Rijksdienst voor Ondernemend Nederland

Aansluiten op WEBSERVICES van RVO

Versie 1.3
Datum: 14-06-2021

Inhoud

Inleiding

Dit document geeft een indruk van wat er voor nodig is om bij een webservices van RVO aan te sluiten. Enige voorkennis bij de gebruiker, met name van het OAuth koppelvlak, is vereist om te kunnen beginnen met bouwen en testen van de gewenste aansluiting. Wanneer u dit document hebt doorgenomen en u voldoende geïnformeerd bent kunt u contact opnemen met een RVO-beheerder.

Om een webservice te gebruiken moet uw softwaresysteem bij ons bekend zijn. Ook moet u testen of het digitaal uitwisselen van de gegevens goed gaat. Hiervoor heeft u een testaccount nodig. U kunt zich hiervoor aanmelden via het formulier ‘Gebruik webservices’ onder ‘Direct regelen’.

U krijgt dan van ons het **aansluitdocument**, de codes voor de testomgeving en een aantal testsituaties.

Beveiligingsmaatregelen

Als de test goed is gegaan, kunt u met de codes voor de productieomgeving de webservice gebruiken.

RVO is verantwoordelijk voor de informatiebeveiliging van de eigen gegevens, maar ook voor het beschermen van persoonsgegevens. Wij willen daarom zeker weten dat de informatie die wij uitwisselen met uw applicatie, goed beveiligd is.

Daartoe stelt RVO een aantal regels die door de softwareleverancier moeten worden geborgd. De softwareleverancier overlegt daartoe een verklaring welke beveiligingsmaatregelen zijn toegepast aan RVO.

Verstuur deze via Digitaal post versturen onder Direct regelen. Kies in het formulier voor Bedrijfsregistratie > IT-auditverklaring.

OAuth koppelvlak

Bedrijfsmanagementsystemen kunnen voor het uitwisselen van berichten met RVO gebruik maken van webservices. RVO gebruikt voor de identificatie van de gebruiker eHerkenning. De autorisatie voor het gebruik van de webservice verloopt via het OAuth koppelvlak.

De nieuwste standaard hiervoor is OAuth NL GOV

https://publicatie.centrumvoorstandaarden.nl/api/oauth/

Het koppelvlak wordt toegepast voor de RVO webservices van de afdelingen I&R, GEO en Mest.

Na de identificatie en autorisatie kan het bedrijfsmanagementsysteem de berichtuitwisseling met RVO starten. Deze berichtuitwisseling staat beschreven in de diverse berichtenboeken van RVO.

Dit document is bedoeld voor de ICT-ontwikkelaars van de bedrijfsmanagementsystemen en andere toepassingen die gebruik maken van elektronische gegevensuitwisseling met RVO.

Het OAuth koppelvlak is volledig gebaseerd op de OAuth standaarden. Standaard OAuth implementaties kunnen dus zonder enige aanpassing werken met het koppelvlak.

Het is goed om voorafgaand aan de bouw van een aansluiting kennis op te bouwen over het OAuth koppelvlak.
Onderstaand een aantal links met informatie over OAuth.

https://www.tutorialspoint.com/oauth /index.htm

https://medium.com/google-cloud/understanding-oauth2-and-building-a-basic-authorization-server-of-your-own-a-beginners-guide-cf7451a16f66

https://oauth.net/getting-started/

https://www.udemy.com/course/learn-oauth-2/

https://www.pluralsight.com/courses/oauth-2-getting-started

Daarnaast wordt de kennis natuurlijk ook aangeboden door alle reguliere opleidingsinstituten.

