Titel	:	Ketendoelarchitectuur Strafrechtketen
Datum	:	14-09-2020
Versie	:	1.0 (definitief)
Auteur	:	Strafrechtketen Architectuurraad
www	:	https://www.astraonline.nl

Inhoudsopgave

Deel 0: Inleiding en samenvatting 4
Status document 4
Samenvatting 4
De strafrechtketen 4
Ketendoelarchitectuur 4
Inleiding & leeswijzer 7
Positionering van de KDA 7
Documentstructuur, samenhang en versies 8
Leeswijzer 8
Toekomstige delen van de ketendoelarchitectuur 8
Deel 1: De strafrechtketen 10
De strafrechtketen 11
Visie op de Strafrechtketen 11
Pijnpunten 12
Informatiehuishouding in beweging 13
Duurzaam digitaal stelsel 13
Het strafrecht 14
De wet is basis 14
Ketenpartijen 14
Basisproces 15
Betrokkenen 16
Ontwikkelingen 18
Wetgeving 18
Nieuwe vormen van samenwerken 18
Kaders voor de architectuur 20
Rechtsstatelijkheid 20
Leidende principes digitalisering strafrechtketen 20
De “strafrechtketenbrug” 20
Digitaliseren in ketens 21
Architectuurprincipes strafrechtketen 23
Relaties met andere architecturen 25
Gegevensbescherming 25
Informatiebeveiliging 25
Deel 2: Essenties van de ketendoelarchitectuur 26
Mantra 27
De brug en de architectuur 30
Kernelementen 30
Interoperabiliteit 30
Informatiedomeinen 31
Het begrip zaak 32

Het begrip dossier 32
Originelen en kopieën 33
Maximale ontkoppeling 33
Dienstoriëntatie 33
Gelaagdheid 35
Interactiepatronen 36
Patroon: Afsprakenpatroon 37
Patroon: Notificatie- / Signaleringpatroon 38
Patroon: Vraaggestuurde informatiedeling 38
Verantwoorden en “historische gegevens” 38
Gemeenschappelijke voorzieningen 39
Ketensteunpuntvoorzieningen 39
Ketencommunicatievoorzieningen 42
Werking van de keten-communicatievoorzieningen in een casus 45
Casus – Overdacht PV van Politie naar het OM 45
Casus – Informeren advocaat van de verdachte tijdens de fase vervolging 46
Gegevensbescherming 47
Informatiebeveiliging 47
Bijlage 1: Aandachtspuntenlijst 49
Bijlage 2: Referenties 50
Bijlage 3: SRK bedrijfsfuncties en organisatieverantwoordelijkheden 51
Bijlage 4: A3 formaat platen 52
Grondvorm strafrechtproces 52
Hoofdfuncties Strafrechtketen 53
Samenhang ketencommunicatievoorzieningen 54
Informatiemakelaar 55
Lagen van IV-diensten 56
Informatiedomeinen 57

Deel 0: Inleiding en samenvatting

Status document

Dit document is opgesteld door de architectuurraad strafrechtketen in opdracht van het opdrachtgeversberaad (OGB). De leden van de architectuurraad komen vanuit de ketenpartijen, op het moment van schrijven zijn dat de Politie, het Openbaar Ministerie, de Rechtspraak (rechtbanken en hoven), Reclassering Nederland, de Koninklijke Marechaussee, Justid, Dienst Justitiële Inrichtingen, Centraal Justitieel Incassobureau, Jeugdzorg, Raad voor de Kinderbescherming, en de ketenondersteunende afdelingen Bureau Ketenregie en Directie Strafrechtketen beiden ondergebracht bij het ministerie ven JenV. De leden van de architectuurraad handelen daarbij vanuit hun kennis en expertise en vervullen een liaison rol naar hun achterban.

Dit document is in de OGB-vergadering van 8 juli 2020 besproken en door de voorzitter vastgesteld als sturingskader. Na toetsing bij de achterban in de verschillende ketenpartnerorganisaties en bij het Architectuurforum JenV is het document met een positief advies van de OGB ingebracht in het BKB. Het BKB heeft in haar vergadering van 10 september 2020 de ketendoelarchitectuur als sturingskader bekrachtigd.

Samenvatting

De strafrechtketen

De uitdaging van het strafrecht is om een eerlijke en tijdige reactie te geven op strafbare feiten c.q. crimineel gedrag, van incident t/m interventie – dan wel juist te voorkomen dat het tot crimineel gedrag komt. Het aldus functioneren van de strafrechtreten (SRK) kent ernstige knelpunten, niet alleen op het gebied van effectiviteit en efficiëntie, maar zelfs in het waarmaken van rechtsstatelijkheid. Daarnaast komen twee grote vernieuwingen op de strafrechtketen af, namelijk die van (1) Wetboek van Strafvordering (WvSv), en die van (2) de Wet politiegegevens (Wpg) en de Wet Justitiële en Strafvorderlijke gegevens (WJSG). Gebaseerd op het rapport van Van den Emster zijn daartoe veranderinitiatieven gestart. Dit geheel aan initiatieven voor het verbeteren van de samenwerking en informatievoorziening heeft richtlijnen en kaders nodig zodat de effectiviteit, samenhang en evolueerbaarheid van de strafrechtketen toeneemt.

Het opdrachtgeversberaad, tevens opdrachtgever van de architectuurraad strafrechtketen (OGB), legt met de “leidende principes digitalisering strafrechtketen” de nadruk op de onafhankelijkheid van de deelnemende organisaties en de noodzaak om veilig, betrouwbaar, gestandaardiseerd en eenvoudig informatie te kunnen delen tussen deze organisaties waarbij de informatievoorzieningen losjes aan elkaar gekoppeld worden.

Ketendoelarchitectuur

De ketendoelarchitectuur (KDA) faciliteert deze veranderinitiatieven en de leidende principes digitalisering SRK door negen architectuurprincipes en elf keten-communicatievoorzieningen te benoemen en een inventarisatie van ketensteunpuntvoorzieningen op te nemen. Samen creëren die de voorwaarden om de doelstelling te realiseren zoals verwoord in het mantra:

“… **digitaal, betrouwbaar en eenvoudig (informatie over) personen, zaken, beslissingen en bewijsmiddelen van begin tot eind van de keten volgen zodat de informatie tijdig en volledig beschikbaar is** …”.

De negen architectuurprincipes in de KDA formuleren de kern van het ‘beleid’ dat gevolgd wordt bij het realiseren van deze doelstelling. Ze verdiepen de Leidende principes digitalisering Strafrechtketen en specifiek toegespitst op de strafrechtketen ten opzichte van de meer algemeen geldende principes van de Nederlandse Overheid Referentie Architectuur en de Enterprise Architectuur principes “De Afspraken” van het ministerie JenV.

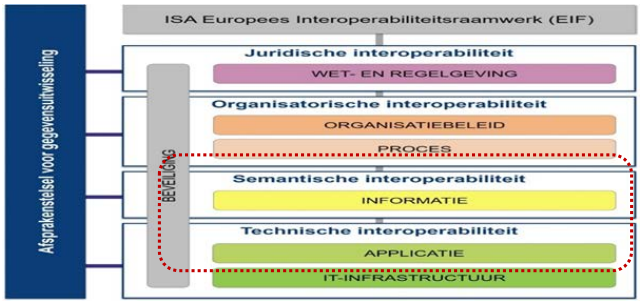
Tabel 1 De negen architectuurprincipes van de ketendoelarchitectuur

AP0 – Rechtstatelijkheid	**AP5 – Differentiatie waar nodig**
AP1 – Samenwerken	**AP6 – Digitaal is onze taal**
AP2 – Transparantie	**AP7 – Gegevenskwaliteit**
AP3 – Aanpassingsvermogen	**AP8 – Zaakgericht én persoonsgericht**
AP4 – Dienstoriëntatie	

De Leidende principes Strafrechtketen en de architectuurprincipes borgen dat ook op het vlak van digitale uitwisseling van gegevens

- de rechtstatelijke scheiding van de verschillende rollen en bevoegdheden in het strafproces gegarandeerd blijft (AP0),
- zodat partijen met behoud van die eigen zelfstandigheid goed en efficiënt kunnen samenwerken (AP1),
- de juistheid, tijdigheid en zorgvuldigheid (met name integriteit en authenticiteit) van gegevens gegarandeerd kan worden (AP7) en
- zowel persoonsgericht als zaakgericht gewerkt kan worden (AP8).

Het realiseren van de KDA verhoogt de interoperabiliteit in de strafrechtketen. In termen van het Europees interoperabiliteitsraamwerk (EIF) richt de KDA zich op informatie (semantische interoperabiliteit), applicaties (technische interoperabiliteit), beveiliging (authenticiteit, integriteit, beschikbaarheid) en de meer algemene aspecten van het proces (organisatorische interoperabiliteit).



Figuur 1 Afbakening van de Ketendoelarchitectuur op basis van het Europees Interoperabiliteitsraamwerk

De elf keten-communicatievoorzieningen in de KDA beschrijven een streefsituatie van een stelsel. Dit stelsel beperkt zich tot het verbeteren van de interoperabiliteit op de aspecten informatie en applicatie en de algemene aspecten van het proces. In termen van de in de Leidende principes Strafrechtketen gebruikte 'brug' analogie, vormen ze samen de concretisering van de horizontale legger en de verbinding naar de pijlers. De voorzieningen bestaan minimaal uit afspraken (toe te passen standaarden en richtlijnen) tussen ketenpartners en schrijven in de meeste gevallen ook het gebruik van specifieke ondersteunende keten IT-systemen voor.

*Tabel 2 De elf keten-communicatievoorzieningen van de ketendoelarchitectuur die samen de streefsituatie beschrijven. De met *) gemarkeerde voorzieningen zijn niet strafrechtketen specifiek.*

- **E-semantiek**
- **E-distributie**
- **E-index**
- **E-status**
- **E-portalen**
- **E-handtekening *)**
- **E-compliance**
- **E-toegang *)**
- **E-koppeling**
- **E-archief *)**
- **E-makelaar**

Het stelsel van keten-communicatievoorzieningen draagt zorg voor het gestandaardiseerd (interoperabel) E-semantiek)) ontsluiten (E-distributie, E-koppeling., E-makelaar, E-portalen) van de gegevens naar elkaar op een wijze die voldoet aan de genoemde Strafrechtketen specifieke principes en maakt daarbij de traceerbaarheid (E-index, E-status, E-archief) van informatie over personen, zaken, beslissingen en bewijsmiddelen ter ondersteuning van de samenwerking mogelijk. Dit uiteraard binnen de grenzen van grondslagen en verantwoordelijkheden (E-toegang, E-compliance) en de waarborgen voor de authenticiteit van informatie (E-handtekening).

Bij een volledig werkend en in gebruik genomen stelsel wordt het mogelijk om bijvoorbeeld de afhandeling van een winkeldiefstal inzichtelijk te maken ('te volgen') aan de hand van het ontstaan en uitwisselen van informatie in de keten zoals de registratie van het incident, de videobestanden in het dossier, de identificatie van de verdachte, het openen van een zaak ter vervolging en de afdoening. Dit vormt de basis voor het kunnen vinden van de juiste informatie voor professionals die betrokken zijn in die 'zaak' en van andere betrokkenen zoals slachtoffers en verdachten. Het feitelijk beschikbaar stellen van de informatie is en blijft een zaak van de verantwoordelijke ketenpartner.

Bij de opzet van deze voorzieningen is rekening gehouden met de grote vernieuwingen die op de strafrechtketen afkomen én het feit dat het in ketenverband niet mogelijk is om alle aanpassingen altijd synchroon te laten lopen. Dit maakt dat de communicatie aanpasbaar moet zijn, mee kan bewegen met de ontwikkelingen en prioriteiten en dus slechts 'losjes' is gekoppeld.

Naast de keten-communicatievoorzieningen beschrijft de KDA een tweede categorie ketenvoorzieningen genaamd **ketensteunpuntvoorzieningen**. Ketensteunpuntvoorzieningen ondersteunen inhoudelijke (proces)coördinatie en afstemming waarbij iedere organisatie afzonderlijk zijn verantwoordelijkheid behoudt. Daarmee richten ze zich in termen van het Europees interoperabiliteitsraamwerk (EIF) op organisatorische en juridische interoperabiliteit in de strafrechtketen. Bepalen welke ketensteunpuntvoorzieningen nodig zijn valt buiten de verantwoordelijkheid van de KDA, maar volgt uit de programma's en projecten en de achterliggende doelstellingen.

Ketensteunpuntvoorzieningen volgen wel de principes en worden gerealiseerd met behulp van de keten-communicatievoorzieningen. De KDA inventariseert ketensteunpuntvoorzieningen wel zodat we kunnen adviseren over hergebruik en er geen dubbele of overlappende voorzieningen ontstaan voor hetzelfde specifieke proces. Voorbeelden van ketensteunpuntvoorzieningen die in voorbereiding zijn of al bestaan zijn: Persoonsidentificatie en -verificatie, Advocatenportaal, Track & Trace bewijsmiddelen (forensisch materiaal).

Inleiding & leeswijzer

Positionering van de KDA

Waarom en waartoe dient deze KetenDoelArchitectuur (KDA)?

> *De KDA geeft kaders en richting aan het geheel van veranderinitiatieven van de StrafRechtKeten (SRK), zodat de effectiviteit, samenhang en evolueerbaarheid daarvan toeneemt.*

De **toename in samenhang** dient zowel te gebeuren op **operationeel** niveau – dat in het dagelijks werk beter met elkaar wordt samengewerkt en dat die samenwerking goed wordt ondersteund door automatisering – als op **transformationeel** niveau – dat programma's en projecten in hun resultaten slim op elkaar aansluiten en op elkaar voortbouwen. Het gaat hierbij om het **geheel van veranderinitiatieven** – immers, ieder los veranderinitiatief kan naar volle tevredenheid van de opdrachtgever zijn uitgevoerd, terwijl het gerealiseerde geheel toch volstrekt ineffectief en star is. Bij **effectiviteit** beperkt de KDA zich qua ambitie bewust tot de effectiviteit van de StrafRechtKeten (SRK) als geheel; dus niet om de prestaties van de individuele ketenpartijen, maar om de prestaties die alleen **de StrafRechtKeten als geheel** kan leveren, zoals samenhangend optreden naar en informeren van een slachtoffer, of het grip houden op de doorlooptijden van een individuele casus. Verder beperkt de KDA zich bewust tot het **geven van kaders en richting** – het geeft geen *Grand Design* voor de hele strafrechtketen – maar het geeft bewust gekozen inperkingen van ontwerpruimte, zodanig dat, als project en programma's zich bij het ontwerp daaraan houden, de effectiviteit, samenhang en evolueerbaarheid van het geheel voldoende is geborgd, zonder dat ieder project zich daarover zorgen hoeft te maken.

De Strafrechtketendoelarchitectuur richt zich dus op de keten. Daarmee is deze anders dan de architectuur voor een organisatie. Aspecten als eigen verantwoordelijkheid van de deelnemende partijen, in de strafrechtketen extra onderstreept door rechtsstatelijkheid, en uitwisseling met andere ketens of netwerken leggen een sterk accent op uitwisselbaarheid (interoperabiliteit) en de afspraken daarover. En die eigen verantwoordelijkheid is een extra motief om als KDA ons niet te bemoeien met de inrichting van de informatiehuishouding van de individuele ketenpartners – naast het feit dat iedere ketenpartner zijn eigen tempo van ontwikkeling daarvan zoveel mogelijk zelf moet kunnen blijven bepalen.

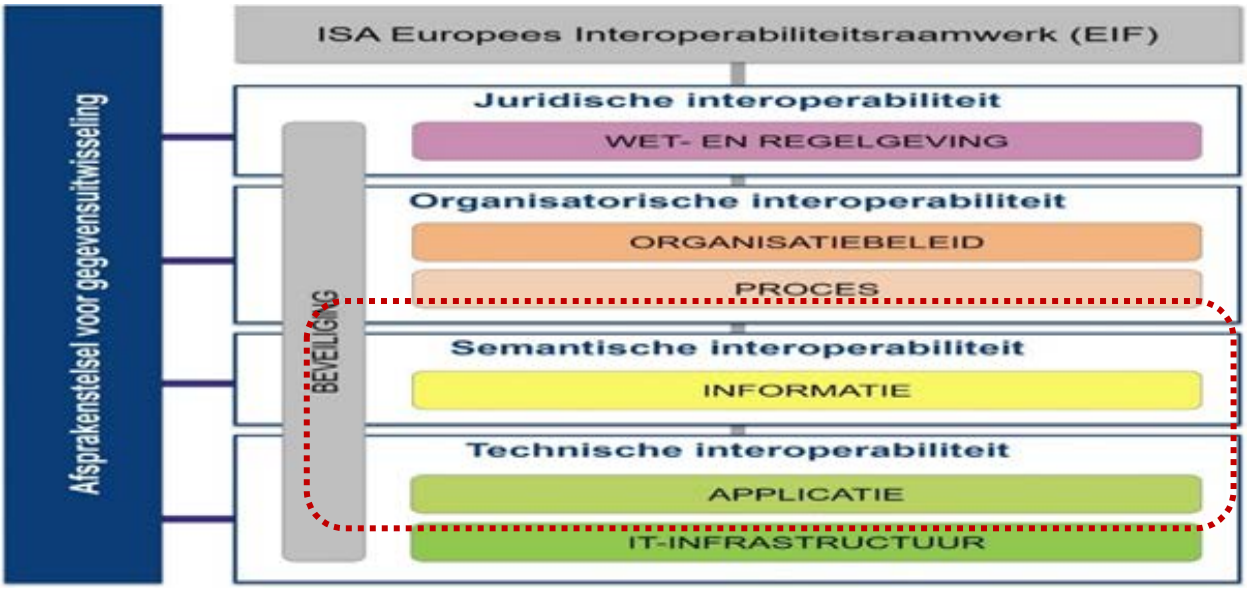
Als we het over de Strafrechtketen hebben, dan is daarbij ook het netwerkperspectief inbegrepen, met nadruk op wederzijdse afhankelijkheden. Over ketens en netwerken merkt W. Borst [VIK] op: "Het strafrechtproces kent een juridische sequentie en is daarmee een keten, ook al wordt er in netwerken samengewerkt. Een keten is een netwerk, maar een netwerk is niet altijd een keten." De "keten" werkt in de praktijk ook niet altijd volgordelijk: executieverantwoordelijken zoals de Kinderbescherming dragen bij aan het begin van de keten, en de politie kan worden ingezet voor lijfsdwang aan het eind van de keten.

De samenwerking waaraan de Strafrechtketendoelarchitectuur wil bijdragen wordt aangeduid als "interoperabiliteit" in het ISA Europees interoperabiliteitsraamwerk[1]. Deze mikt op

> *…het verbeteren van openbare diensten door middel van eind-tot-eindintegratie en -automatisering, het beter benutten van betrouwbare informatiebronnen en het openbaar maken van publieke gegevens, waarbij men ervoor zorgt dat de omgang met documenten van burgers en ondernemingen verloopt overeenkomstig de regelgeving voor gegevensbescherming, ten einde het vertrouwen te vergroten. (…) Daartoe is een gecoördineerde aanpak nodig, op alle niveaus, bij het voorbereiden van wetgeving, wanneer overheidsdiensten hun bedrijfsprocessen organiseren, bij het beheren van informatie en bij de ontwikkeling van IT-systemen voor de tenuitvoerlegging van openbare diensten."*

De Strafketendoelarchitectuur is, geplot op ISA Europees interoperabiliteitsraamwerk (Figuur 2), leidend voor de lagen *informatie* en *applicatie* uit het raamwerk. Daarnaast is er een sterke samenhang met de andere gebieden van het raamwerk, in het bijzonder de eisen die aan de lagen *proces* en *infrastructuur* worden gesteld.

[1] https://ec.europa.eu/isa2/eif_en



Figuur 2 ISA Europees interoperabiliteitsraamwerk

Documentstructuur, samenhang en versies

Deze KetenDoelArchitectuur (KDA) is bedoeld als een zelfstandig leesbaar geheel. Tegelijk is het een samenvatting en een momentopname van veel onderliggende documenten, die ieder op zich in beweging zijn, zoals contextkaders, principes, architectuurbouwstenen en richtlijnen. In de lopende tekst wordt dan ook regelmatig verwezen naar die onderliggende documenten. Als er wijzigingen in die documenten zijn, dan worden die eerst in de onderliggende documenten doorgevoerd en bestuurlijk geaccordeerd. Deze goedgekeurde wijzigingen worden vervolgens in de eerstvolgende versie van de KDA ingepast. Waar de onderliggende documenten en de KDA niet synchroon lopen, zijn de goedgekeurde onderliggende documenten bepalend.

Leeswijzer

De KDA vertrekt in deel 1 vanuit de grotere **context van de strafrechtketen**. Wat is de visie van de Strafrechtketen en welke pijnpunten ervaren de ketenpartners? Welke kaders zijn nu al van kracht om deze visie gestalte te geven, zoals rechtsstatelijkheid, de leidende principes van het OGB, en de inbedding in bredere architecturen? En wat de veranderingen betreft, in welk landschap en welke dynamiek bevinden we ons – welke wetgeving komt eraan, welke programma's (gaan binnenkort) spelen op ketenniveau en binnen de ketenpartners, en welke invloed heeft het verscherpt toezicht door de Tweede Kamer, Bureau ICT Toetsing en CIO-oordelen?

In deel 2 lopen we de stijl en **de essenties van de ketendoelarchitectuur** door. Hoe hangen de ketendoelstellingen eigenlijk samen, en welke partijen zijn betrokken bij het behalen daarvan? Met enkele grondplaten schetsen we grote lijnen van waar het in de strafrechtketen om gaat. Hieruit leiden we systematisch af welke vormen van samenwerken in de keten nodig zijn, en welke architectuurprincipes ons helpen om die koers te gaan zetten. Inzetten op ontkoppeling tussen ketenpartners, het toepassen van dienstoriëntatie, het kunnen beschikken over enkele gemeenschappelijke voorzieningen, de systematische toepassing van interactiepatronen – dit alles binnen privacy en security *by design* - blijken vitaal te zijn voor interoperabiliteit en het "mantra": (…) het van begin tot eind kunnen volgen van personen, zaken, beslissingen en bewijsmiddelen. We sluiten af met een groeipad: hoe dit stapsgewijs, met *just enough, just in time architecture* voor de programma's en projecten, in beweging te krijgen?

En natuurlijk is de KDA een levend document; we sluiten af met een lijst van openstaande punten.

Verwijzingen naar bronnen zijn herkenbaar aan [XXX]. De lijst met bronnen staat in "Bijlage 2: Referenties".

Van alle sterk gecomprimeerde figuren in dit document zijn voor de leesbaarheid in de bijlagen afbeeldingen op A3 formaat opgenomen

Toekomstige delen van de ketendoelarchitectuur

Deel 3 **verdiept** de essenties van de KDA. Wat doen de benoemde ketenvoorzieningen eigenlijk? Wat moet er eigenlijk voorgeschreven worden aan interactiepatronen, en wat zijn daarvan de consequenties? Welke gelaagdheden in de informatievoorziening onderkennen we, en hoe belangrijk zijn de daarin aangegeven

ontkoppelingen? Zo gaat het bij ketenvoorzieningen altijd om een afsprakenstelsel (met bijbehorend beheer en financiering; nog uit te werken in voorschriften, standaarden en richtlijnen), een aantal keren aangevuld met gemeenschappelijke “dingen” (b.v. data, applicaties, en infrastructuur).

Deel 4 behandelt het **werken met architectuur**. Welke ordening zit er in de architectuurproducten zelf, en hoe wordt bestuurd dat de juiste architectuurproducten er komen, van kracht worden en worden gepubliceerd? Daarnaast gaat het in op de wijze van samenwerken van architecten van de ketenpartners, de Strafrechtketen-architectuurraad (SRK-AR), in relatie tot de besturing van programma’s en projecten. Tenslotte gaan we in op het begeleiden van programma’s en projecten, het toezien en het toetsen van resultaten.

Deel 5 behandelt de **transitie**. Hoe te komen tot een keteninformatiehuishouding in lijn met de doelarchitectuur? Wat is de strategie? Wat eerst, wat later? Welke hulpconstructies zijn nodig?

.

Deel 1: De strafrechtketen

In deel 1 beschrijven wij eerst de strafrechtketen en de ambities en uitdagingen waar deze keten mee te maken heeft. Vervolgens gaan we in op het strafrecht: de wetgeving, de betrokken organisaties en de grondvorm van het strafrechtproces en de daarvoor benodigde functies in de keten. Ook staan we stil bij grote ontwikkelingen voor de keten.

