

Bijlage 16

Toelichting VOR-IN

Gemeente Amsterdam

Opdrachtgever:	Verkeer & Openbare Ruimte Gemeente Amsterdam
Contractnummer:	AI 2021-0047
Versie:	1.1 met revisies uit Nvl 1 en 2
Datum:	13-09-2021

Inhoudsopgave

1	Over dit document.....	3
2	Inleiding	4
3	De datacentra	5
4	VOR-IN	6
4.1	Inleiding.....	6
4.2	Hosting omgeving.....	7
4.3	Toegang tot hosting omgeving	7
4.4	Dagelijks beheer	9
4.5	Modulariteit en standaardisatie virtualisatie-omgeving.....	9
5	Applicatieomgeving.....	12

1 Over dit document

Dit document geeft aan Inschrijvers relevante achtergrondinformatie en beschrijft op hoofdlijnen de huidige ICT keten waarbinnen de IDMA dient te gaan functioneren.

Deze achtergrondinformatie betreft onder andere het geheel van interne en externe systemen, software, databanken, koppelingen, apparatuur, ICT infrastructuur en hulpmiddelen die voor de Opdrachtgever de geautomatiseerde informatievoorziening vormt waarbinnen de IDMA ingepast wordt.

Bij discrepanties tussen dit document en het Programma van Eisen prevaleert het Programma van Eisen.

2 Inleiding

De afdeling Stedelijk Beheer van Verkeer en Openbare Ruimte beheert een fors areaal aan assets in de openbare ruimte. Het areaal bestaat onder meer uit verkeersregelininstallaties, parkeerverwijsdisplays, zichtcamera's, slimme sensoren, Dynamische Route Informatie Panelen, Kentekenherkenningscamera's en verzinkbare palen.

Voor het beheer en onderhoud wordt gebruik gemaakt van diverse applicaties die de assets van afstand kunnen monitoren en beheren. Veel van deze applicaties functioneren tevens als aansturing- en bedien-software voor de afdeling Verkeersmanagement. De verkeerskundigen configureren services met maatregelen en beoordelen de werking van de instrumenten, terwijl de verkeersleiding de verkeersdoorstroming monitoren en bijsturen als daar een aanleiding toe is.

De meeste assets zijn aangesloten op het industriële netwerk van de afdeling Stedelijk Beheer, het digitale hart van diverse applicatieketens. Deze ketens bestaan uit apparatuur zoals sensoren en displays geplaatst in de openbare ruimte, applicaties in het Datacenter, bedienposten en datakoppelingen met ketenpartners en leveranciers. De naam van dit netwerk en de bijbehorende hosting faciliteiten is Verkeer en Openbare Ruimte Intelligent Netwerk, kortweg: VOR-IN.

Deze netwerkomgeving is gebaseerd op 3 pijlers:

- Besturing
- Beveiliging
- Data

De verschillende assets kennen verschillen gebruikersgroepen, beheerders en applicaties, elk met hun eigen autorisaties. Een groep verkeersregelkundigen moet over het netwerk bij alle verkeersregelininstallaties kunnen komen, terwijl de ANPR camera's - voor de handhaving van de milieuzone - door een beperkt aantal andere gebruikers te beheren zijn. De assets zijn om redenen van Informatiebeveiliging van elkaar gescheiden.

De data die omgaan binnen deze assets zijn ook verschillend van aard. Vanuit beveiligingsperspectief mag geen ongecontroleerde vermenging ontstaan. De tweede pijler is daarom beveiliging en monitoring. Het netwerk, de daarop aangesloten serversystemen en de bedienposten moeten goed beveiligd worden tegen onrechtmatig gebruik. In sommige gevallen is sprake van de verwerking van privacy gevoelige gegevens en zijn aanvullende beschermende maatregelen noodzakelijk.

De derde pijler betreft data. De assets die in beheer zijn genereren data die voor onderhoud, besturing en analyse relevant zijn. Het inwinnen van data is niet langer een bijvangst vanuit beheer, maar is een structurele taak die doelbewust wordt ingeregeld in het kader van Dynamisch Verkeersmanagement.

