

Bijlage 6 Programma van Eisen

Europese openbare aanbesteding Cloud Service Provider Brandweer (Talking Traffic)

Versie 1.0

Datum 22 augustus 2025

Colofon

Projectnaam

Europese openbare aanbesteding CSP-
BW

Versienummer

1.0

Afzendgegevens

NIPV

VERTROUWELIJK

INHOUD

COLOFON	2
1 INLEIDING	5
1.1 DOEL.....	5
1.2 EISEN.....	5
1.3 DEFINITIES	5
1.4 ANNEXEN	6
1.5 LEESWIJZER.....	6
2 PRESTATIE	7
2.1 INLEIDING.....	7
2.2 DOELSTELLINGEN VAN DE VERWERVING VAN DE CSP-BW DIENSTVERLENING VOOR DE BRANDWEER.....	7
2.3 DE TALKING TRAFFIC KETEN	8
2.4 PROCES PRIORITEITSAANVRAAG BRANDWEER EN WAARSCHUWINGSBERICHTEN (EVA-BERICHTEN)	8
2.5 SCOPE VAN DE VERWERVING VAN DE CSP-BW DIENSTVERLENING	10
<i>TECHNISCHE SCOPE CSP-BW DIENSTVERLENING</i>	11
2.6 FASERING	12
2.7 BESTURING VAN DE DIENSTVERLENING.....	14
3 FUNCTIONELE EN NIET-FUNCTIONELE EISEN	15
3.1 ALGEMENE EISEN AAN HET ONTWERP VAN DE CSP-BW	15
3.2 FUNCTIONELE EISEN.....	15
3.2.1 <i>Opstellen en verzenden aanvraag iVRI-prioriteit</i>	15
3.2.2 <i>Verwerken ontvangen resultaatberichten prio-aanvraag</i>	17
3.2.3 <i>Opmaken EVA-bestanden</i>	17
3.3 KOPPELINGEN	17
3.4 NIET-FUNCTIONELE EISEN.....	18
3.4.1 <i>Algemene eisen</i>	18
3.4.2 <i>Eisen/Opties aan de continuïteit</i>	19
3.4.3 <i>Certificering en testen</i>	20
3.4.4 <i>Loggings en rapportages</i>	20
3.4.5 <i>Eisen ten aanzien van capaciteit van de Productieomgeving</i>	21
3.4.6 <i>Eisen met betrekking tot de inpassing binnen de bestaande ICT - architectuur</i>	21
3.4.7 <i>Eisen ten aanzien van Productieomgeving</i>	21
3.4.8 <i>Eisen ten aanzien informatiebeveiliging</i>	21
4 REALISATIEFASE	22
4.1 EISEN AAN HET REALISATIEPLAN.....	22
4.2 EISEN AAN DE REALISATIE	22
4.3 NAZORG.....	23
4.4 RAPPORTAGE.....	23
5 OPERATIONELE FASE	24
5.1 EISEN AAN HET INSTANDHOUDINGSPLAN EN SLA/DAP.....	24
5.2 INSTANDHOUDING KETEN	25
5.3 LIFECYCLE MANAGEMENT	26
5.4 INCIDENTBEHEER.....	26

5.5	WIJZIGINGSBEHEER	28
5.6	ADVIESDIENSTEN.....	29
5.7	PROBLEEM BEHEER.....	30
5.8	ONDERSTEUNENDE DIENSTEN	30
5.8.1	<i>Bereikbaarheid van de CSP-BW dienstverlener.....</i>	<i>31</i>
5.8.2	<i>Risicomanagement.....</i>	<i>31</i>
5.8.3	<i>Rapportages.....</i>	<i>32</i>
5.8.4	<i>Klachten en escalaties.....</i>	<i>32</i>
6	EXITFASE.....	33
7	INFORMATIEBEVEILIGING, PRIVACY EN BUSINESS CONTINUITY	34
7.1	BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO).....	34
7.2	EISEN AAN DE CSP-BW DIENSTVERLENER EN DE CSP-BW DIENSTVERLENING..	34
7.3	INFORMATIEBEVEILIGINGSPLAN.....	35
7.4	PRIVACY.....	35
7.5	BUSINESS CONTINUITY MANAGEMENT.....	36
	ANNEX A: INTERFACEBESCHRIJVING KOPPELING CSP-BW	
	APPLICATIE – UDAP (EVA-BERICHT).....	38
	ANNEX B: INTERFACEBESCHRIJVING KOPPELING VPS – CSP-BW	
	APPLICATIE	40
	ANNEX C – EISEN AAN RAPPORTAGES IN DE OPERATIONELE FASE	44

1 Inleiding

1.1 Doel

Dit Programma van Eisen (PvE) heeft de status van definitief uitvraagdocument. Deze definitieve versie is tot stand gekomen in interactie tussen het Nederlands Instituut Publieke Veiligheid (NIPV) en het ministerie van Infra en Waterstaat (IenW). Dit PvE is de basis om te komen tot een meerjarige overeenkomst tussen het NIPV en de geselecteerde Cloud Service Provider Brandweer, die gedurende de looptijd van deze overeenkomst verantwoordelijk is voor het via UDAP in de Talking Traffic dataketen brengen van relevante data van Brandweervoertuigen die met spoed (categorieën "prio 1" en "prio 2") onderweg zijn naar een incidentlocatie. De Cloud Service Provider brandweer dienstverlener (CSP-BW) is daarbij verantwoordelijk voor het ten behoeve van die Brandweervoertuigen geven van invulling aan de in dit PvE beschreven eisen.

Dit Programma van Eisen (PvE) bevat de Eisen die Opdrachtgever stelt aan: (de resultaten van) de Prestatie; de beveiliging en veiligheid van de aangeboden oplossing en de CSP-BW dienstverlener.

1.2 Eisen

Eisen zijn als volgt aangegeven: [*<letter code E>-<volgnummer>*].

Ten aanzien van Eisen geldt het volgende:

- De oplossing die Inschrijver door middel van zijn Inschrijving aanbiedt, moet invulling geven aan alle Eisen.
- De Eisen hebben een knock-outkarakter. Indien uit een Inschrijving volgt dat niet onvoorwaardelijk aan alle Eisen zal worden voldaan, zal deze Inschrijving terzijde gelegd worden.
- De kosten verbonden met (de uitvoering van) de Eisen dienen inbegrepen te zijn in de prijzen en tarieven die Inschrijver opneemt in de Prijsopgavetabel van zijn Inschrijving (Bijlage 11 prijzenblad CSP-BW).

Relatie met fasering

De Eisen en Opties in dit PvE zijn onderverdeeld in verschillende hoofdstukken die de door de CSP-BW dienstverlener te leveren diensten reflecteren die onderdeel uitmaken van de Prestatie.

De Eisen die zijn beschreven in paragraaf 3.2 (Functionele Eisen), 3.3 (Koppelingen) en 3.4 (Niet-functionele Eisen) en hoofdstuk 7 (Veiligheid en beveiliging) zijn van toepassing in alle fasen van de Prestatie. De Eisen in de overige delen van het PvE zijn van toepassing in de fase waaraan de desbetreffende dienst is gekoppeld zoals benoemd in de desbetreffende paragraaf of hoofdstuk.

1.3 Definities

Hoofdletterbegrippen

Gedefinieerde begrippen worden in het PvE geschreven met een hoofdletter. Deze hoofdletterbegrippen hebben de betekenis die daaraan is toegekend in de begrippenlijst (Bijlage 00 bij het Beschrijvend document).

Afkortingen

Naast bovenstaande hoofdletterbegrippen worden er in PvE en in de Annexen gebruik gemaakt van afkortingen en benamingen van systemen en/of omgevingen. In Bijlage 0 Begrippenlijst is als aanvulling een overzicht gemaakt met de meest gebruikte afkortingen en benamingen.

1.4

Annexen

Het PvE kent een aantal Annexen die daarvan integraal onderdeel uitmaken. Het gaat om de volgende Annexen:

- Annex A – Interfacebeschrijving koppeling CSP-BW – UDAP (EVA-bericht)
- Annex B – Interfacebeschrijving koppeling VPS -CSP-BW
- Annex C – Eisen aan rapportages in de operationele fase

1.5

Leeswijzer

In hoofdstuk 2 wordt in algemene zin de Prestatie toegelicht. Hier staan doelstellingen van Opdrachtgever beschreven alsmede de scope van de Prestatie in relatie tot de verschillende fasen van de Prestatie.

Hoofdstukken 3, 4, 5 en 6 beschrijven specifiek de diensten die De CSP-BW dienstverlener dient te leveren aan Opdrachtgever gedurende de:

- (i) Realisatiefase: Realisatie en Operationalisering;
- (ii) Operationele Fase: Instandhouding, en;
- (iii) Exitfase: Exit.

Hoofdstuk 7 beschrijft de informatiebeveiliging, privacy en business continuity eisen waar de CSP-BW dienstverlener aan dient te voldoen.

2 Prestatie

2.1 Inleiding

Het is voor de brandweer van groot belang om zo snel mogelijk op een veilige manier van A naar B te kunnen rijden. Enkele secondes kunnen letterlijk het verschil maken tussen leven en dood. Om de rit naar het incident zo snel mogelijk te laten verlopen moet een Brandweervoertuig op de rit zo snel en veilig mogelijk kunnen uitvoeren. Bij kruispunten kan dit worden gerealiseerd door het krijgen van groen licht. Steeds meer wordt in Nederland gebruik gemaakt van intelligente verkeersregelininstallaties, die het mogelijk maken om verkeerslichten of bollards en slagbomen aan te sturen op het moment dat dit nodig is.

Daarnaast is het van belang, voor de verkeersveiligheid en het verkrijgen van voorrang voor het Brandweervoertuig, dat bestuurders gewaarschuwd worden indien er een Brandweervoertuig in de buurt is.

Om deze situatie te kunnen creëren bestaat er een keten van de intelligente verkeersinstallaties (iVRI's) tot en met de bestuurders van voertuigen om bestuurders te informeren en iVRI's te kunnen aansturen. Deze keten wordt nog niet gebruikt door de brandweer, omdat er een Cloud Service Provider ontbreekt. Deze aanbesteding geeft invulling aan de realisatie van een Cloud Service Provider brandweer dienstverlening (CSP-BW) om hiermee de voorrang voor Brandweervoertuigen en het informeren van bestuurders mogelijk te maken.

2.2 Doelstellingen van de verwerving van de CSP-BW dienstverlening voor de brandweer

Aanbestedende Dienst wenst met de verwerving van de CSP-BW dienstverlening voor de brandweer de volgende doelstellingen te bereiken:

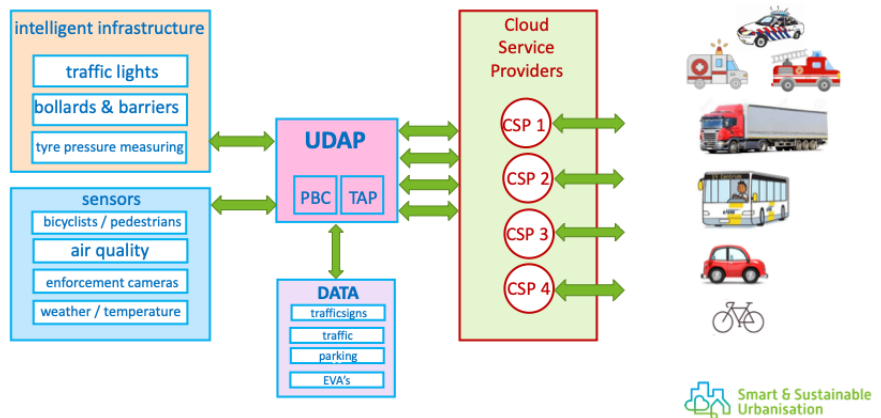
- Te komen tot een effectieve en efficiënte CSP-BW dienstverlening die erop ingericht is om maximaal bij te dragen aan de keten die ervoor zorgt dat de Brandweervoertuigen prioriteit krijgen bij iVRI's en dat weggebruikers worden geïnformeerd over naderende Brandweervoertuigen;
- Een toekomstbestendige CSP-BW applicatie te laten creëren die in hoge mate configureerbaar is en daarmee snel aan te passen aan wijzigende omstandigheden;
- Een veilige CSP-BW dienstverlening te verkrijgen waar het niet mogelijk is om ongeautoriseerd toegang te krijgen tot de dienstverlening;
- De beoogde CSP-BW dienstverlening te verkrijgen met een zo hoog mogelijk niveau van beschikbaarheid en robuustheid;
- Een CSP-BW dienstverlening te verkrijgen die eenvoudig te koppelen is met bestaande systemen in de keten;
- Het laten realiseren van koppelingen van de CSP-BW applicatie met een voertuigpositieserver (VPS), UDAP en optioneel in de bestaande in-car informatiediensten in de Brandweervoertuigen;
- Het laten instandhouden van de CSP-BW dienstverlening gedurende de contracttermijn.
- Het afstemmen van de CSP-BW dienstverlener met de overige ketenpartners en de samenwerking met het ketenmanagement.

2.3

De Talking Traffic keten

Het Innovatiepartnership Talking Traffic is een samenwerking van overheden en bedrijven in een volledige dataketen tussen intelligente infrastructuur (zoals iVRI's) en informatiediensten voor weggebruikers. De keten is daarbij ingedeeld in 3 onderdelen: leveranciers van intelligente infrastructuur (onder meer verkeersregelininstallaties), cloud service providers (voor snelle en veilige datacommunicatie) en informatiediensten voor in-car adviezen aan weggebruikers.

