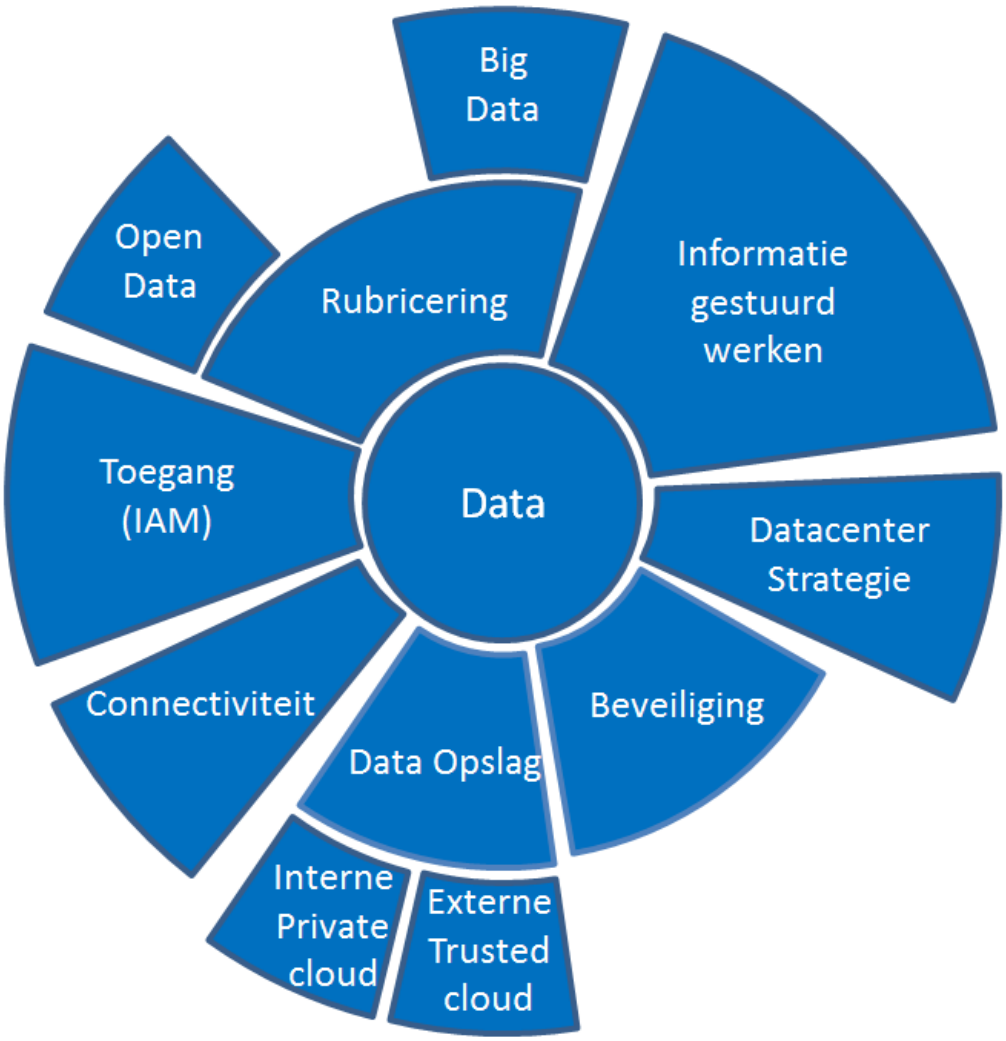
ONGERUBRICEERD

GeTIJ 2017-2025

Strategische Uitgangspunten Gemeenschappelijke
Technische Infrastructuur Justitie 2017-2025

Versie 1.0 (definitief)



Colofon

Afzender	**Directie Informatisering en Inkoop** Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag
Contactpersoon	Zie bijlage I
Auteurs	Zie bijlage I

Versiebeheer

Versie	**Datum**	
0.1	4 augustus 2017	CTO's JenV & afgevaardigden
0.2	28 september 2017	Review versie 0.1
0.3	25 oktober 2017	Concretisering & alignment veranderaanpak (bijlage 3) Alignment met Architectuur JenV
1.0	13 november 2017	CTO Overleg JenV

Tabel 1. Versiebeheer

Inhoud

Managementsamenvatting

De gemeenschappelijke infrastructuur van JenV is het fundament waarop zowel het primair proces als de bedrijfsvoering opereren. Deze infrastructuur dient optimaal de digitaliseringsdoelstellingen van JenV te ondersteunen.

In deze door én voor Chief Technology Officers (CTO's) opgestelde rapportage zijn de strategische uitgangspunten geformuleerd op functioneel niveau voor de periode 2017-2025 voor de domeinen Gegevensdiensten, Datacentrumdiensten, Connectdiensten en Toegangsdiensten. Daarbij is aangegeven dat op de vier bovengenoemde domeinen in de komende jaren veel ontwikkelingen worden verwacht waarbij binnen JenV een behoefte is uitgesproken voor een functioneel vergezicht. Hoewel de vier domeinen in deze rapportage afzonderlijk worden behandeld is er een sterke onderlinge afhankelijkheid te onderkennen. In relatie tot een datagedreven JenV is een verfijnd samenspel tussen de domeinen nodig om de digitaliseringsdoelstellingen van JenV maximaal te kunnen ondersteunen. Het JenV infrastructuurfundament dient hiervoor betrouwbaar, flexibel op- en af te schalen en bovenal wendbaar te zijn. Met dit laatste wordt het vermogen bedoeld om nieuwe technologie snel te kunnen adapteren. Samenvattend zien we in hoofdlijnen in de komende jaren de volgende beelden. Deze beelden zijn in de rapportage zelf uitgewerkt per domein in een visie met noties en vervolgstappen.

Algemeen

De infrastructuur van JenV faciliteert optimaal het primaire proces en moet daarvoor wendbaar en flexibel zijn. Het toepassen van integrale maatregelen ten behoeve van het mitigeren van cybersecurity en privacy risico's is de komende jaren essentieel. Dreigingen vanaf Internet door criminele organisaties en Overheden nemen substantieel toe. Om deze dreigingen te kunnen weerstaan is een nauwe samenwerking met eigen onderdelen, maar ook commerciële partijen nodig. JenV dient jong talent te blijven benutten maar ook te werven. Doordat diensten vaker buiten de deur, maar ook bij andere onderdelen worden afgenomen is het noodzakelijk een regieorganisatie in te richten die over de ketens heen de regie voert. Bovenal is een trend waar te nemen waarbij medewerkers onafhankelijk van de tijd, plaats of apparaat willen kunnen werken in een veilige omgeving.

Gegevensdiensten

Het belang van data en het daardoor kunnen bewegen naar een informatie gestuurde JenV-keten nemen in zeer sterke mate toe. Het primaire proces zal substantieel veranderen doordat vanuit de Gegevensdiensten geleverde functionaliteiten leiden tot nog niet eerdere onderkende verbanden en inzichten. Hierdoor kan JenV efficiënter en doeltreffender haar diensten verlenen aan de burger en bedrijfsleven. Door deze verandering in de informatievoorziening beweegt JenV steeds meer van een ketenpartner naar een netwerkpartij die partijen (ook buiten JenV) aan elkaar verbindt.

Datacentrumdiensten

De toepassing van Cloud-technologie vanuit de zogenoemde Trusted Cloud-aanbieders binnen en buiten de Rijksoverheid vereist een sterke mate van standaardisatie. Zo wordt een uniform landschap gerealiseerd op zowel het niveau van de infrastructuur als op het niveau van de applicaties. Onderdelen van JenV kunnen zich ten behoeve van de gestandaardiseerde diensten zowel opstellen als aanbieder of afnemer. De

(infrastructurele) beheerlast wordt zo substantieel verlaagd, de continuïteit van de eigen organisatie wordt sterk verbeterd, en JenV kan zich ontwikkelen tot een regie-organisatie. Bovendien biedt de toepassing van Cloud-technologie binnen- en buiten JenV de mogelijkheid om capaciteit op- en af te schalen. In plaats van gebruik te maken van op investering gebaseerde financiële modellen maakt JenV gebruik van operationele financieringsmodellen.

Connectdiensten

Connectdiensten zijn essentieel voor de verdere digitalisering binnen JenV. In toenemende mate wordt gevraagd naar bandbreedte en naar snelheid. Het netwerk voldoet in de komende jaren aan de volgende kenmerken:

- Het netwerk is schaalbaar, open en transparant en voorziet in de toenemende behoefte aan samenwerkingen met ketenpartners en onderdelen binnen JenV, onder andere in Rijksverzamelpanden, maar ook bij de ontsluiting van het RijksOverheidsNetwerk (RON);
- Het netwerk zorgt voor transparante uitbreiding naar publieke vertrouwde Cloud-aanbieders[1];
- Het netwerk borgt in samenhang met omliggende diensten de vertrouwelijkheid en integriteit van informatie door het faciliteren van security zones. Encryptie technieken worden hierbij toegepast;
- Security diensten, evenals Toegangsdiensten worden centraal aangeboden door een door JenV geselecteerde partij.

Toegangsdiensten

Samenwerking over organisatiegrenzen heen neemt exponentieel toe de komende jaren. De samenleving digitaliseert steeds verder. Het organiseren van toegang tot data is een randvoorwaarde in een omgeving waar ook de dreigingen toenemen. Dit vraagt om het gemeenschappelijk ontwikkelen van expertise en de uitbouw van de huidige Toegangsvoorzieningen van JenV en zijn onderdelen, naast een gemeenschappelijke aanpak op het niveau van de overheid en JenV. Dit moet op een zodanige manier gebeuren dat de samenwerking binnen het primaire proces maar ook de bedrijfsvoering op een veilige en gebruikersvriendelijke manier kan worden gefaciliteerd. Dit kan vooral worden bereikt door de toepassing van federatieve technieken.

Vervolg

De noodzakelijke verdere ontwikkeling in samenhang van deze domeinen tot 2025 is een behoorlijke veranderopgave en vraagt om investeringen. De verandering zal vertaald moeten worden in activiteiten en onderdeel uit maken van de informatieplannen en jaarplannen van JenV voor 2018 tot 2025. In bijlage 3 van het rapport GeTIJ staat hiervoor een handreiking op hoofdlijnen.

Niet vergeten mag worden dat op verzoek van de opdrachtgever voor deze rapportage 'out of the box' is gedacht. Dat wil zeggen dat de domeinen zijn benaderd buiten de huidige financiële- en beleidskaders. Dit is ook relevant voor wat betreft de veranderaanpak. De handreiking voor een veranderaanpak (zie bijlage 3) moet, indien besloten wordt deze daadwerkelijk uit te voeren (of delen daarvan), verwerkt worden in de informatieplannen / jaarplannen van JenV. De besluitvorming over de veranderaanpak zal voorgelegd dienen te worden aan de CIO Raad. De uitvoering van het veranderplan valt buiten het project GeTIJ.

[1] Dit zijn door JenV geselecteerde aanbieders waarmee sterke contractuele afspraken zijn gemaakt om integriteit, beschikbaarheid en vertrouwelijkheid van data is gewaarborgd. De verzameling van JenV eigen infrastructuur gecombineerd met publieke aanbieders wordt de Trusted Cloud genoemd.

Hoofdstuk 1. Inleiding

Voor u ligt de rapportage 'Strategische Uitgangspunten Gemeenschappelijke Technische Infrastructuur van Justitie 2017-2025' (GeTIJ). Doelstelling van dit rapport is het formuleren van strategische uitgangspunten richtinggevend op functioneel niveau voor de periode 2017-2025 ten behoeve van de gemeenschappelijke technische infrastructuur van Justitie. Deze rapportage is opgesteld voor én door het CTO-overleg, en wordt vastgesteld door het CTO-overleg JenV.

De rapportage heeft betrekking op vier domeinen van de Enterprise Architectuur Rijk (EAR), te weten: Gegevensdiensten (GD), Datacentrumdiensten (DCD), Connectdiensten (CD) en Toegangsdiensten (TD)[2]. Deze dienstverleningsdomeinen zijn een fundament voor een verdere digitalisering binnen JenV. De digitalisering van onder meer de primaire processen is belangrijk om deze primaire processen efficiënter, effectiever en transparanter te maken. Op verzoek van het CTO-overleg en het Centraal Strategisch Beheer (CSB) JenV is deze rapportage opgesteld. Daarbij is aangegeven dat op de vier bovengenoemde domeinen in de komende jaren veel ontwikkelingen worden verwacht waarbij binnen JenV er een behoefte is uitgesproken voor een functioneel vergezicht. Er moeten keuzes voor de vernieuwing of aanpassing van de infrastructuur gemaakt worden. Keuzes die passen bij een gedragen vergezicht of bewust daarvan afwijken indien dit nodig mocht zijn.

1.1 Werkwijze GeTIJ

Deze rapportage is opgesteld door leden van het CTO-overleg JenV (of hun vervangers) en het projectteam GeTIJ. In dit kader zijn bij smaakmakers binnen JenV maar ook daarbuiten beelden opgehaald en getoetst in relatie tot de geselecteerde EAR domeinen[3]. Daarnaast zijn er relevante rapportages geraadpleegd zoals de 'Informatie Strategie JenV 2017-2022'[4]. Deze rapportage is opgesteld op basis van huidige inzichten en marktbewegingen. Nieuwe ontwikkelingen van substantiële omvang kunnen mogelijk leiden tot aanpassing van de in deze rapportage weergeven visie.

Niet vergeten mag worden dat op verzoek van de opdrachtgever 'out of the box' is gedacht. Dat wil zeggen dat de domeinen zijn benaderd buiten de huidige financiële- en beleidskaders. Dit is ook relevant voor wat betreft de veranderaanpak. De handreiking voor een veranderaanpak (zie bijlage 3) moet, indien besloten wordt deze daadwerkelijk uit te voeren (of delen daarvan), verwerkt worden in de informatieplannen / jaarplannen van JenV. De besluitvorming omtrent de veranderaanpak zal voorgelegd dienen te worden aan de CIO Raad (SBR en BR). De uitvoering van het veranderplan valt buiten het project GeTIJ[5].

---

[2] Zie verder de 'Kennisbank van de Enterprise Architectuur Rijksdienst' - http://www.earonline.nl. Gehanteerde definities in deze rapportage kunnen afwijken van de formele EAR definities of patronen.

[3] Zie bijlage 1 'Betrokkenen'.

[4] Zie bijlage 2 'Geraardpleegde documenten'.

[5] GeTIJ met de bijbehorende veranderaanpak zal **periodiek** tegen het licht gehouden moeten worden; in hoeverre zijn de uitgangspunten nog relevant en welke aspecten kunnen opgepakt worden in het jaar daarop.

1.2 Leeswijzer

In hoofdstuk 2 staan de domein overstijgende noties die zijn opgehaald tijdens het traject GeTIJ. In de daarop volgende hoofdstukken worden de domeinen behandeld, hoofdstuk 3 GD, 4 DCD, 5 CD en 6 TD. Deze hoofdstukken zijn (per domein) als volgt ingedeeld:

1. Samenvatting Korte samenvatting van het betreffende domein;
2. Algemeen Algemene, inleidende beschouwing;
3. Visie Doorkijk naar 2025 voor het betreffende domein;
4. Noties Beschrijving van de noties voor het betreffende domein;
5. Uitgangspunten Komen tot een concretisering van de noties (vervolgstappen).

In bijlage 1 staat een overzicht van de personen betrokken bij het opstellen van deze rapportage. In bijlage 2 een overzicht van de documenten die zijn geraadpleegd. In bijlage 3 staat per GeTIJ domein een handreiking op hoofdlijnen voor een veranderaanpak.

