzet van registratie van documenten impliciet op orde gebracht. Door een beroep te doen op de beschikbare gegevens kan de totale actuele voorraad van een instantie worden bepaald en eventueel middels regels worden beoordeeld of er bijvoorbeeld een nieuwe zending benodigd is.

4.2.4 Beleidslijnen, richtlijnen, standaarden

Met betrekking tot de informatiearchitectuur is een aantal generieke richtlijnen te formuleren, die van toepassing zijn op alle in het programma beoogde activiteiten.

- Digitaal blijft digitaal.
- Analoog wordt waar mogelijk digitaal.
- Breng de gebruiker naar de informatie en niet de informatie naar de gebruiker. Dit is een afgeleide van eenmalige opslag, meervoudig gebruik.
- Privacygevoelige gegevens worden waar mogelijk niet (direct) gekoppeld aan een persoon vastgelegd. Herleidbaarheid dient waar nodig te worden voorkomen.
- De systemen in het reisdocumentenstelsel communiceren met elkaar via goed gedefinieerde, uniforme en gestandaardiseerde services/interfaces.
- Na personalisatie geen aanpassingen van de personalisatie- en aanvraaggegevens.
- Kernregistratie wordt bevraagbaar. Er worden geen gegevens meer gekopieerd/geleverd. Als bron moet er voor gezorgd worden dat gegevens niet meer worden rondgepompt maar bij de bron worden opgevraagd.
- Het informatiemodel zal binnen het programma model staan voor de totstandkoming van een volwaardig canoniek datamodel, wat als leidraad zal worden gebruikt voor het ontwerp en totstandkoming van informatieservices. Zo verkleinen we de afhankelijk van afzonderlijke componenten en bewerkstelligen we een 'loosely coupled' stelsel.
- Het informatiemodel, de verdere uitwerking in een canoniek datamodel, eventuele datamodellen ten behoeve van specifieke applicatiecomponenten en het ontwerp/standaardisatie van berichtuitwisselingen (berichtspecificaties) zullen zo veel mogelijk worden gebaseerd op reeds beschikbare standaarden (zoals het logisch ontwerp GBA en het Referentiemodel Stelsel van Gemeentelijke Basisgegevens (RSGB). De RSGB biedt gemeenten en hun leveranciers houvast bij het invoeren en het gebruiken van deze gegevens. Dit objectenmodel voor de gemeentelijke basisgegevens presenteert de samenhang tussen basisregistraties op een logische wijze.
- De historie van een object en/of subject moet inzichtelijk gemaakt kunnen worden.
- De gegevens bevatten elementen die voldoende basis bieden om op te sturen, analyseren en verantwoorden.
- Een informatieservice deelt nooit de gegevens met andere informatieservices. Alle gegevens die moeten worden gedeeld verlopen via de informatie service(s) die ze inpakt en autoriseert als zijn het reisdocument gegevens. Denk aan bijvoorbeeld identiteitsgegevens (vanuit de persoonsregistraties).

- Het publiceren van gegevensbestanden in de vorm van begrippenlijsten, digitale woordenboeken en taxonomieën door overheidsorganisaties gebeurt vaak in de vorm van documenten die niet bruikbaar zijn voor computerprogramma's. Daarom zijn er nu standaarden om deze wel toegankelijk te maken en zijn beschreven op de pas-toe-of-leg-uit lijst van het platform Standaardisatie. De voor RvIG relevantie standaarden zijn dat voor de gegevensset zal SKOS[9] worden toegepast. Bij de metadata beschrijving zal DCAT[10] worden gehanteerd.

Met betrekking tot het verstrekken van gegevens uit de kernregistratie gelden de volgende overwegingen:

- Taken en werkzaamheden van de stakeholders (de doelbinding)
- Gegevensverstrekking op basis van wat toegestaan is en binnen een juiste context van gebruik/grondslag. Daarin kan het gaan om persoonsgegevens, vertrouwelijke bedrijfsinformatie of overige (openbare) gegevens (vb. geaggregeerde informatie). Maar ook of het om incidentele verstrekking of structurele verstrekking gaan en dan nog het verschil tussen actieve verstrekking ((kunnen) worden verstrekt, uit eigen beweging verstrekt) of passieve verstrekking (op verzoek)
- Welke aanvullende voorwaarden stellen wij als RvIG zijnde? Bijvoorbeeld (technische) aansluitvoorwaarden, inzicht in uiteindelijke afnemer (bij koepelpartijen) etc.

  Bevragingen vinden rechtstreeks op de originele en operationele kernregistratie plaats. We gaan geen bevragingsregisters creëren doordat we verwachten een lage load te hebben en technisch voldoende schaalbaar zijn.

De concrete invulling zal in het wetstraject voor de paspoortwet in samenwerking met CZW en beleid worden vastgelegd.

I2-BEH-01 Akkoord	**Bevraging bij de bron**
Statement	Gegevens worden bevraagd bij de bron.
Rationale	Indien gegevens bij de bron worden bevraagd, is het niet meer nodig (dagelijkse) kopieën (afslagen) te maken. Dit scheelt tijd en geld, en de kans op het raadplegen van verouderde gegevens is hierdoor ook lager.
Implicaties	▪ Ontsluiting van gegevens aan de hand van services. ▪ Een uitzondering hierop zijn systemen die brongegevens geaggregeerd of in een ander formaat opslaan, zoals bijvoorbeeld een data warehouse, of een gepseudonimiseerde afslag. ▪ Een tweede uitzondering zijn systemen waarbij rechtstreekse bevraging niet mogelijk is omdat anders niet voldaan kan worden aan prestatie-eisen of beveiligingseisen.

[9] *SKOS: SKOS (Simple Knowledge Organization System) is een algemeen datamodel om kennissystemen (Knowledge Organization Systems) intern als een thesaurus te organiseren en extern onderling op definities van concepten te kunnen vergelijken.*

[10] *DCAT: Om datasets overzichtelijk te kunnen presenteren en om gericht naar datasets te kunnen zoeken, worden datasets in data.overheid.nl beschreven met metadata. Het W3C heeft hiervoor DCAT ontwikkeld, een metadata standaard voor de beschrijving van datasets. Zie ook https://data.overheid.nl/ondersteuning/open-data/dcat*

Kwaliteits-kenmerken	▪ Adequate functionaliteiten en services die bovenstaande mogelijk maken.

5 Technische architectuur

In dit hoofdstuk wordt high level vastgelegd wat het programma verandert op het gebied van de technische architectuur.

Binnen het Reisdocumenten Stelsel worden er veel technische diensten geleverd. Een totaaloverzicht van de huidige en door het programma te realiseren ICT voorzieningen voor de bedrijfsservices, de applicaties met haar informatieservices en onderliggende infrastructuur is in de bijlage "Overzicht componenten Reisdocumenten" te vinden.

Doel in de technische architectuur is om een gedistribueerd systeem op te zetten waarbij er centraal gelezen en geschreven kan worden. Er wordt wel een verschil gemaakt tussen de lezen en schrijven services aangezien het gros lezen functies zijn die je overal kunt laten uitvoeren om de beschikbaarheid ervan te vergroten. Voor de services wordt er gebruik gemaakt van de in de markt gebruikte cloud diensten. Cloud dienstverlening [11]is op zich geen nieuwe technologie maar is eerder een nieuwe manier om bestaande technologieën te combineren en te gebruiken. De gekozen technische architectuur dient weer voor minimaal 10 jaar mee te gaan en daarom wordt er volledig ingezet op deze marktstandaard en niet voor de traditionele dienstverleningsmodellen.

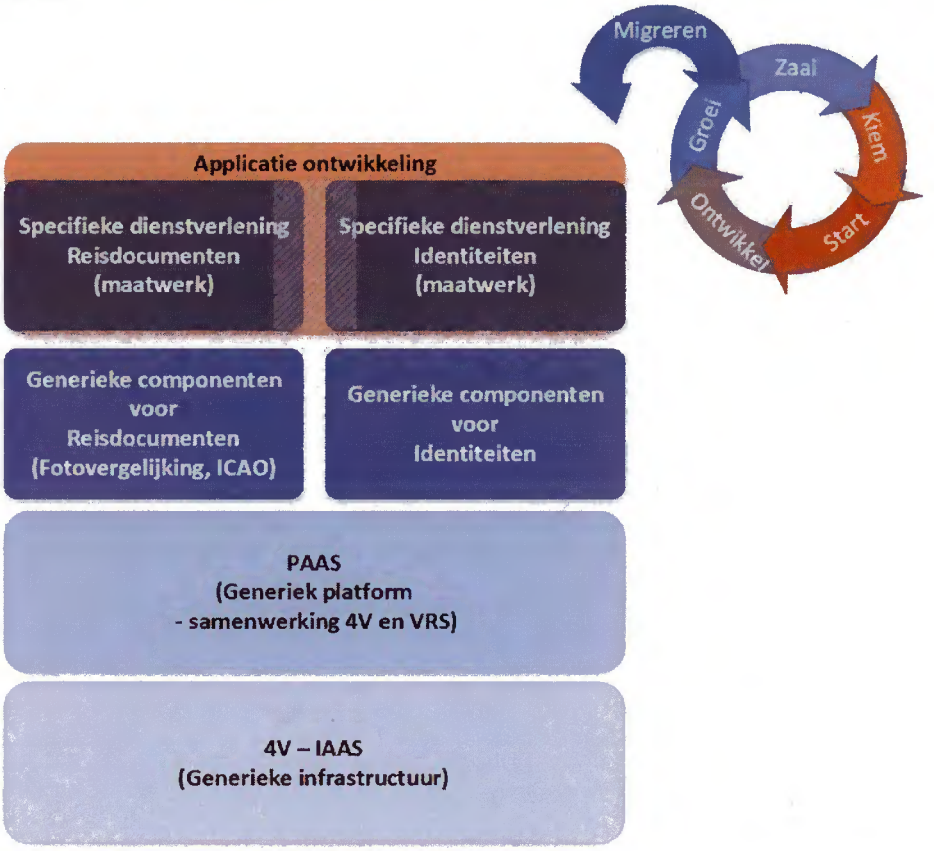
Binnen een cloud dienstverleningsmodel worden tenminste drie lagen onderscheiden: IaaS, PaaS en SaaS.
In het IaaS model worden infrastructuur IT-middelen – zoals rekenkracht, opslag en netwerken – in een gevirtualiseerde omgeving (virtuele machines) als dienst aan de klant aangeboden.
Bij PaaS is de aangeboden dienst een software ontwikkelingsplatform dat ondersteuning biedt voor bepaalde programmeertalen, bibliotheken, tools en diensten en dat gericht is op een bepaald type applicatie (zoals webapplicaties, business applicaties, etc.). PaaS is de laag voor de software ontwikkelaar. Je kunt in de PaaS laag niet meer kiezen voor de programmeertaal of de database. Deze wordt als het ware opgelegd door de PaaS leverancier.
SaaS is software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker, eventueel in combinatie met andere parameters. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer, de gebruiker benadert de software over het internet of privé netwerk bij de SaaS leverancier. Binnen SaaS zul je de applicatie moeten delen met andere bedrijven. Als je die niet wenst, kun je afdalen in de laagstructuur en kiezen voor PaaS. Maar dan moet je dus zelf gaan ontwikkelen.

---

[11] *Cloud dienstverlening is een informatietechnologie (IT) dienstverleningsmodel waarin over het netwerk beschikbare IT-middelen – zoals netwerken, servers, opslagcapaciteit, software, ontwikkelingsplatformen en diensten – via een cloud op aanvraag en dynamisch zeer snel kunnen worden aangeleverd of vrijgegeven en dit met een minimale inspanning van zowel de klant als de dienstverlener. Bovendien betaalt de klant enkel voor de verbruikte IT-middelen zonder een voorafgaande verbintenis of investering. Het verbruik wordt hierbij door de dienstverlener gemeten in een overeengekomen meeteenheid (uren, megabyte, CPU cyclussen. . .).*

Een cloud is een parallel en gedistribueerd systeem waarin via virtualisatie technieken met elkaar verbonden IT-middelen gedeeld worden. Hierdoor is de benutting van deze IT-middelen veel hoger en lijkt de beschikbare hoeveelheid oneindig. (van https://tom.desair.me/blog/2012/10/wat-is-cloud-computing/)

Een andere wijze om met deze beperkingen om te gaan is om te kiezen voor een private cloud of on-premise oplossing in tegenstelling tot de publieke cloud.



Het eerder gestarte project 4V is verantwoordelijk voor de migratie van de identiteiten systemen naar deze cloud dienstverlening. Het programma VRS borduurt voort op dit model. Echter is er in het kader van Reisdocumenten wel aanvullende dienstverlening nodig. Deze is in de paragrafen hieronder beschreven.

5.1 De techniek van het boekje/ID kaart

5.1.1 Afbakening

Aan de techniek (architectuur multisource chip) en wijze van personaliseren zal in het programma niets worden aangepast en is daarmee buiten scope.

5.2 Fysieke apparatuur

5.2.1 Afbakening

Uiterlijk voor het eind van 2024 wordt door het project 'aanvraag, uitgifte en statusbeheer' gezorgd dat de RAAS infrastructuur kan worden uitgefaseerd. Voor de Mobiele Vingerafdruk Apparatuur (MVA) als ook het Aanvraagstation komen nog aanvullende specificaties zodat deze decentrale apparatuur kan blijven functioneren binnen de gecentraliseerde architectuur van VRS.

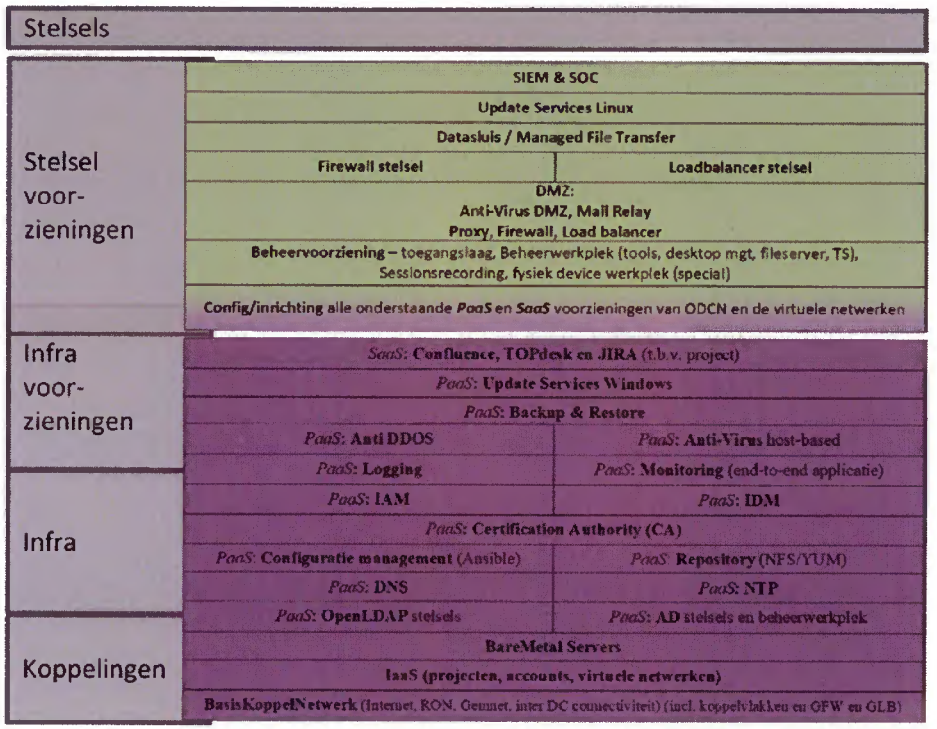
5.2.2 *Beleidslijnen, richtlijnen, standaarden*

Richtlijn is om voor hardware gebruik te maken van de bestaande hardwareleveranciers. Daarnaast is het van belang op basis van (internationale) standaarden voor berichtuitwisseling te werken zodat er meer leveranciersonafhankelijk kan worden gewerkt.