Talking Traffic dataketen



Figuur 1: Componenten Talking Traffic dataketen

Voor de uitrol van de intelligente verkeerslichten is een speciale architectuur ontworpen, die ervoor zorgt dat de drie functionele modules in een iVRI conform gestandaardiseerde interfaces en protocollen onderling kunnen communiceren. Wegbeheerders kunnen als gevolg hiervan bij verschillende aanbieders die functionele modules afnemen: de producten van verschillende leveranciers kunnen dankzij die standaarden probleemloos samen functioneren. Partners in de Talking Traffic dataketen hebben afspraken gemaakt over de wijze waarop berichten in de keten van weggebruiker naar intelligente infrastructuur worden uitgewisseld, daarbij waar mogelijk gebruik makend van Europese standaarden, hoe daarbij de privacy zowel als verkeersveiligheid geborgd kan blijven en een reeks nieuwe toepassingen kan worden gerealiseerd ter verdere verbetering van verkeersveiligheid, doorstroming en comfort.

2.4

Proces prioriteitsaanvraag brandweer en waarschuwingsberichten (EVA-berichten)

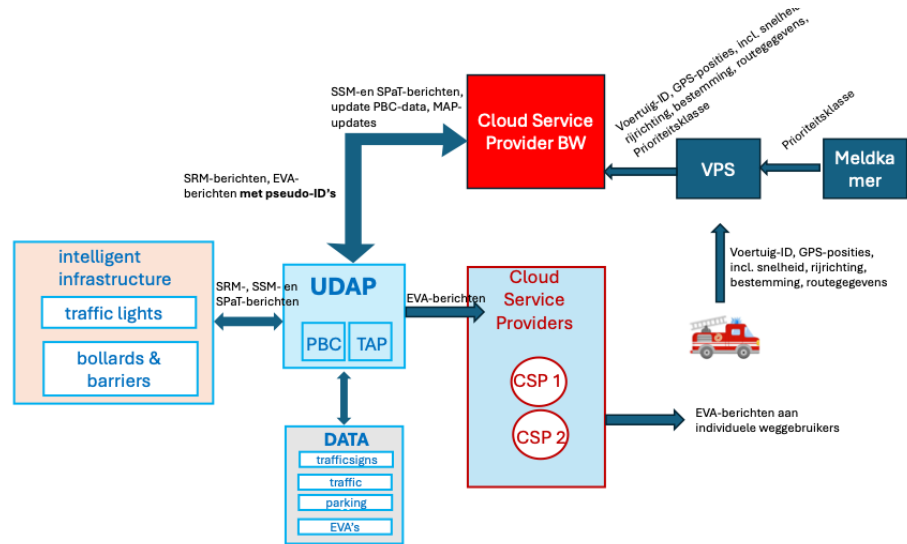
Prioriteitsaanvraag brandweer

Het proces van het afhandelen van een prioriteitsaanvraag kent de volgende stappen:

1. Een voertuig van de geeft iedere 1 seconde haar actuele GPS-positie (incl. snelheid en rijrichting) door aan de voertuigpositieserver (VPS). Losse voertuigposities worden verzameld en vanuit één (1) endpoint doorgezet door de landelijke brandweer-VPS.
2. De meldkamer bepaalt de prioriteitsklasse van een rit van het voertuig. Deze prioriteitsklasse wordt doorgegeven aan de voertuigpositieserver (VPS). De voertuigpositieserver registreert de prioriteitsklasse van de rit.

3. Indien de prioriteitsklasse van de rit op één is gezet, worden de voertuigposities (actuele GPS-positie incl. snelheid en rijrichting) van het Brandweervoertuig samen met de voertuig-ID, de bestemming/routegegevens en de prioriteitsklasse van de rit door de VPS verzonden naar de te selecteren CloudServiceProvider brandweer (CSP-BW). De CSP-BW applicatie neemt de gegevens van de VPS af (gepushed). De CSP-BW applicatie bepaalt op basis van de actuele voertuigpositie en de bestemming/routegegevens de verwachte (meest plausibele) route van het Brandweervoertuig naar diens opgegeven bestemming. Op basis van de meest actuele gegevens die de CSP-BW applicatie periodiek vanuit UDAP ontvangt (ca. eenmaal per etmaal MAP-bestanden (push) en een (pull) update van de PBC (Priority Broker Configurator) data tot eenmaal per enkele minuten), bepaalt deze wat het eerstvolgende intelligente object (iVRI of iBFA) is waarmee het voertuig op diens route geconfronteerd zal worden.
4. De CSP-BW applicatie berekent de aankomsttijd (ETA) van het Brandweervoertuig op de stopstreep van dat eerstvolgende intelligente object op diens route en gebruikt dit samen met de juiste RIL (Request Importance Level) uit de PBC van UDAP om vanaf een ETA van ca. 3 minuten een SRM-bericht samen te stellen en dat (samen met het opgestelde CAM-bericht) via UDAP naar dat eerstvolgende intelligente object te sturen. NB: in het SRM bericht dient de CSP-BW applicatie een pseudo-ID voor het voertuig te gebruiken, met een levensduur tot het passeren van de stopstreep van het intelligente object. Indien sprake is van twee kort achter elkaar op de route van het Brandweervoertuig liggende intelligente objecten en er daardoor twee prioriteitsaanvraagprocessen gelijktijdig lopen, dient door de CSP-BW applicatie voor elk van die twee gelijktijdig lopende processen een andere pseudo-ID voor dat Brandweervoertuig te worden gebruikt.
5. Het SRM-bericht wordt vervolgens naar UDAP verzonden. UDAP zorgt voor de verzending naar het intelligente object.
6. Het intelligente object gaat op basis van dat ontvangen SRM-bericht de noodzakelijke voorbereidingen treffen om het mogelijk te maken dat het naderende Brandweervoertuig zoveel mogelijk ongehinderd kan passeren. Ter bevestiging daarvan stuurt het intelligente object een SSM-bericht via UDAP naar de CSP-BW applicatie. Dit bericht is de bevestiging dat er geheel automatisch een prioriteitsverzoek voor het voertuig is verzonden naar het eerstvolgende intelligente object en dat dit verzoek goed ontvangen is en verwerkt.
7. Deze cyclus herhaalt zich iedere 10 seconden, waarbij de CSP-BW applicatie in het SRM-bericht telkens een bijstelling van de eerder afgegeven ETA vanuit het Brandweervoertuig op de stopstreep van het intelligente object geeft, indien de door de CSP-BW applicatie via de VPS van het voertuig ontvangen positiegegevens daar aanleiding toe geven.
8. Wanneer het Brandweervoertuig binnen het MAP-gebied van het intelligente object is aangekomen (en dan doorgaans nog ca. 300m van de stopstreep is verwijderd), wordt die updatefrequentie verhoogd tot eenmaal per seconde. Betreft het ten aanzien van dat intelligente object een iVRI, dan zullen - enigszins afhankelijk van de lokale situatie- op de arm waarover het Brandweervoertuig de kruising nadert alle signaalgroepen ("lichten") op groen staan. En op alle andere armen van die kruising staan deze op rood. Waardoor al het verkeer stilstaat, uitgezonderd het verkeer voor het Brandweervoertuig: dat kan al weggrijden, zodat het naderende Brandweervoertuig zoveel mogelijk ongehinderd kan doorrijden als het eenmaal op de kruising is aangekomen.

9. Zodra de CSP-BW applicatie aan de hand van diens kennis van de MAP-gegevens van het intelligente object en die iedere seconde ontvangen CAM-berichten (met o.a. de actuele voertuigposities) vaststelt dat het Brandweervoertuig de stopstreep van het intelligente object is gepasseerd, verstuurt de CSP-BW applicatie via UDAP een cancellation-bericht naar het intelligente object, ten teken dat het de reguliere regeling (in geval van een iVRI) of positie (in geval van een bollard of slagboom) weer kan hervatten.



Figuur 2: Prioriteitsaanvraag bij de Brandweer.

Waarschuwingsberichten voor weggebruikers (EVA-berichten)

De CSP-BW applicatie stelt aan de hand van de gegevens vanuit de VPS EVA-berichten op en stuurt deze naar UDAP. Daar worden deze berichten doorgezeten naar de aangesloten cloudserviceproviders, welke deze doorzetten naar de door hen ondersteunde informatiediensten: een app op een smartphone, een navigatiesysteem of een functie in het dashboard van een auto. Aan de hand van deze EVA-berichten kunnen weggebruikers tijdig worden gewaarschuwd voor een naderend Brandweervoertuig in de directe nabijheid op hun route.

2.5

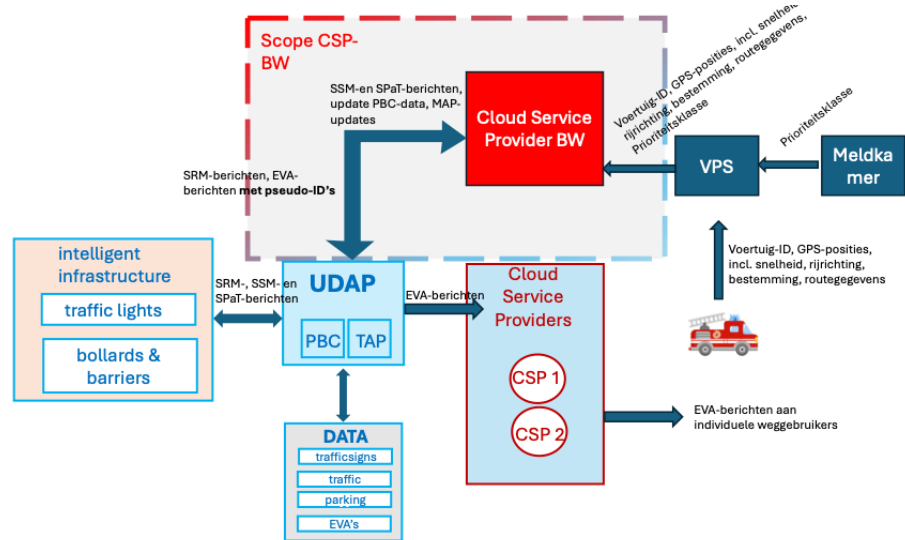
Scope van de verwerving van de CSP-BW dienstverlening

In deze paragraaf wordt de scope van de CSP-BW dienstverlening op hoofdlijnen beschreven. Deze scope wordt in de volgende hoofdstukken uitgewerkt tot specifieke Eisen.

Functionele scope CSP-BW dienstverlening

Een functioneel overzicht van de CSP-BW dienstverlening is weergegeven in figuur 1, in de context waarbinnen de CSP-BW dienstverlening dient te functioneren.

De CSP-BW dienstverlening stelt Brandweervoertuigen in staat om tijdens een inzet de prioriteitsaanvragen bij iVRI's en iBFA's aan te leveren bij UDAP en middels de aflevering van EVA-berichten bij UDAP de waarschuwingen over die inzet te laten communiceren aan nabije weggebruikers.



Figuur 3: Scope aanbesteding CloudServiceProvider Brandweer

In het bovenstaande figuur is de scope weergegeven voor de productieomgeving van de CSP-BW. Voor certificering en testdoeleinden is tevens een testomgeving van de Talking Traffic keten gerealiseerd, waar de CSP-BW dienstverlener op aan dient te sluiten met een testomgeving van de CSP-BW applicatie.

Technische scope CSP-BW dienstverlening

De CSP-BW dienstverlening bevat in ieder geval de ontwikkeling, realisatie, levering van het gebruik en het beheer van de volgende componenten:

1. draadverbinding met de VPS voor:
 - a. ontvangst van voertuigpositiegegevens vanuit Brandweervoertuigen
 - b. ontvangst van de voertuigstatus voor elk van die ontvangen voertuigpositiegegevens (vanuit meldkamer(s))
2. de CSP-BW applicatie in een productieomgeving
3. de CSP-BW applicatie in een testomgeving
4. de cloudomgeving (productieomgeving) waarbinnen de applicatie is geïnstalleerd
5. koppeling (met bijbehorend koppelvlak) met UDAP en VPS
6. draadverbinding van de CSP-BW testomgeving met de Test- en Acceptatieomgeving van UDAP (Internationale Nederlands-Vlaamse Testbed)
7. draadverbinding met UDAP Productie-omgeving voor:
 - a. aanlevering van CAM-berichten
 - b. aanlevering van SRM-berichten
 - c. aanlevering van cancellation-berichten
 - d. aanlevering van EVA-berichten
 - e. ontvangen van SSM-berichten
 - f. ontvangen van granted berichten
 - g. ontvangen van rejected berichten
 - h. ontvangen van MAP bestanden
 - i. ontvangen van SPaT berichten
8. afstemming met de leveranciers van de informatiediensten aan boord van Brandweervoertuigen om voertuigpositiegegevens te verzenden met een frequentie tot 1Hz.