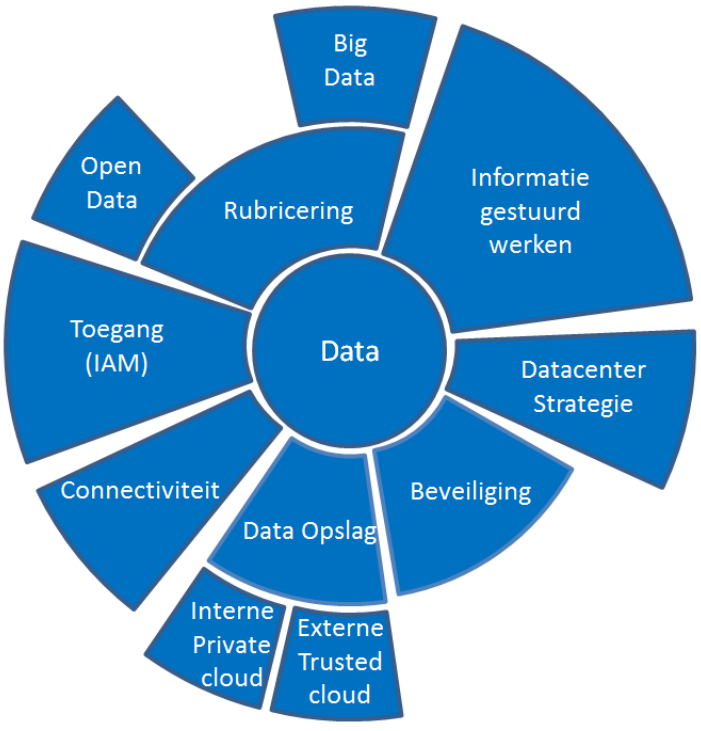
Los van dit rapport is een praatplaat GeTIJ opgeleverd. Op bondige wijze wordt daarin het resultaat van GeTIJ weergegeven.

Hoofdstuk 2. Algemene noties

Hoofdstuk 2 bevat de algemene noties die de domeinen van GeTIJ overstijgen. De algemene noties zijn ook opgesteld in het kader van bijvoorbeeld de 'Informatie Strategie JenV 2017-2022' en het 'Rapport Maak Waar' (zie bijlage 2 'Documenten Geraadpleegd'). Om deze reden worden hier alleen die noties meegenomen die in het kader van de 'Visnetactie'[6] met nadruk zijn genoemd in relatie met de infrastructuur van JenV.

2.1 Samenhang GeTIJ domeinen

Hoewel de in dit rapport beschreven EAR domeinen losstaand zijn opgenomen, dient opgemerkt te worden dat de afzonderlijke domeinen een sterke relatie met elkaar hebben. We bewegen binnen JenV naar een datagedreven organisatie, een zeer belangrijk aspect van de digitale transformatie van de bedrijfsvoering en primaire processen. De centrale doelstelling hiervan is dat de infrastructuur het efficiënter, effectiever en transparanter maken van het primaire proces en de bedrijfsvoering faciliteert.



Figuur 1 Overzicht samenhang datagedreven JenV

Om enerzijds toegang te krijgen tot deze data en anderzijds deze data relevant te maken is een verfijnd samenspel nodig tussen de in deze rapportage beschreven domeinen. Zo faciliteren toegangsdiensten (federatieve) geautoriseerde toegang tot informatie. Datacentrumdiensten (Trusted Cloud) faciliteren de resources voor het kunnen opslaan, raadplegen en aanpassen van informatie. Gegevensdiensten zorgen

[6] Oriënterende bijeenkomsten met partijen binnen en buiten JenV in het kader van GeTIJ.

voor het classificeren van data, een gestructureerde opslag in een machine leesbaar formaat uitwisselen, verrijken en registeren van informatie. Connectdiensten zorgen ervoor dat informatie op een veilige en efficiënte en veilige) wijze wordt getransporteerd.
De gekozen uitgangspunten/vervolgstappen in deze rapportage zijn nodig om de digitalisering binnen JenV optimaal te kunnen faciliteren. In de betreffende hoofdstukken zal naar relevante diensten (andere domeinen) worden verwezen.

2.2 Noties

2.2.1 Belang van integrale security maatregelen en ICT-diversiteit neemt sterk toe

Er is meer dan ooit een stijging te zien van cybercriminaliteit gericht op het verkrijgen van waardevolle informatie of het stilleggen van de dienstverlening. Vanuit financiële, politieke, ideologische of activistische drijfveren worden massale of gerichte aanvallen uitgevoerd. Deze aanvallen worden zowel door criminele organisaties als Overheden van andere landen uitgevoerd en zullen zich met name richten op software met een groot marktaandeel. Een 'software-monocultuur' met markt-leidende software maximaliseert immers de kans getroffen te worden. JenV en de samenleving als geheel kunnen hier grote schade van ondervinden.

Fijnmazige analyses van het Internet verkeer zijn nodig om ongewenst gedrag, of concrete dreigingen tegen ons land de kop in te drukken. Ongetwijfeld zal de discussie over door de staat gecontroleerd Internet in Nederland de komende jaren gevoerd gaan worden.
Daarnaast is mogelijk om het risico te verminderen door ICT-diversiteit te integreren in het beleid rondom strategisch leveranciersmanagement wanneer nieuwe systemen worden aangeschaft of ontwikkeld. Door rekening te houden met ICT-diversiteit wanneer legacy-systemen worden vervangen, kan op termijn geleidelijk een meer divers ICT-landschap ontstaan en dat verhoogt de weerbaarheid van JenV tegen mogelijke aanvallen.

2.2.2 Tijds, plaats en apparaat onafhankelijk werken

Er is steeds meer behoefte aan tijd-, plaats- en apparaat onafhankelijk werken (TPAW). Het leveren van goede kwalitatieve connectiviteit is hiervoor een vereiste. Passende beveiligingsmaatregelen dienen genomen te worden om context afhankelijk passende beveiliging te kunnen leveren. Concreet kan dit betekenen dat afhankelijk van ***wie*** je bent, welke ***rol*** je hebt, op welke ***locatie*** je bent als medewerker specifieke informatie kunt inzien. Dit vereist een gebalanceerd samenspel tussen de GeTIJ domeinen.

2.2.3 JenV beweegt naar domein en landelijk overstijgende regievoering over in- en externe leveranciers en afnemers

Door het steeds verder integreren, automatiseren van de totstandkoming van diensten, platformen en infrastructurele bouwblokken neemt de infrastructurele beheerlast van deze diensten, platformen en bouwblokken af. Hierbij zien we tevens de trend dat standaard -zowel werkplek- als datacenter gerelateerde - diensten meer en meer worden afgenomen bij andere onderdelen of bij derden uit de markt. Hierdoor is enerzijds een verschuiving van operationeel beheer naar regievoering te zien over de diensten die worden afgenomen bij dienstverleners. Anderzijds zien we als gevolg hiervan een verandering in de gevraagde competenties van JenV medewerkers.

Typerend voor de situatie is dat van operationele medewerkers wordt verwacht dat zij op een hoger abstractieniveau gaan werken. De nadruk van hun werkzaamheden gaat

liggen op de innovatie van het betreffende domein. Daarnaast wordt de focus gericht op het aansturen van in- en externe leveranciers en afnemers van diensten op de dienstprestaties.

2.2.4 Aantrekken van talent is een essentieel aandachtspunt

In het huidige aantrekkende economische klimaat is het een uitdaging voor de Rijksoverheid (jong) talent binnen te halen met relevante kennis op de deelgebieden van GeTIJ. De specifieke kennis is nodig om de digitale transformatie binnen JenV vorm te geven is nu veelal bij extern ingehuurde consultants, project managers of engineers belegd. Om de langdurige ontwikkeling en continuïteit van de GeTIJ-domeinen te garanderen zijn - naast het daadwerkelijk beschikbaar stellen van reeds aanwezige kennis binnen JenV - hoog opgeleide personen nodig, bijvoorbeeld door schoolverlaters of starters op de arbeidsmarkt te werven. Specifiek is er kennis nodig op de gebieden van data-analyse, security (onder andere IAM), Cloud en netwerken.

2.2.5 Kwaliteit is een continue factor, kosten vaak eenmalig

JenV heeft in de afgelopen jaren een complex maar betrouwbaar infrastructuurlandschap opgebouwd waarmee de huidige primaire processen worden bediend. Dit infrastructuurlandschap zal enerzijds complexer worden door de verdere digitalisering van verschillende JenV onderdelen en processen, anderzijds is wendbaarheid gewenst om snel in te kunnen spelen op deze veranderende wereld. Complexiteit en wendbaarheid lijken contradicties. Maar deze kunnen hand in hand gaan door onder meer brede standaarden te adapteren en verregaand te automatiseren.
Het verandervermogen van JenV als innoverend ministerie kan vooral bereikt worden door te combineren. Het kan dan gaan om een combinatie van al bestaande oplossingen, diensten of platformen met reeds bewezen innovaties uit de markt. JenV volgt de markt bij het adapteren van nieuwe technologie. Flexibiliteit in de mate van aanpasbaarheid van de infrastructuur en het op- of afschalen van de nodige capaciteit zijn hierbij van belang. De flexibilisering van het gebruik én onderliggende contracten ten behoeve van de GeTIJ-domeinen leveren niet direct kostenbesparingen op. Deze investeringen zijn echter gelegitimeerd doordat de efficiëntie en het verandervermogen van JenV groter wordt en de meetbaarheid van de dienstverlening toeneemt.

Slotopmerking bij dit punt; wel dient in de gaten gehouden te worden dat over het algemeen een kostenbesparing wordt snel ingeboekt en daarna vergeten, kwaliteit van de dienstenverlening staat echter continu in de schijnwerpers.

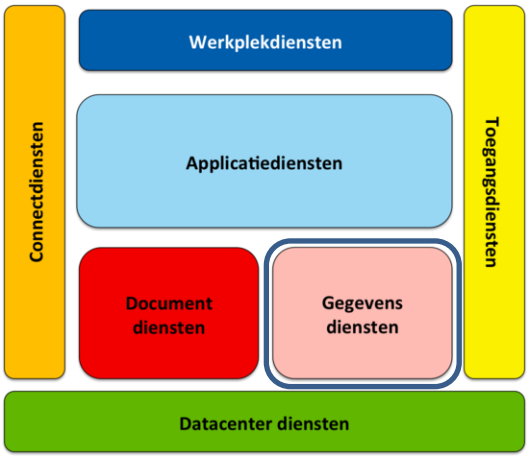
Hoofdstuk 3. Gegevensdiensten

Hoofdstuk 3 bevat de beelden die bij de onderdelen en marktpartijen die bij GeTIJ betrokken zijn, opgehaald zijn. Het gaat hier om de relevante ontwikkelingen binnen het domein Gegevensdiensten.

3.1 Samenvatting

Het belang van data en het daardoor kunnen bewegen naar een informatiegestuurde JenV-keten nemen in zeer sterke mate toe. Het primaire proces zal substantieel veranderen doordat vanuit de Gegevensdiensten geleverde functionaliteiten leiden tot nog niet eerdere onderkende verbanden en inzichten. Hierdoor kan JenV efficiënter en doeltreffender haar diensten verlenen aan de burger en bedrijfsleven. Door deze verandering in de informatievoorziening beweegt JenV steeds meer van een ketenpartner naar een netwerkpartij die partijen (ook buiten JenV) aan elkaar verbindt.

3.2 Algemeen



Figuur 2 EAR domein Gegevensdiensten

Onze samenleving vereist steeds meer een door datagedreven overheid. Data is het nieuwe goud dat JenV in de komende jaren zal helpen bij haar maatschappelijke opgaven. Door het faciliteren van nog niet eerder ontdekte verbanden en inzichten, door het efficiënter maken van processen en procedures wordt besluitvorming binnen het primaire proces efficiënter en relevanter. Hierbij is het essentieel dat de informatiepositie van JenV-functionarissen adequaat wordt vormgegeven. Gegevensdiensten zijn diensten die zorgdragen voor het in context kunnen delen, raadplegen, bewerken, en opslaan van informatie ten behoeve van het primair proces (Kinder-, Straf-, Vreemdelingen- en Slachtofferketen) en bedrijfsvoering van JenV en zijn partners[7]. Gegevensdiensten faciliteren in het efficiënt uitwisselen van gestandaardiseerde informatie. Deelnemende partijen kunnen de gegevens verrijken ten behoeve van het verbeteren van de informatiepositie van de onderdelen van JenV, en hun ketenpartners bij het uitvoeren van hun wettelijke taken.

De digitalisering van processen en ketens binnen JenV ten behoeve van het efficiënt bedienen van zowel burgers als bedrijven vereisen een betrouwbare informatievoorziening. Er is een duidelijke koerswijziging binnen JenV te onderkennen. Nu wordt documentgedreven gewerkt, maar er is een ontwikkeling gaande naar meer informatiegestuurd werken[8]. Bovendien neemt de informatie ook toe door invloeden van buitenaf. Denk aan de invloed van de zogenaamde “betrouwbare” sociale media die in toenemende mate een nieuwe informatiestroom van burgers en bedrijven genereert, maar ook een samenwerkingsplatform voor bijvoorbeeld opsporingstaken. Ook is een

[7] De hier gegeven definitie wijkt af van de formele EAR definitie, ten behoeve van de context van het document is deze aangepast.

[8] De verwachting is dat documenten nooit volledig zullen verdwijnen, echter zal het belang van het gebruik van documenten zoals we deze nu kennen veranderen.

trend zichtbaar waarbij de overheid meer met bedrijven gaat samenwerken in het kader van digitale identiteiten.

Voorbeeld MH 17

In de nasleep van de MH17 ramp heeft een groep vrijwilligers en journalisten[9] een eigen onderzoek uitgevoerd waarbij onder meer geaggregeerde social media informatie is gebruikt als bewijslast.

Voorbeeld I: Betrokkenheid burgers in de opsporing

Deze steeds veranderende informatievoorziening leunt vooral op betrouwbare (externe) gegevensbronnen die afhankelijk van de context de juiste informatie leveren. Het kan hierbij gaan om samengestelde (geaggregeerde) informatie zijn of om ruwe ongestructureerde data dat tot bruikbare informatie door kunstmatige intelligentie (algoritmen) wordt omgevormd.

3.3 Visie

De Justitieketen is – als onderdeel van de samenleving - gedigitaliseerd. Datageneratie en –uitwisseling in het primaire proces (ook over organisatie- en landsgrenzen heen) en met burgers en bedrijven nemen exponentieel toe. Data, informatie en gegevens bieden daarbij nog ongekende mogelijkheden tot het optimaliseren van primaire processen. Er wordt informatiegestuurd gewerkt. Zo wordt een optimale informatiepositie voor de JenV medewerker gecreëerd. Om de informatiepositie te versterken wordt bijvoorbeeld gebruik gemaakt van kunstmatige intelligentie. Hierdoor kan vanuit informatieperspectief een integraal beeld van een persoon of zaak worden gereconstrueerd. Documenten zijn hierbij van een steeds minder groot belang, data vormt de basis van deze beweging. Cruciaal daarbij is het organiseren van betrouwbare data (informatie en gegevens) en het op afgewogen wijze ter beschikking kunnen stellen daarvan aan anderen.

3.4 Noties

In deze paragraaf worden de noties beschreven die zijn opgehaald gedurende de sessies met de betreffende onderdelen en marktpartijen.

3.4.1 Het belang van gegevensdiensten in de JenV-keten

Juistheid van gegevens is essentieel voor het nemen van de juiste beslissingen binnen het primaire proces. Het adequaat vormgeven van de informatiepositie van een JenV medewerker is daarom essentieel. Het uniform gebruik van gegevensdiensten binnen de afzonderlijke ketens is belangrijk opdat er ononderbroken informatiestromen ontstaan (zoals een ononderbroken ID keten, ononderbroken document keten, een ononderbroken rechtsfeiten en rechtsgevolgen keten, enzovoorts).