5.3 Platform

5.3.1 *Afbakening*

De platform en services die onder de stelselapplicaties en gerelateerde tooling liggen om die de stelselapplicaties te ontsluiten naar de buitenwereld zijn vanuit 4V:



Dit platform is een schaalbaar, cloudgebaseerd applicatieplatform met een aantal herbruikbare, generieke componenten met ondersteuning voor automatisch testen en uitrollen van koppelingen, applicaties en releases (een ontwikkelstraat). Hier bovenop levert 4V ook een centrale beheerwerkplek zoals gedefinieerd in hoofdstuk 7. Van de specifieke services die VRS nodig heeft zal de doelarchitectuur steeds worden afgestemd met 4V om de componenten als referentie bouwblok aan RvIG over te dragen. Voor de VRS specifieke services (hieronder beschreven) zal in het deelproject Sourcing de sourcingstrategie worden bepaald om de inkooptrajecten te starten voor een tijdige levering van de gewenste services.

Belangrijkste kenmerken voor het ontwerpen van nieuwe diensten zijn:

- Overal beschikbaar
- Altijd beschikbaar
- Schaalbaar
- Verregaand geautomatiseerd
- Gecontroleerd

- Browser gebaseerd
- Selfservice
- On demand (elastisch)
- Afrekening op basis van gebruik

Om nieuwe functionaliteit conform een Microservices architectuur (te laten) ontwikkelen door meerdere ontwikkelpartners dienen de volgende PaaS voorzieningen aanvullend door VRS te worden gerealiseerd:

- Een dienstenbus ofwel een integration Platform as a service met daarin:
  - API management
  - Een daarbij horende data integration adaptor
  - Enterprise Service Bus (ESB) voor legacy ondersteuning zoals WUS/ebMS
- Een voortbrengingsproces inclusief OTAP straat waarin continuous integration en continuous delivery (CI/CD) de best practice is.
- Een generieke portaalfunctie waarmee de verschillende processen (aanvraag-/uitgifteproces of signaleringenbeheer) gefaciliteerd worden.
- Afhankelijk van de functionele requirements: een zaakmanagement systeem of een Business Process Management systeem
- Een document management systeem / Enterprise content management systeem
- Biometrievergelijking service (in eerste instantie fotovergelijking ten behoeve van een correcte identiteitsverificatie) en indien noodzakelijk beiden.

In het kader van de dienstenbus zijn er een aantal afspraken noodzakelijk voor de standaardisatie van het informatie uitwisselingsprotocol:

- **Webservices (Soap/XML)**
  Worden gebruikt in de backend voor elementaire/basis acties op data (retrieve, update, delete)
  Worden gebruikt binnen (asynchrone) processen en voor interactieve communicatie
  Kunnen toekomstig worden gebruikt voor communicatie met ketenpartners

- **REST services (Rest/JSON en eventueel Rest/XML)**
  Worden gebruikt voor de frontend oplossingen om gegevens uit de backend beschikbaar / toegankelijk te maken
  Zorgt voor de security van de services.
  Kunnen toekomstig worden gebruikt voor communicatie met ketenpartners
  Kunnen toekomstig worden gebruikt ter vervanging / als aanvulling op webservices

- **Messaging Services (JMS / ebXML)**
  Worden gebruikt voor asynchrone communicatie waarbij geen directe response noodzakelijk is.
  Kenmerk: Reliable Messaging.
  In de praktijk wordt dit gebruikt voor het aanleveren van informatie en het verstrekken van informatie van/aan een ketenpartner

Het Identiteiten stelsel kent al halfjaarlijkse releases. Bij Reisdocumenten ligt dat voor de frontend (AS/RAAS) vaak ook halfjaarlijks echter bij de backend

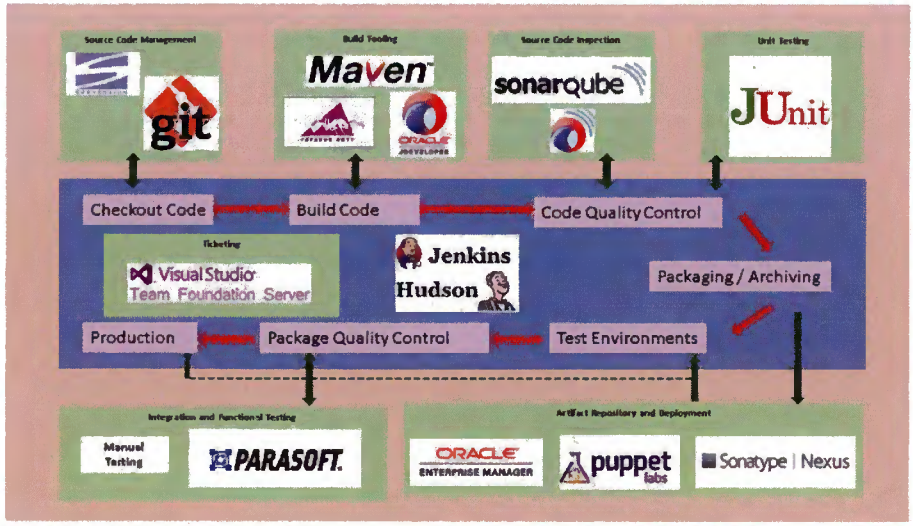
zijn doorlooptijden van meer dan 1 ½ jaar geen uitzondering. Een ontwikkelstraat waarin CI/CD de best practice is, is de marktoplossing om te komen tot snellere oplevermomenten.
De principes hierop van toepassing zijn:

- Iedere handeling die vaker dan eenmalig wordt uitgevoerd wordt gescript (het automatiseren van de automatisering).
- Iedere vorm van digitale voorziening dient softwarematig (via een API) te kunnen worden aangeroepen.
- Voor testen wordt geconformeerd aan de concept visie testinfrastructuur gehanteerd. Deze zal eerst worden bijgewerkt volgens de laatste ontwikkelingen bij 4V en de eisen bij VRS. Belangrijkste punten daaruit zijn:
  - Reduceren van complexiteit: Het aantal en soort elementen, de mate van diversiteit van de elementen, het aantal en soort (onderlinge en externe) relaties en de mate van adaptief vermogen;
  - Differentiëren in producten (BS, Reisdocumenten, PIVA, RNI, GBA, et cetera), toegepaste testsoorten (UT, UIT, ST, SIT, ART, AT, SEC, FAT, GAT, PEN, et cetera), type testobject (Maatwerk, COTS of Infrastructuur) en verschillende releasemomenten;
  - Begin klein met één running version zonder branches. Bij een opzet van bijvoorbeeld meerdere teams is een feature branch mogelijk;
  - Geanonimiseerde/gepseudonimiseerde (keten)testdata dient beschikbaar te zijn;
- Houdt alles onder versie controle
- Automatiseer de 'build'
- Voer een unit test uit in the 'build'
- 'Commit' wijzigingen in de code vroeg en vaak
- Build iedere wijziging
- Los build errors direct op
- Hou de build snel
- Test in een kloon van de productie omgeving
- Maak het gemakkelijk om de build resultaten te verkrijgen
- Zorg ervoor dat het bouwproces voor iedereen transparant is
- Automatiseer de deployment

Dit alles om 3 essentiële doelen te behalen:

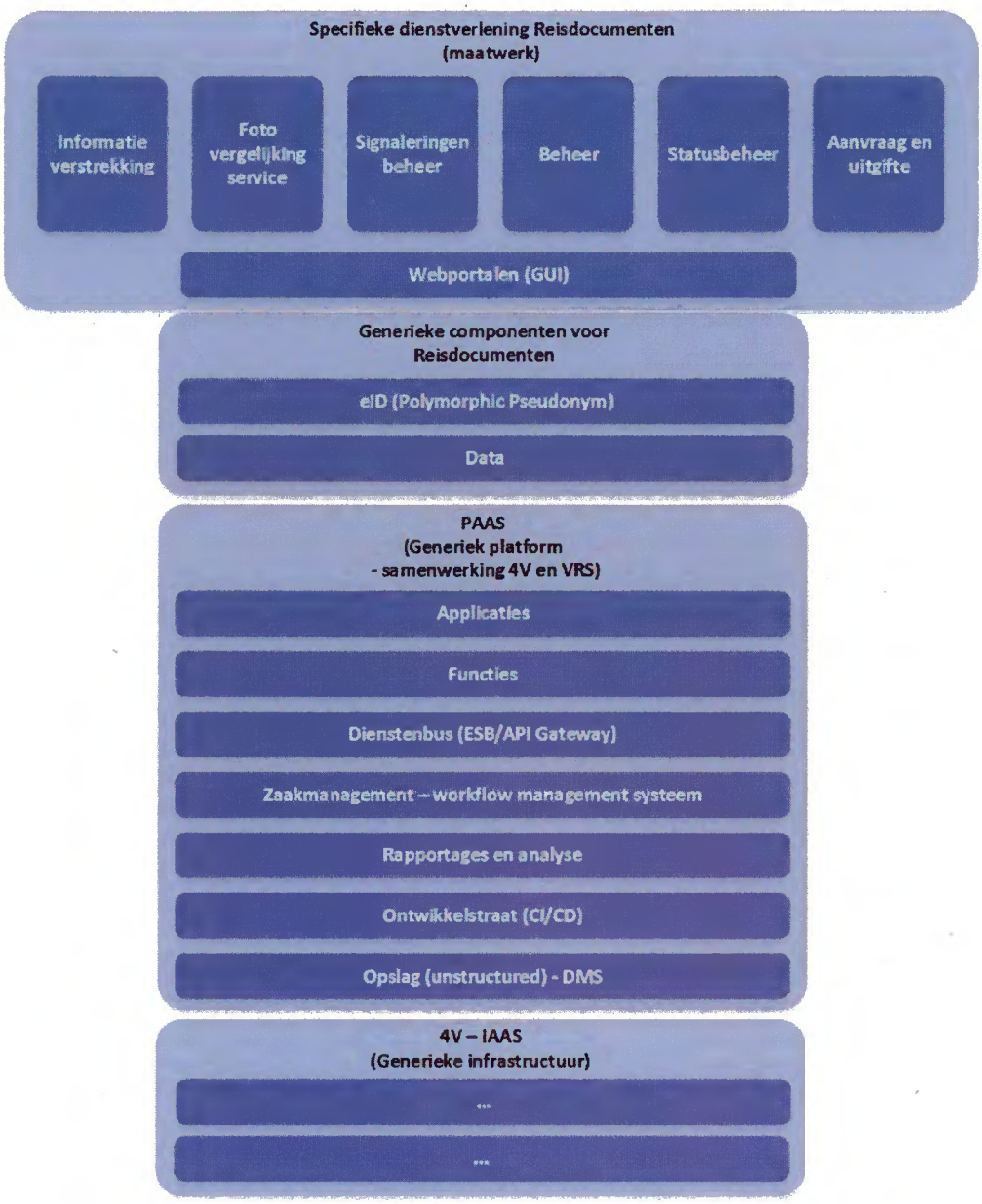
1. Segregatie voor verantwoordelijkheid van belanghebbenden;
2. Risicovermindering
3. Korte feedbacklus

Een voorbeeld van deze ontwikkelstraat kan zijn:



Binnen 4V zijn er stelseldiensten waaronder database opslag (PostgreSQL). Die database oplossing is voor traditionele relationele gegevensopslag. Bij een gang naar een cloud architectuur wordt er door ontwikkelaars steeds vaker gekozen voor een NoSQL database. Deze oplossingen zijn beter schaalbaar en hierbij hoeven de gegevens niet (of anders) genormaliseerd worden opgeslagen. Een NoSQL-database kan veel verschillende datatypen (gestructureerde gegevens, documenten, afbeeldingen, etc) tegelijk bevatten, is hiermee flexibel en kan eenvoudig worden opgeschaald. En ook bij grote hoeveelheden data en veel dataverkeer, blijft de database snel reageren. Dit maakt NoSQL bijzonder geschikt voor werken in de cloud omgevingen en voor agile werkomgevingen met veel wijzigingen. Voor de toekomst met bijvoorbeeld vID, waarin er vanuit de inspectie service veel en grillig dataverkeer zal ontstaan, zien we de behoefte aan het migreren naar een NoSQL database oplossing of in ieder geval een hybride omgeving met SQL en NoSQL databases. Echter vereist dit specifieke kennis van ontwikkelaars en analisten. NoSQL is ook minder geschikt voor toepassingen waar relaties tussen dataverzameling worden gelegd zoals in de huidige situatie. Dit is de reden om binnen VRS nochtans alleen gebruik te maken van SQL databases zoals door 4V geleverd. De beschrijving voor de ontwerpkeuze is opgenomen in de PSA zodat er meer kaderstelling is voor de ontwikkelaars en deze niet geheel vrij te laten in de wijze van ontwikkeling.

Voor VRS voorzien we de hier onderstaande PaaS diensten met daarbovenop de in maatwerk ontwikkelde applicaties en webportalen.



5.3.2 *Aansluiten op de Nederlandse API strategie*

In maart 2019 zijn de Nederlandse inrichtingsprofielen voor de Nederlandse API strategie in consultatie gesteld vanuit het Platform Standaardisatie om daarna op de pas-toe-leg-uit lijst te komen. RvIG neemt die kennis al ter harte en conformeert zich aan deze standaard.
In een digitaal stelsel met 500+ deelnemers is consistentie en uniformiteit noodzakelijk. Door aan te sluiten op de Nederlandse API strategie worden diensten snel en eenvoudig bruikbaar.
De Nederlandse API strategie heeft als doel een eenduidig profiel op te stellen van uitgangspunten voor ontwikkelaars als zij API's programmeren.

Deze API strategie dient echter aangevuld te worden met uitgangspunten om privacy gevoelige gegevens ook te kunnen uitwisselen middels API's. Deze komen in de huidige, in consultatie zijnde, API strategie, nauwelijks voor. In de bijlagen is de gedetailleerde beschrijving van API strategie c.q. uitgangspunten en aanvullingen beschreven.

De NL API strategie is voortgekomen uit een vertaling van documenten die door het programma DSO zijn vastgesteld. Deze zijn te vinden onder

https://aandeslagmetdeomgevingswet.nl/digitaal-stelsel/technisch-aansluiten/standaarden/api-uri-strategie/

Om te kunnen controleren of er wordt voldaan aan de NL API strategie hebben we de uitgangspunten (inclusief aanvullingen) als een checklist opgezet.

De waarden die zijn doorgehaald zijn specifiek voor het GEO domein en niet van toepassing binnen het Reisdocumenten stelsel.

ChecklistAPIStrategie.xlsx

5.3.3 Aansluiten op de Nederlandse URI strategie

Naast een API strategie is er ook een bijhorende URI strategie gedefinieerd. URI's bieden een mechanisme om naar informatie objecten te verwijzen, waar deze zich ook bevinden. Met de URI-strategie wordt alle informatie van digitaal stelsel op een uniforme en samenhangende manier vindbaar en toegankelijk. De URI-strategie schept duidelijkheid hoe URI's opgebouwd moeten worden. Expliciet wordt vermeld dat de URI strategie geen onderdeel uitmaakt van de Nederlandse API strategie. Net zoals bij de API strategie is consistentie en uniformiteit wel noodzakelijk. Daarom is gekozen aan te sluiten bij de kennis en ontwikkeling van de URI strategie bij de Digitale Stelsel Omgevingswet. Middels een URI strategie zorgen we ervoor dat informatie uniform, samenhangend en duurzaam toegankelijk wordt. In de bijlagen is de gedetailleerde beschrijving van URI strategie c.q. uitgangspunten beschreven.