In het kader van efficiënte data uitwisseling is een Enterprise Service Bus (ESB) aanwezig, die alle bericht gebaseerde datastromen tussen applicaties afhandelt. Applicaties dragen zorg voor het uitwisselen van data met het areaal, de doorgifte van data naar andere toepassingen en externe afnemers. Al deze datastromen lopen altijd via de ESB. Zo worden historische gegevens doorgezonden naar het Amsterdams Datapunt en actuele gegevens naar het NDW. Het datapunt stelt op haar beurt de data die voor analyse doeleinden bestemd is, voor zover dat toegestaan is, beschikbaar als open data via <https://data.amsterdam.nl/>.

3 De datacentra

De afdeling Stedelijk Beheer realiseert en beheert datacentra verspreid over meerdere locaties waarin de VOR-IN omgeving wordt gehost.

Het eerste, bestaande datacentrum bevindt zich in de huidige Verkeerscentrale van de gemeente Amsterdam. De verkeerscentrale is gesitueerd in het dienstengebouw van de IJ-tunnel, aan de Dijksgracht 1 in Amsterdam. Deze centrale bevindt zich aan de zuidzijde van het IJ.

Dit pand is niet vrij toegankelijk. Om toegang te verkrijgen dient u zich ruim voorafgaand aan elk bezoek aan te melden bij de Servicedesk VOR-IN, welke vervolgens een systeembeheerder toekent en een afspraak maakt om de benodigde werkzaamheden onder toezicht te kunnen uitvoeren. Contactgegevens van de Servicedesk VOR-IN worden na opdracht verstrekt aan Leverancier. Personen moeten geautoriseerd worden om meldingen te mogen doen aan de Servicedesk VOR-IN.

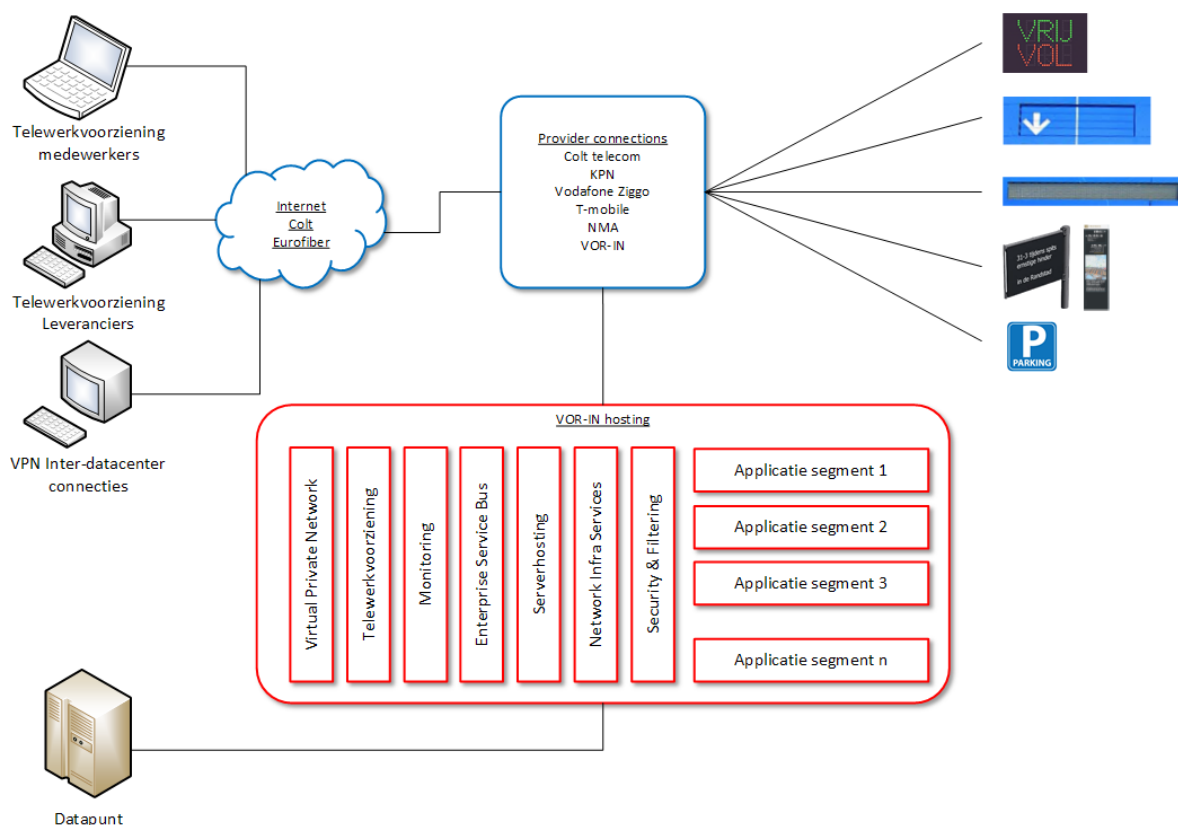
Sinds 2020 worden voorbereidingen getroffen voor een tweede data centrum, onder het Metrostation Noord aan de Nieuwe Leeuwarderweg. Deze locatie ligt aan de noordzijde van het IJ. De realisatie van het tweede datacentrum is gepland in de tweede helft van 2021.