2.6

Fasering

Ten aanzien van de Prestatie identificeert Opdrachtgever drie (3) fasen:

1. Realisatiefase: De CSP-BW dienstverlener realiseert en in bedrijf stellen van de CSP-BW dienstverlening;
2. Operationele fase: De CSP-BW dienstverlening wordt door de CSP-BW dienstverlener uitgevoerd door o.a.: onderhouden en in stand houden van de CSP-BW applicatie, incidentmanagement en Lifecycle Management. De CSP-BW dienstverlener voert indien benodigd tevens functionele wijzigingen door aan de CSP-BW dienstverlening. De CSP-BW dienstverlener dient samen te werken met de ketenpartijen en het ketenmanagement voor de instandhouding van de keten.
3. Exitfase: De CSP-BW dienstverlener zorgt conform het Exitplan voor een geruisloze overgang van de situatie waarin de CSP-BW dienstverlener de diensten uitvoert naar de situatie waarin een nieuwe dienstverlener dan wel Opdrachtgever de diensten uitvoert en/of soortgelijke diensten levert.

Tabel 1 geeft een overzicht van de verschillende fasen in de samenwerking tussen Opdrachtgever en de CSP-BW dienstverlener.

Fase	Start van de fase Telkens te bepalen door Opdrachtgever (onderstaande startmomenten zijn daarmee indicatief)	Einde van de fase	Door de CSP-BW dienstverlener te leveren diensten
Realisatiefase	Na tekenen van de Overeenkomst	Aan het einde van de periode genoemd in paragraaf 5.3 van dit PvE. NB. Maximaal twee (2) maanden na tekenen Overeenkomst dient de mijlpaal "Gereed voor gebruik" te zijn behaald.	Ontwikkelen en inrichten, Implementeren en in bedrijf stellen van de CSP-BW dienstverlening (Hoofdstuk 3, 4, en 5 van dit document)
Operationele fase	Na afronding van de in productiename.	De Operationele Fase duurt tot drie (3) jaar na het afronden van de Realisatiefase, met een optie om onder gelijke voorwaarden één of meerdere keren te verlengen voor een additionele periode van in	Uitvoeren van de Instandhoudingsdiensten conform (in ieder geval) het Instandhoudingsplan, waaronder Lifecycle Management.

		totaal maximaal twee (2) jaar.	
Exitfase	Bij (be)eindigen van de Overeenkomst. Uiterlijk voor het daadwerkelijk eindigen van de Overeenkomst.	Exitplan uitgevoerd. NB.: De Exitfase duurt maximaal 12 maanden.	Uitvoeren van de Exitwerkzaamheden conform (in ieder geval) het Exitplan (hoofdstuk 6 van dit document).

Tabel 1: Fasering

Scope van de Realisatiefase

Tijdens de Realisatiefase richt de CSP-BW dienstverlener onder andere de dienst in en worden alle koppelingen door de CSP-BW dienstverlener gerealiseerd. De CSP-BW dienstverlener realiseert hiertoe koppelvlakken die voor de CSP-BW dienstverlening benodigde zijn en past deze aan op bestaande koppelvlakken van externe systemen teneinde de CSP-BW diensten te kunnen leveren. De CSP-BW dienstverlening en de ervoor benodigde koppelvlakken dienen voorafgaand aan inbedrijfstelling ervan in de Testomgeving te worden getest op conformiteit aan alle eisen en voorwaarden uit dit PvE, alsmede de certificeringsvoorwaarden uit de Talking Traffic dataketen.

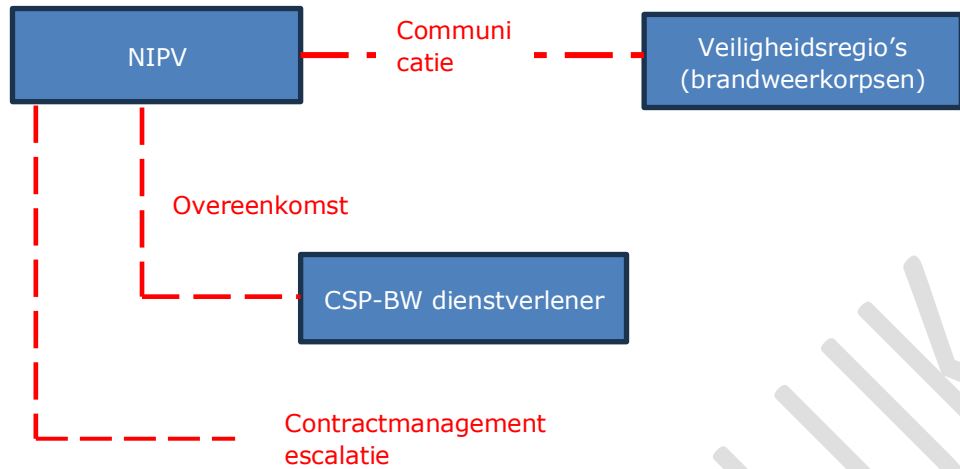
Scope van de Operationele fase

Tijdens de Operationele fase draagt de CSP-BW dienstverlener zorg voor instandhouding van de CSP-BW dienstverlening door het uitvoeren van o.a. het incidentmanagement, releasemanagement en lifecyclemanagement. De CSP-BW dienstverlener draagt ervoor zorg dat gedurende de contractperiode voldaan blijft worden aan de functionele en niet functionele specificaties. Opdrachtgever dient eventuele wijzigingsverzoeken in bij de CSP-BW dienstverlener. Na het overeenkomen van wijzigingen, draagt de CSP-BW dienstverlener zorg voor de uitvoering van de wijziging.

De CSP-BW dienstverlener stelt zich proactief op om continuïteit van de CSP-BW dienstverlening te borgen en Incidenten te voorkomen.

2.7 Besturing van de dienstverlening

In onderstaand figuur is de besturing van de CSP-BW dienstverlening vereenvoudigd weergegeven:



Figuur 4 Besturing van de CSP-BW dienstverlening (vereenvoudigd).

Het NIPV is de organisatie met wie de CSP-BW dienstverlener een Overeenkomst sluit. Het NIPV (als facilitaire dienstverlener van de brandweer) voert het operationeel contractmanagement (waaronder in ieder geval het monitoren van de algehele realisatie en de ketenresultaten) op de te leveren dienstverlening. Onder de besturing valt ook een proactieve rol van het NIPV met betrekking tot:

- 1) Ondersteuning tijdens de realisatie van de CSP-BW dienstverlening;
- 2) Het leggen van de contacten met de contactpersonen van de brandweeronderdelen;
- 3) Het uitvoeren van het escalatieniveau voor de CSP-BW dienstverlener en het brandweerkorps.

3 Functionele en niet-functionele eisen

3.1 Algemene Eisen aan het Ontwerp van de CSP-BW

Eis	Omschrijving
E-001	De CSP-BW dienstverlener dient een Ontwerp te maken voor de CSP-BW applicatie, waarin hij aangeeft op welke wijze hij de Eisen uit hoofdstuk 3 van het PvE invult.
E-002	De CSP-BW dienstverlener dient in het Ontwerp op te nemen: <ul style="list-style-type: none">- Hoe hij de functionaliteit van de CSP-BW applicatie zoals beschreven in de Eisen uit hoofdstuk 3 van het PvE realiseert in een Functioneel Ontwerp;- Van welke softwareproducten hij gebruik maakt om deze functionaliteit te realiseren;- Hoe hij de technische onderdelen realiseert in een Technisch Ontwerp;- Met welke hardwareproducten hij deze functionaliteit realiseert;- Hoe hij de koppelingen met UDAP, VPS en de Testomgeving technisch realiseert.
E-003	De CSP-BW dienstverlener mag het Ontwerp realiseren nadat het positief beoordeeld is door de Opdrachtgever.

3.2 Functionele Eisen

3.2.1 Opstellen en verzenden aanvraag iVRI-prioriteit

Eis	Omschrijving
E-004	De CSP-BW applicatie dient aan te sluiten op de API van de VoertuigPositieServer (VPS) om de gegevens van de VPS te kunnen ontvangen conform Annex B.
E-005	De CSP-BW applicatie dient via de VPS iedere seconde een bericht te kunnen ontvangen en verwerken van ieder Brandweervoertuig dat met spoed onderweg is (dus ook als onderweg de prioriteit naar spoed is veranderd).
E-006	De CSP-BW dienstverlening dient in overeenstemming te zijn (en blijven gedurende de contractperiode) met de door de CROW gepubliceerde standaarden (zoals D3047-15). De CROW standaarden zijn gepubliceerd op het CROW kennisplatform.
E-007	De CSP-BW applicatie dient ook andere frequenties waarmee een bericht vanuit een voertuig via de VPS wordt verzonden te kunnen ontvangen.
E-008	De CSP-BW applicatie dient op basis van de iedere ontvangen actuele voertuigpositie en de actuele bestemming/routegegevens van desbetreffend voertuig de verwachte (meest plausibele) route van dat voertuig naar die opgegeven bestemming te bepalen, indien dit nog is ontvangen vanuit de VPS.
E-009	De CSP-BW applicatie dient de mogelijkheid te hebben om op basis van 'approach based' binnen het MAP gebied te kunnen functioneren.

E-010	De CSP-BW applicatie dient op ieder moment vanuit UDAP actuele MAP-bestanden te kunnen ontvangen (push vanuit UDAP) conform de CROW-standaarden.
E-011	De CSP-BW applicatie dient een update van de PBC-data vanuit UDAP te kunnen ophalen (tot eenmaal per enkele minuten(pull) conform de CROW-standaarden.
E-012	De CSP-BW applicatie dient op basis van het resultaat als bedoeld in E-007 en de meest actuele vanuit UDAP verkregen relevante gegevens de eerstvolgende iVRI of iBFA op de route van een ingezet Brandweervoertuig te bepalen.
E-013	De CSP-BW applicatie dient de verwachte aankomsttijd (ETA) van een ingezet Brandweervoertuig op de stopstreep van de eerstvolgende iVRI of iBFA op de route te berekenen.
E-014	De ETA dient op basis van het resultaat als bedoeld in E-007 en de meest actuele vanuit UDAP verkregen relevante gegevens van de eerstvolgende iVRI of iBFA te worden berekend door het optellen van de volgende tijden: <ul style="list-style-type: none"> • Reistijd tot het MAP-gebied • Reistijd binnen het MAP-gebied
E-015	Zodra de in E-012 bedoelde ETA tussen 3 en 2,5 minuten ligt, dient de CSP-BW applicatie ten behoeve van de prioriteitsaanvraag bij een iVRI of iBFA voor een Brandweervoertuig een SRM- en CAM-bericht aan te maken en via UDAP naar die iVRI of iBFA te zenden, dat is samengesteld aan de hand van de ETA en het juiste RIL (Request Importance Level) voor het voertuig, als afgeleid uit de in de PBC (Priority Broker Configurator) voor desbetreffende iVRI of iBFA opgenomen criteria.
E-016	De door de CSP-BW applicatie opgestelde SRM-berichten dienen de gegevens te bevatten zoals opgenomen in de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-3).
E-017	De door de CSP-BW applicatie opgestelde CAM-berichten dienen de gegevens te bevatten zoals opgenomen in de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-5).
E-018	De CSP-BW applicatie dient in staat te zijn om meerdere prioriteitsaanvraagprocessen gelijktijdig te laten lopen in het geval tussen meerdere opeenvolgend op de route van het Brandweervoertuig gelegen iVRI's of iBFA's minder dan 3 minuten reistijd voor dat voertuig ligt.
E-019	In de SRM berichten die gedurende één prioriteitsaanvraagproces worden aangemaakt en via UDAP naar een specifieke iVRI of iBFA worden gezonden, dient de CSP-BW applicatie één pseudo-ID voor het Brandweervoertuig te gebruiken, waarvan de levensduur eindigt nadat het voertuig de stopstreep van desbetreffende iVRI of iBFA is gepasseerd en de CSP-BW applicatie ter melding daarvan het cancellation-bericht aan die iVRI of iBFA heeft verzonden.
E-020	Indien sprake is van meerdere simultaan lopende prioriteitsaanvraagprocessen voor een Brandweervoertuig, dient door de CSP-BW applicatie voor elk van die processen een andere, niet onderling relateerbare pseudo-ID voor dat Brandweervoertuig te worden gebruikt.
E-021	De CSP-BW applicatie dient tot het moment dat het voertuig op het MAP-gebied is aangekomen, met intervallen van telkens 10 seconden via UDAP een nieuw SRM-bericht naar de iVRI of iBFA te sturen, met daarin een opnieuw berekende waarde van de meest recent afgegeven ETA.

E-022	Wanneer het voertuig op het MAP-gebied van de iVRI of iBFA is aangekomen (en dan doorgaans nog ca. 300m van de stopstreep ervan is verwijderd), dient de CSP-BW applicatie iedere seconde via UDAP een nieuw SRM-bericht naar de iVRI of iBFA te sturen, met daarin een opnieuw berekende waarde van de meest recent afgegeven ETA.
E-023	Zodra de CSP-BW applicatie aan de hand van het beschikbare MAP-bestand van de iVRI of iBFA en de iedere seconde ontvangen actuele positie van het Brandweervoertuig vaststelt dat het voertuig de stopstreep is gepasseerd, dient de CSP-BW applicatie een cancellation-bericht via UDAP naar die iVRI of iBFA te versturen, ten teken dat de iVRI de reguliere regeling, of de iBFA de gesloten positie weer kan hervatten.
E-024	De CSP-BW dienstverlener dient voor bijzondere gevallen (zoals een busbaan) afspraken voor afhandeling van een prioriteitsaanvraag te kunnen maken (en realiseren) met een veiligheidsregio.

3.2.2 Verwerken ontvangen resultaatberichten prio-aanvraag

Eis	Omschrijving
E-025	De CSP-BW applicatie dient het in antwoord op een verzonden SRM-bericht via UDAP ontvangen SSM-bericht te kunnen ontvangen en verwerken.