Vervolgens benoemen we de kaders die richtinggevend zijn voor de architectuur: rechtsstatelijkheid, de leidende principes digitalisering Strafrechtketen en het bijzondere van keteninformatisering. Dit komt samen in de architectuurprincipes, die het vertrekpunt zijn voor de architectuur in deel 2.

De strafrechtketen

De hoofdtaak van het strafrecht is om een eerlijke en tijdige reactie te geven op strafbare feiten c.q. crimineel gedrag, De keten loopt van incident tot en met de interventie (de uitvoering van de straf of maatregel). Vrijspraak kan ook een uitkomst zijn.

De keten bestaat op hoofdlijnen uit de stappen opsporing, vervolging, berechting en ten uitvoerlegging. Deze stappen kennen een sequentiële volgorde, maar niet op iedere stap volgt noodzakelijk de volgende. De hele keten is nodig om het product “bestraffing van een wetsovertreding” [VIK] te leveren. De bij de strafrechtketen betrokken organisaties zijn op uitvoerend niveau van elkaar afhankelijk, echter bestuurlijk autonoom met verschillende verantwoordelijkheden welke zijn vastgelegd in het Wetboek van Strafvordering.

Bovenstaande typering van de keten is de grondvorm van de keten. Bij nadere beschouwing vinden er veel meer interacties en informatie-uitwisseling of -overdrachten plaats dan de strikte sequentiële volgorde. Ook zijn er veel meer organisaties betrokken dan Politie, Openbaar Ministerie, de Rechtspraak, CJIB, DJI en Reclassering. Een uitwerking vindt u in het volgende hoofdstuk “Het strafrecht”.

Het mogelijk maken van veilig en betrouwbaar informatie delen of overdragen met behoud van en respect voor de straatrechtelijke en wettelijke verantwoordelijkheden, is de basis voor de ketendoelarchitectuur.

Visie op de Strafrechtketen

Op basis van diverse vastgestelde strategie- en beleidsdocumenten zoals het rapport *Toekomst van de strafrechtspleging* van de commissie van der Emster [TSRP], de Strategische agenda *Samenwerken aan Recht en Veiligheid* van J&V [SRV] en beleidsstukken die zijn gedeeld met de Tweede Kamer is een visie geformuleerd waarin de strafrechtdoelen [CMSV] zijn geïdentificeerd en geplaatst in gelaagd perspectief van de maatschappelijke ambities.

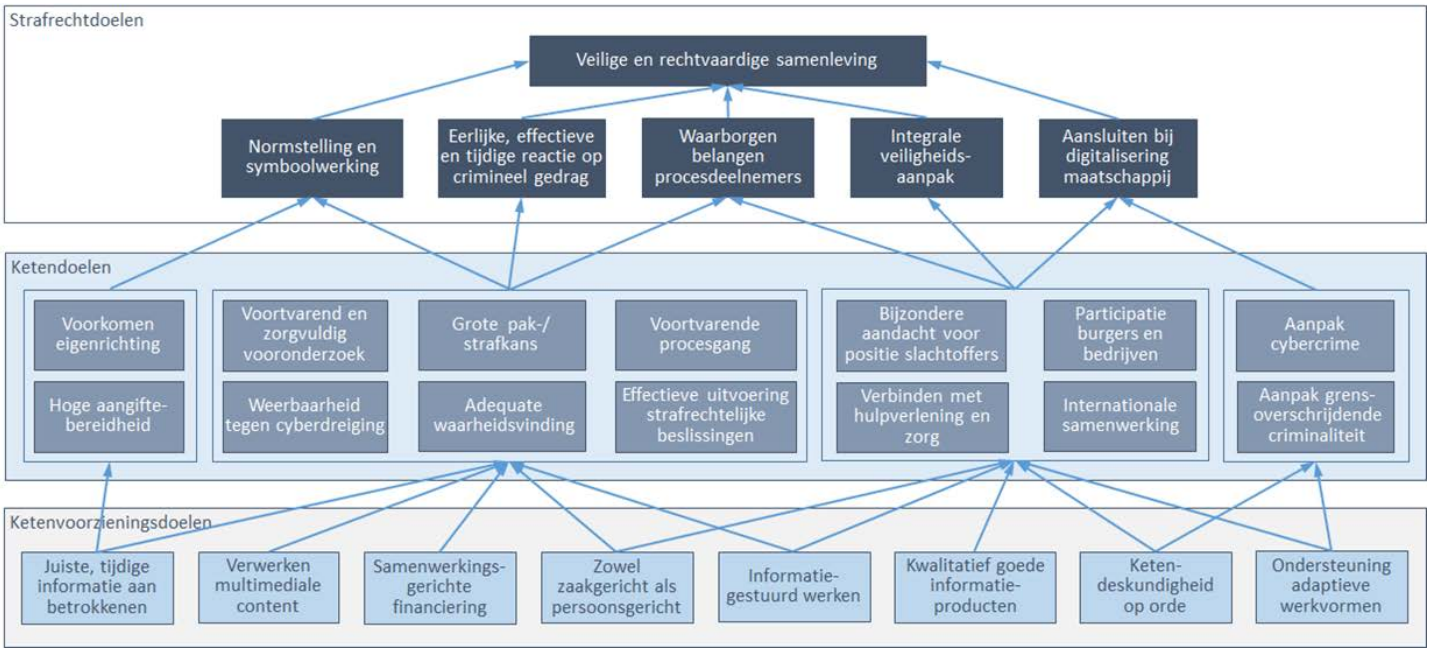
De **strafrechtdoelen** zijn de strategische doelen van het strafrecht. Deze gaan verder dan alleen de strafrechtelijke reactie op crimineel gedrag. Het strafproces maakt deel uit van een breder palet van interventies die tezamen bijdragen aan het realiseren van een veilige en rechtvaardige samenleving. De strafrechtdoelen betreffen daarom ook preventie en hulpverlening die er op gericht is om recidive te voorkomen en de instroom in het strafrecht terug te dringen [CMSV].

De **ketendoelen** beschrijven wat we gezamenlijk in de keten nastreven, zodat we optimaal kunnen bijdragen aan de strafrechtdoelen. De hoofdthema’s die hierin zijn te herkennen zijn ambities op normstelling, strafprocesverbetering, uitbreiding van samenwerking en prioritaire thema’s die met nadruk de aandacht vragen. Hieraan kan iedere ketenpartner vanuit zijn eigen verantwoordelijkheid en expertise een bijdrage leveren, ongeacht de ingerichte structuren en organisaties.

Ketenvoorzieningsdoelen zijn doelen voor de inrichting en werking van de technische en organisatorische voorzieningen die de strafrechtketen ondersteunen in het realiseren van de ketendoelen.

De doelen geven in hun samenhang de legitimatie voor de keuzes tot verandering in de keten, zodat deze optimaal kunnen bijdragen aan het realiseren van de doelen. Ze geven daarmee richting aan de ketendoelarchitectuur.

De strafrechtdoelen, ketendoelen en ketenvoorzieningsdoelen zijn hieronder schematisch weergegeven.



Figuur 3 Voor verdere uitwerking en toelichting: zie Astra Online [Doelenboom Strafrechtketen]

Pijnpunten

Naast ambities zijn er de nodige knelpunten in de huidige informatievoorziening. Knelpunten die medeoorzaak zijn van lange doorlooptijden, fouten en inefficiënties. Knelpunten die zowel de kwaliteit als de productiviteit van de strafrechtketen negatief beïnvloeden.

De Rekenkamer constateerde in 2012: “Er lopen veel stromen tussen de verschillende ketenpartners en veel zaken doorlopen niet de gehele strafrechtketen maar verlaten deze vroegtijdig. De uitstroom van een deel van de zaken is niet in lijn met wet- en regelgeving of anderszins ongewenst. In absolute aantallen is in de opsporingsfase bij veelvoorkomende criminaliteit de ongewenste uitstroom het grootst. Dat daarnaast ook zaken tussen wal en schip vallen, is niet uit te sluiten aangezien veel organisaties zich niet sluitend (in kwantitatieve zin) kunnen verantwoorden over hun zaakafhandeling: instroom-, uitstroom- en voorraadgegevens sluiten niet op elkaar aan of zijn onbekend.” [RAK]. Met het programma Verbeteren Prestaties Strafrechtketen zijn verbeteringen gerealiseerd. Traceerbaarheid van zaken en doorlooptijden zijn nog steeds punten van aandacht.

Van der Emster et al [TRSP] hebben strategische en tactische knelpunten benoemd, zoals:

- de pakkans en het ophelderingspercentage voor overtredingen en misdrijven is laag. De intensiteit van de strafrechtelijke handhaving is voor verbetering vatbaar. Ook de kwaliteit van teveel dossiers en processenverbaal schiet tekort;
- opgelegde straffen en andere strafrechtelijke beslissingen worden niet altijd tijdig of zelfs helemaal niet uitgevoerd;
- door te veel schakels en afhankelijkheden, en een tekort aan samenhang kunnen bedrijfsprocessen kwetsbaar worden;
- reorganisatieprocessen zorgen voor extra werkdruk en verminderde focus op het primaire proces;
- op de werking van de strafketen wordt tegelijkertijd vanuit verschillende en deels tegenstrijdige invalshoeken gestuurd, wat leidt tot verkokering;
- er is weinig onderling begrip van en voor elkaars werk, onder politieagenten, officieren van justitie en rechters;
- het aantal partijen dat betrokken is bij de strafrechtelijke handhaving is toegenomen, wat de afstemming en samenwerking bemoeilijkt.

Ook op operationeel zijn er de nodige pijnpunten. Zonder uitputtend te willen en kunnen zijn:

- Er zijn 50.000 wezen in de SKDB. Dat willen zeggen personen die zijn geïdentificeerd waarbij het niet duidelijk is waarom zij in de SKDB opgenomen zijn omdat de relatie met de reden van opname onbekend is [JMA];
- Er zijn meer dan een miljoen in beslag genomen voorwerpen waarvan de status niet duidelijk is [PBG];
- Jaarlijks zijn er tussen de 100 en 150 onherroepelijke op verkeerde naam gestelde vonnissen [KEB];
- Jaarlijks zijn er ongeveer 1.000 Complexe Dossiers, met een omvang van meer dan 35.000 pagina's. Het ordenen en kopiëren hiervan is een forse administratieve last [CDPO].
- Er is een onbekend aantal onterecht niet verwijderde gegevens (GPS, Compas, JDS, etc.), waardoor niet voldaan niet voldaan wordt aan wet- en regelgeving (AVG, WPG, WJSG, Archiefwet, etc.) [VDA].
- Gegevens van het slachtoffer zijn onvoldoende afgeschermd [PVS].
- Feedbackloops ten behoeve van leren en verbeteren zijn beperkt ingericht.

In het rapport “Knelpunten en breukvlakken” [KEB] is een verdere opsomming van pijnpunten te lezen. Evenzo in de groslijst van pijnpunten in de huidige informatievoorziening zoals opgesteld door het netwerk Datakwaliteit [NDK]. Sommige knelpunten hebben een juridische oorzaak. Breukvlakken in de informatievoorziening tussen ketenpartners veroorzaken ook een groot deel van de pijnpunten. Dit vraagt dat de ketenarchitectuur bijdraagt aan ononderbroken informatiestromen, uiteraard mits daar grondslag voor is.

Informatiehuishouding in beweging

De informatiehuishouding van de keten, als ook bij de afzonderlijke organisaties, is in beweging. Programmatisch wordt de komende jaren gewerkt aan onder andere een papierarme keten (digital born), het ontvangen, verwerken en gebruiken van multimedia-bestanden, digitale dienstverlening aan slachtoffers, advocatuur en verkeersovertreders, het verminderen van handmatig werk en het vergroten van het aanpassingsvermogen van de keten [WDSK, PVTS]. Het huidige IV-Landschap bij de partners is (groten)deels verouderd, intern gericht en beperkt ontworpen voor samenwerking [TKOI]. Meerdere organisaties, o.a. Politie, OM en DJI zijn, delen van, hun IV-landschap en daarmee hun werkwijze aan het vernieuwen om zowel zaak als persoonsgericht te kunnen werken. De partners in en van de keten verschillen, naast (beleids-)prioriteiten, in omvang, capaciteit en tempo bij het doorvoeren van veranderingen en vernieuwingen.

Dit vraagt een architectuur die richting geeft voor de projecten en programma’s, zonder in een groot ontwerp vooraf te vervallen en die tegelijkertijd ruimte laat aan de ketenpartners om in verschillend tempo mee kunnen bewegen en groeien.

Programma’s en projecten staan na de parlementaire enquête [PECE] onder verscherpt toezicht. Extern door de Tweede Kamer en het Bureau ICT-Toetsing. Intern door CIO-oordelen. Dit is geen reden voor een defensieve opstelling. Het is een uitnodiging om kleine haalbare stappen te zetten: kort cyclisch met een snelle feedback loop zodat tijdig bijgestuurd kan worden. Het vraagt daarnaast keuzes te inzichtelijk te maken, deze te onderbouwen, en daarover verantwoording af te leggen.

Duurzaam digitaal stelsel

De Strafrechtketen kent, in tegenstelling tot andere ketens zoals de keten voor Werk en Inkomen, de Onderwijs-keten, het Digitaal Stelsel Omgevingswet en de ketens in de Zorg weinig of geen structurele voorzieningen om de informatiehuishouding van de keten structureel te borgen en verder te brengen. Het programma PDSK heeft als doelstelling om te komen tot een Duurzaam digitaal stelsel waardoor de samenwerking in de keten niet langer afhankelijk is van een programma en eenmalige gelden, maar structureel georganiseerd, bemenst en bekostigd. [WDS] De ketendoelarchitectuur en de Strafrechtketen Architectuurraad (SRK-AR) dienen bij te dragen aan de concretisering van dat duurzaam digitaal stelsel.

Uit het besluit “Duurzaam samenwerken in de strafrechtketen” [DSS] blijkt de sterke intentie en noodzaak tot samenwerking. De ondertekenaars zeggen toe dat de ketenorganisaties op landelijk niveau in gezamenlijkheid voorwaardenscheppende maatregelen treffen die effectieve en efficiënte samenwerking in de operationele keten mogelijk maken. De KDA dient daar voor de informatiehuishouding richting aan te geven.

Het strafrecht

De wet is basis

De Strafrechtketen is streng juridisch gereguleerd. Het wetboek van Strafvordering (WvSv) beschrijft de taken, verantwoordelijkheden en bevoegdheden van de verschillende organisaties en functionarissen. Dit is de grondslag voor het handelen en de processen en daarmee voor de ketendoelarchitectuur.

De Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wahv) is geen strafrecht. Vanwege het feit dat beroep op een opgelegde boete in het kader van Wahv bij het Openbaar Ministerie moet worden ingesteld, neemt de doelarchitectuur ook de Wahv in beschouwing.

Naast het WvSv en de Wahv zijn het wetboek van Strafrecht (WvSr), de Politiewet (Pw), de penitentiaire beginselenwetten, de wet politiegegevens (WPG) en de Wet Juridische en Strafvorderlijke gegevens (WJSG) basis voor de ketendoelarchitectuur.

Om te redeneren over het strafrechtproces en informatisering in de ketendoelarchitectuur is het boek “Verdachte in de ketens” [VIK] ons vertrekpunt.

Ketenpartijen

Bij het uitvoeren van het Strafrecht, van incident tot en met interventie zijn veel partijen betrokken. Een ketenpartij is een organisatie die de KDA op zichzelf van toepassing verklaart en via de besluitvormingslijnen van Opdrachtgevend Beraad (OGB), Coördinerend Beraad Executie (CBE), Bestuurlijk Ketenberaad (BKB) of Bestuurlijk Ketenberaad Plus (BKB+) deelneemt in de besluitvorming.

Ketenpartij / partij bij de keten (in alfabetische volgorde)
Bijzondere opsporingsdiensten [2](BOD'en): 1. FIOD (Fiscale Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Financiën; 2. ISZW-DO (Inspectie Sociale Zaken en Werkgelegenheid, Directie Opsporing), valt onder het ministerie van Sociale Zaken en Werkgelegenheid; 3. NVWA-IOD (Nederlandse Voedsel- en Warenautoriteit, Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Economische Zaken; 4. ILT-IOD (Inspectie Leefomgeving en Transport, Inlichtingen- en Opsporingsdienst), valt onder het ministerie van Infrastructuur en Milieu.
Centraal Justitieel Incassobureau (CJIB)
Centrum voor Criminaliteitspreventie en Veiligheid (CVV)
Dienst Justitiële Inrichting (DJI)
Directie Strafrechtketen (DSK)
Forensische Zorg Instellingen, Koepelorganisatie GGZ Nederland
Gecertificeerde instellingen (G.I.), Koepelorganisatie Jeugdzorg Nederland (JZN)
Halt
De Hoge Raad
Justitiële Informatiedienst (Justid)
Justitiële Uitvoeringsdienst Toetsing, Integriteit, Screening (Justis)
Koninklijke Marechaussee (KMAR)
Leger des Heils
Ministerie van Justitie en Veiligheid
Nederlands Forensisch Instituut (NFI)

[2] BOA in dienst van natuurbeschermingsorganisaties, vervoersbedrijven, etc. laten we buiten beschouwing.

Ketenpartij / partij bij de keten (in alfabetische volgorde)
Nederlandse Gemeenten, Koepelorganisatie Vereniging van Nederlandse Gemeenten (VNG)
Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP)
Openbaar Ministerie (OM)
Perspectief Herstelbemiddeling
Politie
Raad voor de Kinderbescherming (RvdK)
Raad voor Rechtsbijstand (RvR)
De Rechtspraak: Rechtbanken en Hoven
Reclassering Nederland
Regioburgemeester(s)
Schadefonds Geweldsmisdrijven
Slachtofferhulp Nederland
Stichting Verslavingsreclassering GGZ (SVG)
Strafrechtadvocaten, Koepelorganisatie Nederlandse Orde van advocaten (NOvA)

Merk op dat bijna alle bovenstaande organisaties niet alleen betrokken zijn bij de strafrechtketen, zij hebben ook verantwoordelijkheden in het civiele, migratie, sociale of zorgdomein. Dit vereist dat de ketendoelarchitectuur niet in isolement kan bestaan en bruggen moet kunnen slaan naar andere domeinen.

Basisproces

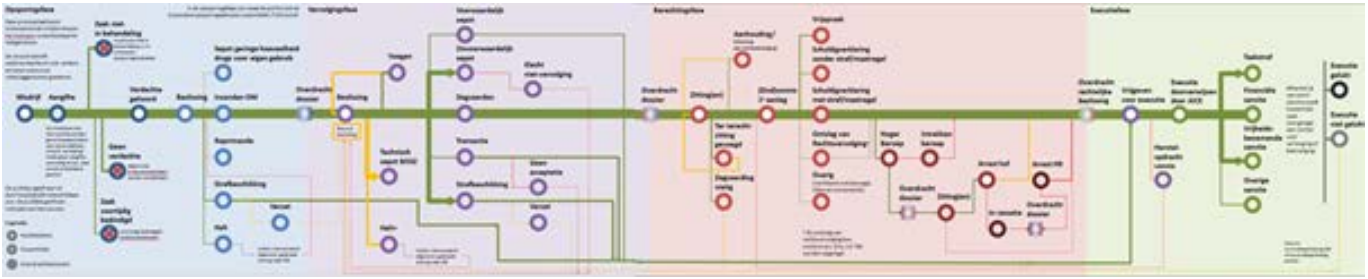
Om over samenhang en samenwerking in de strafrechtketen te kunnen communiceren zijn twee diagrammen[3] behulpzaam. Ze bezien de Strafrechtketen op hoofdlijnen, vanuit verschillend perspectief.

De eerste figuur, de Metroplaat Strafrechtketen, toont het doorlooppad dat karakteristiek is voor het grootste deel van de strafrechtzaken: opsporing, vervolging, berechting en ten uitvoerlegging. Het model wordt o.a. gebruikt bij het zichtbaar maken van doorlooptijden in de keten in de Strafrechtketenmonitor.

De plaat wekt de suggestie van een vaste sequentie. In de praktijk verloopt de behandeling van een strafzaak niet altijd lineair. Behandelingen “springen heen en weer” (bijvoorbeeld omdat iemand zich onttrekt aan de opgelegde straf) of hebben “onverwachte” entrees (bijvoorbeeld het overnemen van een gedetineerde uit het buitenland).

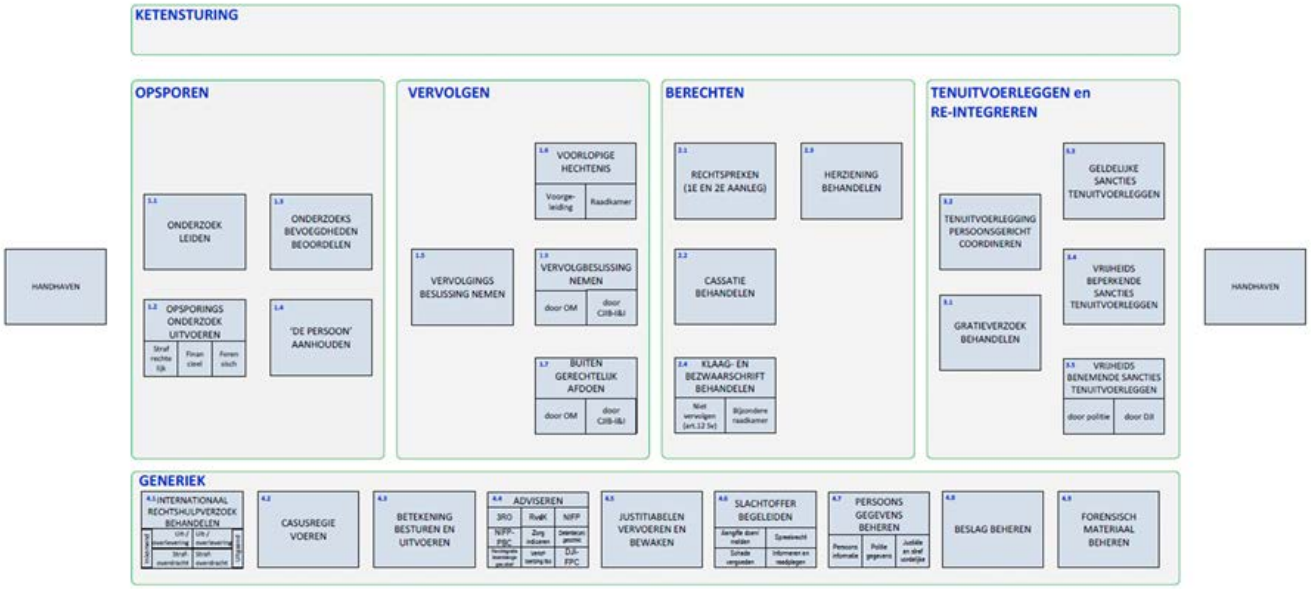
Ook zijn de ketenpartners in meerdere fasen betrokken. Zo doet de politie niet alleen opsporing, ze heeft ook een rol in het innen van boetes of als veroordeelden zich niet melden voor detentie. Het OM heeft een grote rol in vervolging, zij is ook actief bij de tenuitvoerlegging als het gaat over voorwaarden, gratie en verlof.

[3] In de bijlage zijn de diagrammen in A3 formaat opgenomen. N.b.: de diagrammen zijn bedoeld als praatplaat, niet als ontwerpdiagram.



Figuur 4 Metroplaat Strafrechtketen (Data Alliantie Strafrechtketen (zomer 2019)

De tweede figuur toont de hoofdfuncties van de Strafrechtketen, met goed herkenbare functies en verantwoordelijkheidsgebieden. Deze plaat is aanvullend op de “metrokaart” en zeer geschikt om de bijdragen van alle ketenpartners te positioneren. Een gedetailleerde beschrijving van de functies is te vinden in de Werk@Wijzer [W@W]. Dit schema zal in een volgende versie completer gemaakt worden zodat het de belangrijkste functies duidt van alle ketenpartners.



Figuur 5 Grondplaat Strafrechtketen (Werk@Wijzer, Architectuur voor de Uitvoeringsketen Strafrechtelijke Beslissingen, v7.00, april 2018)

In de bijlage is een matrix opgenomen met de hoofdfuncties en ketenpartijen, waarmee de uitvoerende verantwoordelijkheden zijn geëxpliciteerd [W@W].

Betrokkenen

Naast de hiervoor genoemde ketenpartijen zijn er meer partijen betrokken bij de strafrechtketen.