Bij JenV is een duidelijke verschuiving te onderkennen in de wijze waarop ten behoeve van het primair proces om wordt gegaan met informatie. Werkte men tot op enkele jaren geleden nog volledig op basis van documenten (aangevuld met informatie uit administraties, registers en archieven), nu werkt men steeds meer op basis van (samengestelde) informatie en documenten.

[9] Deze groep is ook wel bekend onder de naam 'Bellingcat'

In de komende jaren krijgt JenV te maken met crossmediale informatiestromen van verschillende partijen (overheid, private partijen, burgers en sensornetwerken). Hierdoor kan JenV informatiegestuurd werken. Er kan - ondanks de grote hoeveelheid aan informatie - efficiënter gewerkt worden. Efficiëntie wordt vooral bereikt door het bruikbaar maken van gestructureerde, maar ook ongestructureerde data. Dit kan door het toepassen van innovatieve technologieën.

3.4.1.1 Rijksdata open en transparant voor de buitenwereld

Transparante en efficiënte dienstverlening naar burger en bedrijfsleven zijn belangrijke uitgangspunten voor de Rijksoverheid, maar specifiek ook vanuit de JenV-keten. Het publiekelijk openstellen van gegevens(verzamelingen) is hierbij een belangrijk aspect. Het openstellen van data brengt daarbij nog de nodige uitdagingen met zich mee (denk aan onder andere privacy wet- en regelgeving), maar ook met betrekking tot het actief openstellen van ongestructureerde data (besluiten, rapporten, verslagen, enzovoorts). Dit betekent dat er eisen gesteld worden aan onder andere:

- De kwaliteit van data (hoe actueel is de data en hoe betrouwbaar is het).
- Classificatie van data (hoe borg je privacy en vertrouwelijkheid).
- Standaardisatie van data (vast format voor het publiceren van data).
- Toevoegen van context (context aanbrengen ten behoeve van de leesbaarheid door burger en bedrijfsleven).
- Innovatieve technologie (het geautomatiseerd ter beschikking stellen van data rekening houdend met classificatie en context).

Om de kwaliteitseisen te realiseren dient enerzijds uit de markt specialisten te worden aangetrokken (data-analisten), anderzijds dient een centrale regie-organisatie te worden ingericht om grip te houden op de data en de publicatie ervan.

3.4.2 Rubricering (categorisering) van informatie is essentieel

De JenV-keten werkt vaak in verschillende contexten met gevoelige informatie. Niet alle informatie kan met een onderdeel of met de burger worden gedeeld. Daarom is rubricering van informatie van essentieel belang. Samen met het toepassen van technische-, procedurele- en organisatorische maatregelen wordt het risico op het ongewild blootstellen van vertrouwelijke informatie teruggedrongen. Deze maatregelen worden toegepast op informatie in de vorm van documenten aan de eindgebruikerskant als op informatie binnen ketens en in registers. Door deze integrale aanpak (waarbij het ‘need to know’-principe wordt toegepast) worden risico’s tot een minimum beperkt.

3.4.3 Ontdekking van bredere verbanden door innovatieve technologie

Door dataminingtechnieken en intelligente algoritmen toe te passen kan JenV in de komende jaren haar bedrijfsvoering en primair proces efficiënter maken. Dit kan op basis van nieuwe verbanden en additionele relevante inzichten. Deze (nieuwe) inzichten kunnen ontstaan uit de verbanden die ongestructureerde of gestructureerde bronnen blootleggen. De intelligente algoritmen ondersteunen, maar schrijven ook voor. Dit zal steeds meer gebeuren.

Praktijkcase: De Politie

Voorzieningen zoals auto's beschikken over sensoren die data genereren. Sensoren op belangrijke punten in de stad genereren file - informatie, data over het niveau van luchtvervuiling, enzovoorts. De aanwezigheid van mobiele apparatuur wordt geregistreerd. De politie koppelt deze data aan de misdaden gepleegd in de wijk, zoals inbraken. Intelligente data-analyse technieken kunnen op verfijnde wijze de verbanden uit de verschillende databronnen ophalen en kunnen met een grote mate van zekerheid aanwijzen wie de potentiele dader is. Er kan zelfs voorspeld worden dat er in een bepaalde tijdsperiode in een bepaalde omgeving een inbraak gaat plaatsvinden.

Voorbeeld II: De Politie.

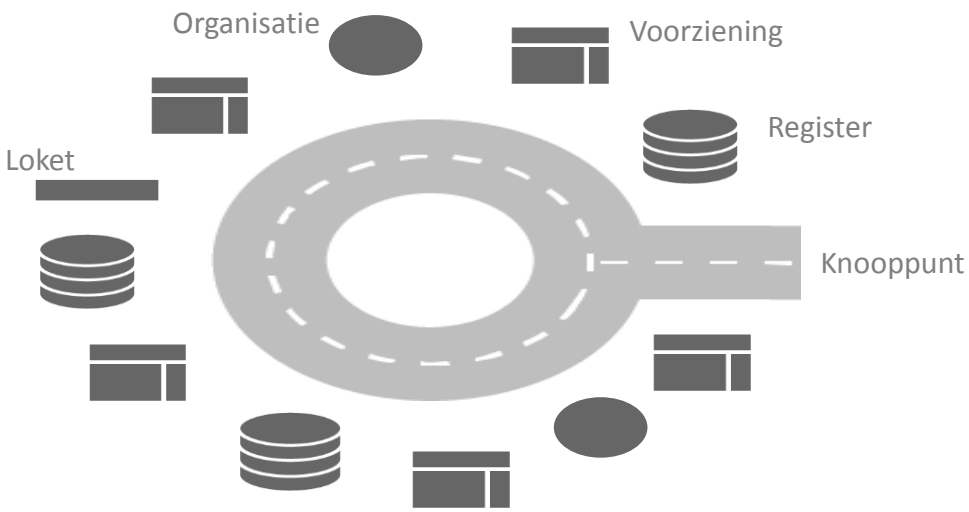
3.4.4 Efficiënte opslag en uitwisseling van informatie in (keten) registers

In de huidige JenV-ketens en onderliggende onderdelen is veel (dubbele) data aanwezig die zorgen voor onduidelijkheid of die leiden tot het uitvoeren van additionele controles. Daarom dienen de verschillende onderdelen van de ketens organisatorische afspraken te maken over welke registers leidend zijn. Maar ook dient technologie te worden ingezet voor het raadplegen van registers op een eenduidige en efficiënte wijze. Deze technologie kenmerkt zich door service gebaseerde toegang. Door daarnaast datavirtualisatietechnieken toe te passen beschikken de JenV onderdelen over de mogelijkheid een logische laag over verschillende databronnen (onder andere registers, administraties, archieven, geleverd vanuit het Gegevensdiensten domein) heen aan te brengen. Verschillende systemen kunnen met behulp van deze logische laag op een eenduidige wijze verschillende registers tegelijkertijd raadplegen. Zo komt informatie in een geaggregeerde vorm beschikbaar.
Met deze aanpak wordt de communicatie tussen de verschillende systemen (in specifieke 'dialecten') efficiënter. Ook bieden portals waar gebruikers data kunnen samenstellen mogelijkheden om relevante inzichten te creëren.
Het is wel nodig dat met de onderdelen een standaard af wordt gesproken maar dat die standaard ruimte biedt voor flexibiliteit. Hierbij wordt gedoeld op specifieke situaties waarbij twee onderdelen uitsluitend met elkaar communiceren.

3.4.4.1 In toenemende mate ontstaan genetwerkte ketens[10]

Samenwerken met partijen buiten JenV wordt steeds belangrijker. Op een steeds groter wordende schaal worden relevante gegevens verzameld die invloed kunnen hebben op de besluitvorming in de Justitiële keten en daarbuiten. Het uitwisselen van informatie vereist coördinatie en standaardisatie. Dit heeft tot gevolg dat JenV zich steeds meer als onderdeel van de genetwerkte keten gedraagt als centraal berichtenknooppunt en daarbij ook een verrijkende rol invult. Functionaliteiten die door het centraal berichtenknooppunt ingevuld kunnen worden zijn onder andere de uitwisseling van berichten en het (her) gebruik daarvan, conversie, faciliteren van databronnen, enzovoorts. Figuur 2. toont een centraal berichtenknooppunt.

[10] Genetwerkte ketens zijn ketens die aan elkaar ontsloten zijn middels een centraal berichten knooppunt.



Figuur 3 Voorbeeld van een centraal berichtenknooppunt: Informatierotonde (bron: Just Id 2017)

3.4.5 Datagedreven processen en vastlegging

Bij de primaire processen van de JenV onderdelen zal meer en meer datagedreven gewerkt worden. Documenten zoals we deze nu kennen (bijvoorbeeld een PDF/A of Word-document) zullen op termijn verdwijnen. Bij JenV verandert de informatievoorziening. Een uitspraak van een rechter wordt niet meer (alleen) vastgelegd in een ondertekend (digitaal) document maar wordt samengesteld vanuit een logische duurzame representatie van informatie (aan elkaar gelinkte informatieobjecten) uit systemen of registers. Hierbij zullen grootboektechnieken[11] een belangrijke rol gaan spelen om redenen van efficiency en betrouwbaarheid.

Datagedreven processen en vastlegging

Gerechtelijke uitspraken zijn niet meer alleen als documenten beschikbaar maar zijn ontleed in objecten en in een database opgenomen. Daar kan op 'google- achtige' wijze worden gezocht. Deze database is beschikbaar voor iedereen: rechters, advocaten, maar ook burgers en bedrijven. Zowel een advocaat als rechter kan op basis van een casus of een wettekst zoeken en zo een eerste oordeel samenstellen, dit op basis van uitspraken uit het verleden. De burger kan dit doen op basis van een casus.
De burger kan enigszins voorspellen wat een uitspraak is en zal geen juridische stappen ondernemen indien de kans op succes klein is. Het vergroot de rechtsgelijkheid en zorgt voor minder werkdruk bij rechters aangezien relatief makkelijk een basisuitspraak samengesteld kan worden, de rechter kan vervolgens naar specifieke (menselijke) aspecten kijken en een definitief oordeel geven. Het biedt eveneens de mogelijkheid om de kosten van een advocaat stevig te laten drukken omdat deze minder tijd nodig heeft om een zaak voor te bereiden en indien zinloos de burger of het bedrijf überhaupt niet langs zal komen.

Voorbeeld III: Datagedreven processen en vastlegging

[11] Hierbij is te denken aan technologie zoals Blockchain

3.5 Vervolgstappen

Data, informatie en gegevens bieden ongekende mogelijkheden ten behoeve van de datagedreven processen van JenV. Om deze visie verder te concretiseren worden de volgende uitgangspunten/vervolgstappen voorgesteld. Het gaat in deze paragraaf over de inhoud van de verandering en niet zozeer over projectdoelstellingen:

1. Verdere standaardisatie van het ketenbrede berichtenverkeer met ruimte voor flexibele invulling ten behoeve van specifieke behoeften van een onderdeel.
    a. Er dienen specifieke afspraken gemaakt te worden over de berichten syntax (structuur);
    b. Er dienen specifiek afspraken gemaakt te worden over de semantiek en context van het bericht (doelstelling);
    c. Indien twee onderdelen buiten de ketens om met elkaar willen communiceren dan kan dit op basis van eigen lokale afspraken rondom standaardisatie. Dit zijn standaarden die twee specifieke onderdelen met elkaar vaststellen.
2. Invoering van intelligente, innovatieve data-analysetechnologieën is een randvoorwaarde voor een efficiënte dienstverlening naar de burger en bedrijfsleven
    a. Het verkrijgen van relevante (additionele) informatie leidt tot nieuwe inzichten of kan helpen bij het nemen van beslissingen. De totale duur van rechtszaken kan hierdoor bijvoorbeeld worden verkort;
3. Het classificeren van data is een randvoorwaarde Bij voorkeur wordt dit gerealiseerd op basis van geautomatiseerde tooling. Naar verwachting kan tot wel 80% van de aanwezige data binnen JenV automatisch worden geclassificeerd.

3.5.1 Specifieke vervolgstappen

1. Optimale ketensamenwerking zal naar verwachting worden gerealiseerd door het inrichten van een centraal berichtenknooppunt waarbij ketenpartijen informatie kunnen uitwisselen.
    a. Deze routeert berichtenverkeer naar de verschillende onderdelen;
    b. Deze faciliteert de verrijking van berichten door verschillende aangesloten onderdelen;
    c. Deze faciliteert de workflow-functionaliteit waarbij input en output van verschillende processen kan worden gemanaged;
    d. Deze faciliteert in portal functionaliteit.

Hoofdstuk 4. Datacentrumdiensten

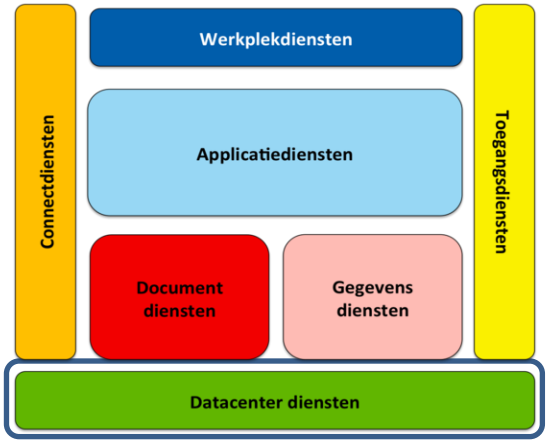
Hoofdstuk 4 bevat de beelden die bij de onderdelen en marktpartijen betrokken bij GeTIJ opgehaald zijn. Het gaat in op de relevante ontwikkelingen binnen het domein Datacentrumdiensten.

4.1 Samenvatting

De toepassing van Cloud-technologie vanuit de zogenoemde Trusted Cloud-aanbieders binnen en buiten de Rijksoverheid vereist een sterke mate van standaardisatie. Hierdoor wordt een uniform landschap gerealiseerd op zowel het niveau van de infrastructuur als op het niveau van de applicaties. Onderdelen van JenV kunnen aanbieder of afnemer van de gestandaardiseerde diensten zijn. De (infrastructurele) beheerlast wordt zo substantieel verlaagd, de continuïteit van de eigen organisatie wordt sterk verbeterd en JenV kan zich ontwikkelen in een regie-organisatie. Bovendien biedt de toepassing van Cloud-technologie binnen- en buiten JenV de mogelijkheid om capaciteit op- en af te schalen. In plaats van gebruik te maken van op investering gebaseerde financiële modellen maakt JenV gebruik van operationele financieringsmodellen.

4.2 Algemeen

Met digitalisering realiseren de organisaties onder JenV een steeds efficiëntere dienstverlening naar de burgers en bedrijven. Het volgens het informatiegestuurd werken principe inrichten (zie hoofdstuk 3, Gegevensdiensten) van de informatievoorziening is essentieel voor het blootleggen van nieuwe verbanden, het verkrijgen van nieuwe inzichten, het bespeuren van trends en het inwinnen van adviezen op basis van kunstmatige intelligentie. Dit verandert de informatiepositie in de ketendienstverlening en de afzonderlijke dienstverlening van verschillende organisaties binnen JenV, maar ook Rijksbreed substantieel.



Figuur 4 EAR domein datacentrum diensten

Deze digitale transformatie en bijbehorende sterk groeiende behoefte naar opslagcapaciteit[12] en rekenkracht vereist een sterke infrastructurele basis. De Trusted Cloud en vertrouwde publieke Cloud-aanbieders bieden deze basis.
In de afgelopen jaren heeft er binnen de Rijksoverheid een sterke consolidatieslag plaatsgevonden waarbij het aantal overheidsdatacenters zijn geconsolideerd tot vier.