3.2.3 Opmaken EVA-bestanden

Eis	Omschrijving
E-026	De CSP-BW applicatie dient voor Brandweervoertuigen die met spoed onderweg zijn iedere seconde een EVA-bericht (conform Annex A) op te stellen en naar UDAP te zenden, aan de hand waarvan weggebruikers in de nabijheid van dat Brandweervoertuig kunnen worden gewaarschuwd voor de nadering ervan.

3.3 Koppelingen

Algemene Eisen aan koppelingen

De koppelingen met UDAP die worden gepubliceerd via het CROW kennisplatform, zijn toegankelijk door middel van een gratis registratieprocedure.

Eis	Omschrijving
E-027	De CSP-BW applicatie dient in staat te zijn om iedere seconde (updates) van meerdere prioriteitsaanvragen te kunnen afhandelen.
E-028	De CSP-BW applicatie dient testberichten te kunnen sturen richting het UDAP-systeem. Dit om de connectiviteit voor/ na een upgrade te testen.
E-029	De CSP-BW applicatie dient te worden gekoppeld met het Internationale Nederlands-Vlaamse Testbed om software upgrades te kunnen testen en certificeren.
E-030	De CSP-BW dienstverlener dient te monitoren of de verbinding met de VPS bereikbaar is voor de CSP-BW applicatie. Bijvoorbeeld door regelmatig (met een interval van maximaal een 1 minuut) een testbericht naar UDAP en de VPS te sturen ('pingen'). Bij een niet reagerende verbinding dient de CSP-BW de Opdrachtgever te alerteren.

Specifieke Eisen aan de koppeling met UDAP

Eis	Omschrijving
E-031	De CSP-BW applicatie dient door de CSP-BW dienstverlener te worden gekoppeld met het UDAP-systeem conform de specificaties die zijn opgenomen op het CROW kennisplatform.
E-032	De CSP-BW applicatie dient de EVA-berichten te communiceren naar UDAP conform Annex A.
E-033	De CSP-BW applicatie dient in staat te zijn meerdere prioriteitsaanvragen en EVA-berichten gelijktijdig naar UDAP te versturen.
E-034	De CSP-BW dienstverlener dient een update van MAP-bestanden en/of PBC-data direct te verwerken, zodat deze update mee wordt genomen in alle lopende en komende prioriteitsaanvragen.
E-035	De CSP-BW applicatie dient SSM-berichten van UDAP te kunnen ontvangen conform de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-4).
E-036	De CSP-BW applicatie dient MAP-bestanden te kunnen ontvangen conform de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-1).
E-037	De CSP-BW applicatie dient SPaT-bestanden te kunnen ontvangen conform de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-2).
E-038	De CSP-BW applicatie dient CAM-bestanden te kunnen verzenden conform de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-5).
E-039	De CSP-BW applicatie dient SRM-bestanden te kunnen verzenden conform de beschrijving op het CROW-kennisplatform (www.kennisplatform/IVRIDutchprofiles/D3046-3).

Specifieke eisen aan de koppeling met de VPS.

Eis	Omschrijving
E-040	De CSP-BW applicatie dient gekoppeld te zijn met de VPS conform de beschrijving in Annex B.
E-041	De CSP-BW applicatie dient in ieder geval de aansluitprotocollen AMQP, SBMP en API te ondersteunen.

3.4 Niet-Functionele eisen

3.4.1 Algemene eisen

Hieronder staan de eisen benoemd die gelden voor de dienstverlening in de gehele keten van iVRI en iBFA tot een eindgebruiker en terug.

Eis	Omschrijving
E-042	De CSP-BW applicatie dient binnen 200 milliseconden na ontvangst van de voertuigpositiegegevens een CAM-bericht en een SRM-bericht te hebben opgesteld en naar UDAP te hebben gezonden, als het voertuig waarvan de voertuigpositiegegevens afkomstig zijn- gerechtigd is tot het doen van een prioriteitsaanvraag.
E-043	De CSP-BW dienstverlener dient ten minste 99% van de ontvangen GPS-gegevens in juiste SRM-berichten om te zetten.

Eis	Omschrijving
E-044	De SCP-BW dienstverlener dient ervoor te zorgen dat ten minste 99% van de SRM-berichten voldoet aan de landelijke iVRI-standaarden.
E-045	De CSP-BW dienstverlener dient de gegevens die zij verkrijgt bij haar CSP-BW dienstverlening alleen voor de CSP-BW dienstverlening te gebruiken.
E-046	De CSP-BW dienstverlening dient te allen tijde te voldoen aan de in Nederland en Europa geldende wet- en regelgeving.
E-047	De CSP-BW dienstverlening dient te allen tijde beschikbaar zijn in de Nederlandse taal.
E-048	De CSP-BW dienstverlening dient gedurende de gehele contractperiode te functioneren binnen de doelstellingen van de CSP-BW zoals opgenomen in paragraaf 2.2 van het PvE.
E-049	De systemen die door de CSP-BW dienstverlener worden ingezet ten behoeve van de CSP-BW dienstverlening, dienen alle, onderling gesynchroniseerd, te functioneren aan de hand van een UTC-tijdssignaal, dat is gesynchroniseerd met het UTC-tijdssignaal aan de hand waarvan UDAP functioneert.
E-050	De CSP-BW dienstverlening dient bij presentatie van de tijd aan de gebruiker altijd gebruik te maken van CET(Central European Time = UTC + one hour) met automatische wisseling van zomertijd CEST (Central European Summer Time) en wintertijd CET (Central European Time).
E-051	De CSP-BW dienstverlener dient aan te tonen dat conform de eisen gebruik is gemaakt van gestandaardiseerde interfaces en dataformats bij de ontwikkeling van de gevraagde producten en diensten. Wijzigingen in de gehanteerde standaarden dienen in overleg met de leveranciers van de VPS, UDAP en informatiediensten in de Brandweervoertuigen te worden doorgevoerd in deze interfaces en dataformats.
E-052	Alle gebruikte en verwerkte data zullen bij voorkeur binnen Nederland maar in ieder geval binnen de grenzen van de Europese Economische Ruimte worden opgeslagen en ver-/bewerkt, zodanig dat deze uitsluitend onder de jurisdictie van EU-wetgeving valt. Door de CSP-BW dienstverlener wordt geen toegang gegeven aan derden tot data die voortkomt uit de uitvoering van de Overeenkomst, tenzij na expliciete toestemming van Opdrachtgever.
E-053	De CSP-BW dienstverlening dient te voldoen aan NORA (Nederlandse Overheid Referentie Architectuur, www.noraonline.nl).

3.4.2 Eisen/Opties aan de continuïteit

Eis	Omschrijving
E-054	De CSP-BW dienstverlening dient op jaarbasis een beschikbaarheid te hebben van minimaal 99,9%. Dit is inclusief gepland onderhoud. Dit betekent dat (cumulatief) de onbeschikbaarheid van de dienstverlening per contractjaar maximaal 31.536 seconden mag zijn (en in een schrikkeljaar 31.622 seconden).
E-055	De maximale duur van onbeschikbaarheid van de dienstverlening bedraagt: <ul style="list-style-type: none"> 1) 5 minuten in de uren tussen 05:00 en 09:30; 2) 5 minuten in de uren tussen 15:30 en 19:00; 3) 15 minuten in de uren tussen 09:30 en 15:30; 4) 15 minuten in de uren tussen 19:00 en 24:00; 5) 120 minuten in de uren tussen 24:00 en 05:00.

	Iedere onderbreking van de dienstverlening geldt als onbeschikbaarheid. Binnen één (1) minuut na het ontstaan ervan moet desbetreffende onbeschikbaarheid door dienstverlener zijn gemeld op een door Opdrachtgever aan te wijzen website. Iedere opgetreden onbeschikbaarheid, de oorzaak en de duur ervan, alsmede de maatregelen die zijn genomen ter inperking en voorkoming van herhaling van de onbeschikbaarheid moeten worden gerapporteerd (zie Annex C) .
--	---

3.4.3 Certificering en testen

Eis	Omschrijving
E-056	De CSP-BW dienstverlener dient de CSP-BW applicatie te testen en te certificeren conform de procedure zoals opgenomen in: verificatie certificering iVRI 2-0-0 compressed.pdf.aspx (crow.nl)
E-057	De CSP-BW applicatie dient gecertificeerd te zijn gedurende tenminste de gehele contractperiode volgens de voorwaarden zoals opgenomen in de meest recente versie van het document iVRI verificatie en certificering (gepubliceerd op crow.nl).
E-058	De CSP-BW dienstverlener dient voorafgaand aan iedere certificering aan te tonen dat de eisen uit hoofdstuk 3,5 en 7 van het onderliggende PvE worden ingevuld.

3.4.4 Loggings en rapportages

Eis	Omschrijving
E-059	De CSP-BW dienstverlener dient alle handelingen in het systeem te loggen en te monitoren op oneigenlijk gebruik.
E-060	De CSP-BW dienstverlener dient elke mutatie in de CSP-BW applicatie van alle gebruikers, beheerders (inclusief alle door de CSP-BW dienstverlener uitgevoerde mutaties) te loggen en te ontsluiten voor analyse en audit doeleinden.
E-061	De CSP-BW dienstverlener dient een risico op misbruik te signaleren door in ieder geval de volgende abuse cases te kunnen herkennen: <ul style="list-style-type: none"> - Een x aantal mislukte inlogpogingen binnen een periode y; - Een x aantal requests van de VPS aan de CSP-BW applicatie binnen een periode y. De variabelen x en y dienen instelbaar te zijn en in overleg met Opdrachtgever ingesteld. Bij een overschrijding van de waarde(n) x dient de CSP-BW dienstverlener dit als Incident te melden aan Opdrachtgever.
E-062	De CSP-BW dienstverlener dient alle communicatie tussen de CSP-BW applicatie en UDAP, VPS en de Brandweervoertuigen te loggen en op verzoek van de Opdrachtgever dient deze logging te exporteren naar een gangbaar formaat en beschikbaar te stellen aan de Opdrachtgever.
E-063	De CSP-BW dienstverlener dient logfiles te bewaren gedurende een door Opdrachtgever te bepalen periode. Opdrachtgever beslist over bewaartermijnen voorafgaand aan de Operationele Fase. De CSP-BW dienstverlener dient de Opdrachtgever middels het verlenen van toegang tot logfiles te faciliteren om management rapportages uit de loggings te genereren met behulp van COTS software van Opdrachtgever.
E-064	De CSP-BW dienstverlener dient te voorkomen dat gelogde informatie zonder opdracht van Opdrachtgever kan worden aangepast of verwijderd.

3.4.5 Eisen ten aanzien van capaciteit van de Productieomgeving

Eis	Omschrijving
E-065	De Productieomgeving van de CSP-BW applicatie dient de situatie te kunnen ondersteunen dat de helft van alle aangesloten Brandweervoertuigen zijn ingezet.

3.4.6 Eisen met betrekking tot de inpassing binnen de bestaande ICT - architectuur

Eis	Omschrijving
E-066	De CSP-BW applicatie dient aan te sluiten op de bestaande infrastructuur in de keten.

3.4.7 Eisen ten aanzien van Productieomgeving

Eis	Omschrijving
E-067	De CSP-BW dienstverlener dient ervoor te zorgen dat de Productieomgeving gelijk is aan de Testomgeving.

3.4.8 Eisen ten aanzien informatiebeveiliging

Eis	Omschrijving
E-068	De CSP-BW applicatie, de bijbehorende technische infra en de CSP-BW dienstverlenersorganisatie (inclusief onderaannemers) dienen te voldoen aan de Eisen ten aanzien van Informatiebeveiliging zoals vermeld in hoofdstuk 7 van het PvE.

4 Realisatiefase

4.1 Eisen aan het Realisatieplan

Eis	Omschrijving
E-069	De CSP-BW dienstverlener dient een Realisatieplan op te stellen dat zijn aanpak beschrijft van de Realisatie conform de Eisen van het PvE.
E-070	Het Realisatieplan dient te zijn goedgekeurd door Opdrachtgever, alvorens de CSP-BW dienstverlener kan starten met de Realisatie.
E-071	De CSP-BW dienstverlener dient in het Realisatieplan te beschrijven hoe hij de koppelingen met de VPS, het UDAP en de Brandweervoertuigen realiseert. Uitgangspunt bij het realiseren van koppelingen is dat de CSP-BW zich aanpast aan de koppelvlakken en functionaliteiten van de andere ketenpartijen.
E-072	De CSP-BW dienstverlener dient bij het Realisatieplan ten minste te worden ingegaan op de volgende aspecten: <ul style="list-style-type: none">• Een realistische planning op A3-formaat en met fasering inclusief belangrijkste activiteiten per veiligheidsregio, onderlinge logische samenhang tussen de verschillende activiteiten, kritieke pad (doorlooptijd) en mijlpalen;• Wijze van kwaliteitsborging;• Wijze waarop invulling wordt gegeven aan communicatie met de Opdrachtgever/ veiligheidsregio, wegbeheerders en iVRI leveranciers;• De belangrijkste risico's die De CSP-BW dienstverlener voorziet:<ol style="list-style-type: none">1. De CSP-BW dienstverlener benoemt de naar zijn oordeel vijf grootste risico's van de Realisatie;2. De CSP-BW dienstverlener geeft aan welke risico beperkende maatregelen die hij gaat nemen;• De wijze waarop zoveel mogelijk grip op de voortgang van het project aan Opdrachtgever wordt geboden• De wijze waarop de afstemming met de ketenpartijen wordt georganiseerd.