ChecklistURIStrategie.xlsx

Vanuit de privacy by design regels is er een aanvulling gedaan op deze lijst van criteria.

URI-40: Vermijdt URL's die gehackt kunnen worden. Ontwikkelaars hebben baat bij gestructureerde URI's. Echter zitten er in het informatiemodel van het reisdocumenten stelsel veel PII - Persoonlijk identificeerbare informatie. Bij veel van de op open data gerichte URI strategieën zie je in de URI strategie duidelijke patronen terug waarop je gegevens kunt herleiden. Dat is bij privacy gevoelige gegevens niet wenselijk. In sommige gevallen kan worden volstaan met het toepassen van UUID's zodat directe afleiding niet mogelijk is. Echter in de meeste gevallen ligt de oplossing in het geheel obfusceren van de URL's en JSON schema's. De wijziging is dan van bijvoorbeeld http://foo.ploeh.dk/customers/1234/orders naar http://foo.ploeh.dk/DC884298C70C41798ABE9052DC69CAEE te gaan. Dit houdt wel in dat de API een soort tweeweg lookup tabel moet bevatten zodat er een juiste mapping kan plaatsvinden. Vanuit performance redenen is het verstandig niet op alle API's dit toe te passen.

5.3.4 *Beleidslijnen, richtlijnen, standaarden*

- De in het MT en door ADM bekrachtigde principes van het project 4V waaronder:
  - Het infrastructuurlandschap is ingericht als collectie van infrastructuurdiensten.
  - Het infrastructuurlandschap ondersteunt zowel de RvIG beheerders als de beheerders van de leveranciers bij het uitvoeren en optimaliseren van hun werkzaamheden.
  - Het infrastructuurlandschap ondersteunt afnemers bij het bieden van een betrouwbare dienstverlening.
  - Uitwisseling van informatie vindt op een eenduidige en uniforme wijze plaats.
- Om applicaties op een cloud-platform te kunnen laten integreren zijn de volgende randvoorwaarden in te vullen:
  - De business services zijn losgekoppeld van de applicatie waardoor functies niet meer vast gecodeerd liggen in de gebruikersinterface, dienstenbus of gegevensset (loosely coupled)
  - Applicaties moeten stateless zijn, oftewel geen sessie informatie opslaan binnen de applicatie
  - Applicatie logging en audit logging worden alleen centraal opgeslagen (richting een centrale log aggregator)
  - Combineer applicatie communicatie zodat applicaties efficiënt met elkaar communiceren.
  - Applicaties worden gebouwd middels het security by design en privacy-by-design principe.
- Conformeer aan de pas-toe-of-leg-uit lijst van het Forum Standaardisatie.

TC-FUN-01 **Akkoord**	**Beperk technische diversiteit**
Statement	Voorkom niet triviale kosten zoveel mogelijk, door middel van de technische diversiteit binnen de organisatie te beperken.
Rationale	De noodzakelijke kosten om alternatieve technologieën operationeel te houden zijn aanzienlijk. Het limiteren van het aantal ondersteunde componenten werkt kostenbesparing en onderhoudbaarheid in de hand.
Implicaties	▪ Nieuwe diensten en applicaties dienen vooraf getoetst te worden aan de standaarden door RvIG gebruikt. ▪ De keuzevrijheid van technologieën wordt beperkt door de huidige technologische blueprint van RvIG. ▪ De technologische baseline is echter geen bevroren toestand. Indien nieuwe technologieën voordelen opleveren in operationele efficiency zijn deze uiteraard welkom. ▪ Bij vervanging van defecte of afgeschreven componenten wordt de huidige standaard geïmplementeerd. ▪ Voor alle infrastructuur functionaliteiten worden, waar mogelijk, standaard ICT-componenten geselecteerd. ▪ Componenten bieden zo min mogelijk functionaliteit die overlappend is met andere componenten. ▪ Componenten worden organisatiebreed hergebruikt. ▪ Netwerkcomponenten, Server- en Werkplekapparatuur zijn gestandaardiseerd op een minimaal aantal platformen en varianten.
Kwaliteits-kenmerken	▪ Uitwisselbaarheid, Onderhoudbaarheid

TC-BEH-01 Akkoord	Infrastructuur is een nutsvoorziening
Statement	Het applicatielandschap dient op eenduidige wijze gebruik te maken van generiek beschikbaar gestelde infrastructurele voorzieningen.
Rationale	Werkt rationalisatie in de hand.
Implicaties	▪ In de architectuur komen veel verschillende functionaliteiten voor m.b.t. authenticatie, foutlogging, loadbalancing, failover, etc. Deze functionaliteiten zijn veelal voor ieder systeem noodzakelijk. ▪ Deze functies moeten generiek beschikbaar worden gesteld in de infrastructuur t.b.v. applicaties. Applicaties maken hierbij gebruik van deze functionaliteit zonder deze zelf te realiseren ▪ Een voorbeeld hiervan is de opslag van gebruikersgegevens t.b.v. toegangsbeheer of het beheer van de certificaten voor toegangsbeheer. Dergelijke voorzieningen kennen een generiek karakter en kunnen generiek in de infrastructuur worden gerealiseerd. Functionele groepering van voorzieningen zoals bijvoorbeeld het combineren van gegevens of gegevensopslag vindt alleen plaats als hier nut en noodzaak is tot het combineren. Deze richtlijnen hebben met name betrekking op de diensten rondom de primaire applicatiefunctie.

5.4 Netwerk

5.4.1 Afbakening

Middels de netwerkvoorzieningen is het mogelijk de RvIG stelselapplicaties de benodigde interne communicatiemogelijkheden te verschaffen, maar ook deze de communicatiepaden te geven, zodanig dat partijen buiten RvIG de stelselapplicaties kunnen bereiken (via de overheidsnetwerken, niet rechtstreeks via het Internet). Ook is het mogelijk via de netwerkvoorzieningen externe leveranciers aan het RvIG infrastructuurlandschap te koppelen.

Pas in de fase na het programma VRS zullen rechtstreekste aanvragen van de burger mogelijk worden en zal een internetontsluiting onontbeerlijk zijn.

Aangezien er bij de verschillende uitgevende instanties een groot verschil in netwerktopologie is zal deze bij de projectstart architectuur van de business projecten worden beschreven. Op voorhand weten we al wel dat bij het Caribische deel van het Koninkrijk der Nederlanden geen stabiele netwerkverbindingen liggen en er beperkte capaciteit is. Bij de KMar is er met name het defensienetwerk beschikbaar met hogere beveiligingseisen. Er zal bij het project platform en services voor dit brede scala aan netwerkvoorzieningen passende oplossingen worden gerealiseerd om toch gecentraliseerde portalen te kunnen benaderen met de juiste beschikbaarheid. Uitgangspunt is wel dat dit netwerken zijn die binnen de GDI gebruikelijk zijn (waaronder Diginetwerk en RON2.0).

De PGK koppeling is er ook nog (Piva GBA koppeling) die ook al een deel van de gaten wegneemt. Die is er alleen niet voor de eilanden Aruba, Curaçao en St-Maarten wel voor de bijzondere gemeenten: de eilanden Bonaire, Sint Eustatius en Saba.

5.4.2 Beleidslijnen, richtlijnen, standaarden

		Kanalen

T3	AP9	De dienst kan via internet worden aangevraagd.
T3	AP10	De dienst kan, behalve via internet, via minimaal één ander kanaal voor persoonlijk contact worden aangevraagd.
T3	AP11	Het resultaat van de dienst is gelijkwaardig, ongeacht het kanaal waarlangs de dienst wordt aangevraagd of geleverd.

TN-BEV-01	**Centraal toegangspunt voor alle diensten**
Akkoord	
Statement	RvIG kent één generieke koppelvoorziening voor alle ingaande en uitgaande koppelingen.
Rationale	Door de diensten maar via één centraal koppelpunt te leveren is de beveiliging en de toetsing daarvan eenvoudig te realiseren en te handhaven.
Implicaties	▪ Netwerktechnisch en logisch moeten deze koppelingen op één generieke manier worden ingericht. ▪ Dit vergemakkelijkt beheer, vermindert de beheerkosten en vergroot de veiligheid en de functionaliteit. ▪ Bestaande en nieuwe ICT diensten dienen via een beveiligd netwerk ontsloten te worden. ▪ Onnodige complexiteit, onbeheersbaarheid en beveiligingsrisico's kunnen optreden, indien diensten niet via één centrale, goed beveiligde netwerk aangeboden worden. ▪ Voor dataverkeer tussen softwareapplicaties heeft RvIG één generieke koppelvoorziening met de buitenwereld. Via een vertrouwd deel worden de diensten aan externe partijen aangeboden. Afnemers kunnen aansluiten op het onbeveiligde deel daarvan of hierop koppelen via een andere partij. Alle verkeer van de RvIG diensten naar afnemers, verloopt langs een managed firewall naar het beveiligde deel. Diensten worden vervolgens benadert via een generieke loadbalancer constructie. Aansluiting op de klantenbus en/of overheid service bus vinden plaats via deze koppelvoorziening. Er zijn geen koppelingen met externe partijen/systemen buiten deze koppelvoorziening om. ▪ Webservice diensten zijn beschikbaar via Diginetwerk.

Andere uitgangspunten zijn:

- Gedeelde infrastructuur: alle ICT infrastructuur moet kunnen worden gedeeld met andere partijen voor een optimale utilisatie en effectief onderhoud.
- De kennis rondom alle tooling en ontwikkeling moet in de markt eenvoudig te verkrijgen zijn.

6 Informatiebeveiliging

6.1 Informatiebeveiliging

De belangrijkste richtinggevende en kaderstellende uitspraken op het gebied van informatiebeveiliging zijn:

1. Aanbieders van VRS systemen moeten conformeren aan de Baseline Informatiebeveiliging Rijksdiensten (BIR) en de aanvullende eisen van RvIG zoals beschreven in het IBB2018 (Informatiebeveiligingsbeleid 2018). We gaan over op het hanteren van de BIO (ter opvolging van de BIR) zodra dat opportuun is, zulks in afstemming met de CISO RvIG.

2. De beveiliging van de systemen zal op niveau DepV BBN2 worden ingericht. De beveiliging van de in het kader van VRS op te leveren systemen en registraties wordt zoveel mogelijk op een gelijke basis geschoeid.

3. Aangenomen wordt, hangende formele BIA's en risicoanalyses, dat er ten opzichte van het BBN2 niveau specifieke aanvullende maatregelen zijn te treffen op de volgende gebieden:
   - Centrale cloud-infrastructuur, zulks in lijn de beveiliging van 4V. Uitgangspunt daarbij is dat gevoelige persoonsgegevens zoals die in het reisdocumentenstelsel worden verwerkt, daarmee op deze infrastructuur verwerkt kunnen en mogen worden;
   - De biometrieketen, in het bijzonder de centrale opslag van gelaatsopnames, handtekeningen(en tijdelijk vingerafdrukken);
   - Specifieke beveiligingsmaatregelen voor de op enig moment in gebruik te nemen containerinfrastructuur;
   - Bewaking van het serviceplatform via een SIEM/SOC. Dit dient voldoende betrouwbaar te zijn om APT's van statelijke actoren te detecteren.

4. Hantering van een zero trust filosofie in de bouw van applicaties. Dit om de kans op compromittatie te minimaliseren. Concreet behelst dit:
   - Extreem doorgevoerde defence-in-depth. Het tegenovergestelde van het klassieke 'kasteel' model. Dit is mede in het logisch toegangsmodel vormgegeven;
   - Ontsluiting van data uitsluitend via een afgescheiden laag dataservices;
   - Applicatie-level firewalling en anomalie detectie om interactie met en tussen services te beperken op toegestane communicatiepatronen van de applicaties. (preventief danwel detectief);

   En op enig moment, zodra containertechnologie is geadopteerd:
   - Services zijn van elkaar te scheiden in containers;
   - Sterke 2-zijdige authenticatie van containers i.c. de services in die containers (Istio e.d.).

5. Toepassing van technische richtlijnen van NCSC en WASP. Dit betreft onder meer de toepassing van de ICT-Beveiligingsrichtlijnen voor

Webapplicaties: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

6. Security by design ontwikkeling volgens ISO/IEC TS 17961:2013 standaard.

7. Toepassing van evaluatiecriteria voor informatiebeveiliging. Bij onderhoud en vernieuwing van software in het kader van adaptief, preventief en correctief beheer is van belang dat informatiebeveiliging is geborgd.

8. Webrichtlijnen overheid: http://versie2.webrichtlijnen.nl

9. De ondersteuning van de systemen moet 24x7 zijn ivm de wereldlijke ondersteuning van onze ketenpartners. De eisen rondom de beschikbaarheid, onderhoudbaarheid en andere kwaliteitseisen worden in de projecten bepaald. Er wordt wel voortborduurd op de Non functional requirements zoals bepaald in het eID (CORI) traject.

Daarnaast geldt dat er voor de bouw een aantal aanvullende vuistregels wordt gehanteerd:

1. Authenticatie geschiedt middels een twee-factor authenticatieregel (voor de beheerders) en via attribute en/of role based authenticatie. IAM vindt binnen de applicaties plaats op basis van gecentraliseerd identity en access management. Eventueel kan dat een federatief systeem betreffen, dat samen kan werken met DigiD en eHerkenning.

2. Gebruikersnaam/wachtwoordcombinaties moeten zonder aanvullende maatregelen niet onversleuteld in configuratiebestanden of programmacode worden opgenomen. Hier zal de IAM service voor moeten worden geraadpleegd.

3. Log alle significante/belangrijke security events in een 'sabotage resistente' opslag. In het geval van VRS een centrale logserver.

4. Verander standaard security gevoelige parameters zoals bv default wachtwoorden, poorten en security rules.

5. Ga ervan uit dat een aanvaller uitstekend op de hoogte is van de omgeving, vertrouw niet op 'sleutel onder de mat principe' vroeg of laat wordt dit ontdekt opzettelijk dan wel per ongeluk.

6. Ontwikkel niet je eigen security technology maar gebruik bij voorkeur aanwezige 'proven technology'. Als er toch eigen kritische security technology wordt ontwikkeld, laat deze dan en detail beoordelen door een externe onafhankelijke en ter zake kundige partij.

7. Privacy gevoelige gegevens worden versleuteld bij data in transport en data at rest. Dit gebeurt wanneer de gegevens de systeemgrenzen van het fysieke afgeschermde ruimte verlaten en de disks waarop de persoonsgegevens opgeslagen zijn.

8. Hanteer uitsluitend de meest recente libraries (in ieder geval die libraries zonder bekende security issues) en waar dit niet mogelijk is,

houd bij waar er wordt achtergelopen. Bespreek hoe en wanneer dit wordt hersteld.