Allereerst zijn dat de direct betrokkenen (natuurlijke en rechtspersonen): justitiabelen (verdachte, veroordeelde), benadeelden (slachtoffer, nabestaande) en getuigen.

De strafrechtketen heeft verder nauwe verbindingen met andere ketens zoals de migratieketen, de zorgketen en sociale keten. De sociale keten en gemeenten hebben een belangrijke rol bij preventie en re-integratie, evenzo voor schuldsanering en huisvesting. Veel verdachten hebben al een zorgverleden dat ook na een eventuele veroordeling doorloopt. Overheidsinstanties als het UWV en de Belastingdienst gebruiken strafrechtinformatie (voornamelijk detentiegegevens) voor het wel/niet toekennen/staken van uitkeringen en toeslagen. De Dienst Domeinen heeft een rol bij in beslag genomen goederen.

Het is voor betrokkenen van belang dat ze op een eenvoudige, eenduidige en veilige wijze informatie kunnen delen en uitwisselen met de Strafrechtketen zonder de volledige complexiteit van de keten te moeten doorgronden.

De hoeveelheid betrokken organisaties en de variaties in werkprocessen en samenwerking vraagt een architectuur die standaardiseert op semantiek en techniek en de uitwisseling van informatie vereenvoudigd met behoud van de eisen uit oogpunt van wetgeving, beveiliging en gegevensbescherming.

Ontwikkelingen

Voor het ontwikkelen van de ketendoelarchitectuur is het van belang te weten welke ontwikkelingen en of veranderingen de komende jaren gaan spelen. De architectuur zal deze moeten ondersteunen of in ieder geval niet in de weg mogen staan. In de paragraaf “Informatiehuishouding in beweging” schetste we reeds dat de informatiehuishouding bij meerdere ketenpartijen de komende jaren flink op de schop gaat. Daarnaast zijn er ontwikkelingen op het gebied van wetgeving en de oriëntatie van de strafrechtketen, wat zich vertaalt in aanvullende vormen van samenwerken.

Wetgeving

Er zijn twee grote wetgevingstrajecten onderhanden:

1) Vernieuwing wetboek strafvordering;
2) De vernieuwing van de Wet Politiegegevens (Wpg) en de Wet Justitiële en Strafvorderlijke gegevens (WJSG).

Ad 1) Vernieuwing Wetboek van Strafvordering (WvSv)
Het huidige wetboek van strafvordering is honderd jaar oud. J&V werkt aan een integrale modernisering, die moet leiden tot een geheel nieuw Wetboek, ter vervanging van het huidige. Die modernisering beoogt vooral een stroomlijning en het bij de tijd brengen van het Wetboek. Er vindt een codificatie plaats op basis van staande praktijk. Het wetboek wordt minder techniekafhankelijk. Het huidige wetboek is sterk papier- en tekst-georiënteerd. Na inwerkingtreding van het nieuwe wetboek kan bijvoorbeeld een multimediabestand als bewijsmiddel worden erkend en hoeft daar geen papieren en/of uitgeschreven verbaal van gemaakt te worden. Het wetboek beoogt ook een hernummering van de artikelen. Een fundamentele herziening van de beginselen waarop de strafvordering berust, is niet beoogd.

Ad 2) Vernieuwing Wpg en WJSG
Er bestaan speciale regels voor de verwerking van politiegegevens (gegevens die worden verwerkt in het kader van de uitoefening van de politietaak), justitiële gegevens (alles wat in de justitiële documentatie zit) en strafvorderlijke gegevens (alles wat het OM in huis heeft aan data en dossiers). Deze regels zijn vastgelegd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Deze wetten zijn ingewikkeld geworden en deels op oude Informatiehuishouding gebaseerd. Daarom worden beide wetten in samenhang integraal herzien.
Deze wetten, en dan vooral de Wpg, hebben grote consequenties voor de inrichting van de informatiehuishouding van de betrokken organisaties, met name de politie. De huidige Wpg is geheel geschreven op de destijds (vijftien jaar geleden) bestaande systemen bij de Politie. En wetgeving en systemen beïnvloeden elkaar in hoge mate wederzijds.

Naast deze twee aanpassingen zijn de implementaties van eerdere wetgeving nog niet volledig afgerond. Denk hierbij aan de Wet Forensische Zorg (WFZ), de wet Verplichte GGZ (WVGGZ), de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen (USB) en de Algemene Verordening Gegevensbescherming (AVG).

De aanpassingen in de informatievoorziening ten gevolge van de wetgeving zal bij de betrokken organisaties ongetwijfeld in verschillend tempo plaatsvinden. Dit vraagt een ketenarchitectuur waarin “losjes” gekoppeld waardoor de interne complexiteit voor de keten is afgeschermd.

Nieuwe vormen van samenwerken

Om de bijdrage van het strafrecht aan een veilige en rechtvaardige samenleving te vergroten is het nodig dat een veel groter deel van de incidenten tegen burgers tot een strafrechtelijke afdoening komt, dat recidive wordt teruggedrongen en dat het strafrecht onderdeel vormt van een integrale veiligheidsaanpak [CER]. De inzet daarbij is om meer aan de voorkant van de problematiek te komen. Waar het strafrecht vooral achteraf en repressief ingrijpt is het ook zinvol om de instroom in het strafrecht te beperken door preventief op te treden [TSRP].

Voor deze integrale veiligheidsaanpak is samenwerking met partners buiten de keten nodig. De strafrechtketen positioneert zich dan als één van de spelers die samen met organisaties vanuit bijvoorbeeld zorg, wonen, werk en inkomen zorgt voor een samenstel van interventies. Die moeten er voor zorgen dat de persoon in kwestie niet meer terugkomt in de keten. De ketenpartners in de strafrechtketenorganiseren hun samenwerking in de vorm van diensten. Dit maakt het mogelijk dat de ketenpartners niet alleen lineair en

met elkaar samenwerken maar ook kunnen ook samenwerken in wisselende coalities met nieuwe partners zoals zorginstellingen, onderwijs, burgers en bedrijven. De informatievoorziening moet deze nieuwe vormen van samenwerken kunnen ondersteunen door het vergroten van het aanpassingsvermogen door gestandaardiseerde informatie-uitwisseling en het voorkomen van een ongebreidelde groei aan bilaterale verbindingen.

Kaders voor de architectuur

Het speelveld van de ketendoelarchitectuur wordt begrensd door kaders en richtlijnen. Deze paragraaf geeft een overzicht van de kaders en richtlijnen die op strategisch niveau richting geven aan de ketendoelarchitectuur.

Rechtsstatelijkheid

Binnen de staat zijn de taken verdeeld, maar de staatsorganen vormen gezamenlijk de Nederlandse staat. Het doel van een staat is - naar de woorden van de Nederlandse filosoof Spinoza - het organiseren van vrijheid voor de burgers in de staat. Omdat absolute macht altijd tot misbruik leidt moet binnen de eenheid van de staat, voor iedere overheidsmacht ook een tegenmacht worden georganiseerd. Voor de vrijheid van burgers in een staat is het noodzakelijk dat de trias politica (de wetgevende macht, de uitvoerende macht en de rechtsprekende macht) elkander in balans houden. De wetgever (regering en parlement) maakt de wetten die worden toegepast door de uitvoerende macht (zoals politie en het openbaar ministerie). De rechter controleert die toepassing geeft daarbij een uitleg aan de wet in een concrete zaak. In onze rechtsstaat is geen van deze staatsmachten de baas. Als de wetgever het niet eens is met de uitleg die de rechter aan een wet geeft, dan kan hij de wet aanpassen. Daarna wordt de nieuwe wet weer toegepast door de uitvoerende macht en opnieuw door de rechter uitgelegd bij controle van die toepassing in concrete (straf-)zaken.

Voor een balans tussen de staatsmachten moeten de rechters onafhankelijk zijn van de twee overige staatsmachten. De onafhankelijke positie van de rechter is geen privilege voor de rechter, maar is een noodzakelijke voorwaarde voor de handhaving van de vrijheid van de burgers in de Nederlandse staat. De (institutionele, functionele en persoonlijke) onafhankelijke positie van de rechter stelt hem in staat om in iedere zaak onpartijdig recht te spreken ('zonder aanzien des persoons').[4]

Leidende principes digitalisering strafrechtketen

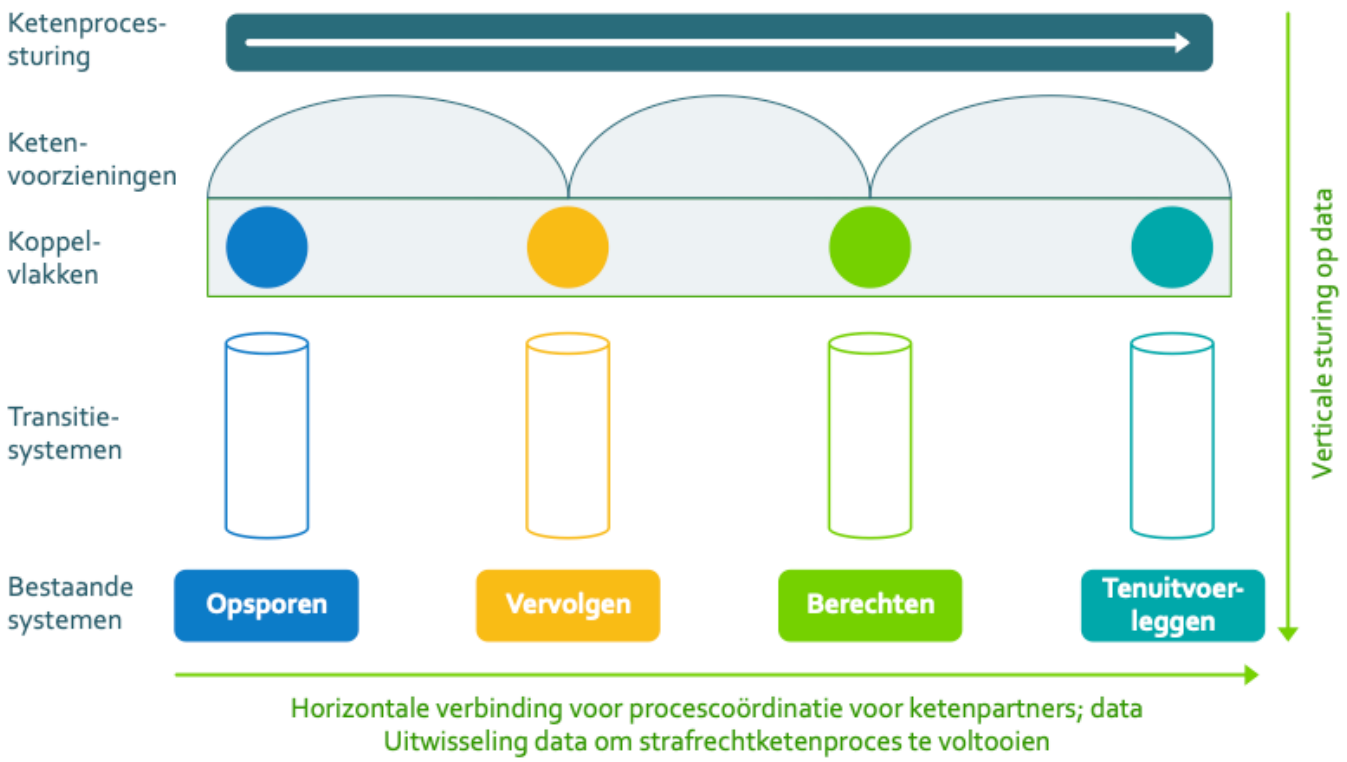
OM richting te geven aan de digitalisering van de strafrechtketen heeft het Opdrachtgevend beraad (OGB) leidende principes opgesteld [LPD], welke in februari 2020 door het Bestuurlijk Keten Beraad (BKB) zijn bekrachtigd. Voor het uitwerken van de ketendoelarchitectuur zijn dit de essenties:

- Rechtsstatelijkheid respecteren en ondersteunen. Wetgeving (o.a WvSv) is de basis voor rollen en verantwoordelijkheden;
- De keten bestaat uit zelfstandige organisaties met heldere verantwoordelijkheden en stuurmogelijkheden. Dat betekent:
  - Organisatie hebben hun eigen informatiehuishouding;
  - Gegevens zijn vastgelegd bij de verantwoordelijke organisatie (In termen van de brug, zie hierna: in de fundament / pijler, niet in de legger).
  - Geen ketenapplicaties voor primair proces.
- De keten loopt van incident tot en met interventie;
- Informatievoorzieningen van ketenpartners worden los gekoppeld om verschillen in tempo of prioriteit mogelijk te maken en de onafhankelijkheid te waarborgen;
- Er is een beperkt aantal gemeenschappelijke of ketenvoorzieningen t.b.v. betrouwbaar overdragen of delen van informatie;
- Bewaken chain of evidence / waarborgen onweerlegbaarheid van informatie (document, film, etc.) dient geborgd te zijn;
- Hanteer het FAIR principe: Findable - vindbaar; Accessible - toegankelijk; Interoperable - uitwisselbaar; Reusable - herbruikbaar ;
- De architectuur dient te voldoen aan eisen m.b.t. security, privacy, ethiek en compliancy.

De "strafrechtketenbrug"

De "strafrechtketenbrug" (hierna "de brug") is een visualisatie van de leidende principes (zie Figuur 6).

[4] Deze alinea's zijn overgenomen uit de bijlage bij de Leidende principes digitalisering Strafrechtketen [LPS]



Figuur 6 De brug, onderdeel leidende principes digitalisering Strafrechtketen

Met deze metafoor wordt uitgedrukt:

- een scherpe demarcatie tussen eigen verantwoordelijkheid en gezamenlijke voorzieningen;
- dat de leggers en bogen staan voor het overdragen en delen van informatie. De transitiesystemen zijn van de ketenpartners en zijn de verbinding tussen de interne systemen (het fundament) en de keten.

Ook hier: het lijkt een sequentieel proces van links naar rechts. Dat is slechts de grondvorm. In de praktijk gaan de interacties en informatie-uitwisseling alle kanten uit.

Digitaliseren in ketens

In het taalgebruik spreekt men makkelijk over ketenprocessen en ketendoelen. In de praktijk is er geen ketenproces, er is wel een keten van processen. Immers de keten is een abstractie en gedachteconstruct. Het is geen entiteit die zelfstandig verantwoordelijkheid kan dragen of actie kan ondernemen. Er zijn wel wederkerige afhankelijkheden tussen de partners in de keten. Geen van allen kan zelfstandig, dat wil zeggen zonder de andere organisaties, haar resultaat behalen. De gezamenlijke inspanning van de ketenpartners bepaalt het resultaat. Voor sommige diensten is gezamenlijk optrekken noodzakelijk.

In de strafrechtketen leggen de rechtsstatelijkheid en de leidende principes digitalisering de nadruk op de verantwoordelijkheid, de handelingsruimte en daarmee de autonomie en onafhankelijkheid van de afzonderlijke partners in de keten. Zulk gezamenlijk optrekken is in de strafrechtketen niet onbeperkt mogelijk.

Voor het redeneren over ketens baseren wij ons op de uitgangspunten van Grijpink over keteninformatisering [KKB]. Deze visie en uitgangspunten staan dicht bij de leidende principes. Grijpink stelt dat in een keten het communiceren (informatie verkrijgen en delen) in plaats van het registreren centraal. Dat betekent dat het alleen gaat om gemeenschappelijke informatie in een “kale” informatie-infrastructuur die de communicatie ondersteunt. Dit in tegenstelling tot gemeenschappelijke primaire procesapplicaties op ketenniveau. Keteninformatisering betreft dus vooral structureren (denk aan semantische afspraken en het beheer ervan) en automatiseren van de communicatie die nodig is om gegevens aan elkaar beschikbaar te stellen.

Een keten kan geen verantwoordelijkheid dragen, die blijft altijd bij de ketenpartners. Als er een gezamenlijke voorziening met verantwoordelijkheid komt dan is daar een grondslag voor nodig en is de verantwoordelijkheid, in de zin van accountability, toe te wijzen aan een entiteit. Daarnaast zijn besturing, financiering en beheer duidelijk afgesproken [KNP]. Dit is in lijn met de leidende principes digitalisering.

Grijpink stelt dat het dominante businessprobleem leidend is voor de keten. Dit moet zo klein mogelijk gemaakt worden. In onze architectuur zullen wij hiervan afwijken omdat er een veelheid is aan businessproblemen, die samen te vatten zijn in ons mantra. Zie daarvoor het hoofdstuk “Mantra”.

Architectuurprincipes strafrechtketen

De architectuurprincipes voor de strafrechtketen (SRK-principes) zijn als ontwerpconsequenties afgeleid van de strategische doelen van de strafrechtketen, het leidende principe van rechtsstatelijkheid en de leidende principes digitalisering strafrechtketen. Ze beschrijven de samenwerkingsafspraken in de strafrechtketen zonder uitspraken te doen over de interne organisatie van de ketenpartners.

Waarom juist deze architectuurprincipes?

De architectuurprincipes voor de strafrechtketen geven op hoofdlijnen aan hoe de samenwerking en de informatievoorziening in de strafrechtketen moeten worden ingericht om de strategische doelen te kunnen bereiken.

In de strategie zijn die doelen nadrukkelijk breder dan alleen strafrechtpleging en omvatten zij ook andere instrumenten die bijdragen aan een eerlijke en rechtvaardige samenleving. Daarbij horen in ieder geval ook de symboolwerking en de normstelling van het strafrecht die tezamen met maatschappelijke partners als onderwijs en zorg bijdragen aan preventie van crimineel gedrag. De strafrechtketen zorgt voor een eerlijke, effectieve en tijdige reactie op crimineel gedrag. Bij nieuwe en grensoverschrijdende vormen van criminaliteit zijn maatschappelijke partners betrokken bij de opsporing. Bij de nazorg zijn ook weer andere partners betrokken om recidive te voorkomen en re-integratie te bevorderen. De strategische doelen beschrijven nieuwe vormen van ***Samenwerken*** en het principe dat daarover gaat beschrijft de consequenties voor de organisatie en de informatievoorziening. Het principe van ***Transparantie*** draagt bij aan zowel de symboolwerking en de normstelling als aan de eerlijke reactie op crimineel gedrag door verantwoording af te leggen aan de maatschappij. Het principe over ***Aanpassingsvermogen*** stelt de ketenpartners in staat om snel in te spelen op nieuwe en grensoverschrijdende vormen van criminaliteit. ***Dienstoriëntatie*** is een principe dat aangeeft hoe ketenpartners effectief kunnen samenwerken met behoud van hun eigen ***Rechtstatelijke*** verantwoordelijkheden. Met het principe van ***Differentiatie waar nodig*** geven we aan hoe de toegankelijkheid van het strafrecht georganiseerd wordt om recht te doen aan de verschillende behoeften van alle verschillende betrokkenen. ***Digitaal is onze taal*** is een principe dat aangeeft dat digitale gegevensverwerking de basis vormt voor de samenwerking in de strafrechtketen omdat daarmee de informatievoorziening en de procesgang het beste georganiseerd kunnen worden. Het principe van ***Gegevenskwaliteit*** geeft daarbij aan welke eisen we stellen aan de kwaliteit van de gegevens en de organisatie van de gegevensverwerking. Het principe ***Zaakgericht én persoonsgericht*** beschrijft hoe informatieverwerking georganiseerd moet worden om de informatie zo optimaal mogelijk voor meerdere strafrechtdoelen te kunnen gebruiken.

Architectuurprincipe	Toelichting
Rechtstatelijkheid (AP0)	De wijze van organiseren en samenwerken in de strafrechtketen geeft invulling aan de rechtsstatelijke scheiding van de verschillende rollen en bevoegdheden in het strafproces (WvSv).
Samenwerken (AP1)	Dit betreft de samenwerking tussen de ketenpartners onderling maar ook de samenwerking in netwerken en wisselende samenwerkingsverbanden met maatschappelijke partijen. Samenwerken betekent dat de keten als 'team' kan acteren. Bij samenwerken wordt uitgegaan van gemeenschappelijke doelen en van het onderlinge begrip van het effect van handelingen voor de keten als geheel. Verder is samenwerken is niet alleen een technisch proces maar vooral ook mensenwerk met relationele en culturele dimensies.
Transparantie (AP2)	Inzage en verantwoording bestaat uit zaakinformatie naar direct betrokkenen, uit prestatie-informatie ten behoeve van sturing en rapportage en uit normstelling naar de maatschappij over het geldende recht. De inhoud, vorm, actualiteit en pro-activiteit van die inzage is afhankelijk van de rol van de betrokkene in het strafrechtketenproces en hun behoefte. Voor de heimelijke onderdelen van het onderzoek is de transparantie beperkt tot verantwoording achteraf en in beperkte kring.
Aanpassingsvermogen (AP3)	Omgevingsveranderingen – zoals wijzigende verwachtingen vanuit de maatschappij, veranderende vormen van criminaliteit en nieuwe technologische

	mogelijkheden – dienen zich van buiten aan. De aanpassing betreft zowel de dienstverlening van de strafrechtketen (b.v. vergelding versus interventie gericht op gedragsverandering) als de inrichting met mensen, middelen en werkwijzen. Voorbeelden hiervan zijn mediation en wisselende samenwerkingsverbanden met instanties in zorg of werk en inkomen. Zo'n slimme aanpassing is gepast, proportioneel, doordacht, mogelijk innovatief en vaak met een korte terugverdientijd.
Dienstoriëntatie (AP4)	Een dienst is een afgebakende prestatie van een persoon of organisatie (de dienstverlener) die voorziet in een behoefte van haar omgeving (de afnemer). Het resultaat van een dienst is bijvoorbeeld een aangehouden verdachte, een vastgestelde identiteit, een rechterlijke uitspraak (bedrijfsprestaties), een risicoprofiel van een persoon of een geleverde VOG of ID-staat (informatieproducten). Over het leveren van diensten worden afspraken gemaakt ten aanzien van prestatie, kwaliteit en coördinatie in een dienstniveau-overeenkomst (DNO), zonder voorschriften voor de interne voortbrenging bij de dienstverlener.
Differentiatie waar nodig (AP5)	Betrokkenen zijn de partners in de strafrechtketen (politiemensen, officieren, rechters en advocaten), de deelnemers in het strafproces (verdachten, slachtoffers en getuigen) maar ook externe samenwerkingspartners (gemeenten, bedrijven en zorginstellingen). Afstemmen op maat gaat over de keuze van het kanaal, de vorm en de formulering van berichten en het communicatiepatroon (bijvoorbeeld op aanvraag, proactief, persoonlijk contact of een via een berichtendienst).
Digitaal is onze taal (AP6)	De strafrechtketen verwerkt zijn gegevens digitaal en maakt gebruik van digitale mogelijkheden om werkprocessen slim te organiseren. 'Digitaal is onze taal' betekent dat: • alle in de keten geproduceerde informatie direct digitaal worden vastgelegd (digital born), en dat • alle van buiten de keten verkregen informatie digitaal wordt ontvangen of terstond naar digitale informatie wordt omgezet, en dat • digitale informatie digitaal wordt gehouden ("eens digitaal, blijft digitaal"), en dat • interacties die digitaal worden gestart ook digitaal worden voortgezet. Voor betrokkenen die daar behoefte aan hebben is daarnaast ook niet-digitale interactie mogelijk. Dit vanwege de noodzakelijk balans met het principe van Differentiatie.
Gegevenskwaliteit (AP7)	De gegevenskwaliteit betreft hier voor individuele gegevens: juistheid (correspondeert met de werkelijkheid), integriteit (niet onderweg veranderd), authenticiteit (vanuit gezaghebbende bron verkregen, met vermelding van die bron), actualiteit (tijdstip van besluit of waarneming) en rechtsgrondslag voor verkrijging. Voor een verzameling van gegevens heeft die kwaliteit ook betrekking op volledigheid (compleetheid). Doordat de kwaliteit van een gegeven bekend is kunnen de waarde en toepasbaarheid van het gegeven voor de uitoefening van een taak worden vastgesteld. Borging zorgt dat erop kan worden vertrouwd dat gegevens voldoen aan de afgesproken kwaliteit.
Zaakgericht én persoonsgericht (AP8)	De organisatie van werkzaamheden en de informatievoorziening maken het mogelijk om informatie volgens verschillende perspectieven te ordenen voor een betekenisvolle aanpak van veiligheidsproblemen (zaakgericht en persoonsgericht, maar ook locatiegericht en fenomeengericht, etc.). Zaakgericht (opsporing, vervolging, berechting op basis van de gepleegde feiten) en persoonsgericht (omstandigheden, geschiedenis) werken moeten beide mogelijk zijn.