1 Gebruik access token

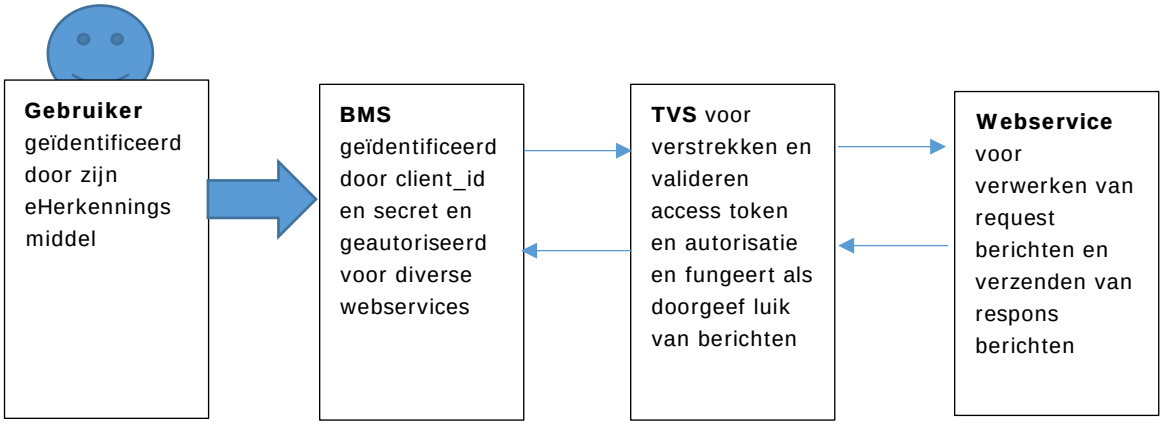
Het OAuth koppelvlak is gebaseerd op het gebruik van een access token.

Er zijn twee stappen:

1. Een gebruiker meldt zich via zijn bedrijfsmanagementsysteem bij RVO aan voor het gebruik van webservices. De gebruiker identificeert zich daarbij vanuit zijn bedrijfsmanagementsysteem bij RVO met behulp van eHerkenning. Na een geslaagde identificatie verstrekt RVO een access token aan het BMS.

2. Het bedrijfsmanagementsysteem wisselt met het verkregen access token de berichten uit met de webservice van RVO. RVO valideert daarbij het gebruikte access token.

Communicatie tussen het bedrijfsmanagementsysteem, de eHerkenningsmakelaar, het OAuth koppelvlak en de diverse webservices wordt afgehandeld door de Toegang Verlening Service (TVS) van RVO zoals in onderstaande afbeelding schematisch weergegeven.



Een bedrijfsmanagementsysteem bevat hiervoor de volgende functies:

- Het bedrijfsmanagementsysteem laat een gebruiker het access token bij RVO aanvragen. De gebruiker logt hiervoor in bij een eHerkenningsmakelaar en identificeert zich met eHerkenning. De gebruiker dient binnen eHerkenning voor zijn onderneming gemachtigd te zijn om de eHerkenningsdienst van RVO '*mijn.rvo.nl (tevens nodig voor NVWA Client Export)*' met betrouwbaarheidsniveau 2+ uit te voeren.
- De login wordt via een embedded browser in het bedrijfsmanagementsysteem gestart.
- Het access token wordt via het OAuth koppelvlak door het bedrijfsmanagementsysteem opgehaald.
- Het access token kan in-memory worden bewaard of worden opgeslagen gerelateerd aan de gegevens van de onderneming waarvoor de gebruiker inlogt. Indien het access token opgeslagen wordt dient de opslag aan de gestelde voorwaarden te voldoen. Zie hiervoor Beveiligingsmaatregelen access token in hoofdstuk 5.
- Het bedrijfsmanagementsysteem geeft het access token mee in de berichten voor de webservice. TVS valideert het acces token en stuurt, bij akkoord, de berichten door naar de webservice.
- In het bedrijfsmanagementsysteem dient een functie aanwezig zijn waarmee de aanwezige access tokens (van de betreffende onderneming) ongeldig gemaakt kunnen worden.

2 OAuth Koppelvlak

2.1 Procedure aansluiten

De leverancier van het BMS voorziet zijn systeem van de mogelijkheid om berichten uit te wisselen met RVO via één of meer webservices van RVO.

De diverse webservices staan beschreven in de berichtenboeken op https://mijn.rvo.nl/webservices.

Een webservice kan alleen via het aangegeven endpoint en met een geldig access token worden benaderd.
Het SOAP bericht van de webservice is beschreven in het betreffende berichtenboek.

TVS valideert het access token. Als de validatie positief is, kan het bericht door de webservice worden verwerkt. TVS geeft dan tevens de bedrijfsgegevens (KVK- en vestigingsnummer) door die met de identificatie met eHerkenning zijn vastgesteld.

Voor het ontwikkelen van de berichtuitwisseling biedt RVO de leverancier de volgende stappen:

- **Ontwikkeling en test**

  De leverancier test en realiseert de aanpassingen op zijn BMS met een eigen test eHerkenningsmiddel in combinatie met een standaard testinrichting van RVO.