4.2 Eisen aan de Realisatie

Eis	Omschrijving
E-073	De CSP-BW dienstverlener dient het door Opdrachtgever goedgekeurde Realisatieplan uit te voeren en aan de Eisen in hoofdstuk 3 invulling te geven
E-074	De CSP-BW dienstverlener dient alle koppelingen van de CSP-BW applicatie met gekoppelde systemen (UDAP, VPS en optioneel de software in de Brandweervoertuigen) te realiseren om aan de Eisen van hoofdstuk 3 van het PvE te voldoen.
E-075	De CSP-BW dienstverlener dient de koppelingen met UDAP, de VPS en optioneel de Brandweervoertuigen in de CSP-BW applicatie aan te passen aan de bestaande externe systemen.
E-076	De CSP-BW dienstverlener dient zijn organisatie in te richten voor de Instandhouding.

E-077	De CSP-BW dienstverlener dient per veiligheidsregio in overleg met de veiligheidsregio en de wegbeheerders de dienstverlening af te stemmen en te starten (in bedrijf stellen).
-------	---

4.3 Nazorg

Eis	Omschrijving
E-078	De CSP-BW dienstverlener dient direct na de Realisatiefase een periode van "verhoogde dijkbewaking" in te stellen bij de CSP-BW dienstverlenersorganisatie (inclusief eventuele onderaannemers). Onder "verhoogde dijkbewaking" wordt verstaan dat de CSP-BW dienstverlener (inclusief onderaannemers) capaciteit met voldoende kwaliteit voor Opdrachtgever reserveren om issues die zich voordoen met prioriteit in behandeling te nemen en op te lossen in nauwe samenwerking en overleg met Opdrachtgever. De periode van verhoogde dijkbewaking eindigt 2 maanden nadat de eerste veiligheidsregio gestart is met de prioriteitsaanvragen.

4.4 Rapportage

Eis	Omschrijving
E-079	De CSP-BW dienstverlener dient maandelijks de voortgang van de realisatie ten opzichte van het realisatieplan te rapporteren.

5 Operationele fase

De CSP-BW dienstverlener heeft tijdens de Operationele Fase een verantwoordelijkheid in de Instandhouding van de CSP-BW dienstverlening waaronder oa het Operationeel Keten Management (OKM) van de UDAP-keten. De Eisen aan de Instandhouding zijn in dit hoofdstuk beschreven.

5.1 Eisen aan het Instandhoudingsplan en SLA/DAP

Eis	Omschrijving
E-080	De CSP-BW dienstverlener dient een Instandhoudingsplan op te stellen dat zijn aanpak beschrijft van de Instandhouding conform de Eisen van het PvE.
E-081	De CSP-BW dienstverlener dient in het Instandhoudingsplan onderscheid aan te brengen tussen OKM diensten en Instandhouding van de overige CSP-BW dienstverlening.
E-082	Het Instandhoudingsplan dient te zijn goedgekeurd door Opdrachtgever, alvorens de CSP-BW dienstverlener kan starten met de Instandhouding.
E-083	In het Instandhoudingsplan dient De CSP-BW dienstverlener te beschrijven hoe De CSP-BW dienstverlener invulling geeft aan de Instandhouding.
E-084	<p>In het Instandhoudingsplan dient verder minimaal te worden ingegaan op ten minste de volgende aspecten:</p> <p>A. Algemeen:</p> <ol style="list-style-type: none">1. De CSP-BW dienstverlener geeft een gedetailleerde beschrijving en onderbouwing van de werkzaamheden en activiteiten m.b.t. Instandhoudingsdiensten;2. De CSP-BW dienstverlener dient te beschrijven:<ul style="list-style-type: none">• de wijze waarop de Instandhoudingsdiensten als opgenomen in het PvE zullen worden uitgevoerd;• de borging van het (blijven) halen van servicelevels voor Instandhouding;• de communicatie met Opdrachtgever en Veiligheidsregio's;• de inrichting van een dienstenloket (SPoC) en de coördinatie van de diensten;• de inrichting van het proces van incidentbeheer tussen De CSP-BW dienstverlener, Opdrachtgever en de UDAP-keten. <p>B. Organisatie en resources:</p> <ol style="list-style-type: none">1. De CSP-BW dienstverlener geeft een gedetailleerde beschrijving en onderbouwing van de organisatie. Hierbij gaat het om de inrichting en omvang van de Instandhoudingsorganisatie, die noodzakelijk is voor de uitvoering van de diensten, inclusief een beschrijving van eventuele onderaannemers en hun taken en verantwoordelijkheden;2. De CSP-BW dienstverlener beschrijft de rollen, taken, verantwoordelijkheden en bevoegdheden van ieder lid van de Instandhoudingsorganisatie;

	<p>C. Risico's:</p> <ol style="list-style-type: none"> 3. De CSP-BW dienstverlener benoemt de naar zijn oordeel vijf grootste risico's van de Instandhoudingsdiensten; 4. De CSP-BW dienstverlener geeft aan welke risico beperkende maatregelen hij daarbij gaat nemen; 5. De CSP-BW dienstverlener geeft aan welke werkwijze hij gebruikt om deze risico's vroegtijdig te signaleren.
E-085	De CSP-BW dienstverlener dient de Model SLA en DAP op te stellen en goed te laten keuren door Opdrachtgever alvorens De CSP-BW dienstverlener kan starten met de Instandhouding.

5.2 Instandhouding keten

Opdrachtgever wenst een deel van het ketenmanagement te beleggen bij de CSP-BW dienstverlener, hierna genoemd het Operationeel Keten Management (OKM).

Eis	Omschrijving
E-086	De CSP-BW dienstverlener dient een constructieve bijdrage te leveren aan het oplossen van technische en functionele problemen in de informatieketen.
E-087	De CSP-BW dienstverlener is verantwoordelijk voor de werking van de informatiedienst in de iVRI-keten.
E-088	De CSP-BW dienstverlener dient een CSP-ketencoördinator in de organisatie op te nemen die als schakelpunt functioneert tussen enerzijds de aangesloten InformatieServiceProviders, de Veiligheidsregio en eindgebruikers hierbinnen en anderzijds UDAP en de iVRI ketencoördinator.
E-089	De CSP ketencoördinator bewaakt (tevens m.b.v. door UDAP geleverde keteninformatie) het functioneren van de informatiedienst binnen de aansluitvoorwaarden en eisen vanuit de veiligheidsregio's. Hij kan hierbij gebruik maken van de KPI's van UDAP en de streefwaardes.
E-090	De CSP ketencoördinator neemt meldingen aan van UDAP, de iVRI ketencoördinator en ketenmanagement en werkt mee aan de storingsoplossing.
E-091	De CSP-BW dienstverlener dient het ontstaan en afmelden van een Incident met (mogelijke) impact bij andere ketenorganisaties of de werking van de usecases, te melden aan de ketenorganisaties waar sprake is van (mogelijke) impact.
E-092	Indien een onderdeel van de keten niet bereikbaar is, of de afhandeling van een prioriteitsaanvraag niet of met onvoldoende kwaliteit lukt, dient de CSP-BW dienstverlener het betreffende onderdeel van de keten te informeren en dit als ketenissue te melden aan Opdrachtgever (ketenmanagement), vast te leggen en op te volgen.
E-093	De CSP-BW dienstverlener dient haar onderhoudsplan voor aanvang van het kalenderjaar aan te bieden aan de Opdrachtgever, zodat de Opdrachtgever een ketenonderhoudskalender kan samenstellen en ter beschikking kan stellen aan de partijen in de keten. De CSP-BW dienstverlener dient altijd vooraf toestemming voor het uitvoeren van gepland onderhoud te vragen aan Opdrachtgever alvorens deze kan worden uitgevoerd.
E-094	De CSP-BW dienstverlener dient het functioneren van de verbindingen minimaal iedere minuut te controleren.

5.3 Lifecycle Management

Eis	Omschrijving
E-095	De CSP-BW dienstverlener dient ervoor te zorgen dat de voor de CSP-BW dienstverlening toegepaste hard-, software, firmware en diensten (van De CSP-BW dienstverlener en alle eventuele onderaannemers) te allen tijde up-to-date zijn, zodat de continuïteit en veiligheid van de CSP-BW dienstverlening maximaal is geborgd. Hieronder vallen bijvoorbeeld het uitvoeren van functionele updates/upgrades, veiligheidsupdates of het tijdens de looptijd vervangen van hardware.
E-096	De CSP-BW dienstverlener dient veiligheidsupdates/patches binnen 48 uur nadat deze beschikbaar komen, in overleg met Opdrachtgever door te voeren in de CSP-BW software/hardware en/of firmware.
E-097	Indien Opdrachtgever oordeelt dat er sprake is van een calamiteit dan wel dat operationele omstandigheden dit vereisen, dan wel dat Opdrachtgever besluit tot een Freeze periode, kan Opdrachtgever aan CSP-BW dienstverlener verzoeken het Lifecycle Management af te breken en de situatie voorafgaande aan het onderhoud te herstellen (rollback). De CSP-BW dienstverlener dient aan een dergelijk verzoek onmiddellijk gevolg te geven.

5.4 Incidentbeheer

Beschrijving van de dienst

Incidentbeheer is erop gericht om door of namens Opdrachtgever of door de CSP-BW dienstverlener geconstateerde Incidenten af te handelen afhankelijk van de Prio die Opdrachtgever aan het Incident toekent.

Opdrachtgever meldt een Incident aan bij het SPoC van de CSP-BW dienstverlener. Indien de CSP-BW dienstverlener een Incident opmerkt, meldt de CSP-BW dienstverlener dit per ommegaande bij Opdrachtgever.

Prioriteiten

Voor Incidenten met betrekking tot de Productieomgeving is de volgende prioriteitenmatrix van toepassing. Indien een van de beschreven situaties optreedt, zal het Incident in overeenstemming met de aangegeven prioriteit worden geregistreerd en behandeld:

Productieomgeving	Prio		
	1	2	3
Functionaliteit CSP-BW en keten			
Het kunnen behandelen van een prioriteitsaanvraag*	Functionaliteit is niet beschikbaar in meer dan één Veiligheidsregio/hoge ernst van het incident	Functionaliteit is niet beschikbaar voor één Veiligheidsregio/medium ernst van het incident	Functionaliteit is deels niet beschikbaar voor één of meer Veiligheidsregio's/ lage ernst van het incident
Security Incident			

Productieomgeving	Prio		
	1	2	3
Risico op impact van het Incident op de CSP-BW dienstverlening	Hoog	N.v.t	Medium en laag
Calamiteit			
Calamiteit die impact heeft of kan hebben op de CSP-BW dienstverlening	Door Opdrachtgever bepaald	Door Opdrachtgever bepaald	Door Opdrachtgever bepaald

*) Hieronder vallen ook ketenincidenten zoals bijvoorbeeld:

- het afbreken van de prioriteitsaanvraag met als gevolg het uitblijven van tijdige positie updates vanuit het VPS;
- Het uitblijven van een SSM-bericht op een prioaanvraag;
- Het niet verkrijgen van een 'granted' bij iVRI's;
- Afwijkingen van de berekende route;
- Verkrijgen van 'rejected' na 'granted' of 'max. presence' na 'granted'.

Functiehersteltijden

De onderstaande tabel geeft de prestatie-indicatoren weer die samenhangen met Functieherstel door de CSP-BW dienstverlener.

Functiehersteltijden	
Prioriteit	Functiehersteltijd
Prio 1	2 uur (24 uur per dag/7 dagen per week)
Prio 2	8 Kantooruren
Prio 3	16 Kantooruren

Start en einde van de dienst

Wanneer start de dienst?	Deze dienst start nadat Opdrachtgever een Incident inclusief een Diagnose heeft aangemeld bij de CSP-BW dienstverlener of door melding van een Incident door de CSP-BW dienstverlener. Opdrachtgever classificeert vervolgens het Incident.
Wanneer is de dienst gereed?	De dienst is gereed nadat het Incident door de CSP-BW dienstverlener is afgemeld bij Opdrachtgever, Functieherstel heeft plaatsgevonden en de afmelding door Opdrachtgever is geaccepteerd.

Eisen aan de dienst

Eis	Omschrijving
E-098	De CSP-BW dienstverlener dient Incidenten af te handelen conform de door Opdrachtgever vastgestelde Prio en Functiehersteltijden, zoals beschreven in paragraaf 5.4.
E-099	De CSP-BW dienstverlener dient op Werkdagen beschikbaar te zijn voor Opdrachtgever om Incidenten af te handelen en er te allen tijde voor te zorgen dat hij de Functiehersteltijden voor Incidenten zoals gedefinieerd in paragraaf 5.4 kan realiseren.
E-100	De CSP-BW dienstverlener dient te accepteren dat de administratie van Opdrachtgever leidend is voor het bepalen van Functiehersteltijden.

E-101	De CSP-BW dienstverlener dient de van Opdrachtgever verkregen informatie betreffende een Incident zoals een uniek incidentnummer, locatie, tijd, omvang, klacht en symptomen van het Incident te registreren en het Incident direct in behandeling te nemen.
E-102	Opdrachtgever kan besluiten om de Classificatie van een Incident te wijzigen indien de impact van een incident ernstiger of juist minder ernstig blijkt te zijn dan initieel ingeschat. Na melding van deze wijziging door Opdrachtgever, dient de CSP-BW dienstverlener per direct te handelen conform de gewijzigde Classificatie. De Functiehersteltijd wordt gemeten vanaf het moment van wijzigen van de Classificatie indien de Classificatie is verhoogd.
E-103	De CSP-BW dienstverlener dient alle Incidenten te registreren onder een registratienummer en dit registratienummer per ommegaande door te geven aan Opdrachtgever, het Incident nader te beschrijven en aan te vullen met relevante bevindingen.
E-104	De CSP-BW dienstverlener dient maandelijks een rapportage, die op een in overleg met Opdrachtgever overeengekomen wijze is beveiligd, in Excel-formaat te verstrekken aan Opdrachtgever met de in de afgelopen maand geregistreerde Incidenten (zie Bijlage D).
E-105	De CSP-BW dienstverlener dient alle communicatie met betrekking tot Incidenten aan te melden bij het single point of contact van Opdrachtgever.
E-106	Indien de CSP-BW dienstverlener een Incident heeft opgelost middels een tijdelijke oplossing, blijft de CSP-BW dienstverlener verantwoordelijk voor het vervangen van deze tijdelijke oplossing door een definitieve oplossing. De CSP-BW dienstverlener dient ervoor te zorgen dat een tijdelijke oplossing binnen maximaal 10 Werkdagen is vervangen door een definitieve oplossing, tenzij Opdrachtgever akkoord gaat met een continuering van de tijdelijke oplossing.
E-107	Bij Incidenten van Prio 1 dient de CSP-BW dienstverlener reguliere statusupdates te verstrekken. Bij Prio 1 is er minimaal elk half uur telefonisch een statusupdate. Bij Prio 2 en 3 is er een eerste status update binnen 1 kantoor uur. Een statusupdate bevat minimaal de status quo en de verwachte resterende Functiehersteltijd.
E-108	Indien het Incident voortkomt uit acties van derden (bijvoorbeeld bij cybercrime), dient Opdrachtgever onverwijld te worden geïnformeerd en dient de CSP-BW dienstverlener onverwijld maatregelen te treffen om verder misbruik te voorkomen. De CSP-BW dienstverlener dient voor zover redelijkerwijs mogelijk bewijs te verzamelen dat Opdrachtgever in staat stelt om deze derden aansprakelijk te kunnen stellen. De CSP-BW dienstverlener dient het verzamelde bewijs (waaronder loggings) middels een rapportage ter beschikking te stellen aan Opdrachtgever.
E-109	De CSP-BW dienstverlener dient Opdrachtgever onverwijld telefonisch te informeren over (potentiële) overschrijding van de Functiehersteltijd.

5.5 Wijzigingsbeheer

Beschrijving van de dienst

Opdrachtgever kan gedurende de looptijd van de Overeenkomst de behoefte hebben aan functionele wijzigingen aan de CSP-BW dienstverlening. Opdrachtgever kan de CSP-BW dienstverlener verzoeken een impactanalyse op het wijzigen van de functionele behoefte uit te voeren en, na akkoord van Opdrachtgever, dient de CSP-BW dienstverlener de wijzigingen te realiseren.

Het voorstel voor een functionele wijziging kan eveneens van de CSP-BW dienstverlener komen. Het proces van Wijzigingsbeheer kan slechts worden gestart indien Opdrachtgever akkoord is met het voorstel van de CSP-BW dienstverlener.

Start en einde van de dienst

Wanneer start de dienst?	Dit proces start nadat Opdrachtgever, middels een behoeftestelling, aan de CSP-BW dienstverlener verzoekt een impactanalyse uit te voeren voor een functionele wijziging aan de CSP-BW dienstverlening.
Wanneer is de dienst gereed?	Dit proces eindigt na afronding van de in de behoeftestelling en nadere offerte beschreven resultaten en/of werkzaamheden door de CSP-BW dienstverlener en acceptatie daarvan door Opdrachtgever.

Eisen aan de diensten

Eis	Omschrijving
E-110	De CSP-BW dienstverlener dient binnen 10 Werkdagen na het ontvangen van de behoeftestelling van Opdrachtgever een impactanalyse voor het realiseren van de behoefte van Opdrachtgever te maken.
E-111	De impactanalyse van de CSP-BW dienstverlener bevat in ieder geval een beschrijving van de werkzaamheden en de tijd en kosten om de behoefte van Opdrachtgever in te vullen, eventuele aanpassingen om aan de geldende beveiligingsmaatregelen te blijven voldoen en een nadere offerte aan Opdrachtgever.
E-112	Na akkoord door Opdrachtgever realiseert de CSP-BW dienstverlener de in de nadere offerte afgesproken functionaliteit/diensten tegen de in de nadere offerte opgenomen voorwaarden.

5.6

Adviesdiensten

Beschrijving van de dienst

Opdrachtgever verwacht dat er tijdens de looptijd van de Overeenkomst behoefte ontstaat aan advies rondom de scope van de dienstverlening.

Start en einde van de dienst

Wanneer start de dienst?	Dit proces start nadat Opdrachtgever, middels een behoeftestelling, aan de CSP-BW dienstverlener verzoekt een nadere offerte uit te brengen voor adviesdiensten.
Wanneer is de dienst gereed?	Dit proces eindigt na afronding van de in de behoeftestelling en nadere offerte beschreven resultaten en/of werkzaamheden door de CSP-BW dienstverlener en acceptatie daarvan door Opdrachtgever.

Eisen aan de dienstverlening

Eis	Omschrijving
E-113	De CSP-BW dienstverlener dient op basis van een behoeftestelling door Opdrachtgever adviesdiensten te leveren.
E-114	De CSP-BW dienstverlener dient Opdrachtgever binnen 10 dagen na het ontvangen van de behoeftestelling te voorzien van een nadere offerte betreffende de gevraagde adviesdiensten en, na goedkeuring van de nadere offerte door Opdrachtgever, deze adviesdiensten vervolgens te leveren.

5.7 Probleem beheer

Beschrijving van de dienst

Problemen zijn:

- Incidenten die zich blijven herhalen, of
- Incidenten met een onbekende oorzaak

Opdrachtgever is er bij gebaat dat Problemen in een zo vroeg mogelijk stadium worden herkend, geanalyseerd en opgelost.

Start en einde van de dienst

Wanneer start de dienst?	Dit proces start indien Opdrachtgever een Probleem heeft aangemeld bij de CSP-BW dienstverlener.
Wanneer is de dienst gereed?	Dit proces eindigt nadat de CSP-BW dienstverlener het Probleem heeft opgelost.

Eisen

Eis	Omschrijving
E-115	De CSP-BW dienstverlener dient potentiële Problemen te signaleren en als Probleem kandidaat aan te melden bij Opdrachtgever. Opdrachtgever bepaalt of een kandidaat kwalificeert als Probleem.
E-116	De CSP-BW dienstverlener dient Opdrachtgever binnen 2 weken na aanmelding van het Probleem een plan te verstrekken met daarin: <ul style="list-style-type: none">• Probleem omschrijving;• Onderliggend bewijs/gegevens;• Een analyse van de oorzaak van het Probleem;• Advies ten aanzien van een oplossing of een tijdelijke maatregel;• Een aanpak hoe het Probleem op te lossen;• Een planning wanneer het Probleem is opgelost;• De kosten voor het oplossen van het Probleem.
E-117	De CSP-BW dienstverlener dient dit plan na goedkeuring door Opdrachtgever uit te voeren en koppelt dit na uitvoering terug aan Opdrachtgever.

5.8 Ondersteunende diensten

Deze paragraaf beschrijft de Eisen die Opdrachtgever aan De CSP-BW dienstverlener stelt ten aanzien van ondersteunende diensten als communicatie, coördinatie en kwaliteit.

5.8.1 Bereikbaarheid van de CSP-BW dienstverlener

Beschrijving

Het is noodzakelijk dat de CSP-BW dienstverlener een single point of contact (SPoC) inricht ten behoeve van Opdrachtgever. Dit SPoC dient voor de aanmelding en borging van een adequate afhandeling van Incidenten en calamiteiten door de CSP-BW dienstverlener. Tevens dient het SPoC voor de afroep van andere diensten zoals beschreven in het PvE.

Eisen

Eis	Omschrijving
E-118	De CSP-BW dienstverlener richt een SPoC in en deze dient op Werkdagen (8.30 – 17.00 uur) zowel telefonisch als per e-mail bereikbaar te zijn voor de aanmelding en registratie van Incidenten.
E-119	De CSP-BW dienstverlener dient op Werkdagen (8.30-17.00 uur) zowel telefonisch als per e-mail bereikbaar te zijn als SPoC voor de aanmelding, borging en adequate afhandeling van alle CSP-BW diensten.
E-120	De CSP-BW dienstverlener dient zich te houden aan de volgende normen: <ul style="list-style-type: none">- Menselijke response op telefoon binnen 30 seconden na binnenkomst oproep (voice-mail, VRS of andere automatische beantwoording geldt niet als response);- Responsetijd op email binnen 30 minuten na ontvangst.
E-121	Het SPoC van de CSP-BW dienstverlener dient in de Nederlandse taal te communiceren.

5.8.2 Risicomanagement

Eis	Omschrijving
E-122	De CSP-BW dienstverlener dient tijdens de looptijd van de Overeenkomst risicomanagement uit te voeren op de CSP-BW diensten.
E-123	De CSP-BW dienstverlener dient in het kader van risicomanagement de volgende processtappen eenmaal per kwartaal te doorlopen en de resultaten (stap 6) met Opdrachtgever te bespreken: <ul style="list-style-type: none">• Risicostap 1 – Doel(en) bepalen, vanuit de context.• Risicostap 2 – Risico's identificeren: wat zijn ze?• Risicostap 3 – Risico's classificeren: hoe klein of groot zijn ze?• Risicostap 4 – Omgaan met risico's: al dan geen maatregelen nemen en vaststellen wie deze maatregelen neemt• Risicostap 5 – Maatregelen op effectiviteit en efficiëntie evalueren.• Risicostap 6 – Over stap 1 t/m 5 communiceren en rapporteren.

5.8.3 Rapportages

Beschrijving

Opdrachtgever wenst regulier een rapportage over de door de CSP-BW dienstverlener geleverde diensten te ontvangen.

E-124	De CSP-BW dienstverlener dient maandelijks conform Annex D de rapportages op te stellen en beschikbaar te stellen.
E-125	Bij een Prio 1 Incident dient de CSP-BW dienstverlener binnen 1 Werkdag uur na het ontstaan van het Incident een rapportage op te leveren. In die rapportage dient de CSP-BW dienstverlener de oorzaak van de verstoring te beschrijven. Uiterlijk 3 Werkdagen na het ontstaan van het Incident dient de rapportage te zijn geactualiseerd en aangevuld met oplossingsrichtingen om herhaling van het Incident te kunnen voorkomen.
E-126	De CSP-BW dienstverlener is verplicht om, indien de NIPV daarom verzoekt, inzage te geven in de wijze waarop de vereiste KPI's worden gemeten en vastgesteld, onderbouwd met logbestanden of andere inputdata.
E-127	De exacte inhoud, vorm en opzet van de periodieke rapportages dient jaarlijks door de CSP-BW dienstverlener met de NIPV te zijn afgestemd.

5.8.4 Klachten en escalaties

E-128	De CSP-BW dienstverlener dient binnen 5 werkdagen schriftelijk te reageren op een klacht van Opdrachtgever
E-129	De CSP-BW dienstverlener dient het escalatieproces overeen te komen met Opdrachtgever in het DAP.

6 Exitfase

Dit hoofdstuk beschrijft de diensten die de CSP-BW dienstverlener dient uit te voeren tijdens de Exit van de CSP-BW diensten.

Eis	Omschrijving
E-130	De CSP-BW dienstverlener dient een Exitplan te schrijven en actueel te houden waarin de activiteiten zijn beschreven die de CSP-BW dienstverlener uitvoert met als doel de CSP-BW diensten naadloos te laten overgaan op (een) door Opdrachtgever geselecteerde partijen.
E-131	De CSP-BW dienstverlener dient in het Exitplan onderscheid aan te brengen tussen de volgende Exitscenario's: i) Exitscenario 'tijdens Realisatiefase tussentijds stoppen' In dit scenario wordt de Overeenkomst tussentijds beëindigd gedurende de Realisatiefase. ii) Exitscenario 'tijdens Operationele fase tussentijds stoppen' In dit scenario wordt de Overeenkomst tussentijds beëindigd tijdens de Operationele fase van de Overeenkomst. iii) Exitscenario 'aan einde looptijd Overeenkomst stoppen' In dit scenario wordt de Overeenkomst beëindigd door het verstrijken van de (verlengde) looptijd van de Overeenkomst.
E-132	De CSP-BW dienstverlener dient in het Exitplan bij elk Exitscenario de volgende informatie op te nemen: a) De wijze waarop informatie en knowhow zal worden overgedragen en gedeeld met Opdrachtgever en overige bij de Exit betrokken partijen, zodat deze inzicht krijgen in de wijze waarop de CSP-BW dienstverlener zijn diensten heeft verleend in relatie tot de CSP-BW diensten. b) De wijze waarop de CSP-BW ervoor zorgdraagt dat de nieuwe CSP-BW naadloos de diensten kan overnemen.
E-133	De CSP-BW dienstverlener dient het Exitplan door Opdrachtgever goed te laten keuren alvorens met de Exit kan worden gestart.

7 Informatiebeveiliging, privacy en Business Continuity

Dit hoofdstuk bevat een aantal Eisen die aan de diensten worden gesteld voor wat betreft informatiebeveiliging, privacy en Business Continuity. De in dit hoofdstuk geformuleerde Eisen gelden voor alle fasen van de samenwerking tussen Opdrachtgever en de CSP-BW dienstverlener en hebben betrekking op zowel de CSP-BW dienstverlening alsmede de organisatie van de CSP-BW dienstverlener.

7.1 Baseline Informatiebeveiliging Overheid (BIO)

Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines voor Rijk, Gemeenten, Waterschappen en Provincies.

De BIO (www.bio-overheid.nl) beschrijft de invulling van NEN/ISO27001 en 27002 voor de overheid. De BIO bevat zowel Eisen die relevant zijn voor de CSP-BW dienstverlener als voor eventuele onderaannemers die de CSP-BW dienstverlener betreft in de Prestatie.

Opdrachtgever heeft vastgesteld dat **BIO Basis Beveiligings Niveau (BBN) 2** van toepassing is voor de CSP-BW.

7.2 Eisen aan de CSP-BW dienstverlener en de CSP-BW dienstverlening

Eis	Omschrijving
E-134	De CSP-BW dienstverlener en de CSP-BW dienen bij de uitvoering van de Prestatie telkens te voldoen aan de geldende wet- en regelgeving op het gebied van informatiebeveiliging, waaronder maar niet beperkt tot de BIO, VIR-BI en de WBNI.
E-135	De CSP-BW dienstverlener dient een organisatie rondom informatiebeveiliging te hebben ingericht overeenkomstig ISO270001/27002 en BIO, conform beveiligingsniveau BBN 2.
E-136	De CSP-BW dienstverlener dient aan te tonen op welke wijze invulling wordt gegeven aan de gestelde Eisen ten aanzien van informatiebeveiliging middels het Informatiebeveiligingsplan. Ten aanzien van de organisatie van de CSP-BW dienstverlener kan dit plaatsvinden middels certificering (waarbij de scope dient aan te sluiten op de organisatie die benodigd is voor het uitvoeren van de Prestatie).
E-137	De CSP-BW dient te voldoen aan de BIO BBN2.

7.3 Informatiebeveiligingsplan

Eis	Omschrijving
E-138	De CSP-BW dienstverlener dient een Informatiebeveiligingsplan te maken en dit door Opdrachtgever te laten goedkeuren. De CSP-BW dienstverlener dient het Informatiebeveiligingsplan jaarlijks te actualiseren en laten goedkeuren door Opdrachtgever.
E-139	De CSP-BW dienstverlener dient in het Informatiebeveiligingsplan te beschrijven hoe hij invulling geeft aan de BIO. Indien (delen van) deze controls binnen scope vallen van een behaalde (iso)certificering, kan de CSP-BW dienstverlener de invulling achterwege laten en de door de CSP-BW dienstverlener behaalde certificering te gebruiken als onderbouwing.
E-140	De CSP-BW dienstverlener dient maatregelen die van toepassing zijn op de CSP-BW dienstverlening(sorganisatie) en de Instandhouding daarvan, te hebben getroffen voorafgaand aan de Instandhouding.

7.4 Privacy

Eis	Omschrijving
E-141	De CSP-BW dienstverlener en de CSP-BW dienen bij de uitvoering van de Prestatie telkens te voldoen aan de geldende wet- en regelgeving op het gebied van privacy, waaronder maar niet beperkt tot de AVG.
E-142	De CSP-BW dienstverlener is verantwoordelijk voor de beveiliging van de in beheer genomen informatie, waaronder maar niet beperkt tot persoonsgegevens in de zin van de AVG. Niets van deze informatie mag zonder toestemming van Opdrachtgever, al dan niet via externe informatiedragers, voor derden toegankelijk zijn danwel aan derden ter beschikking worden gesteld.
E-143	Indien Opdrachtgever vaststelt dat in het kader van de uitvoering van de Prestatie sprake is van de verwerking van persoonsgegevens door de CSP-BW dienstverlener dient de CSP-BW dienstverlener de verwerkersovereenkomst die als Bijlage bij het Beschrijvend document is gevoegd, aan te vullen en te ondertekenen. In voorkomend geval wordt de desbetreffende ondertekende verwerkersovereenkomst als Appendix opgenomen bij de Overeenkomst. Verder zal de CSP-BW dienstverlener met de door hem in te zetten onderaannemers eenzelfde verwerkersovereenkomst sluiten, indien zij in het kader van de uitvoering van de Prestatie (een gedeelte van de) persoonsgegevens verwerken. In voorkomend geval hoeven de desbetreffende verwerkersovereenkomsten slechts te worden overgelegd indien Opdrachtgever daar in het kader van een audit om vraagt.
E-144	Indien sprake is van de verwerking van persoonsgegevens door de CSP-BW dienstverlener en zijn onderaannemers geldt dat de CSP-BW dienstverlener en zijn onderaannemers medewerking dienen te verlenen aan verzoeken van de betrokken onderzoeksorganisatie ten aanzien van de AVG, zoals inzageverzoeken. Ook ten aanzien van eventuele maatregelen (bijvoorbeeld indien een betrokkene verzoekt tot het bevriezen van persoonsgegevens) dienen de CSP-BW dienstverlener en zijn onderaannemers mee te werken.

7.5 Business Continuity Management

Inleiding

In deze paragraaf zijn de Eisen beschreven die Opdrachtgever stelt aan business continuity management (ofwel continuïteitsbeheer) bij de CSP-BW dienstverlener zelf en bij haar onderaannemers.

Business continuity management bij de CSP-BW dienstverlener, bedreigingen en tegenmaatregelen

De CSP-BW dienstverlener zal informatie aan Opdrachtgever moeten verschaffen over (i) welke bedreigingen (en in welke intensiteit deze) zijn onderkend voor de (voor de diensten noodzakelijke) bedrijfsprocessen van de CSP-BW dienstverlener, (ii) of een afhankelijkheids- en kwetsbaarheidsanalyse is uitgevoerd inclusief de uitkomsten daarvan en (iii) welke maatregelen zijn genomen om deze bedreigingen of de negatieve gevolgen daarvan te voorkomen. Deze verplichting van de CSP-BW dienstverlener heeft niet alleen betrekking op de bedrijfsprocessen die het daadwerkelijk realiseren van de diensten betreffen, maar omvat bijvoorbeeld ook het in stand houden van de daartoe benodigde communicatie met Opdrachtgever.

Onderaannemers en toeleveranciers

De continuïteit van CSP-BW is voor een groot deel afhankelijk van verschillende marktpartijen die onderdeel zijn van een totale beheer- en onderhoudsketen, waaronder de CSP-BW dienstverlener en zijn onderaannemers en toeleveranciers. Derhalve zijn afspraken nodig met alle partijen met wie Opdrachtgever (indirect) zakendoet voor het geval er sprake is van een noodsituatie die de organisatie van een dergelijke marktpartij treft.

Noodsituaties kunnen het gevolg zijn van bijvoorbeeld (niet uitputtend):

- Omgevingsgebeurtenissen zoals een aardbeving, overstroming/wateroverlast, brand, blikseminslag, neerslag en storm, hitte, een aanslag, uitval van elektriciteit of verbindingen, etc.;
- Personele gebeurtenissen zoals ziekte, staking, fraude, etc.;
- Organisatorische gebeurtenissen zoals reorganisatie, wegvallen van de diensten van onderaannemers/toeleveranciers, financiële instabiliteit, etc.

Indien de CSP-BW dienstverlener voor de uitvoering van de diensten gebruik maakt van onderaannemers of toeleveranciers, is en blijft de CSP-BW dienstverlener jegens Opdrachtgever verantwoordelijk voor de correcte en tijdige uitvoering daarvan. Daarmee is het van belang dat de CSP-BW dienstverlener ook ten opzichte van zijn onderaannemers of toeleveranciers maatregelen neemt om Incidenten te voorkomen dan wel indien deze optreden, deze zo snel mogelijk te laten herstellen. Het betreft hier bedrijfsprocessen waarvan de diensten van De CSP-BW dienstverlener aan Opdrachtgever afhankelijk is.

Eisen met betrekking tot Business Continuity Management

Eis	Omschrijving
E-145	De CSP-BW dienstverlener dient binnen een maand na het sluiten van de Overeenkomst een Business Continuity Plan (BC Plan) op te leveren, waarin is beschreven hoe hij bij een ramp of crisis de Prestatie blijft leveren.
E-146	De CSP-BW dienstverlener dient in het BC Plan van de CSP-BW dienstverlener de risico's te onderkennen die een bedreiging zijn voor de continuïteit van de levering van de diensten. De maatregelen en de impact op de duur van het niveau van de diensten zijn hierin beschreven. Hierin neemt De CSP-BW dienstverlener ook zijn onderaannemers en toeleveranciers en afhankelijkheden in de totale keten van de diensten mee. De CSP-BW dienstverlener specificeert

	met welke frequentie welke voorzieningen voor noodsituaties worden getest op juiste, volledige en tijdige inzetbaarheid en met welke frequentie procedures voor noodsituaties worden geoefend.
E-147	De CSP-BW dienstverlener dient het BC Plan ter goedkeuring aan Opdrachtgever aan te bieden. De instandhouding kan pas starten nadat Opdrachtgever het BC Plan van de CSP-BW dienstverlener heeft geaccepteerd en de CSP-BW dienstverlener de in het BC Plan beschreven maatregelen heeft geïmplementeerd.
E-148	De CSP-BW dienstverlener dient minimaal jaarlijks het BC Plan te actualiseren en zo nodig nieuwe maatregelen voor stellen. De CSP-BW dienstverlener dient de testen en oefeningen te evalueren en dient op basis van deze evaluatie de noodzakelijke organisatorische en technische verbetermaatregelen te treffen. In de actualisatie van het BC Plan dienen ook de maatregelen van de uitkomsten van de audits te worden meegenomen en aangevuld. Het geactualiseerde plan dient door De CSP-BW dienstverlener aan Opdrachtgever ter acceptatie te worden aangeboden.
E-149	De CSP-BW dienstverlener dient een Incident aan te melden bij Opdrachtgever indien de voor de diensten relevante bedrijfsprocessen zijn verstoord of dreigen te worden verstoord en dit mogelijk gevolgen heeft voor (het niveau van) de diensten.

Annex A: Interfacebeschrijving koppeling CSP-BW applicatie – UDAP (EVA-bericht)

Wanneer een veld niet is gevuld in de tabel, dan moet het ook niet worden gevuld. In dit geval zullen de standard waarden worden gebruikt voor dit veld.

RESPONSE		
ATTRIBUTE	DESCRIPTION	SAMPLE
header.protocolversion	The DENM protocol version	1
Header.messageID	The messageID conform ETSI EN 302 637-3 V1.3.1	1
Header.stationID	The stationID of the vehicle sending the early warning message. This stationID is obfuscated and the same as the TLC subject ID. The obfuscated ID is kept constant for a single vehicle. DENM messages containing the same header.stationID therefore are originated from the same vehicle and can/must be processed in order of receiving.	10030060
denm.management.actionID.originatingStationID	Same stationID as the header. Is the obfuscated vehicle ID of the ambulance/firebrigade vehicle.	10030060
denm.management.detectionTime	The detection time as defined in ETSI EN 302 637-3 V1.3.1	633269652000
denm.management.referenceTime	The reference time as defined in ETSI EN 302 637-3 V1.3.1	633269652000
denm.management.eventPosition.latitude	Latitude of the current vehicle position. Encoded according to ETSI EN 302 637-3 V1.3.1 specifications	530895860

denm.management.eventPosition.longitude	Longitude of the current vehicle position. Encoded according to ETSI EN 302 637-3 V1.3.1 specifications	66676055
denm.validityDuration	The duration for which this denm message may be considered valid. Default 2 seconds as positions are sent every second	2
denm.stationType	The vehicle modality of the sending actor. Currently set to 10 (special vehicle) in accordance with ETSI EN 302 637-3 V1.3.1 specifications	10
denm.situation.eventType.causeCode	The DENM event cause code, according to ETSI EN 302 637-3 V1.3.1 specifications. Set to code 95	95
denm.situation.eventType.subCauseCode	The DENM event subcause code, according to ETSI EN 302 637-3 V1.3.1 specifications. Set to code 2.	2
denm.location.eventSpeed.speedValue	The speed of the vehicle, encoded according to ETSI EN 302 637-3 V1.3.1 specifications.	694
denm.location.eventPositionHeading.headingValue	The heading of the vehicle, encoded according to ETSI EN 302 637-3 V1.3.1 specifications.	2450

Annex B: Interfacebeschrijving koppeling VPS – CSP-BW applicatie

1. Inleiding:

Dit document beschrijft welke data zal worden verstrekt aan de CSP-BW vanuit de VPS. De VPS zet de inkomende voertuig posities één op één door, tenzij hieronder beschreven is dat de VPS hiervan afwijkt. Dit is dan beschreven onder toelichting. De leverancier van de VPS 1.0 heeft dit document één op één uitgewerkt in een technische vertaling in Jason.

2. Data die betrokken wordt uit web service van GMS

De VPS maakt een koppeling met de web service van GMS om de te kunnen toetsen of een voertuig gekoppeld is aan een incident.