De rapporten van de Ombudsman en het boek de Digitale Kooi van de Kafka-Brigade [DDK] zijn aanleiding om een 10e principe te overwegen. Een principe gericht op het vergroten van het vermogen om fouten en hun doorwerking ervan te kunnen herstellen.

Relaties met andere architecturen

De strafrechtketen en zijn ketendoelarchitectuur zijn geen eiland. De ketendoelarchitectuur dient zich te verhouden tot architectuur van de Nederlandse Overheid. Veel werk is al verzet en daarmee een gegeven. Daarbij gaat het met name om de principes van de Nederlandse Overheid Referentiearchitectuur (NORA) en de enterprise architectuur V&J (EA V&J). Deze architectuurprincipes zijn ook van toepassing op de strafrechtketen. De SRK principes moeten worden gezien als een verbijzondering die nodig is waar de strafrechtketen afwijkt van bovenliggende principes.

De EA J&V bevat principes die daar 'afspraken' worden genoemd en die gelden voor alle onderdelen van het ministerie en dus ook voor de J&V-onderdelen die deel uitmaken van de strafrechtketen. Hierbij moet worden aangetekend dat voor de Rechtspraak, het Openbaar Ministerie en de Nationale Politie bijzondere afspraken zijn gemaakt, vanwege de rechtstatelijke scheiding der machten. Deze partijenzijn niet automatisch gebonden aan de EA J&V maar kunnen wel door afstemming en zelfbinding deelnemen. De EA J&V geeft kaders voor zowel over diensten en doelgroepen als voor applicaties en infrastructuur en heeft vooral betrekking op de gemeenschappelijke diensten van J&V en de eigen informatievoorziening van het bestuursdepartement. De SRK-principes hebben vooral betrekking op de samenwerkingsrelaties in het primaire proces van de strafrechtketen en geven aan hoe de strafrechtketen afwijkt van de EA J&V.

De architectuur Uitvoering Strafrechtelijke Beslissingen (USB) is geïntegreerd in de Architectuur Strafrechtketen, waarmee deze KDA ook geldt voor het Executiedomein van de SRK.

Voor verdere uitwerking van de principes en verantwoording daarvan zie www.astraonline.nl en SRK Leidende principes Monthly Build 201912.

Openstaand in deze versie: de relatie met Europese initiatieven en kaders

Gegevensbescherming

De Strafrechtketen verwerkt veel persoonsgegevens. Ongeacht de grondslag moet in alle gevallen gewogen worden naar proportionaliteit, subsidiariteit, dataminimalisatie, informatiebeveiliging, etc.

Binnen de keten is dit grotendeels geregeld in specifieke wetten, de WPG en de WJSG. Deze gaan boven de meer algemene verordening van de AVG. Daarmee is voor een groot deel de grondslag voor het uitwisselen van informatie binnen de keten aanwezig.

Voor uitwisseling van informatie met partijen buiten de keten zijn Wpg en WJSG niet toereikend, en is de AVG of andere specifieke wetgeving van toepassing.

Privacy in de keten vraagt extra aandacht om toe te zien dat de verstrekte gegevens niet ongewenst of onrechtmatig gebruikt worden. Knellende voorbeelden daarvan zijn de schending van de privacy van het slachtoffer [PVS] en het openbaar worden van persoonsgegevens van anonieme getuigen.

De Strafrechtketen opereert waar mogelijk in lijn met de J&V strategie en aanpak [KIBV]. Afwijkingen dienen gemotiveerd en vastgesteld te worden.

Informatiebeveiliging

De vele gevoelige informatie vraagt vanuit oogpunt van gegevensbescherming een goede informatiebeveiliging uitgedrukt in Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Ook vanuit informatie gelijkheid, "equality of arms", is het van belang dat partijen gelijke toegang hebben tot dezelfde informatie. Tenslotte is de informatie in de keten voor criminele organisaties en personen interessant. Dit vraagt extra aandacht voor de beveiliging van gegevens.

De Strafrechtketen opereert waar mogelijk in lijn met de J&V strategie en aanpak [KIBV]. Afwijkingen dienen gemotiveerd en vastgesteld te worden.

Deel 2: Essenties van de ketendoelarchitectuur

In dit deel beschrijven we de essenties van de ketendoelarchitectuur. We beginnen met de mantra van de SRK-AR dat de noodzaak van gegevens- en informatielogistiek onderstreept. Vervolgens vertalen de brug-metafoor in architectuur consequenties, om daarna de kernelementen van de architectuur uit te werken. Tenslotte staan we stil bij gegevensbescherming en informatiebeveiliging.

Mantra

Uit *"Deel 1: De strafrechtketen"* blijkt, kort samengevat, dat:

- rechtsstatelijkheid en eigen verantwoordelijkheid van organisaties uitgangspunt zijn voor de architectuur;
- belanghebbenden zoals slachtoffers betere informatiediensten krijgen;
- tegelijkertijd er veel (nieuwe) samenwerking ontstaat en soepelere (informatie-)logistiek nodig is;
- de strafrechtketen steeds meer digitaal gaat communiceren, zowel binnen als buiten de keten;
- de strafrechtketen meer gaat sturen op prestaties;
- de huidige informatievoorziening een aantal pijnpunten kent;
- het Ketenlandschap een grote verwevenheid kent, zowel op procesniveau als op informatievoorzieningsniveau;
- iedere organisatie in zijn eigen tempo en binnen de eigen mogelijkheden dient mee te kunnen bewegen in de keten.

Dit is lijn met de in 2016 aan de kamer aangeboden visie op de informatievoorziening Strafrechtketen [VIS]. De KDA bouwt daarop voort.

Om hier een antwoord op te geven heeft de SRK-AR de ambitie van de ketendoelarchitectuur verwoord in het mantra [JAR].

In 2024 kunnen wij in de strafrechtketen digitaal, betrouwbaar en eenvoudig personen, zaken, beslissingen en bewijsmiddelen van begin tot eind van de keten volgen zodat de informatie tijdig en volledig beschikbaar is voor wie dat nodig heeft en mag hebben, binnen en buiten de keten, ten behoeve van informeren, handelen, beslissen, leren, besturen en verantwoorden.

Het mantra geeft richting aan de architectuurkeuzes die in de ketendoelarchitectuur gemaakt zijn. In onderstaande tabel is per onderdeel van het mantra aangegeven tot welke keuzes dat heeft geleid.

In 2024 …	**Tijdshorizon** Het doel ligt niet heel ver weg in de tijd. Dat voorkomt overspannen verwachtingen en geeft focus aan wat er moet gebeuren. Het biedt echter wel een perspectief dat verder reikt dan het oplossen van de huidige problemen in de keten. In de transitiearchitectuur schetsen we hoe in beheerste stappen de huidige belemmeringen in de keten worden weggenomen en hoe de ambitie die uit het mantra spreekt, wordt waargemaakt. *[zie Deel 5: Transitiearchitectuur]*
… kunnen wij in de strafrechtketen …	**Samenwerkende (keten)partijen** De Strafrechtketen bestaat in enge zin uit de organisaties die een rol spelen bij Opsporen, Vervolgen, Berechten en Tenuitvoerleggen. Deze organisaties werken onderling nauw samen. In bredere zin werken de ketenpartners samen met partijen in andere ketens, zoals Migratie, Zorg en Werk en Inkomen. *[zie Ketenpartijen en In* de bijlage is een matrix opgenomen met de hoofdfuncties en ketenpartijen, waarmee de uitvoerende verantwoordelijkheden zijn geëxpliciteerd [W@W]. Betrokkenen*]*
… digitaal, betrouwbaar en eenvoudig …	**Kwaliteit van de samenwerking** Communicatie tussen partijen, verwerking en uitwisseling van informatie vindt binnen de strafrechtketen en met partijen in andere ketens digitaal plaats. Betrouwbare, integere en veilige uitwisseling van informatie is daarbij van cruciaal belang. Dat stelt hoge eisen aan de middelen waarlangs die informatie tussen partijen wordt uitgewisseld (informatielogistiek). Ook moet de informatie die uitgewisseld worden eenvoudig te vinden,

	te gebruiken en te corrigeren zijn (conform de FAIR-principes). Om daaraan te voldoen is nodig dat er voorzieningen op ketenniveau beschikbaar zijn, die voorzien in: - Het vinden en gebruiken van informatie (Portalen en Distributie); - Het geven van betekenis aan de informatie (Semantiek); - Het kunnen relateren van informatie in verschillende domeinen bij verschillende partijen (Nummerstelsels); - Het lokaliseren van de bron waarin de informatie te vinden is (Verwijsindexen); - Het assembleren en leveren van de informatie (Informatiemakelaar); - Het kunnen corrigeren van fouten in informatie en de gevolgen daarvan (Terugmelden); - Het verantwoording kunnen afleggen over verstrekte informatie (Compliance); - Het kunnen achterhalen van afspraken en de voortgang daarvan (Status). *[zie Interactiepatronen en Ketencommunicatievoorzieningen]*
… personen, zaken, beslissingen en bewijsmiddelen …	**Ketenrelevante informatiedomeinen** De logistiek van informatie staat centraal. Informatie moet beschikbaar zijn voor diegene die deze voor de uitoefening van zijn taak nodig heeft. Informatie wordt geordend naar kennisgebieden of –domeinen; niet naar het proces waarin die informatie ontstaat of wordt gebruikt. Op deze manier is het mogelijk processen en technologieën aan te passen, zonder dat dat buitensporige consequenties heeft voor de informatie en de logistiek ervan. Informatie die binnen en buiten de strafrechtketen wordt uitgewisseld is geordend in vier gebieden: - Personen: informatie over de direct betrokkenen (verdachte, slachtoffer, getuige, …) in de strafrechtketen. - Zaken[5]: informatie over het juridisch traject dat binnen de keten wordt afgelegd van incident tot interventie. - Beslissingen: informatie over de beslissingen die gedurende het strafrechttraject zijn genomen. - Bewijsmiddelen: informatie over goederen of sporen die als bewijs kunnen dienen in een strafrechttraject. *[Zie Informatiedomeinen, Het begrip zaak en Het begrip dossier]*
… van begin tot eind volgen …	**Volgen van informatie over personen, zaken, beslissingen en bewijsmiddelen** Om de juiste beslissingen te kunnen nemen over personen, zaken, beslissingen en bewijsmiddelen, is het nodig de beschikking te hebben over een volledig beeld van datgene/diegene (het *object/subject*) waarover in het strafrechttraject een beslissing genomen moet worden. Op ketenniveau moet daarvoor een aantal *ketensteunpunten* ingericht worden, die het mogelijk maken objecten/subjecten op ketenniveau te kunnen volgen, door informatie vanuit de verschillende strafrechtketenpartners met elkaar te kunnen verbinden. *[Zie Ketensteunpuntvoorziening]*
… zodat de informatie tijdig en volledig beschikbaar is …	**Kwaliteit van informatie** De kwaliteit van een beslissing of handeling wordt in hoge mate bepaald door de kwaliteit van de informatie die beschikbaar is. Partijen

[5] Met zaken bedoelen we hier het juridisch strafrechttraject. Van incident tot en met interventie. In de paragraaf “Het begrip zaak” gaan we hier verder op in.

	leveren informatiediensten aan elkaar, waarin het te verwachten resultaat (o.a. in termen van tijdigheid en volledigheid) duidelijk is afgesproken. *[Zie Dienstoriëntatie]*
… voor wie dat nodig heeft en mag hebben …	**Op maat informatie beschikbaar stellen** Professionals moeten tijdig en volledig over betrouwbare informatie kunnen beschikken voor de taak waarvoor zij zich gesteld zien. Dat betekent echter niet dat iedereen zomaar onverkort over alle informatie die bekend is over een bepaald *object* of *subject* mag beschikken. Informatie wordt daarom 'op maat' verstrekt aan diegene die dat voor uitoefening van zijn taak op dat moment nodig heeft (*dataminimalisatie*) en waarover hij op grond van een gerechtvaardigd doel mag beschikken (*doelbinding*). *[Zie Gegevensbescherming en Informatiebeveiliging]*
… binnen en buiten de strafrechtketen …	**Dienstverlening aan elkaar en daarbuiten** Partijen binnen en buiten de strafrechtketen werken met elkaar samen door diensten aan elkaar te verlenen, vertrekkend vanuit de *overall* ketenprestatie. De samenwerking wordt georganiseerd door het maken van afspraken op koppelvlakken (*ontkoppeling*). Dit heeft als voordeel dat ketenpartners met behoud van hun eigen rechtstatelijke verantwoordelijkheid informatie kunnen delen en samenwerken. Ketenpartners kunnen hierbij hun eigen voorzieningen inrichten en hun eigen ontwikkeltempo aanhouden. De gegevens kunnen beter worden beheerd en actueel gehouden doordat noodzakelijke redundantie wordt gecontroleerd. Fouten in de vastlegging kunnen vroegtijdig worden onderkend en in samenwerking worden hersteld. De gegevens kunnen bovendien op verschillende manieren worden gecombineerd: in de vorm van dossiers maar ook rond personen (voor de persoonsgerichte aanpak), fenomenen, gebeurtenissen, locaties, etc. De gegevensdiensten zijn vervolgens niet alleen voor de ketenpartners in enge zin beschikbaar maar kunnen ook gebruikt worden voor dienstverlening aan een bredere kring van betrokkenen. *[Zie Maximale ontkoppeling]*
… ten behoeve van informeren, handelen, beslissen, leren, besturen en verantwoorden.	**Bijdrage aan Ketendoelstellingen** De strafrechtketen moet bijdragen aan een veilige en rechtvaardige samenleving. Professionals binnen de strafrechtketen moeten daarom over informatie beschikken om juist te kunnen handelen of beslissen. Het resultaat van hun handelen en beslissen levert ook weer informatie voor leren en besturen. Ook moet er informatie uitgewisseld worden met partijen buiten de strafrechtketen om hen te informeren of verantwoording af te leggen over de gang van zaken binnen de strafrechtketen. *[Zie Visie op de Strafrechtketen]*

De brug en de architectuur

De brug is de metafoor om de eigenstandige verantwoordelijkheid (zie “Rechtsstatelijkheid”) van de ketenpartners duidelijk te maken (die krijgt vorm in de pijlers van de brug) alsook om uit te drukken dat informatie op een gestandaardiseerde manier wordt uitgewisseld (dat gebeurt via de leggers en de bogen). Daarmee ligt de verantwoordelijkheid voor inhoud en betekenis van de gegevens in de pijlers en niet bij de leggers en bogen. De leggers en de bogen van de brug ondersteunen de communicatie en coördinatie tussen alle ketenpartners, en in alle richtingen. De brug krijgt vorm vindt plaats met behulp van een beperkt aantal gemeenschappelijke en ketenvoorzieningen. Deze voorzieningen werken wij uit in het hoofdstuk “Gemeenschappelijke voorzieningen”.

Bij het ontwerp van de brug zijn ontkoppeling (zie uitwerking in “Maximale ontkoppeling”) en eenheid van taal (zie “Interoperabiliteit) kernbegrippen. Daarmee geeft de brug niet alleen een technische oplossing voor de informatie-uitwisseling, het behelst ook afspraken maken, daarop toezien en die handhaven.

De verbinding tussen de leggers van de brug en de pijlers vindt plaats met behulp van transitiesystemen[6]. Deze verzorgen de aansluiting van de systemen van de ketenpartner op de brug en de eventuele vertaling (van formaten, protocollen en gegevens) die daarbij nodig is. Iedere organisatie is zelf verantwoordelijk voor de realisatie en instandhouding van zijn eigen transitiesystemen. Partijen kunnen daarbij wel gebruik maken van dezelfde technologie. Om interoperabiliteit te waarborgen vindt de uitwisseling tussen legger en transitiesysteem plaats volgens afgesproken semantische en technische standaarden.

De transitiesystemen verbergen voor de keten het interne applicatielandschap van de ketenpartner (*information hiding*), terwijl ze intern met de systemen van de ketenpartner verbonden zijn[7]. Met het maken van (afspraken over het gebruik van de) ketenvoorzieningen wordt voorkomen dat er *point2point* koppelingen ontstaan tussen primaire processystemen van verschillende ketenpartners.

Kernelementen

Interoperabiliteit

Communicatie en gezamenlijke gegevens vragen eenheid van taal en begrip. Vindbaarheid, toegankelijkheid en interoperabiliteit, zowel semantisch als technisch (FAIR[8]) zijn voorwaardelijk om zinvol met elkaar te communiceren.

In de strafrechtketen zijn het canonieke datamodel (CDM) en de standaardreferentiegegevens een formele standaard. Tussen ketenpartners wordt conform het canonieke datamodel uitgewisseld. Zowel de standaard als de toepassing daarvan laat op dit moment te wensen over. Ook het aanwijzen van de verantwoordelijkheid voor gegevens is in onvoldoende mate gebeurd.

Daarnaast is het voor de samenwerking in de keten van belang dat de gegevens vindbaar, toegankelijk, uitwisselbaar en herbruikbaar zijn (FAIR). In het bijzonder is het van belang dat de ketenpartners afspraken maken over de ketensemantiek. Die is noodzakelijk om tot zinvolle uitwisseling van gegevens te komen. De achtergrond daarbij is de volgende. Iedere ketenpartner hanteert “in eigen huis” zijn eigen taal, vaak bepaald door wet- en regelgeving en/of internationale afspraken. Dat roept vragen op als: Wordt met een “adres” bedoeld het woonadres volgens de BRP, het laatst bekende verblijfadres, het adres dat voor betekenen van een vonnis wordt gebruikt of een van de adressen waarop een verdachte zich weleens zou kunnen bevinden?

Het gevolg van het een en ander is dat het delen van gegevens dan wel met “koud” toegang te geven tot de eigen interne Oorsprong-gegevens niet voldoende is. De ketenpartners kunnen uit deze Oorsprong-gegevens namelijk geheel onbedoelde en onwenselijke conclusies voor hun eigen werk trekken [WIO]. De beheerder van de Oorsprong-gegevens dient er dan ook voor te zorgen dat bij het ontsluiten van zijn gegevens voor een bredere kring van betrokkenen via een Bron gebruik gemaakt wordt van de semantiek van de Strafrechtketen, zoals uitgedrukt in het Canoniek DataModel (CDM). Indien nodig vertaalt hij de Oorsprong-gegevens naar dit CDM.

[6] In de bruggenplaat wordt gesproken over transitiesystemen. Om verwarring van transitiesystemen en met transitiearchitectuur te voorkomen spreken wij liever over ketenaansluitsysteem of ketenaansluitvoorziening
[7] In de bruggenplaat wordt gesproken over bestaande systemen. Omdat wij een doelarchitectuur opstellen spreken wij liever over ketenpartnersystemen wat zowel bestaande als toekomstige systemen omvat.
[8] FAIR: findability, accessibility, interoperability, and reusability.

Openstaand: Onderzocht dient te worden of CDM uitgebreid moet worden voor het gebruik van semantische modellering van gegevens (b.v. conform de MIM-standaard [MIM]) die in de keten gedeeld worden. Hiermee kan een grote flexibiliteit en ontkoppeling gerealiseerd worden, welke ook transities vereenvoudigt.

In het onderzoek "Informatie-uitwisseling in samenwerkingsverbanden" [ISV] wordt benadrukt dat eenheid van begrip en taal over disciplines en organisatie zijn grenzen heeft. Verschillen in methodes, werkwijzen, socialisatie en cultuur noodzaken tot onderlinge professionele uitwisseling in plaats van gestructureerd digitaal. Kijken in elkaars dossiers is om die reden af te raden. In het rapport iOverheid [RIO] van de WWR wordt het probleem van het uit context halen van gegevens in combinatie met het samenvoegen met gegevens uit andere contexten beschreven. Indien noodzakelijk dient het strikt beperkt te worden tot die informatie waarover geen misverstanden kunnen zijn. De facto beperkt het zich dan tot feitelijke informatie mits de semantiek expliciet gemaakt en afgesproken is.

Afspraken maken over semantiek is stap een. Het naleven, toezien, handhaven en verbeteren van die afspraken in ketenverband dient hiermee onlosmakelijk verbonden te zijn, te meer daar juistheid, volledigheid en controleerbaarheid van informatie een voorwaarde is voor het nemen van ingrijpende beslissingen door de ketenpartners. Dit vraagt om het inrichten van ketenbrede datagovernance, te positioneren in het Duurzaam digitaal stelsel.

Informatiedomeinen

De strafrechtketen is omvangrijk, daarom is de informatie geordend in 5 informatiedomeinen:

1) Personen;
2) Strafrechttraject;
3) "Bewijs en beslag";
4) Beslissingen;
5) Operatie.

De domeinen zijn gegroepeerd rond informatieobjecten uit het CDM. De basis voor de clustering is de materie- en informatiekundige samenhang van de gegevens binnen een domein.

Per informatiedomein worden semantische afspraken gemaakt over de aan dat domein toegewezen informatieobjecten en de samenhang daartussen, en die tussen de informatiedomeinen, als ook afspraken over de voor de keten aangewezen bron inclusief de verantwoordelijke voor dat gegeven. Voor verdere verdieping zie: Raamwerk gegevenskwaliteit strafrechtketen [RGK] en DAMA-Body of Knowledge kader van de informatiehuishouding.

Toelichting per domein:

Ad 1) Personen

Binnen dit domein worden de afspraken gemaakt over: betrokkenen (verdachte, veroordeelde, etc.), slachtoffer (en nabestaande) en getuigen.

Ad 2) Strafrechttraject

Binnen dit domein worden de afspraken gemaakt over: de juridische begrippen van incident tot en met interventie. Het gaat hier om belangrijke informatieobjecten zoals – incident, strafbaar feit, ten laste legging – en hun onderlinge afhankelijkheden.

Merk op dat het begrip zaak hier niet voor komt. Zaak is geen juridisch begrip, het is een logistiek begrip, het is een eenheid van werk of behandeling.

Ad 3) "Bewijs en beslag"

Binnen dit domein worden de afspraken gemaakt over: (potentiële) bewijsmiddelen / forensisch materiaal en in beslag genomen objecten.

Ad 4) Beslissingen

Binnen dit domein worden de afspraken gemaakt over: beslissingen die rond een persoon of zaak zijn genomen. Zoals rechterlijke uitspraken, de inzet van dwangmiddelen, plaatsingsbesluiten, afdoeningsbeslissingen.

N.B.: De inhoud van dit domein schuurt tegen het domein "Strafrechttraject". Waar het bij het strafrechttraject gaat om de sequentie van de juridische stappen gaat het hier om de uitkomst van

alle beslissingen die in dat traject genomen worden. Bij verdere uitwerking moet blijken of het zinvol is het onderscheid tussen de twee domeinen te handhaven.

Ad 5) Operatie

Binnen dit domein worden de afspraken gemaakt over de logistieke begrippen in de keten. Zoals zaaknummers, attentiesignalen, dossiers, opdrachten, verwijsindices. Het gaat om die informatie die nodig is om het strafproces op operationeel niveau uit te voeren en te volgen. Het is geen inhoudelijk domein.

In de bijlage "Informatiedomeinen" is een eerste invulling aan de hand van CDM opgenomen.

In het denken, werken en het dagelijks taalgebruik in de strafrechtketen hebben de begrippen zaak, dossier, origineel en kopie een belangrijke plaats. Daarom gaan we daar hieronder dieper op in. We staan daarbij op de schouders van de inzichten die opgedaan zijn in het programma Digitaal Werken Strafrechtketen (DWS).

Het begrip zaak

Het NORA katern *Zaakgericht werken* beschrijft een zaak als '*een samenhangende hoeveelheid werk met een gedefinieerde aanleiding en een gedefinieerd resultaat waarvan kwaliteit en doorlooptijd bewaakt moeten worden'*. En wat die samenhangende hoeveelheid van werk is, wordt bepaald door de organisatie van de behandelaar. Dit maakt dat "de zaak" in de Strafrechtketen eigenlijk niet bestaat. Elke ketenpartner die een taak, een samenhangende hoeveelheid werk, in de strafketen uitvoert, heeft daarmee ook zijn eigen zaak.

