Technical Sciences
Kampweg 5
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77

TNO-rapport

TNO 2017 R10283

Realisatie van een eOverheid Logistiek - verkenning

Datum	23 februari 2017
Auteur(s)	Wout Hofman, senior research scientist
Aantal pagina's	51
Aantal bijlagen	3
Projectnummer	060.26239

Alle rechten voorbehouden.
Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor opdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.
Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2016 TNO

Inhoudsopgave

Management samenvatting **4**

1 Inleiding **5**
1.1 Probleemstelling 5
1.2 Achtergrond – gesloten (sub)systemen voor interoperabiliteit 5
1.3 Uitgangspunten 6
1.4 Indeling van dit rapport 6

2 eOverheid Logistiek **7**
2.1 Doelstelling 7
2.2 Uitgangspunten, randvoorwaarden en afbakening 9
2.3 eOverheid Logistiek op hoofdlijnen 10
2.3.1 Scheiding in lagen met hun koppelvlakken 10
2.3.2 De drie lagen 12
2.3.3 De koppelvlakken tussen de lagen 13
2.4 Inrichtingsvarianten voor een eOverheid Logistiek 14
2.5 Conclusies 17

3 Inrichtingseisen **19**
3.1 Inrichting 19
3.1.1 Terminologie 19
3.1.2 Gebruik door ondernemingen 19
3.1.3 Gebruik door autoriteiten 20
3.2 Eisen aan een Platform Infrastructuur 20
3.2.1 Eisen aan de Platform Infrastructuur: passieve en actieve inbraak 21
3.2.2 Datakwaliteit 22
3.2.3 Platform Infrastructuur Diensten en – Protocol 23
3.2.4 Data: semantiek, syntax en (open en defacto) standaard(en) 23
3.3 Conclusies 24

4 Digitalisering van vervoersdocumenten **25**
4.1 Functionaliteit van vervoersdocumenten 25
4.2 Elektronische vrachtbrief voor het wegtransport: eCMR 26
4.3 Oplossing voor een autoriteit 28
4.4 Conclusie 28

5 Conclusies en aanbevelingen **30**
5.1 Conclusies 30
5.2 Aanbevelingen 31

Bijlage A – conceptuele interoperabiliteit **33**
A.1 Wat is conceptuele interoperabiliteit? 33
A.1.1. Aanzet tot conceptuele interoperabiliteit 33
A.1.2 Soorten semantische modellen voor logistiek 34
A.1.3 Semantische modellen en hun samenhang 36
A.2 Autoriteiten en ondernemingen - conceptueel 37
A.3 Autoriteiten en ondernemingen - technisch 39
A.4 Conclusies 40

Bijlage B – Platform Infrastructuur raamwerk 41
B.1 Platform Infrastructuur Diensten 41
B.2 Platform Infrastructuur Protocol 42
B.3 Bestaande nodes en hun dienstverlening 43
B.4 Conclusies 46

Bijlage C Invoeringsscenario's 47
C.1 Mogelijke scenario's 47
C.2 Overwegingen voor een keuze 49
C.3 Conclusie en aanbeveling 50

Management samenvatting

ICT, Informatie – en Communicatie Technologie, wordt gezien als drijvende kracht achter vernieuwing. Autonoom opererende productie-eenheden en voertuigen zullen industrie en logistiek verregaand automatiseren. Daarnaast betreden ook nieuwe dienstverleners met nieuwe bedrijfsmodellen de markt. Overheidsinstanties, bedrijfsleven en ook leveranciers van data delingsdiensten zullen moeten anticiperen op deze veranderingen.

Dit rapport is een verkenning naar de rol van de overheid in een dergelijke veranderende logistieke omgeving, waarbij de overheid als aanjager van elektronische integratie van het bedrijfsleven functioneert. Dit is de zogenaamde elektronische overheid voor logistieke oftewel *eOverheid Logistiek*: overheidsinstanties specificeren vanuit wet- en regelgeving bepaalde regels voor logistiek (bijvoorbeeld op het gebied van veiligheid). Voor de handhaving van deze regels is toegang nodig tot data die bedrijven onderling delen. Deze data is toegankelijk via een (virtuele) private data infrastructuur, te vergelijken met het Internet, maar dan op het niveau van data die bedrijven onderling delen.

De eOverheid Logistiek stelt daartoe bepaalde eisen aan deze data infrastructuur en zijn gebruikers rond:

- datakwaliteit (volledigheid, correctheid, eenduidigheid, consistentie);
- functionaliteit van de federatieve opgebouwde infrastructuur die met verschillende technologieën (denk ook aan blockchain technologie) door verschillende leveranciers te realiseren is;
- vertrouwen die infrastructuur, zoals data die alleen toegankelijk is voor degene die geautoriseerd is; en
- de data en hun betekenis waartoe overheidsinstanties toegang wensen voor toezicht en handhaving, waarmee via piggy backing op bedrijfsdata een virtueel Single Window Handel en Transport is te realiseren.

Het bedrijfsleven stelt ook gelijksoortige eisen voor efficiënte inrichting van processen en optimale goederenstromen. De infrastructuur zelf wordt door het bedrijfsleven gerealiseerd, al dan niet met bestaande of nieuwe platformen.

Uitgangspunt voor het realiseren van een eOverheid Logistiek is de mogelijkheid voor de overheid om snel aan te passen aan innovaties in het bedrijfsleven - een adaptieve overheid. Niet alleen gelden er vanuit de overheid eisen aan een private infrastructuur voor data delen tussen bedrijven, maar zullen overheidsinstanties ook een andere ICT inrichting krijgen. In plaats van verzamelen en opslag van data, al dan niet met formele declaraties, monitoren overheidsinstanties een logistiek netwerk via een infrastructuur voor Business-to-Business (B2B) data delen (“piggy-backing”).

Een vernieuwing is tot stand te brengen door de huidige infrastructuur te verrijken, bijvoorbeeld voor eCMR in de EU, en zo snel mogelijk met nieuwkomers afspraken te maken over diensten en protocollen voor deze infrastructuur. De overheid komt daarmee optimaal tegemoet aan keuzes van het bedrijfsleven en stuurt de realisatie van deze keuzes vanuit eisen aan zodat naar verwachting data delen eenvoudiger wordt.

1 Inleiding

1.1 Probleemstelling

Het ministerie van Infrastructuur en Milieu heeft voor het programma Vermindering van Regeldruk TNO gevraagd uitwerking te geven aan elektronische vrachtbrieven voor alle modaliteiten. Aanleiding is het inrichten van een infrastructuur voor een elektronische vrachtbrief in het wegtransport, de eCMR. TNO is gevraagd hiervoor alle mogelijke oplossingen te verkennen en te komen tot een aanbeveling.

Bij de uitwerking dient aansluiting gezocht te worden met andere relevante ontwikkelingen zoals het Single Window Handel en Transport (SWHenT), het iShare project van het Neutraal Logistiek Informatie Platform (NLIP) en het EC DG Move Digital Transport Transport and Logistics Forum (DTLF), waarbij die laatste mogelijk vanuit dit project van input wordt voorzien. Het SWHenT richt zich op de ontwikkeling van een overheidsinfrastructuur dat eenmalig beschikbaar stellen door bedrijven van data en meervoudig gebruik van die data door overheden mogelijk maakt. Het iShare project beoogt een afsprakenstelsel voor Identiteit, Authenticatie en Autorisatie (IAA) in te richten; het DTLF richt zich, naast meervoudig gebruik van data en efficiënte data-uitwisseling, op digitalisering van alle transport begeleidende documenten.

1.2 Achtergrond – gesloten (sub)systemen voor interoperabiliteit

Dit onderzoek neemt de huidige resultaten van DTLF als uitgangspunt (zie de stukken van de plenary meeting van DTLF, juli 2016). Deze geven onder meer aan dat interoperabiliteit in de logistieke toeleveringsketens naar een meer conceptueel niveau moet (‘conceptuele interoperabiliteit’). De huidige manier van implementatie van standaarden resulteert in gesloten oplossingen:

1. Een <u>dominante speler</u> legt zijn implementatierichtlijnen van open standaarden op aan zijn toeleveranciers. Grote supermarktketens, producenten en overheidsorganisaties zijn hiervan voorbeelden.
2. Gemeenschappen <u>(communities)</u> ontwikkelen implementatierichtlijnen van open standaarden. IATA is een voorbeeld voor luchtvracht met aansluiting bij luchthavens en ook voor zeevracht zijn dergelijke standaarden ontstaan, waar havens aansluiting bij hebben gezocht. Rail en binnenvaart hebben alleen standaarden ontwikkeld voor het (optimaal) benutten van de infrastructuur en niet voor transactie ondersteuning.

Dit betekent dat vervoerders en Logistieke Dienstverleners (Logistic Service Providers of LSPs) verschillende implementatierichtlijnen implementeren met daarmee hoge beheerskosten (TCO: Total Cost of Ownership). Doorlooptijden voor implementatie zijn ook te lang (maanden), zodat LSPs en vervoerders alleen in raamwerkcontracten elektronisch data met elkaar kunnen delen. Dit is een drempel voor logistieke vernieuwing gericht op terugdringen van uitstoot door betere benutting van bestaande capaciteit. Logistieke vernieuwing als supply chain agility, supply chain resilience en synchromodaliteit zijn daarmee in de praktijk niet te realiseren.

Het bedrijfsleven alleen is onvoldoende in staat om een open systeem voor (gecontroleerd) delen van data tot stand te brengen. De overheid kan geen

standaarden opleggen voor Business-to-Business (B2B) data delen, aangezien hier geen toezicht- en handhavingstaken voor de overheid aanwezig zijn en daarmee moeilijk om in te richten is. Overheidsinstanties dienen zoveel als mogelijk ISO standaarden (International Standardisation Organisation) te gebruiken, maar conformeren zich aan eigen standaarden zoals die ontwikkelde door de World Customs Organization (WCO). In voorkomende gevallen leggen ze deze op aan het bedrijfsleven en gedragen zich als een dominante speler. Dit kan zover gaan dat ook toepassingen worden geboden die die standaarden ondersteunen, vooral gericht op consumenten (bijvoorbeeld voor belastingaangifte) en MKB (denk bijvoorbeeld aan BICS voor scheepsmeldingen binnen River Information Services). Dergelijke oplossingen die bilaterale communicatie ondersteunen staan vernieuwing van bedrijven in de weg, aangezien IT dienstverleners beperkte mogelijkheden zien voor een rendabele afzetmarkt. Voor consumenten hoeft dit geen probleem te zijn.

1.3 Uitgangspunten

Deze verkenning is gericht op realisatie van conceptuele interoperabiliteit met bestaande platformen en infrastructuren - overheid dan wel bedrijfsleven - en de rol van de overheid in deze realisatie. Enerzijds wordt een vergezicht voor data innovatie bij autoriteiten geboden, anderzijds dient aansluiting bij de huidige invulling van electronische vrachtdocumenten, zoals eCMR en andere verplichte documenten, geboden te worden. Dit rapport adresseert realisatie van eCMR vanuit conceptuele interoperabiliteit met bestaande infrastructuren.

Dit rapport is gericht op de rol van de overheid voor het tot stand komen van conceptuele interoperabiliteit vanuit de noodzaak tot data delen. Financiële instellingen die een noodzaak kennen van zichtbaarheid op goederenstromen vanuit supply chain finance, kunnen een gelijksoortige rol als de overheid spelen om conceptuele interoperabilteit te realiseren. Een voorbeeld is Stichting Focafet met het Universele Economische Transactie Protocol (UETP) en Denars als zogenaamde Registry Node (zie bijlage B) die interoperabiliteit in de logistiek nastreven, zonder echter aan te sturen op conceptuele interoperabiliteit.

1.4 Indeling van dit rapport

De structuur van dit rapport is als volgt

- Hoofdstuk 2 geeft een beschrijving van de oplossingsrichting
- Hoofdstuk 3 detailleert de eisen vanuit de overheid aan de inrichting van een IT infrastructuur voor bedrijven.
- Hoofdstuk 4 werkt de oplossingsrichting uit met eCMR als voorbeeld
- Hoofdstuk 5 geeft conclusies en vervolgstappen

In de verschillende bijlagen worden conceptuele interoperabiliteit (bijlage A), een structuur voor huidige platformen en oplossingen (bijlage B) en een invoeringsscenario voor de voorgestelde oplossing (bijlage C) aangegeven.

2 eOverheid Logistiek

Dit hoofdstuk geeft de voorgestelde oplossing om conform uitgangspunten en randvoorwaarden de doelstelling te realiseren. Daartoe wordt allereerst de doelstelling geformuleerd, vervolgens de uitgangspunten en randvoorwaarden en daarna de inrichting van de overheid voor logistiek, eOverheid Logistiek.

2.1 Doelstelling

Doelstelling bij deze verkenning naar een eOverheid Logistiek is: de overheid stimuleert het tot stand komen van een open systeem voor data delen tussen ondernemingen en de overheden en tussen ondernemingen (B2B) tegen lagere administratieve lasten voor deze ondernemingen en lagere kosten voor de overheid om zijn taken beter uit te voeren met logistieke innovaties door ondernemingen:

- Lagere administratieve lasten impliceert dat ondernemingen geen extra kosten maken om data met overheidsinstanties te delen. Er zal sprake zijn van ‘piggy-backing’ door overheidsinstanties op data die ondernemingen delen.
- Lagere kosten bij de overheid impliceert dat overheidsinstanties met minder mensen en/of middelen toezicht en handhaving kunnen houden op gelijke of groeiende goederenbewegingen.
- Een betere uitvoering van taken door een overheidsinstantie impliceert efficiënter toezicht en handhaving. Dit is op allerlei manieren mogelijk, bijvoorbeeld door een verbeterde risico-analyse met hogere kwaliteit data of een beter overzicht van goederenbewegingen voor handhaving (descriptive en diagnostic analytics).
- De overheid moet kunnen inspelen op logistieke innovaties en nieuwkomers. Denk aan een Tesla of Uber4Freight. Dit wordt in de volgende paragraaf nader toegelicht. Daarnaast zijn er ook logistieke innovaties gericht op vermindering van uitstoot door betere benutting van beschikbare capaciteit. Vanuit IT perspectief zijn dit bundelingstoepassingen gebaseerd op elektronisch data delen.

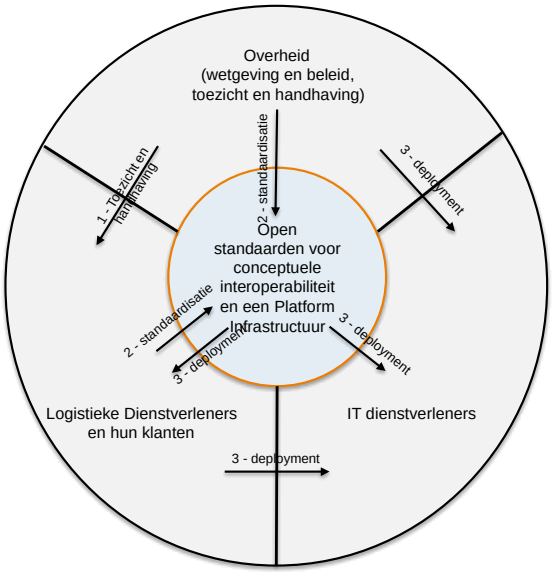
Deze doelstelling is daarmee gericht op een actieve rol van de overheid bij het verminderen van administratieve belemmeringen om digitaal data aan de overheid te rapporteren en het tot stand komen van B2B data delen, zonder aanvullend toezicht en handhaving door die overheid op de inrichting daarvan. Wel zal de overheid eisen stellen aan die inrichting (zie het volgende hoofdstuk). Realisatie van deze doelstelling impliceert ook een andere inrichting bij de overheid. Dit wordt op de navolgende pagina’s vanuit een IT perspectief nader uitgewerkt, maar er zijn ook andere aspecten van belang (b.v. mensen, organisatie, financiën).

Het bedrijfsleven heeft een noodzaak voor een open systeem om te voldoen aan doelstellingen vanuit (inter-)nationale overheden, bijvoorbeeld vermindering van uitstoot. Multi-modaal transport, dynamische keteninrichting, synchromodaliteit en bundling dragen bij aan betere benutting van capaciteit en geven daarmee vermindering van uitstoot. Schattingen over het besparingspotentieel zijn al in diverse onderzoeken gedaan. Elektronisch data delen, toegang tot data en innovatieve IT oplossingen zijn hiervoor een randvoorwaarde volgens de kenmerken van de logistieke sector zoals grote aantal MKB ondernemingen,

beperkte IT kennis, verouderde (legacy) IT oplossingen, lage marges en beperkte investeringsmogelijkheden in nieuwe IT oplossingen (zie onderzoeken naar IT binnen de logistieke sector).

Realisatie van deze doelstelling is een proces dat bestaat uit de volgende stappen (zie ook de volgende figuur):

1. Data gedreven innovatie van toezicht en handhaving. Hieruit vloeit voort dat overheidsinstanties van een dominante speler die voorschrijft hoe data aangeleverd moet worden, transformeert naar een organisatie die vanuit zijn taakstelling data van het bedrijfsleven gebruikt en daarbij wel condities stelt in de vorm van bijvoorbeeld volledigheid, etc. (Hoofdstuk 3).
2. Ontwikkeling van open standaarden voor conceptuele interoperabiliteit en een (federatieve) Platform Infrastructuur in samenspraak met het bedrijfsleven, conform eerdere kenmerken van de logistieke sector.
3. Zorgdragen voor implementatie van ontwikkelde standaarden in producten en diensten van IT dienstverleners.



Standaardisatie van een open omgeving voor het elektronisch delen van data in B2B lijkt vanuit het bedrijfsleven, noch vanuit de IT dienstverleners tot stand te komen. Mogelijkerwijs zijn er nieuwkomers (bijlage C – nieuwkomerscenario) die andere oplossingen aanbieden; deze zullen in samenspraak met deze nieuwkomers doorontwikkeld kunnen worden.