[12] Zie ook Investeringsagenda voor de SCO-ICT infrastructuur: 2017-05-11 agpt 3b Rapport tbv Investeringsagenda infra 2017-2027 (2).pdf

Cloud technologie, of beter gezegd de typische karakteristieken[13] die door de NIST (National Institute of Standards and Technology) zijn voorgeschreven spelen een sleutelrol bij de verdere standaardisatie en rationalisatie van de bouwstenen voor applicaties en infrastructuur van verschillende ministeries.

4.3 Visie

In 2025 opereert JenV op een Cloud platform (Bimodal IT omgeving welke zowel innovatieve als legacy systemen huisvest) dat zich zowel binnen de organisatiegrenzen bevindt maar ook daarbuiten (de zogenoemde Trusted Cloud)[14]. Deze Trusted Cloud biedt naast de infrastructurele mogelijkheden voor Cloud native applicaties ook de mogelijkheid om traditionele applicaties te laten landen. JenV voert de regie over haar diensten die ze afneemt van de Trusted Cloud volgens een operationeel model. Zij schaalt op- en af naar wens en betaalt naar afname. Via een JenV Producten- en dienstencatalogus (PDC) van JenV worden gestandaardiseerde bouwblokken voor applicaties en infrastructuur afgenomen. Deze kunnen binnen korte tijd (30-60min) beschikbaar zijn voor de aanvrager. Meerdere bouwblokken kunnen gezamenlijk een werkend platform vormen. Configuratie van deze infrastructurele bouwblokken is inclusief configuratie van omliggende basisdiensten zoals firewall-, en load balancing diensten, enzovoorts. De infrastructurele bouwblokken worden automatisch aan de eindgebruiker ter beschikking gesteld.
Het is voor de aanvrager volledig transparant waar deze diensten technisch leven: binnen de Rijksoverheid (Overheids DataCenters, nader ODC's) of bij de publieke vertrouwde aanbieders. De beheerafdelingen binnen JenV hebben nadrukkelijk een verandering doorgemaakt van operationeel beheer naar regievoering. Handmatige configuratie is tot een minimum gereduceerd en de werkzaamheden focussen zich vooral op het (door)ontwikkelen van templates of blauwdrukken en bijbehorende workflows ten behoeve van de automatische uitrol van infrastructurele bouwblokken. JenV wordt wendbaar en kan snel inspelen op wisselende omstandigheden van capaciteits- en innovatievraagstukken door de toepassing van Cloudtechnologie.

4.4 Noties

In deze paragraaf worden de noties beschreven die zijn opgehaald gedurende de sessies met de betreffende onderdelen en marktpartijen.

4.4.1 Veranderende rol van datacenters

In de commerciële markt is een veranderende rol van datacenters waar te nemen. De datacentermarkt beweegt zich van het leveren van zogenoemde housing concepten (voorzien in snelle netwerkconnectiviteit, koeling en rackspace) naar het leveren van fijnmazige connectiviteit tussen datacenters en publieke Cloud-aanbieders.
Voorheen werden Cloud-aanbieders betrokken over het publieke Internet ten behoeve van proces ondersteunende kantoorautomatiseringsdiensten, nu is er (mede door het huidige volwassenheidsniveau van de Cloud-aanbieders) een sterke behoefte aan directe connectiviteit van de Cloud-aanbieders ten behoeve van het onderbrengen van primair proces diensten. Het portfolio van de datacenterpartijen is hierdoor verschoven naar een makelaar (broker) van verkeersstromen.

Binnen de Rijksoverheid zien we een eenduidige beweging: er is behoefte aan het flexibel kunnen afnemen van capaciteit (op- en afschalen indien nodig met bijbehorend afrekenmodel) zowel over de ODC's heen als bij publieke vertrouwde aanbieders.

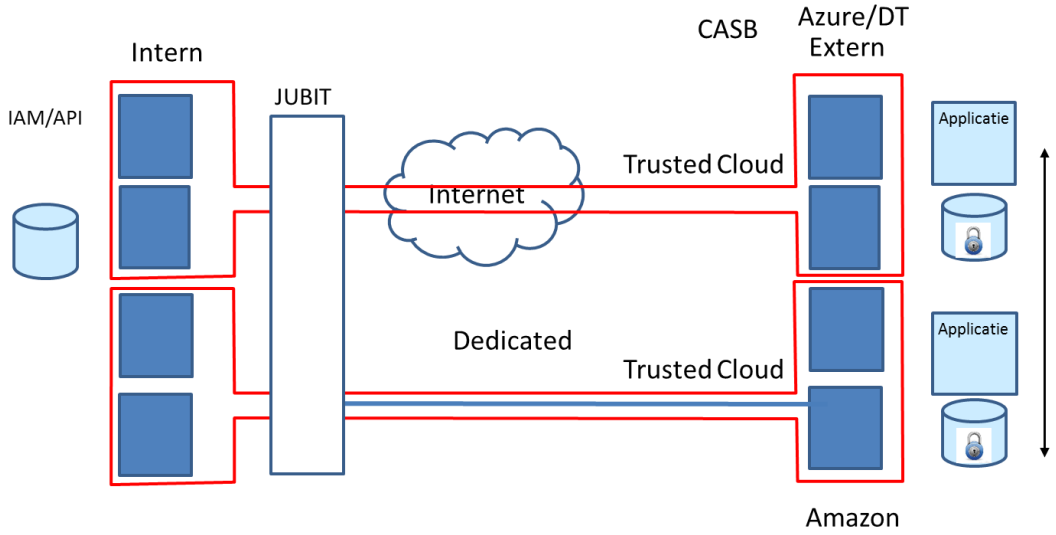
---

[13] Zie http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[14] Nader onderzoek is nodig om te bepalen of de huidige uitgangspunten in de 'Enterprise Architectuur VenJ' aanpassing behoeven.

4.4.2 *Trusted Cloud*

Uitgangspunt van de Trusted Cloud is het vanuit meerdere overheidsdomeinen kunnen leveren van (gestandaardiseerde) resources. JenV wijst voor de Trusted Cloud een marktpartij of een onderdeel aan.
Deze gestandaardiseerde platformen en resources worden toegepast bij uitwijkscenario's en scenario's waarbij capaciteit is gewenst bij een specifieke organisatie (denk bijvoorbeeld aan de belastingdienst waar extra resources nodig zijn ten tijde van de aangifte periode).
De Trusted Cloud is het stelsel van afspraken en eisen (organisatorisch en technologisch) dat de interoperabiliteit regelt van de decentrale Clouds (onder andere de ODC's) binnen de Rijksoverheid en bij commerciële aanbieders (zie ook voetnoot 14). Hierbij zijn de eisen in relatie tot de vertrouwelijkheid en integriteit van geclassificeerde data geborgd. Zie Figuur 5 voor een schematische representatie van de Trusted Cloud.



Figuur 5 Schematische weergave Trusted Cloud

4.4.2.1 Missie kritische workloads

De Trusted Cloud is zodanig ontwikkeld dat vanuit technische optiek primaire processen hierin ondergebracht kunnen worden. De Trusted Cloud biedt afdoende ingebouwde zekerheden om de vertrouwelijkheid, beschikbaarheid, betrouwbaarheid en performance van de specifieke dienst te kunnen garanderen. Om dit mogelijk te maken is een cultuurverandering binnen JenV noodzakelijk: het kunnen loslaten van (delen van) controle op infrastructuur.

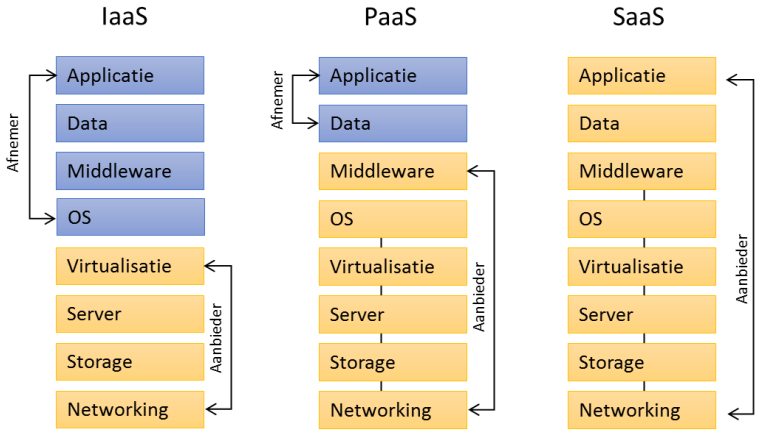
4.4.2.2 Één logische pool van infrastructurele resources

De Trusted Cloud vormt voor JenV een uitwisselbare pool van infrastructurele resources over de onderdelen van JenV heen, maar ook bij commerciële aanbieders. In het geval van calamiteiten of bij de behoefte aan extra capaciteit kan gebruik gemaakt worden van de (over) capaciteit van onderdelen binnen JenV. Het op een betrouwbare wijze gebruik kunnen maken van gedeelde resources over onderdelen heen vereist een verregaande mate van standaardisatie.

4.4.3 Reductie van complexiteit door platform- en bouwblok standaardisatie

4.4.3.1 Applicaties en infrastructuur

Standaardisatie van de bouwblokken voor infrastructuur en applicaties is nodig. Het uitgangspunt voor infrastructurele standaard 'Infrastructure as a Service' (IaaS) bouwblokken is immers dat de opslag-, reken- en netwerkcapaciteit wordt gestandaardiseerd. In de bovenliggende lagen kan een JenV onderdeel zelf de inrichting van de applicaties bepalen. Maar een onderdeel kan zich committeren aan verder gestandaardiseerde 'Platform as a Service' (PaaS) of afnemer worden van de volledig afgeconfigureerde SaaS (Software as a Service) diensten[15]. Zie **Figuur 6** voor een grafische representatie van de Cloud dienstverleningsmodellen.



Figuur 6 Dienstverleningsmodellen IaaS, PaaS, SaaS

4.4.3.2 Cloud platform standaardisatie

De onderdelen van JenV dragen zelf zorg voor de eigen infrastructuur en applicaties. Dit leidt tot grote verschillen in uitvoering en standaardisatie. De interoperabiliteit tussen de verschillende JenV onderdelen is daarom voor verbetering vatbaar. De mogelijkheden om samen te werken zijn daarom niet optimaal. Het is in de periode 2017-2025 van groot belang dat binnen JenV of zelfs Rijksbreed een platformstandaard[16] wordt gekozen. Dit platform is bij voorkeur een op open standaarden gebaseerd platform met ruimte voor eigen ontwikkelingen zonder dat de uitwisselbaarheid tussen de onderdelen van JenV hierdoor in gevaar komt. Hierbij dient wel opgemerkt te worden dat er specifieke afspraken gemaakt dienen te worden over communicatiestandaarden (inclusief bericht formaten, gezamelijke semantische definities, etc.).

4.4.4 Gecentraliseerde JenV PDC faciliteert standaardisatie

Door nieuw te bouwen applicaties of te upgraden platformen op te ontwikkelen op basis van bouwblokken uit de PDC wordt langzaam maar zeker een gestandaardiseerd landschap gecreëerd op basis van Cloud-technologie.

---

[15] Zie ook rapportage KPMG: Cloudcondities Digitale Werk Omgeving (VenJ, 10 november 2016) .

[16] Hierbij dient opgemerkt te worden dat een balans tussen standaardisatie en diversiteit moet zijn. Single vendor beleid kan leiden tot een vendor lock-in.

4.4.5 Betrouwbare uitrol van bouwblokken door orkestratie

ICT-infrastructuren kenmerken zich door een toenemende dynamiek. De autonome groei in vraag naar capaciteit, werkwijzen zoals DevOps (Agile ontwikkelen van software) en de razendsnelle ontwikkeling van nieuwe technieken en behoefte naar snelle adoptie ervan vereisen een geautomatiseerde totstandkoming (en afbraak) van platformen en infrastructurele bouwblokken.
De zogenoemde orkestrator (dirigent van de infrastructuur) stuurt geautomatiseerd volgens een werkvolgorde de verschillende infrastructurele onderdelen aan. Zo is het mogelijk de gestandaardiseerde bouwblokken voor infrastructuur en applicaties tot stand te laten komen. Deze orkestrator rolt de vastgestelde standaarden uit en configureert deze af. Daarnaast coördineert de orkestrator de juiste inrichting van omliggende systemen.

4.4.5.1 Veranderde rol operationele taken rondom systeembeheer

Door het breed toepassen van orkestratietechnieken vindt een verschuiving plaats in de wijze waarop de operationele afdelingen acteren. Er zijn steeds minder operationele handelingen op systemen nodig. Deze taken zullen worden overgenomen door zogenaamde deployment-systemen voor de verschillende platform die door de orkestrator worden aangestuurd. De verschuiving van het werk zal vooral zichtbaar worden bij de werkzaamheden rondom het semi-handmatig configureren van systemen. Deze werkzaamheden veranderen in werkzaamheden voor het standaardiseren en modelleren van infrastructuurbouwblokken in de vorm van templates. Daarnaast wordt voorzien dat de operationele taken zich meer bewegen op een tactisch/strategisch niveau. Het gaat dan om sturing op het nakomen van gemaakte afspraken over afgenomen diensten. Door het wegvallen van operationele taken komt er bovendien meer tijd beschikbaar voor innovatie.

4.4.6 Gestandaardiseerde koppelvlakken voor Trusted Clouds

Het onderbrengen van specifieke workloads bij Trusted Cloud-aanbieders vereist helder gedefinieerde koppelvlakken. Deze koppelvlakken zijn centraal ondergebracht bij een door JenV aangestelde partij. Dit zou bijvoorbeeld Jubit kunnen zijn.
Vanuit het veiligheidsperspectief wordt een Trusted Cloud-aanbieder -hoe volwassen ook- in principe gezien als ‘semi-vertrouwd’. Dit betekent dat JenV of onderdelen additionele mitigerende maatregelen dienen te nemen.
Het centraal beleggen en definiëren van koppelvlakken stelt JenV bovendien in staat wendbaar te zijn tussen verschillende Trusted Cloud-aanbieders. Dit geldt zowel voor de interne ODC’s als daarbuiten voor de grote commerciële aanbieders.

Los van de technische complexiteit is het in theorie wenselijk workloads onafgebroken te kunnen migreren tussen verschillende Trusted Cloud-aanbieders. Dit kan om de volgende redenen het geval zijn:

1. Specifieke type workloads zijn overall of op bepaalde dagdelen bij specifieke Trusted Cloud-aanbieders goedkoper. Dit levert een reductie van kosten op;
2. De aanwezigheid van innovaties waar JenV graag gebruik van wil maken voor delen van haar infrastructurele landschap;
3. Het verspreiden van workloads vanuit continuïteitsoverwegingen.

Om bovenstaande technisch mogelijk te maken zal JenV in de komende jaren zelf de regisseursfunctie in procesmatige als technische zin op zich moeten nemen aangezien de markt hier nog niet gereed voor is. Er is echter wel een beweging gaande die voorziet in integratievoorzieningen tussen verschillende publieke Trusted Cloud-aanbieders. Dit wordt ook wel de ‘integration Cloud’ genoemd.

4.4.7 Regie op Trusted Cloud dienstverlening, innovatie en roadmap ontwikkeling

In een snel digitaal transformerende wereld is het vermogen om snel nieuwe technologie te kunnen adapteren een vereiste. Dit vraagt om een organisatie die regie voert binnen de eigen organisatie en richting leveranciers. Er tekent zich hierbij een verandering af: JenV gaat van een op investeringen georiënteerd model naar een operationeel gedreven kostenmodel. In dit laatste model wordt uitsluitend betaald voor de afgenomen diensten per JenV onderdeel.