Het kernproces, de grondvorm, van de strafrechtketen wordt gedefinieerd als opsporing, vervolging, berechting en uitvoering van straffen. Verschillende ketenpartners zijn de dominante uitvoerder van een activiteit in dit proces. Elke ketenpartner heeft zijn eigen zaak, daarmee wordt de keten een aaneenschakeling van zaken. Voor eenvoudige politie-onderzoekszaken met een beperkt aantal feiten en één verdachte lijkt het alsof 'de zaak' door de keten stroomt. Het onderzoekdossier wordt als Eind-PV aangeboden aan het OM en als één parketnummer ingeschreven, het wordt vervolgens als één zaak aangeboden voor vervolging bij de rechter, enz. Maar dat is een uitzondering. Verschillende verdachten bij een incident kunnen leiden tot meerdere zaken bij het OM, zaken kunnen om bepaalde redenen worden gesplitst of samengevoegd. Dat vergroot de complexiteit, waardoor het volgen van de zaak uiterst moeizaam wordt. Zie ook het rapport van de Algemene Rekenkamer. [RAK]

In lijn met "de verdachte in de ketens" [VIK] zetten we het juridisch strafrechttraject centraal: *van incident tot en met interventie*. Het zijn juist deze elementen die de aaneengeschakelde producten vormen in de strafrechtketen, ongeacht de activiteiten die in het werkproces worden uitgevoerd. Uiteraard moet de relatie tussen de onderlinge stappen in het werkproces van het juridisch strafrechttraject herkenbaar zijn, evenals in welke fase een zaak zich bevindt. Voor een slachtoffer is het dan mogelijk zijn incident te volgen zonder in zaken verdwaald te raken.

Hiermee nuanceren we vanuit informatiekundig perspectief het begrip zaak en zetten in op traceerbaarheid van zowel zaken als de elementen in een zaak. Er is geen streven naar een standaardisatie van "de zaak".

Het begrip dossier

Een dossier is een bundeling van stukken met een bepaald doel en/of voor een gegeven doelgroep. In de strafrechtketen wordt de term processtuk gebruikt voor alle stukken waarop een strafrechtelijke beslissing kan worden genomen. Stuk of document is de meer algemene term die voor alle ketenpartners bruikbaar is.

Dezelfde stukken kunnen deel uitmaken van meerdere dossiers. Een dossier kan zelf ook weer uit meerdere (sub)dossiers bestaan. Als voorbeeld: meerdere verdachtendossiers in een politieprocesdossier kunnen verwijzen naar dezelfde aangifte.

Een document is de vastlegging van een verzameling van gegevens met een vastgesteld doel op een bepaald moment in een bepaalde vorm (vergelijkbaar met een snapshot). In een digitaal dossier kunnen documenten bestaan in meerdere vormen, zoals tekst, beeld, video, XML.

In iedere fase in het strafrechttraject is een strafrechtketenactor (wettelijk) verantwoordelijk voor een dossier. Voorbeelden van strafrechtketenactoren zijn opsporingsambtenaar, Officier van Justitie en Rechter. Andere actoren waarmee wordt samengewerkt kunnen bijdragen leveren aan het dossier. De verantwoordelijke bepaalt de regels die gelden voor het dossier, zoals welke stukken in het dossier worden geplaatst en wie ze mag inzien. Daarnaast moet hij/zij zorgen voor "equality of arms", waarmee bedoeld wordt dat de

verantwoordelijke er voor moet zorgen dat het dossier zo wordt ingericht dat alle procesdeelnemers in een strafrechttraject gelijke proceskansen krijgen en een partij procesrechtelijk niet achtergesteld wordt ten opzichte van een andere partij.

Bij het overdragen van een dossier dienen zowel de afzonderlijke processtukken gewaarmerkt te zijn (E-handtekening) als de samenstelling van het dossier.

Originelen en kopieën

In de papieren wereld is het origineel goed herkenbaar. Het is een papieren document met de natte handtekening en een paraaf van de auteur of aanbieder op alle pagina's. In de digitale wereld is dat minder helder. In de Memorie van Toelichting op de Wet digitale Processtukken Strafvordering 2014 wordt hier uitgebreid bij stil gestaan:

"Voor elektronische documenten is het niet mogelijk onderscheid te maken tussen een origineel en een kopie. Hier komt bij dat de inhoud van een elektronisch document eenvoudig te wijzigen is. De integriteit van elektronische documenten is lastiger vast te stellen dan de integriteit van papieren documenten. Met het begrip integriteit wordt gedoeld op de zekerheid dat het document volledig is en niet onbevoegdelijk is gewijzigd. Daarom is het noodzakelijk informatie vast te leggen en te bewaren over de eigenschappen van elektronische documenten, de auteur(s) hiervan en de in de tijd daarin aangebrachte wijzigingen, zodat het altijd mogelijk is de integriteit ervan te verifiëren. Het vastleggen en bewaren van die informatie vereist een zogeheten «unbroken custody» ofwel ononderbroken beheer van elektronische documenten. Zo kan inzicht worden verkregen in de levenscyclus van elk elektronisch document dat onderdeel uitmaakt van het strafdossier: van het moment van creatie of inzending tot de archivering."

Digitalisering vraagt digitaal waarmerken, een chain-of-custody met wijzigingshistorie en de mogelijkheid de integriteit van een document te controleren.

Maximale ontkoppeling

Ontkoppeling – zoals verbeeld in de metafoor van de 'strafrechtketenbrug' en uitgedrukt in de leidende principes digitalisering (AP6), het vergroten van het aanpassingsvermogen (AP3) en de noodzaak te kunnen differentiëren (AP5) – krijgt vorm langs twee assen:

1) Dienstoriëntatie (AP4) waarmee we de binnenwereld van organisaties en informatievoorziening verbergen en werken aan verzakelijking;

2) Gelaagdheid in de informatiehuishouding wat leidt tot een *loosely coupled* landschap.

Dienstoriëntatie

Om samen te werken in ketens en netwerken is het van belang dat op ieder moment helder is welke actor aan welke andere actor een dienst verleent, wat de vragende actor ermee bedoelt, en welk resultaat die dan mag verwachten. Dit samenwerken volgens diensten heeft als operationeel voordeel dat op ieder moment duidelijk is wie aan zet is of wanneer die de zet van een ander verwacht. Samenwerken volgens diensten heeft verder als voordeel dat het partijen ontkoppelt, zodat iedere partij zich intern op eigen tempo en met eigen prioriteiten kan ontwikkelen, terwijl dit de dienstverlening van en naar andere partijen niet wordt beïnvloed.

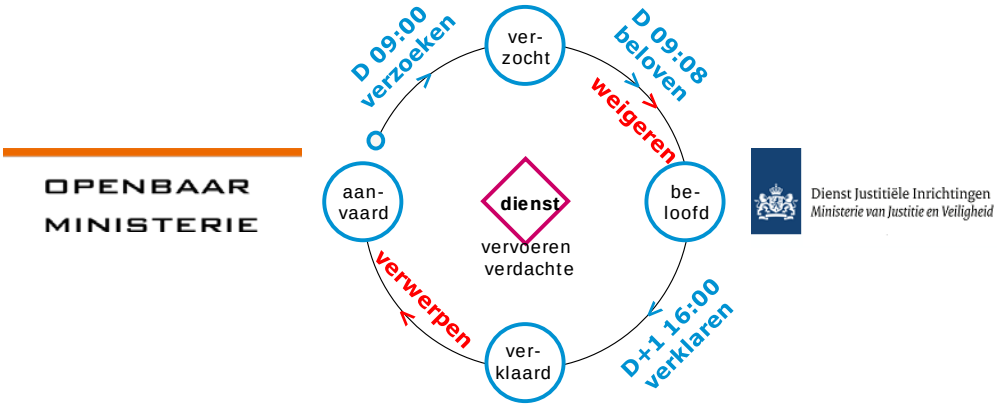
Dienstoriëntatie is een concept dat toepasbaar is voor samenwerkingsafspraken en processen én bij het verkrijgen van informatie. We spreken dan ook over bedrijfsdiensten en informatiediensten. Een voorbeeld van een bedrijfsdienst is "het vervoeren van de justitiabele". Een voorbeeld van een informatiedienst is "het leveren van de bejegeningsgegevens van een justitiabele". Waarbij die informatiedienst niet alleen bij een vervoersopdracht gebruikt kan worden, maar bijvoorbeeld ook bij de bedrijfsdienst "het plaatsen van een justitiabele p in een inrichting".

In de Strafrechtketendoelarchitectuur concentreren we ons op het vormgeven van en sturen op diensten op koppelvlakken tussen ketenpartners. Daarnaast reiken we handvatten aan hoe die diensten systematisch in te passen in door ketenpartners vorm te geven processen, door gebruik te maken van coördinatie-acties (zoals verzoeken en beloven).

Om dit te realiseren is het van belang dat op ieder moment helder is wie aan wie een dienst verleent, wat die ermee bedoelt, en welk resultaat die mag verwachten. Zo kan om de bedrijfsdienst "het vervoeren van een justitiabele" worden verzocht vanuit diverse ketenpartners. Op het koppelvlak wordt aangegeven wat het verwachte resultaat is, wie daarvoor gaat zorgen en op welke termijn. Zo'n verzoek kan worden beantwoord met een belofte, maar ook met een weigering (uiteraard op verantwoorde wijze onderbouwd). Op

een verzoek of belofte moet uiteraard ook kunnen worden teruggekomen als daar reden voor is – bijvoorbeeld als het inmiddels niet meer nodig, mogelijk of verantwoord is om de justitiabele in kwestie te vervoeren. Door iedere stap van het aangaan en naleven van afspraken voor het afnemen van een dienst op het koppelvlak tussen ketenpartners expliciet te maken (zie “Patroon: Afsprakenpatroon”) is op ieder moment duidelijk bij wie de bal ligt, zodat iedere netwerkpartner daar zijn eigen voorgenomen gedrag op kan afstemmen.

Van groot belang is dat de coördinatie bij het uitvoeren van diensten uniform en aantoonbaar volledig kan plaatsvinden. Bekend is de zogenaamde “happy flow” van een dienst, met het verzoeken, beloven, verklaren en aanvaarden daarvan. Hierbij verzoekt de ene partij (afnemer) de andere partij (dienstverlener) een (bedrijfs)dienst te verlenen - bijvoorbeeld "het vervoeren van de verdachte uit bewaring naar de rechtszitting morgen om 16:00". Normaal gesproken zal de dienstverlener (in dit geval: DJI) deze dienst toezeggen en uitvoeren en het resultaat opleveren aan de dienstafnemer (in dit geval: OM). Deze flow is vaak de eerste kandidaat om goed in te regelen en van geautomatiseerde ondersteuning te voorzien. Heel anders is het gesteld met coördinatie-acties in de zogenaamde “crappy flow” zoals weigeren, verwerpen en op je woorden terugkomen. Waar een standaardverzoek in een ommezien kan worden afgewikkeld, kan een correctie of intrekking daarvan moeizaam tot onbegonnen werk zijn omdat deze zich door de keten verspreid kan hebben [VIK, DDK]. Dit laatste maakt het noodzakelijk om te investeren in foutherstelvermogen in de keten: “het herstellen van fouten door alle publieke organisaties dient te worden erkend als te behoren tot hun kerntaken" [VIK]. Hierbij wordt dan gebruik gemaakt van het “universele transactiepatroon”, dat zowel “happy flow” als “crappy flow” omvat (zie Patroon: Afsprakenpatroon).



Diensten vormen verder het aanknopingspunt voor **afspraken** tussen ketenpartners. Die afspraken kunnen gaan over de kwaliteit van de operatie, zoals levertijd, leverbetrouwbaarheid, bedientijden, *Mean Time Between Repairs*, etc. (zogenaamde *Quality of Service* indicatoren). Daarbovenop komen de rechten en plichten voor degene die de dienst afneemt respectievelijk levert; wie mag bijvoorbeeld verzoeken indienen, via welke kanalen, en aan welke vormvereisten moet zo'n verzoek dan voldoen; en hoe houdt degene die de dienst levert de afnemer op de hoogte van de voortgang en hoe geeft die de afnemer de kans om bij te sturen. Verder afspraken over inrichting van de dienst: wie is verantwoordelijk voor totstandbrenging, instandhouding en financiering van de dienst, en aan welke aansluitvoorwaarden dient de afnemer te voldoen (b.v. "moet correcties even vlot kunnen verwerken als de originele opdrachten").

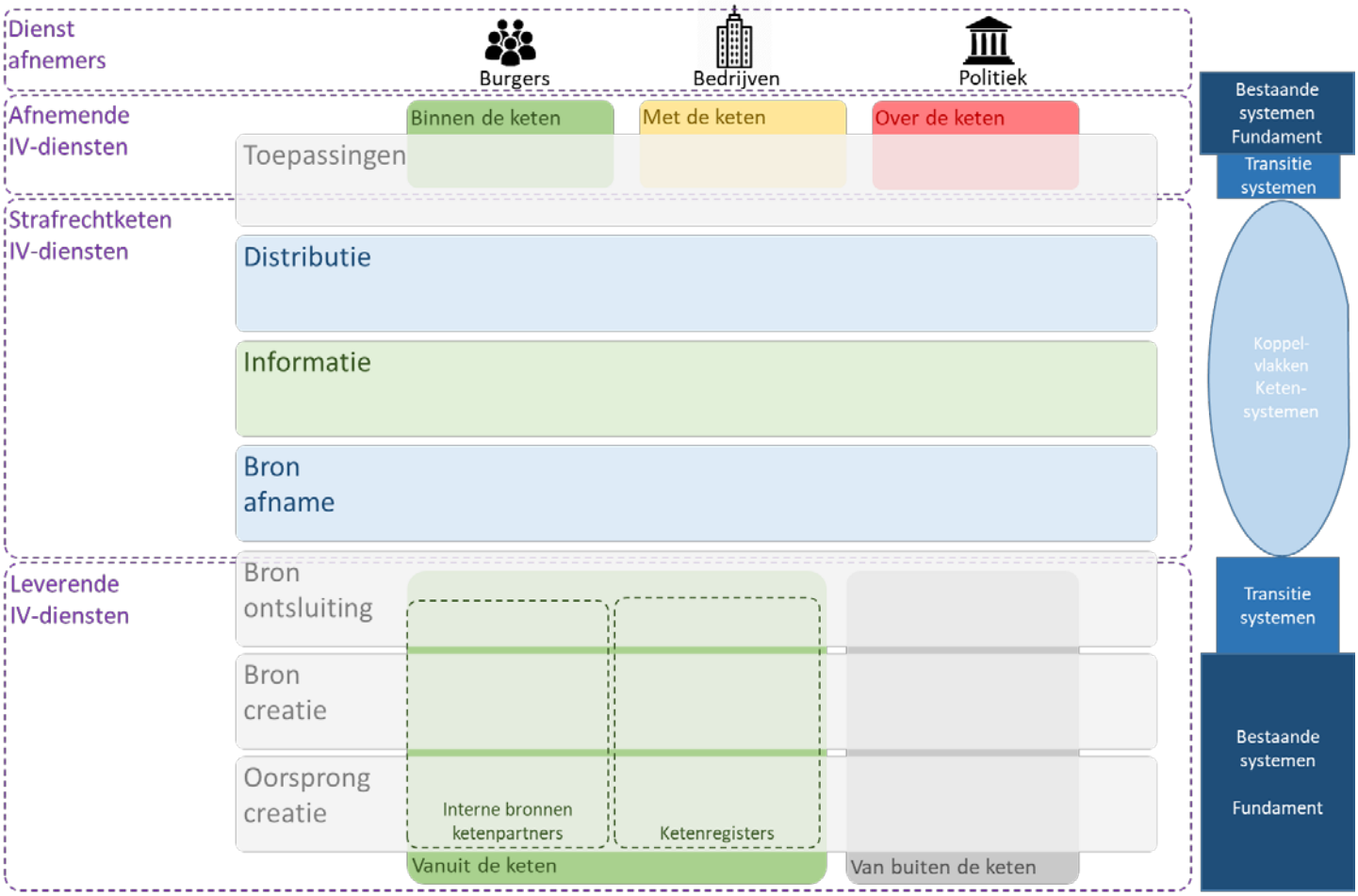
Samenvattend: dienstoriëntatie past bij een context waarin niemand de baas is, maar waar eenieder afhankelijk is van het aangaan en naleven van commitments. Het patroon maakt bewuste keuzes mogelijk over expliciete bevestiging en terugkoppeling, en de mate waarin foutherstel wordt gefaciliteerd. Door toepassing van dit patroon ontstaat tevens traceerbaarheid in de tijd en daarmee transparantie. Hetgeen bijdraagt aan verzakelijking, transparantie en feedback. Voorwaarden voor het realiseren van het mantra.

Gelaagdheid

Maximale ontkoppeling in de informatiehuishouding wordt bereikt door het uitwisselen van informatie te structureren in verschillende, onafhankelijk van elkaar functionerende lagen. Elke laag heeft zijn eigen functionele verantwoordelijkheid en schermt de interne werking daarvan af voor de andere lagen. De lagen sluiten op elkaar aan door middel van goed gedefinieerde diensten. Op die manier heeft een laag geen last van de complexiteit van de inrichting van andere lagen en kan verandering / vernieuwing van de voorzieningen in een laag in het eigen ontwikkeltempo plaatsvinden, zonder dat dat effect heeft op het functioneren van de andere lagen.

In onderstaande figuur zijn die lagen vereenvoudigd weergegeven (in "*Fout! Verwijzingsbron niet gevonden.*" gaan we hier dieper op in). Als toelichting daarbij het volgende:

1. Toepassingen (zoals portalen, applicaties, apps of websites) die informatie nodig hebben worden ontkoppeld van de bronnen bij die leverende partijen door een aantal tussenliggende lagen. Afnemende partijen hoeven zo niet te weten bij welke bronnen zij informatie moeten halen om in hun informatiebehoefte te voorzien. De afspraken die hierover zijn gemaakt, zijn geïmplementeerd in de Informatielaag, evenals de voor de keten afgesproken bron. Starre 1-op-1 koppelingen worden hiermee voorkomen.
2. Partijen stellen hun (bron)informatie ter beschikking van andere ketenpartners door middel van een Bronontsluitingslaag. Bij het ontwerpen en inrichten van deze Bronontsluiting hoeft geen rekening gehouden te worden met elke mogelijke afnemer van die informatie om toch informatie ter beschikking te kunnen stellen. De inrichting van de achterliggende operationele systemen in de Oorspronglaag worden zo ontkoppeld van het gebruik van de informatie in die operationele systemen door afnemers buiten de leverende partij. Op die manier houdt de leverende partij haar vrijheid haar eigen operationele systeemlandschap in eigen tempo en naar eigen inzicht aan te passen, zonder dat de afnemers daar last van hebben (zolang afspraken over inhoud en semantiek van de te leveren gegevens niet wijzigen).
3. De Informatielaag zorgt voor het inhoudelijk bij elkaar brengen van vraag en aanbod, op grond van van overeenkomsten tussen leverende en afnemende partijen, zonder zelf informatie te registreren of kennis te hebben over de (proces)context waarbinnen de informatie zal worden gebruikt. De Distributie- en Bronafnamelagen zijn bedoeld om de eventuele technische verschillen in formaat waarin de informatie wordt geleverd, te overbruggen.



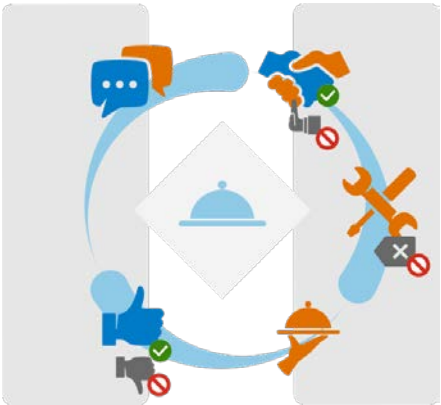
Figuur 7 Lagen van IV-diensten

Merk op dat de lagen zich verhouden tot de brug-metafoor uit de leidende principes. De leverende en afnemende IV-diensten zijn de pijlers, inclusief het fundament. De strafrechtketen IV-diensten zijn de leggers en de bogen.

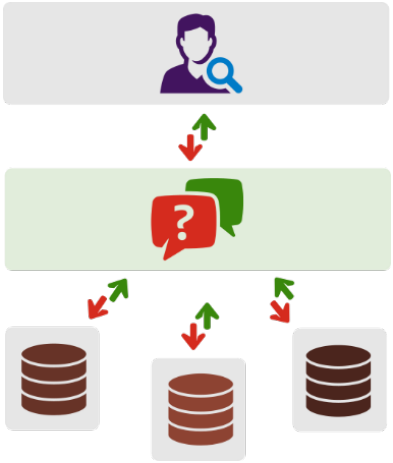
Interactiepatronen

In lijn met Grijpink [KKB], die communicatie in de keten gericht op het bereiken van een gemeenschappelijk ketenresultaat centraal stelt, is het uitgangspunt bij het ontwerpen van samenwerking in ketens de wijze van ontkoppeling van partijen waartussen interactie plaatsvindt. Die manieren noemen we *interactiepatronen*.

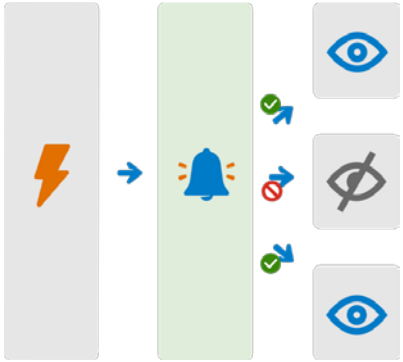
Afsprakenpatroon
Partner A vraagt Partner B een dienst voor hem uit te voeren



Vraaggestuurde informatiedeling
Partner A vraagt andere partners hem informatie te leveren voor taakuitoefening



Notificatie
Partner A maakt andere partners attent op veranderde, belangwekkende informatie



Patroon: Afsprakenpatroon

In dit patroon verzoekt de ene partij (dienstafnemer) de andere partij (dienstverlener) een dienst te verlenen - bijvoorbeeld "het vervoeren van de verdachte uit bewaring naar de rechtszitting morgen om 16:00". Normaal gesproken zal de dienstverlener (in dit geval: DJI) dit doen en het resultaat opleveren aan de dienstafnemer (in dit geval: OM). Het is mogeijk dat de dienstverlener het verzoek weigert, b.v. omdat de risico-analyse of medische gegevens aanleiding geven tot extra maatregelen, die in het gegeven tijdsbestek niet haalbaar zijn. Normaal zal de dienstverlener in overleg treden met de afnemer over aanvaardbare en uitvoerbare oplossingen. Daarnaast is het mogelijk dat zowel dienstverlener als afnemer terugkomen op hun eerdere commitments, bijvoorbeeld omdat de rechter bij nader inzien de wens van de verdachte accepteert om niet ter zitting te verschijnen.

Het nut van dit patroon is dat op ieder moment duidelijk is wie waarvoor verantwoordelijk is. Tijdens het ontwerp van ketensamenwerking kan van iedere stap systematisch worden besloten of het nuttig is om deze expliciet te maken en het resultaat vast te leggen, of dat met impliciete aannames volstaan kan worden.

Afsprakenpatroon

Verzoeken: De ene partij (**dienstafnemer**) vraagt aan de andere partij (**dienstverlener**) hem een dienst te verlenen.
- **Beloven**: De dienstverlener belooft de dienst te leveren onder de afgesproken voorwaarden.
- ***Weigeren***: *de dienstverlener weigert de dienst te leveren.*

Uitvoeren: De dienstverlener gaat aan de slag om de beloofde dienst te produceren.

Verklaren: De dienstverlener verklaart dat hij de dienst heeft geproduceerd zoals beloofd.
- **Aanvaarden**: De dienstafnemer aanvaardt de geproduceerde dienst.
- ***Afwijzen***: *de dienstafnemer wijst de geleverde dienst af.*

Herroepen: *de dienstverlener en dienstafnemer kunnen op enig moment hun aangegane commitment (b.v. verzoek, belofte, maar ook verklaring of aanvaarding)* ***herroepen****, zodat b.v. de dienst niet geleverd gaat worden.*

Dit "Afsprakenpatroon" is een Nederlandse vertaling van het "universal transaction pattern" [EO, Ch. 8].

Het patroon is toepasbaar voor verschillende vormen het maken van een afspraak of het aangaan van een verplichting: het doen van een verzoek, het geven van opdrachten, het overdragen van processtukken en het zelf initiëren van een verplichting, bijvoorbeeld het autonoom starten van een onderzoek.

Patroon: Notificatie- / Signaleringpatroon

De ene partij (de *signalerende partij*) legt op grond van de uitoefening van zijn taak informatie vast die ook (kritisch) relevant is voor andere partijen (bijv. 'persoon is voortvluchtig'). Die andere partijen (de *abonnerende partij*en) willen actief geïnformeerd worden over het feit dat die informatie is vastgelegd of gewijzigd. Zij abonneren zich op een dienst die signaleert dat er voor hen relevante informatie beschikbaar is.