  De RVO-beheerder verstrekt de gegevens van het test eHerkenningsmiddel op aanvraag van de leverancier. Tussen aanvraag en verstrekken van het test middel zit gewoonlijk een doorlooptijd van 3 tot 4 werkdagen. De werkwijze met het test eHerkenningsmiddel en de testinrichting is beschreven in het hoofdstuk 4 Login Flow.

  De aanvraag doet u door het formulier op de website https://mijn.rvo.nl/webservices in te vullen. U geeft daarin aan op welke webservice(s) u wilt aansluiten.

- **Productie**

  Als de leverancier de test met de berichtenuitwisseling succesvol heeft afgerond ontvangt hij van de RVO-beheerder de parameters voor zijn ‘eigen’ aansluiting op productie.
  Wij vragen u een verklaring bij ons in te dienen voorafgaand aan het in productie nemen van de aansluiting op de gevraagde webservices (zie hoofdstuk 5 en 6).

2.2 Parameters OAuth koppelvlak

Ontwikkeling, test en productie

De gegevens die kunnen worden gebruikt in het OAuth koppelvlak voor de berichtenuitwisseling met de standaard testinrichting van RVO ontvangt de leverancier van de RVO-beheerder.

Voor de productie omgeving ontvangt de leverancier zijn eigen specifieke parameter set van de RVO-beheerder.

3 Login flow voor Ontwikkeling en test

Dit hoofdstuk beschrijft globaal hoe de login flow werkt en hoe een access token verkregen, gevalideerd en verwijderd kan worden. De beschrijving is toegespitst op de stap ontwikkeling en test.
RVO-beheerder verstuurt op aanvraag een **aansluitdocument** met alle benodigde codes, voorbeelden en URL's.

3.1 Opvragen authorization code

De eerste stap om een access token te ontvangen is het opvragen van een authorization code, door de specifieke url op te vragen.

Met het client_id bepaalt TVS welk bedrijfsmanagementsysteem de identificatie en autorisatie wil laten uitvoeren. De redirect_uri geeft aan waar de verkregen authorization code naar toe wordt gestuurd nadat identificatie succesvol is uitgevoerd. De scope geeft aan welke webservice(s) het bedrijfsmanagementsysteem voor zijn gebruiker wil aanroepen.

De gebruiker stuurt vervolgens de URL naar de toegangverleningservice (TVS) van RVO.

3.2 Inloggen eHerkenning

TVS stuurt de gebruiker na het uitvoeren van 4.1 naar het eHerkenning login scherm. De gebruiker dient vervolgens de drie stappen te doorlopen zoals in onderstaande figuur is weergegeven..

1 - Selecteer de optie Z login AD 1.9 Preprod

2 - Vul de door de RVO-beheerder verstrekte gebruikersnaam en wachtwoord combinatie in.

3 - Vul door eHerkenning verstrekte SMS code in.

Het KVK- en eventueel Vestigingsnummer, verkregen uit de identificatie met eHerkenning, worden door webservice gebruikt voor de verwerking van het bericht (opvragen van gegevens en eventuele controle van machtigingen).

3.3 Authorization code

Als de identificatie in eHerkenning succesvol is verlopen wordt de gebruiker doorgestuurd naar de redirect_uri waarbij de authorization code als URL parameter “code” op de URL staat.