6.2 Logische toegangsbeveiliging

6.2.1 Definities

Hieronder de definitie van enkele in het kader van logische toegang veel gehanteerde termen en begrippen:

1. *Autorisatie* is het samenstel van activiteiten, waarmee de rechten op bepaalde functionaliteit en/of gegevens worden bepaald en geadministreerd. De geadministreerde rechten worden ook wel aangeduid als autorisaties.
2. *Authenticatie* is het in elektronisch verkeer aantonen en verifiëren van de identiteit van een actor.
3. *Access control* is de activiteit waarbij er, op basis van authenticatie en controle van de autorisaties, wel of geen toegang wordt verleend tot bepaalde functionaliteit en/of gegevens.
4. *Toegang* is het samenhangende mechanisme van authenticatie, autorisatie, access control en logging, waarmee geborgd wordt dat slechts die actoren toegang hebben tot functionaliteit / gegevens die daartoe gerechtigd zijn.
5. *Toegelaten applicatie*. Een applicatie in gebruik bij een ketenpartij welke als individuele applicatie of als type applicatie is toegelaten en daarmee toegang krijgt tot de voor deze applicatie benodigde API's.
6. *API*. Letterlijk een Application Programmer's Interface. De gepubliceerde en door ketenpartners te gebruiken informatieservices, voorzien van de passende beveiliging en beheer. Functioneel komt een API overeen met een een informatieservice.
7. *Functie*. Een stuk functionaliteit dat een duidelijk afgebakende (deel)taak vervult, een goed te onderkennen deel van een applicatie

6.2.2 Lagen in de toegangsbeveiliging

De toegangsbeveiliging is in een aantal lagen georganiseerd. Dit betreft in de uitgangssituatie in ieder geval:

- Toegang van interactieve gebruikers tot applicaties en de specifieke functies in die applicaties;
- Toegang van applicaties tot de benodigde API's die RvIG openstelt;
- Toegang van API's tot onderliggende kritische resources, met name data.

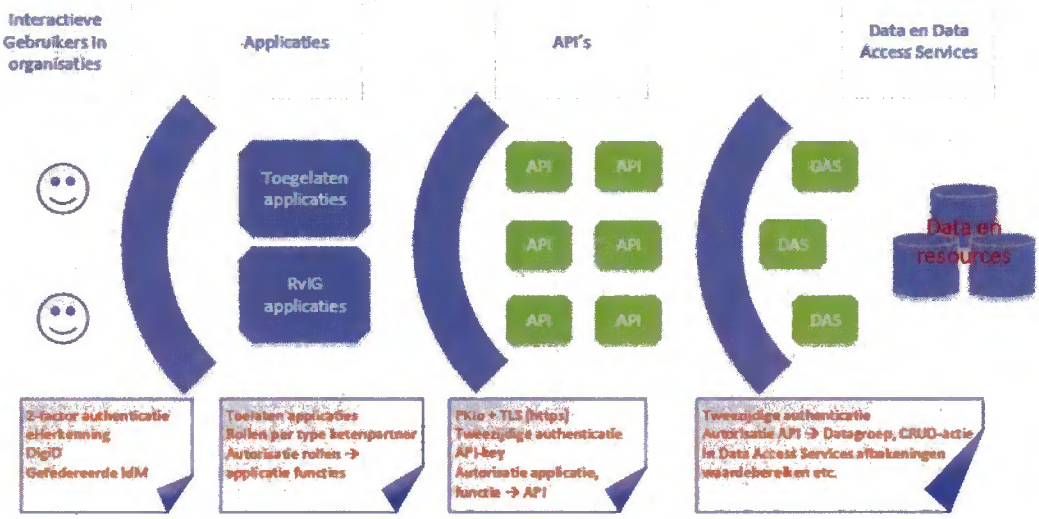
NB Het is denkbaar dat er in een later stadium nog een tussenliggende toegangslaag wordt gecreëerd, waarbij toegang verleend wordt tot meer samenhangende combinaties van *resources* (data in combinatie met elementaire bewerkingen en functionaliteit).

Voor samenhang tussen deze lagen geldt steeds dat:

- Op een bepaalde toegangsschil zijn ook de toegangsgegevens van de daarbuiten liggende toegangsschil(len) beschikbaar. Identiteit en rol van interactieve gebruiker, de organisatie van de eindgebruiker, de organisatie van de applicatie, de identiteit van de applicatie zijn bijvoorbeeld beschikbaar binnen de API's. Op de toegangsschil tot kritische resources / data is bovendien ook bekend welke API toegang vraagt en eventueel via welke tussenliggende informatieservices.

- Er vindt logging / vastlegging plaats van alle service aanroepen en antwoorden, waarbij genoemde toegangsgegevens worden gelogd, naast de relevante applicatieve gegevens.
- Op elk van de lagen vindt authenticatie, autorisatie, operationele aceess control en logging plaats.

Dit model is als volgt weer te geven:



6.2.3 *Toegang van interactieve gebruikers tot applicaties*

De volgende richtinggevende uitspraken zijn van toepassing:

1. Eindgebruikers zijn natuurlijke personen die gebruik maken van die *toegelaten applicaties* en/of *RvIG-applicaties* in het reisdocumentenstelsel. Eindgebruikers behoren tot de organisatie van een bepaalde ketenpartner in het reisdocumentenstelsel, of tot RvIG.
2. RvIG-applicaties zijn toegankelijk via een eindpunt op het Internet.
3. Eindgebruikers vervullen een of meer *rollen*.
4. Autorisatie van eindgebruikers binnen toegelaten applicaties en RvIG-applicaties betreft <organisatie, rol_eindgebruiker> → functionaliteit (functionaliteit is dan te definiëren als schermen of functies in schermen).
5. De definitie van rollen binnen een toegelaten applicatie is de verantwoordelijkheid van de ketenpartner.
6. De definitie van rollen binnen een RvIG-applicatie is de verantwoordelijkheid van RvIG.
7. Nader te bezien is of roldefinities binnen VRS gestandaardiseerd moeten worden.
8. Rolscheiding (het wederzijds uitsluiten van bepaalde rollen) is mogelijk en wordt geïmplementeerd door businesslogica binnen de applicatie.

Authenticatie

9. Eindgebruikers worden voorzien van een authenticatiemiddel door de organisatie waartoe zij behoren.

10. RvIG stelt eisen aan het betrouwbaarheidsniveau van het authenticatiemiddel waarmee toegang tot RvIG-applicaties kan worden verkregen.
11. RvIG standaardiseert de authenticatiediensten / stelsels, waarmee toegang tot RvIG-applicaties kan worden verkregen.
12. Authenticatie van eindgebruikers is zowel mogelijk via federatie van IdM-systemen van ketenpartners, mits deze aan de gestelde eisen voldoen, alsmede via commercieel verkrijgbare authenticatiediensten (denk aan eHerkenning).
13. De RvIG-applicaties kunnen hiermee zowel de organisatie herkennen van waaruit een toegangsverzoek / loginpoging wordt gedaan, als de individuele gebruiker.

Autorisatie binnen toegelaten applicaties

14. Autorisatie van interactieve gebruikers binnen toegelaten applicaties is de verantwoordelijkheid van ketenpartners. De administratie hiervoor voeren de ketenpartners in de toegelaten applicaties en/of hieraan gekoppelde IdM-systemen.
15. Toegang voor interactieve gebruikers is een mogelijk te borgen onderwerpen in het *kwaliteitsmanagementsysteem* voor het reisdocumentstelsel.

Autorisatie binnen RvIG-applicaties

16. RvIG-applicaties (portalen zoals RAP) kennen gebruikers, rollen en functies.
17. De toegang tot bepaalde functies is in RvIG-applicaties afhankelijk van het vervullen door een gebruiker van bepaalde rollen.
18. Toekennen van een rol wordt vormgegeven als het koppelen van een attribuut aan een gebruiker. In de zuivere zin is er dus sprake van Attribute Based Acess Control (ABAC) in plaats van RBAC.
19. Consequentie hiervan is dat de rechten van een gebruiker de verzameling is van de rechten die gekoppeld zijn aan elk van de rollen die aan die gebruiker zijn gekoppeld.
20. Eventuele rolscheidingen dienen te worden geïmplementeerd door businesslogica in de applicatie. Deze kan beschikken over de rollen van de gebruiker.

6.2.4 Toegang van applicaties tot API's

De volgende toegangslaag betreft de toegang van applicaties tot API's. Daarbij worden ook regels geformuleerd over API's zelf:

1. Applicaties kunnen slechts worden aangesloten op het serviceplatform via een verbinding die met een PKIo-certificaat is beveiligd, dat de technisch aan te sluiten organisatie identificeert. De verbindingsbeveiliging biedt 2-zijdige authenticatie alsmede vertrouwelijkheid van het transport.
2. Applicaties van ketenpartners kennen een *toelatingsregime*, in het model van een 'typegoedkeuring' of een 'individuele goedkeuring'. Goedkeuring vindt plaats op basis van ordentelijke omgang met de business services en de gegevens in het reisdocumentenstelsel, alsmede een ordentelijk geregelde toegang voor eindgebruiker. (Vooralsnog wordt dit toelatingsregime vormgegeven via een lichtgewicht model, op termijn kan dit zwaarder worden aangezet.)
3. De API's zijn zo vormgegeven dat zij een welbepaalde set *gegevenselementen* betreffen. Zijn variaties van een API aan de orde met een afwijkende set gegevenselementen, dan wordt er een nieuwe

(verbijzonderde) API gecreëerd. (NB Dit is een werkwijze totdat een noodzaak voor een andere aanpak evident wordt.)
4. Toegang wordt verleend tot een API op basis van de identiteit van de de applicatie die toegang verzoekt en de organisatie die functioneel toegang zoekt. Dit wordt geregeld middels een API-key (NB De organisatie die technisch aansluit, is geregeld met het PKIo-certificaat).
5. Access control pogingen (geslaagd of niet geslaagd) worden gelogd, alsmede de gegevens van de uitkomst van de controles van authenticatie en autorisatie.
6. Autorisaties tot API's zijn onderdeel van de verantwoordelijkheid van RvIG.

6.2.5 Toegang tot kritische resources / data

Hier geldt:
1. Toegang tot data in de kernregistratie vindt steeds plaats via deze laag.
2. Toegang kan dan op bepaalde datagroepen plaatsvinden, waarbij de acties typisch de Create, Read, Update, Delete zijn.
3. In deze laag worden ook beperkingen van waardebereiken voorzien, waarbij gekeken wordt naar de actor in kwestie (welke organisatie kan detailgegevens van welke residocumenten zien bijvoorbeeld). Dit wordt zo georganiseerd, om dit soort access control regels zoveel mogelijk centraal te formuleren.

6.3 Privacy

De privacy risico's binnen het reisdocument stelsel liggen met name in:
- Datalekken door kopieslagen van reisdocument gegevens buiten RvIG bijvoorbeeld t.b.v. handhaving (Fysieke CD's, enz.);
- Er vindt geen maatwerk (hit/no-hit) bevraging plaats op de gegevens (geen dataminimalisatie);
- Lekken van tot persoon herleidbare biometrische gegevens of verwisseling, morphing van biometrische gegevens;
- Identiteitsverificatie vindt niet plaats op basis van dataminimalisatie. Er wordt veel informatie gevraagd voor een correcte identiteitsvaststelling;
- Signaleringsgegevens zijn privacy gevoelige gegevens.

Voor de beschrijving van de privacy principes hebben we gebruik gemaakt van de universele privacy principes van de OESO/OECD, het raamwerk Privacy by Design gepubliceerd door Cavoukian, de handleiding AVG ministerie Justitie & Veiligheid en de privacyontwerpstrategieën uit het 'Blauwe Boekje'. De privacy ontwerpprincipes zijn op gesteld op basis van de reeds gemaakte keuzes dat er een logische kernregistratie Reisdocumenten is met daarbinnen procesondersteunende gegevens- en statusinformatieregistratie, signaleringsregistratie en biometrie opslag voor ondersteuning van het aanvraag en uitgifte proces. Dit biedt primair scheiding van opslag en verstrekking van informatie. Het is bijvoorbeeld onontkoombaar dat het aanvraagportaal alle informatie benodigd voor een aanvraag en personalisatie verwerkt. Dit levert de volgende principes op:

6.3.1 Verantwoordelijkheid

- De verwerkingsverantwoordelijke en bewerker voor de gegevensverwerking is duidelijk benoemd.

- De verantwoordelijke maakt afspraken met de bewerker(s) over de veilige en zorgvuldige verwerking van persoonsgegevens. Het is voor de bewerker duidelijk waarover deze zich moet verantwoorden en op welke wijze dit gerapporteerd wordt.

6.3.2 Legitiem doel en doelbinding

- De reden voor het verwerken van persoonsgegevens in het kader van uitvoering van de paspoortwet (het verwerkingsdoel) is vooraf bepaald en voldoende duidelijk omschreven.
- De verwerking van persoonsgegevens moet gebaseerd kunnen worden op één van de grondslagen uit de Wbp (artikel 8 Wbp).
- Wanneer ondubbelzinnige toestemming (artikel 8a Wbp) als grondslag wordt gebruikt wordt deze voorafgaand aan het verwerken van de persoonsgegevens gevraagd.

6.3.3 Doelbinding

Gegevens mogen alleen verwerkt worden voor het doel waarvoor ze verzameld zijn, tenzij het nieuwe doel verenigbaar is met het oorspronkelijke doel.

6.3.4 Delen van gegevens met derden

Gegevens worden alleen gedeeld met derden als daar een rechtmatige grondslag voor is

6.3.5 Principes privacy-by-design

De volgende principes hanteren we voor een privacy vriendelijke omgeving:

- Beperk de rechten binnen een bepaalde context
- Maak onderscheid en compartimenteer verantwoordelijkheden en rechten
- Ga ervan uit dat onbekende entiteiten onvertrouwd zijn, een duidelijk proces om het vertrouwen te bevestigen en valideer wie verbinding wil maken. Hierdoor mogen bij een ingekochte dienst geen gegevens van de burger bewaard worden

6.3.6 Dataretentie

De bewaartermijnen die in het systeem gehanteerd worden hebben een wettelijke grondslag in het paspoortbesluit, AVG en archiefwet. Zodra de gegevens de bewaartermijn hebben bereikt, worden ze uit het systeem verwijderd of geanonimiseerd. Daarmee moeten alle gegevens worden voorzien van een bewaartermijn.

6.3.7 Dataminimalisatie wordt toegepast bij alle persoonsgegevens.

Er wordt bij de bevraging uit het kernregister alleen de nodige gegevens opgehaald. Om die gegevens te mogen gebruiken is een autorisatiebesluit geregeld. Daarnaast wordt deze regel ook toegepast voor *alle* andere gegevensuitwisselingen.
Uitgangspunt voor de nieuwe infrastructuur is dat er geen verandering komt in de persoonsgegevens die worden verwerkt voor aanvraag en uitreiking alsmede die worden vastgelegd voor de archieffunctie. Bij het vastleggen van persoonsgegevens voor archivering kan overwogen worden of het nodig is om alle gegevens vast te leggen of dat deze gegevens reeds bekend zijn in bv de

BRP en dat er met een verwijzing gewerkt kan worden. Daar waar in deze paragraaf wordt gesproken over een business service is dat een dienst tussen RvIG en de ketenpartners én over de gehele keten heen.

- Voor elke business service geldt dat deze niet meer gegevens verwerkt dan noodzakelijk is voor de functies van de business service, zodat de verwerking van persoonsgegevens minimaal is en niet op plaatsen staat waar dit niet nodig is. *[selecteer, sluit uit]*
- Voor elke business service geldt dat deze niet meer gegevens opslaat dan noodzakelijk is voor de primaire functie, het beheer en de verantwoording, zodat de opslag van gegevens minimaal is en niet op plaatsen waar dit niet nodig is. *[selecteer, sluit uit, verwijder]*
- Voor elke business service geldt dat deze gegevens die elders zijn/worden opgeslagen hergebruikt en niet opnieuw voor eigen gebruik opslaat zodat onnodige opslag wordt voorkomen. Houdt hierbij rekening met het opslaan van proces- en statusinformatie die gevoelig zijn zoals een weigering. *[selecteer, sluit uit, verwijder]*
- Gegevens die een business service niet opslaat worden direct na verwerking vernietigd, zodat er niet onbedoeld een dataverzameling ontstaat. Deze gegevens mogen ook niet in logging voorkomen of op andere plaatsen opgeslagen blijven. *[vernietig]*

6.3.8 Maak onherleidbaar

Verbreek waar mogelijk de link tussen personen en gegevens (anonimiseer en pseudonimiseer)

6.3.9 Informeren

Informeer gebruikers over de verwerking van hun persoonsgegevens en voor welk doel.