De signalerende partij is na het afgeven van het signaal niet meer verantwoordelijk voor verdere verwerking. De abonnerende partij dient tijdig te beslissen of op het signaal gereageerd wordt. Signalen hebben immers een beperkte levensduur. Dit is per signaaltype vast te stellen.

Voor een abonnement op een notificatie dient een juridische grondslag aanwezig te zijn en er is een verwerkingsovereenkomst tussen de signalerende partij en de abonnerende partij.

De 'dikte van het event' (de compleetheid van de informatie die met de notificatie wordt meegestuurd) is afhankelijk van de gevoeligheid van de informatie en de bevoegdheden van de abonnees. Bij het ontwerp en implementatie van een op dit patroon gebaseerde informatie-uitwisseling moet bepaald worden wat de juiste 'dikte' van het signaal is. Daarbij moet het uitgangspunt zijn dat een signaal niet moet leiden tot (herhaalde) opvraag van informatie.

Notificatiepatroon

Er is een ***ketenvoorziening*** waarbij partijen eventtypes *(synoniem van signaleringtypes/notificatietypes)* kunnen vastleggen, eventueel aangevuld met abonnee-beperkingen (*privacy by design*). Eventtypes zijn gekoppeld aan afgesproken processtatussen en/of informatieovergangen van de betreffende partij.

- Andere partijen kunnen zich abonneren op deze eventtypes.
- Events worden naar de abonnees gestuurd zodra deze ontstaan, deze abonnees kunnen hier vervolgens acties op ondernemen
- Events **kunnen 'dun', 'middel' of 'dik**' zijn, dit is afhankelijk van de gevoeligheid van de informatie en de bevoegdheden van de abonnees. Alle business objecten hebben hierbij een uniek en betekenisloos nummer (*privacy by design*)

Voorbeelden:
- ***Dun:*** *Status verandering in zaak 1234*
- ***Middel:*** *zaak 1234 is in status: 567*
- ***Dik****: Bij zaak 1234 heeft de verdachte 887 status 987*

Patroon: Vraaggestuurde informatiedeling

De ene partij (de *afnemende partij*) heeft behoefte aan informatie die nodig is voor het kunnen uitoefenen van zijn taak over welke informatie hij (nog) niet beschikt. Die informatie is (mogelijk) beschikbaar bij verschillende andere partijen (de *leverende partij*en). De *afnemende partij* vraagt via een intermediair (makelaar) de *leverende partij*en hem een dienst te leveren in de vorm van een informatieproduct dat zijn behoefte afdekt.

De makelaar voert een door de afnemende partij gedefinieerd recept uit. Bij uitvoering wordt gevalideerd op grondslag, doelbinding en autorisaties.

Voor het afnemen van een informatieproduct dient een juridische grondslag aanwezig te zijn en er is een verwerkingsovereenkomst tussen de afnemende partij en de leverende partijen.

Met dit patroon
1) voorkomen we dat onjuiste, dat wil zeggen niet afgesproken, bronnen worden geraadpleegd. Men krijgt altijd de op ketenniveau afgesproken informatie.

2) verbergen we de complexiteit van de keten voor de afnemende partij. Concreet: de burgemeester die in het kader van de BIJ-regeling recht heeft op informatie over een terugkerende gedetineerde hoeft niet te weten welke gegeven van DJI, CJIB of het OM komt. Hij/zij krijgt een eenduidig product aangeboden.

Vraaggestuurde informatiedeling patroon

- **Informatie vragen**: De *informatievrager* werkt voor de uitoefening van zijn taak met de toepassing die hem door de organisatie waar hij voor werkt, ter beschikking is gesteld. Met die toepassing vraagt hij het *informatieproduct* aan dat hij nodig heeft.
- **Informatie vragen**: De vraag wordt behandeld door de **informatiemakelaar** die het informatieproduct gaat samenstellen.
- **Routeren**: De informatiemakelaar vraagt de informatie op bij verschillende **informatiebronnen** die nodig zijn om het informatieproduct te kunnen leveren en door de leverende partijen ten behoeve van ketenbreed gebruik zijn ontsloten.
- De makelaar assembleert de opgevraagde **broninformatie** tot een informatieproduct voor de afnemer. Er wordt geen nieuwe informatie gecreëerd.
- Het **informatieproduct** wordt vervolgens in het gevraagde formaat via het afgesproken kanaal geleverd aan de toepassing van de **informatievrager**.

Verantwoorden en "historische gegevens"

Het verantwoorden van beslissingen is een belangrijk en groot goed in het Strafrecht. Dat betekent ook het inzichtelijk kunnen maken van de informatie waarop de beslisser zijn beslissing heeft gebaseerd. Ongeacht welk interactiepatroon: de beslisser (ontvanger) is zelf verantwoordelijk om dit aan te tonen.

De huidige digitale Informatiehuishouding biedt nauwelijks mogelijkheden om de stand van zaken in het verleden te reconstrueren. Ketenpartners kunnen er dus niet op vertrouwen dat de leverende partij zorg

draagt voor het kunnen reconstrueren van de informatie op het moment van verstrekken, maar moeten hier zelf zorg voor dragen.

Gemeenschappelijke voorzieningen

In de strafrechtketen maken we gebruik van gemeenschappelijke voorzieningen. Een gemeenschappelijke voorziening:

- bestaat altijd uit een afsprakenset (bijvoorbeeld over het toepassen van standaarden (zoals het CDM) of het gebruik maken van bepaalde implementaties);
- kan daarnaast gebruikmaken van een implementatie in de vorm van een (gemeenschappelijke) applicatie, al dan niet met een gemeenschappelijke database (bijvoorbeeld SKDB), met behoud van gescheiden verantwoordelijkheden;
- kan daarnaast gebruikmaken van een implementatie van een (gemeenschappelijk) bedrijfsproces (bijvoorbeeld de Matchingsautoriteit);

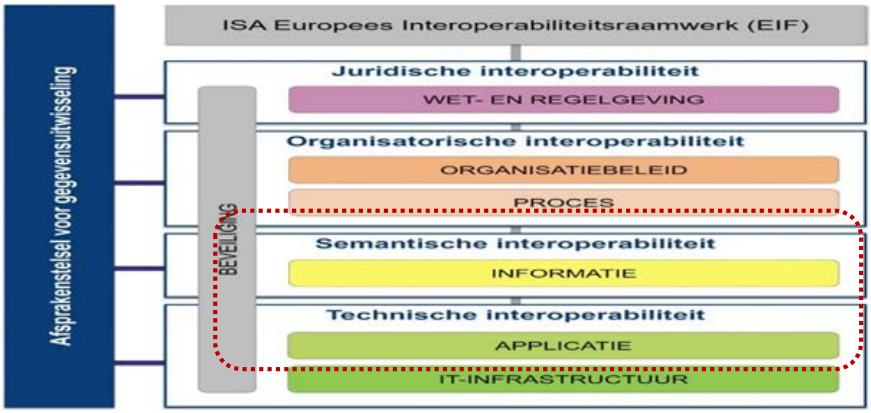
Indien er sprake is van door de voorziening geleverde diensten, dan maken afspraken over de Quality of Service (QoS) deel uit van de afsprakenset. In alle gevallen dienen ook beheer en governance (inclusief financiering) van de gemeenschappelijke voorziening zeker gesteld te zijn.

Implementatiekeuzes worden niet vanuit de KDA voorgeschreven, maar zullen worden uitgewerkt in implementatievoorstellen van voorzieningen. Denk daarbij aan keuzes of de technische of organisatorische implementatie centraal, decentraal, eenmaal of meerdere malen wordt gerealiseerd wordt, evenals de sourcing.

We onderscheiden twee categorieën gemeenschappelijke voorzieningen:

1) Ketencommunicatievoorzieningen
   Voorzieningen die de communicatie en de gegevensuitwisseling in de keten ondersteunen. Deze hebben geen materiële en toepassingskennis van de gegevens die zij verwerken. Denk hierbij aan E-Toegang, E-Index of E-Distributie. We noemen deze voorzieningen ketencommunicatievoorzieningen.
2) Ketensteunpuntvoorzieningen
   Voorzieningen die inhoudelijke samenhang in de keten ondersteunen. Een dergelijke voorziening ondersteunt inhoudelijke (proces)coördinatie en afstemming waarbij iedere organisatie afzonderlijk zijn verantwoordelijkheid behoudt. Voorbeeld hiervan zijn de identiteitsvaststelling en verificatie, biometrie voorziening en de digitale samenwerkingsruimte ZSM. We noemen een dergelijke voorziening een ketensteunpuntvoorziening. Een ketensteunpuntvoorziening maakt gebruik van ketencommunicatievoorzieningen.

Als we deze twee categorieën afbeelden op het Europees interoperabiliteitsraamwerk (EIF) dan valt een ketencommunicatievoorziening (1) binnen de domeinen informatie en/of applicatie. Een ketensteunpunt (2) voorziening levert een bescheiden bijdrage aan meerdere processen, namelijk voor zover dat nodig is voor inhoudelijke coördinatie over organisaties heen.



Ketensteunpuntvoorzieningen

Onderstaand zijn de volgende ketensteunpuntvoorzieningen voor de strafrechtketen die wij nu onderkennen. Een aantal ervan is nieuw, deze zijn kenbaar aan (*).

Persoonsidentificatie en -verificatie

Het identificeren van justitiabelen (verdachte/veroordeelde) door middel van persoonsgebonden gegevens zoals personalia, biometrische gegevens DNA, etc. Justitiabelen hebben een uniek Strafrechtketennummer (SKN), waarmee de leidende identiteit van de justitiabele met de daarbij behorende gegevens te achterhalen is voor verificatie.

Biometrische identificatie en -verificatie
Het identificeren van een persoon door middel van beschikbaar gestelde biometrische gegevens behorende bij een justitiabele met een SKN.

Justitiële documentatie
Het beschikbaar stellen van juridische documentatie (bv strafblad, persoonsdossiers en persoonsrapportage) en justitiële documentatie uit EU-landen aan ketenpartners van de strafrechtketen en EU-landen op basis van doelbinding.

Persoonsbeeld op maat (*)
Het leveren aan ketenpartners van informatie (persoonsinformatie, juridische documentatie, etc.) over een justitiabele op basis van geldende wet- en regelgeving om een handeling uit te kunnen voeren en/of een beslissing te kunnen nemen. Afhankelijk van de informatiebehoefte en de daarbij behorende doelbinding ontvangt de aanvragende functionaris een subset van de beschikbare informatie van de betreffende justitiabele.

Slachtoffers informeren
Slachtoffers (incl. nabestaanden, vertegenwoordigers, enz.) hebben gedurende het strafrecht-, executie- en re-integratieproces op verschillende momenten contact met ketenpartners, waarbij zij geïnformeerd worden over onder andere de voortgang van de zaak waarin zij betrokken zijn en de besluiten die door de verschillende ketenpartners zijn genomen. Het Slachtofferportaal is een van de implementaties.

Melding gerede twijfel en ketenfoutherstel (*)
De ketenpartners in de strafrechtketen moeten werken met gegevens waarop zij kunnen vertrouwen. Bij twijfel over de kwaliteit van de gegevens moet de bronhouder van het betreffende gegeven hier uitsluitsel over geven. Indien foutieve gegevens zijn verstrekt, dienen de ketenpartners die deze gegevens ontvangen hebben geïnformeerd te worden. Er dient een voorziening te zijn die fouten en de gevolgen ervan, met een verantwoorde Quality of Service, in de keten kan herstellen.

Track & Trace "Strafrechttraject" (*)
In de strafrechtketen kan een persoon aan één of meerdere zaken of een zaak aan één of meerdere personen gekoppeld zijn. Voor de ketenpartners is het van belang om te weten dat deze koppelingen er zijn. Het verwijzen van persoon naar zaak en andersom is hierbij noodzakelijk. Hierdoor weet het slachtoffer wat de status is van de behandeling van zijn/haar incident of aangifte. Evenzo voor de verdachte en de verdediging.

Track & Trace "Bewijsmiddelen" (Forensisch materiaal) (*)
Verschillende ketenpartners hebben een verantwoordelijkheid voor het behandelen, onderzoeken van forensisch materiaal. Met track & trace is altijd duidelijk waar het materiaal is, wie welke activiteit uitvoert en in opdracht van wie.

Track & Trace Beslag goederen (*)
Verschillende ketenpartners nemen goederen in beslag waar de rechter een uitspraak moet doen of deze al dan niet worden teruggegeven aan de rechthebbende. Met track & trace is altijd duidelijk waar het in beslag genomen goed is, wie welke activiteit uitvoert en in opdracht van wie.

Samenwerkingsruimte (*)
Binnen de strafrechtketen zijn er verschillende overleggen waar meerdere ketenpartners tegelijkertijd samenwerken aan dezelfde casus. Voorbeelden hiervan zijn onder andere ZSM en Veiligheidshuizen. De ketenpartners zitten hier in hun eigen rol en verantwoordelijkheid. Tijdens deze overleggen hebben alle ketenpartners behoefte aan een persoonsbeeld op maat voor het behandelen van de casus.

Ketenmonitor en data-analyse
De Data Alliantie Strafrechtketen (DAS) is een samenwerkingsverband binnen de strafrechtketen die ketenmonitoring en data-analyse mogelijk maakt, ondersteund door een dashboard. Het doel van de data alliantie is om de gegevens van de strafrechtketen op *één (logische)plek*[9] *te verzamelen*, te *veredelen* en onderling aan elkaar *gerelateerd* en *afloopbaar* te maken. Dit betreft informatie over de werking van de keten, niet over individuele casuïstiek.

[9] Er is wel 1 plek waar informatie opgevraagd kan worden ("single point of truth") maar deze kan fysiek overal in de keten opgeslagen zijn.

Advocatenportaal
Portaal voor de advocatuur voor het stellen van advocaten en het uitwisselen van informatie en processtukken tussen advocatuur en de strafrechtketen.

Verkeersportaal
Geeft de burger de mogelijkheid om verkeerovertredingen in te zien, te betalen en eventueel in verzet te gaan.

Medewerkerportaal (*)
Te onderzoeken: is het wenselijk dat voor het inzien van bronnen buiten de eigen organisatie een standaard portaal beschikbaar is?

n.b. Er is op dit moment geen vastgestelde doelgroepen- en kanalenstrategie voor de Strafrechtketen en voor J&V. Deze dient op korte termijn ontwikkeld te worden. Dit is geen activiteit van de Architectuurraad.

Ketencommunicatievoorzieningen

De volgende tabel benoemt de ketencommunicatievoorzieningen die we op dit moment onderkennen. De laatste kolom geeft aan of de voorziening naast de ketenbrede afspraken ook ondersteunende ICT-systemen vereist.

Keten-communicatie-voorziening	Omschrijving op hoofdlijnen	ICT-systemen
E-semantiek	E-semantiek gaat over het ***uitwisselen van gegevens*** in de SRK, en partners buiten de SRK (bijvoorbeeld gemeenten, zorgdomein, internationale rechtshulpverzoeken). Om dit gestructureerd te doen zijn er afspraken gemaakt over de ***betekenis*** en vorm van de gegevens. Deze afspraken betreft: - **Definities** van gegevens; - ***Gegevenstypes en hun onderlinge samenhang*** in het Canoniek Datamodel (CDM); - ***Referentiegegevens*** en Code-stelsels (gegevens en bijbehorende waarden); - ***Afleidingsregels*** voor communicatie met andere partijen (zoals Migratieketen, Zorgketen en Burgerdomein), voor zover voor meer informatieproducten en/of ketenpartners relevant. Semantiek wordt inhoudelijk bepaald door de betrokken ketenpartners.	Ja
E-portalen (afsprakenset, gericht op technische implementatie)	**Portalen** geven gebruikers de mogelijkheid om digitaal te communiceren met de strafrechtketen. Hierdoor hebben burgers en partijen de mogelijkheid digitale stukken uit te wisselen en processtatussen te kunnen zien. E-portalen omvat **de afspraken** om dit op uniforme wijze te doen. We kennen organisatieportalen en doelgroepportalen. Organisatieportalen zijn gescheiden om geen misverstand te laten ontstaan over de rechtstatelijk gescheiden verantwoordelijkheden in de strafrechtketen. Doelgroepportalen geven aan doelgroepen die dat behoeven extra ondersteuning door informatie doelgroepsgewijs te bundelen.	Nee
E-koppeling	E-koppeling is een voorziening van elke ketenpartner om **gegevens** op applicatief en infrastructureel te kunnen **uitwisselen** met partijen binnen en buiten de strafrechtketen. Alle ketenpartners dienen hierop aan te sluiten. Deze voorziening bestaat uit: - ***afspraken*** hoe gegevens uit te wisselen (infrastructurele *patronen zoals fire-forget en verzekerd verzenden a la WUS of eBMS; applicatieve patronen zoals push-pull);* - ***infrastructuur*** om deze gegevens conform deze afspraken uit te wisselen (zoals JUBES of API-gateway).	Ja, infrastructureel eenmalig op ketenniveau + per KP regelen aansluiting daarop; applicatief uitsluitend per KP
E-distributie	E-distributie is een voorziening(en) die de **uitwisseling** van gegevens (via E-koppeling) in technische zin **aanstuurt en routeert** conform afgesproken uitwisselingspatronen, en waar nodig code- en formaatconversies (zoals STUF, datum, landcode, JSON-XML) uitvoert – dus conversies met een syntactisch karakter. E-distributie dient tevens de semantische vertalingen te verzorgen tussen partijen binnen en buiten de StrafRechtKeten (SRK) – gebruikmakend van e-Semantiek. Het daadwerkelijk uitvoeren van deze semantische regels zou kunnen worden ondergebracht in een aparte sub-component, werknaam “E-ontsluiting”.	Ja, iedere KP + ketenbreed

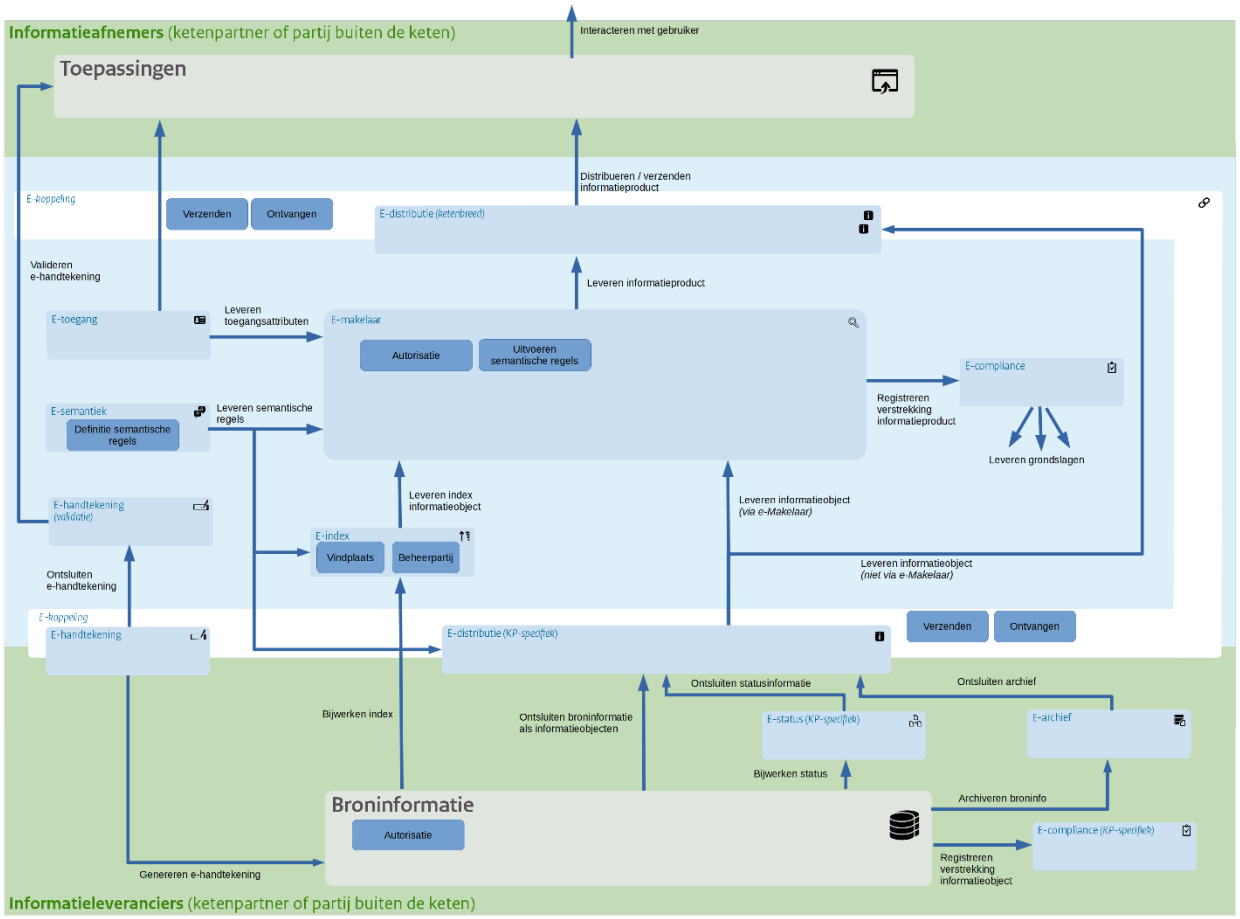
Keten-communicatie-voorziening	Omschrijving op hoofdlijnen	ICT-systemen
E-handtekening *)	E-handtekening is de ketenvoorziening waarmee **digitale stukken** en -informatie-objecten volgens de wet worden **gewaarmerkt, getekend** en **gevalideerd**. Het (digitaal) tekenen en waarmerken gebeurt bij de ketenpartners zelf. Het **valideren** vindt plaats met een centrale voorziening zodat voor alle partijen de status van het stuk of het informatie-object duidelijk is. Deze centrale voorziening raadpleegt daarbij de door de ketenpartner uitgegeven (digitale) handtekening.	Ja, voor valideren
E-archief *)	E-archief is een digitale **bewaarplaats** van digitale stukken. Het E-archief heeft ook een **depot-functie** waar originele media geplaatst kunnen worden. Er is geen sprake van ketenarchivering, organisaties zijn afzonderlijk verantwoordelijk voor **schoning**, **overdracht** en **duurzame opslag**. Wel zijn ketenbrede afspraken nodig (o.a. metadata).	Ja, een ketenpartner kan dit zelf doen of gebruik maken van centrale voorziening
E-index	E-index zorgt met **verwijzingen** voor de **vindbaarheid** van **objecten** (stukken, zaken*)* en **subjecten** (personen*)* en afgesproken **relaties** daartussen conform afspraken binnen de strafrechtketen (E-semantiek). Daartoe legt E-index indices aan die verwijzen naar objecten, subjecten en hun onderlinge verbanden. Verder houdt E-index per gegeven bij (a) wie de inhoudelijk verantwoordelijke beheerpartij is, en (b) wat de fysieke vindplaats (zoals database, API-adres) is. Hiervoor zijn centraal vastgestelde nummerstelsels noodzakelijk.	Ja, deels per ketenpartner
E-compliance[10]	E-compliance is een voorziening die helpt te kunnen **verantwoorden** welke gegevens met welk doel (op basis van grondslagen en doelbindingen) aan wie zijn verstrekt. Dit omvat afspraken over de wijze waarop verstrekkingen dienen te worden verantwoord en geregistreerd. Ieder ketenpartner dient zelf verstrekkingen bij te houden, en daarbij het grondslagenregister te raadplegen. Daartoe beheert E-compliance een **grondslagenregister**. Voor ketenpartner-overstijgende verstrekkingen houdt E-compliance daarnaast een **centraal verstrekkingenregister** bij.	Ja, deels per ketenpartner
E-makelaar	E-makelaar is een voorziening die de **inhoudelijke beantwoording van informatievragen** – eventueel door meerdere bronnen te bevragen – **in één keer verzorgt**. Hiermee wordt het mogelijk (niet verplicht) om: - integrale beelden inhoudelijk op te bouwen (bv. een persoonsbeeld, een zaaksbeeld, etc.) op basis van in informatiedomeinen (bv. Persoonsbeeld op maat) gedefinieerde en in E-semantiek vastgelegde semantiek. - informatievragen af te handelen (via E-distributie bij informatieleveranciers) zonder dat de vrager kennis hoeft te hebben over waar deze gegevens vandaan komen of hoe de strafrechtketen georganiseerd is. De makelaar gebruikt daarbij alleen erkende identificerende gegevens (nummerstelsels etc. via E-index), toetst grondslagen/doelbindingen (met raadpleging van het grondslagenregister via E-	Ja; in ieder geval gedeeld ontwerp; mogelijk meervoudige implementaties

[10] Het begrip 'compliance' past beter bij een ketensteunpuntvoorziening. Om die reden wordt nog overwogen de naam voor de communicatievoorziening te wijzigen en deze naam te reserveren voor een ketensteunpuntvoorziening.