De regie-organisatie of het competence center voert de volgende activiteiten uit:

1. Vult de rol in van een kenniscentrum:
   Het nauw volgen van ontwikkelingen op het gebied van Cloud en het op organisatie specifieke context toepassen ervan;
2. Definiëren van standaarden en richtlijnen voor JenV workloads:
   Vaststellen van de wijze waarop workloads voor infrastructuur en applicaties ondergebracht worden bij JenV eigen maar ook publieke Trusted Cloud-aanbieders;
3. Aansturing van Trusted Cloud-aanbieders (in- en extern):
   Regievoering over contracten, capaciteit ten behoeve van de JenV operatie en behoefte vanuit projectportfolio's;
4. Ontwikkelen van templates voor bouwblokken ten behoeve van applicaties en infrastructuur;
5. Definiëren van beheeraspecten rondom de bouwblokken voor de infrastructuur en de bouwblokken;
6. Definiëren van processen over ontwerp, intake, implementatie, beheer;
7. Het testen van nieuwe technologieën en standaarden in de context van JenV (innovatie).

Met een centrale regieorganisatie krijgt en behoudt JenV grip op ICT.

4.4.8 Versterking in kennis en kunde binnen JenV

Om daadwerkelijk verregaande standaardisatie en automatisering van handmatige taken mogelijk te maken binnen de Trusted Cloud is specifieke kennis nodig. Die kennis is op dit moment onvoldoende aanwezig bij JenV. Deze expertises zijn bovendien ook schaars in de markt. Het is dan ook lastig om binnen JenV dergelijke deskundigen aan boord te trekken. Overigens rijst de vraag of JenV alle expertise zelf aan boord dient te halen of dat deze expertise in dienstvorm bij marktpartijen belegd dient te worden.

4.5 Vervolgstappen

De Trusted Cloud biedt JenV wendbaarheid en het vermogen in te kunnen spelen op een snel veranderende wereld. Om deze visie verder te concretiseren worden de volgende uitgangspunten/vervolgstappen voorgesteld. Het gaat in deze paragraaf over de inhoud van de verandering en niet zozeer een projectdoelstelling;

1. Verdere standaardisatie creëert de basis voor de Trusted Cloud;
    a. Vaststellen van Rijksbrede IaaS bouwblokken: standaardisatie op varianten tot en met het besturingssystem;
    b. Vaststellen van Rijksbrede PaaS bouwblokken: standaardisatie op varianten en bijvoorbeeld database gebaseerde bouwblokken tot en met middleware niveau;
    c. Aanleggen van een Rijksbrede PDC met deze gestandaardiseerde bouwblokken;
    d. Vaststellen van uitrolmechanismen (workflow en provisioning) voor deze gestandaardiseerde bouwblokken.
2. Vaststelling Rijksbreed Cloud platform;
    a. Adoptie van een commercieel of platform gebaseerd op open standaarden; uniformiteit over de ministeries heen;
    b. Sterfhuisconstructie voor traditionele omgevingen tenzij er een business case te maken is voor het Cloud-ready maken van het platform;
3. Creatie van een Cloud Exchange koppelvlak;
    a. Uitwisseling van verkeer met publieke Trusted Cloud-aanbieders over een directe lijn
4. Oprichten van een (virtueel) Cloud expertise en regie centrum;
    a. Oprichten van een (virtueel) team met afgevaardigden met mandaat vanuit de verschillende ministeries. Doestelling is het vanuit de gezamenlijke standaard te redeneren;
    b. Doorontwikkelen van Rijksbrede standaarden op infrastructuur bouwblok niveau.
    c. Opstellen van richtlijnen voor het gebruik van (publieke) Trusted Cloud diensten (IaaS, PaaS, SaaS).
5. Opstellen van rubriceringskader voor JenV informatie(objecten) in de (publieke) Trusted Cloud.

Hoofdstuk 5. Connectdiensten

Hoofdstuk 5 bevat de beelden die bij de onderdelen en marktpartijen betrokken bij GeTIJ opgehaald zijn. Het gaat in op de relevante ontwikkelingen binnen het domein Connectdiensten[17].

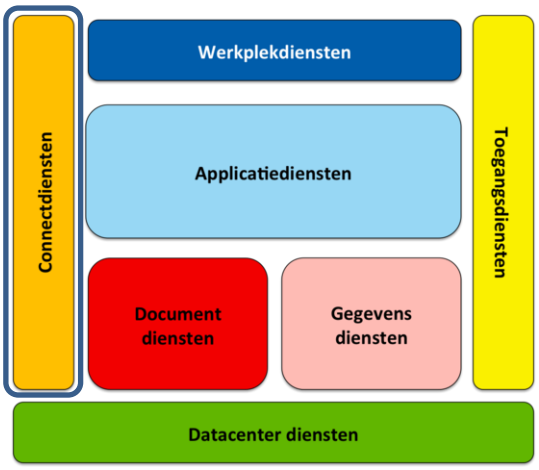
5.1 Samenvatting

Connectdiensten zijn essentieel voor de verdere digitalisering binnen JenV. In toenemende mate wordt gevraagd naar bandbreedte en naar snelheid. Het netwerk voldoet in de komende jaren aan de volgende kenmerken:

- Het netwerk is op- en af te schalen, open en transparant en voorziet in toenemende behoefte tot samenwerkingen met ketenpartners en onderdelen binnen JenV, onder andere in Rijksverzamelpanden, maar ook bij de ontsluiting van het RijksOverheidsNetwerk (RON);
- Het netwerk zorgt voor transparante uitbreiding naar publiek vertrouwde Cloud-aanbieders[18];
- Het netwerk borgt in samenhang met omliggende diensten de vertrouwelijkheid en integriteit van informatie door het faciliteren van security zones. Encryptie technieken worden hierbij toegepast;
- Security diensten, evenals Internet Access worden centraal aangeboden vanuit een door JenV geselecteerde partij.

5.2 Algemeen

Voor de periode 2017-2025 voorzien we voor netwerkinfrastructuren als Justitienet en Justitie Beveiligde Internet Toegang (JuBIT)[19] de nodige ontwikkelingen. Zo neemt de digitalisering binnen JenV steeds verder toe, gebruiken we in toenemende mate apps, ook via de Cloud, en communiceren we via meerdere apparaten met het internet. Het dataverkeer neemt stevig toe en het aantal mobiele medewerkers groeit flink. Hierdoor komen diensten als Justitienet en JuBIT onder grotere druk te staan. Een toekomst-bestendige netwerkinfrastructuur dat met deze ontwikkelingen kan meegroeien is dan ook essentieel.



Figuur 7 EAR domein Connect diensten

[17] Relevant is om hierbij te melden dat de uitgangspunten genoemd in dit hoofdstuk de basis vormen voor de verwerving van JustitieNet 4 (start oktober 2017).

[18] Dit zijn door JenV geselecteerde aanbieders waarmee sterke contractuele afspraken zijn gemaakt om integriteit, beschikbaarheid en vertrouwelijkheid van data is gewaarborgd. De verzameling van VenJ eigen infrastructuur gecombineerd met publieke aanbieders wordt de Trusted Cloud genoemd.

[19] Domein Connectdiensten binnen de Enterprise Architectuur Rijk (EAR)

5.3 Visie

In 2025 zien we een verregaande integratie tussen vaste, mobiele en draadloze netwerken van JenV. De behoefte aan het tijd, plaats en apparaat onafhankelijk samenwerken (TPAW) wordt zo mogelijk maakt. De eindgebruiker merkt niet welke diensten erachter zitten. Er is een eenduidige gebruikerservaring waar op basis van Single SignOn (SSO) gewerkt wordt. Daarnaast zullen besloten en openbare netwerken steeds verder naar elkaar toetrekken. Het netwerk is fijnmazig en verbindt Rijksverzamelpanden, Overheidsdatacenters en Rijksoverheidsnetwerken. Het netwerk schaalt dynamisch mee met de sterk groeiende vraag naar capaciteit. Daarnaast ondersteunt het netwerk, door toepassing van zoneringstechnieken in de security, de opslag van gerubriceerde informatie. Op basis van gestandaardiseerde koppelvlakken worden publieke Cloud-aanbieders transparant ontsloten (zie ook hoofdstuk 4 Datacentrumdiensten). JenV is hierdoor optimaal wendbaar in haar ICT-strategie en uitvoering van haar primair proces.

5.4 Noties

In deze paragraaf worden de noties beschreven die zijn opgehaald gedurende de sessies met de betreffende onderdelen en marktpartijen.

5.4.1 Mobility in toenemende mate van belang

Ten gevolge van de ontwikkeling van de zogenoemde mobility nemen JenV medewerkers niet alleen meer op een vaste werkplek in een kantoorlocatie plaats, maar werken zij ook thuis, onderweg of vanuit andere (rijks)overheidslocaties. Werkplekapparaten die daarvoor gebruikt worden, zijn naast pc’s en laptops ook tablets en smartphones. Kortom,de toepassing van TPAW (Tijd, Plaats en Apparaat onafhankelijk Werken) neemt in omvang steeds verder toe. Dit stelt ook de nodige uitdagingen aan het security-terrein: mobiele security vraagt om meer aandacht.

Daarnaast vinden er binnen het Rijk een aantal ontwikkelingen plaats zoals:

- De inzet en het gebruik van Rijksverzamelpanden;
- Het onderling koppelen van departementale netwerken aan het RijksOverheidsNetwerk;
- De inrichting en gebruik van ODC’s;
- De ontwikkeling van Rijksbreed internetconnectiviteit en Partner-aansluitingen;
- Het leveren van diensten zoals (draadloze) internet toegang aan andere rijksoverheidsmedewerkers (GovRoam).

5.4.2 Verschuiving van in aanpak informatiebeveiliging

Naast de rijksbrede ontwikkelingen vinden er diverse ontwikkelingen binnen JenV plaats, waarbij de huidige beveiliging op netwerkniveau door middel van crypto’s verschuift naar de beveiliging van de data, systemen en applicaties. Ook nemen de behoefte aan en de noodzaak om aantoonbaar te voldoen aan wettelijke kaders als de Wet bescherming persoonsgegevens (WBP) en de opvolger Algemene Verordening Gegevensbescherming (AVG) toe. De in de AVG opgenomen meldplicht datalekken en de aspecten van Beschikbaarheid, Integriteit en Vertrouwelijkheid van de rijksbrede BIR (Baseline Informatiebeveiliging Rijk) moeten bovendien zijn geborgd.

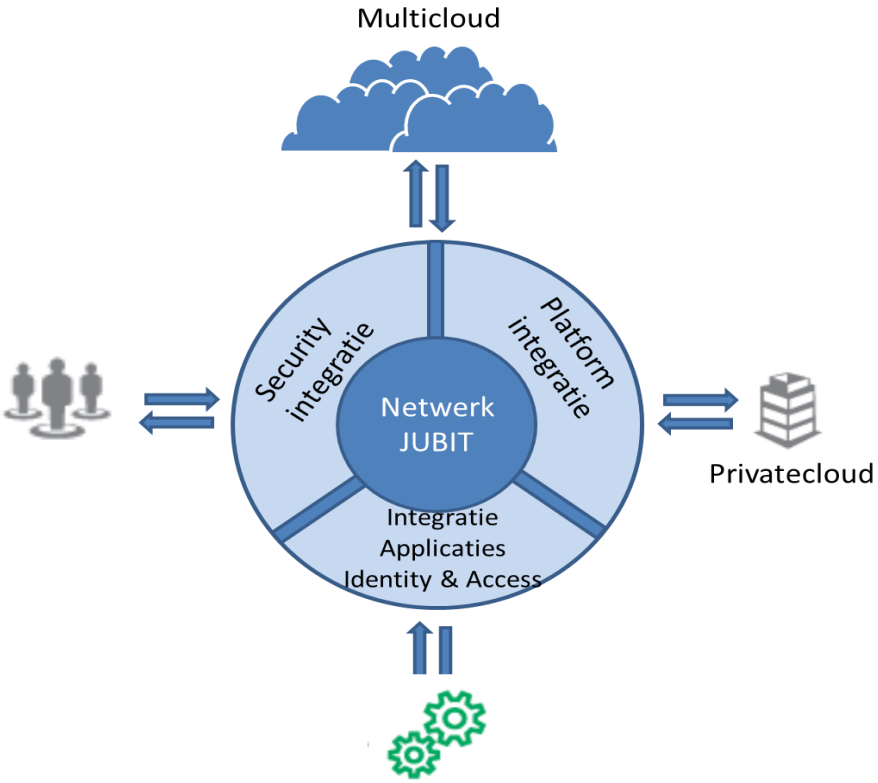
5.4.3 Internet of Things is in opmars binnen JenV

Eveneens zien we binnen het openbare orde en veiligheidsdomein een toenemende rol van bijvoorbeeld sensoren, onder andere binnen penitentiaire inrichtingen of in openbare

omgevingen zoals rechtszalen. Hierbij wordt meestal gerefereerd aan het begrip Internet-of-Things (IoT). Voor de inzet van sensoren is een goed beveiligd draadloze netwerkinfrastructuur nodig die een hoge performance en een goede dekking garanderen. Dit betekent dat draadloze toegang als een onderdeel van het vaste netwerk wordt gezien. Een infrastructuur die gezien de diensten als telefonie, bedrijfsapplicaties, back-ups, virtuele werkplekken 7 keer 24 uur beschikbaar dient te zijn.

5.4.4 Buiten wordt binnen

Naast functionele ontwikkelingen van mobility en TPAW zijn er een aantal technologische ontwikkelingen die een belangrijke rol spelen voor de connectdiensten. Dit zijn vooral de ontwikkelingen die spelen op het terrein van Clouddiensten, applicaties en systemen die meer en meer zullen worden afgenomen vanuit de Cloud. Dit levert vraagstukken op als; hoe verbinden we 'buiten' met 'binnen', welke security-policies zijn van toepassing en hoe kunnen we onze security-policies op externe omgevingen 'afdwingen'. Hoe wordt toegang tot deze applicaties geregeld en welke ontwikkelingen stelt dat aan onze IAM (Identity en Access Management) processen en systemen.



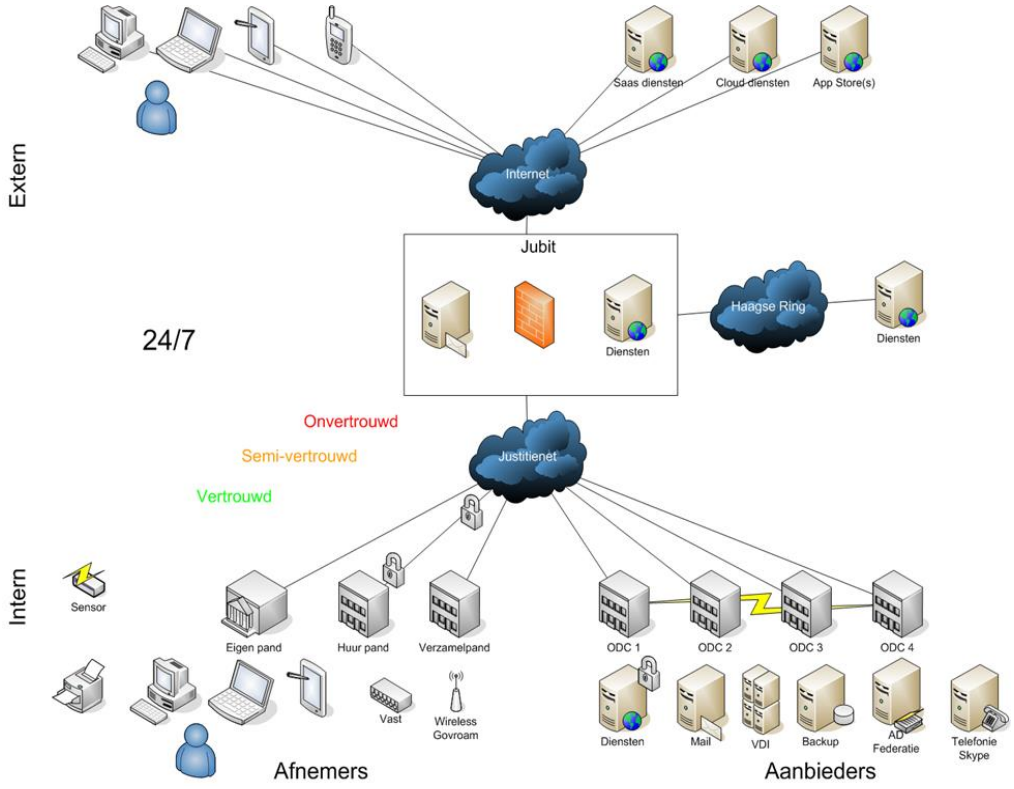
Figuur 8 Schematische representatie: buiten wordt binnen

Bovenstaande ontwikkelingen leiden tot een aantal uitgangspunten waar in de toekomst rekening mee moet worden gehouden. Deze zullen hieronder worden benoemd en verder worden uitgewerkt. Ze zijn te splitsen in meer algemene uitgangs- en aandachtspunten en meer specifieke.