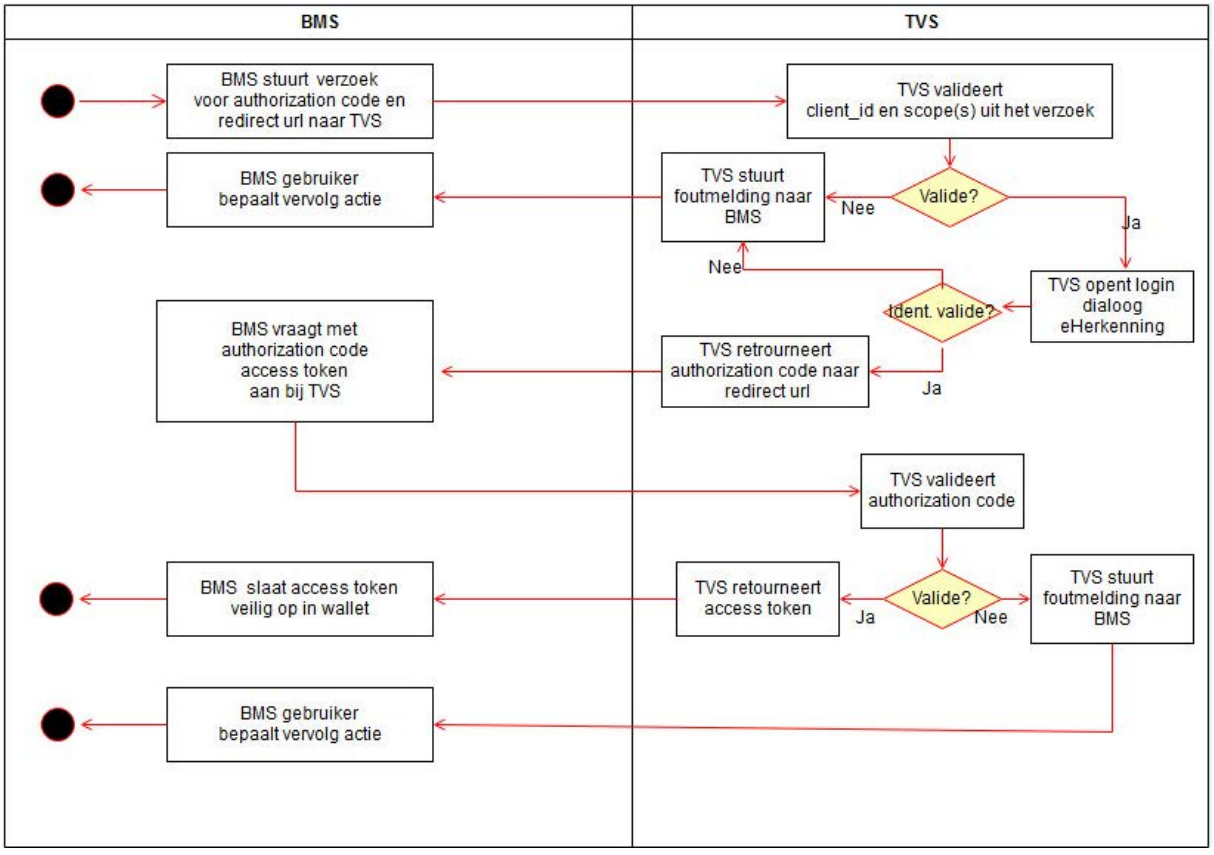
De gebruikersflow is hierbij afgelopen en het embedded browser venster kan worden afgesloten.

3.4 Ophalen access token

De authorization code kan gedurende 5 minuten éénmalig worden gebruikt om een access token bij de TVS REST service op te halen. Dit access token is opgebouwd in het standaard JWT formaat.

Dit access token wordt vervolgens meegestuurd op de authorization header van het SOAP bericht.

De stappen (4.1 t/m 4.4) in deze flow zijn in onderstaande afbeelding schematisch weergegeven.



3.5 Access token gebruiken

Gebruik het access token als HTTP Authorization Header bij de aanroep van de webservice,