De twee datacentra worden met meerdere zeer breedbandige glasvezelverbindingen met elkaar verbonden. Zij zijn tezamen als een stretched layer 2 datacentrum ingericht. Hierdoor is het mogelijk dat de virtualisatie omgeving gebaseerd op hyper-V technologie, ingericht op beide locaties, als één logisch datacentrum functioneert.

4 VOR-IN

4.1 Inleiding

De VOR-IN hosting omgeving bestaat uit diverse voorzieningen die het complete IT landschap vormen. Het IT landschap is in de volgende figuur schematisch en vereenvoudigd weergegeven, met daarin een beperkt aantal assets opgenomen.



Figuur 1: Schets Network

Het datacenter van Verkeer en Openbare Ruimte is gevestigd in een moeilijk toegankelijke locatie. De mogelijkheid om koppelvlakken met telecom providers te realiseren is daarom zeer beperkt. Het datacenter beschikt over hoogwaardige redundante Internetkoppelingen van Colt Telecom, KPN, Ziggo, T-Mobile en Netwerk Metro Amsterdam (NMA). Er zijn geen nieuwe koppelingen mogelijk.

Vanuit het perspectief van IT is een display een apparaat dat zich in de openbare ruimte bevindt en dat een netwerkverbinding met het datacenter onderhoudt. De (draadloze) dataverbinding wordt gebruikt voor het aansturen van het display, het onderhouden van de systeemsoftware en het overdragen van gewenste en actuele beelden en storingsmeldingen. De garages maken gebruik van draadloze of bedrade (ADSL) verbindingen.

4.2 Hosting omgeving

De hosting omgeving wordt gevormd door meerdere Hyper-V hyper converged cluster opstellingen op basis van Microsoft Windows Server 2016 of nieuwer. Op dit virtualisatie platform draaien zowel Virtuele machines op basis van Windows Server 2016 of nieuwer als ook Redhat Enterprise Linux (RHEL). Het standaard database platform is MS SQL. Er wordt gewerkt aan een bredere ondersteuning en andere aanvullende hosting faciliteiten, om de capaciteit te vergroten, de productie en acceptatieservers beter te scheiden en voor te sorteren op een stretched datacenter configuratie. Op het moment van schrijven van dit stuk kan daar nog geen definitieve toezegging over gedaan worden.

De virtuele machines maken gebruik van Infrastructuur faciliteiten van het VOR-IN netwerk. Te denken valt daarbij bijvoorbeeld aan tijdsynchronisatie, DNS en Internet faciliteiten.