5.5 Vervolgstappen

De netwerken ondersteunen op een eenduidige en transparante wijze de I-strategie van JenV. Om deze visie verder te concretiseren worden de volgende uitgangspunten/vervolgstappen voorgesteld. Het gaat in deze paragraaf over de inhoud van de verandering en niet zozeer over projectdoelstellingen;

- Connectdiensten zorgen voor een transparante, voldoende beschikbare, op- en af te schalen veilige en economische voordelige verbinding tussen de eindgebruikers, devices en diensten:
    - Transparant: Op elke locatie krijgt de gebruiker toegang tot zijn werkomgeving;
    - Voldoende beschikbaar: De verbindingen zijn geschikt om de gebruiker gebruik te laten maken van diensten die via het netwerk worden aangeboden op basis van de afgestemde beschikbaarheidspercentages;
    - Veilig: De gebruiker kan veilig zijn diensten benaderen, ook in verzamelpanden;
    - Economisch verantwoord: de verbindingen kunnen worden afgestemd op het gebruik en aantal gebruikers;
- Optimaliseer en uniformeer de inkomende en uitgaande verkeerstromen, opdat een verscheidenheid aan oplossingen wordt voorkomen;
- Creëer zogenoemde multi-Cloud connectiviteit (zie ook hoofdstuk 4 Datacentrumdiensten) die geborgd wordt met security-maatregelen;
- Termineer Internet centraal in het netwerk waarop security-maatregelen van kracht zijn alvorens dit door te zetten naar de werkplek.



Figuur 9. Schematische representatie JenV netwerktopologie

5.5.1 Specifieke vervolgstappen en aandachtspunten

5.5.1.1 Het netwerk ondersteunt de aansluiting van Rijksverzamelpanden

Door de Rijksbrede concern-ontwikkeling is er een toename van de Rijksverzamelpanden. Deze panden kenmerken zich door het feit dat meerdere Rijksoverheidspartijen in een gebouw zijn ondergebracht waarbij de zogenaamde IDV-P (ICT-Dienstverlener-Pand) de gebouwgebonden infrastructuur levert als Netwerk, Wifi, printfunctionaliteit enzovoorts. Dit is vastgelegd in de beschrijving 'ICT in het Rijkskantoor v 1_3 definitief_26aug2015'. De IDV-G (ICT-Dienstverlener Gebruiker) levert daarbij de logische werkplek voor haar gebruikers.

De consequentie van deze ontwikkeling is, dat een onderdeel van JenV niet alleen verantwoordelijk is voor de IDV-P maar ook voor de WAN-aansluiting in het pand waar de medewerkers van dat onderdeel werken.

Deze ontwikkelingen zorgen er voor dat naast onderdelen van JenV ook andere rijksoverheidspartijen het Justitienetwerk als dragernetwerk zullen gebruiken om bij hun gecentraliseerde werkomgeving te komen. Vaak is deze centrale werkplekfunctionaliteit geplaatst op een ODC.
Het ontsluiten van deze rijksoverheidspartijen naar hun ODC zal daarbij plaatshebben over een ander compartiment dan het Departementaal Vertrouwelijk (DEP-V) compartiment van Justitienet. Het gaat om een strikte scheiding tussen de domeinen, waarbij de werkplekdiensten in de komende jaren meer verdeeld zullen zijn tussen interne en externe partijen.

5.5.1.2 Het netwerk voorziet in zoneringsdomeinen

Het netwerk voorziet in de verschillende vertrouwensniveaus zoals (Zeer) Vertrouwd, Semi-vertrouwd en Onvertrouwd, conform Nederlandse Overheid Referentie Architectuur (NORA) beginsel. Belangrijke randvoorwaarden voor de bescherming van privacy gevoelige data zijn dat de verschillende netwerken logisch zijn gescheiden en dat op de overgangen afdoende controles ingevuld zijn. IAM, Logging en monitoring hiervan zijn instrumenten voor controle daarop.

Niet ieder JenV-onderdeel zal deze zoneringsdomeinen met dezelfde snelheid kunnen uitvoeren. Om in het huidige netwerk meerdere behoefte en ontwikkelingssnelheden te kunnen faciliteren, zal het netwerk meerdere beveiligingsdomeinen met verschillende vertrouwensniveaus moeten kunnen ondersteunen conform het (Nederlandse Overheid ReferentieArchitectuur) NORA-beginsel.

5.5.1.3 Het netwerk ondersteunt (draadloze) Internettoegang voor andere Rijksoverheidsmedewerkers (middels GovRoam).

Naast de bovengenoemde voorzieningen wordt van de IDV-P verwacht dat deze Internettoegang kan leveren voor de (rijks)overheidsmedewerkers in het pand die daar op bezoek zijn. Deze voorziening dient laagdrempelig te worden aangeboden. De Rijksoverheid heeft daarvoor GovRoam als dienst ontwikkeld.
Voor bezoekers die niet in dienst zijn van het Rijk is voorzien in een Gasten-WiFi, die vergelijkbaar als GovRoam wordt gerealiseerd, maar een eigen authenticatie oplossing kent.

5.5.1.4 Het netwerk sluit aan op het RijksOverheidsNetwerk (RON)

Vanuit het Rijk wordt het RijksOverheidsNetwerk gerealiseerd. Dit netwerk levert naast een backbone voorziening tussen de verschillende ODC's ook het aansluitnetwerk naar de verschillende verzorgingsgebieden. Hieronder wordt verstaan het WAN-netwerk van JenV (Justitienet) maar ook de netwerken van RWS, Belastingdienst, DUO/DICTU en SSC-ICT. Hierbij zal Justitienet telkens voor ieder vertrouwensniveau een aansluiting krijgen op het RijksOverheidsNetwerk.

5.5.1.5 Het netwerk realiseert ontsluiting van de ODC's

De Rijksoverheid ontwikkelt bij de ODC's zogenaamde ODC koppelnetwerken. De verschillende zogenaamde back-end omgevingen worden zo ontsloten richting het WAN. Om de eindgebruikers te laten verbinden met hun datacentervoorzieningen zal ook het Justitienet een koppeling met de ODC-koppelnetwerken moeten krijgen.

5.5.1.6 De connectiviteitdienst kent hybride vormen

Het netwerk zal niet alleen bestaan uit een besloten private netwerk zoals nu met het huidige Justitienet het geval is. Er dient in de toekomst rekening te worden gehouden met een grotere verscheidenheid aan ontsluitingen van panden en medewerkers. Locaties met een kleine groep eindgebruikers of tijdelijke locaties kunnen met behulp van Internetverbindingen met het eigen interne domein worden verbonden. Of waarbij met behulp van mobiele/draadloze verbindingen (LTE/4G/5G) deze verbindingen worden gerealiseerd.

5.5.1.7 Er is een centraal beveiligd koppelvlak (JUBIT) naar partners en Internet.

Omdat de beveiliging van de data en applicatie/systemen steeds essentiëler wordt zal er ook op centraal niveau voor de koppelingen naar Internet en partnernetwerken inspectie van verkeer op malware en virussen worden uitgevoerd om een eerste laag van 'defense' te hebben. Hier zullen ook meer toegespitste oplossingen worden geplaatst die dreigingen als Advanched Persitent Threat (APT) detecteren en mitigeren. Daarnaast speelt het centrale beveiligd koppelvlak niet alleen een rol in de garantie van vertrouwelijkheid en integriteit maar ook voor een beschikbaarheidsgarantie na het interne netwerk door anti-DDOS maatregelen en andere aanvullende maatregelen.

5.5.1.8 Zone-overgangen vinden zoveel mogelijk op een centraal punt plaats (JUBIT)

Inmiddels kent het Justitienet verschillende vertrouwenszoneringen, te weten (zeer) vertrouwd, semi-vertrouwd en onvertrouwd. Communicatie tussen verschillende vertrouwensniveaus lopen daarbij via een beveiligd koppelvlak waarbij een prominente rol is weggelegd voor een omgeving als JUBIT.

Hoofdstuk 6. Toegangsdiensten

Hoofdstuk 6 bevat de beelden die bij de betrokken onderdelen en marktpartijen over GeTIJ zijn opgehaald. Het gaat in op de relevante ontwikkelingen binnen het domein Toegangsdiensten.

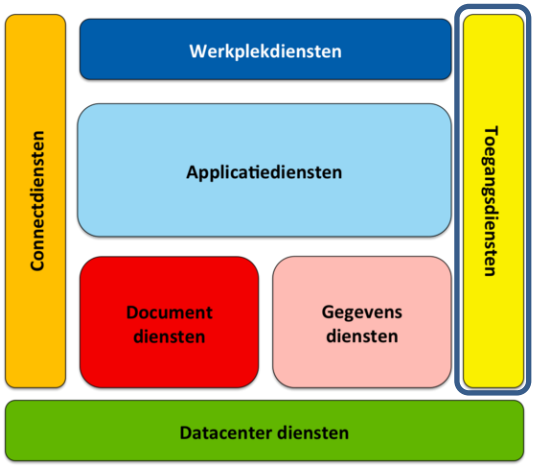
6.1 Samenvatting

Samenwerking over organisatiegrenzen neemt exponentieel toe de komende jaren. De samenleving digitaliseert steeds verder. Het organiseren van toegang tot data is een randvoorwaarde in een omgeving waar ook de dreigingen toe nemen. Dit vraagt om het gemeenschappelijk ontwikkelen van expertise en de uitbouw van de huidige Toegangsvoorzieningen van JenV en zijn onderdelen, naast een gemeenschappelijke aanpak op het niveau van de overheid en JenV. Dit moet op een zodanige manier gebeuren dat de samenwerking binnen het primaire proces maar ook de bedrijfsvoering op een veilige en gebruikersvriendelijke manier kan worden gefaciliteerd. Dit kan vooral worden bereikt door de toepassing van federatieve technieken.

6.2 Algemeen

In sterke mate neemt het belang van het adequaat beveiligen van informatie en assets toe. Enerzijds nemen dreigingen vanuit criminele organisaties via het Internet substantieel toe, anderzijds zien we dat organisaties worstelen met interne dreigingen vanuit personeel of gecompromitteerde ICT.

Het geheel van processen, procedures en techniek rondom het beheren van identiteiten en het toekennen van autorisaties aan assets en informatieobjecten wordt gefaciliteerd door het domein Toegangsdiensten[20].



Figuur 10 EAR domein Toegangsdiensten

De wereld om ons heen wordt steeds complexer door digitalisering. We werken steeds meer samen. Afhankelijk van de context wordt geautoriseerde toegang vereist. Bij voorkeur inloggen via SingleSignOn (SSO) over meerdere applicaties of platformen heen.
Afhankelijk van wie men is (burger, bedrijf of ambtenaar), welke (actuele) rol men binnen de organisatie heeft, de locatie van waaruit vanuit men de bron wilt benaderen en vanaf welk device worden fijnmazige autorisatiematrixen toegepast. Bovendien is er in onze maatschappij waarbij informatie steeds meer waard wordt een sterke behoefte te onderkennen aan dataclassificatie en deze fijnmazig toe te kunnen passen op niet-publiekelijke informatie.

[20] Ietwat vrijer vertaald - 'Toegang' betekent volgens de 'Van Dale' de weg waarlangs je ergens kunt komen. Toegang in de context van dit stuk is de weg die gevolgd moet worden om gebruik te kunnen maken van de voorzieningen (data en assets) die benodigd zijn om (werknemers, burgers of bedrijven) taken uit te voeren.

Daarnaast wordt een nog omvangrijker (internationaal) netwerk van opdrachtgevers, opdrachtnemers en dienstverleners voorzien. Dit versterkt de behoefte aan het veilig kunnen uitwisselen van informatie. Complex is dat de rollen of eigenschappen van de in het netwerk of keten aanwezige identiteiten regelmatig kunnen wisselen.
JenV beweegt van een informatiebeveiligingsconcept 'muur-om-stad-principe' naar het beveiligen van individuele data (hek om huis in de stad principe) waarbij het wenselijk is altijd en overal op een veilige wijze te kunnen beschikken over informatie (zie ook hoofdstuk 5, CD).

6.3 Visie

Samenwerking heeft steeds meer plaats buiten het eigen domein c.q. de infrastructuur van JenV en de onderdelen in het kader van zowel de ketensamenwerking als de bedrijfsvoering. Er worden steeds meer data uitgewisseld. Deze ontwikkeling gaat verder door bijvoorbeeld de groei van de Cloud-dienstverlening en de verdiepende Justitie samenwerking met andere landen. In dat kader dient toegang tot relevante informatie en assets integraal (met een nadruk op data), afhankelijk van de gewenste context georganiseerd te worden.

6.4 Noties

6.4.1 Federatie als basis

Federatie is de basis voor zowel toegang buiten een eigen veiligheidsdomein toegang tot eigen voorzieningen van JenV, evenals voorzieningen van (in- en externe) partners. De op open standaarden gebaseerde concepten van federatieve toegang ondersteunen een overheid die steeds verder digitaliseert in ketensamenwerkingen, niet alleen met overheidsorganisaties, maar ook in contact met burgers en bedrijven (de samenleving). Er is hierbij binnen JenV maar ook daarbuiten een sterke beweging te onderkennen waarbij het onderscheid tussen authenticatie en autorisatie op interne- en externe voorzieningen vervaagt. De wijze waarop dit intern en extern wordt ingevuld is functioneel en technisch hetzelfde.

Federatieve uitgangspunten zijn essentieel bij het adapteren van (externe) diensten waarbij de controle over de organisatie-eigen identiteit gehandhaafd blijft. Met andere woorden: met een logische identiteit en administratief beheer kan vanuit de eigen organisatie toegang worden verleend tot omgevingen bij derden waarmee een vertrouwensrelatie is opgebouwd.
Bij het autorisatie- en authenticatieproces kan het noodzakelijk zijn bij meerdere partijen of bronnen bij een identiteit behorende attributen te verifiëren. De communicatie met vertrouwde partijen wordt centraal aangestuurd vanuit een centrale federatieve gedistribueerde infrastructuur waaraan deelnemer partijen verbonden zijn.