Belastingdienst/Douane experimenteert binnen het EU FP7 SEC CORE project met deze benadering - open omgeving voor het elektronisch delen van data - door een minimale set van (open defacto) standaarden af te stemmen met het bedrijfsleven en geen structuur en semantiek voor te schrijven voor transactiedata. Vooralsnog lijkt dit nog onvoldoende bij te kunnen dragen aan conceptuele interoperabiliteit voor B2B toepassingen (zie ook bijlage A, waar conceptuele interoperabiliteit verder uitgewerkt wordt) omdat veelal gesloten systemen worden ontwikkeld, hetzij vanuit een dominante partij hetzij door een community zoals voor lucht- en zeevracht met (luch)havens. Het resultaat is dat logistieke dienstverleners bilaterale koppelingen realiseren tegen relatief hoge kosten. Platformen bieden oplossingen (zie bijlage B),

maar vooral het Midden- en Klein Bedrijf (MKB) heeft onvoldoende kennis en investeringskracht om te participeren in verschillende omgevingen.

Het voorstel om de overheid aanjager te laten zijn voor vernieuwing in het bedrijfsleven of gebruik te maken van faciliteiten van het bedrijfsleven is ook in andere sectoren al zichtbaar. Denk bijvoorbeeld aan de verplichting voor het installeren van een slimme meter om het energienet 'slimmer' te maken of het gebruik van identiteit en authenticatie van financiële instellingen te gebruiken voor overheidstoepassingen.

2.2 Uitgangspunten, randvoorwaarden en afbakening

De volgende uitgangspunten gelden voor de uitwerking:

- Adaptieve overheid. Er wordt gestreefd naar een adaptieve overheid die snel reageert op veranderende omstandigheden en om kan gaan met verschillende technologische ontwikkelingen. Dergelijke veranderingen kunnen ook van toepassing zijn op arbeidsomstandigheden en –verhoudingen, waarbij uitvoerenden worden aangestuurd door tweezijdige platformen en moeten voldoen aan hun eisen. Zij worden daarmee een soort zelfstandigen zonder personeel die moeten voldoen aan kwaliteitseisen van deze platformen. Veranderingen zijn bijvoorbeeld:
    - De snelle groei van eCommerce en daarmee de toename van pakketjes geeft nieuwe vormen van toezicht met beschikbare menskracht. In feite is dit een andere inrichting van verkoop – en distributiekanalen door ondernemingen naar consumenten met fijnmazige distributie. Denk ook distributie van maaltijden.
    - Verandering in technologie door de invoering van gedistribueerde toepassingen gebaseerd op block chain (-achtige) databases. Data is gedecentraliseerd. Nieuwe technologie moet mogelijk zijn en ook nieuwe diensten moeten door nieuwkomers geëxploiteerd kunnen worden.
    - Vernieuwing van bedrijfsmodellen of intrede van nieuwkomers zoals tweezijdige platformen als Uber4Freight, Tesla voor autonoom vervoer en Amazon voor het bieden van een (fijnmazig) distributienetwerk.
- Keuzevrijheid van ondernemers.
    - Er zijn community systemen (b.v. Portbase en Cargonaut), commerciële Integration Service Providers (ISPs als Descartes), boekingsplatformen (INNTRA), non-repudiation oplossingen (b.v. TransFollow), visibility platformen (Descartes, Shipping Information Pipeline), logistieke marktplaatsen (LogisticsMarketPlace) en andere vormen van platformen en/of technologische oplossingen zijn (zie bijlage B).
    - Er zullen altijd ondernemingen zijn die hun eigen IT systemen en oplossingen gebruiken, al dan niet met Commercial Of The Shelve (COTS) software zoals een Transport Management Systeem (TMS).
    - Innovaties voor het bedrijfsleven komen uit nieuwe technologie, zowel voor het delen van data als ook autonoom opererende objecten (voertuigen, kranen, etc.) die een databehoefte hebben en gevolgen hebben voor ondernemingen (denk ook aan de sociale

impact). Deze innovaties zullen gevolgen hebben voor de bestaande logistieke bedrijven en hebben andere behoeften voor het delen van data.

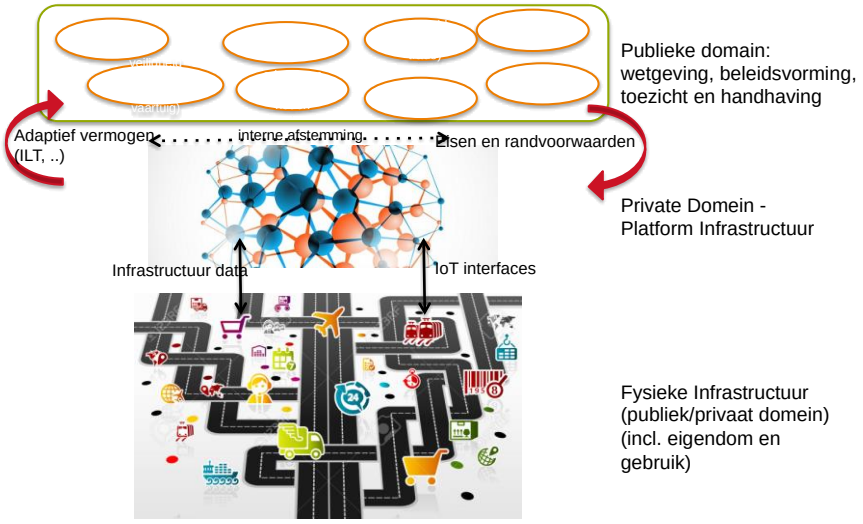
Een afsprakenstelsel voor toezicht en handhaving dient in bestaande wetgeving inpasbaar te zijn.

De voorgestelde afbakening is (in deze versie) toezicht en handhavingstaken voor logistieke activiteiten. Het gaat dan om goederenbewegingen en –opslag in de meest ruime zin, inclusief de inzet van mensen en/of middelen (denk hier ook bij belastingaanslag voor autonome opererende middelen ('robots' zoals autonome voertuigen) in het gebied waar ze hun activiteiten verrichten). Cross-docking en tijdelijke opslag vallen hier ook onder. Toezicht kan vanuit verschillende perspectieven zoals veiligheid bij opslag van gevaarlijke lading. (Complexe) bewerkingen van goederen vallen nu buiten de scope, maar moeten vanuit belastingsperspectief wel meegenomen worden (denk aan in- of uitvoerbelastingen bij verandering van waarde en beperkingen op heruitvoer van componenten in een product).

2.3 eOverheid Logistiek op hoofdlijnen

2.3.1 Scheiding in lagen met hun koppelvlakken

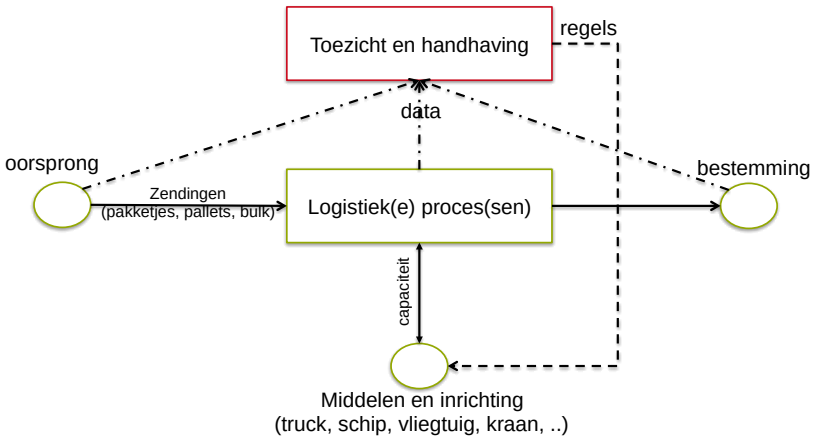
Een eOverheid Logistiek op hoofdlijnen is in te delen naar drie aspecten die we 'lagen' zullen noemen. Het zijn in wezen verschillende domeinen met hun verantwoordelijkheden en autonomie, waarbij in de fysieke infrastructuur de scheiding tussen publiek en privaat diffuus is. Denk aan overheidspartijen als Rijkswaterstaat of ProRail die verantwoordelijk zijn over de publieke infrastructuur om deze aan te bieden voor optimale doorstroming met private en publieke vervoermiddelen, waarbij de publieke infrastructuur aan kan sluiten op een private infrastructuur in bijvoorbeeld de haven van Rotterdam. Deze lagen hebben onderling hun koppelvlakken voor het delen van data (figuur). Deze drie lagen en hun koppelvlakken worden hierna toegelicht.



Figuur – drie lagen met hun koppelvlakken

De achterliggende gedachte van deze drie lagen is gelijk aan die van een voorraadbeheerssysteem van een warehouse: de Platform Infrastructuur in het private domein bevat een weergave van de fysieke werkelijkheid waarop een overheidsinstantie vanuit zijn taken toezicht op moet houden of delen van deze werkelijkheid onder zijn beheer heeft. In deze analogie stelt een overheidsinstantie bijvoorbeeld eisen aan de inrichting van het warehouse (de infrastructuur), maar moet die overheidsinstantie ook toezicht houden op de goederen die in opslag liggen en in en uit worden geslagen door ondernemingen (data). Door net als in een warehouse in toenemende mate de fysieke werkelijkheid te voorzien van sensoren en robots, zal in de logistieke omgeving de kwaliteit van de weergave van die werkelijkheid in een Platform Infrastructuur toenemen (kwaliteit is hier uitgedrukt als volledig, consistent en juist, zie het volgende hoofdstuk).

Een abstract gezichtspunt voor toezicht en handhaving is enerzijds het stellen van regels aan het gebruik van middelen (vrachtwagens, schepen, etc.) en inrichting van systemen vanuit bijvoorbeeld het gezichtspunt van veiligheid en anderzijds het daadwerkelijk krijgen van data over zendingen en de uitvoering van processen. Bij dit laatste horen ook de betrokken bedrijven; deze bedrijven zijn niet in de volgende figuur getoond.



Figuur – abstractie van toezicht en handhaving

De vorige figuur is een abstractie voor processen (vierkantje) en lokaties (rondjes). Lokaties zijn niet alleen voor zendingen met hun oorsprong en bestemming, maar ook voor transportmiddelen en fysieke overslag- en opslaglokaties. Ook transportmiddelen zullen na gebruik op een lokatie zijn; vrachtwagens hebben bijvoorbeeld een vaste lokatie van waaruit ritten plaatsvinden, containers zijn in depots opgeslagen, etc.

Vanuit deze abstractie is een analogie naar auditing te maken. Auditing is, kort gezegd, controle op de correcte afhandeling van inkomende en uitgaande goederenstromen in een organisatie, gekoppeld aan financiële stromen en met eisen voor de inrichting van die organisatie. Over organisaties heen stelt auditing geen regels, omdat een auditor gericht is op één organisatie. Een toezichthouder kan wel kwaliteitseisen stellen over de afhandeling van goederen- en geldstromen over meerdere organisaties heen, bijvoorbeeld dat uitgaande goederenstromen bij één organisatie identiek moeten zijn aan inkomende goederenstromen bij één of meer andere organisaties. De regel is dan dat er alleen goederen verloren gaan (denk aan ongelukken of diefstal) of bij komen gedurende transport als dit expliciet

door betrokken logistieke ondernemingen wordt aangegeven. Dit en andere regels zijn te controleren via een Platform Infrastructuur waar gegevensuitwisseling over goederen en geld plaatsvindt. Deze aanpak zal alleen werken bij volledige elektronische gegevensuitwisseling tussen ondernemingen: iedereen moet meedoen. Er zullen altijd regels zijn waar een individueel onderneming verantwoordelijk voor is, bijvoorbeeld regels voor de toestand van een transportmiddel tijdens zijn inzet op de publieke, fysieke infrastructuur. Daarmee dienen ondernemingen ook interne data toegankelijk te maken voor overheidsinstanties.
De regels vormen de eisen en randvoorwaarden waaraan het bedrijfsleven moet voldoen.

De voorgestelde werkwijze is dat de overheid (1) regels in gestructureerde, digitale vorm beschikbaar stelt waaraan logistieke ondernemingen moeten voldoen en (2) toegang tot data in of via de Platform Infrastructuur vraagt vanuit het oogpunt van toezicht en handhaving van die regels. Dit stelt verschillende eisen aan de Platform Infrastructuur.

2.3.2 De drie lagen

De volgende drie lagen worden onderscheiden

- Publiek domein - wetgeving, beleidsvorming, toezicht en handhaving. De Europese Commissie (EC) ontwikkelt in nauwe afstemming met nationale overheden van de EU Lidstaten wetten, waarbij elke Lidstaat zijn eigen implementatierichtlijnen van die wetten heeft. Het betreft bijvoorbeeld veiligheid van handelsstromen en van voer- en vaartuigen.
  Toezichthouders en handhavers zien toe op naleving van deze wetten, waarbij het bedrijfsleven de nodige data moet aanleveren (b.v. aangifte voor inkomende lading) of handhavers toegang tot data kunnen vragen (bijvoorbeeld inzage in vrachtdocumenten). Douane, ILT, Havenbedrijf Rotterdam en politie zijn voorbeelden van dergelijke overheidspartijen.
- Privaat domein - Platform Infrastructuur. Dit is de verzameling van IT systemen en diensten voor het delen en uitwisselen van data tussen logistieke bedrijven (B2B – Business-to-Business), zie bijlage B. Hier zijn verschillende leveranciers actief.
- Fysieke Infrastructuur (publiek en privaat domein). Hier zijn alle fysieke middelen, goederen en fysieke infrastructuur. Veel van de vervoermiddelen beschikken al over identificaties (AIS voor schepen en binnenvaartschepen en On Board Units (OBUs) voor vrachtwagens). Met de komst van geavanceerde communicatienetwerken en lagere communicatiekosten (LoRa en 5G) zal naar verwachting de toepassing van sensoren toenemen en wordt het Internet of Things voor logistiek gerealiseerd. Leveranciers van sensoren bieden veelal geen kosten voor sensoren, maar voor data afname.
  Beheer en onderhoud van de fysieke infrastructuur is veelal bij een publieke organisatie als Rijkswaterstaat (RWS – (vaar)wegen) of ProRail (spoor) belegd, maar kan ook in het private domein zijn. Denk bij het laatste aan de haventerreinen of distributielokaties, maar ook private rail infrastructuur beheerders.

Daarnaast zal de fysieke infrastructuur steeds meer IT verwerkingscapaciteit krijgen ('ubiquitous computing'). Onderdelen van de infrastructuur hebben verwerkingscapaciteit en ondersteunen nieuwe toepassingen van derden (onder

voorwaarden). Voorbeelden zijn Tesla en BMW die auto's als met een Operating Systeem aanbieden, inclusief een appstore voor downloaden en installeren van nieuwe toepassingen. Deze rijdende 'computers' hebben direct verbinding met de fysieke omgeving via sensoren/actuatoren en zijn dus programmeerbare platformen. Ze zijn aanwezig in de publieke, fysieke infrastructuur, maar zijn private platformen die zich moeten houden aan publieke regels. Ook overheden kunnen programmatuur voor deze platformen ontwikkelen.

2.3.3 De koppelvlakken tussen de lagen

Elke laag heeft koppelvlakken met een andere laag, terwijl ook binnen lagen data onderling gedeeld kan worden. De volgende koppelvlakken worden onderkend:

1. <u>Sensor (IoT – Internet of Things) data</u>: dit betreft data over de fysieke lokatie van een object op een bepaald tijdstip, de fysieke toestand van een object (temperatuur, gewicht, gas, etc.), het aanbrengen of verbreken van relaties tussen objecten (b.v. laden van een container op een schip) en openen van deuren (b.v. van een container of een vrachtwagen), maar ook het meten van doorstroming van vervoermiddelen of het detecteren van uitstoot. Het gaat hier over sensoren/actuatoren met een relatief beperkte rekenkracht.
   Naarmate de prijs van sensoren zakt en de mogelijkheden van communicatie met de komst van LoRa en 5G verbeteren, is de verwachting dat sensoren meer gebruikt gaan worden. Het is dan mogelijk elk pakketje en pallet te voorzien van een sensor die gescand wordt als dat pakketje in een container wordt gepakt, waarmee automatisch een stuffing lijst van die container wordt opgemaakt.
   Veelal zullen leveranciers van sensoren data platformen bieden voor IoT data met alleen kosten voor data afname. Objecten genereren streaming data. Er zijn al diverse commerciële dienstverleners voor IoT data in de logistiek. Het interface naar leveranciers van deze data moet voldoen aan een standaard om deze eenvoudig door bedrijven te laten verwerken, waarbij bedrijven mogelijk niet de volledige streaming data willen.
2. <u>Infrastructuur data</u>: alle data uit en naar de infrastructuur die van belang is om het gebruik van die infrastructuur beter te benutten en vervoer te optimaliseren. Dit betreft publieke data als (niet uitputtend):
   a. Gepland onderhoud van de infrastructuur, omleidingen
   b. Ongelukken, vertragingen
   c. Fileinformatie en – voorspellingen
   d. Specifieke kenmerken van de infrastructuur. Denk hier ook aan diepte van vaarwegen, getijdebewegingen, vaargeul, beperkingen voor tunnels en viaducten, etc. Kenmerken als diepte van een vaarweg zijn afhankelijk van andere kenmerken als wind, smeltwater, etc.

   Een overweging voor beter benutten van de infrastructuur is het kenbaar maken van bestemmingslokatie en – tijdstip van een transportmiddel aan die infrastructuur. Voor wegtransport is dit veelal een private functie; voor spoor en binnenvaart is dit mogelijk anders in te richten op het grensvlak van publiek/privaat (d.w.z. een onderneming kan een door de infrastructuur afgegeven Estimated Time of Arrival (ETA) ook beschikbaar maken voor zijn klant en/of terminal bij bestemming).
3. <u>Private (bedrijfs-)data</u>: dit is alle data die bedrijven onderling uitwisselen voor het uitvoeren en synchroniseren van logistieke processen en alle data

die door commerciële dienstverleners wordt aangeboden en bruikbaar is voor logistieke toepassingen.
Data die bedrijven uitwisselen wordt als volgt gegroepeerd:

a. logistieke diensten ('timetables', 'voyages') en beschikbare capaciteit,
b. transactiedata (boekingen, orders),
c. visibility data, mogelijk gebaseerd op IoT data ((snelheid en richting van verplaatsing,) locatie en tijd van objecten en/of ETA),
d. financiële data (facturatie en betaling).

Standaardisatie voor de elektronische uitwisseling van deze data is in principe aan het bedrijfsleven, maar als overheidsinstanties deze data kunnen gebruiken voor de invulling van hun taken, dan kan de overheid de semantiek van deze data (mee)bepalen en mogelijkerwijs opleggen.
Commerciële data voor optimalisatie van logistieke processen is bijvoorbeeld (niet uitputtend, ook publieke data als KvK inschrijving kan hier van toepassing zijn):

a. Betalingsgedrag, kredietwaardigheid en prestatie indicatoren van ondernemingen.
b. Weersvoorspellingen (mogelijk kan dit ook publieke data zijn).
c. Verwachte vertragingen in reistijd. Dit is een vorm van file informatie gebaseerd op historische data met weersvoorspelling en reistijden tot het punt waar een vertraging wordt voorspeld.
d. (natuur)rampen, opstanden, oorlogsgebieden.
e. Stakingen, blokkades, etc., veelal afleidbaar uit bijvoorbeeld social media en nieuwswebsites.

Het is de vraag of het mogelijk en nodig is bovenstaande commerciële data te standaardiseren. Er dient vooral een vorm van afbeelding van deze data op logistieke stromen met een risico-analyse plaats te vinden.

4. Overheidsdata: de regels om te voldoen aan wet- en regelgeving en de benodigde data voor toezicht van die wet- en regelgeving. Afhankelijk van de inrichting van systemen en processen bij de overheid kunnen zij onderling ook data met elkaar delen (denk aan coordinated border management).

2.4 Inrichtingsvarianten voor een eOverheid Logistiek

Een overheidsinstantie of de overheid heeft nu de volgende keuzes rond de inrichting van deze drie lagen:

- Systemen in het publieke domein. Dit is de huidige situatie. Elk van de toezichthouders en handhavende instanties heeft zijn eigen systemen met dataopslag en –archivering, ingericht conform de uitgangspunten die de overheid hiervoor heeft geformuleerd. Deze systemen bevatten een weergave van de fysieke werkelijkheid. Zij putten hun data uit de Platform Infrastructuur en verzamelen IoT data waar dit geëist of gewenst is. Risico-analyses worden op de data verzameld in de eigen systemen uitgevoerd. Overheidsinstanties definiëren semantiek en syntax voor benodigde data, bijvoorbeeld door het World Customs Organization (WCO) data model te gebruiken of een Europese afgeleide als het EC Customs Data Model (EC CDM). Er zijn nu ook voor verschillende toezichthoudende taken verschillende oplossingen, binnenvaart kent bijvoorbeeld andere specificaties voor toezicht op gevaarlijke ladingstromen dan wegtransport.

Deze specificaties zijn verder te harmoniseren als dit voordelen voor de overheid en het bedrijfsleven op kan leveren. Voor aanlevering zijn er twee oplossingen:

- Het bedrijfsleven zorgt dat elk van de overheidssystemen zijn juiste data krijgt. Dit kan via een push (berichten) of pull (toegang tot de data) mechanisme. Voor elk van de systemen implementeert een bedrijf een berichtstructuur of toegangscontrole.
- Het bedrijfsleven levert eenmalig data of ontsluit deze voor de gehele overheid (eenmalig aanleveren, meermalig gebruik). De overheid heeft een Single Window (push) om de juiste data op het juiste tijdstip naar de juiste instanties te verdelen en onderlinge processen op elkaar af te stemmen (b.v. coordinated border management).

- Toegang tot bedrijfsdata. Elke overheidsinstantie die vanuit zijn taken bepaalde data nodig heeft, heeft toegang tot deze data bij ondernemingen via de Platform Infrastructuur. Hiermee ontstaat een virtueel Single Window Handel en Transport. Risico-analyse vormt de kern van de IT systemen van een overheidsinstantie voor toezicht. Een overheidsinstantie kan met het resultaat van risico-analyse over gaan tot inspectie en handhaving of bij geconstateerde overtredingen direct sancties opleggen (binnen bestaande wet- en regelgeving). Een overheidsinstantie dient zich eenduidig te identificeren om toegang tot data te krijgen. Zodra de data is geanalyseerd en geen risico's zijn gedetecteerd, kan de data in principe verwijderd worden uit het overheidsdomein.
  Ook nu moet de data een structuur (syntax) en te herleiden zijn tot informatie (semantiek). Afhankelijk van wetgeving en daarbij horende risico-analyse is door bedrijven onderling uitgewisselde data voldoende. Mogelijk moet een aparte codering (HS- of Harmonized Systems code) gehanteerd worden voor financiële afhandeling om uniformiteit in belastingafdracht te verkrijgen (import- en exportstromen), maar vanuit andere toezichtperspectieven is dit niet nodig.
  Er zijn verschillende technieken om data te verzamelen, bijvoorbeeld:
  - Automatisch verzamelen ('crawling'): op regelmatige tijdstippen wordt data bij elk bekend bedrijf opgehaald. Bedrijven stellen data via een server beschikbaar. Om onnodige belasting van deze server te voorkomen, zou er één overheidscrawler ingericht kunnen worden.
  - Application Programming Interface (API): elk bedrijf heeft APIs om data beschikbaar te stellen aan overheidsinstanties. De overheid roept op regelmatige tijdstippen deze APIs aan.
  - Informeren dat nieuwe data beschikbaar is ('events'). Een bedrijf informeert de overheid over nieuwe zendingen en goederenbewegingen. Deze events hebben identificaties om verdere data op te vragen via een API. Overheidsinstanties kunnen zelf ook events beschikbaar stellen en deze ook onderling delen voor het realiseren van bijvoorbeeld coordinated border management, mogelijk via de private infrastructuur van het bedrijfsleven.
- Systemen op platformen in het private domein. Overheidsorganisaties ontwikkelen toepassingen die aanwezig zijn op platformen in het private domein. Denk bijvoorbeeld het on-board installeren van

overheidstoepassingen op platformen in voertuigen. Deze systemen monitoren de toestand en het gedrag van een voertuig, personen op/in dat voertuig en lading om te voldoen aan wet- en regelgeving. Een voorbeeld is het installeren van een component op een vrachtwagen die aangeeft dat de lading voldoet aan wet- en regelgeving gebaseerd op de daadwerkelijke gegevens van die lading (oorsprong, bestemming, inhoud), zonder die gegevens beschikbaar te maken aan een overheidsinstantie, en rekening houdt met de omgeving (b.v. het feit dat twee schepen met gevaarlijke lading elkaar op een minimale afstand mogen passeren en een schip altijd een bepaalde hoeveelheid water onder de kiel moet hebben). Dit zijn zogenaamde compliance 'apps' die in een voertuig (of ander object) aanwezig zijn. Invoering van sensoren met toenemende rekencapaciteit (zie het eerder genoemde ubiquitous computing) maakt dit mogelijk. Het is dan voldoende voor een overheidsorganisatie om alleen te monitoren of deze compliance apps functioneren en of zij geen onregelmatigheden constateren. De compliance apps moeten niet te wijzigen zijn door anderen dan de bevoegde overheidsinstanties. Een dergelijke compliance app zou op het Tesla platform kunnen draaien om snelheidsovertredingen te signaleren (denk ook aan apps als Flitsmeister die mensen nu al gebruiken op hun smart phone, maar dan in de auto met een koppeling naar de bevoegde instantie die trajectcontrole overbodig maken; een autofabrikant kan ook snelheidsbeperkers inbouwen conform maximaal geldende snelheden, maar zal dit veelal niet doen).

Verzamelen van data door toegang kan altijd identificaties opleveren die gebruikt kunnen worden om nieuwe data op te halen, mogelijk bij een ander bedrijf dan het bedrijf dat de data aanbood ('Linked Data').

Een overgangssituatie wordt gekenmerkt door een combinatie van eigen systemen en toegang tot bedrijfsdata. Dit impliceert dat een risico assessment systeem toegang tot twee soorten data heeft: interne en externe data. Daarop moeten deze systemen ingericht worden. De volgende tabel geeft een afweging van de voor- en nadelen van de verschillende inrichtingsvarianten.

Tabel – Overzicht van inrichtingsvarianten eOverheid Logistiek

Varianten	Voordelen	Nadelen
1. Systemen in het publieke domein	Data in eigen beheer Autonomie voor uitvoeren van taken en inrichten processen	Afwijkingen met de data van bedrijven Databeheer Hoge TCO van systemen Hogere kosten door opslag historische data (archiefwet) Onderlinge afstemming bij Single Window Voldoet niet aan de doelstelling in dit rapport
2. Toegang tot bedrijfsdata	Hogere kwaliteit van data voor de overheid Lagere TCO door eenvoud van systemen Voldoet aan de doelstelling in dit	Alle bedrijven moeten elektronisch data delen om volledig zicht te hebben. Alle bedrijven moeten toegang autoriseren

Varianten	Voordelen	Nadelen
	rapport Lagere administratieve lasten voor het bedrijfsleven Adaptieve overheid	Nieuwe concepten, nieuwe systemen, impact op wetgeving? Complexiteit in afleiden regels
3.Overheidssystemen op platformen in het private domein	Eenvoud, lage kosten Gebruik appstore mechanismen Alleen monitoring Voldoet aan de doelstelling in dit rapport Lagere administratieve lasten voor het bedrijfsleven Adaptieve overheid	Afhankelijk van voortgang ontwikkeling autonome objecten. Voor de (nabije) toekomst. Eerste experimenten in experimentele omgevingen (universiteiten).

De eerste optie is de huidige situatie. Dit draag niet bij de doelstelling zoals dit in het begin van dit hoofdstuk is vermeld, te weten het stimuleren van interoperabiliteit in het bedrijfsleven. Alleen de tweede en derde optie dragen bij aan de doelstelling.

In de tweede optie, toegang tot data, vormt effectieve handhaving met IT systemen die zichtbaarheid van goederenbewegingen en eventueel risico-analyse de kern. Transparantie is te realiseren met zogenaamde dashboards voor visualisatie van data. Risico-analyse analyseert deze data tegen bekende patronen uit historische data of tegen regels, waarbij het resultaat van die analyse ook in het dashboard getoond kan worden. Risico-analyses kunnen verschillen per overheidsinstantie vanuit hun taakstelling en hebben andere data nodig. De benodigde data is afleidbaar uit wet- en regelgeving (zie verder). Daarmee wordt ook inzichtelijk of hergebruik van data die het bedrijfsleven onderling uitwisselt, mogelijk is.

Een betere vergelijking tussen varianten één en twee vereist een nadere analyse van wetgeving rond vaststelling van besluiten (data waarop een besluit is genomen, moet beschikbaar blijven), databeheer door de overheid en archivering (archiefwet). Deze wetgeving heeft impact op een keuze en daarmee samenhangende kosten.

De derde optie lijkt op korte termijn nog niet haalbaar voor vrachtvervoer, maar is mogelijk al wel te testen voor personenvervoer. De tweede en derde optie vergen een nadere analyse van opslag van historische data en zijn exploitatie ('level playing field' voor big data en data analytics, aandachtspunt van het Ministerie van EZ).

2.5 Conclusies

Vanuit de doelstelling om B2A data rapportage – en A2B terugkoppeling van data te vergemakkelijken - en B2B data delen te stimuleren is de optimale inrichtingsvariant voor een eOverheid Logistiek die van toegang tot bedrijfsdata die ondernemingen onderling uitwisselen. Dit kan nog in allerlei vormen zoals het continu verzamelen van die data (crawling) en een combinatie van events met Application Programming Interfaces. De voorgesteld inrichtingsvariant geeft naar verwachting ook de gewenste voordelen, zowel bij de overheid als bij ondernemingen. Om dit te bereiken zijn eisen aan een Platform Infrastructuur te formuleren (zie het volgende hoofdstuk).

Hoewel het draaien van overheidstoepassingen bij ondernemingen (al dan niet in een Platform Infrastructuur) toekomstmuziek lijkt, is dit technisch al wel te realiseren. Op dit moment wordt dit niet verder uitgewerkt.

3 Inrichtingseisen

De voorgestelde inrichtingsvariant is hergebruik van bedrijfsdata uitgewisseld wordt via een Platform Infrastructuur door overheidsinstanties (de eerder genoemde variant 2). Deze bedrijfsdata en de infrastructuur dient wel te voldoen aan een aantal eisen. Deze eisen worden in dit hoofdstuk verder uitgewerkt.

Om algemene eisen aan inrichting in het private domein te kunnen formuleren is het nodig een technologie – en implementatie onafhankelijke (en daarmee bedrijfsmodel onafhankelijke) beschrijving van deze infrastructuur te geven. Eisen zijn vervolgens voor de verschillende componenten van een dergelijke Platform Infrastructuur te specificeren.

3.1 Inrichting

3.1.1 Terminologie

Gegeven dat er vele oplossingen zijn voor het delen en ontsluiten van data, zijn eenduidige termen nodig om deze oplossingen te beschrijven en is een model nodig voor vergelijking van diensten van die oplossingen te geven. Bijlage B geeft het model, met een opsomming van soorten oplossingen conform dit model.

Om geen onderscheid te maken tussen (fysieke) objecten (met sensoren of actuatoren, al dan niet met IT verwerkingscapaciteit) en ondernemingen wordt hierna de term ‘actor’ gehanteerd.

Deze paragraaf geeft generieke termen voor de specificatie van de Platform Infrastructuur, te weten:

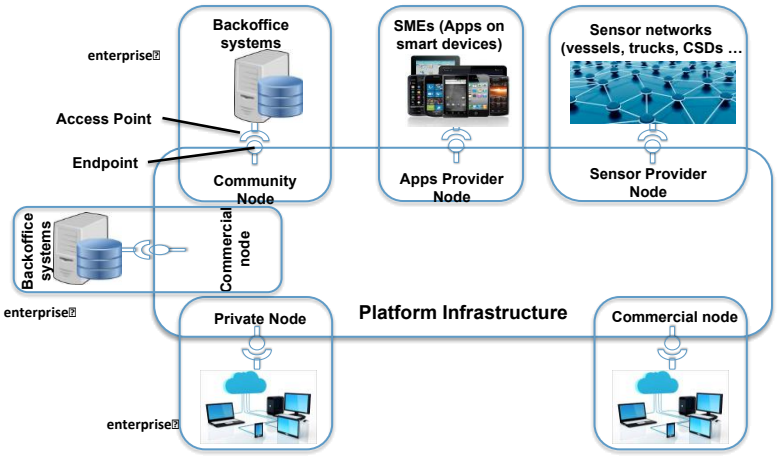
- **Node**: een node levert diensten aan zijn gebruikers. Nodes (zie bijlage B) zijn onderling gekoppeld via een (verzameling van) protocol(len).
- **Platform Infrastructuur**: de verzameling van nodes die diensten aan gebruikers bieden en onderling interoperabel zijn.
- **Endpoint**: het adres waar een actor is gekoppeld aan de Platform Infrastructuur. Een organisatie kan meerdere endpoints hebben met één endpoint per node.
- **Access Point**: software component voor de integratie van back-office systemen van een actor aan één of meer endpoints is gekoppeld.
- **Ondersteunende hulpmiddelen**: alle hulpmiddelen die een gebruiker nodig heeft voor registratie en aansluiting op de Platform Infrastructuur om zo eenvoudig zaken te kunnen doen.

3.1.2 Gebruik door ondernemingen

Er is een onderscheid te maken tussen (internationaal opererende)grote - en MKB ondernemingen. Gelet op hun geringe investeringsmogelijkheden en beperkte kennis van ICT hebben MKB ondernemingen behoefte aan een Access Point met alle door hen gewenste diensten toegankelijk via een user interface. Denk hierbij aan apps op smart devices.
Grotere ondernemingen zullen een eigen Access Point willen inrichten voor integratie met hun back office systemen. Dit Access Point ondersteunt mogelijkerwijs ook meerdere endpoints. Ondernemingen kunnen ook afspreken om

voor een bepaald doel (tijdelijk of voor langere duur) data te delen en zo een community vormen. Een community kan ontstaan, veranderen en verdwijnen, gekoppeld aan logistieke stromen en objecten en/of rond een logistieke hub. Er zijn dan bijvoorbeeld ook twee soorten nodes vanuit een gebruikersperspectief: een keten-node (ondersteuning van hun logistieke keten(s)) en een hub-node (ondersteuning van processen in een hub).

Deze keuzevrijheid resulteert in verschillende nodes met onderlinge koppelingen en gebruik door ondernemingen (zie de volgende figuur). Mocht een onderneming een keuze maken een eigen node in te richten, dan moet deze onderneming ook aangeven welke diensten deze node ondersteund. Sensor provider nodes zijn ook onderdeel van de infrastructuur. Het betreft leveranciers van sensor gebaseerd data diensten aan logistieke ondernemingen zoals Transics voor On Board Units.



3.1.3 *Gebruik door autoriteiten*

Autoriteiten hebben te maken met een verscheidenheid van nodes en keuzevrijheid van ondernemingen voor één of meer nodes. Om deze verscheidenheid tegemoet te treden, richten autoriteiten nu eigen nodes in, bijvoorbeeld Single Window toepassingen. Een adaptieve overheid (zie hoofdstuk 2) moet omgaan met deze verscheidenheid aan nodes en vanuit zijn taakstelling toegang hebben tot de log en audit trail van de nodes waar bedrijven hun endpoints hebben met als doel data voor geleverde diensten van nodes aan bedrijven te verzamelen en analyseren. Autoriteiten gebruiken daarmee de monitoring diensten van één of meer nodes. Nieuwe transacties die gelogd worden door een node zouden een event kunnen genereren om data op te halen (zie hoofdstuk 2).

3.2 Eisen aan een Platform Infrastructuur

Waar in het vorige actoren een veralgemenisering is van fysieke objecten en organisaties, wordt hierna dit concept uitgebreid met programmatuur. Programmatuur kan namelijk ook (autonoom) bewerkingen op data uitvoeren, denk aan virussen of malware.

Een adaptieve overheid stelt dezelfde eisen als het bedrijfsleven aan het delen van data in het private domein. Deze eisen zijn als volgt te groeperen:

- Eisen voor delen en (tijdelijke) opslag van data via de infrastructuur:
    - Het voorkomen van passieve inbraak: alleen geautoriseerde actoren hebben toegang tot data ontsloten of wordt gedeeld via de Platform Infrastructuur.
    - Het tegengaan van actieve inbraak: alleen geautoriseerde actoren kunnen data wijzigen die is ontsloten of wordt gedeeld via de Platform Infrastructuur.
- Kwaliteit van data: de beschikbare data dient volledig en correct te zijn en dient consistent te zijn als ze in meerdere systemen is opgeslagen.
- Eisen aan de diensten van de verschillende nodes om ondernemingen keuzevrijheid te bieden en eisen aan het protocol tussen deze nodes om een Platform Infrastructuur te realiseren.
- Eisen aan de data die in een log en audit trail is opgeslagen. Dit betreft semantiek en ondersteuning van één of meer syntaxes voor de weergave van die data, met aansluiting bij bestaande (open of defacto) standaarden. Ook moet de taal voor teksten in datavelden bekend zijn.

Deze eisen worden hierna verder uitgewerkt.

3.2.1 Eisen aan de Platform Infrastructuur: passieve en actieve inbraak

De eisen in deze groep zijn gerelateerd aan vertrouwen in de Platform Infrastructuur: functioneert deze naar behoren. Elke node moet aantonen welke mechanismen worden gehanteerd om aan deze eisen te voldoen. Bij de eisen worden ter illustratie oplossingen gegeven om die eisen in te vullen. Deze lijst met oplossingen is niet volledig en zal ook afhankelijk zijn van de gebruikte technologie. De volgende eisen gelden:

- Toegang tot data: alleen daartoe geautoriseerde actoren hebben, al dan niet met machtigingen, toegang tot data gedeeld tussen bedrijven via de Platform Infrastructuur. Een classificatie van data met bijvoorbeeld een onderscheid naar open data en bilateraal toegankelijke data is een eerste aanzet, waarna vercijfering, toegangscontrole en een firewall een vorm van afscherming zijn. In sommige gevallen kan ook worden volstaan met hashing, waarbij de berekende hash over de inhoud bijvoorbeeld alleen door een ontvanger te controleren is of alleen door een bepaalde verzender toegevoegd is. De inhoud is zichtbaar voor derden, maar kan niet gewijzigd worden. Deze technieken worden toegepast in bijvoorbeeld blockchain.
  Deze eis geldt voor:
    - (Tijdelijke) opslag van data in een node.
    - Uitwisseling van data tussen nodes. Hiervoor zijn bijvoorbeeld server certificaten te gebruiken.
    - Integratie van een access point met een endpoint. Ook hier zijn server certificaten bruikbaar, maar dient een node ook de identificatie van gebruiker van een access point te authenticeren.
    - Peer-to-peer data uitwisseling over de Platform Infrastructuur tussen twee Access Points. Dit is bijvoorbeeld met asymmetrische encryptie in te vullen.
- Peer-to-peer authenticatie: dit betreft het eenduidig vaststellen van de identiteit van Access Points die onderling via de Platform Infrastructuur data delen. Er zijn verschillende mechanismen mogelijk, bijvoorbeeld authenticatie van een Access Point door de node waar een onderneming

zijn endpoint heeft en onderling vertrouwen tussen de nodes, het toepassen van asymmetrische encryptie met een hash die alleen een zender kan toevoegen en door een ontvanger is te valideren, etc.

- Non-repudiation: onomstotelijk kunnen aantonen dat de data die zender en ontvanger hebben uitgewisseld bij beide actoren identiek is. Hiervoor zijn drie functies nodig:
    - Audit trail: vastleggen van alle (trans)acties op data tussen ondernemingen door elke node.
    - Log: vastleggen van alle data die is uitgewisseld.
    - Archieffunctie: de volgens wettelijke termijnen benodigde bewaarplicht voor audit trail en log.

  Deze drie functies kennen vercijferde opslag. Blockchain vervult deze functionaliteit. Een log en een audit trail leveren Monitoring services (zie bijlage B).
- Reputatie: het betreft het vertrouwen dat een gebruiker zich gedraagt volgens de regels voor het gebruik van de Platform Infrastructuur Diensten. Allereerst geldt dat een gebruiker ook is die hij zegt dat hij is, zodat hij een elektronische identiteit kan krijgen. Deze identiteit, verstrekt door een Identity Provider, kan ingetrokken worden bij ongeoorloofd gedrag. Reputatie zal gekoppeld zijn aan dienstverlening van gebruikers, zodat ze (normaliter) het afgesproken gedrag hebben.
- Auditability: elke node beschrijft zijn processen tussen invoer en uitvoer, waarbij die processen ook auditable moeten zijn. Auditability kan door vanuit log en audit trail deze processen te reconstrueren en te valideren (proces mining).

3.2.2 Datakwaliteit

De kwaliteit van data wordt gekenmerkt door:

- Volledigheid: alle data van fysieke objecten en hun samenhang en de infrastructuur in plaats en tijd is toegankelijk via de Platform Infrastructuur. Dit kan gaan om een deel van de fysieke infrastructuur, bijvoorbeeld een vaarweg die onder het beheer van een bepaalde autoriteit valt.
- Consistentie: dubbele data over identieke objecten is gelijk. Platformen verrichten geen manipulatie van data.
- Eenduidigheid: data moet niet voor verdere interpretatie mogelijk zijn. Dit betekent bijvoorbeeld dat tijdzones bekend moeten zijn, eenheden van maten en gewichten, valuta, etc.
- Correctheid: de data is een juiste weergave van de fysieke werkelijkheid en de transacties tussen actoren om die werkelijkheid te wijzigen. Een eis is bijvoorbeeld: alles wat in deze infrastructuur door verschillende actoren wordt ingebracht in de vorm van data moet niet leiden tot strijdigheid in de fysieke omgeving. Dit geeft twee eisen:
    - Een fysieke object mag op een bepaald moment maar eenmaal gebruikt worden. De capaciteit van een schip, vrachtwagen of sluis kan maar één keer tegelijk door meerdere andere objecten gebruikt worden.
    - Een fysiek object mag op een bepaald moment maar op één locatie zijn. Een voorbeeld is dat een container maar één keer op een bepaalde plek aanwezig kan zijn.

Het moment kan in het verleden, heden of toekomst liggen. Tegenstrijdigheden in de toekomst kunnen voorkomen, maar dienen tijdig opgelost te zijn. Mogelijk zijn hier nog meer eisen te formuleren.

Kwaliteit van data wordt verhoogd als alle ondernemingen in logistieke netwerken data eenmalig opslaan en elkaar (gecontroleerd) toegang geven tot data. Conceptuele interoperabiliteit is hiervoor noodzakelijk. Dit geldt niet alleen voor beschikbare capaciteit en logistieke diensten, maar ook voor transactiedata. Bij commerciële overdrachtsmomenten wijzigt het eigendom van data.

3.2.3 Platform Infrastructuur Diensten en – Protocol

Om een voor autoriteiten transparante Platform Infrastructuur te realiseren dienen de volgende eisen ingevuld te worden:

- Platform Infrastructuur Diensten: gelijksoortige diensten van verschillende nodes voldoen aan dezelfde specificaties.
- Minimale en maximale dienstverlening: monitoring van data delen door autoriteiten stelt eisen aan het type diensten dat een Platform Infrastructuur levert. Bijlage B geeft een indeling naar diensten. Een autoriteit heeft altijd toegang tot het log en de audit trail die de basis vormen voor Monitoring Services. We onderscheiden:
    - Minimale dienstverlening is toegang tot het log en de audit trail voor technische diensten: welke data is met wie uitgewisseld en wie heeft toegang tot welke data gehad. Op basis van dit log en de audit trail reconstrueert een autoriteit logistieke processen conform zijn taakstelling.
    - Maximale dienstverlening is toegang tot het log en de audit trail met het gebruik van logistieke diensten: wie is betrokken bij de afhandeling van goederenstromen. Dit omvat enerzijds de data over de goederenstromen conform gepubliceerde logistieke diensten en anderzijds de samenstelling van logistieke ketens. Data kent een hoger aggregatieniveau dan hetgeen in een log en audit trail van technische diensten is opgeslagen.
- Platform Infrastructuur Protocol: gelijksoortige diensten van verschillende nodes zijn onderling gekoppeld via een protocol (functionele afspraken) met aanvullende niet-functionele afspraken zoals verrekening, snelheid van verwerking (performance), inzage in eventuele vertragingen, onderhoud en (tijdelijke) storingen en aantal gelijktijdige transacties per tijdseenheid.
- Ontkoppeling tussen diensten en protocol: er zijn verschillende manieren om bepaalde diensten te leveren. Een voorbeeld is het herleiden van events uit berichten of data die uit een externe bron wordt ontvangen. Op protocolniveau zijn berichten afgesproken, terwijl op dienstenniveau events worden geproduceerd. De transformatie en regels tussen protocol en diensten moeten herleidbaar zijn (auditable).

3.2.4 Data: semantiek, syntax en (open en defacto) standaard(en)

Vanuit het perspectief van autoriteiten dient er een eenduidige specificatie van semantiek te zijn van de data die in een log en audit trail is opgeslagen (zie ook bijlage A). Dit is data die wordt uitgewisseld tussen bedrijven en tussen bedrijven en overheden en kan aanvullende eisen voor data vanuit autoriteiten omvatten. Het gaat over logistieke – en gerelateerde objecten met het relevante gezichtspunt voor een betreffende autoriteit, zoals dat in bijlage A is aangegeven, op technisch niveau

(berichten, API data) en logistiek niveau (ketenpartners, transacties tussen partners, logistieke objecten).

Data is vanuit semantische modellen weer te geven met een syntax (EDIfact, XML, JSON, …) en kan op verschillende manieren worden uitgewisseld (berichten, APIs, etc.). Datastructuren en semantiek zijn herleidbaar uit achterliggende modellen (WCO data model, Common Framework, UN/CEFACT supply chain reference model). Eventuele implementatierichtlijnen dienen wel te voldoen aan de eisen die een autoriteit aan datakwaliteit stel (zie eerder).

Een overheidsinstantie dient daarmee ook de door hem benodigde semantiek van data te koppelen aan semantische modellen die conceptuele interoperabiliteit ondersteunen. Zij moeten bijvoorbeeld aangeven uit welk perspectief zij data willen voor bepaalde objecten. Uniformiteit van semantische begrippen is een randvoorwaarde voor hergebruik van data.

In een nieuwkomerscenario (bijlage C) is een implementatie in bestaande modellen en implementatierichtlijnen niet nodig en volstaat een afbeelding van interne data structuren van IT systemen van ondernemingen naar semantiek voor interoperabiliteit. In een verrijkingsscenario is de implementatie in bestaande modellen en richtlijnen nodig. In het verrijkingsscenario kunnen hulpmiddelen ontwikkeld worden die conform het nieuwkomersscenario interne systemen aan de infrastructuur verbinden, met bestaande implementatierichtlijn. Deze implementatierichtlijnen zijn niet zichtbaar voor een onderneming; een onderneming maakt alleen een keuze die samenhangt met bijvoorbeeld de mogelijke implementaties van zijn partner(s). Daarmee heeft een individuele onderneming een open omgeving met aansluiting bij al geïmplementeerde implementatierichtlijnen.

3.3 Conclusies

Dit hoofdstuk geeft vier groepen van eisen voor een Platform Infrastructuur, zijn verschillende onderdelen en de aansluiting op en het gebruik van die infrastructuur. Daarmee worden geen uitspraken over de implementatie gedaan, maar worden alleen eisen aan de inrichting en het gebruik gesteld.

Het volgende hoofdstuk geeft aan op welke wijze deze eisen voor een concrete toepassing ingevuld kunnen worden, waarbij verschillende oplossingen voor de invulling gebruikt kunnen worden.

4 Digitalisering van vervoersdocumenten

Een elektronische vrachtbrief is een voorbeeld van een document dat verplicht bij goederenvervoer aanwezig moet zijn, in dit geval bij goederenvervoer over de weg. Dit hoofdstuk specificeert de toepassing van de generieke eisen voor een infrastructuur rond elektronische vrachtbrieven (eCMR). Er zijn verschillende 'nodes' in een dergelijke infrastructuur, zoals TransFollow en een Deense toepassing.

Allereerst wordt de functionaliteit van dit soort documenten ('contract of carriage') toegelicht om vervolgens aan te geven hoe dit voor een eCMR ingevuld kan worden.

4.1 Functionaliteit van vervoersdocumenten

Alle modaliteiten kennen een vrachtbrief, denk aan een Bill of Lading (B/L) of sea waybill voor zeetransport, (House(Airway Bill ((H)AWB) voor lucht en CIM voor spoorvervoer. Veelal combineren deze documenten verschillende functies en worden voor verschillende doelen gebruikt:

- Eigendom: degene die het document heeft kan daarmee aantonen eigenaar van de goederen te zijn of namens een eigenaar op te treden. Een B/L heeft deze functie, die vooral van toepassing is bij verhandelen van bulkgoederen ('commodity trading').
- Condities voor aansprakelijkheid: een document vermeldt de condities waaronder vervoer plaatsvindt. Hieronder vallen ook aansprakelijkheid bij schade of verlies van lading. Wegvervoer is veelal onder de zogenaamde CMR-condities. In zeetransport liggen condities vast in verschillende afspraken stelsels zoals Incoterms (voor betaling) en Rotterdam Rules (voor inzage in lading); voor luchttransport zullen gelijksoortige afspraken stelsel ontwikkeld zijn. Alle vervoerders in die modaliteiten vervoeren onder deze internationale overeengekomen afspraken en regels.
- Inspectie: het document wordt gebruikt voor het inspectie van vervoersmiddelen. Dit is vooral in het wegtransport, waarbij voor afvaltransport specifieke oplossingen zijn ingericht. Inspectie is gericht op handhaving van veiligheidsregels, waarbij vooral gelet wordt op gevaarlijke lading. Andere modaliteiten zoals zee, binnenvaart en rail gebruiken hier aparte aangiften, bijvoorbeeld infrastructuurbeheerders zoals Havenautoriteiten, RWS en ProRail om veiligheid in de door hen beheerde infrastructuur te handhaven.
- Zending en lading: beschrijving van de opdracht die een vervoerder verricht voor zijn klant. Dit omvat de lading en hun conditie, opdrachtgever, afhaallokatie, etc. De conditie van lading wordt bij ontvangst door een vervoerder gecontroleerd en bij aflevering door de ontvanger. Dit zijn twee punten van overdracht waar controle plaatsvindt. Deze controle is voor alle modaliteiten, omdat elke volgende schakel aansprakelijk is volgens overeengekomen condities.

Gebruik van (elektronische) documenten kan bij wet zijn vastgelegd vanuit de functie van inspectie, denk aan het eCMR verdrag.

4.2 Elektronische vrachtbrief voor het wegtransport: eCMR

Een eCMR bevat de functies ‘condities voor aansprakelijkheid’, ‘inspectie’ en ‘zending en lading’. De functies ‘condities voor aansprakelijkheid’ en ‘zending en lading’ hangen samen: vooral de punten van overdracht tussen verlader en vervoerder en vervoerder en ontvanger moeten onomstotelijk vastliggen. De inspectiefunctie eist alleen toegang tot de data, waarbij onomstotelijk vast moet staan dat de data van een zending correct is.

De kwaliteit van de data over zending en lading staat los van de Platform Infrastructuur. Deze kwaliteit kan voor papieren documenten en elektronische oplossingen gelijk zijn.

Er zal altijd één onderneming zijn die voor een zending de eCMR opmaakt en afhandelt. De eCMR ontstaat uit een transportopdracht van een verlader aan een LSP/vervoerder. Deze data is de basis voor de eCMR, die vervolgens wordt gevalideerd bij overdracht van lading door consignor aan LSP en door LSP aan ontvanger. In de praktijk kan een verlader of een LSP/vervoerder een vrachtbrief afdrukken. Als een verlader dit doet, is dat meestal op het moment van overdracht van de goederen aan een vervoerder. Als een vervoerder of LSP dit doet, is het veelal na ontvangst van een transportopdracht. De twee statuswijzigingen bij overdracht zijn vast te leggen, voorzien een unieke handtekening van betrokken partijen en eventuele opmerkingen bij de overdracht.

Elke onderneming of oplossing die functionaliteit voor een eCMR levert, functioneert als een node met een beperkte functie in de Platform Infrastructuur en dient te voldoen aan de eisen die in paragraaf 3.2 zijn geformuleerd voor een individuele node. Er is nu wel een afbakening in de vorm van semantiek: deze beperkt zich tot transportdiensten via de weg, maar kan in wezen alle typen lading omvatten. De eisen zijn verder aan te scherpen:

- Identiteit, Authenticatie en Autorisatie: elke actor moet zich eenduidig kunnen identificeren om toegang te kunnen krijgen voor de voor hem beschikbare data over zending en lading. Voor verlader, vervoerder en ontvanger geldt dat zij alleen toegang hebben tot data van zendingen en lading waar zij bij betrokken zijn. Een autoriteit heeft alleen toegang tot die zendingen, waar (1) bepaalde kenmerken voor gelden vanuit wet- en regelgeving (denk aan gevaarlijke lading) of (2) bij aanhouding en mogelijk fysieke inspectie gecontroleerd kan worden dat de data klopt met de feiten. Onder (1) valt bijvoorbeeld een volledig overzicht van bepaalde ladingstromen in een periode en/of een regio.
  Identiteit van elke actor moet voor wegvervoer op EU niveau vast te stellen zijn. Er moet dus een Europees systeem komen voor het bepalen Identiteit en Authenticatie, bijvoorbeeld eIDas als CEF – building block. Toegangscontrole is op dit punt eenvoudig gekoppeld aan de data zelf.
- Non-repudiation: zodra overdracht van goederen door een volgende schakel in de keten heeft plaatsgevonden, kan de data en het moment van overdracht niet meer gewijzigd worden. Handelingen zijn vastgelegd in een log en een audit trail. Mogelijkerwijs wordt er bij overdracht data toegevoegd aan de oorspronkelijke data, bijvoorbeeld opmerkingen over eventuele schade bij in ontvangst nemen van goederen.

Non-repudiation is op verschillende manieren in te vullen, bijvoorbeeld
  - Onafhankelijke partij ('trusted third parties'): er is een onafhankelijke organisatie die deze functie invult. TransFollow en de Deense oplossing zijn hiervan een voorbeeld en vormen eCMR nodes. Zij dienen te voldoen aan de eisen aan nodes binnen een Platform Infrastructuur. Hun diensten zijn onderling afgestemd en zij hebben een protocol zodat verladers, LSP en ontvangers verschillende platformen kunnen gebruiken.
  - Vertrouwen en reputatie: veel grote verladers of logistiek dienstverleners bieden de garantie aan hun klanten dat zij data niet wijzigen. Dit hangt samen met reputatie: zodra ze dit wel doen, verliezen ze het vertrouwen in hun diensten bij hun gebruikers. Dit is niet anders dan bij de huidige wijze van data delen met documenten. Er ontstaan zo peer-to-peer of privately owned nodes. Ook deze moeten geïntegreerd worden met andere nodes als TransFollow.
  - Infrastructuur: een infrastructuur maakt het onmogelijk om data te wijzigen nadat die eenmaal is toegevoegd. Blockchain als technologie voor data delen is hiervan een voorbeeld, waarbij aspecten als governance van data in de blockchain ('mining') nader uitgezocht moet worden. De blockchain bestaat uit verschillende nodes, waar elk van de nodes voldoet aan de eisen, een deel of alle data bevat en de totale blockchain een volledig log en audit trail in een logistiek netwerk vormt.
- Log en audit trail: een autoriteit moet toegang hebben tot een log en audit trail voor de endpoints van de betrokken ondernemingen van alle relevante nodes: verladers, ontvangers en vervoerders. Indien een eCMR met verschillende nodes wordt gerealiseerd, dient een autoriteit geautoriseerd toegang te hebben tot elke betrokken node. Als dit bijvoorbeeld een privately owned node van een vervoerder is, zal die zijn log en audit trail moeten ontsluiten, zoals TransFollow dit ook kan doen. Voor elke betrokken onderneming dient een endpoint beschikbaar te zijn.
- Semantiek: dit beperkt zich tot transportdiensten via de weg, maar kan in wezen alle typen lading omvatten. Zodra een vraag voor transport of de gebruikte dienst eenduidig bekend is, is ook bekend welke data aanwezig moet zijn. Als dus een vraag komt voor het vervoer van pallets en hier een dienst voor transport van gevaarlijke lading wordt aangeboden, zou kunnen blijken dat er sprake is van pallets met gevaarlijke lading.
- Techniek: de technische oplossing inclusief op welke wijze die wordt gebruikt dient vast te stellen te zijn. Denk bijvoorbeeld aan het toepassen van XML vanuit het Common Framework of het WCO data model. Vanuit conceptuele interoperabiliteit is dit oplosbaar.
- Taal: er zullen meerder talen (en mogelijk ook verschillende alfabetten) gehanteerd worden. Denk aan het Cyrillisch en Grieks alfabet. Hier zijn twee benaderingen te kiezen:
  - Zoveel mogelijk gebruik van coderingen. Een codewaarde kan in verschillende talen en alfabetten worden weergegeven.
  - Automatisch vertalen: teksten worden zoveel mogelijk automatisch vertaald. Programmatuur is hiervoor beschikbaar.
- Toegankelijkheid: de data moet toegankelijk zijn voor alle betrokkenen, op het moment dat dit gewenst is. Hier zullen de nodige

communicatienetwerken ondersteund moeten worden met voldoende dekking, evenals (een verwijzing naar) de locatie (server) waar de data opgeslagen is.

Bij de toepassing van blockchain technologie is semantiek en techniek met een deel van de toegankelijkheid met zogenaamde smart contracts (stukje programmacode) te realiseren, waarbij elke stakeholder een smart contract heeft (met daarin zijn acties). Deze moeten wel ontwikkeld worden. Elk van de betrokken actoren kan zijn smart contract inrichten, maar wel vanuit een gezamenlijk semantisch model. De Smart Contracts voor een eCMR vormen de Access Points, zij kunnen worden voorzien van een toepassing (b.v. een app op een Smart Device). Er is onderzoek nodig of er één of meer onafhankelijke partijen nodig zijn die acties van stakeholders valideren en toevoegen aan de blockchain; mogelijk is dit te integreren met een reputatiemanagement oplossing. Ook integratie met IoT kan extra controles geven.

Als een Platform Infrastructuur met meerdere nodes (of peer-to-peer oplossingen) wordt gebruikt, is een zogenaamde Registry node nodig om organisaties en de door hen gehanteerde techniek met endpoint te vinden, waarbij dat endpoint gekoppeld is aan een node. Als bijvoorbeeld een vervoerder de oplossing van TransFollow hanteert, levert TransFollow zijn endpoint voor data over elektronische vrachtbrieven.

4.3 Oplossing voor een autoriteit

Gebaseerd op bovenstaande eisen komen er meerdere nodes in het private domein voor een eCMR. Een toezichthouder of handhaver moet de beschikking hebben over een eenvoudige toepassing, gebaseerd op de semantiek van de eCMR met toegang tot de logs en audit trails van de nodes.

Zoeken en vinden van de juiste node verloopt via een zogenaamde Registry Node. Zoekstructuren dienen ontwikkeld te worden door bijvoorbeeld via kentekens van voertuigen of AIS data van vaartuigen te komen tot de organisatie die het voer- of vaartuig exploiteert om vervolgens een endpoint te vinden voor eCMR data. Andere zoekstructuren zijn bijvoorbeeld in een gebied op een bepaald type gevaarlijke lading in een periode (dag, week, etc.), waarna via een Registry node de alle endpoints worden ontsloten om deze zoekvragen door eCMR nodes te laten beantwoorden. Deze zoekstructuren zullen nadere uitgewerkt moeten worden.

Invoering van een Registry Node is conform het verrijkingsscenario waar ontbrekende functionaliteit in de huidige realisatie van de Platform Infrastructuur wordt aangevuld.

4.4 Conclusie

Het is goed mogelijk om een eOverheid Logistiek in te richten die toegang heeft tot data uit verschillende nodes van een Platform Infrastructuur voor een eCMR, mits deze nodes voldoen aan een subset van de algemene eisen (alleen die eisen die voor een eCMR infrastructuur nodig is). Daarvoor is het ook nodig dat autoriteiten hun zoekstructuren specificeren, mogelijk met koppeling naar andere bronnen dan

alleen deze nodes. Het vereist zeer waarschijnlijk ook aansluiting van bestaande nodes en verrijking met functionaliteit.

5 Conclusies en aanbevelingen

5.1 Conclusies

Dit rapport geeft een voorstel voor invoering van een open systemen voor gecontroleerd delen van data tussen ondernemingen volgens een nieuwe vorm data gedreven van toezicht en handhaving in de logistiek, te weten directe toegang voor toezicht en handhaving tot data die bedrijven onderling delen als basis voor handhaving bij inspectie van fysieke stromen. Deze bedrijfsdata vormt daarmee een (virtueel) Single Window voor Handel en Transport.
Het uitgangspunt is op deze manier een adaptieve overheid in te richten, met keuzevrijheid van oplossingen in het bedrijfsleven en flexibel in te spelen op innovaties. De nieuwe vorm van toezicht geeft een andere inrichting van systemen bij de verschillende autoriteiten en stelt eisen aan het delen van data tussen ondernemingen.

Deze eisen zijn op vier aspecten te formuleren:

- Eisen aan een (federatieve) Platform Infrastructuur om passieve (ongeautoriseerde toegang tot data) en actieve (ongeautoriseerde wijziging van data) te voorkomen.
- Eisen aan kwaliteit van data: volledig, consistent, eenduidig en correct om de kwaliteit van toezicht te verbeteren.
- Eisen aan diensten en afspraken voor de koppeling tussen nodes binnen een Platform Infrastructuur om toegang tot de juiste data te krijgen.
- Eisen de te delen data: eenduidige specificatie en hergebruik van eigenschappen van logistieke objecten en – diensten voor verwerking van data bij toezicht. Vanuit het perspectief van toezicht en handhaving geeft dit één of meer (virtuele) Single Windows in de vorm van semantische modellen gekoppeld aan taakstellingen. Beheersmatig is het aan te bevelen om te komen tot meerdere semantische modellen voor autoriteiten om zo onderlinge afhankelijkheden voor data behoeften te verkleinen door deze zoveel mogelijk alleen te baseren op beschikbare data van het bedrijfsleven.

Deze eisen zijn de basis voor de inrichting van een oplossing van eCMR die werkbaar is voor de overheid. Daartoe zal ook de overheid zijn systemen moeten aanpassen.

Conceptuele interoperabiliteit omvat semantiek als middel voor de registratie en aansluiting van een onderneming bij de Platform Infrastructuur. Daarvoor is het nodig verschillende softwarecomponenten te ontwikkelen, die er nog niet zijn. Hiervoor worden verschillende scenario’s onderzocht, gebaseerd op huidige ontwikkelingen. Het blijkt dat een verrijkings- of een nieuwkomerscenario de meest haalbaar oplossing is, zie bijlage C. Op korte termijn kan het verrijkingsscenario voor het invullen van een eCMR infrastructuur al worden opgepakt door realisatie van een zogenaamde Registry Node met zoekstructuren.

5.2 Aanbevelingen

Aanbevelingen op hoofdlijnen zijn:

- Verrijking van de bestaande infrastructuur voor specifieke toepassingen als eCMR. Hiervoor dient een blauwdruk ontwikkeld te worden met invulling door verschillende nodes, waaronder disruptieve technologie als blockchain technologie. Dit is het verrijkingsscenario.
- Identificeren van ondernemingen die autonome assets (voer-/vaartuigen, kranen, etc.) ontwikkelen en met hen komen tot afspraken rond diensten en protocollen voor een Platform Infrastructuur. Dit is het nieuwkomerscenario.

Beide scenario's vormen een basis voor verandering in het bedrijfsleven en bij de overheid. Uit deze scenario's volgen detailaanbevelingen als stappen voor het vervolg. De volgende stappen worden voorgesteld:

1. Draagvlak en beleidsmatige keuze: een beleidsmatige keuze voor de inrichting van een eOverheid Logistiek moet gebaseerd zijn op draagvlak bij overheidsinstanties en het bedrijfsleven. Een dergelijke keuze heeft meer afstemming en onderbouwing nodig, dit rapport is een verkenning van de richting.
2. Detaillering van de oplossing: het verder detailleren van eOverheid Logistiek en uitwerken van de eisen en (laten) ontwikkelen van prototype(s) voor bijvoorbeeld eCMR als verrijking van bestaande nodes in een eCMR infrastructuur. Deze prototypes kunnen in een later stadium als communicatiemiddel gehanteerd worden. De in dit rapport geformuleerde eisen worden hier nader afgestemd met ondernemingen om onderdeel van eOverheid Logistiek te vormen.
3. Impact assessment: als er een zekere mate van awareness is, is het nodig de gevolgen van de oplossing te onderzoeken. Welk scenario moet gevolgd worden (bijlage C), wat zijn eventuele nieuwkomers en wat is de business case voor een autoriteit en een onderneming. Bij de business case hoort ook een analyse van eventuele drempels gebaseerd op de gevolgen van de invoering.
4. Awareness creëren: het inzichtelijk maken van de mogelijkheden die de voorgestelde oplossing biedt met de eerder genoemde prototypes. Deze prototypes bij voorkeur toepassen op use cases met ondernemingen om daaruit best practices te herleiden.
5. Ontwikkeling: specificatie en beheer van open standaarden voor een Platform Infrastructuur. Dit zijn open standaarden voor conceptuele interoperabiliteit (semantiek, registratie en aansluiting; bijlage A) en Platform Infrastructuur Diensten en – Protocollen (bijlage B) met een keuze voor een invoeringsscenario (bijlage C):
    - Conceptuele interoperabiliteit: specificatie van logistieke diensten, logistieke objecten en eventuele aanvullende eisen vanuit wetgeving die de basis is van taakstelling, met hergebruik van bestaande modellen en implementatierichtlijnen.
    - Implementatiemethodiek: een methode voor de implementatie van conceptuele interoperabiliteit door ondernemingen en node leveranciers.
    - Beheer en invoeringsondersteuning (governance): dit richt zich vooral op decentraal beheer en onderhoud van standaarden en generieke middelen die nodig zijn om ondernemingen te registreren en verbinden met een Platform Infrastructuur. Validatie van

aansluitingen, implementatie van diensten en protocollen en het voldoen aan de eisen door node leveranciers kan onderdeel van governance zijn.
    - Platform Infrastructuur Diensten en – Protocollen (blauwdruk): de verschillende categorieën (bijlage B) dienen in overleg met het bedrijfsleven verder uitgewerkt te worden.
    - Invoeringsscenario: er dient zicht te komen op de haalbaarheid van het nieuwkomer- en verrijkingsscenario. Mogelijk kan disruptieve technologie met nieuwkomers een rol spelen; anders is de keuze voor een verrijkingsscenario voor de hand liggend.
6. Herinrichting van systemen bij autoriteiten: vanuit wet- en regelgeving dienen regels geformuleerd te worden voor toezicht en handhaving. Deze regels dienen zodanig te zijn dat ze in nodes van de Platform Infrastructuur te implementeren zijn.
7. Deployment: afstemmen met leveranciers van nodes voor door ontwikkeling en inrichting van die nodes. Voor het nieuwkomerscenario gaat het om de realisatie van nieuwe nodes; het verrijkingsscenario sluit aan bij bestaande nodefunctionaliteit. Aanvullend dient elke een zogenaamde verticale of horizontale node (bijlage B) die bepaalde diensten aanbiedt deze conform de specificaties leveren en ook conform het protocol koppelen met een andere node. Dit biedt ondernemingen de keuze om een oplossing te kiezen die het beste bij hen past (functionele eisen als diensten en hun implementatie en niet functionele eisen als snelheid van verwerking en hoeveelheid gelijktijdige diensten).

Elke stap geeft een voortdurende bijstelling van het concept en de visie. Er is dus een voortdurende terugkoppeling.

Parallel aan deze stappen dient ook internationale toepassing en overeenstemming gezocht te worden. Dit kan bijvoorbeeld vanuit de invoering van een eCMR. Vooral wegtransport met zijn grote aantal MKB ondernemingen, maar ook binnenvaart zijn gebaat bij een internationale oplossing gebaseerd op conceptuele interoperabiliteit. Overheden kunnen hier een sturende rol hebben.

Bijlage A – conceptuele interoperabiliteit

Deze bijlage geeft een verkenning van conceptuele interoperabiliteit vanuit een standaardisatie perspectief: wat is het en hoe is het te realiseren. Enerzijds betreft dit een aanvulling op bestaande standaarden, anderzijds een vernieuwde implementatie en gebruik van standaarden, waarbij eisen gesteld worden aan de functionaliteit van een Platform Infrastructuur. Allereerst geeft deze bijlage een inleiding tot conceptuele interoperabiliteit, vervolgens hoe conceptuele interoperabiliteit ingezet kan worden door autoriteiten en ondernemingen en als laatste eisen aan de technologie met als uitgangspunt dat er bestaande nodes in een Platform Infrastructuur zijn.

De achterliggende reden voor conceptuele interoperabilteit is in de inleiding van dit document aangegeven: het komen tot open systemen voor delen van data met gecontroleerde toegang van autoriteiten tot data.

A.1 Wat is conceptuele interoperabiliteit?

A.1.1. Aanzet tot conceptuele interoperabiliteit

Conceptuele interoperabiliteit is een top-down benadering voor het gestructureerd delen en toegankelijk maken van data met eenmalige registratie en aansluiting van gebruikers bij een Platform Infrastructuur. Daarmee wordt grootschalig data delen en dynamische ketenvorming met bijvoorbeeld synchromodaliteit mogelijk. De benadering is gebaseerd op vraag naar en aanbod van logistieke diensten. Een vraag zal altijd gaan over lading met zijn kenmerken, waarbij die vraag afgebeeld moet worden op beschikbaar aanbod.

Het aanbod naar diensten is gebaseerd op de middelen die een LSP heeft of kan inzetten. Een binnenvaartschip voor bulk kan dus geen containers vervoeren, zodat een vervoerder met een dergelijk schip dit niet als zijn dienst zal opnemen. Als LSP dan wel verschillende middelen kan inzetten, een expediteur heeft bijvoorbeeld een relatie met meerdere vervoerders, dan zal dit leiden tot verschillende diensten.
Logistieke vraag en aanbod hebben dus kenmerken zoals type lading, kenmerken van die lading (denk aan de mogelijkheid om koel- of gevaarlijke lading te

vervoeren), een gebied of corridor (denk aan de Rijn als corridor, transport tussen Nederland en Zuid Duitsland), tijdsduur en ook de periode waarop een dienst beschikbaar is (denk ook aan openingstijden van een terminal). De transportmodaliteit kan ook nog toegevoegd worden, zodat bij de vraag naar bijvoorbeeld een transportdienst ook rekening gehouden kan worden met eventuele vertragingen door ongelukken.
Elke specifieke dienst verwijst dus bijvoorbeeld naar het type objecten zoals containers voor een transportdienst. Kenmerken van deze objecten zijn al vanuit verschillende gezichtspunten gestandaardiseerd door verschillende organisaties. Het object 'container' heeft bijvoorbeeld kenmerken als type en nummer. Deze objecten hebben ook al een weergave in verschillende standaarden, bijvoorbeeld in het data model van de World Customs Organization of de UN/CEFACT standaarden.
Bovenstaande figuur maakt dus een onderscheid naar standaardisatie en specificatie op de volgende manier:

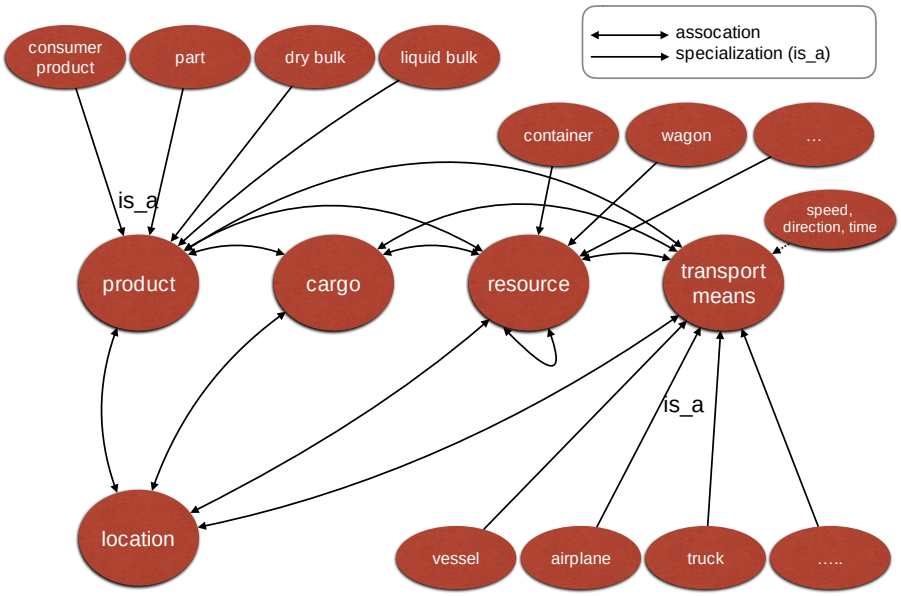
- Standaardisatie: het overeenkomen en vastleggen van in dit geval kenmerken voor vraag naar en aanbod van logistieke diensten, inclusief weergave van deze kenmerken in een bestaande standaard.
- Specificatie: elke onderneming registreert vraag naar of aanbod van logistieke diensten, of beiden.

De registratie van vraag naar of aanbod van logistieke diensten is dus een keuze op hoog niveau ('conceptueel') van het soort lading en zijn kenmerken dat wordt aangeboden en afgehandeld in een logistiek netwerk met daarbij specifieke patronen (tijd en plaats of gebied). Door ook een standaard voor uitwisseling te kiezen specificeert elke onderneming zijn data aanbod en – behoefte.

Dit onderscheid tussen standaardisatie en specificatie geeft eisen aan technologie voor conceptuele interoperabiliteit. Een onderneming moet bijvoorbeeld ondersteunende hulpmiddelen (zie paragraaf **Error! Reference source not found.**) hebben om zijn diensten te formuleren en er moeten hulpmiddelen zijn om vraag naar diensten te specificeren. Voor het laatste zijn al verschillende zogenaamde logistieke markten beschikbaar, voorbeelden zijn Transportmarketplace en TEUBooker, elk met eigen diensten rond het samenbrengen van aanbod en vraag naar diensten. In bijlage B is dit een zogenaamde marketplace dienst.

A.1.2 Soorten semantische modellen voor logistiek

De vorige figuur geeft aan dat in stap 2 verschillende gezichtspunten gehanteerd kunnen worden. Logistieke objecten wen hun samenhang is de basis voor conceptuele interoperabiliteit (zie volgende figuur).



Fysieke objecten als producten, lading (cargo), middelen om transport te vereenvoudigen (resources) en transportmiddelen met hun onderling associaties en hun associatie met een lokatie staan centraal in de vorige figuur. Alle associaties tussen de fysieke objecten hebben een tijdscomponent: een associatie is tot stand gekomen en verbroken op een bepaald tijdstip. Een container is bijvoorbeeld op een bepaald tijdstip op een schip geladen. Ook de associatie tussen fysieke objecten en locatie kent dezelfde tijdscomponent: een object is op een bepaalde locatie op een bepaald tijdstip aangekomen en mogelijk vertrokken (anders is het in opslag of is het een onderdeel van een ander product).

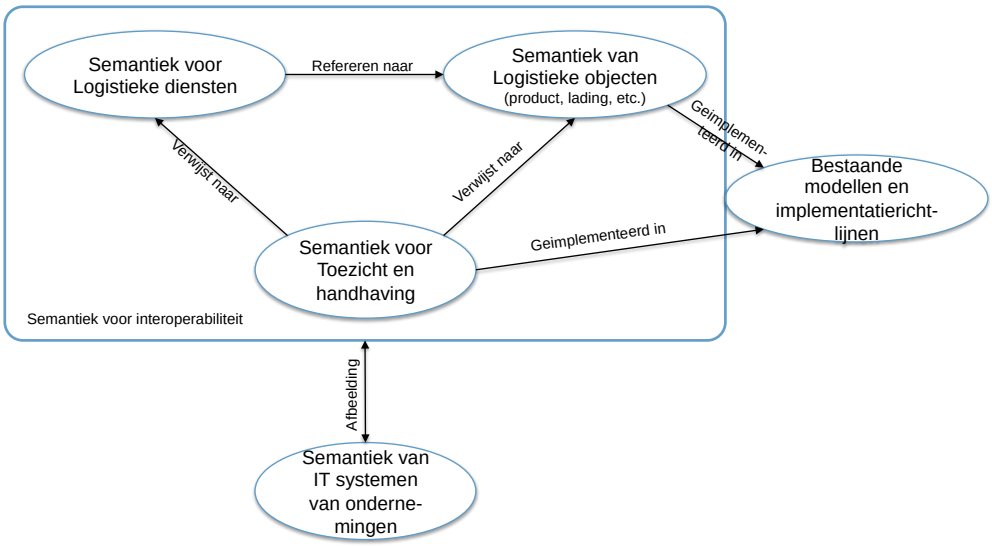
Waar data van fysieke objecten en hun samenhang in plaats en tijd logistiek representeren, zijn daar nog verschillende gezichtspunten op te specificeren. De volgende figuur toont voorbeelden van die gezichtspunten.

Elk van de gezichtspunten geeft specifieke eisen aan informatie. Het is ook niet gezegd dat bijvoorbeeld milieueisen geen invloed hebben op producten en logistieke stromen vanuit een data behoefte.

Een commercieel gezichtspunt is te representeren met transactiedata die twee ondernemingen uitwisselen. Een transactie gaat altijd over de afhandelingen fysieke objecten in combinatie met plaats en tijd. Er worden drie soorten tijdstippen onderscheiden: het door een klant gewenste tijdstip van afleveren opgenomen in zijn vraag, het geplande tijdstip dat een LSP aangeeft en het daadwerkelijke tijdstip waarop het is aangekomen. Dit onderscheid is van belang om bijvoorbeeld in te grijpen bij afwijkingen door te late aankomst (supply chain resilience).

A.1.3 Semantische modellen en hun samenhang

Vanuit elk van de gezichtspunten zijn nu semantische modellen te ontwikkelen en ook te beheren. De volgende figuur geeft de samenhang tussen enkele modellen die verschillende perspectieven representeren. Hergebruik van semantische stelt eisen aan de representatie van die modellen. Een semantisch model als het Common Framework is ontwikkeld als Unified Modeling Language (UML) klassediagram. Hier zijn geen referenties tussen modellen mogelijk als die modellen door verschillende organisaties zijn ontwikkeld en beheerd. Het WCO data model en ook het UN/CEFACT model zijn ontwikkeld met een modelleertool dat een volledig eigen representatie voor modellen heeft. Ook hier is het niet mogelijk om te refereren naar modellen en is onderhoud van het volledige model gecentraliseerd (bij respectievelijk WCO en UN/CEFACT). Gebruik van één van deze modellen betekent duplicatie en mogelijk aanpassing. Daarnaast is er één enkel hulpmiddel, terwijl voor UML klassediagrammen meerdere (open source) hulpmiddelen zijn. Voor het gebruik van UML geldt ook het argument van dupliceren en aanpassen. Ontology Web Language (OWL) is een alternatief, met bovendien meer uitdrukkingskracht, ondersteuning met open source middelen, aansluitend bij innovatieve technologie en toegepast in verschillende domeinen.



De vorige figuur toont een mogelijke samenhang tussen modellen, waar het semantisch model voor logistieke objecten de basis vormt (het wordt ook wel een zogenaamde ‘upper ontology’ genoemd). Deze ‘upper ontology’ dient gekoppeld te worden aan bestaande modellen zoals WCO data model om verschillende representaties te ondersteunen.

Er zijn één of meer semantische modellen voor toezicht en handhaving te ontwikkelen, gebaseerd op de logistieke modellen. Als er één semantisch model is, kunnen we spreken van een (virtueel) Single Window. Er zijn ook combinaties van

verschillende taken met daarbij horende semantische modellen mogelijk, zodat er varianten in dit Single Window ontstaan. Door semantische modellen voor toezicht en handhaving zoveel mogelijk te baseren op logistieke semantische modellen, worden afhankelijkheden tussen databehoeften voor de verschillende taakstellingen van de overheid verkleint. Daarmee wordt de overheid adaptiever.

Deze semantische modellen moeten alle modaliteiten omvatten, waarbij die standaarden op identieke wijze door alle betrokkenen geïmplementeerd zijn zodat een open systeem ontstaat voor monitoring van logistieke stromen door overheidsinstanties. Binnen EC DG Move – Digital Transport and Logistics Forum is hiervoor een voorstel gedaan.

Binnen het NWO ISCOM programma onderzoekt een promovendus aan de TUDelft de semi-automatische generatie van afbeeldingen tussen interne datastructuren en een semantisch model voor interoperabiliteit. Dit is nodig om snel en eenvoudig ondernemingen aan te sluiten op een Platform Infrastructuur (zie bijlage B).

A.2 Autoriteiten en ondernemingen - conceptueel

Deze paragraaf gaat kort in op welke wijze autoriteiten en ondernemingen conceptuele interoperabiliteit kunnen hanteren.

Autoriteiten houden (met risicoanalyse) toezicht op data die logistieke stromen representeren en verrichten waar nodig fysieke inspecties. Zij ‘piggy backen’ op data van ondernemingen, al dan niet met een push of pull (berichten) mechanisme, waarbij het pull mechanisme ondersteund kan worden met events/alerts. Willen autoriteiten direct gebruik maken van data uit de Platform Infrastructuur, dan zal de semantiek van die data bekend moeten zijn, evenals de syntactische weergave. Vanuit hun taakstelling zullen autoriteiten eisen stellen aan de benodigde data. Toezicht op veiligheid van een vervoermiddel stelt bijvoorbeeld andere eisen dan toezicht op transport van gevaarlijke lading. Het gezichtspunt van autoriteiten moet daarmee geïntegreerd worden in het logistieke gezichtspunt. Het tweede punt in de figuur in het begin van deze bijlage geeft aan dat autoriteiten hun gezichtspunten kunnen toevoegen.
Uitgangspunt is dat autoriteiten geen aanvullende eisen opleggen in de vorm van groepering of coderingen (dus: geen Harmonised Systems code (HS-code)) voor groepering. Internationaal zijn bijvoorbeeld de douanes overeengekomen deze HS-code te gebruiken om geen onderscheid tussen gelijksoortige producten van verschillende producenten te maken. Een televisie heeft daarom één HS-code, ongeacht de producent van een televisie die zijn eigen productcode heeft. Automatische detectie van groeperingen door op patroonherkenning gebaseerde risico analyse kan voorkomen dat een extra codering nodig is.

Autoriteiten kunnen eventueel de patronen die ze herkennen vanuit risicoanalyse te koppelen aan logistieke diensten van ondernemingen. Dat zou impliceren dat logistieke diensten gepaard gaan met een vorm van certificering, waarbij vanuit transacties met andere partijen inzichtelijk wordt of deze voldoen aan de gepubliceerde diensten. Een dergelijke vorm van certificatie zou ook nog gekoppeld kunnen worden aan data over klanten en/of interne validatieprocessen om nieuwe transacties met (on)bekende klanten aan te gaan.

Ondernemingen maken gebruik van (vraag) en/of bieden logistieke diensten aan (aanbod). Transport, opslag en overslag zijn voorbeelden van logistieke diensten. Deze diensten hebben verschillende kenmerken, waarbij waarden voor die kenmerken refereren naar fysieke objecten met hun eigenschappen.
Logistieke diensten hebben ook een (on)bepaalde levensduur en/of zijn niet op alle (werk)dagen beschikbaar. Een onderneming kan gedurende zijn bestaan bijvoorbeeld transportdiensten leveren met een bepaalde modaliteit (b.v. wegvervoer), maar kan ook zogenaamde timetables aanbieden (denk aan slots voor overslag, voyage schemes voor schepen, etc.). Timetables kunnen een beperkte levensduur hebben, zij kunnen bijvoorbeeld jaarlijks wisselen. Vervolgens kan op een reis of rit nog capaciteit beschikbaar zijn die als (tijdelijke) logistieke dienst wordt aangeboden. In het laatste geval is de capaciteit eenmalig beschikbaar.

Diensten hebben dus kenmerken. Transportdiensten hebben bijvoorbeeld de volgende kenmerken:

- Tijdsduur: hoelang neemt een dienst in beslag. De tijdsduur heeft een relatie tot de modaliteit en de regio's waartussen de dienst wordt geleverd.
- Regio's (geografie): tussen welke regio's en/of langs welke corridor wordt de dienst geleverd. Dit kan een land zijn, maar ook tussen twee landen of tussen regio's in verschillende landen. Het concept 'locatie' dient dus goed gespecificeerd te worden en is ruimer dan een fysieke plaats.
- Soort goederen: dit zijn de objecten die vervoerd kunnen worden, zoals 'cargo' of bulklading, al dan niet vervoerd met containers (als equipment, denk ook aan dry – en liquid bulk containers voor bijvoorbeeld chemicaliën).
- Kenmerken van de goederen: dit zijn specifieke eisen die een aanbieder van diensten stelt aan het vervoer van het soort goederen. Deze eisen worden veelal omgezet in specifieke tarieven, bijvoorbeeld aparte tariefklassen gekoppeld aan gewichtsklassen of omvang van de goederen. In het algemeen worden in logistiek tarieven niet (open) gepubliceerd, zodat hier alleen onder- en bovengrenzen van gewichten en afmetingen gelden. Aanvullend is er een indicatie of er gevaarlijke lading en/of koellading getransporteerd kan worden.

Veelal hebben LSPs aanvullende diensten aan hun basisdiensten, bijvoorbeeld het opmaken van de benodigde documenten of betalen van vrachtkosten. Deze zijn als administratieve diensten te vermelden. Overslag kent als aanvullende dienst (tijdelijke) opslag; dit gaat veelal in na enkele dagen. Andere diensten zijn het aanbieden van inhuur van gekwalificeerd personeel, het wisselen van de juiste locomotief voor internationaal railvervoer, etc. Deze laatste vorm van diensten zou eigenlijk in het tarief opgenomen moeten zijn, maar wordt vermeld om transparantie van tarieven inzichtelijk te maken.

Het zal blijken dat LSPs moeite hebben hun diensten op een gestructureerde wijze weer te geven. Mogelijk kost het veel inspanning om deze diensten eenduidige te specificeren. Veelal zijn deze diensten ook impliciet, ze worden altijd afgesproken met klanten tijdens een onderhandeling over tarieven, al dan niet binnen een raamcontract. Er zijn verschillende aanpakken om logistieke diensten expliciet te maken:

- Voor zogenaamde 'timetables' is er geen probleem. Deze worden vaak al gepubliceerd.

- Vanuit de beschikbare assets en de interne processen is veel af te leiden over de vorm van dienstverlening. Een vervoermiddel is bijvoorbeeld alleen geschikt voor containertransport, een ander voor bulk, etc. Een terminal heeft bijvoorbeeld alleen kranen en processen voor overslag van containers met een aansluiting op spoor, weg en binnenvaart. De processen zeggen iets over de regio's en klanten die worden bediend.
- De order- en facturatiehistorie bevat alle diensten die een onderneming heeft geleverd en dus ook kan leveren. Data mining op deze historische orderdata geeft patronen die de basis zijn voor logistieke diensten.

A.3 Autoriteiten en ondernemingen - technisch

Toepassing van conceptuele interoperabiliteit betekent voor een dienstverlener (aanbodzijde) de volgende twee stappen:

1. Registreren ('register'): eenmalige registratie bij (een node van) de Platform Infrastructuur en publicatie van vraag naar en/of aanbod van logistieke diensten en beleid rond het delen van data (data policy) om zo direct transacties via de Platform Infrastructuur elektronisch af te handelen. Een geregistreerde onderneming moet vindbaar zijn via elke node van de Platform Infrastructuur. Dit zijn de diensten 'Profile registration' en 'Data policy specification' (zie bijlage B).
2. Aansluiten ('connect'): het inrichten van een Access Point om interne ICT systemen te koppelen aan (een node van) de Platform Infrastructuur. Door de eenmalige koppeling met de Platform Infrastructuur is het mogelijk data vanuit de eigen ICT systemen te ontsluiten en te delen met ICT systemen van andere ondernemingen via de Platform Infrastructuur. Dit is de ondersteunende dienst 'Infrastructure Connection' (zie bijlage B).

Vanuit de vraagzijde naar logistieke diensten kan een onderneming zich ook registreren en verbinden met een node. Bij registratie wordt het vraagpatroon aan diensten vastgelegd met de behoefte aan specifieke data, bijvoorbeeld in de vorm van milestones tijdens de uitvoering van logistieke processen. Niet alleen vragen om logistieke diensten worden gekoppeld aan aanbod; dit geldt ook voor een databehoefte en – aanbod.

Een autoriteit kan zijn interne ICT systeem (systemen) zich ook registreren bij en verbinden aan (een node van) de Platform Infrastructuur. Registratie is vanuit de taakstelling met de daarbij horende databehoefte. Deze databehoefte is gekoppeld aan een object met daarbij het gezichtspunt van dat object (zie eerder). Bij registratie vanuit de aanbodzijde zullen ondernemingen moeten voldoen aan deze databehoefte en dit meenemen in de specificatie van hun data policy.

Enerzijds zullen organisaties hun data policies hebben, al dan niet opgelegd door autoriteiten of gekoppeld aan klantvragen, anderzijds dient die policy toegepast te worden op een fysiek object. Wie mag bijvoorbeeld de locatie en inhoud van een container weten, zonder dat die betreffende organisatie een directe transactie heeft met de organisatie die de data verschaft. Binnen het iShare project wordt hier gewerkt aan machtigingen, wat mogelijk resulteert in een token om toestemming te krijgen tot toegang van data (de pull variant).
Het gebruik van machtigingen impliceert dat een onderneming continue kijkt of een nieuwe milestone, van bijvoorbeeld een container, beschikbaar is gedurende de geldigheidsduur van een machtiging. Mogelijkerwijs wil een organisatie hier alerts

voor inrichten (push gecombineerd met pull), maar moet die organisatie ergens aangeven dat hij zich wil abonneren op milestones van een specifiek object. Het abonnement kan via een machtiging tot stand komen, waarna vervolgens de alerts ontvangen worden zodra ze beschikbaar komen. Regels voor abonnementen kunnen worden afgesproken tussen organisaties, maar mogelijk zijn deze regels ook in een gemeenschap af te spreken. Denk aan zich steeds herhalende patronen voor containeroverslag door een terminal en daarbij horende abonnementen op milestones. Dit soort gemeenschapsregels kan een onderneming ook meenemen bij het vaststellen van zijn data policy. Een organisatie kan ook worden uitgenodigd voor een abonnement of dit zelf aanvragen. Dit abonnement kan voor één enkel object, bijvoorbeeld een container of een schip (dynamisch abonnement).

Community management – en Identification and Authentication diensten (bijlage B) ondersteunen deze mechanismen van machtigingen, gemeenschapsregels en dynamisch abonnementen.

A.4 Conclusies

Deze bijlage geeft een verkenning van conceptuele interoperabiliteit om dynamisch ketens samen te stellen in logistieke netwerken en synchromodaliteit te realiseren met een werkwijze voor autoriteiten en ondernemingen. Er is al aangegeven dat de Platform Infrastructuur hiervoor bepaalde functionaliteit biedt. Deze functionaliteit wordt in de volgende bijlage toegelicht, ook om witte vlekken in het aanbod van functionaliteit te identificeren.

Bijlage B – Platform Infrastructuur raamwerk

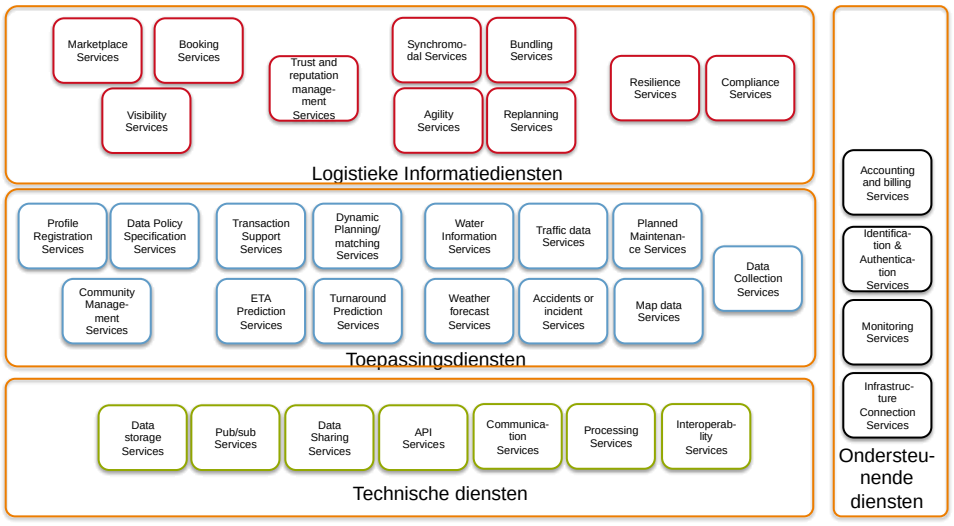
Hoofdstuk 3 geeft de terminologie voor een Platform Infrastructuur, bijlage A formuleert een aantal diensten voor conceptuele interoperabiliteit. Deze bijlage geeft een overzicht van mogelijke diensten van de Platform Infrastructuur en gaat in op de koppeling tussen verschillende nodes die deze diensten leveren (het protocol). Daarnaast wordt ook aangegeven op welke wijze deze diensten door leveranciers van bestaande nodes worden geleverd. Het raamwerk van diensten tracht daarmee een structuur te zijn om verschillende oplossingen onderling te vergelijken.

B.1 Platform Infrastructuur Diensten

Platform Infrastructuur Diensten vormen de basis voor ontwikkeling van innovatieve logistieke toepassingen. Uniformiteit in diensten maakt het mogelijk om toepassingen op smart devices voor het MKB te ontwikkelen, afhankelijk van de categorie van diensten van de Platfrom Infrastructuur.
Diensten zijn in vier categorieën in te delen:

- **Technische Diensten**: diensten van technische componenten, bijvoorbeeld communicatie -, opslag -, data uitwisselings- en API diensten. Deze diensten valideren ook veelal de correctheid van data op syntax niveau (voldoet de structuur, zijn er ontbrekende elementen, hebben velde de goede waarde, etc.).
- **Toepassingsdiensten**: diensten van toepassingen voor data delen in de logistiek, bijvoorbeeld een registry voor opslag en beheer van logistieke profielen, transactieondersteuning en voor dynamisch plannen van logistieke ketens.
- **Logistieke Informatiediensten**: diensten die logistieke bedrijfsprocessen verbeteren zoals visibiity, agilty, resilience, logistieke markt, en boekingsdiensten. Dit zijn voor eindgebruikers relevante diensten. Logistieke Informatiediensten gebruiken Toepassingsdiensten.
- **Ondersteunende Diensten**: deze diensten zijn gericht op de ondersteuning van de werking van een node in de Platform Infrastructuur, zoals Identity en Authenticatie (denk aan iShare), monitoring, facturatie en node beheer.

De volgende figuur doet een voorstel voor invulling van de soorten diensten, waarbij geen onderscheid naar het soort platform wordt gemaakt.



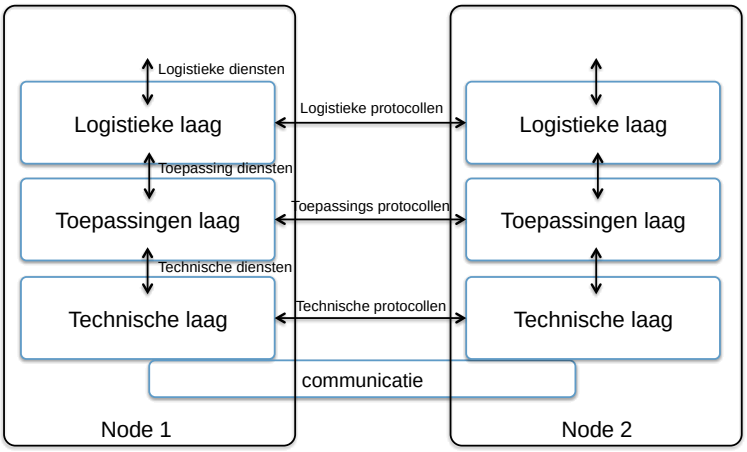
Niet alle nodes zullen alle logistieke informatiediensten leveren. Mogelijk leveren nodes ook alleen eenvoudige versies van logistieke informatiediensten, zoals de mogelijkheid om berichten als boekingen en transportopdrachten uit te wisselen. Er zullen ook nodes zijn die alleen visibility diensten leveren, al dan niet gebaseerd op events. Binnen het EU FP7 SEC CORE project ontwikkeld Maersk een dergelijke dienst, gebaseerd op door het project ontwikkelde (defacto) standaarden.
Veel toepassingsdiensten zijn nodig voor de logistieke informatiediensten, terwijl technische diensten ook voor meerdere toepassingsdiensten inzetbaar zijn. De inrichting van de toepassingsdiensten zal afhankelijk zijn van logistieke informatiediensten. Registratie van een gebruiker met zijn beschikbare data is bijvoorbeeld anders voor berichten gebaseerde transacties dan voor uitwisseling van events met logistieke milestones.

Als autoriteiten besluiten data te verzamelen van het bedrijfsleven via toegang tot die data, zullen deze autoriteiten aangeven bij welke diensten ze aansluiten. Ze kunnen bijvoorbeeld aangeven ook de logistieke milestones met events te ontvangen of order data te krijgen. Autoriteiten ‘tappen’ als het ware logistieke data af door logistieke informatiediensten te monitoren (‘piggy backing’). Als deze diensten op private nodes draaien, kan een autoriteit real time monitoring en analyse verrichten om direct waarschuwing af te geven.

B.2 Platform Infrastructuur Protocol

Elk van de Platform Infrastructuur Diensten kan door één of meer nodes geboden worden. Deze nodes maken nu onderling afspraken over integratie vanuit een behoefte van een klant. Er zijn pogingen ondernomen om nodes onderling te verbinden, bijvoorbeeld in EPCSA (European Port Community System Association) of door ze onderling te koppelen met een gateway (zie ook bijlage C).

Het Platform Infrastructuur Protocol is een stelsel van afspraken om implementaties van diensten door verschillende nodes onderling te verbinden. Er is een onderscheid te maken tussen technische - , toepassings- en logistieke protocollen. Niet alle protocollen zijn volledig technisch van aard. Visibility als logistieke dienst kent bijvoorbeeld afspraken over lokatie en mogelijk snelheid van een object (‘descriptive’ visibility), onderscheiden van specifieke objecten en mogelijke milestones of het interpreteren van disrupties (‘diagnostic’ visibility) of berekening van een Estimated Time of Arrival gebaseerd op mogelijke vertragingen, omleidingen (‘predictive’ visibility).



Elke dienst op een bepaald niveau wordt ingevuld door software op een laag, waarbij die software het protocol met een andere laag implementeert en diensten aan een hogere laag biedt.
De technische laag bevat een component om data sharing diensten te leveren. Deze component kan bijvoorbeeld berichten conform de EDIfact standaard uitwisselen met een andere node, waarbij die andere node wel de berichten moet kunnen verwerken. EDIfact standaard is dan het protocol geworden voor data sharing tussen twee nodes. De component die data sharing levert kan complex zijn door bijvoorbeeld bestanden uit interne systemen in andere formaten te combineren tot één EDIfact bericht, terwijl een ontvangende component hetzelfde bericht omzet in één bestand met een ander formaat. De huidige implementaties voor elektronisch data delen hebben veelal impliciet het technisch protocol gespecificeerd als EDIfact of XML berichten.

B.3 Bestaande nodes en hun dienstverlening

Dit rapport onderscheid twee soorten nodes:

1. Integratienodes (horizontale nodes): deze bieden Technische Diensten als data sharing (berichten en/of alerts/events met abonnementen (zogenaamde publish/subscribe oplossingen)) - , interoperability (datatransformatie) – en communicatiediensten. Om dit goed te kunnen hebben ze eigen Identificatie en Authenticatie - (veelal gebruikersnaam, wachtwoord voor portals, gecombineerd met server certificaten), monitoring - en accounting and billing diensten. Daarnaast moeten gebruikers zich registreren en een keuze maken uit een template van berichten (met standaarden) die ze ondersteunen (soort van community template voor rollen). Vanuit eigendom en zeggenschap zijn hier commerciële nodes als Descartes met zijn Global Logistics Network (GLN) en community nodes als Portbase te onderscheiden. Bij community nodes liggen de te gebruiken standaarden en hun implementatierichtlijnen vast; commerciële dienstverleners bieden de optie om willekeurige standaarden te ondersteunen.
   Dit zijn ook wel horizontale nodes te noemen, omdat zij zich onderscheiden op een bepaald niveau van diensten. Een community node als Cargonaut die in eerste instantie technische diensten bood, heeft zich (deels) ontwikkeld tot een toepassingsnode; TransFollow biedt zogenaamde non-repudiation diensten die onderdeel zijn van monitoringdiensten met daarbij registratie van gebruikers.
2. Toepassingsnodes (vertical nodes): deze bieden één of meer Logistieke Diensten met daaronder de benodigde Toepassings- en Technische Diensten. We maken hier een onderverdeling naar:
   a. Logistieke marktplaatsen vormen zogenaamde tweezijdige platformen. Transportmarketplace en Uber4Freight brengen partijen samen (implementatie van marktplaatsdiensten), waarbij Uber4Freight ook de volledige financiële afhandeling verricht. Meer traditionele logistieke marktplaatsen done dit niet.
   b. Booking en visibility nodes: partijen die een combinatie van booking – en visibility diensten bieden. Daarbij kunnen ze zich richten op een bepaalde (deel)sector zoals zeetransport (INNTRA die integreert met alle reders en verladers ondersteunt in hun

boekingen en zichtbaarheid) of een bepaald type lading (denk aan TEUBooker voor achterland transport van containers).

c. Visibility nodes: er zijn ook partijen die alleen visibility bieden. In het railtransport zijn er bijvoorbeeld ook nodes met visibility diensten volgens een ingeregelde governance structuur: Rail Net Europe levert visibility op treinniveau aan alle Railway Undertakings die een trein rijden op de infrastructuur en Raildata levert aan een afgeschermde groep rail operators visibility van wagons en treinsamenstelling. River Information Services bieden visibility via AIS, waarbij toegang tot AIS data van binnenvaartschepen afgeschermd is; MarineTraffic biedt visibility voor zee- en binnenvaartschepen met AIS. Andere voorbeelden zijn Transics en Astrata voor zogenaamde On Board Units (OBUs) voor vrachtwagens die data diensten leveren. In toenemende mate komen er ook sensorleveranciers die visibility leveren via LoRa en/of 5G netwerken.
d. Registry nodes: dit betreft nodes die alleen een registry bijhouden van ondernemingen en bepaalde aspecten rond data deling van die ondernemingen. Stichting Focafet ontwikkelt een Registry voor identificatie van willekeurige objecten (DENARS) en GS1 heeft een globale productcatalogus met (verwijzingen naar) alle productcodes.
e. Bundling nodes: de mogelijkheid om lading en/of transport capaciteit te bundelen om zo kosten te besparen, beladingsgraad te verhogen, etc. Dit wordt ook wel Cross Chain Collaboration of Control Center genoemd (4C). Voorbeelden van leveranciers zijn IDS (idsnl.com) en Tri-Vizor (trivizor.com). Dit zijn zogenaamde toepassingsnodes. De functionaliteit is te beschouwen als die van een (complex) logistieke marktplaats met boekingsfunctionaliteit, maar nu door vraag van meerdere klanten te bundelen met aanbod van meerdere dienstverleners. Een leverancier als Marlo levert hiervoor algoritmes (MixMoveMatch algoritme).
f. Dynamische planning nodes: dit is een vorm van nodes die dynamische ketenplanning ontwikkelen. Veelal komen ze voort uit visibility nodes. LogitOne is een voorbeeld van een leverancier van dit soort nodes; leveranciers als PTV bieden dynamische planningsalgoritmes.

Logistieke marktplaatsen en Bookings- en visibility nodes zijn veelal ingericht op het samenbrengen van één aanbod met één vraag voor één traject (ook wel ‘leg’ genoemd in een keten). Zogenaamde bundling functionaliteit voor die leg (meerdere vragen combineren met willekeurig aanbod) worden beperkt ondersteund. Decompositie van een vraag in een keten van meerdere legs is nog niet mogelijk, hoewel hier al wel eerste aanzetten voor algoritmes zijn.

Er komen in toenemende mate ook leveranciers van toepassing specifieke diensten zoals ETA voorspelling. Zij gebruiken visibility diensten om met data analytics ETA voorspellingen te maken (bijvoorbeeld Transics en Simacan).