4.3 Toegang tot hosting omgeving

Vanuit Informatiebeveiliging, reductie en beheer van het aantal koppelvlakken wordt een aantal eisen gesteld:

1. Data uitwisselingen over de grenzen van het VOR-IN netwerk zijn **daar waar mogelijk** altijd encrypted.
2. Koppelingen met ketenpartners en leveranciers vinden altijd plaats over een site-to-site IPSEC VPN verbinding.
3. Indien meer dan 1 datastroom met een ketenpartner of leverancier wordt opgezet, dan worden deze gecombineerd in één VPN verbinding.
4. Zelfs als gewerkt wordt met TLS encrypted verkeer en beveiligde API koppelingen blijft nog steeds eis 2 van kracht omwille van reductie en controle van de koppelvlakken.
5. De data uitwisselingen worden getoetst tegen de kaders van privacy wetgeving (AVG) en Informatiebeveiliging (BIO).

De Leverancier krijgt via de Telewerkvoorziening, die gebaseerd is op een Remote Desktop Protocol (RDP) sessie naar een management server in het applicatiesegment, toegang tot de omgeving waarvoor de Leverancier verantwoordelijk is. De toegang tot de telewerkvoorziening is gepersonaliseerd en beveiligd met een Azure 2-Factor autorisatie op basis van een App op de Smartphone van de support engineer. Het is niet mogelijk of toegestaan met groepsaccounts te werken. Activiteiten zullen door Opdrachtgever worden gelogd. Het aantal personen dat toegang krijgt wordt geminimaliseerd en nut & noodzaak wordt periodiek herzien. De lijst met geautoriseerde personen wordt zo vaak als nodig en ten minste jaarlijks herzien.

De management server wordt in overleg met de systeembeheerders ingericht met de noodzakelijke software die nodig is voor het beheer van het areaal en vervolgens ter beschikking gesteld. Het is niet toegestaan om remote access tools zoals bijvoorbeeld TeamViewer of (web) VPN verbindingen te gebruiken. Dit ondermijnt de beveiliging van de omgeving en vergroot de kans op een datalek.

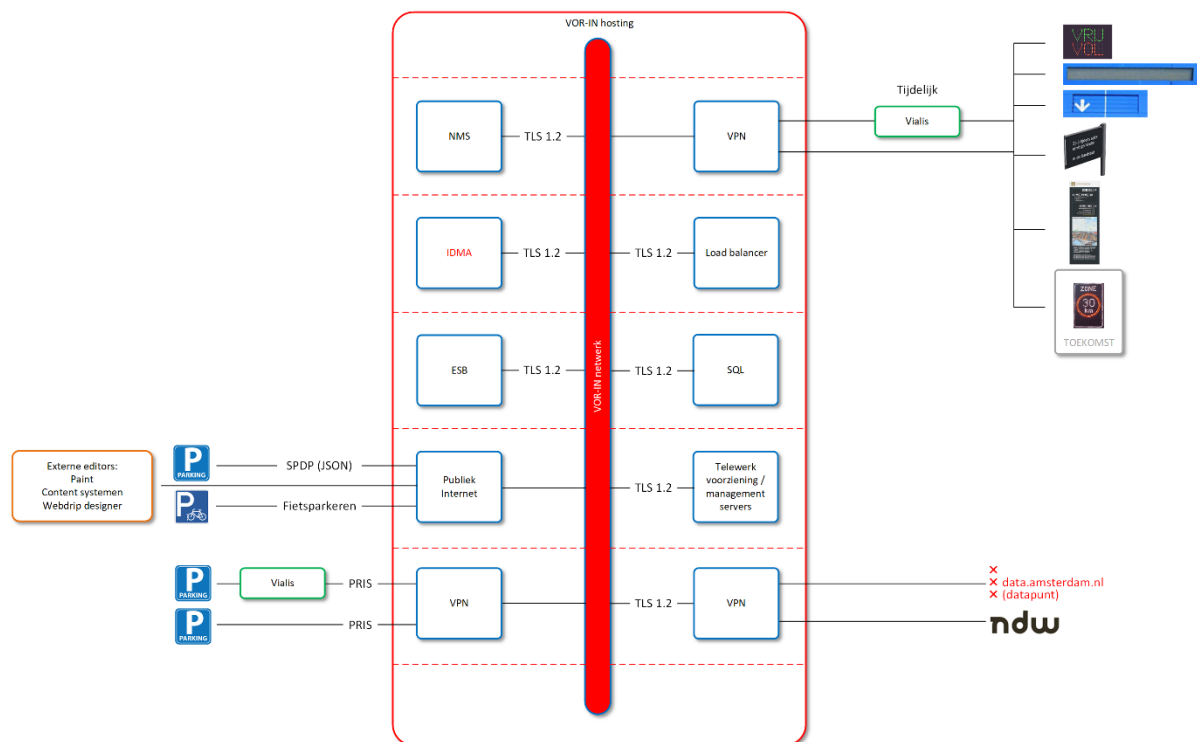
De Leverancier verleent hiermee 2e lijn ondersteuning en wordt door medewerkers van VOR-IN Infrastructure Services aangesproken voor applicatie specifieke zaken.