JenV voorziet de volgende toepassingen ondersteund door federatieve technieken:

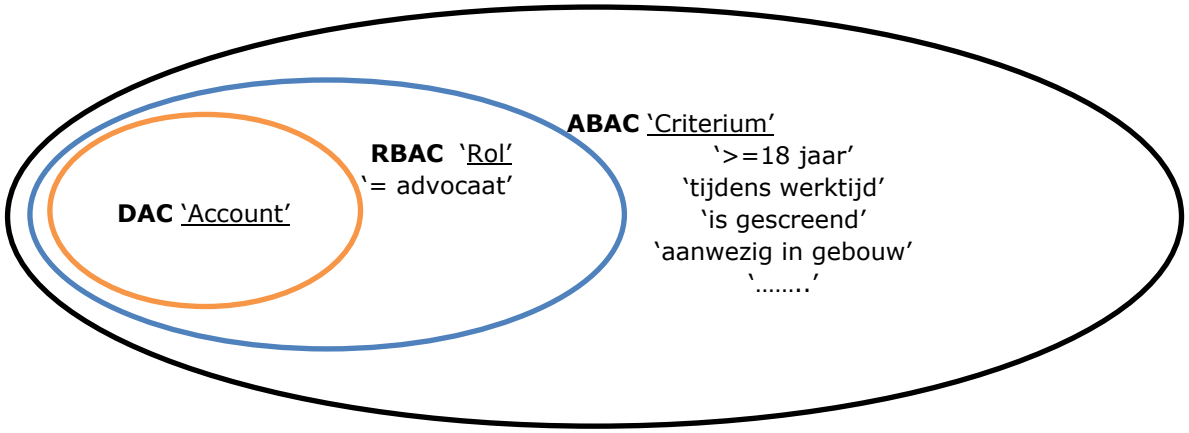
1. Samenwerkingsverbanden tussen overheidsorganisaties. In het kader van een efficiënte dienstverlening naar de burger en het bedrijfsleven (de samenleving) is er een noodzaak ontstaan om organisaties beter te laten samenwerken. Denk aan IDENSYS / EIDAS, waarop JenV naadloos moet aansluiten. De Gemeenschappelijke Digitale Infrastructuur (GDI) is de verplichte standaard van de overheid voor toegang van burgers en bedrijven (onder andere advocaten) tot de overheid van Nederland en de overheden binnen de Europese Unie;
2. Het toevoegen van vertrouwelijkheids- en betrouwbaarheidsfuncties bij het uitwisselen van gegevens over identiteiten. Het betrouwbaar laten verlopen van

zogenoemde 'realtime' sessies is hier van specifiek belang bij de dienstverlening naar de burger en bedrijven;
3. Het samenvoegen van infrastructuren met verschillende identiteitsbronnen en domeinen;
4. Het afnemen van diensten bij derden op basis van een identiteit van het eigen JenV domein. Dit kunnen externe (commerciële) partijen zijn, maar dit kunnen ook ministeries zijn die diensten aanbieden binnen het Rijk.

De uitgangspunten rondom federatieve diensten passen bij het steeds complexer, en organisatie- en grensoverschrijdend groeiende infrastructuurlandschap binnen JenV voor de periode 2017-2025 waarbij grip op autorisaties op vertrouwelijke informatie kan worden gegarandeerd.

6.4.1.1 Naar Context gerelateerde toegang

Er ontstaat steeds meer behoefte aan context afhankelijke toegang tot diensten, applicaties en informatie. Toegang verlenen vanuit een eenvoudige, maar toch fijnmazige autorisatiestructuur is hierbij van belang. Bij de complexiteit en fijnmazigheid van de infrastructuur- en voorzieningen voor applicaties passen flexibele en effectieve autorisatiemiddelen gebaseerd op het koppelen van attributen (eigenschappen) aan een identiteit.
Waar 'Discretionary Access Control' (DAC) alleen autorisaties op basis van een account toepast en 'Role Based Access Control' (RBAC) alleen op een rol of identiteit autorisaties kan toepassen kent 'Attribute Based Access Control' (ABAC) attributen per gebruiker, waarbij de attributen kunnen verschillen. Zie hiervoor Figuur 9. ABAC past bij de functionele behoefte voor fijnmazige autorisatie die er in de komende jaren binnen JenV zich verder ontwikkelt.



Figuur 11 Schematisch overzicht paradigma's toegang

6.4.2 Bring Your Own Identity (BYOID) als uitgangspunt

Steeds meer wil men van het gemak maar ook vanwege efficiency publieke identiteiten met een hoog betrouwbaarheidsniveau kunnen gebruiken in JenV context. Concreet betekent dit dat een rijbewijs of identiteitsbewijs verkregen bij de gemeente kan worden aangemerkt als 'vervanger' voor de Rijkspas. Een uniek identificatienummer van het rijbewijs of paspoort wordt gekoppeld aan het systeemlandschap van JenV en verschaft

daarmee de toegang tot assets (gebouw, werkplek, enzovoorts) binnen JenV. Privacy is een belangrijk aspect waarmee rekening gehouden moet worden bij Toegangsdiensten en in het bijzonder bij BYOID.

Een praktijkvoorbeeld uit 2025

Mevrouw Pieterse is naast een burger van Nederland ook een advocaat gevestigd in Maastricht. Het Advocatenregister is een gezaghebbende bron met alle formeel aangestelde advocaten van Nederland. Dit register is opgenomen in IDENSYS (het Nederlandse systeem voor elektronische identificatie (eID)). Met een digitale sleutel is een 2 factor authenticatie (dubbele sloten op de deur) mogelijk en is het mogelijk om het dossier van haar cliënten in te zien bij het OM van Nederland en over de grens het OM van België. Maar daar gaat het nu niet om bij mevrouw Pieterse. Ze heeft een boete gekregen van € 260,-. Ze is geflitst bij het door rood rijden in Almelo. Dit wil mevrouw Pieterse met eigen ogen zien. Met dezelfde digitale sleutel die mevrouw Pieterse gebruikt als advocaat logt zij in op de CJIB voorziening en kan de foto zien op grond waarvan zij de bekeuring heeft gehad. Het klopt, ... de foto is haarscherp. Vervelend maar waar. Maar goed, morgen naar de rechtbank van Den Bosch om de afhandeling bij te wonen van de zaak 'Postbankdiefstal'. Haar IDENSYS pas geeft haar gasttoegang tot de rechtbank. Grappig hoe dit soort zaken zich ontwikkelt, de rechter van de zaak ging naar binnen met zijn Legitimatiebewijs. Erg blij kijkt hij niet, en met reden…... Hij zat in een café en wilde de zaak gaan bestuderen, toegang werd echter geweigerd, wat blijkt, conform het toegangsbeleid. Een gevoelig dossier als de 'Postbankdiefstal' mag alleen vanaf kantoor, de rechtbank of de gecontroleerde thuislocatie van de rechter ingezien worden

Voorbeeld IV. De Advocaat

6.4.3 Toezicht

Toegangsdiensten hebben een stevige relatie met toezicht. De volgende noties zijn in dit kader te duiden naar 2025:

Auditen. 'Vertrouwen' in een partner of partners in een federatief stelsel is cruciaal. Dit is een randvoorwaarde voor succes. Relevant daarbij is het vaststellen / adopteren van normen / standaarden ten behoeve van het opzetten en in stand houden van vertrouwensrelaties in een federatief stelsel. Een uniforme systematiek voor het auditen maakt daar onderdeel van uit.

Logging & monitoring. De behoefte van JenV aan het context afhankelijk toegang kunnen verschaffen tot JenV omgevingen vereist maatregelen die zorgdragen voor het detecteren van afwijkingen, trends en onrechtmatigheden. Specifiek is er een noodzaak voor het kunnen correleren van verschillende loggings- bronnen om relevante verbanden te kunnen leggen ten behoeve van de analyse van dreigend gedrag op de infrastructuur van JenV. Voorbeelden hiervan zijn:

1. Herkennen van een gedistribueerde 'brute-force' attacks waarbij op een of meerdere accounts vanaf geografisch verspreide locaties wordt geprobeerd in te loggen'. Dit kan zowel plaatsvinden op de generieke infrastructuur zoals datacenters, als werkplekken maar ook op data ontsluitingsmechanismen zoals Application Programming Interfaces (API's);

2. Herkennen van afwijkend gedrag van medewerkers in relatie tot hun werkzaamheden (auditeerbaarheid). Voorbeeld: het onrechtmatig benaderen van een dossier waartoe ze niet zijn geautoriseerd, of het tonen van bovenmatige interesse in informatie waartoe deze wel toegang toe heeft, maar geen directe betrokkenheid;

3. Herkennen van afwijkend gedrag door apparaten (denk aan o.a. IoT toepassingen);

4. Herkennen van trends in de infrastructuur: plotselinge uitzonderlijke toename van netwerkverkeer, resourcegebruik, enzovoorts.

Geautomatiseerd kunnen medewerkers met bijbehorende identiteiten en attributen preventief worden geblokkeerd om het risico van potentiele (imago)schade door dergelijke aanvallen te minimaliseren.

6.5 Vervolgstappen

Samenwerking vindt steeds meer buiten het eigen domein plaats, zowel binnen ketens als met externe partijen. Voor de verdere concretisering van de noties worden de volgende uitgangspunten voorgesteld. Het gaat in deze paragraaf over de inhoud van de verandering en niet zozeer over projectdoelstellingen;

1. Het JenV Identity en Access management platform voorziet in context-bewuste autorisatie en authenticatie voorzieningen:
    - Informatie is geclassificeerd en passende autorisatie en authenticatie maatregelen worden toegepast[21];
    - We werken steeds meer samen binnen de Rijksoverheid op verschillende plaatsen met verschillende apparaten, specifiek voor elk apparaat worden specifieke toegang verleend tot informatie.
2. Federatieve toegang is de basis voor in- en externe authenticatie en autorisatie verzoeken;
    - Grip op eigen identiteiten, op het 'life cycle management' van eigen identiteiten door middel van beheer van identiteiten en autorisaties in binnen eigen organisatie domein;
    - Voorzien wordt dat toegang tot interne- en externe assets of informatie-objecten steeds fijnmaziger wordt, op basis van meerdere eigenschappen (attributen), potentieel uit meervoudige bronnen wordt toegang verleend;
    - Federatie voorziet in een het mogelijk maken van een hogere gebruikerstevredenheid (faciliteert onder andere SingleSignOn en het inloggen op diensten van derden met een organisatie-eigen gebruikersnaam).
3. Zonder governance geen toegangsdiensten;
    - Toegangsvraagstukken kennen een groot business component, autorisaties zijn tenslotte afgeleiden van functiehuizen en bijbehorende takenpakketten. Het is essentieel dat er regie wordt gevoerd over de huidige- en nog te ontwikkelen toegangsdiensten. Hierbij wordt voorzien in de volgende taken voor dit regieteam:
        - Tactisch en strategisch beheer over de diensten binnen het toegangsdomein;
        - Door ontwikkelen van de toegangsdiensten: het opstellen van een roadmap en definiëren van de software lifecyle;
        - Contact met commerciële marktpartijen.

6.5.1 Specifieke vervolgstappen

De volgende specifieke uitgangspunten op het domein Toegangsdiensten worden onderkend:

1. Een Federatieve Authenticatie en Autorisatie Service (FAAS) hanteert breed door de markt geaccepteerde standaarden.
    - De FAAS dienst wordt bij gelijke geschiktheid en functionaliteit ontwikkelt op basis van open standaarden. Het onderliggende platform kan worden geleverd door een commerciële partij, echter dient deze partij open standaarden in haar pakket op te nemen;
    - Uitwisseling van authenticatie- en autorisatie attributen vindt plaats op basis van standaarden zoals Security Assertion Markup Language (SAML) en eXtensible Access Control Markup Language (XACML);

[21] Zie verder het domein Gegevensdiensten (GD).

- Traditionele platformen dienen (zover van belang in dit kader) via federatieve technieken ontsloten te kunnen worden, hiervoor dient een platform ingericht te worden waarbij onderwater ABAC technologie en onderliggende protocollen worden gebruikt om met de rest van het landschap te kunnen communiceren.

Bijlage 1. Betrokkenen

Personen betrokken / geraadpleegd in het kader van het project GeTIJ.

Naam	Organisatie	Betrokken / geraadpleegd
David Allessie	GARTNER	Review rapport GeTIJ, versie 0.1
Danny Appelboom	DI&I	Visnetactie CSB 28 juni, 4 EAR domeinen Review initieel concept
Floris van der Bas	RWS	Visnetactie 17 mei, 4 EAR domeinen
Robert Bennis	RWS	Visnetactie 17 mei, 4 EAR domeinen
Maarten van de Berg	BZK/Rijkscloud	Visnetactie DCD 24 april 2017
Ben Binnendijk	DJI	Visnetactie TD Programma Toegang 20 april 2017 Review initieel concept GeTIJ
Rene Bladder	DI&I	Visnetactie TD Programma Toegang 20 april 2017 Review kopij TD Review veranderaanpak Toegang
Luc Boelhouwer	OM	CTO workshop GeTIJ 3 mei
Remco Boersma	DI&I	Project GeTIJ business consultant / redactie
Wouter Borremans	Strict Consultancy	Project GeTIJ business consultant / redactie
Wim Bovendeert	DJI	Visnetactie CD Technisch Architecten 13 april (…)
Erik-Olaf Brinkers	CJIB	Visnetactie TD Programma Toegang 20 april 2017 Review kopij TD Review veranderaanpak Toegang
Anny Brouwers	DI&I	Visnetactie GD 8 mei
Geert Dedden	CJIB	CTO aanspreekpunt GeTIJ/DCD CTO workshop GeTIJ 3 mei
Ronald Doest	Politie	Review rapport GeTIJ, versie 0.1 (via AF JenV)
Peter Don	DJI	CTO aanspreekpunt GeTIJ/DCD en CD CTO workshop GeTIJ 3 mei
Jos van Dijk	DI&I	Visnetactie GD 8 mei Review kopij GD
Arnout Drenthel	Bento Presentaties	Totstandkoming praatplaat GeTIJ
Michel Eindhoven	Reclassering	Terugkoppeling en review GeTIJ concept versie
Martina Gaiser-Janáčková	GARTNER	Review rapport GeTIJ, versie 0.1
Marco Groenestein	Informatieplan JenV	Rapport GeTIJ, versie 0.1 in Informatieplan 2018
Dick Groeneveld	DI&I	Review initieel concept GeTIJ Alignment met Architectuur JenV
Paul Grooten	CBS	Visnetactie GD 21 juni
Annelies Hermans	DP&O	Redactie (Communicatieadviseur) GeTIJ rapport
Steven Jansen	SHELL	Visnetactie 17 mei, 4 EAR domeinen
Dennis Kersens	BZK/Rijkscloud	Visnetactie DCD 24 april 2017
Peter Kivits	GATNER	Review rapport GeTIJ, versie 0.1
Wilbert van der Kolk	DI&I	Visnetactie CSB 28 juni, 4 EAR domeinen
Jeroen Krikke	BZK/ SSC ICT	Visnetactie CD Technisch Architecten 13 april (…)
Richard van der Kroft	Informatieplan JenV	Rapport GeTIJ, versie 0.1 in Informatieplan 2018
Leon Kuunders	IND	CTO workshop GeTIJ 17 juli
Gino Laan	BZK	Review rapport GeTIJ, versie 0.1
Gert-Jan Landwaart	OM	Visnetactie CD Technisch Architecten 13 april (…)
Steven Levelt	SHELL	Visnetactie 17 mei, 4 EAR domeinen
Jan van Lingen	CJIB	Review rapport GeTIJ, versie 0.1
Wijnand Lodder	DJI	CTO aanspreekpunt GeTIJ/DCD en CD
Michiel van der Meer	Surfnet	Visnetactie 13 juni, 4 EAR domeinen
Margreet Meijer	IND	CTO aanspreekpunt GeTIJ/TD CTO workshop GeTIJ 3 mei en 17 juli
Gerard Middendorp	Politie	Review rapport GeTIJ, versie 0.1 (via AF JenV)
Henk Jan van der Molen	DI&I	Informatiebeveiliging JenV