Keten-communicatie-voorziening	Omschrijving op hoofdlijnen	ICT-systemen
	compliance), toetst of de afnemer geautoriseerd is (via E-toegang) en legt de verstrekking vast (via E-compliance). E-makelaar bestaat in ieder geval uit een afsprakenset en een gedeeld ontwerp. Implementatie zou meervoudig kunnen worden uitgevoerd. Zie ook figuur in Bijlage 4: A3 formaat platen Informatiemakelaar.	
E-status	E-status geeft **de toestand** weer van het **aangaan en nakomen van afspraken**, zoals of iets beloofd, verzocht, inmiddels aanvaard, geweigerd of ingetrokken is (zie Patroon: Afsprakenpatroon). Daartoe omvat E-status een afsprakenset over welke toestanden het betreft, de syntax waarin daarover kan worden gecommuniceerd en de wijze waarop tot deze informatie toegang kan worden verkregen (b.v. APIs). Iedere KP die ketentoegang wil verlenen tot diens statusgegevens dient daarvoor zelf de technische voorzieningen te regelen.	Ja
E-toegang *)	E-toegang is een voorziening die **identificeert** en **autoriseert**. Het vaststellen van de identiteit van een gebruiker van de voorzieningen in strafrechtketen kan door middel van: - digitale **inlogmiddelen** vanuit de overheid; - een **federatiesysteem** waarbij de identiteiten van een andere ketenpartner transparant zijn. Voor autorisatie • omvat E-toegang regels en afspraken, zoals de benodigde doelbinding en grondslagen (met raadplegen van E-compliance voor het grondslagenregister) en daaruit volgende benodigde te presenteren attributen; • kan E-toegang machtigingenregisters van derden (zoals BOA-register of advocatenregister) raadplegen.	Ja, deels per ketenpartner

Ad *): Voorzieningen die niet specifiek voor de strafrechtketen is.

Onderstaande figuur beeldt de keten-communicatievoorzieningen af op de lagenplaat en toont de onderlinge samenhang.



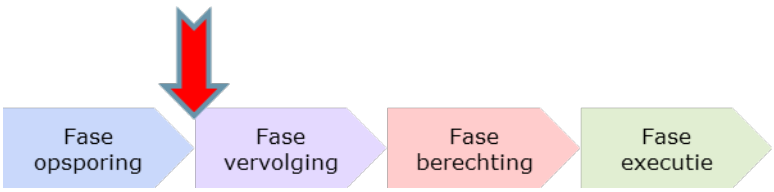
Figuur 8 Samenhang keten-communicatievoorzieningen

Werking van de keten-communicatievoorzieningen in een casus

Het toelichten van de werking en de samenhang van de E-voorzieningen en de interactiepatronen hebben we in voorgaande hoofdstukken modelmatig behandeld. In dit hoofdstuk gebruiken we een simpele casus ter verduidelijking. De casus is gebaseerd op een eenvoudige winkeldiefstal met één verdachte, één winkelier. De zaak komt wél voor de rechter omdat verdachte een veelpleger is. Merk hierbij op dat de casus wordt gebruikt om de werking van de voorzieningen te behandelen, waarbij mogelijk de juridische werkelijkheid niet volledig correct wordt afgebeeld.

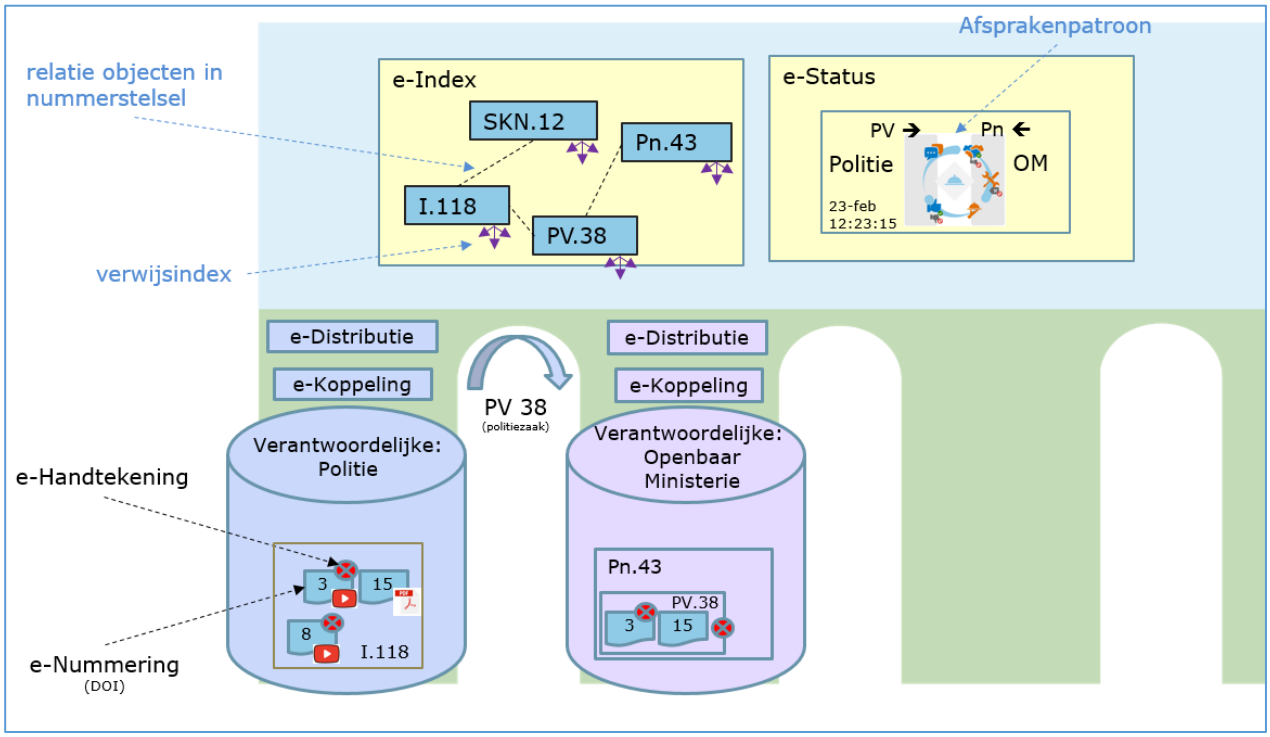
Casus – Overdacht PV van Politie naar het OM

Startmoment: Politie biedt PV aan bij OM voor vervolging



Tijden de opsporingsfase heeft de politie (of andere opsporingsinstantie) voor het incident een opsporingsdossier aangelegd met daarin het videomateriaal dat is verkregen van getuigen. Alle objecten en documenten die van belang zijn voor de keten zijn voorzien van een unieke identificatie door toepassing van de e-

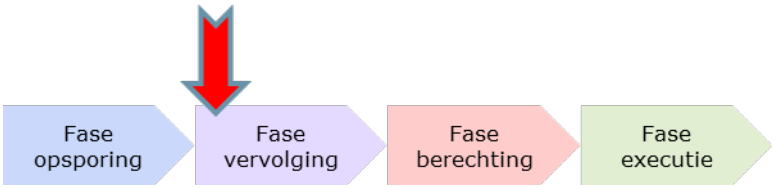
nummering (onderdeel van E-index). In dit beknopte voorbeeld zijn document DOI.3 en DOI.8 de identificaties van videobestanden en is I.118 de identificatie van het Incident. Unieke identificaties zijn van belang om de objecten en documenten te kunnen relateren en te volgen in de keten. Zo wordt ook de relatie gelegd met de verdachte (SKN.12) De integriteit van de documenten worden gewaarborgd door ze te voorzien van een E-handtekening. De politie heeft procesverbaal PV.38 klaargemaakt om aan te bieden aan het OM voor vervolging. Op dat moment wordt er ook een digitale handtekening gezet op de verzameling stukken zodat gecontroleerd kan worden of de set stukken in PV.38 compleet is.



Het aanbieden van PV.38 van politie aan het OM verloopt via E-koppeling en E-distributie. Deze voorzieningen vormen samen het (ont)koppelvlak waarmee de interne ICT voorzieningen van de politie en het OM richting de keten worden afgeschermd. Het aanbieden van het PV betreft een communicatie en (keten)samenwerking tussen de politie en het OM volgens het afsprakenpatroon (zie Hoofdstuk interactiepatronen). De essentiële kenmerken van de afspraak worden vastgelegd in E-status, zodat duidelijk is waar de verantwoordelijkheid ligt voor verdere actie. Voor de verdere vervolging van PV.38 opent het OM een zaak waaraan een uniek parketnummer Pn.43 wordt toegekend. Deze relatie tussen wordt gemeld aan E-index, zodat deze ketenbreed bekend is. In dit voorbeeld kiest het OM ervoor om het PV.38 op te slaan in haar eigen omgeving en wordt de verwijsindex voor PV 38 bijgewerkt.

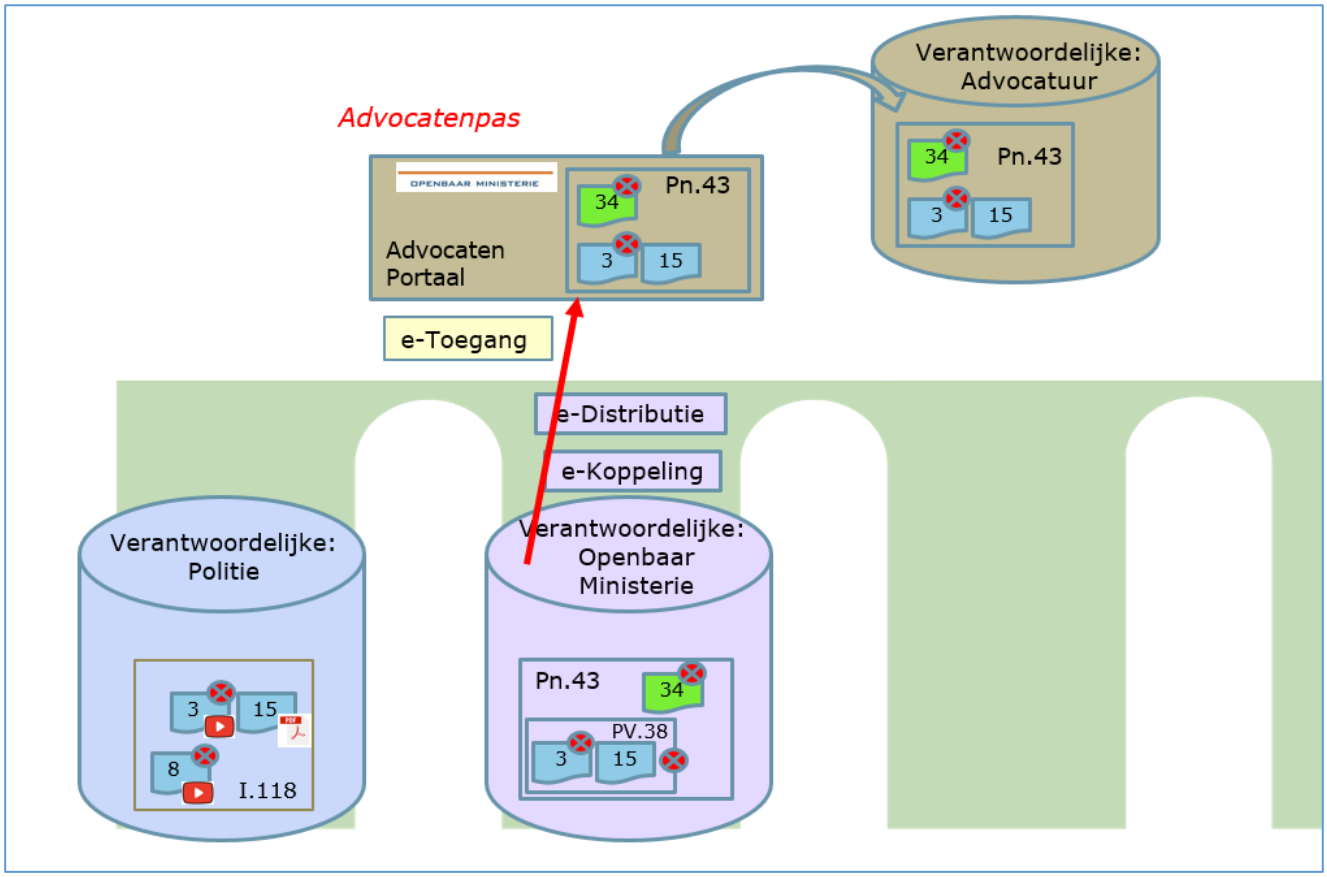
Casus – Informeren advocaat van de verdachte tijdens de fase vervolging

Startmoment: Fase vervolging is gestart. Advocaat is bekend.



Inmiddels is het OM (de OvJ) gestart met de vervolging van de verdachte. De Advocaat van de verdachte heeft zich gesteld en is gekoppeld aan de zaak Pn.43. De OvJ heeft inmiddels het dossier uitgebreid met een het ondertekende document DOI.34. De advocaat meldt zich bij het advocatenportaal en logt in met zijn advocatenpas, een erkend authenticatiemiddel van E-toegang. De advocaat verzoekt via het portaal toegang tot de stukken behorend bij de zaak. Deze stukken beschikbaar stellen in het portaal betreft een communicatie tussen de advocaat en het OM volgens het patroon van vraaggestuurde informatiedeling (zie Interactiepatronen). De gevraagde stukken worden via E-koppeling en E-distributie aangeleverd bij het advocatenportaal. Hierbij wordt voor de advocaat nadrukkelijk zichtbaar gemaakt dat de stukken afkomstig zijn van het OM, zodat voor hem duidelijk is wie verantwoordelijk is voor de kwaliteit. De verstrekking van

de stukken wordt geregistreerd E-compliance zoals het wordt vereist door wetgeving. Indien gewenst kan de advocaat de stukken overbrengen naar de eigen digitale omgeving van zijn kantoor.



Gegevensbescherming

De toekomstige informatievoorziening in de strafrechtketen is toegesneden op wat een organisatie of functionaris (de afnemer) vanuit diens rol in de uitvoering van haar werkzaamheden daadwerkelijk nodig heeft, conform de wettelijke taak en de toepasselijke privacy- en justitiële wetgeving. Dit betekent dat de informatiebehoefte door de afnemer in kaart gebracht is.

Vertrekpunt is hierbij het juridisch kader en het doel waarvoor de informatie nodig is (doelbinding, proportionaliteit, subsidiariteit, transparantie). Binnen de keten worden vervolgens door de leverancier en afnemer afspraken gemaakt en vastgelegd over de toegang tot gegevens. Het is van belang dat de kaders zodanig zijn opgezet dat de privacy van individuen over de keten heen geborgd wordt. Zo is het ontoelaatbaar dat adresgegevens van slachtoffers of getuigen op het bureau belanden van de advocaat van de verdachte.

Informatiebeveiliging

De strafrechtketen bestaat uit partijen die merendeels onderdeel uitmaken van de rijksoverheid en gehouden zijn aan de Baseline Informatiebeveiliging Overheid [BIO]. De BIO onderkent drie basisbeveiligingsniveaus. Voor de uit te wisselen informatie moet helder zijn welk beveiligingsniveau van toepassing is en hoe de gegevens onderweg beveiligd worden. Daartoe worden gegevens gerubriceerd en de classificatie van gegevens is uitgewerkt op ketenniveau. Het is van cruciaal belang dat ook dit laatste punt binnen de strafrechtketen nader wordt ingevuld.

Het belang van informatie in combinatie met wet- en regelgeving vormt de basis voor informatiebeveiliging en bepaalt de geldende beveiligingseisen en de definitie en implementatie van de beveiligingsmaatregelen. Het belang van informatie dient te worden bepaald op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid.

Partners in de Strafrechtketen borgen dat informatie en gegevens in goede handen zijn met gebruikmaking van een veilige opslagvoorziening. Gerubriceerde en privacygevoelige gegevens worden alleen in gesloten omgevingen opgeslagen en bewerkt. Ingevolge de AVG is opslag van dit soort gegevens buiten de EU voor strafrechtketendata niet toegestaan.

Uitzoekpunt: eisen vanuit de WJSG en Wpg. En uitkomsten van het onderzoek naar staatsrechtelijke soevereiniteit.

Voor JenV is er een cloud-afwegingskader [CAJ]. Dit biedt handreikingen voor het afwegen van sourcingsvraagstukken. Daarmee maken organisaties hun eigen afweging, Politie, Rechtspraak en OM doen dat ook op een eigen afwegingskader. Voor de ketenvoorzieningen dient steeds een ketenbrede afweging gemaakt te worden, die recht blijft doen aan de verantwoordelijkheid en autonomie van de betrokken organisaties. Dit is een afweging die op bestuurlijk niveau wordt gemaakt.

Voorts hanteert de strafrechtketen de kaders die voor dit thema worden meegegeven in de NORA en de EA JenV.

Uitzoekpunt: Hoe ketenbreed om te gaan met geclassificeerde informatie.

Bijlage 1: Aandachtspuntenlijst

- Principe: Foutherstel in de keten (staat dat ergens in de implicaties? Digitale Kooi principes)
    - Element voor melden en uitzoeken (keten ombudsman?)
- Relatie andere architecturen: de relatie met Europese initiatieven, kaders en voorzieningen
- Interoperabiliteit: Onderzocht dient te worden of door het gebruik van semantische modelering voor gegevens die in de keten gedeeld worden een grote flexibiliteit en ontkoppeling gerealiseerd kan worden, welke ook transities vereenvoudigt.
- Informatiebeveiliging: Extra veiligheidseisen / security / classificatie
    - Hoe ketenbreed om te gaan met geclassificeerde informatie.
    - eisen vanuit de WJSG en Wpg. En uitkomsten van het onderzoek naar staatsrechtelijke soevereiniteit.
- “Non functionals“
    - Wat te doen als uitwijk? (uitval netwerk, stroom, servicevensters)
    - Noodzaak tot 24 uurs dienstverlening

Bijlage 2: Referenties

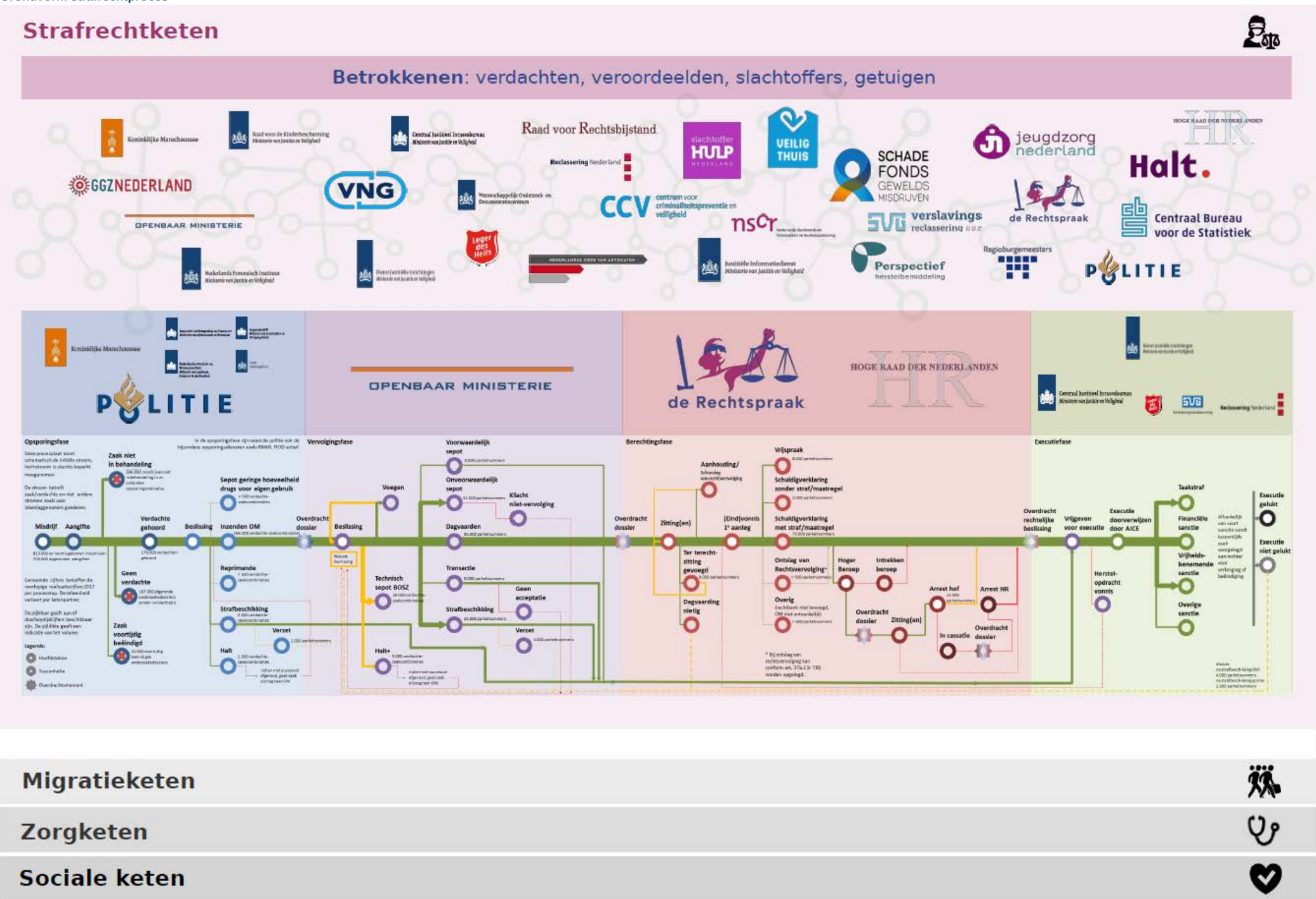
Afk.	Bron	Auteur	Versie / Datum
BIO	Baseline informatiebeveiliging overheid	VNG	Versie 1.04 6 januari 2020
CAJ	Cloudafwegingskader JenV	Ministerie JenV	December 2019
CDPO	Business analyse Complexe dossiers	Politie, OM	
CER	Criminaliteit en rechtshandhaving 2018	WODC Cahier	2019
CMSV	Contourennota Modernisering Wetboek van Strafvordering	Ministerie JenV	2015
DDK	De digitale kooi	Kafka Brigade (A. Witlak)	2018
DSS	Duurzame samenwerking in de strafrechtketen	Ketenpartijen, Ministerie JenV	Oktober 2015
EO	Enterprise Ontology; A Human-Centric Approach to Understanding the Essence of Organisation	J.L.G. Dietz, J.B.F. Mulder	April 2020
ISV	Informatie-uitwisseling in domein overstijgende samenwerkingsverbanden	Ministerie JenV/ DGSenB	Februari 2019
JAR	Jaarplan architectuurraad / Visie op informatievoorziening	SRK-AR	Augustus 2019
JEW	Jegens en wegens	W. Borst	
JMA	Jaarverslag	Matchingsautoriteit	2019
KDB	Ketens de Baas		
KEB	Rapport Knelpunten en breukvlakken in de Strafrechtketen	Ministerie JenV/DGRR/DVB/KIV	Januari 2018
KIBV	Kaderdocument informatiebeveiliging ministerie Justitie en Veiligheid	Ministerie van JenV	Versie 0.41 7 juni 2019
KKB	Keteninformatisering in kort bestek	J.H.A.M. Grijpink	2016, 3e druk
KNP	ABB Knooppunten	SRK AR	April 2020
LPD	Leidende principes digitalisering Strafrechtketen	OGB & BKB	Versie 1.1. Januari 2020
MIM	Metamodel voor Informatiemodellering	Geonovum	25 januari 2020
NDK	Plan van Aanpak 2020	Netwerk Datakwaliteit	2020
PBG	Analyse beslaggoederen	Project Beslaggoederen	2019
PECE	Parlementair onderzoek naar ICT-projecten bij de overheid	Commissie Elias	September 2014
PVS	Privacy van het slachtoffer – feit of fictie?.	Slachtofferhulp Nederland	2020
PVTS	Programmaplan “Verbetering tenuitvoerlegging strafrecht (VTS)	Programma VTS	Januari 2020
RAK	Prestaties in de strafrechtketen	Algemene Rekenkamer	Februari 2012
RGK	Raamwerk Gegevenskwaliteit	Ministerie JenV	2015
RIO	Rapport iOverheid	WRR	15 maart 2011
SRV	Samenwerken aan Recht en Veiligheid	Ministerie JenV	
TKOI	Tweede Kamerbrief Ontwikkeling van de informatievoorziening bij VenJ	Ministerie VenJ. DI&I	December 2016
TSRP	Toekomst van de strafrechtspleging	Commissie van den Emster	
VDA	Visie Digitaal Archiveren	Project Digitaal archiveren	2020
VIK	Verdachte in de Ketens	W. Borst	2019
VIS	Visie IV Strafrechtketen	Min. JenV	2016
W@W	Werk@Wijzer		
WDSK	Werkplan Digitalisering Strafrechtketen	Programma DSK	Februari 2020
WIO	I-Overheid	WRR	2011