Het is mogelijk IPSEC site-to-site VPN verbindingen met datacenters van leveranciers of ketenpartners te leggen. Afhankelijk van de toepassing kunnen hierop (aanvullende) aansluitvoorwaarden van toepassing zijn. Het is niet mogelijk client-to-site VPN inbelverbindingen op te zetten.

Voor het instellen van de VPN verbindingen dient minimaal de technische details van het koppelvlak van de tegenpartij (bandbreedte, protocollen etc.) en contact gegevens van een technische beheerder te worden aangeleverd. Tevens kunnen aanvullende specifieke informatiebeveiligingsmaatregelen worden geëist.

Met het oog op beheersbaarheid en informatiebeveiligingseisen van de omgeving is het nadrukkelijk niet de bedoeling beheertaken over een datalink uit te voeren. Hiervoor wordt de telewerkvoorziening ingezet. Verkeer door een VPN tunnel zal worden gelimiteerd tot datgene wat noodzakelijk is voor de correcte werking van de applicatie.

In onderstaande figuur is een schets van enkele VOR-IN faciliteiten opgenomen, met daarbij de datastromen. De duiding van TLS-verbindingen is indicatief.



Figuur 2: VOR-IN faciliteiten

Binnen VOR-IN wordt netwerksegmentering toegepast. De segmentering heeft tot doel de systemen en applicaties van elkaar te scheiden. Verkeer tussen de segmenten is mogelijk mits toegestaan en specifiek geconfigureerd door de centrale firewall.

4.4 Dagelijks beheer

Het dagelijks beheer van VOR-IN en de daarin aanwezige serversystemen wordt door medewerkers van VOR-IN Infrastructure Services gedaan. Het gaat daarbij om regulier onderhoud van de netwerk- en hosting omgeving alsmede bewaking van deze omgeving.

Infrastructure Services vervult de volgende taken:

1. Bewaking van de hosting omgeving.
2. Bewaking van de netwerk omgeving.
3. Het onderhouden van de backup van complete virtuele machines.
4. Het automatisch installeren van updates voor het Windows / Linux platform.
5. Het faciliteren van werkplekken met applicaties.

Hiervoor worden de systemen opgenomen in het Active Directory domein en hebben de beheerders 100% controle over het systeem. De leverancier kan op machine-lokaal niveau aanvullende rechten krijgen die noodzakelijk zijn voor de correcte werking van de applicaties.

Infrastructure Services maakt gebruik van een SNMP gebaseerde monitoring tool. Ten behoeve van disaster – recovery wordt de eis gesteld dat alle bronbestanden (installatiebestanden) van de applicaties alsmede alle (elektronische-) licenties en installatie documentatie op Disk1 van elke Virtuele Machine worden opgeslagen. Op deze wijze worden deze vitale gegevens op regelmatige momenten in de backup meegenomen.

In het algemeen treedt Infrastructure Services VOR-IN als eerste lijn op voor het vaststellen en oplossen van eventuele incident meldingen vanuit de gebruikers. Indien het incident niet opgelost kan worden zal de leverancier 2e lijnsondersteuning moeten leveren.

Indien Leverancier storingen signaleert, dient registratie plaats te vinden door een incident te melden bij de Servicedesk VOR-IN.

In de DAP (Dossier Afspraken en Procedures) moet duidelijk zijn vastgelegd hoe Leverancier aanspreekbaar is voor VOR-IN voor het aan- en afmelden van incidenten en het inplannen van wijzigingen.