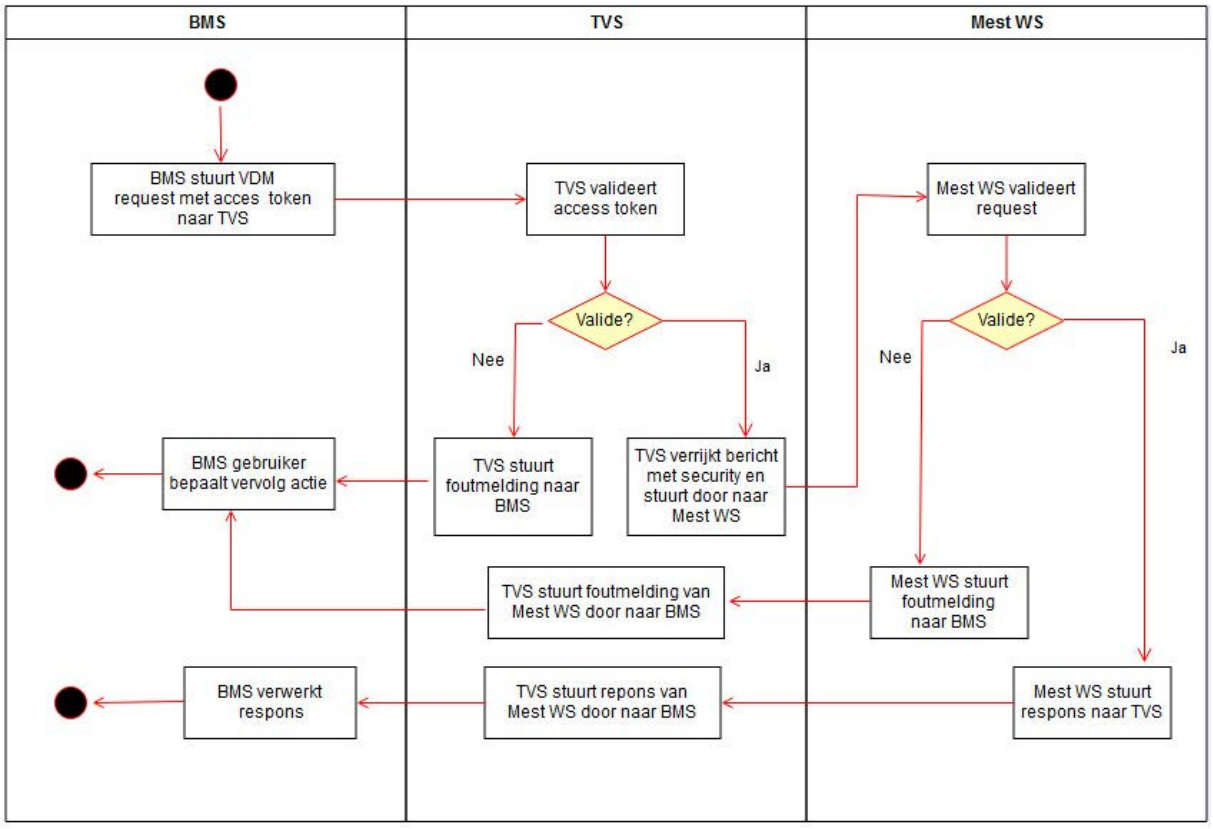
Met als resultaat een SOAP response of met behulp van SOAPUI.

3.6 Foutmeldingen

Voor de testinrichting verloopt het access token na 60 dagen. Dat betekent dat het access token na 60 dagen niet meer gebruikt kan worden om de webservice aan te roepen. Hier wordt dan door TVS een HTTP 401-melding (Unauthorized) voor teruggegeven.

Er kan ook een HTTP 403- (Forbidden) of een HTTP 500-melding (Internal Server Error) worden teruggegeven. Dat betekent dat de webservice, dus niet TVS, het bericht niet kan verwerken.

De stappen (4.5 en 4.6) in deze flow zijn in onderstaande afbeelding schematisch weergegeven voor één van de mest webservices.



3.7 Access token verwijderen

Het access token zal na 1440 uur automatisch worden gedeactiveerd. Hierdoor kan het access token niet meer worden gebruikt. Het token kan ook via de TVS REST service worden verwijderd.

4 Beveiligingsmaatregelen access token

Bij opslag van het access token gelden de volgende voorwaarden.

- In de lokale software moet een functie aanwezig zijn waarmee de aanwezige tokens (van de betreffende onderneming) ongeldig gemaakt kunnen worden;

- Het token wordt op slechts één plaats opgeslagen. Indien zonering wordt toegepast vindt opslag plaats in zone Vertrouwd of Zeer Vertrouwd;

- Het token dient versleuteld te worden opgeslagen door de software van de leverancier.
  de sleutel is veilig opgeslagen en uitsluitend toegankelijk voor de software van de leverancier;

- Toegestane manieren van opslag van het token met een toenemend niveau van informatiebeveiliging:
  1. Het token wordt versleuteld opgeslagen;
  2. Het token wordt versleuteld opgeslagen, de daarbij gebruikte sleutel is gegenereerd op basis van het wachtwoord dat de gebruiker bij authenticatie t.b.v. de applicatie software heeft gebruikt (password-based key derivation);
  3. Het token wordt versleuteld opgeslagen, de daarbij gebruikte sleutel wordt opgeslagen in een Trusted Platform Module (TPM);
  4. Het token wordt versleuteld opgeslagen, de daarbij gebruikte sleutel wordt opgeslagen in een Hardware Secure Module (HSM);

- Als het token mee gaat in een back-up, dan is het ook daarin versleuteld opgeslagen;

- Het token is alleen toegankelijk voor de modules (in de software van de leverancier) die de versleuteling/ontsleuteling en de communicatie met de RVO-systemen verzorgen, dus niet voor andere modules of gebruikers;

- Indien autorisatie op de data wordt toegepast binnen de software van de leverancier:
  het token is alleen toegankelijk voor gebruikers die de communicatiefuncties met de RVO-systemen mogen gebruiken ten behoeve van de belanghebbende die het token na inlog heeft verkregen.