6.3.10 Scheid

Scheid persoonsgegevens zoveel mogelijk van elkaar en werk zo gedistribueerd mogelijk.

Essentie van de nieuwe infrastructuur is dat deze van decentraal naar centraal gaat, dit is in beginsel tegen het beginsel distribueer in. Argument voor centralisatie is dat het met de bestaande decentrale oplossing niet goed mogelijk is om een aantal controles uit te voeren om misbruik van persoonsgegevens te voorkomen. Dit doet afbreuk aan de privacy bescherming. Besloten is dat het versterken van het controle proces meer bijdraagt aan de bescherming van de privacy dan dat centralisering afbreuk doet. Het scheiden van proces ondersteunende informatie van de opslag van persoonsgegevens is een belangrijke privacy design beginsel voor de centralisatie. Hetzelfde geldt voor het scheiden van biometriegegevens van de overige persoonsgegevens. Op deze manier kan de waarborg van de toegang tot persoonsgegevens beter gerealiseerd worden en zijn persoonsgegevens niet (onbedoeld) beschikbaar voor functies en processen waarin deze niet noodzakelijk zijn.

- De opslag van persoonsgegevens (het documentnummer is een persoonsgegeven) is alleen toegestaan in de kernregistratie (alle gegevens behalve biometrie) en de opslag van biometrie, zodat persoonsgegevens gescheiden zijn van procesgegevens en zodat biometrische gegevens gescheiden zijn van de overige persoonsgegevens. *[isoleer, distribueer]*
- Opslag van procesondersteunende en status informatie ligt zo veel mogelijk buiten de kernregistratie en de biometrie opslag zodat proces en persoonsgegevens niet door elkaar lopen. *[distribueer]*

Voorbeelden ten behoeve van de realisatie: Persoonsgegevens zoals een BSN of documentnummer kunnen de ingang zijn voor een bevraging van aanvraaggegevens. In dat geval moet het aanvraagportaal de gevraagde gegevens uit het kernregister opvragen met dezelfde sleutel.

6.3.11 Abstraheer

Aggregeer tot het hoogst mogelijke niveau. Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.

Voor de primaire processen zijn gegevens niet te aggregeren omdat het juist gaat om het produceren van paspoorten en identiteitskaarten met de specifieke persoonsgegevens van de houder. Welke persoonsgegevens daarvoor nodig zijn is vastgelegd in wet- en regelgeving. Het aggregeren is wel van toepassing op gegevens in logbestanden en rapportages.

- Loginformatie van succesvol afgeronde transacties worden voor opslag gereduceerd tot de minimale gegevens om na te gaan dat de transactie heeft plaatsgevonden en waarom, zodat er geen persoonsgegevens achterblijven in logbestanden *[vat samen]*
- Loginformatie van niet geslaagde transacties of andere problemen kunnen langer bewaard blijven voor analyse en oplossen van problemen. Na herstel moeten de persoonsgegevens uit de log verwijderd worden en mogen alleen technische gegevens bewaard blijven, zodat er geen persoonsgegevens achterblijven in de logbestanden *[vat samen]*
- Voor rapportage en trendanalyse mogen geen persoonsgegevens worden gebruikt, gegevens moeten samengevat worden in anonieme vorm zodat er geen persoonsgegevens worden verwerkt. *[groeperen, vat samen]*
- Voor verantwoording moet een audit log bijgehouden worden zodat kan worden nagegaan wanneer en door wie en waarom gegevens van een persoon zijn verwerkt. *[vat samen]*

6.3.12 Toon aan

Toon aan dat op een privacy vriendelijke wijze persoonsgegevens worden verwerkt. Verzamel logs, doe audits en rapporteer.

Elke business service dient een audit log te hebben die kan aantonen dat de gedefinieerd processen juist zijn verlopen of dat er een fout is opgetreden.

6.3.13 Gegevensexport

Gegevens mogen niet naar een land worden verstuurd waar géén adequaat niveau van privacybescherming is.

7 Beheer

In dit hoofdstuk worden beheersaspecten beschreven.

De volgende beheerstandaarden worden binnen RvIG gebruikt in het kader van beheerswerkzaamheden:
- BiSL voor het uitvoeren van functioneel beheer en informatievoorziening
- ASL voor het uitvoeren van applicatiebeheer
- ITILv4/ISM voor het uitvoeren van het beheer van de infrastructuur

Recentelijk zijn deze aangevuld met USM (Universeel Service Management) vanuit de agile optiek die 4V hanteert.

Vanuit de RvIG referentiearchitectuur is het volgende principe van toepassing.

TN-BEV-01 **Akkoord**	**Op iedere dienst zijn dienstverleningsafspraken gemaakt.**
Statement	Voor iedere afgenomen of aangeboden dienst is een dienstverleningsafspraak gemaakt (DVO, DVA of SLA).
Implicaties	Er moeten specifieke afspraken gemaakt worden voor de SLA met de hosting- en beheerpartijen Afspraken kennen de volgende aspecten: • Beschikbaarheid • Openstellingstijden • Performance • Verwacht gebruik • Doorbelasting • Audit en beveiliging • Doelbinding en noodzaak gebruik van gegevens • Rapportages • Incidenten • Wijzigingen • Releases • Problemen • Onderhoudswindow • Back-up en restore mogelijkheden (i.v.m. bv dataverlies) In detail moet worden gecontroleerd op aanwezigheid: • Toetsingscriteria inbeheername

7.1 Informatievoorzieningenbeheer

Contentmanagement van de verschillende portalen vindt plaats door RvIG. Wijzigingen vinden plaats op de PaaS omgeving van RvIG. Er komen 'informatie stekkers' op de huidige applicaties bij ID&D (CORI) en Dictu (BR/VR en RPS). Uiteindelijk zullen de bestaande applicaties en databases gemigreerd moeten worden naar de RvIG PaaS omgeving. Op die wijze vindt het beheer vanuit één centraal punt gecoördineerd plaats.

7.2 Applicatiebeheer

Beheer vindt nu vaak door de beheerders rechtstreeks plaats op de systemen (bijvoorbeeld via de command line) of via applicatie aanpassingen bij de leverancier. Dit zal gezien de best practice DevOps anders verlopen. In de business projecten zullen de beheerders gelijk oplopen en wensen of eisen definiëren die middels webportalen tot uitvoering kunnen komen.

7.3 Beheervoorzieningen

Onderstaande figuur geeft een uittreksel van de voorzieningen vanuit de voorzieningencatalogus die RvIG zelf minimaal nodig heeft voor het uitvoeren van haar functionele beheerwerkzaamheden op de RvIG stelselapplicaties en de daar direct onder liggende infrastructuurdiensten. Deze voorzieningen moeten beschikbaar zijn in het infrastructuurlandschap, alvorens het infrastructuurlandschap door RvIG in beheer genomen kan worden en de RvIG stelselapplicaties gemigreerd kunnen worden. In het kader van deze PSA zijn de voorzieningen onderverdeeld in twee groepen: Digitale werkruimte-voorzieningen en Management-voorzieningen:

Figuur 7. Beheervoorzieningen

7.3.1 Digitale Werkruimtevoorzieningen

1. Werkruimte RvIG toegangspoort

Middels deze voorziening kunnen medewerkers van RvIG toegang verkrijgen tot de digitale beheerwerkruimte van RvIG, van waaruit zij hun werkzaamheden (functioneel beheer op stelselapplicaties, gegevens en/of het RvIG infrastructuurlandschap) kunnen verrichten.

2. Gesloten werkruimte RvIG

Middels deze voorziening kunnen medewerkers van RvIG op Windows draaiende applicaties uitvoeren die direct interacteren met de data en/of bedrijfsapplicaties van RvIG.

Het gaat hier om een gesloten werkruimte ten behoeve van beheer van de RvIG productie stelselapplicaties. Deze geeft de RvIG beheerders toegang tot basisfunctionaliteit met betrekking tot het uitvoeren van beheertooling. Vanuit deze digitale werkruimte kunnen RvIG gebruikers beheer uitvoeren op de RvIG stelselapplicaties. Toegang is nodig vanaf deze beheerwerkruimte tot de productie stelselapplicaties waaronder de web servers, applicatie servers en database servers.

Deze gesloten werkruimte zal ook worden gebruikt door de RvIG testers. Vanuit deze werkruimte kunnen de RvIG testers testwerkzaamheden uitvoeren op de RvIG stelselapplicaties. Het gaat hier om test ten behoeve

van het oplossen van problemen of testwerkzaamheden die uitgevoerd moeten worden als onderdeel van het voortbrengingsproces.

3. Open werkruimte RvIG

Ontwikkelaars en testers hebben speciale vereisten waardoor een gesloten werkruimte voor hen niet voldoet. De Open werkruimte RvIG voorziening is hierop het antwoord. Middels deze voorziening kunnen medewerkers van RvIG en leveranciers (de technisch beheerders) op Windows draaiende applicaties uitvoeren die direct interacteren met de data en/of bedrijfsapplicaties van RvIG. Deze geeft de RvIG testers en ontwikkelaars toegang tot basisfunctionaliteit met betrekking tot het uitvoeren van testtooling en ontwikkeltooling. Daarnaast is het (binnen grenzen) mogelijk de werkruimte uit te breiden door eigen programmatuur te installeren, en de configuratie te wijzigen van de aanwezige software.

Vanuit deze digitale werkruimte kunnen RvIG testers tests uitvoeren op de RvIG stelselapplicaties, en kunnen ontwikkelaars applicaties ontwikkelen zoals analysetooling. Toegang is nodig vanaf deze werkruimte tot de niet-productie stelselapplicaties, waaronder de web servers, applicatie servers en database servers.

7.3.2 Managementvoorzieningen voor beheer RvIG

Middels de set aan voorzieningen in deze categorie kunnen medewerkers van RvIG functionele beheerswerkzaamheden uitvoeren op de RvIG stelsel-applicaties, en kan RvIG servicelevelmanagement de kwaliteit van de dienstverlening meten en controleren. Het gaat hier om managementvoorzieningen voor het monitoren, loggen en beheren van de RvIG stelselapplicaties. Dit is bij voorkeur business activity monitoring (end-to-end in de keten).

8 Programma overstijgende ontwerpkeuzen

In dit hoofdstuk worden ontwerpkeuzen weergegeven die het programmabelang overstijgen en op lange termijn (positieve) gevolgen hebben voor de RvIG architectuur, maar waar wellicht nog geen architectuurrichtlijnen voor zijn. Voor elke keuze wordt een aparte paragraaf opgenomen waarin de keuze, de alternatieven en de beslissingscriteria gegeven zijn.

8.1 Keuze service gerichte architectuur

- In de bijlage 'toekomstvisie' zijn de knelpunten van het huidige reisdocumenten beschreven. Op hooflijnen komt het erop neer dat de decentrale inrichting heeft geresulteerd in een complexe beheersituatie, dat er veel verschillende gegevensleveringen in gebruik zijn en er veel gegevens gekopieerd worden. Een service gerichte architectuur kan deze problemen en onwenselijke situaties tegengaan.
- Het stelsel kan in kwaliteit en uniformiteit sterk verbeterd worden indien dezelfde type business services op verschillende plaatsen worden hergebruikt. Deze toetsing wil men vanuit zowel het aanvraag en uitgifte proces als ook bij signaleringenbeheer.
- Het is bij onderzoek gebleken dat verschillende uitgevende instanties reeds gebruik maken van (frontoffice) applicaties die in een brede context worden gebruikt, zoals de Reisdocumenten Modules als onderdeel van een brede 'Burgerzaken' applicatie. Tijdens analyse, waarbij de vraag werd gesteld of de functie van RDM in reisdocument gerelateerde processen kan worden uitgefaseerd, werd duidelijk dat er meerdere andere functies in de RDM waren ingebouwd en dat iedere uitgevende instantie op verschillende wijze gebruik maakt van deze functies. Een registratie aanvraag en uitgifte portaal (RAP) naast de RDM betekent voor de gemeente medewerker dan twee schermen naast elkaar en dat is niet wenselijk. Een sterkere integratie tussen de kernregistratie en applicatie leveranciers van RDM is daarmee noodzakelijk, welke door middel van een service gerichte architectuur (lees: flexibiliteit in integratie van noodzakelijke functies) kan worden gefaciliteerd.
- De sterkere integratie is ook van toepassing op de interne reisdocumenten huishouding; voor bijvoorbeeld een betere identiteitsvaststelling zullen er meerdere verschillende registraties/registers geraadpleegd moeten worden, die op dit moment zijn ondergebracht bij verschillende leveranciers. Mogelijk kan biometrische vergelijking ten opzichte van eerder afgenomen biometrie plaatsvinden.
- Gedurende de kwartiermakersfase is gebleken dat de destijds gepresenteerde beoogde projectresultaten te groot in omvang waren. Zo zou het RAAS uitgefaseerd kunnen worden als alle RAAS functionaliteiten in het aanvraag en uitgifte portaal én er een Registratie opvraagbare biometrie (ROB) gerealiseerd zouden zijn. Daarmee zou de ontwikkeling veel langer dan 1 ½ jaar duren en er pas veel later aan de gewenste beleidseisen voldaan kunnen worden. Het gewenste alternatief is echter om niet meer

grootschalige verandertrajecten te hebben maar incrementeel en kort cyclisch nieuwe functionaliteiten te leveren. Door functionaliteiten in goed af te bakenen services te realiseren wordt direct ook een beter beheersbare programma aanpak mogelijk, waarbij steeds waardevolle en gebruiksklare onderdelen worden gerealiseerd.

- Door het verservicen van de architectuur is het mogelijk scheiding in systemen en processen aan te brengen en verantwoordelijkheden expliciet vast te stellen en de services te standaardiseren. Als er ergens in de keten veranderingen optreden of wanneer je gewenst of ongewenst overstapt naar een andere leverancier is dit daardoor eenvoudiger te bewerkstelligen. De architectuur is als het ware modulair opgebouwd waardoor een bepaalde service vervangbaar is en gecombineerd kan worden met andere services. Integratie is dankzij (open) API' s te realiseren. Een service gerichte architectuur is in veel gevallen de oplossing voor herbruikbaarheid, beheersbaarheid, snelle time-to-market en zorgt ervoor dat afzonderlijk opererende applicaties en systemen verbonden kunnen worden.

9 Architectuurgovernance binnen VRS

In deze paragraaf is aangegeven hoe architectuurgovernance (sturing, controle en verantwoording) plaatsvindt binnen VRS. Architectuurgovernance is noodzakelijk omdat de programmastartarchitectuur een product is van de kwartiermakersfase en per definitie op hoofdlijnen blijft. Een 'grand design' vooraf van het gehele stelsel is niet uitvoerbaar zonder een zeer lange ontwerpfase en dat is ongewenst en binnen VRS dus ook niet voorzien.

Dit hoofdstuk geeft antwoord op de volgende vragen:

- Wat zijn de doelen van architectuurgovernance?
- Wat zijn de relevante objecten waarop architectuurgovernance van toepassing is?
- Hoe is architectuurgovernance georganiseerd?

9.1 Doelen van de architectuurgovernance in VRS

We onderkennen de volgende doelen van architectuurgovernance:

- Om te borgen dat ontwerp- en realisatieactiviteiten een goede nadere invulling vormen van de programmastartarchitectuur;
- Dat de samenhang met de omgeving (RvIG, ketenpartners) op de lagen business, informatie en techniek, beheer en informatiebeveiliging goed is verzorgd;
- Dat in ontwerp en realisatie voldaan wordt aan standaarden en kaders die vanuit de omgeving worden opgelegd aan VRS. Voor wat betreft de inhoud van business, informatie en techniek, maar ook voor de op te leveren ontwerpartefacten en documentatie.