4.5 Modulariteit en standaardisatie virtualisatie-omgeving

De Virtualisatie-omgeving is opgebouwd uit Hyper-V nodes met capaciteit voor virtuele machines tot een maximum van 20 vCPU cores, 128GB RAM, 500GB disk space (exclusief dataopslag) en 1 Gb/s per virtuele machine.

Binnen het VOR-IN netwerk is gestandaardiseerd op Microsoft SQL Server als databaseplatform. Leverancier mag gebruik maken van dit platform, welke beschikbaar is op de in te zetten Hyper-V nodes. Microsoft-licenties worden door Opdrachtgever beschikbaar gesteld.

Het gebruik van een andere database dan MS SQL is toegestaan, echter met de volgende consequenties en nadere eisen - die ook gelden in het geval van een Postgres database, met dien verstande dat Opdrachtgever wel de installatie en updates zal verzorgen:

- De database wordt gerealiseerd in het database cluster. Installatie van een database op de applicatieserver is niet toegestaan. Uitzondering hierop is een lichte database, met weinig impact op CPU, disk en geheugen, bijvoorbeeld voor het vasthouden van status of configuratie informatie.
- Opdrachtgever richt hiertoe een database server in met het OS op advies van de leverancier (Windows of Red Hat). Opdrachtgever verzorgt de OS patches en OS onderhoud. Updates aan Microsoft producten worden meegenomen in de Windows updates. In het geval van Red Hat via "yum update" commando. Indien de programmatuur niet geleverd wordt door de OS vendor (uit de standaard repository van Red Hat), is dit de verantwoordelijkheid van Leverancier.
- Leverancier installeert de database op de database server. Het beheer en onderhoud van de database maakt inherent onderdeel uit van het beheer en onderhoud van IDMA. Dat houdt in dat leverancier verantwoordelijk is voor onderhoud, bugfixes, updates, patches.
- Opdrachtgever maakt alleen backups van MS SQL databases. In alle andere gevallen maakt Opdrachtgever snapshots van de gehele virtuele machine. Data maintenance inclusief backups van andere databases dan MS SQL is verantwoordelijkheid van leverancier. Indien snapshots niet voldoende zijn (vanwege verschillende versies, dagen, etc.) kan Opdrachtgever een netwerklocatie ter beschikking stellen waar Leverancier de database backups kan wegschrijven (gelijk aan het MS SQL model).
- Alle eenmalige en terugkerende licentiekosten voor de database dienen onderdeel te zijn van de inschrijfsom.
- Leverancier werkt in onderdeel D (Beschikbaarheidsmaximalisatie) van zijn inschrijving uit hoe hij het beheer en onderhoud van de database verzorgt en wat eventuele gevolgen zijn voor Opdrachtgever.

Aanvullend geldt voor de backups van de database in het geval dat het gewenst is dat Opdrachtgever hiervoor een netwerklocatie beschikbaar stelt, het volgende:

Er is sprake van een 2-traps model. Opdrachtgever stelt een fileshare beschikbaar waarop een backup van de database kan worden weggeschreven. Dit backup bestand wordt vervolgens in de reguliere backup en restore procedures opgenomen. In geval van een restore verzoek zal de backup van de database op de fileserver worden teruggezet en kan de leverancier hiervandaan een herstelactie van de applicatie uitvoeren. In verband met automatische verwerking van backupbestanden in relatie tot de retentie is het niet toegestaan meerdere versies van het backupbestand op de share te plaatsen. Oudere versies binnen de retentietijd van de backup zijn opvraagbaar bij Systeembeheer VOR-IN.

De virtuele servers worden standaard als één geheel in de backup opgenomen en vallen onder het standaard backup regime. Om dit proces efficiënt te laten verlopen zal elke virtuele machine voorzien worden van tenminste 2 virtuele disks:

- Disk 1 is voor het besturingssysteem en de geïnstalleerde applicatie en zal met een lage frequentie in de backup meedraaien (ca. 1x per maand).
- Disk 2 is bedoeld voor alle data die met de applicatie gemoeid is en draait met een hogere frequentie mee in de backup (ca 1x per dag).