Naast deze functionele nodes zijn er ook nog twee andere vormen van dienstverlening, te weten:

1. Node deployment leveranciers: er is een aantal leveranciers van Technische Diensten die vanuit het perspectief van data delen via Application Programming Interfaces (APIs) een platform aanbieden voor ontwikkeling en deployment van toepassingen. Een gebruikersgroep kan de toepassingen ontwikkelen, waarna de leverancier voor de ontwikkeling en deployment zorgt. Een voorbeeld is Nalian die met gebruikers op Zaventem bijvoorbeeld BruCargo heeft ontwikkeld. Een ander voorbeeld is Oracle. Oracle ontwikkelt een gelijksoortige dienst in als Descartes GLN, maar gebaseerd op het zogenaamd UETP protocol van Stichting Focafet. Binnen een TKI programma worden eerste toepassingen ontwikkeld, waarvoor ook een governance structuur gelijksoortig als BruCargo wordt ingericht.
2. Node leveranciers: dit betreft leveranciers van functionaliteit om technische diensten voor logistiek te realiseren. De volgende indeling is te hanteren:
    a. Integratiecomponenten: API management oplossingen of Enterprise Service Busses (ESB) als Commercial Of The Shelve (COTS) of open source oplossingen. Deze kunnen de basis vormen voor de inrichting van alle vorige varianten. Open source componenten zijn bijvoorbeeld gebaseerd op de defacto standaard voor Message Queueing, ontwikkeld door IBM. Binnen het EC H2020 Aeolix project wordt hiervoor een node ontwikkeld met publish/subscribe diensten voor het delen van events met een eigendoms- en zeggenschapsstructuur. Niet alleen IT leveranciers als Oracle, Microsoft, IBM, Tibco en anderen bieden deze oplossingen, er zijn ook oplossingen gericht op enkelvoudige Logistieke Diensten, bijvoorbeeld de zogenaamde EPCIS server voor het inrichten van visibility diensten. Node leveranciers hebben veelal verschillende implementatie – en deployment partners, zogenaamde Integration Service Providers.
    b. FiWare: het Public Private Partnership (PPP) Future Internet (een samenwerking tussen de Europese software industrie getrokken door Atos Spanje en de Europese Commissie) een aantal open source componenten opgeleverd (zogenaamde FiWare) die inzetbaar zijn node. Een deployment partner als Civity heeft FiWare toegepast voor het inrichten van een node. De verwachting is dat FiWare een langzame dood zal sterven, aangezien er geen actieve ontwikkelgemeenschap is.
    c. CEF Building Blocks: de Europese Commissie heeft zogenaamde Connecting European Facilities (CEF) building blocks ontwikkeld, waarvan eDelivery Technische Diensten voor beveiligde uitwisseling van data biedt gebaseerd op de open standaard electronic business XML Messaging Service (ebMS). Een ander building block is eIDAS, relevant voor het iShare project.

Hoewel veel van dit soort nodes overlappende functionaliteit hebben, is het niet eenvoudig ze aan elkaar te verbinden. Vanuit hun dienstverlening hebben ze eigen interne datastructuren en functionaliteit ontwikkeld, waarbij geen van deze datastructuren gedocumenteerd is.

B.4 Conclusies

Er is een veelheid van nodes met verschillende eigendom – en zeggenschapstructuren op de markt aanwezig, waarbij de diensten van de nodes onderling verschillen en deze nodes alleen bilateraal koppelen. Een Platform Infrastructuur is er daarmee niet. Hiervoor is het nodig invoeringsscenario's verder te onderzoeken (zie bijlage C).

Het ontwikkelde raamwerk om functionaliteit en koppeling van nodes te beschrijven kan nog verder uitgewerkt worden, bijvoorbeeld tot Application Programming Interfaces, bijvoorbeeld voor visibility diensten waar nog geen standaarden voor logistiek zijn.

Bijlage C Invoeringsscenario's

In de context van dit rapport is invoering gericht op deployment van de Platform Infrastructuur diensten door meerdere leveranciers met conceptuele interoperabiliteit. Dit laatste impliceert dat een organisatie zich eenmalig registreert en aansluit bij een node om vervolgens zaken te kunnen doen (zie bijlage A). Deze bijlage geeft een aantal invoeringsscenario's met hun voor- en nadelen.

C.1 Mogelijke scenario's

Traditioneel wordt voor de invoering van nieuwe ICT middelen een onderscheid gemaakt tussen een zogenaamd 'big bang' en 'winkel is open tijdens verbouwing' scenario (verbouwingsscenario) met meerdere tussenvormen. De volgende scenario's worden nader toegelicht, waarna in de volgende paragraaf een afgewogen keuze wordt voorgesteld:

- Big bang
- Verbouwing
- Verrijken
- Nieuwkomers
- Encapsulation
- Gateway

Het big bang scenario impliceert dat alle gewenste functionaliteit op hetzelfde ogenblik in gebruik wordt genomen. Dit scenario gaat uit van volledige vervanging van huidige nodes door nieuwe functionaliteit. Alle betrokkenen dienen overeenstemming te krijgen over functionaliteit en planning van vervanging. Er dienen ook afspraken gemaakt te worden over eventuele vertragingen tijdens ontwikkeling.

Het verbouwingsscenario wordt gekenmerkt door een roadmap van functionaliteit die stapsgewijs wordt ingevoerd, bijvoorbeeld ook door het upgraden van bestaande diensten naar standaarden met hun APIs. Deze roadmap is in te richten vanuit bijvoorbeeld invoering van logistieke diensten, waarna toepassingen en techniek zal volgen. Alle betrokkenen hebben overeenstemming over de roadmap en voeren deze ook conform afspraak in.

Verrijken is het oplossen van een deel van de uitdagingen, te weten alleen conceptuele interoperabiliteit. Hiervoor is het nodig zogenaamde Registry Nodes te ontwikkelen voor conceptuele interoperabiliteit, inclusief Registry Diensten en –Protocol voor delen van profielen, en zorgen dat organisaties eenmalig kunnen aansluiten bij een node. Dit laatste impliceert dat vanuit conceptuele interoperabiliteit verschillende (open) standaarden en implementatierichtlijnen van die standaarden ondersteund moeten worden. Het gaat daarbij vooral om de (automatische) generatie en beheer van transformaties tussen verschillende structuren en mechanismen. Alle nodes hanteren hier het (impliciete) berichtenprotocol om onderling te koppelen.

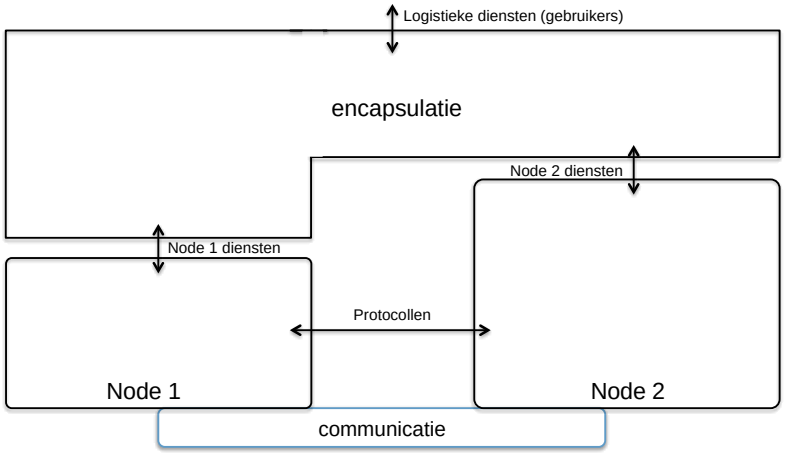
Het type Registry node dat hier gerealiseerd wordt kan ook de basis zijn voor dynamische ketenmodellering. Immers, het aanbod van diensten met mogelijke Key Performance Indicators kan ook toegevoegd worden. Naast samenstelling van

ketens is het ook mogelijk ketens op hun performance te beoordelen en te kiezen. Gecombineerd met beschikbare capaciteit is dan een keuze uit een (onderdeel van een) keten te maken.

Het nieuwkomerscenario is gebaseerd op nieuwe leveranciers (nieuwkomers) die zich zeer waarschijnlijk onderscheiden door het hanteren van nieuwe, disruptieve technologie, bijvoorbeeld

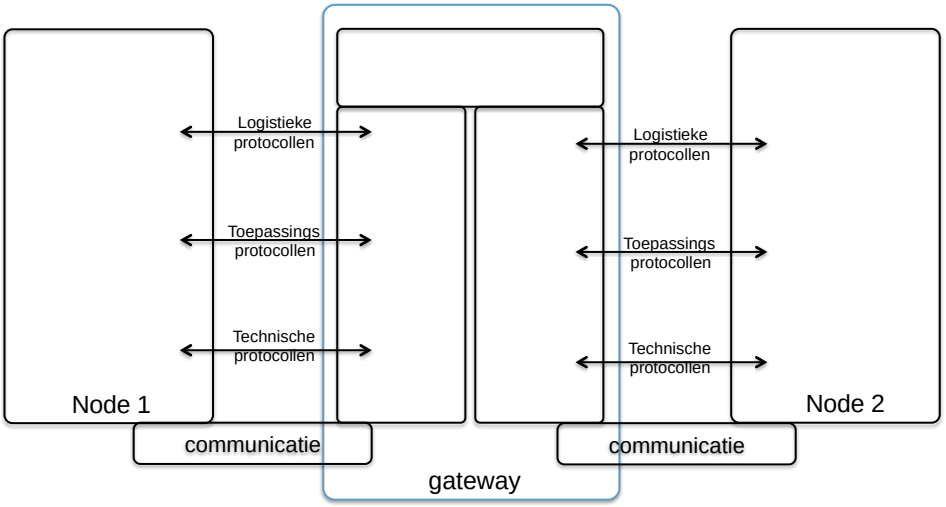
- Toepassing van blockchain technologie voor het invullen van de technische diensten. De verwachtingen zijn hoog, maar blockchain technologie voor logistiek vereist nog het nodige onderzoek en ontwikkeling en zal dus niet snel beschikbaar komen (deze bewering is gebaseerd op intern TNO onderzoek naar toepasbaarheid van blockchain technologie voor logistieke toepassingen). Er zijn al wel eerste ontwikkelingen van toepassingen voor documenten als Bills of Lading, die waarschijnlijk ook bruikbaar zijn voor eCMR.
- Voortbouwen op autonoom opererende objecten als voertuigen (AGVs, vrachtwagens, (binnenvaart)schepen) en andere assets (kranen, sorteer- en distributiecentra, warehouses). Deze autonome objecten hebben een noodzaak voor data; producenten van deze objecten zullen nodes gaan leveren met de door hen benodigde functionaliteit om deze objecten optimaal in te zetten tijdens productie.

Een volgend scenario is de ontwikkeling van een tijdelijke oplossing door het inpakken ('encapsulation') van diensten van individuele nodes tot een (sub)set van nieuwe diensten zoals die nodig zijn voor conceptuele interoperabiliteit. Er ontstaat een 'nieuwe etalage en toonbank van de huidige winkel'. Deze aanpak werkt het best voor nodes die Technische Diensten leveren, bijvoorbeeld voor het uitwisselen van data.
De volgende figuur toont twee nodes met een verschillend niveau van interoperabiliteit. Om het vereiste, gemeenschappelijk gewenste niveau te bereiken zullen de diensten van beide nodes verpakt worden.



Verbinden van nodes voor het delen van data tussen de gebruikers van die nodes via een zogenaamde gateway is een volgend scenario. Een gateway zorgt voor de nodige transformaties tussen de protocollen. Functionaliteit van een gateway kan zich beperken tot de technische protocollen, bijvoorbeeld het vertalen tussen een EDIfact - en een XML bericht. Het Descartes GLN netwerk (zie paragraaf B.3) is

een vorm van gateway voor berichten. Voor de integratie tussen systemen van luchthavens wordt op dit moment ook een gateway ontwikkeld door Ericsson. De eIDAS component van de CEF building blocks is ook een vorm van een gateway, maar dan tussen kenmerken om een identiteit te bepalen.
Het NLIP iShare project heeft als doelstelling om Identiteit en Authenticatie van gebruikers van verschillende nodes te regelen. Dit kan zonder een gateway als de verschillende nodes dezelfde protocollen hanteren en overeenstemming hebben over het te hanteren Identity Scheme. Als dat niet het geval is, dient een gateway ontwikkeld te worden.



C.2 Overwegingen voor een keuze

De volgende tabel geeft aan in hoeverre de verschillende scenario's leiden tot een Platform Infrastructuur met conceptuele interoperabiliteit. Daarbij wordt een inschatting van de haalbaarheid gegeven.

Scenario	Platform Infrastructuur	Conceptuele Interoperabiliteit	Haalbaarheid
Big Bang	X	X	-
Verbouwing	X	X	-
Verrijking	+	X	++
Nieuwkomer	?	?	++
Encapsulatie	X	X	+/-
Gateway	X	-	+

De haalbaarheid is als volgt onderbouwd:

- Een <u>big bang</u> scenario is vrijwel onhaalbaar door het groot aantal organisaties dat al data deelt, met of zonder 'nodes' die hierin geïnvesteerd hebben en/of beschikbare standaarden. Het betekent dat alle nodes gelijktijdig over moeten naar nieuwe functionaliteit met mogelijk heraansluiting van hun gebruikers. Dit is ook niet wenselijk voor alle nodes, denk aan toepassingsnodes (bijlage B) die geen of geringe noodzaak hebben over te gaan op nieuwe logistieke diensten.

Mogelijkerwijs is dit scenario wel in te voeren met een beperkt aantal leveranciers van nodes, zoals dit bijvoorbeeld getracht wordt in het NLIP. Dit geeft echter onvoldoende zicht op een Europese oplossing, laat staan een wereldwijde oplossing.

- Verbouwing van bestaande nodes is vrijwel onhaalbaar, volgens dezelfde argumenten als het big bang scenario. Alleen als de node leveranciers een bedreiging van nieuwkomers voelen, zullen ze overgaan tot dit scenario. Leveranciers van toepassingsnodes (bijlage B) zijn niet gebaat bij dit scenario, omdat leveranciers van integratienodes gelijksoortige functionaliteit gaan leveren.
- Verrijking biedt slechts ten dele de gewenste functionaliteit, maar maakt optimaal gebruik van wat er al is en voegt daar nieuwe functionaliteit aan toe. Het kan ook nieuwe logistieke diensten leveren. Leveranciers van toepassingsnodes krijgen hiermee geen concurrentie van leveranciers van integratienodes die hun functionaliteit verrijken met logistieke diensten. Daarmee is naar verwachting dit scenario acceptabel voor alle bestaande node leveranciers, hoewel er nog geen integratie is tussen de verschillende nodes voor logistieke diensten.
- Het nieuwkomerscenario vormt een bedreiging voor alle vormen van nodes (zie paragraaf B.3), zodra nieuwe node functionaliteit wordt ontwikkeld door leveranciers van autonome objecten. Een bekend voorbeeld is Apple die OEM voor automobielfabrikanten wordt als het zelf niet in staat is een autonoom rijdend voertuig te ontwikkelen. Een nieuwkomerscenario komt uit een volledig andere ontwikkeling en heeft dus niet noodzakelijk de vereiste diensten van een Platform Infrastructuur en/of conceptuele interoperabiliteit. Wel zal er een grote noodzaak voor conceptuele interoperabilteit zijn om snel en eenvoudig een autonoom object onderdeel te maken van de infrastructuur. Een nieuwkomerscenario biedt ook mogelijkheden als nieuwe leveranciers snel nieuwe produkten met standaarddiensten kunnen invoeren. Standaard diensten van een Platform Infrastructuur biedt nieuwkomers mogelijkheden.
- Het encapsulatie scenario vereist integratie met de verschillende node leveranciers. Dit is technisch een uitdaging en daarom is de haalbaarheid twijfelachtig.
- De gateway oplossing zorgt alleen voor vertalingen van protocollen en is nog steeds gebaseerd op bestaande mechanismen voor interoperabiliteit. Het is zeker haalbaar en vergt afstemming met de verschillende node leveranciers. Het vereist de invoering van een nieuwe organisatie met eigendom – en zeggenschapsstructuur.
  Gateway oplossingen om een Platform Infrastructuur te creëren zijn wel mogelijk als alle modaliteiten ook beschikken over nodes. Dit is echter niet het geval, ook omdat het merendeel van EU continentale transportondernemingen MKB is en zij bij voorkeur bediend moeten worden met een direct bruikbare toepassing. MKB ondernemingen hebben weinig of geen behoefte aan standaarden, zij willen oplossingen die voldoen aan standaarden.

C.3 Conclusie en aanbeveling

Uit voorgaande blijkt dat het nieuwkomer- en verrijkingsscenario het meest haalbaar zijn, waarbij we willen opmerken dat het nieuwkomerscenario zeker zal

plaatsvinden. Aanbod van standaard diensten versnelt de adoptie van produkten en diensten van nieuwkomers en biedt hen mogelijkheden. Met als uitgangspunt dat deze twee scenario's relevant zijn, gelden de volgende aanbevelingen:

1. Specificatie van de Platform Infrastructuur Diensten en – Protocol. Dit is vooral nodig voor het nieuwkomerscenario.
2. Ontwikkeling van conceptuele standaarden met een gedistribueerde governance structuur, ondersteunende hulpmiddelen en Registry Nodes voor conceptuele interoperabiliteit en bepaalde logistieke diensten zoals dynamische ketenplanning.
3. Afbeeldingen van conceptuele standaarden naar bestaande (open) standaarden en hun implementatierichtlijnen. Dit is vanuit het verrijkingsscenario van belang om aansluiting met bestaande oplossingen te realiseren.

Binnen de EU FP7 SEC Cassandra (2011-2014), EU FP7 INFSO iCargo (2011-2014), EU FP7 SEC CORE en H2020 SmartRail projecten zijn voor bovenstaande aanbevelingen eerste aanzetten tot specificatie van diensten met hun semantiek ontwikkeld.