9.2 Relevante architectuur- en ontwerpobjecten

Op welke objecten is architectuurgovernance van toepassing? In deze paragraaf een overzicht daarvan.

De volgende architectuurproducten worden nog opgesteld binnen VRS:

- Security concept, dit is inclusief een autorisatiemodel en regels voor de business continuity;
- Nadere ontwerpkeuzen voor informatieverstrekking;
- PaaS / platform solution architectuur (in diverse versies);
- Services register, en bijbehorende regels van sturing op de services (SOA governance);
- Datamodel voor het reisdocumentenstelsel met bijbehorend gegevenswoordenboek;
- Model voor statussen van aanvragen en documenten, alsmede het beheer van deze statussen;
- Begrippenlijst;

- Huisstijl voor webdiensten en apps. Look and feel en interaction design regels voor alle user facing informatievoorzieningscomponenten;
- Programmastandaard voor werkwijzen en ontwerpartefacten. Inpassing in c.q. aansluiting op de set RvIG architectuurmodellen.

Naast bovengenoemde architectuurproducten zijn er diverse meer gedetailleerde ontwerpproducten voorzien:

- Procesmodellen. Per hoofdproces wordt er verdiept van een 'hoog over' procesmodel voor het hoofdproces verbijzonderd naar specifieke situaties en ketens;
- Use case modellen;
- User stories. User stories worden aangevuld met architectuuraanwijzingen door de programma-architecten;
- Solution architecturen van portalen en andere componenten.

Ten slotte zijn te onderkennen:

- Nadere ontwerpbesluiten;
- Gerapporteerde architectuur- c.q. ontwerpissues en afwijkingen (waar realisatie afwijkt of dreigt af te wijken van ontwerp- en architectuurdocumenten of waar ontwerpdocumenten afwijken of dreigen af te wijken van architectuurdocumenten)

9.3 Organisatie architectuurgovernance, ontwerpautoriteit

Binnen VRS wordt er een ontwerpautoriteit ingericht, die functioneert als een architectuurboard voor VRS.

De volgende uitgangspunten zijn van toepassing op deze ontwerpautoriteit:

1. De ontwerpautoriteit adviseert gevraagd en ongevraagd over architectuur- en ontwerpobjecten binnen VRS, nadere ontwerpbesluiten alsmede issues en afwijkingen.
2. Het proces van de ontwerpautoriteit is in eerste aanleg gericht op het bereiken van overeenstemming met projectleiders in het programma of stakeholders. Bij overeenstemming stelt de ontwerpautoriteit de betreffende (gedocumenteerde) ontwerpbesluiten vast.
   Waar meningen (blijven) verschillen, worden de betreffende ontwerpbesluiten door de ontwerpautoriteit in samenwerking met de betreffende andere actoren beslisbaar gemaakt. Afhankelijk van het onderwerp wordt er dan besloten door de programmamanager VRS of door de opdrachtgever, gehoord hebbende het RvIG brede architectuuroverleg alsmede de leden van de stuurgroep VRS.
3. Aan de ontwerpautoriteit worden alle bovengenoemde architectuur- en ontwerpobjecten voorgelegd om te laten voorzien van een advies. De vaststelling vindt plaats conform de reguliere programmabesturing (zie. programmaplan).
4. Indien relevant kan de ontwerpautoriteit afstemmen met andere actoren binnen en buiten RvIG (ADM, IB, klankbordgroepen) alvorens een advies te formuleren.

5. De ontwerpautoriteit kan acties uitzetten om de voor VRS vastgestelde architectuur (c.q. het vastgestelde ontwerp) nader te borgen. Dit bijvoorbeeld door het verrichten van een architectuurtoets.
6. In de ontwerpautoriteit zijn vertegenwoordigd:
   - Architecten van VRS;

     Afhankelijk van het onderwerp:

     a. Leveranciers die direct voor VRS werkzaam zijn;

     b. Ook architecten van ketenpartners of hun leveranciers;
   - Een linking pin met het RvIG brede architectuuroverleg (opvolger van de opgeheven ADM)

     a. RvIG, in casu het programma VRS levert de voorzitter van de ontwerpautoriteit.

     b. De voorzitter van de ontwerpautoriteit besluit over de formulering van het advies van de ontwerpautoriteit, gehoord hebbende de deelnemers. Waar geen gekwalificeerde meerderheid achter de vastgestelde formulering staat, wordt dit vermeld als onderdeel van betreffend advies met de relevante toelichting.

Bredere afstemming zoals bedoeld onder punt 4 is tenminste aan de orde voor:

- Het te ontwikkelen security concept;
- De architectuur van het generieke platform (PaaS);
- Programmastandaard voor werkwijzen en ontwerpartefacten.
- API management

9.4 Vastgestelde en uit te werken ontwerpkeuzes

In de afgelopen periode zijn de volgende ontwerpkeuzes vastgesteld:

Issue 19-001
ontwerpautoriteit v.

Voor een overzicht van de uit te werken ontwerpkeuzes is er een Trello bord aangemaakt. De architecten kunnen hier inzicht in geven.

Bijlage 1: Actuele knelpunten

Actuele knelpunten in het reisdocumentenstelsel:

1. Het niet kunnen beschikken op één plaats over een volledige en actuele registratie van in omloop zijnde reisdocumenten. Doordat er niet één kernregistratie van aangevraagde en uitgegeven reisdocumenten bestaat, is niet met 100% zekerheid aan te geven of een reisdocument in omloop zou mogen zijn of over welke actuele reisdocumenten een persoon beschikt;
2. Het niet beschikken over middelen om toenemende look-a-like fraude in het aanvraag- en uitgifteproces tegen te gaan. Ook zijn er aanwijzingen dat er fraude door 'morphing' voorkomt. Daarbij vloeit de ene gezichtsopname geleidelijk over in een andere en is deze voor twee personen bruikbaar;
3. Het niet op eenvoudige wijze kunnen doen van een identiteitsverificatie aan de hand van een foto in een eerder uitgegeven reisdocument, indien dat reisdocument is uitgegeven door een andere uitgevende instantie;
4. Het niet hebben van eenvoudige middelen om 'shopgedrag' van burgers tegen te gaan bij grensgemeenten, posten in het buitenland en de Caribische Landen/Caribisch Nederland.;
5. Het niet consequent controleren op (actuele) signaleringen bij de aanvraag van een reisdocument;
6. Beperkte ondersteuning van het aanvraagproces voor sommige uitgevende instanties aanvraag wordt nu direct ingegeven in het RAAS;
7. Geen gebruik van de gegevens uit de BRP (c.q. PIVA – de persoonsregistratie van Caribisch Nederland en de Caribische landen) bij sommige uitgevende instanties;
8. Het niet hebben van een (doorlopende) registratie in BRP of PIVA van de houders van reisdocumenten en het niet bijhouden van de gegevens over uitgegeven reisdocumenten in de Registratie Niet Ingezetenen (RNI);
9. Veelvuldig gebruik van papieren formulieren in het reisdocumentenstelsel, wat tijdrovend en foutgevoelig is.

De knelpunten zijn niet alleen theoretisch, ze hebben ook in de praktijk geleid tot een aantal incidenten in de afgelopen jaren.

Bijlage 2: Toekomstvisie

In deze bijlage is een beeld geschetst van de toekomstige ontwikkelingen in het reisdocumentenstelsel. Vanuit externe maatschappelijke trends, ontwikkelingen in onder meer wetgeving en beleid, alsmede vanuit de wens om een aantal knelpunten weg te nemen, zijn doelen geformuleerd. Dit zijn de doelen, waarvan RvIG verwacht dat deze op enig moment op de middellange termijn (5-10 jaar) gaan leiden tot concrete veranderingen.

1.1 Externe maatschappelijke trends

Externe maatschappelijke trends die van invloed zijn op het reisdocumentenstelsel zijn:

1. De voortschrijdende digitalisering van de maatschappij en allerhande vormen van dienstverlening. De hiermee gepaard gaande 24/7 economie;
   Hieraan gekoppeld is de behoefte aan een digitaal identiteitsmiddel (eID) op hoog betrouwbaarheidsniveau;
2. Toenemend gebruik van biometrische gegevens en biometrische identiteitsverificatie. We zien biometrische technieken gebruikt worden buiten het klassieke domein van reisdocumenten, toegangscontrole en forensisch onderzoek. Mobiele apparaten ondersteunen vingerafdruk- en gezichtsherkenning, waar ondermeer banken gebruik van maken;
3. Toenemend volume van internationaal reizen. We zien dat Schiphol stijgende aantallen reisbewegingen en daarmee gepaard gaande grenspassages kent. Dit jaagt de behoefte aan geautomatiseerde grenscontroles aan;
4. Toenemende identiteitsfraude, waarbij het identiteitsdocument zèlf niet de zwakste schakel is;
5. De steeds verdere adoptie van mobiele apparaten en de toenemende mogelijkheden daarvan.

1.2 Ontwikkelingen in wetgeving en beleid:

Ontwikkelingen in wetgeving en beleid zijn:

1. De AVG en de daaruit voortvloeiende wens om de burger meer middelen te geven voor (een afgebakende vorm van) informationele zelfbeschikking. Dit komt in de Agenda Digitale Overheid met name terug als Regie op Gegevens. De consequentie hiervoor;
2. De vorming van één Europese infrastructuur voor eID en elektronische dienstverlening in navolging van de eIDAS verordening alsmede de eerdere Dienstenrichtlijn;
3. De beleidswens om dienstverlening van de overheid te digitaliseren en meer plaats- en tijdonafhankelijk te maken, dit in lijn met de algemene maatschappelijke trend. Deze beleidswens ligt ook vast in de Agenda Digitale Overheid;
4. De in de Agenda Digitale Overheid besloten wens en plicht om een sterk Stelsel Overheidsgegevens te hebben en hiervan zo goed mogelijk gebruik te maken.
5. Behoefte aan een betere integratie van identiteitsprocessen en -diensten op Koninkrijksniveau, teneinde administratieve processen te vereenvoudigen en kwaliteit te verbeteren.

1.3 Overige ontwikkelingen

En dan zijn er nog functionaliteiten in voorbereiding, actuele proeven en behoeftes:

1. E-functionaliteit op de NIK, de zogenaamde eNIK, waarmee de NIK bruikbaar wordt als authenticatiemiddel binnen DigiD Hoog;
2. Proeven met een beperkte vorm van 'plaàtsonafhankelijk' aanvragen van reisdocumenten, waarbij de burger op afspraak op specifieke plaatsen kan langskomen. Voor mensen die niet kunnen reizen is het mogelijk de aanvraag te doen in hun woning of in een zorginstelling, indien ze daarin zijn opgenomen;
3. Proeven met het thuis bezorgen van reisdocumenten;
4. Proeven met een app, die van een geschikte mobiele telefoon een reisdocument maakt, de zogeheten vID;
5. Proeven met Self Sovereign Identity op mobiele telefoons.

1.4 Veranderdoelen voor het reisdocumentenstelsel

Welke doelen streeft RvIG na met het reisdocumentenstelsel?
Hieronder zijn de doelen geformuleerd, die voor het reisdocumentenstelsel op lange termijn aan de orde zijn. Dit zijn met name de veranderdoelen. Onveranderd is de ambitie om een zeer betrouwbaar reisdocument uit te geven tegen een redelijke prijs. Steeds blijft het doel het uitgeven van een betrouwbaar reisdocument van hoge kwaliteit, wat een belangrijke bouwsteen is in een breder identiteitsstelsel. RvIG heeft tot doel de regie te voeren over dit identiteitsstelsel.

De business veranderdoelen die voor het reisdocumentenstelsel op lange termijn aan de orde zijn:

1. Verbetering van de kwaliteit en de efficiëntie van het proces voor het aanvragen tot en met uitreiken van reisdocumenten. We doen dit vooral door beter gebruik te maken van achterliggende registraties waarbij gedacht kan worden aan persoonsgegevens uit de BRP, biometrie, signaleringen, overige gegevens uit eerdere aanvragen. Het proces kan (voor aanvragers in het buitenland) ook winnen aan kwaliteit en efficiëntie door het kunnen bevragen van met BRP vergelijkbare systemen van andere landen;
    - Ter ondersteuning hiervan *uniformeren* we het *proces* aan de balie verder dan momenteel het geval is. Betere ondersteuning van de medewerker voor kennisintensieve taken en geautomatiseerde checks tegen of prefills uit achterliggende registers. Kortom het voor de uitgevende instanties eenvoudiger en transparanter maken.
    - *Doorlópende procesverbetering*. We bewerkstelligen een situatie waarin men de operationele processen en besturende processen voortdurend bewaakt, evalueert en incrementeel verbetert. De verbetering is per definitie stelsel-/partij overstijgend. RvIG is een lerende organisatie, deelt zijn lessen met de ketenpartners en voert regie op de keten van aanvraag tot en met uitreiken. Daarbij neemt RvIG een meer actieve en dienstverlenende rol in zijn toezichthouderfunctie met als voorbeeld LAA.
2. Betere dienstverlening aan de burger, mèt behoud van veiligheid en privacy. Daarbij er is er behoefte aan:
    - Plaats- en tijdonafhankelijke dienstverlening naar de burger, zich uitend in nieuwe varianten van aanvraag- en uitgifteprocessen. Online aanvraag is daarbij één van de varianten. Overigens zal er altijd een face-to-face identiteitsverificatie en afname van biometrie plaatsvinden, zij

het dat dit mogelijkerwijs op een ander moment en/of een andere plaats wordt uitgevoerd.
    - Alternatieve reisdocumenten en identificatiedocumenten (eID, vID) alsmede faciliteiten voor documentloos reizen. Met name een geïntegreerde eID / vID die op de mobiele telefoon landt zorgt voor èn een wezenlijke stap in de beschikbaarheid van authenticatiemiddelen en een laagdrempelig alternatief identiteitsdocument;
    - Het kunnen gebruiken van het reisdocument als drager van de gegevens van geselecteerde andere documenten of specifieke rechten. Stel dat men een UZI-pas zou kunnen vervangen door een reisdocument, waarop bepaalde rollen en/of rechten elektronisch zijn geplaatst, na het moment van uitgifte. In dit kader is er op de Sédula al een zorgverzekeringsattribuut gezet dat dienstverlening door zorgverleners borgt. Nieuwe ontwikkelingen in de ICAO-standaarden maken het ook mogelijk dit soort toepassingen veilig toe te voegen. Dit biedt interessante nieuwe gebruiksmogelijkheden met een aanzienlijk besparingspotentieel. Ook biedt dit de mogelijkheid om de 'sleutelbos' van de burger te beperken;
    - De mogelijkheid voor de burger om zijn eigen reisdocument tijdelijk te blokkeren of definitief als vermist of gestolen aan te melden;
    - De mogelijkheid voor de burger om selectief zijn (identiteits-) gegevens aan dienstverleners ter beschikking te stellen, de zogenaamde Regie op Gegevens. De vorm waarin dat plaatsvindt is nog te bepalen, mede afhankelijk van de ervaringen met Self Sovereign Identity, die nu onder meer wordt beproefd door het ministerie van BZK met gemeenten in het kader van Samen Organiseren en het Beleidslab Digitale Identiteit.
3. Om de kwaliteit van het stelsel duurzaam te borgen wordt de mogelijkheid gecreëerd om backoffice processen te consolideren en/of te centraliseren. Zowel lokale, regionale als centrale backoffices zijn daarbij mogelijk. Inrichtingsvarianten zijn onderwerp van gesprek met uitgevende instanties;
4. De kostenstijging per document als gevolg van het afgenomen aantal reisdocumenten en identiteitskaarten wordt beperkt. Dit gebeurt enerzijds door strategisch in te kopen, het aanvraag- en uitgifteproces slimmer te organiseren (zie ook voorgaande punt) en de kosten voor decentrale hardware en het beheer daarvan terug te dringen. Tevens wordt bezien of de omzet ook kan worden verhoogd door nieuwe producten en diensten te leveren, zoals alternatieve documenten en diensten als vID en SSI. Aan de andere kant geldt ook dat alternatieve documenten waarschijnlijk een deel van de bestaande behoefte aan met name de NIK zullen verdringen;
5. Het leveren van een set aan (zo mogelijk online) informatiediensten, waarmee identiteitsverificatie alsmede controle op het recht om te reizen elders in de maatschappij optimaal ondersteund wordt. RvIG houdt wel een kernregistratie van reisdocumenten bij, maar hij levert deze gegevens niet breed aan andere partijen zoals dat bij basisregistraties gebruikelijk is. De te leveren diensten betreffen:
    - Breder toepassen van (biometrische) identiteitsverificatie, waar dit wettelijk toegestaan is en de doelbinding voldoende wordt geacht;
    - Controles op de echtheid en de status van het document;
    - Controles op het recht om te reizen tegenover een online registratie.
6. Het moderniseren van de systematiek van signaleringen en het omvormen naar een effectieve oplossing om het 'recht om te reizen' van een houder aan te passen.
   Deels is het signaleren een doel om burgers te verhinderen uit te

reizen. Deels wordt er gesignaleerd om burgers onder druk te zetten om problematische schulden bij overheidsinstanties af te laten betalen. Hoe de behoeftes achter het signaleren het beste kunnen worden ingevuld en hoe signaleren daarin een rol kan spelen, is een nóg uit te werken vraag. Tegelijkertijd is er geen eigenlijk expliciet vastgelegd 'recht om te reizen' van burgers;