Het is niet toegestaan inefficiënt gebruik te maken van de hosting omgeving, wat het dagelijks beheer door VOR-IN beheerders lastig of onmogelijk maakt. Te denken valt hierbij aan ernstige beperking veroorzaakt door licentiebescherming met node-lock mechanismen, het encrypten van Virtuele Machines, het installeren van beveiligingsupdates of het niet kunnen updaten van het onderliggende besturingssysteem.

Het is niet acceptabel als vanuit VOR-IN systeembeheer perspectief een black-box situatie ontstaat ten aanzien van een applicatieserver. Te allen tijde moet VOR-IN systeembeheer volledige en ongehinderde toegang tot het systeem kunnen hebben. Leverancier draagt zorg voor een gedegen kennisoverdracht aan de VOR-IN Infrastructure Services Systeembeheerders, zodat het dagelijks systeembeheer over de IDMA door hen kan worden uitgevoerd.

5 Applicatieomgeving

De applicatie functioneert binnen de VOR-IN omgeving en moet ten behoeve van het verzamelen en ontvangen van data alsmede het aansturen en beheren van displays gekoppeld worden aan een groot aantal objecten en systemen. Daarbij wordt gebruik gemaakt van de standaard faciliteiten die in het VOR-IN beschikbaar zijn.

In de figuur op de volgende pagina is een schets van de relevante objecten, applicaties, systemen, databanken en partijen opgenomen. Hieronder volgt een toelichting op diverse onderdelen van deze schets.

Toelichting:

- In de huidige situatie zijn het IDPA (Integraal Dynamisch Parkeerverwijssysteem Amsterdam) en CDMS (Centraal DRIP Management Systeem) gehost bij Vialis. Zij leveren de verbindingen naar de garages en displays. Deze verbindingen worden vanaf medio 2021 omgezet naar Amsterdamse verbindingen. Dit proces zal tot in 2022 doorlopen. De IDMA zal dus bij een aantal parkeervoorzieningen en displays in eerste instantie over verbindingen van (en via) Vialis communiceren, totdat alle verbindingen zijn overgezet naar verbindingen van Amsterdam.
- De IDMA zal een aantal displays moeten aansturen via een Translator, die zorg draagt voor de vertaling van Disperanto naar het propri  tair PRIS Display protocol en vice versa. Deze Translator functioneert binnen het VOR-IN. De meeste displays die met PRIS Display protocol communiceren zullen in 2022 vervangen worden door displays die communiceren met het Disperanto protocol.
- De IDMA zal van diverse (Amsterdamse) parkeervoorzieningen dynamische data in SPDP formaat moeten uitleveren, die via de ESB wordt gepubliceerd. Steeds meer van deze garages zullen deze data zelf in SPDP publiceren.
- De IDMA kan SPDP data ophalen van parkeervoorzieningen. Dit is niet beoogd ter vervanging van de data die via PRIS wordt uitgewisseld, maar zorgt voor toekomstvastheid (bijvoorbeeld data van telpunten). Daarnaast zal data van fietsparkeervoorzieningen middels een op SPDP gebaseerd protocol beschikbaar komen.
- De IDMA zal via de ESB data ontvangen van het ATT reistijdensysteem (Amsterdam Travel Time). Dit vindt plaats middels XML berichten met reistijden van alle trajecten.
- De IDMA zal via de ESB data ontvangen van het CMSA (Crowd Monitoring Systeem Amsterdam). Het betreft JSON berichten met drukte informatie (passages over lijnen en dichtheid in gebieden)
- De IDMA wordt met een DVM-Exchange koppelvlak gekoppeld aan het Netwerkmanagementsysteem (MobiMaestro) van Opdrachtgever. Het NMS draait in het VOR-IN.
- De publicatie van wat op (een subset van) de displays staat, vindt plaats in het DATEX-II formaat (VmsPublication) naar de ESB. De ESB verstuurt de berichten naar NDW. voor verdere verspreiding.
- Niet in de figuur opgenomen is de berichtgeving vanuit de IDMA bij storingen, middels onder meer e-mail en JSON berichten.