Nico van Oldenbeek	DI&I	Project GeTIJ projectleider
Johan Oostveen	Politie	CTO workshop GeTIJ 3 mei
Kim Öztürk	DI&I	Project GeTIJ projectondersteuner
Emine Özyenici	DI&I	Project GeTIJ opdrachtgever
Sven Peeman	COA	Visnetactie CD Technisch Architecten 13 april (…) CTO workshop GeTIJ 3 mei
Hans Poort	IND	CTO workshop GeTIJ 17 juli Review initieel concept GeTIJ
Cas Roest	DI&I	Project GeTIJ CSB
Peter van Schaik	RvdR	CTO workshop GeTIJ 3 mei
Dirk Scholten	Just Id	CTO aanspreekpunt GeTIJ/GD CTO workshop GeTIJ 3 mei & 17 juli
Ger Slootenbeek	RWS	Visnetactie GD 21 juni,4 EAR domeinen
Ronald Smit	DI&I	Project GeTIJ opdrachtnemer
Evert Straatman	COA	CTO workshop GeTIJ 3 mei
Lieven van der Tas	DJI	Visnetactie CD Technisch Architecten 13 april (…) CTO workshop GeTIJ 3 mei Review initieel concept GeTIJ
Harold Teunissen	Surfnet	Visnetactie 13 juni alle EAR domeinen
Edwin Tjon-a-meeuw	Reclassering	Visnetactie CD Technisch Architecten 13 april (...)
Danny Venema	Just Id	CTO Contactpersoon GeTIJ/GD Visnetactie GD 8 mei
David Vermeulen	RvdR	Visnetactie CD Technisch Architecten 13 april (…)
Peter Vermeulen	BD/DVB	Visnetactie GD 8 mei
Fanny Wallebroek	DI&I	Openbaarheid Data JenV
Ruud van der Wouden	RvdR	CTO workshop GeTIJ 17 juli
Wil Wijnen	DI&I	Project GeTIJ CSB
Marianne Zijderveld	BD/DGVZ	Visnetactie DCD 24 april 2017 Review initieel concept GeTIJ Totstandkoming praatplaat GeTIJ
Tjerk Zwanenburg	CJIB	Review AF JenV concept rapport GeTIJ, versie 0.1

Tabel 2. Personen betrokken / geraadpleegd in het kader van het project GeTIJ.

Bijlage 2. Geraadpleegde documenten

De volgende documenten zijn in het kader van dit onderzoek geraadpleegd:

- Cloudcondities Digitale Werkomgeving (VenJ, 10 november 2016).
- Cloudstrategie VenJ (VenJ, juli 2015).
- Enterprise Architectuur Rijk (ICCIO 2014)
- Enterprise Architectuur VenJ (VenJ, 2016)
- Informatiestrategie VenJ 2017-2022 (VenJ, juli 2016).
- Maak Waar (Studiegroep Informatiesamenleving en Overheid, 2017).
- Recht en Veiligheid in de 21e eeuw (VenJ 2017).
- Technologiescan VenJ (VenJ, maart 2017).
- Vervolg rapport t.b.v. de Investeringsagenda voor de SSO-ICT infrastructuur 2017-2027, versie 0.99 (BZK, 2017).

Bijlage 3. Handreiking veranderaanpak

In deze bijlage treft u een handreiking voor projecten en activiteiten op hoofdlijnen aan voor een veranderaanpak. Deze handreiking is samengesteld op basis van de uitgangspunten zoals die in deze rapportage zijn benoemd. Belangrijk hierbij te melden is dat op verzoek van de opdrachtgever 'out of the box' is gedacht. Dat wil zeggen dat de domeinen zijn benaderd buiten de huidige financiële- en beleidskaders. De handreiking voor een veranderaanpak moet indien besloten wordt deze daadwerkelijk uit te voeren (of delen daarvan) verwerkt worden in de informatieplannen / jaarplannen van JenV. De besluitvorming omtrent de veranderaanpak zal dan voorgelegd dienen te worden aan de CIO Raad (SBR en BR). Indien het verzoek voor 2018 is gedaan dan staat dit uitgewerkt ('waarom' en 'wie'). Doelstelling moet zijn om de verandering zoveel mogelijk 'kortcyclisch' en kleinschalig op te pakken.

I. Gegevensdiensten Veranderaanpak 2018-2025

De volgende relevante projecten en activiteiten dienen uitgevoerd te worden voor een veranderaanpak Gegevensdiensten:

A. Integrale aanpak binnen JenV om informatiegestuurd te werken op basis van een helder informatiebeleid, datastrategie en data governance;
    - Waarom: Deze activiteit is randvoorwaardelijk om dit onderwerp in samenhang op te kunnen pakken binnen JenV;
    - Door wie: Verzoek wordt meegenomen in het Informatieplan JenV 2018.
B. Adapteren of ontwikkelen van standaarden die informatie gestuurd werken in de keten efficiënter én aantrekkelijker maken binnen JenV;
    - Waarom: Deze activiteit is randvoorwaardelijk om dit onderwerp in samenhang op te kunnen pakken binnen JenV;
    - Door wie: Het verzoek wordt meegenomen in het Informatieplan JenV 2018.
C. Integrale aanpak (JenV breed) ten behoeve van het classificeren/rubriceren van informatie. Aanschaffen of activeren van reeds bestaande tooling voor het geautomatiseerd rubriceren van informatie en data uit verschillende bronnen. Zie ook IV.B;
    - Waarom: Ervaring opdoen met het automatisch classificeren van data. Classificatie is randvoorwaardelijk zowel voor in het kader van DCD en TD;
    - Door wie: Het verzoek wordt meegenomen in het Informatieplan JenV 2018.
D. Per keten én op JenV niveau een verantwoordelijke te installeren die ten behoeve van een centraal berichten knooppunt standaardiseert, adviseert en de kwaliteit van data garandeert. Dit kan in de vorm van een expertisecentrum maar kan ook worden belegd op directieniveau in de vorm van een Chief Data Officer (CDO);
    - Staat open voor 2019 en verder, de noodzaak is echter erg groot om indien mogelijk de positie eerder in te vullen.
E. Elke partij in de keten heeft een koppeling naar een centraal berichten knooppunt. Een centraal berichten knooppunt draagt zorg voor distributie, uitwisseling van data en beantwoording van vragen van ketenpartijen.
    - Staat open voor 2019 en verder. Uitkomst van I. A en I.B is sterk bepalend voor de invulling van dit project / deze actie.

Verander roadmap GD	2018	2019	2020	2021	2022	2023	2024	2025
A. Integrale aanpak								
B. Standaarden								
C.. Data classificatie PoC								
D. Data classificeren								
E. Installatie								
F. Realisatie								

Tabel 3. Gegevens Diensten - Voorzet projecten / activiteiten roadmap[22].

II. Data Centrum Diensten Veranderaanpak 2018-2025

De volgende relevante projecten en activiteiten dienen uitgevoerd te worden voor een veranderaanpak Data Centrum Diensten. Een kleinschalige en kortcyclische aanpak moet de doelstelling zijn waarbij binnen afzienbare termijn (eerste) resultaten worden geboekt.

A. Het oprichten en inrichten van een (virtueel) JenV Cloud regie/competence center;
   - Waarom: het (door)ontwikkelen en vastleggen van kennis rondom het eenduidig toepassen van Cloud technologie binnen JenV en haar onderdelen is essentieel bij het infrastructureel automatiseren en faciliteren van gestandaardiseerde bouwblokken en diensten binnen de context van de Trusted Cloud;
   - Door wie: Het verzoek wordt meegenomen in het DI&I jaarplan 2018/Informatieplan JenV 2018.

B. Het vaststellen van een rijksbrede standaard met betrekking tot het interne- en externe Trusted Cloud platform;
   - Waarom: platform- en leverancier standaardisatie zijn noodzakelijk voor de realisatie van de Trusted Cloud. Platformkeuzes (zowel intern als extern) bepalen de wijze waarop gestandaardiseerde infrastructurele bouwblokken en diensten geautomatiseerd tot stand kunnen komen (orkestratie en provisioning);
   - Door wie: Het verzoek wordt meegenomen in het DI&I jaarplan 2018/Informatieplan JenV 2018.

C. Opstellen van een hoog-over ontwerp voor ene gestandaardiseerd Trusted Cloud platform binnen JenV en de implementatie daarvan;
   - Waarom: uniformiteit over onderdelen heen. Vanuit continuïteits- en standaardisatieoptiek is het wenselijk over de onderdelen heen een gestandaardiseerd platform te realiseren;
   - Door wie: Het verzoek wordt meegenomen in het DI&I jaarplan 2018/Informatieplan JenV 2018.

[22] Legenda Tabel 3- 7 – 'Donker Oranje' is eenmalig project of activiteit. 'Licht Oranje' is een doorlopende lijnactiviteit.

D. Uitvoeren van een Proof of Concept: gestandaardiseerd Trusted Cloud platform ten behoeve van een ontwikkelomgeving;
   - Waarom: Ervaring opdoen, verificatie stabiliteit, performance, security en orkestratie aspecten;
   - Door wie: Het verzoek wordt meegenomen in het DI&I jaarplan 2018/Informatieplan JenV 2018.

E. Realisatie JenV Platform.
   - Waarom: realisatie infrastructurele wendbaarheid en bouwblok- en dienst standaardisatie;
   - Door wie: DI&I (regie) en betrokken onderdelen zoals beschreven onder 'C'.

Verander roadmap DCD	2018	2019	2020	2021	2022	2023	2024	2025
A. Inrichten virtueel centr.								
B. Rijksbrede Standaard								
C. Ontwerp JenV Platform								
D. Uitvoeren van een Proof of Concept								
C. Realisatie JenV platform								

Tabel 4. Data Centrum Diensten - Voorzet projecten / activiteiten roadmap.

III. Connectdiensten Veranderaanpak 2018-2025

De volgende relevante projecten en activiteiten voor een veranderaanpak voor Connectdiensten. De noodzaak voor het hebben van een Justitie netwerk blijft bestaan in de komende jaren, zie verder hoofdstuk 5 'Connectdiensten' voor een onderbouwing.

A. Verwerving JN 4.De volgende stappen daarin op hoofdlijnen voor 2018: [1] Evaluatie JN3 (door JenV), [2] Bepalen scope JN4 (door JenV), [3] Opstellen specificaties JN4 (door JenV), [4], Opstellen bestek JN4 (door RWS), [4] Uitvraag markt (door RWS);
   - Waarom: Aangezien het contract JustitieNet 3 (JN3) met Tele2 afloopt in januari 2019 moet er in 2018 een 'verwerving van Justitienet 4' (JN4) plaatsvinden;
   - Door wie. Het verzoek is meegenomen in het jaarplan DI&I 2018 en wordt opgepakt door DII.

B. Migratie JN4. Migratie van JN3 naar JN4.
   - Noodzakelijk van start in 2019.

Verander roadmap CD	2018	2019	2020	2021	2022	2023	2024	2025
A. Uitvraag markt JN4								
B. Migratie JN 4								

Tabel 5. Connectdiensten - Voorzet projecten / activiteiten roadmap.

IV. Toegangsdiensten Veranderaanpak 2018-2025

De volgende relevante projecten en activiteiten dienen uitgevoerd te worden voor een veranderaanpak Toegangsdiensten:

A. Het opstellen of adopteren van normen/standaarden t.b.v. het opzetten en in stand houden van een federatie en de vertrouwensrelaties. Dit bij voorkeur in overeenstemming of anders in afstemming met de Overheid (BZK & EZ);
   - Waarom: In het kader van een vertrouwensrelatie bij Federatieve Toegang moet het duidelijk zijn wie waar aan moet voldoen;
   - Door wie: De activiteiten worden door de domeinhouder Toagang/ het programma Toegang/Informatieplan JenV 2018 opgepakt.

B. Het kwalificeren van bestaande data binnen de onderdelen van JenV. Het inrichten van een proces voor kwalificatie van nieuwe data binnen de onderdelen. Start met een 'proof of concept' met automatisch kwalificeren van data binnen een onderdeel. De in 'I GD' opgestelde normen zijn daarbij het uitgangspunt;
   - Zie verder I GD, punt C en D.

C. Het aanwijzen en inrichten van een (virtueel) 'Centre of Excellence' of 'expertisecentrum' ten behoeve van Toegang binnen JenV of de rijksoverheid;
   - Zie verder I GD, punt C en D.

D. Het opstellen van een globaal ontwerp van een FAAS ten behoeve van (de onderdelen van) JenV. De afstemming van het ontwerp met de Overheid (BZK & EZ);
   - Waarom: Het helder maken wie wat moet realiseren tot 2025;
   - Door wie: Activiteiten worden door de domeinhouder Toegang / het programma Toegang / Informatieplan JenV 2018 opgepakt.

E. De realisatie van het FAAS of bouwstenen (roadmap) daarvan bij de onderdelen en / of (verder) op JenV niveau, dit laatste indien de uitkomst het toelaat.
   - Waarom: Realisatie bouwstenen Toegang op basis van afzonderlijke business case;
   - Door wie: Activiteiten worden door de domeinhouder Toegang / het programma Toegang / Informatieplan 2018 JenV opgepakt.

Verander roadmap TD	2018	2019	2020	2021	2022	2023	2024	2025
A. Normen & standaarden								
B. Kwalificeren data PoC	I.GD							
C. Kwalificeren Data		1. GD						
C. Inrichten FAAS								
D. Globaal ontwerp								
E. Realisatie								

Tabel 6. Toegangsdiensten - Voorzet projecten / activiteiten roadmap.

Afkortingen

Gebruikte afkortingen

- ABAC Attribute Based Access Control
- API Application Programming Interface
- APT Advanced Persistent Threat
- AVG Algemene Verordening Gegevensbescherming
- BIR Baseline Informatiebeveiliging Rijk
- BYOID Bring Your Own Identity
- CD Connectdiensten (domein EAR)
- CDO Chief Data Officer
- CTO Chief Technology Officer
- CASB Cloud Access Broker
- CSB Centraal Strategisch Beheer
- DAC Discretionary Access Control
- DCD Data Centrum Diensten (domein EAR)
- DEP-V Departementaal Vertrouwelijk
- EAR Enterprise Architectuur Rijk
- FAAS Federatie Authenticatie en Autorisatie Service
- FS Federatie Service
- GeTIJ Generieke Technische Infrastructuur Justitie 2017-2025
- GD Gegevensdiensten (domein EAR)
- GDI Gemeenschappelijke Digitale Infrastructuur
- PDC Producten en Diensten Catalogus
- JN Justitie Net
- JUBIT Centraal Beveiligd koppelvalk van JenV partners en Internet
- IaaS Infrastructure as a Service
- IAM Identity Access Management
- IDV-G ICT Dienstverlener Gebruiker
- IDV-P ICT Dienstverlener Pand
- IOT Internet of Things
- NIST National Institute of Standards and Technology
- NORA Nederlandse Overheid Referentie Architectuur
- ODC Overheids Data Center
- PaaS Platform as a Service
- RBAC Role Based Access Control
- RON Rijks Overheids Netwerk
- SaaS Software as a Service
- SAML Security Assertion Markup Language
- SSO Single Sign On
- Stg Staatsgeheim
- TA Technisch Architecten
- TD Toegangsdiensten (domein EAR)
- TPA Tijd, plaats en apparaat onafhankelijk
- TPAW Tijd, plaats en apparaat onafhankelijk werken.
- WAN Wide Area Network
- ODC Overheids Data Center
- XACML eXtensible Access Control Markup Language