7. Verbeteren van de weerbaarheid tegen oude maar vooral ook nieuwe dreigingen en vormen van fraude. Dit impliceert:
    - Kennis opbouwen en onderhouden over mogelijke en/of gangbare vormen van misbruik;
    - Mogelijke invoer van 'live capture' van biometrische gegevens om morphing fraude tegen te gaan;
    - Beter zicht op het gebruik van reisdocumenten (fysieke document, vID en eID), om daarmee verdacht gebruik beter te kunnen detecteren en nader te kunnen onderzoeken. Om een beter zicht te krijgen op de keten wordt de ketensamenwerking met de 'afnemers' van reisdocumentendiensten geïntensiveerd;
    - 'Dynamisch beheer' van de reisdocumenten, dat wil zeggen dat naar behoefte het fysieke document (echtheidskenmerken) en de in het document geïntegreerde digitale toepassingen kunnen worden aangepast zonder een volledig nieuw ontwerp te hoeven maken.
8. Het realiseren van een ICT die kan meegroeien met de genoemde ontwikkelingen, alsmede een regieorganisatie binnen RvIG die deze (door)ontwikkeling kan begeleiden.
9. Het verkorten van de time-to-market: de tijd van conceptie van het idee tot aan structurele invoering.
10. Het creëren van een bestendige en gezaghebbende samenwerking met andere uitgevers èn gebruikers van identiteitsdocumenten, met als doelen:
    - Het realiseren van één infrastructuur voor het aanvragen en uitgeven van identiteitsdocumenten;
    - Het borgen van één betrouwbaarheidsniveau voor wettelijke identificatie, zodat er geen 'shopgedrag' kan ontstaan voor identiteitsfraude;
    - Het voeren van de integrale regie op de identiteitsketen. Wat gaat goed, wat minder, wat gaan we verbeteren? RvIG vervult hierin een trekkende rol.

1.5 VRS als fundament voor de veranderingen

Het programma VRS levert voor bovenstaande veranderdoelen het fundament. Processen worden in dat kader verbeterd, ICT wordt vernieuwd en vooral flexibel en toekomstvast opgezet. Veel van de bovengenoemde doelen zijn wezenlijk verstrekkender dan het leggen van een fundament en vallen derhalve buiten VRS. De inhoud en de (operationele) doelen voor het programma VRS zijn beschreven in het hoofdstuk Eindbeeld VRS.

1.6 Na VRS

Na VRS zijn er vier soorten verbeteringen aan de orde:

- Verbeteringen in de dienstverlening aan de burger;
- Mogelijke invoering 'live capture';
- Verdere verbeteringen backoffice;
- Ketenintegratie en regie op de keten;

Deze soorten verbetering worden hieronder puntsgewijs toegelicht.

Verbeteringen dienstverlening burger.

Gedurende de looptijd van VRS pilots of losstaande dienstverlening:

- Plaatsonafhankelijk aanvragen en uitgeven van reisdocumenten,
- Andere aanvraag- en uitgiftemodaliteiten en

vID / eID / SSI op mobiel worden geïntegreerd en landelijk als dienst geleverd.

Een specifiek aandachtspunt voor de procesgang is dat het procesmatig mogelijk moet worden om mobiele identiteitsdiensten (vID, eID, SSI) te leveren volgens het model: 'de klant met een werkend product de deur uit'.

Specifiek voor aanvragen in het buitenland wordt onderzocht om het verschijningsmoment, met de processtap 'identiteitsverificatie en afname biometrische gegevens' los te koppelen van de aanvraag. Dit in lijn met de kabinetsreactie op de Motie Sjoerdsma. Het is ook nodig voor een eventuele 'online' aanvraag van reisdocumenten, aangezien de fysieke verschijning niet ter discussie staat.

Mogelijke invoering live capture.
Afhankelijk van de resultaten van proeven met 'live capture' van de foto, kan dit breed worden ingevoerd. Dit zal zeker na het programma VRS plaatsvinden.

Verdere verbeteringen backoffice.
Tevens worden de volgende verbeteringen in de backoffice gerealiseerd:

- 'Eerst registreren, dan aanvragen'. Dit is een belangrijk uitgangspunt dat een betere kwaliteit gaat opleveren èn betere dienstverlening aan de burger. Het is ook nodig om de processtap 'identiteitsverificatie en afname biometrische gegevens' los te kunnen nemen, wat bijvoorbeeld voor verbeterde dienstverlening in het buitenland (Motie Sjoerdsma) gewenst is;
- Nauwere integratie met de identiteitsketen in de Caribische landen en openbare lichamen;
- Verdere koppelingen met registers. Denk bijvoorbeeld aan koppelingen met persoonsregistraties van andere landen, om het Nederlanderschap eenvoudiger te controleren. Verkend kan ook worden of hiervoor gebruik kan worden gemaakt van de eIDAS infrastructuur;
- Introductie van een centrale backoffice met meer controleprocessen op mogelijk misbruik en fraude;
- 'Zicht op procesgang' van aanvraag tot en met uitgifte ten behoeve van latere stappen in de procesverbetering. Aansluiting bij en gebruik door een QA-functie binnen RvIG.

Betere integratie in de identiteitsketen. Meer zicht op de identiteitsketen binnen en buiten RvIG.
Verbeteringen worden gerealiseerd op het grensvlak van reisdocumenten en BRP / PIVA, en wellicht aanpalende stelsels als Burgerlijke Stand. De input hiervoor zal de strategische visie Identiteit zijn die BZK in samenspraak met haar stakeholders ontwikkelt. Enkele punten kunnen bij wijze van voorbeelden nu reeds worden geïdentificeerd:

- De biometrie die in eerste instantie nog hangt aan de reisdocumenten, wordt gekoppeld aan de persoon;
- Er is continuïteit van biometrie, dat wil zeggen dat er vanaf een bepaald moment in het leven van een kind bij voortduring goed bruikbare biometrische gegevens beschikbaar zijn waarmee betrouwbare identiteitsverificatie mogelijk is;
- Voor identiteitsverificatie worden geïntegreerde services aangeboden vanuit BRP en het reisdocumentenstelsel. Het gebruik hiervan (waar nuttig en nodig) wordt gestimuleerd. Samenwerkingsverbanden met andere partijen in de identiteitsketen worden versterkt en services

worden hierop aangepast. Denk bijvoorbeeld aan attribuutdiensten c.q. attribuutverificatie;
- Van personen worden de bereikbaarheidsgegevens beter bijgehouden;
- Personen beschikken – breder dan nu het geval is – over een eID van hoge betrouwbaarheid.

Aan de aanbodzijde wordt tevens de wijze van het aangeven en bijhouden van het 'recht om te reizen' herzien in samenspraak met ketenpartners. De effectiviteit van het signaleren in de RPS in relatie tot de doelstellingen van signalerende instanties wordt daarbij beschouwd en worden mogelijk andere maatregelen op het gebied van beperkingen van de mogelijkheid om te reizen verkend.

De verbeteringen zijn niet beperkt tot de 'aanbodzijde', maar betreffen nadrukkelijk ook de gebruiksfase van reisdocumenten:
- Verificatiediensten worden verrijkt, zodat RvIG een beeld opbouwt van plaatsen en handelingen, waar het reisdocument wordt gebruikt;
- Een integraal beeld van dat gebruik wordt benut om verdachte gebruikspatronen te kunnen detecteren en hierop onderzoek uit te voeren (fraudepreventie).

RvIG leert in dit stadium niet alleen van de managementinformatie uit zijn eigen operationele processen, hij is ook voortrekker in de afstemming met belangrijke ketenpartners. Beleid en uitvoering spelen hierbij beiden een rol en versterken elkaar.

1.7 Ten slotte

VRS is derhalve een programma dat een aantal zeer gewenste verbeteringen in businessprocessen realiseert.
- Het moderniseren van de methode van signaleringen. Dit in eerste instantie door de signaleringen direct te laten beheren door signalerende instanties.
- Het verbeteren van het proces van aanvraag tot en met uitreiking van reisdocumenten, met name in kwaliteit. Dit wordt bereikt door controles op recente / lopende aanvragen mogelijk te maken (grensgemeenten en buitenland), geautomatiseerde controles tegen RPS in het aanvraagproces, alsmede een vergelijking van de foto van de houder met eerder vastgelegde foto's. Grensgemeenten en de Koninklijke Marechaussee worden beter ondersteund in het aanvraagproces.
- Het verbeteren van de dienstverlening aan de burger, met name door in RAP reeds voorbereidingen te treffen, alsmede door het bieden van de dienst StopID.

Tegelijkertijd legt VRS ook de basis voor toekomstige verbeteringen. In de uitvoering zal derhalve ook worden bewaakt dat dit voorbereidende karakter niet in de hectiek van de programmauitvoering ondergesneeuwd raakt.

Bijlage 3: Begrippenlijst

Begrippenlijst wordt gerealiseerd op programma niveau.

Bijlage 4: Openstaande punten

Onderstaande punten moeten nog uitgezocht worden:

Punt	Omschrijving	Aanpak
1	cursieve terminologie voor begrippenlijst en glossary	Aan de begrippenlijst toevoegen en glossary maken.
2	Paragraaf 3.4: Vraag over status aparte van diplo paspoorten?	
3	Par. 4.2.2: Informatieverstrekking: Sommige partijen moeten we daarvoor nog spreken zoals Politie	Inplannen
4	Par.5.4.1: Hoe zit dit functioneel in elkaar. Met ook de 3 aparte wetten van de 3 eilanden.	Met Eddy afstemmen en dit deel verhuizen naar business architectuur.
5	Technische beschrijving hoe biometrieafname in (nabije) toekomst moet gaan werken.	Afgesproken is dat dit eind Q2 wordt opgepakt i.s.m. de lijnorganisatie.
6		

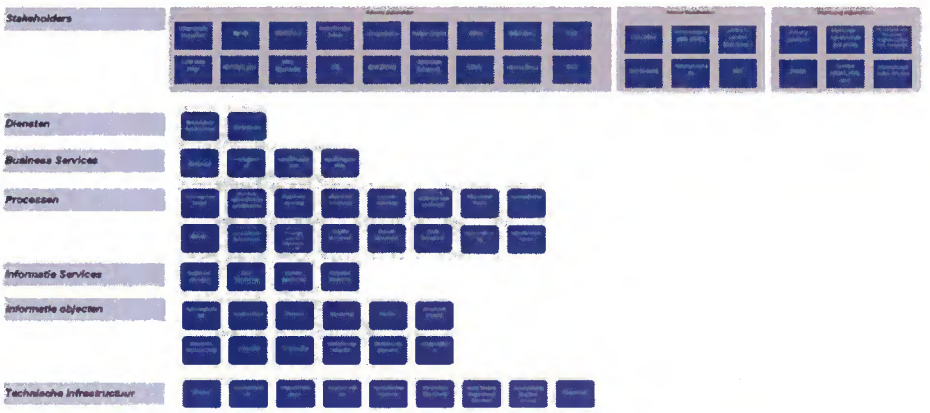
Bijlage 5: Overzicht componenten Reisdocumenten

In bijgevoegd overzicht is af te lezen welke componenten er op dit moment binnen het stelsel Reisdocumenten en op het einde van programma VRS afgenomen zullen worden.

20180910-ARCH-RD
-Matrix_Visie_ICT_20

Bijlage 6: Overzicht deelproducten VRS

In onderstaand overzicht is af te lezen welke producten het programma VRS raakt op Business, Informatie en Technische laag binnen het stelsel Reisdocumenten.



In PDF vorm bijgevoegd zodat er voldoende vergroot kan worden.

20190208-ARCH-Co
mponentenoverzich

Bijlage 7: overzicht van Business Services

Een tweede decompositie is in bijgevoegde lijst af te lezen.

Reisdocumenten Serviceregister.xlsm

Services voor thuisbezorgdienst en MVA nog toevoegen

Bijlage 8: Eisen functionaliteit datamigratie v05.docx

De meer uitgebreide eisen rondom de functionaliteit van de datamigratie zijn in onderstaand document geformuleerd. De originele locatie van dit bestand is: G:\Projecten\VRS\11. Datamigratie\07. Diversen\Akkoord op inhoud\ Eisen functionaliteit datamigratie v05.docx

Eisen functionaliteit datamigratie v05.doc

Bijlage 9: Architectuurafwijkingen

In deze bijlage zijn de afwijkingen benoemd van de RvIG referentiearchitectuur.

Afwijking 1 – Reisdocumenten diensten via internet toegankelijk

Afwijking

De RvIG informatiediensten voor het reisdocumentenstelsel (externe informatieservices en portalen) zijn via het Internet toegankelijk.

Reden

We hebben de volgende redenen om deze informatiediensten via Internet beschikbaar te maken:

- Het eenvoudig kunnen koppelen van ketenpartners. Met name voor signaleringenbeheer is er sprake van een zeer groot aantal ketenpartners. Ook voor diensten op het gebied voor identiteitsverificatie worden zeer veel aangesloten partijen verwacht.
- Het gebruik kunnen maken van een publieke authenticatievoorziening als eHerkenning. eHerkenning is de geprefereerde publieke authenticatievoorziening maar dit impliceert dat de diensten via Internet toegankelijk moeten zijn.
- In de toekomst dienen ook diensten aan de burger te worden geleverd.

Consequenties

Aanpassing aan de paspoortuitvoeringsregelingen aan de orde, omdat deze momenteel de technische wijze van verstrekking van informatiediensten uitputtend beschrijven. Dit is overigens het geval voor veel wijzigingen die VRS introduceert.

Inhoudelijk dient uiteraard een zeer goede beveiliging te worden gerealiseerd. Het programma regelt dit, in afstemming met de security actoren.

Maatregelen

Concrete maatregelen om de beveiliging afdoende te regelen zijn voorzien. Gedacht kan worden aan ondermeer:

- Toegang tot informatie services is beperkt tot bekende en geauthentiseerde organisaties, die met bekende applicaties koppelen. Dit is voorzien van sterke authenticatie en toegang tot informatieservices wordt op maat geboden, afhankelijk van de organisatie
- Interactieve toegang wordt slechts geboden via Internet portalen.
- Bij het bovengaande wordt gebruik gemaakt van zonering in de infrastructuur (DMZ).
- Bovendien worden maatregelen getroffen om het gebruik te monitoren en anomalieën de detecteren en hierop tijdig maatregelen te nemen.

	Gebruik wordt gemaakt Programma VRS zorgt er gefaseerd voor dat reisdocument diensten steeds meer beschikbaar komen over meerdere kanalen waaronder internet. De eerste dienst die gerealiseerd wordt is StopID. Pas na Programma VRS zullen andere diensten beschikbaar gemaakt kunnen worden. Allereerst zal de decentrale architectuur aangepast moeten worden.

Bijlage 10: Inzicht in uitvoering van NORA principes

Onderstaand overzicht geeft een beeld in welke mate (wel/niet/gedeeltelijk) wordt voldaan aan de NORA principes bij uitvoering van het programma. We vermelden dat voordat het programma is gestart er een NORA toets op het stelsel is uitgevoerd. Met die resultaten in het achterhoofd is deze PSA tot stand gekomen. Indien gewenst kan de NORA toets worden opgevraagd bij de architecten.

		Dienstenaanbod	**Voldoet wel/niet**
B2	AP1	De dienst is zodanig opgezet, dat andere organisaties deze in eigen diensten kunnen hergebruiken.	
B3	AP2	De stappen uit het dienstverleningsproces zijn ontsloten als dienst.	
B2	AP3	De dienst vult andere diensten aan en overlapt deze niet.	
B2	AP4	De dienst is helder gepositioneerd in het dienstenaanbod.	
B2	AP5	De dienst is nauwkeurig beschreven.	
		Standaard oplossingen	
I2	AP6	De dienst maakt gebruik van standaard oplossingen.	
I1	AP7	De dienst maakt gebruik van de landelijke bouwstenen van de e-overheid.	
I2	AP8	De dienst maakt gebruik van open standaarden.	
		Kanalen	
T3	AP9	De dienst kan via internet worden aangevraagd.	
T3	AP10	De dienst kan, behalve via internet, via minimaal één ander kanaal voor persoonlijk contact worden aangevraagd.	
T3	AP11	Het resultaat van de dienst is gelijkwaardig, ongeacht het kanaal waarlangs de dienst wordt aangevraagd of geleverd.	
		Informatie	
I3	AP12	De afnemers wordt niet naar reeds bekende informatie gevraagd.	
T2	AP13	Alle gebruikte informatie-objecten zijn afkomstig uit een bronregistratie.	
T2	AP14	De dienstverlener meldt twijfel aan de juistheid van informatie aan de bron.	
I3	AP15	Het doel waarvoor informatie wordt (her)gebruikt is verenigbaar met het doel waarvoor deze is verzameld.	
T2	AP16	Alle gebruikte informatie-objecten zijn uniek geïdentificeerd.	

I2	AP17	Alle gebruikte informatie-objecten zijn systematisch beschreven.	
I3	AP18	De dienst ontsluit ruimtelijke informatie locatiegewijs	N.v.t.
		Vraaggerichtheid op een hoger plan	
B2	AP19	De dienst is opgezet vanuit het perspectief van de afnemer.	
B3	AP20	De dienst benadert geïdentificeerde afnemers op persoonlijke wijze.	
B2	AP21	De dienst is gebundeld met verwante diensten zodat deze samen met één aanvraag afgenomen kunnen worden.	
B1	AP22	Overheidsloketten verwijzen gericht door naar de dienst.	
B2	AP23	De dienst wordt na bepaalde signalen automatisch geleverd.	
B2	AP24	De dienst ondersteunt proactiviteit van dienstverleners binnen en buiten de organisatie.	
I2	AP25	De afnemer wordt geïnformeerd over de stand van zaken bij de gevraagde dienst.	
I2	AP26	De afnemer heeft inzage in de eigen informatie en het gebruik ervan.	
		Sturing en verantwoordelijkheid	
B1	AP27	Eén organisatie is verantwoordelijk voor de dienst.	
B2	AP28	Dienstverlener en de afnemer hebben afspraken vastgelegd over de levering van de dienst.	
B3	AP29	De dienstverlener draagt zelf de consequenties wanneer de dienst afwijkt van afspraken en standaarden.	
B2	AP30	De wijze waarop de dienst geleverd is, kan worden verantwoord.	
B3	AP31	De kwaliteit van de dienst wordt bestuurd op basis van cyclische terugkoppeling.	
B1	AP32	Sturing op de kwaliteit van de dienst is verankerd op het hoogste niveau van de organisatie.	
B2	AP33	De dienst voldoet aan de baseline kwaliteit.	
B1	AP34	De dienstverlener legt verantwoording af over de mate van control, in overleg met de afnemers.	
		Betrouwbaarheid	
B3	AP35	De levering van de dienst is continu gewaarborgd.	
T2	AP36	Wanneer de levering van de dienst mislukt, wordt de uitgangssituatie hersteld.	
I1	AP37	De dienstverlener en de afnemer zijn geauthenticeerd wanneer de dienst een vertrouwelijk karakter heeft.	

T3	AP38	De betrokken faciliteiten zijn gescheiden in zones.	
T1	AP39	De betrokken systemen controleren informatie-objecten op juistheid, volledigheid en tijdigheid.	
I3	AP40	De berichtenuitwisseling is onweerlegbaar.	

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Nota actief openbaar
Ja

Onze referentie
2022-0000160332

Datum
23 maart 2022

Opgesteld door
[redacted]
BZK/CZW/DS
[redacted]

Samengewerkt met

Bijlage(n)
0

Aan Staatssecretaris BZK
Van CZW/DGOO

nota

0 Nota consultatie wijziging Paspoortwet ivm centrale voorziening biometrische gegevens

Met opmerkingen [MS1]: 25/3 [redacted]

Aanleiding

De wijziging van de Paspoortwet ivm de centrale opslag (voorziening) voor biometrische gegevens voor reisdocumenten (gezichtsopname, handtekening en vingerafdrukken) is gereed voor consultatie.

Geadviseerd besluit

- Instemmen met het in consultatie brengen van dit voorstel van rijkswet.
- Buiten reikwijdte [redacted]

Kern

De wijziging van de Paspoortwet is onderdeel van het programma Verbeteren Reisdocumentenstelsel (VRS). Op 16 maart jl. heeft u de Kamer geïnformeerd over de voortgang van het programma. Fase 2 hiervan, de centrale opslag van biometrische gegevens, vraagt wetgeving. In de brief is aangegeven dat het consultatieproces naar verwachting in het eerste kwartaal van 2022 zal aanvangen. De consultatieversie wordt hierbij aan u voorgelegd.

Met de wijziging van de Paspoortwet (rijkswet) wordt een centrale voorziening gerealiseerd waarin de biometrische aanvraaggegevens ten behoeve van reisdocumenten worden opgeslagen: de gezichtsopname, twee vingerafdrukken (slechts tijdelijk voor productiedoeleinden, de periode tussen de aanvraag en de uitreiking van het reisdocument) en de handtekening van betrokkene. Nu worden deze gegevens nog decentraal opgeslagen.
De centrale voorziening en het (per 1 januari 2021 gerealiseerde) basisregister reisdocumenten (bevat de overige aanvraaggegevens) zullen de twee cruciale digitale voorzieningen vormen voor de verwerking van de gegevens voor reisdocumenten.

Het voorstel met de memorie van toelichting zijn gereed voor consultatie (zie bijlage nr. 2). Buiten reikwijdte

Toelichting
Het voorstel is onderdeel van de tweede fase van VRS (centrale voorziening voor biometrie) en is gereed voor consultatie. In de eerste fase is het basisregister reisdocumenten gerealiseerd.
Met het voorstel wordt een uitdrukkelijke wettelijke grondslag voor de centrale voorziening voor biometrische gegevens gecreëerd.
Met de voorgestelde wijziging van de Paspoortwet worden geen extra biometrische of andere gegevens verzameld dan thans het geval is. Het enige verschil ten opzichte van de bestaande situatie is dat de biometrische gegevens voortaan centraal zullen worden opgeslagen in plaats van decentraal bij de afzonderlijke uitgevende instanties. De uitgevende instanties blijven verwerkingsverantwoordelijk voor de in de voorziening opgenomen gegevens, zoals thans het geval is.

Op de grondrechtelijke gevolgen van de verwerking van persoonsgegevens, te weten het recht op privacy en de overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), in het bijzonder de noodzaak om van het in artikel 9 van de AVG bedoelde verbod om bijzondere categorieën van persoonsgegevens te verwerken af te wijken om redenen van zwaarwegend algemeen belang, is uitvoerig ingegaan in paragraaf 3 van het algemeen deel van de memorie van toelichting. Omdat de vingerafdrukken en de gezichtsopname als biometrische gegevens in de zin van de AVG dienen te worden aangemerkt, vallen zij onder het regime voor de verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9 van de AVG. Zoals in paragraaf 3 van het algemeen deel uitgebreid is toegelicht, is aan de normen van de AVG voor de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon (artikel 9 van de AVG) voldaan.

Buiten reikwijdte

Noodzaak
De centrale voorziening is nodig om de biometrische gegevens voor de uitgevende instanties centraal beschikbaar te stellen. Hiermee wordt het aanvraag- en uitgifteproces en daarmee de dienstverlening verbeterd. De gegevens zijn thans slechts decentraal aanwezig in het reisdocumentenaanvraag- en archiefstation (RAAS) van de uitgevende instantie die het document heeft uitgegeven. Indien de instantie die de aanvraag ontvangt een andere is dan die het te vervangen reisdocument heeft uitgegeven, moet deze bij twijfel aan de identiteit van de aanvrager de gegevens bij de vorige uitgevende instantie per e-mail of fax opvragen. Dit is een inefficiënte en uit het oogpunt van gegevensbeveiliging kwetsbare werkwijze. Met de komst van de centrale voorziening behoeven de

RAAS-en niet meer te worden vervangen en kunnen deze worden uitgefaseerd. Het voorstel is tevens nodig om op termijn plaatsonafhankelijke dienstverlening voor het verstrekken van reisdocumenten mogelijk te maken, zoals de NVVB en VNG hebben verzocht in hun reactie op de consultatie van het voorgaande voorstel van rijkswet voor de wijziging van de Paspoortwet ten behoeve van elektronische identificatie en de invoering van een vernieuwd basisregister reisdocumenten.

Het voorstel bevat naast de centrale voorziening voor biometrische gegevens de volgende onderdelen:

- het schrappen van de vermelding van het geslacht op de Nederlandse identiteitskaart, als voortvloeisel van het waar mogelijk beperken van onnodige geslachtregistratie zoals in het Regeerakkoord 'Vertrouwen in de toekomst'[1] van 2017 is opgenomen en in Kamerbrieven[2] is aangekondigd;
- de aanvulling van het basisregister met gegevens over vermiste, gestolen of van rechtswege vervallen documenten en gegevens over de voortgang van een aanvraag voor een reisdocument;
- de omvorming van de bestaande reisdocumentenadministratie die de uitgevende instanties voeren tot een 'restadministratie" waarin alleen nog overige documenten en gegevens (anders dan de biometrische gegevens en de verplichte aanvraaggegevens) zullen worden opgenomen die de aanvraag ondersteunen (gaat met name om papieren documenten).

Politieke context
De centrale voorziening biometrie kan de zorg oproepen dat bij inbraak/lek in dit systeem biometrische gegevens van personen openbaar en/of misbruikt kunnen worden. Daarom wordt er extra aandacht besteed aan de beveiliging van de centrale opslag. De gezichtsopnames, handtekeningen en vingerafdrukken zijn – bij een inbraak in de centrale opslag – niet te relateren aan een persoon. Ook is niet te herleiden welke gezichtsopnames, handtekeningen en vingerafdrukken bij elkaar horen. Tot slot is er de zorg dat deze gegevens voor opsporingsdoeleinden zouden kunnen worden ingezet. Opsporingsinstanties kunnen in gevallen waarin zij daartoe bevoegd zijn een gemotiveerd verzoek doen aan de uitgevende instantie om deze gegevens aan hen te verstrekken voor een concreet onderzoek. Dit verzoek wordt per geval beoordeeld door de uitgevende instantie en beperkt zich tot uitsluitend het verstrekken van de gezichtsopnames en/of handtekeningen. Dit is al zo in het huidige systeem en wordt niet anders.

Eerder, in 2009 is getracht met een voorstel tot wetswijziging verbeteringen in het reisdocumentstelsel aan te brengen door centralisatie van systemen. Onderdelen van de wijzigingen toen waren het permanent opslaan van vingerafdrukken in een centrale database onder verantwoordelijkheid van de Minister en de verstrekking van vingerafdrukken uit de centrale database aan het Openbaar Ministerie. Op verzoek van de Tweede Kamer zijn deze ontwikkelingen gestopt. Deze beide elementen zijn geen onderdeel van het voorliggende voorstel noch VRS.

[1] Regeerakkoord 'Vertrouwen in de toekomst', blz. 10. Bijlage bij Kamerstukken II 2017/18, 34 700 nr. 34
[2] *Kamerstukken II* 2019/20, 34650, nr. I en *Kamerstukken II* 2020/2, 34650, nr. L.

Financiële/juridische overwegingen
5.1.2.b

Krachtenveld
De Kamer wordt met voortgangsbrieven over het programma VRS geïnformeerd. Daarin is gecommuniceerd dat er een wetsvoorstel in voorbereiding is voor een centrale voorziening voor biometrische gegevens van reisdocumenten. Bij de behandeling van het voorstel van rijkswet voor de wijziging van de Paspoortwet ten behoeve van de uitvoering van de Verordening 2019/1157 die verplicht tot het opnemen van vingerafdrukken op de Nederlandse identiteitskaart, heeft de Eerste Kamer reacties ontvangen van de vereniging Vrijbit en de stichting Privacy First. Deze reacties hadden betrekking op het opnemen van vingerafdrukken op de Nederlandse identiteitskaart en leidden niet tot een wijziging van het toen aanhangige wetsvoorstel.

Strategie
De voorgeschreven wetgevingsprocedure voor een rijkswet wordt gevolgd.

Uitvoering
Hoofdstuk 5 van de memorie van toelichting beschrijft de uitvoeringsaspecten. Tijdens de consultatieperiode zal de Rijksdienst voor Identiteitsgegevens (RvIG) een uitvoeringstoets uitvoeren.

Communicatie
Het voorstel van rijkswet wordt ter consultatie voorgelegd aan de Autoriteit Persoonsgegevens, de toezichtsorganen gegevensbescherming in het Caribisch deel van het Koninkrijk, de Vereniging van Nederlandse Gemeenten (VNG), de Nederlandse Vereniging voor Burgerzaken (NVVB), de landen van het Koninkrijk alsmede de openbare lichamen. Daarnaast wordt het voorstel ter consultatie gelijktijdig op internet gepubliceerd. De consultatieperiode zal worden gebruikt voor een uitvoeringstoets door de RvIG, de wetgevingstoets door J&V en het voorleggen aan het Adviescollege Toetsing Regeldruk (ATR).

Informatie die niet openbaar gemaakt kan worden
Persoonsgegevens van ambtenaren

Motivering
In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd.

Bijlagen

Volgnummer	Naam	Informatie
1	Buiten reikwijdte	
2	2 Wetsvoorstel en memorie van toelichting	
3	[redacted]	