5 Eigen verklaring beveiligingsmaatregelen

RVO is verantwoordelijk voor de informatiebeveiliging van de gegevens onder haar beheer, alsmede voor de bescherming van persoonsgegevens. Bij geautomatiseerde gegevensuitwisseling naar externe applicaties is het noodzakelijk dat in deze externe software ook de nodige beveiligingsmaatregelen zijn getroffen.

Een softwarebedrijf dat wil aansluiten op een webservice van RVO met eHerkenning als authenticatimiddel, is verplicht om een aantal door RVO voorgeschreven beveiligingsmaatregelen te nemen. Hiertoe vraagt RVO een eigen verklaring van dat bedrijf, zie bijlage 1.

In de eigen verklaring staat hoe de relevante softwarematige eisen en de organisatie en werkwijze binnen de organisatie zijn vorm gegeven om het door RVO voorgeschreven beveiligingsniveau te kunnen garanderen. De eigen verklaring moet herhaald worden wanneer het bedrijf aanpassingen doet in de authenticatie-software.

Als bewijs dienen enkele screenshots op basis waarvan een oordeel kan worden gevormd over de mate waarin het softwarebedrijf voldoet aan de gestelde veiligheidseisen.
De mogelijkheid bestaat dat RVO na verloop van tijd een auditverklaring van een externe auditeur op gaat vragen.

Bijlage 1: Eigen verklaring eHerkenning

In het vakje ‘bewijs’ graag verwijzen naar de naam of het nummer van 1 of meerdere screenshots, die in de bijlagen te vinden zijn.

1	
Eis	In de lokale software moet een functie aanwezig zijn waarmee de aanwezige tokens (van de betreffende onderneming) ongeldig gemaakt kunnen worden;
Bewijs	Beschrijving en screenshot

2	
Eis	Het token wordt op slechts één plaats opgeslagen. Indien zonering wordt toegepast vindt opslag plaats in zone Vertrouwd of Zeer Vertrouwd;
Bewijs	Beschrijving en screenshot

3	
Eis	Het token dient versleuteld te worden opgeslagen door de software van de leverancier. De sleutel is veilig opgeslagen en uitsluitend toegankelijk voor de software van de leverancier;
Bewijs	Beschrijving en screenshot, indien mogelijk

4	
Eis	Toegestane manieren van opslag van het token met een toenemend niveau van informatiebeveiliging: a. Het token wordt versleuteld opgeslagen; b. Het token wordt versleuteld opgeslagen, de daarbij gebruikte sleutel is gegenereerd op basis van het wachtwoord dat de gebruiker bij authenticatie t.b.v. de applicatie software heeft gebruikt (password-based key derivation); c. Het token wordt versleuteld opgeslagen, de daarbij gebruikte sleutel wordt opgeslagen in een Trusted Platform Module (TPM); d. Het token wordt versleuteld opgeslagen, de daarbij gebruikte sleutel wordt opgeslagen in een Hardware Security Module (HSM).
Bewijs	Beschrijving en screenshot, indien mogelijk

5	
Eis	Als het token mee gaat in een back-up, dan is het ook daarin versleuteld opgeslagen;
Bewijs	Beschrijving en screenshot, indien mogelijk

6	
Eis	Het token is alleen toegankelijk voor de modules (in de software van de leverancier) die de versleuteling/ontsleuteling en de communicatie met de RVO-systemen verzorgen, dus niet voor andere modules of gebruikers;
Bewijs	Beschrijving en screenshot, indien mogelijk

7	
Eis	Indien autorisatie op de data wordt toegepast binnen de software van de leverancier: het token is alleen toegankelijk voor gebruikers die de communicatiefuncties met de RVO-systemen mogen gebruiken ten behoeve van de belanghebbende die het token na inlog heeft verkregen.
Bewijs	Beschrijving en screenshot

Opgesteld door Directeur:

Bedrijf:

Plaats en datum: