



Specificatie digitale berichtuitwisseling

Versie 4.0
Status: Definitief
November 2020



Inhoudsopgave

1.	INLEIDING	3
1.1	ALGEMEEN	3
1.2	DOELSTELLING	3
1.3	DOELGROEP	3
2.	DATACOMMUNICATIE MET DE RDW	4
2.1	UITGANGSPUNTEN	4
2.2	DE DIENST BERICHTUITWISSELING	4
2.3	DE EISEN	4
3.	BESCHRIJVING VAN DE KOPPELVLAKKEN	5
3.1	KOPPELVLAK INTERNET	5
3.1.1	<i>Certificaten</i>	5
3.2	PROTOCOL	6
3.2.1	<i>Headers</i>	6
4.	GEBRUIK CERTIFICAAT	7
5.	KNOCKING SERVICE	7



1. Inleiding

1.1 Algemeen

De RDW heeft voor communicatie met klanten onder andere een dienst Berichtuitwisseling. Met de dienst Berichtuitwisseling kunnen berichten naar de RDW worden verstuurd die direct worden afgehandeld. Er zijn berichten waarmee bevestigingen op registers kunnen worden gedaan, maar ook berichten waarmee registers gewijzigd kunnen worden.

1.2 Doelstelling

Het doel van dit document is te beschrijven hoe externe klanten technisch een koppeling op dienen te zetten voor berichtuitwisseling. De inhoud van de berichtuitwisseling wordt in dit document niet behandeld.

1.3 Doelgroep

Dit document is geschreven voor architecten, ontwerpers, systeembeheerders en ontwikkelaars die betrokken zijn bij het bouwen en onderhouden van applicaties t.b.v. gegevensuitwisseling met de RDW.



2. Datacommunicatie met de RDW

2.1 Uitgangspunten

De RDW hanteert de volgende uitgangspunten voor datacommunicatie met klanten:

- De uitwisseling van berichten over internet vindt plaats conform de in dit document benoemde specificaties;
- De uitwisseling van informatie is beveiligd met een SSL-tunnel. Door deze techniek te gebruiken, wordt de vertrouwelijkheid van de uitgewisselde gegevens geborgd.
- De SSL-tunnel is tweezijdig. Dit houdt in dat de klant en de RDW zich identificeren met een certificaat. De klant neemt het initiatief tot het opzetten van de verbinding.

2.2 De dienst Berichtuitwisseling

Bij berichtuitwisseling stuurt de klant een bericht naar de RDW dat direct door de RDW verwerkt zal worden. Het antwoord van de verwerking wordt vervolgens naar de klant verstuurd. Communicatie bij het gebruik van de dienst verloopt hiermee synchroon conform de HTTP POST request.

2.3 De eisen

De eisen voor gegevensuitwisseling staat beschreven in:

1. Verstrekkingvoorwaarden inzake het Kentekenregister van de Dienst Wegverkeer
2. Het Certificate Practice Statement (CPS).

Het eerste document wordt toegezonden, en is ook op de volgende locatie te downloaden:

<https://zoek.officielebekendmakingen.nl/stcrt-2015-14523.html>

Het tweede is te downloaden op:

www.rdw.nl (zoek op: CPS)



3. Beschrijving van de koppelvlakken

De dienst berichtuitwisseling wordt aangeboden via internet. De RDW beschikt over een acceptatieomgeving die wordt gebruikt voor acceptatietesten bij het aansluiten van nieuwe klanten.

3.1 Koppelvlak internet

De technische specificaties van dit koppelvlak zijn:

Productie	URL	https://berichten.rdw.nl/start.rdw
-----------	-----	---

Aanroep van deze URL's dient altijd op basis van de hostnaam te gebeuren, en niet op basis van het IP adres.

3.1.1 Certificaten

Voor de beveiliging van dit koppelvlak heeft de RDW gekozen voor een tweezijdige SSL tunnel. Dit betekent dat beide partijen bij het opzetten van de verbinding zichzelf authenticeren door middel van een certificaat. De klant maakt gebruik van een clientcertificaat en de RDW maakt gebruik van een SSL servercertificaat.

Het clientcertificaat wordt door de RDW uitgegeven. Daarnaast wordt aan iedere klant een account en wachtwoord verstrekt. Bij het aanbieden van een XML bericht dient in de meeste gevallen dit account en wachtwoord mee te worden gegeven. De verbinding wordt dus geïnitieerd middels het client certificaat, de account gegevens worden in het bericht mee gestuurd.