Toelichting: de VPS maakt hier gebruik van bij de API 'Talking Traffic' en de API 'aan incident gekoppelde voertuigen' om alleen voertuigen door te laten die gekoppeld zijn aan een incident.

Dit betreft het de volgende data:

- incident nummer indien een voertuig aan een incident is gekoppeld. Toelichting: VPS geeft dit nummer níet door aan de uitgaande API's, wordt slechts gebruikt voor filtering binnen de VPS.
- de inzet rol ofwel voertuigsoort (beiden gangbaar),
- de status van het voertuig (buiten dienst, op kazerne, aanrijdend, ...) . webservice is zowel push service als opvraagbaar,
- En de prioriteit van het voertuig,
- Aanrijcoördinaat van het incident. Toelichting: wordt gebruikt indien het voertuig bericht deze niet bevat. Toelichting bij GMS data: Status: deze moet de VPS continu bijhouden als je naar restdekking kijkt. Stilstaande voertuigen hebben zeer beperkte status updates.

3. De data die de regio's aanleveren verdelen we onder in 4 categorieën.

Dit wordt gedaan omdat verschillende toepassingen verschillende data gebruiken. Per toepassing is genoemd welke data hierbij nodig is.

3i. Categorie Basis:

Hier beschrijven we de minimale databehoeftes voor de toepassingen:

- Specialismen, in het bijzonder natuurbrand beheersing,
- interregionale inzet en
- landelijk inzicht t.b.v. crisisbeheersing:

De update frequentie moet voor een rijdend voertuig minimaal iedere 30 seconde zijn voor de volgende data:

- a. Actuele GPS-positie van het voertuig.
- b. Gebruik coördinatenstelsel (indien anders dan WGS84).

Toelichting: De VPS vertaalt de inkomende voertuig positie naar WGS84, indien deze in ander formaat wordt aangeleverd. Create timestamp van de positie. Toevoeging Steven van format zie 3i.a Onderstaande velden worden bij iedere wijziging van dat veld doorgegeven:

- c. Roepnummer (uniek per voertuig)¹. Toelichting: Roepnummer en roepnaam zijn synoniem bij de brandweer.
- d. Status voertuig; deze komt uit de web service, dus niet van de regio!

Optioneel

- e. Voertuig alleen zichtbaar voor de meldkamer? (boolean Ja/ Nee, default op Nee). Indien deze boolean op Nee staat of indien dit veld niet meegegeven wordt, dan zal het voertuig zichtbaar zijn voor alle toepassingen die een doelbinding hebben. Indien dit veld de waarde Ja heeft, geeft de VPS de positie van het voertuig alleen door aan de Toepassing meldkamer en eventueel aan de toepassing Talking Traffic indien boolean TT op Ja staat (zie 3iv. i) Toelichting: dit veld kan de regio gebruiken om bijvoorbeeld dienstvoertuigen wel of niet zichtbaar te maken voor toepassingen. Dit kan ook tijdelijk zijn, bijvoorbeeld buiten kantooruren. Indien deze boolean met Ja wordt doorgegeven, dan geeft de VPS voor dit voertuig in de navolgende update de positie NULL, NULL door. Toelichting: Meldkamers willen alleen inzetbare voertuigen zien, geen voertuigen die niet aan een incident zijn te koppelen. Voertuigen voor verplaatsen van kantoorpersoneel zou je dus altijd buiten de VPS moeten houden/ niet moeten aanleveren als regio. Daarom zijn ook lang niet alle DA's zijn als voertuig in GMS opgenomen omdat ze alleen voor dienstreizen gebruikt worden en niet voor inzet.

3ii. Categorie Gebruik meldkamers: n.v.t..

3iii. Categorie dynamisch alarmeren: n.v.t.

3iv Gebruik Connected Traffic:

Hier beschrijven we de aanvullende databehoeftes (naast die hierboven beschreven onder 3.i basis) voor de toepassing:

- Talking Traffic

Als de regio gebruik wil maken van Talking Traffic dan worden de hoogste eisen gesteld aan de voertuig posities.

De aansluitvoorwaarden voor gebruik Talking Traffic, tezamen met de basis voorwaarden en de gebruik meldkamer voorwaarden zijn:

De minimale update frequentie moet voor een rijdend voertuig minimaal iedere 1 seconde (tijdelijke afwijkingen in de frequentie zijn toegestaan) zijn voor de volgende data:

- Geschikt voor TT (boolean ja/ nee). Deze Boolean moet waarde Ja hebben. Toelichting: de VPS controleert voor deze voertuigen: Indien het dataveld 'geschikt voor Talking Traffic = Ja' én het roepnummer is gekoppeld aan een actueel incident én de update frequentie is minimaal iedere seconde, dan dient de VPS deze voertuigposities, inclusief datavelden door te zetten naar de koppeling voor Talking Traffic. Ook als het veld alleen zichtbaar voor de meldkamer op Ja staat.
- Actuele snelheid in km/uur.
- gps-positie in WGS84
- Timestamp uit de GPS ontvanger per doorgegeven voertuig positie

Onderstaande velden worden bij iedere wijziging van dat veld doorgegeven:

- Zichtbaarheid voertuig (boolean ja/ nee, default op nee). Deze moet waarde Ja hebben.
- Voertuigrol (primaire rol conform de landelijke standaardisering) komt uit Web service!.
- Aanleveren regionummer; dit komt mee in het roepnummer (eerste 2 cijfers)

- p. (Toelichting: 26 voor NIPV materieel, 32 voor België, 49 voor Duitsland, 28 voor defensie. Wordt gemeld door ingezette regio? Of 26 uit NIPV volgsysteem? Defensie volgsysteem?)
- q. Prioriteit soms ook als Type rit aangeduid conform de indicatie van de prioriteit klassen als gehanteerd door de meldkamer. Wordt aangeleverd door de meldkamer

Toelichting : Voor de brandweer is dit de Prioriteit. Dit gegeven kan uit GMS gehaald worden. Het is echter geen onderdeel van de eenheid gegevens volgens de GMS-GIS koppel spec's maar van de Incident gegevens. Het is een getal tussen de 1 t/m5 of kan leeg/0 zijn. Het incident krijgt in NL prioriteit, niet het voertuig. Gevolg is dat ieder voertuig gekoppeld aan een incident dezelfde prioriteit krijgt. Als het er puur om gaat of het voertuig met optische en geluidssignalen rijdt zou die informatie eigenlijk vanaf het voertuig binnen gehaald moeten worden. Een voertuig kan onder bijzondere omstandig heden ook bij Prio 2 incident met OGS te gaan rijden b.v. bij file.

- r. Status voertuig, toelichting: voor de Early Warning (EVA) toepassing is het nuttig om te weten of het Voertuig 'actief' is, ook al staat het stil. Op deze manier kunnen naderende weggebruikers worden gewaarschuwd voor een stilstaand Voertuig dat een incident aan het "behandelen" is.
- s. Roepnummer: door te geven zoals een voertuig dat voert, al dan niet zichtbaar op het voertuig.
- t. Bestemming als WGS84 coördinaatpaar komt van de routenavigatie. Als dit niet bekend is komt dit van de web service, dit wordt de aanrij coördinaat genoemd. Een eis is dat dit een coördinaatpaar is en geen adres: een adres kan tot verschillende interpretaties leiden qua locatie van de bestemming per serviceprovider, dit is onwerkbaar. De service provider gebruikt de bestemming om de route te (her)berekenen vanaf de actuele locatie van het Voertuig.
- u. EN/OF Route als WGS84 WKT linestring + indicatie gebruik: indien het mogelijk is een route mee te geven heeft dit de voorkeur. Let wel: deze route is idealiter de route waarop de navigatie in het Voertuig gebaseerd is. Komt de route uit een tussenliggend systeem en wordt deze niet tot in het Voertuig gebracht, markeer dat als dusdanig in het koppelvlak. Dit laat service providers toe om, in afstemming met de nood- en hulpdiensten, te bekijken of eigen routeplanner beter geschikt is voor de routeberekening. Indien routes worden doorgegeven, dan is de eis dat het systeem de route bijwerkt als het voertuig van de route afwijkt. Zo niet, dan wordt teruggevallen op approach prioriteit door de service provider.

Annex C – Eisen aan rapportages in de operationele fase

Ter inleiding

In deze Bijlage zijn de gegevens vermeld welke de CSP-BW dienstverlener vanaf de start van de instandhoudingsfase dient te registreren en periodiek in rapportage aan te leveren.

Het veiligheidsregio's en namens haar de NIPV, wensen middels die periodieke rapportage vanuit de CSP-BW dienstverlener een deugdelijk en betrouwbaar inzicht te krijgen in de breedte en diepgang van data-uitwisseling via de CSP-BW applicatie met de VPS en UDAP, als ook de kwaliteit van de ontvangen en verstrekte data. Op geaggregeerd niveau zullen de door de CSP-BW dienstverlener gerapporteerde gegevens gebruikt worden voor periodieke externe communicatie over ondermeer dekking, spreiding en kwaliteit van zowel data, als uitwisseling daarvan.

De rapportages dienen in een middels HTTPS beveiligde web interface te worden gepresenteerd. De toegang tot deze rapportage dient door de NIPV te worden beheerd.

De periodieke rapportage dient telkens op de 5e dag van de maand beschikbaar te zijn via de web interface.

Navolgend staat aangegeven welke informatie tenminste moet worden gerapporteerd over iedere rapportageperiode.

1. Rapportage over geleverde diensten

In de rapportage door CSP-BW dienstverlener dient voor de rapportageperiode het volgende te zijn opgenomen:

1. Naam van de Veiligheidsregio's waar de CSP-dienstverlening is uitgevoerd;
2. Datum met start- en eindtijd van iedere aan dezen geleverde ondersteuning;
3. Welke onderdelen van de CSP-BW dienstverlening zijn verleend per veiligheidsregio;
4. Totaal aantal aangesloten Brandweervoertuigen per veiligheidsregio;
5. Totaal aantal voertuigen per veiligheidsregio, die gebruik hebben gemaakt van de prioriteitsaanvraagfunctionaliteit;
6. Totaal aantal prioriteitsaanvragen per veiligheidsregio en de spreiding over de aangesloten Brandweervoertuigen per veiligheidsregio;
7. Totaal aantal mislukte prioriteitsaanvragen met de reden van de mislukking onderverdeeld naar de volgende categorieën:

1. Geen juist VPS-bericht ontvangen
2. Fouten in SRM/CAM bericht
3. Geen SSM bericht ontvangen op juist SRM bericht
4. Geen verbinding met UDAP
5. Overig

8. De daadwerkelijk geleverde overige servicelevels per dienst te rapporteren versus de gestelde normen voor de betreffende dienst.
9. De openstaande acties van de CSP-BW dienstverlener en vragen en opdrachten van Opdrachtgever.
10. De kwaliteit van de berekende ETA door inzichtelijk te maken in welke mate berekende ETA's moesten worden bijgesteld.

2. Rapportage over onbeschikbaarheid van de dienstverlening

In deze rapportage dient door de CSP-BW dienstverlener de onbeschikbaarheid die gedurende de rapportageperiode is opgetreden (alsmede de onbeschikbaarheden welke in de voorgaande rapportageperiode zijn opgetreden, maar pas in actuele rapportageperiode zijn geëindigd) te rapporteren. De navolgende gegevens dienen per onbeschikbaarheid te zijn opgenomen:

1. Datum/Tijd (yyyy/mmm/dd - hh/mm/ss) aanvang;
2. Datum/Tijd (yyyy/mmm/dd - hh/mm/ss) einde (indien nog niet geëindigd per einde rapportageperiode: 0000/00/00 – 00/00/00);
3. Totale tijdsduur tussen ontstaan en einde
4. Oorzaak;
5. Genomen maatregelen ter beperking
6. Genomen maatregelen ter voorkoming van herhaling

Daarnaast moet over de totale rapportageperiode worden aangegeven:

1. het totale aantal opgetreden onbeschikbaarheden;
2. het totale aantal geëindigde onbeschikbaarheden;
3. de totale duur van de opgetreden onbeschikbaarheden;
4. de cumulatieve onbeschikbaarheid gedurende de afgelopen 12 maanden. Indien de dienstverlening aan het eind van de rapportageperiode nog niet gedurende 12 maanden operationeel was: de cumulatieve onbeschikbaarheid sinds aanvang instandhouding;
5. de duur van de gerealiseerde beschikbaarheid van de dienstverlening;

6. de cumulatieve gerealiseerde beschikbaarheid gedurende de afgelopen 12 maanden. Indien de dienstverlening aan het eind van de rapportageperiode nog niet gedurende 12 maanden operationeel was: de cumulatieve gerealiseerde beschikbaarheid sinds aanvang instandhouding;
7. Een aanduiding van het onderhoud dat is uitgevoerd (correctief, preventief, adaptief en perfectief) en de effecten daarvan op de CSP-BW dienstverlening;
8. Een aanduiding van het onderhoud dat komende rapportageperiode is voorzien (correctief, preventief, adaptief en perfectief) en de te verwachten effecten daarvan op de CSP-BW dienstverlening;
9. Resterende geldigheid certificaat (UDAP) in maanden.

Rapportage over het functioneren van de keten

1. Percentage afwijkingen van berekende route;
2. Percentage vroegtijdig ingetrokken door andere route;
3. Percentage mislukte prioriteitsaanvragen door te lage frequentie voor ontvangst locatiegegevens.
1. Percentage mislukte prioriteitsaanvragen door een te slechte GPS- kwaliteit