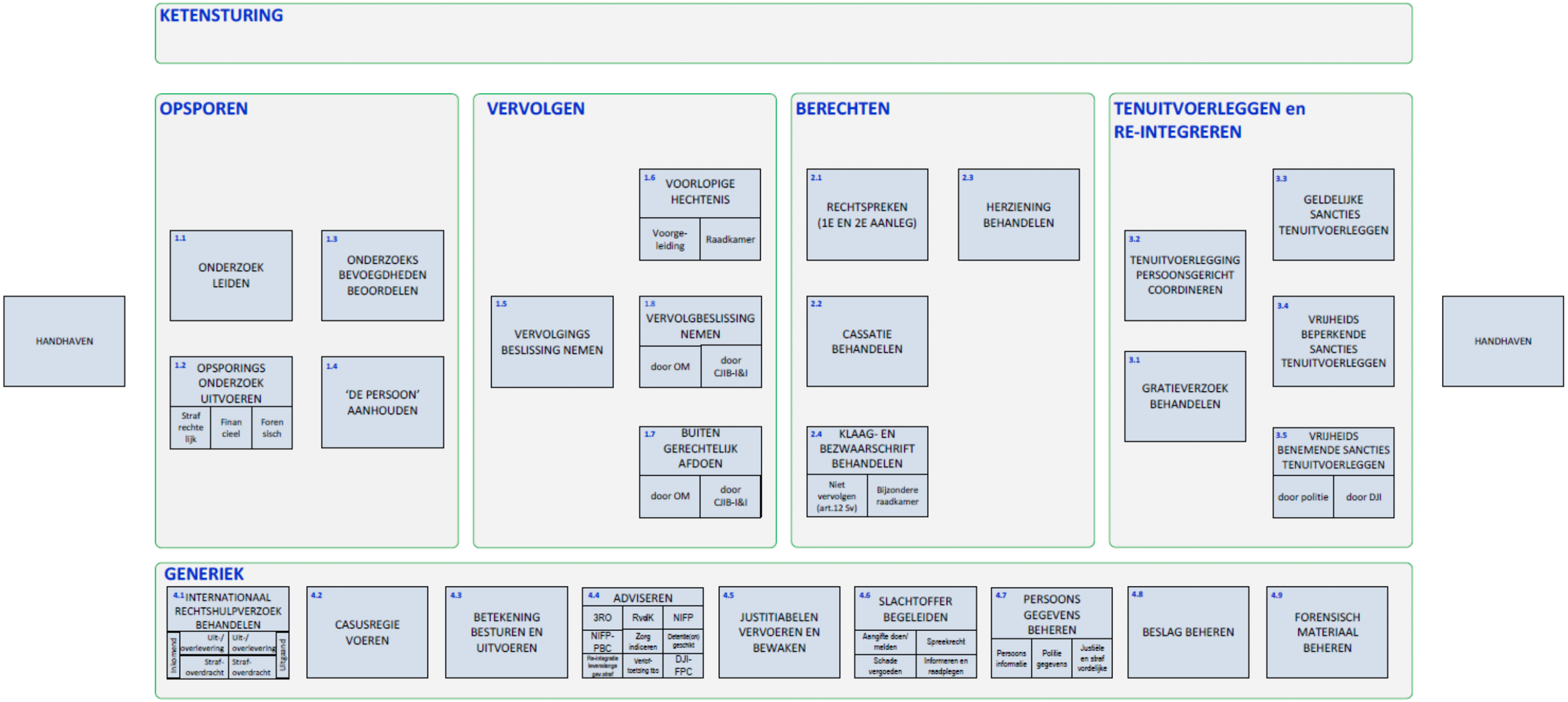
Bijlage 3: SRK bedrijfsfuncties en organisatieverantwoordelijkheden

	Uitgevoerd door:	Politie	KMAR	BOA	CJIB-I&I	CJIB-AICE	ZM (RC)	OM	Rechtspraak	Hoge Raad	Dienst Justis	RvdK	3RO	GI	DJI	DJI-DV&O	DJI-IMA	Centrale Autoriteit	Buitenlandse auto-	IPDK/Post NL	NIFP deskundigen	NIFP/PBC	NIFP-IFZ	Slachtofferhulp	Justid
1.	**Opsporen**																								
1.1	Onderzoek leiden							X																	
1.2	Strafrechtelijk en Financieel opsporings onderzoek uitvoeren	X		X	X																				
1.3	Onderzoeksbevoegdheden beoordelen						X																		
1.4	De persoon aanhouden	X	X																						
1.5	Vervolgingsbeslissing nemen							X																	
1.6	Voorlopige Hechtenis						X	X																	
1.7	Buitenrechtelijk afdoen				X			X																	
1.8	Vervolgbeslissing nemen				X			X																	
2.	**Berechten**																								
2.1	Rechtspreken (1e en 2e aanleg)							X	X																
2.2	Cassatie behandelen									X															
2.3	Herziening behandelen									X															
3.	**Tenuitvoerleggen en re-integreren**																								
3.1	Gratieverzoek behandelen										X														
3.2	Teuitvoerlegging persoongericht coordineren					X																			
3.3	Geldelijke sancties ten uitvoerleggen				X																				
3.4	Vrijheid beperkende sancties ten uitvoerleggen	X										X	X	X											
3.5	Vrijheidsbenemende sancties ten uitvoerleggen	X				X									X										
4.	**Generieke processen**																								
4.1	Internationaal Rechtshulpverzoek behandelen							X	X									X	X						
4.2	Casusregie voeren											X													
4.3	Betekenen	X	X		X	X		X		X	X				X			X		X					
4.4	Adviseren											X	X				X				X	X			
4.5	Justitiabelen vervoeren															X									
4.?	Elektronisch monitoren															X									
4.6	Slachtoffers begeleiden																							X	
4.7	Justitiële en strafvorderlijke gegevens beheren																								X

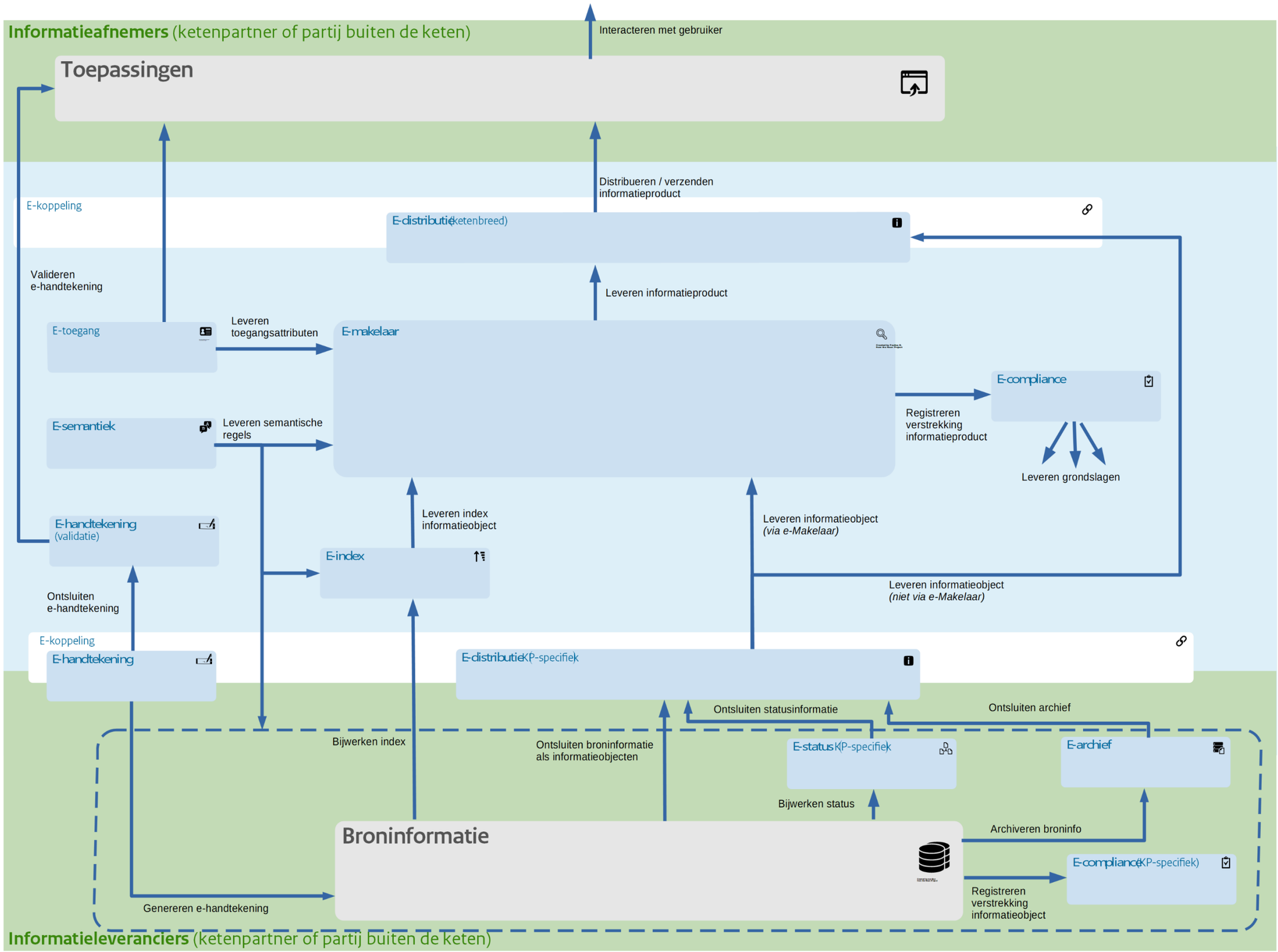
Bijlage 4: A3 formaat platen

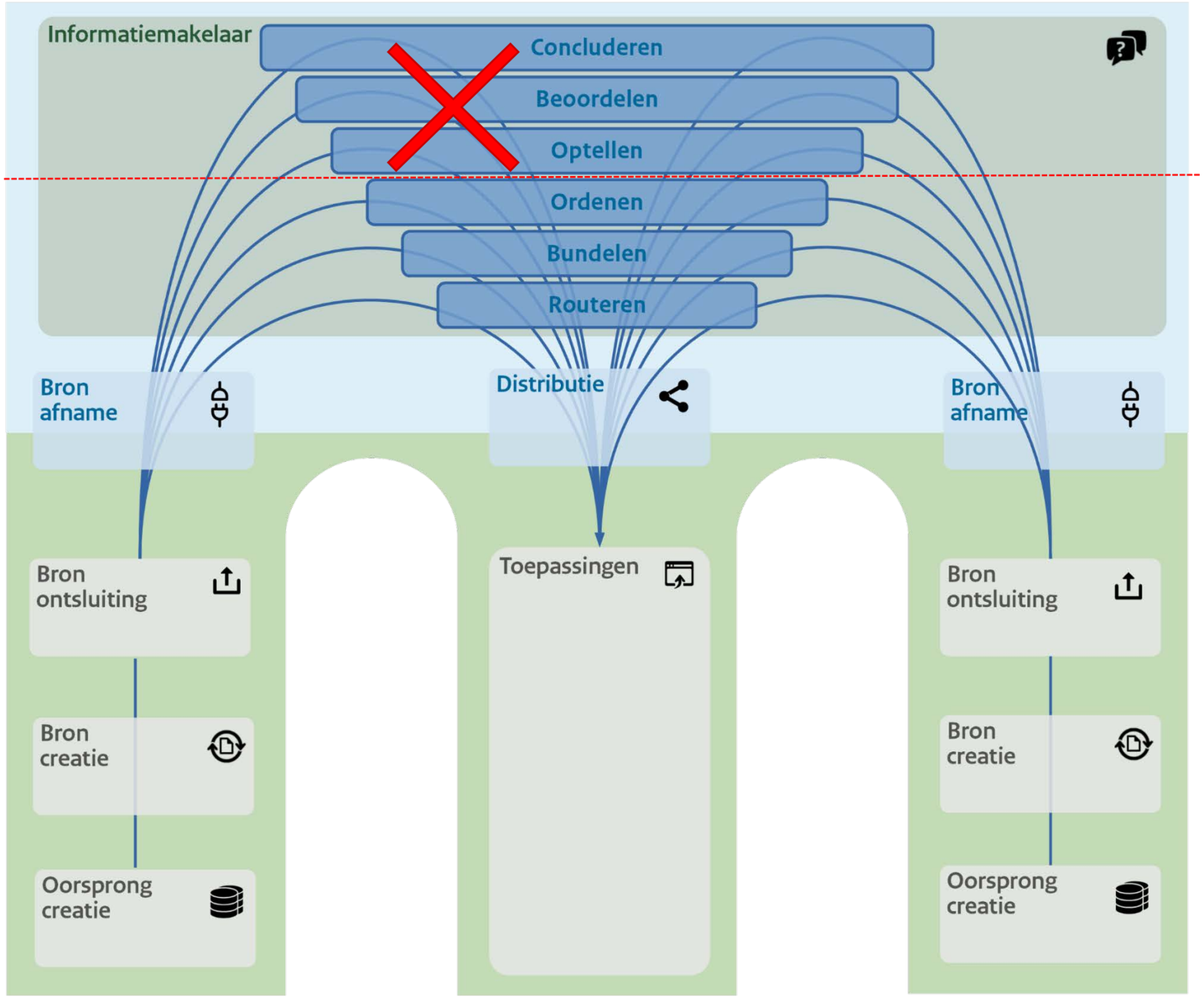
Grondvorm strafrechtproces




KETENSTURING
OPSPOREN
1.1 ONDERZOEK LEIDEN
1.3 ONDERZOEKS BEVOEGDHEDEN BEOORDELEN
HANDHAVEN
1.2 OPSPORINGS ONDERZOEK UITVOEREN
Straf rechte lijk
Finan cieel
Foren sisch
1.4 'DE PERSOON' AANHOUDEN
VERVOLGEN
1.6 VOORLOPIGE HECHTENIS
Voorge-leiding
Raadkamer
1.5 VERVOLGINGS BESLISSING NEMEN
1.8 VERVOLGBESLISSING NEMEN
door OM
door CJIB-I&I
1.7 BUITEN GERECHTELIJK AFDOEN
door OM
door CJIB-I&I
BERECHTEN
2.1 RECHTSPREKEN (1E EN 2E AANLEG)
2.3 HERZIENING BEHANDELEN
2.2 CASSATIE BEHANDELEN
2.4 KLAAG- EN BEZWAARSCHRIFT BEHANDELEN
Niet vervolgen (art.12 Sv)
Bijzondere raadkamer
TENUITVOERLEGGEN en RE-INTEGREREN
3.3 GELDELIJKE SANCTIES TENUITVOERLEGGEN
3.2 TENUITVOERLEGGING PERSOONSGERICHT COORDINEREN
3.4 VRIJHEIDS BEPERKENDE SANCTIES TENUITVOERLEGGEN
HANDHAVEN
3.1 GRATIEVERZOEK BEHANDELEN
3.5 VRIJHEIDS BENEMENDE SANCTIES TENUITVOERLEGGEN
door politie
door DJI
GENERIEK
4.1 INTERNATIONAAL RECHTSHULPVERZOEK BEHANDELEN
Uit-/ overlevering
Uit-/ overlevering
Straf-overdracht
Straf-overdracht
4.2 CASUSREGIE VOEREN
4.3 BETEKENING BESTUREN EN UITVOEREN
4.4 ADVISEREN
3RO
RvdK
NIFP
NIFP-PBC
Zorg indiceren
Detentie(on) geschikt
Re-integratie leverslange gev.straf
Verlof-toetsing tbs
DJI-FPC
4.5 JUSTITIABELEN VERVOEREN EN BEWAKEN
4.6 SLACHTOFFER BEGELEIDEN
Aangifte doen/ melden
Spreekrecht
Schade vergoeden
Informeren en raadplegen
4.7 PERSOONS GEGEVENS BEHEREN
Persoons informatie
Politie gegevens
Justitiële en strafvordelijke
4.8 BESLAG BEHEREN
4.9 FORENSISCH MATERIAAL BEHEREN

Samenhang ketencommunicatievoorzieningen





De figuur hiernaast toont de werking en begrenzing van de makelaarsfunctie.

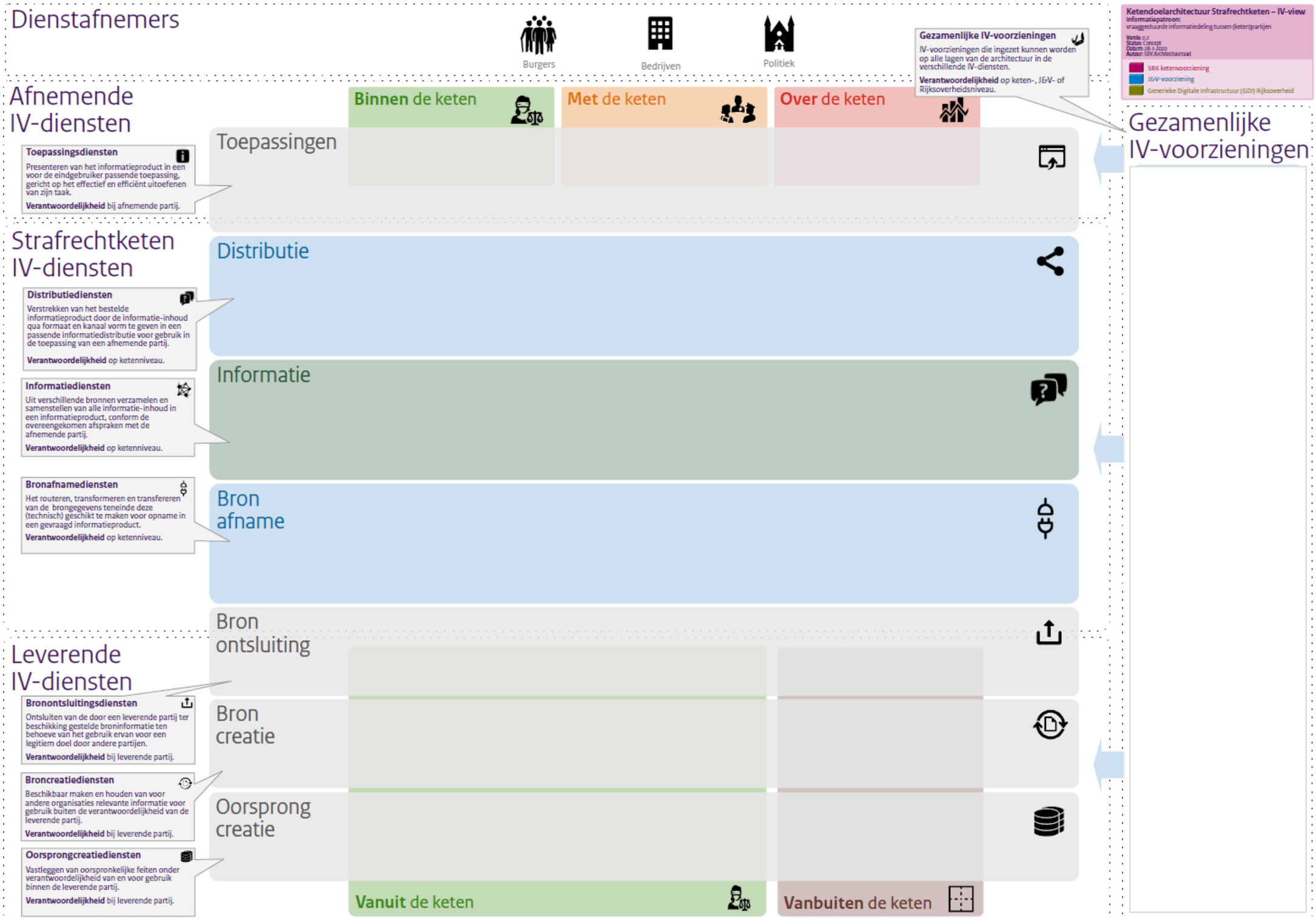
De makelaar brengt gegevens vanuit verschillende bronnen bijeen en stelt deze beschikbaar aan de afnemer. Dit volgens een door gegevensleveranciers en afnemers vastgesteld protocol/recept.

Daarvoor worden gegevens gebundeld, geordend en gerouteerd. De makelaar doet geen inhoudelijke verwerking of interpretatie van de gegevens (optellen, beoordelen en concluderen). Dat is aan de afnemer.

De figuur maakt ook duidelijk dat de makelaar zelf, geen gegevens heeft of bewaard, op de protocollen / recepten na.

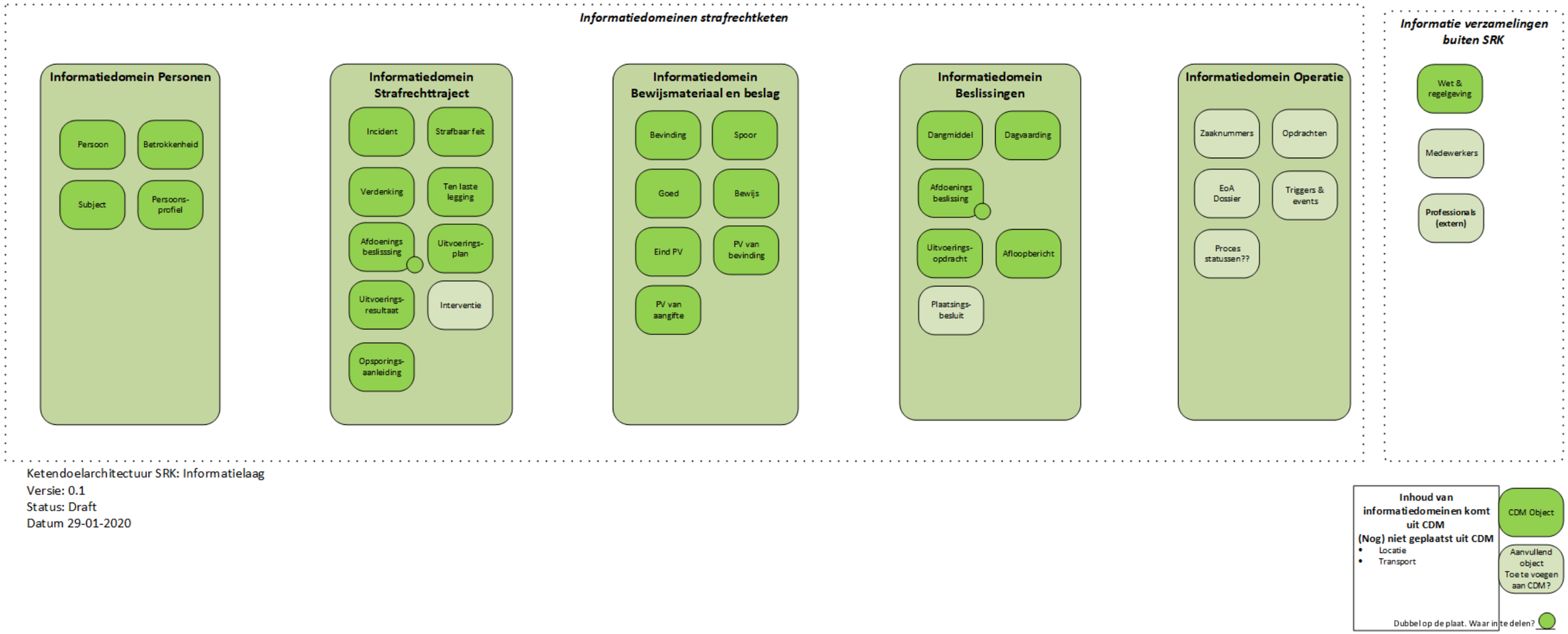
Voor de eenvoud van het figuur zijn autorisatie en compliancy (o.a. verantwoorden verstrekkingen) buiten beschouwing gelaten.

Lagen van IV-diensten



Informatiedomeinen

Indeling van informatiedomeinen aan de hand van de objecten uit het CDM.



Ketendoelarchitectuur SRK: Informatielaag
Versie: 0.1
Status: Draft
Datum 29-01-2020