Het Certificate Practice Statement (CPS) beschrijft hoe de RDW met haar certificaten omgaat en welke verplichtingen certificaathouders hebben. Het CPS is te vinden op www.rdw.nl (zoek op: CPS)

RDW-certificaten die gecompromitteerd zijn, worden ingetrokken. De Certificate Revocation List (CRL) is een lijst met nummers van ingetrokken certificaten. Voor zowel de acceptatie- als de productieomgeving wordt dezelfde CRL gebruikt. Deze CRL is te vinden op <http://crl.rdw.nl/crl/RDWIssuingCA02.crl>

De RDW checkt bij een aanlogpoging of het clientcertificaat op de CRL staat. Indien dat het geval is, dan wordt de verbinding geweigerd.



3.1.1.1 Servercertificaat

Het SSL-servercertificaat dat de RDW gebruikt, is uitgegeven door QuoVadis. Bij het opzetten van de verbinding moet u de geldigheid van het server certificaat controleren. Hiervoor heeft u twee rootcertificaten nodig. Deze kunt u bij de uitgever downloaden. Het SSL certificaat van de RDW is uitgegeven door de volgende CA:

QuoVadis Root CA 2

QuoVadis Global SSL ICA G2

Onafhankelijk door wie het SSL-servercertificaat is uitgegeven dient bij het opzetten van een verbinding met de RDW altijd onderstaande controles te worden uitgevoerd m.b.t. het SSL-certificaat:

- a. of het certificaat wordt gebruikt binnen de geldigheidsperiode;
- b. of het certificaat is ingetrokken (hiervoor moet de Certificate Revocation List bij de betreffende Certificaat Autoriteit worden geraadpleegd);
- c. of het certificaat is uitgegeven door een vertrouwde Certificaat Autoriteit;
- d. of de bovenliggende certificaten geldig zijn (controle van de certificate chain).

SSL-protocollen

Omdat de oudere SSL protocollen niet veilig genoeg zijn, stelt de RDW de eis dat gewerkt dient te worden met SSL-versies die veilig zijn (SSL-LABS minimaal A-.rating).

SSL session caching

Het opzetten van een SSL-verbinding kost tijd omdat onderhandeld wordt over te gebruiken protocollen, de identiteit van de klant en de RDW wordt gecontroleerd en er sleutels worden berekend om de data te versleutelen. Een groot deel van deze onderdelen kan eenmalig worden uitgevoerd en opnieuw worden gebruikt door SSL session caching toe te passen. Vooral bij het frequent uitwisselen van berichten zal dit significant tijd schelen. Het gebruik van SSL session caching wordt aangeraden. De maximale tijd waarbinnen session resumption is toegestaan is dertig minuten.

3.2 Protocol

De RDW biedt de dienst Berichtuitwisseling aan op basis van het HTTP protocol, waarbij het XML-bericht in de requestbody van een HTTP POST wordt verstuurd. De communicatie verloopt synchroon waardoor het antwoordbericht direct in de responsebody van de HTTP POST wordt meegestuurd. Het HTTP protocol wordt hier puur als transportprotocol gebruikt, waarbij alle functionaliteit van het proces door de inhoud van de berichten wordt afgehandeld. De HTTP statuscode zal dan ook altijd 200 OK zijn, tenzij er technische fouten in de communicatie optreden.

3.2.1 Headers

De volgende HTTP headers moeten worden gevuld:

```
[Content-type: text/xml; charset=utf-8]  
[Host: (RDW URL)]
```

Waarbij RDW URL moet worden vervangen door de aangeroepen URL. Dus voor productie via internet zou de HTTP header zijn: Host: berichten.rdw.nl/start.rdw



4. Gebruik certificaat

Het door de RDW uitgegeven clientcertificaat is uitsluitend bedoeld voor berichtuitwisseling met de RDW. De RDW controleert de berichtenstromen actief op misbruik. Bij constatering van misbruik kan het clientcertificaat worden ingetrokken.

5. Knocking service

Om te controleren of de RDW te bereiken is, kunt u een http get request sturen naar <https://berichten.rdw.nl/knock>. U krijgt vervolgens een http bericht retour met als tekst “OK”.

U kunt deze service op 2 manieren aanroepen: middels uw client certificaat, of door uw klantnaam/bedrijfsnaam in de header te verwerken onder het volgende element: user-agent

Op deze ingang is een rate limit van 1 bericht per seconde ingesteld.