Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Wilhelmina van Pruisenweg
52
2595 AN Den Haag
Postbus 20011
2500 EA Den Haag

Onze referentie
2026-0000145787

Bijlage(n)
1

Datum 27 maart 2026
Betreft Gebruik PKio-certificaat bij aansluiting op de BRP Berichten API

Geachte heer/mevrouw,

De Rijksdienst voor Identiteitsgegevens (RvIG) heeft als voorkeursstrategie het gebruik van Application Programming Interfaces (API's) voor het uitwisselen van gegevens, zoals die wordt toegepast voor onder andere de BRP Berichten API met betrekking tot de BRP-berichtendienst, BRP API inclusief informatieproducten, Reisdocumenten Informatiesystemen (ReIS) en andere diensten. Voor aansluiting op deze voorzieningen gelden specifieke beveiligingsrichtlijnen. In deze brief worden deze richtlijnen toegelicht en wordt het belang hiervan beschreven.

Wat zijn de beveiligingsrichtlijnen?
Om te voldoen aan de geldende beveiligingsrichtlijnen, zoals o.a. Baseline Informatiebeveiliging Overheid 2 (BIO2), is het belangrijk dat iedere organisatie die gegevens van RvIG afneemt, een eigen PKIo-certificaat gebruikt. PKIo is de voorziening van de overheid voor veilige digitale communicatie. Hiermee kunnen overheden onderling veilig met elkaar communiceren, maar ook met burgers en bedrijven. Het PKIo-certificaat bevat een uniek Organisatie-identificatienummer (OIN), waarmee organisaties voor RvIG herkenbaar zijn. Het PKIo-certificaat werkt dus als een digitaal identificatiemiddel voor organisaties.

Waarom is dit nodig?
RvIG beheert de Basisregistratie Personen (BRP) en is daarom verantwoordelijk om de daarin opgenomen persoonsgegevens veilig op te slaan en zorgvuldig uit te wisselen. Om deze verantwoordelijkheid goed te kunnen blijven waarborgen, stelt RvIG eisen met betrekking tot aanvullende veiligheidsmaatregelen. Wanneer deze gegevens worden verstrekt aan een organisatie verschuift de verantwoordelijkheid voor die gegevens naar de afnemende organisatie. Het is dus belangrijk dat duidelijk is wie deze gegevens ontvangt. Alleen door het gebruik van PKIo-certificaten kan RvIG organisaties betrouwbaar identificeren. Dit helpt om misbruik te voorkomen en zorgt ervoor dat gegevens alleen worden gedeeld met geautoriseerde organisaties.

Wat moet je doen?
Om gegevens te blijven uitwisselen, moet jouw organisatie in bezit zijn van een PKIo-certificaat. Jouw technische aansluitpartij of de verantwoordelijke afdeling binnen jouw organisatie, zoals informatiebeveiliging of ICT, is op de hoogte van wat er moet gebeuren en kan hierbij helpen. In de bijlage vind je een technische toelichting en praktische stappen om een PKIo-certificaat aan te vragen.

Datum
27 maart 2026

Onze referentie
2026-0000145787

Vragen?
Heb je vragen of loop je ergens tegenaan? Bekijk dan rvig.nl/veelgestelde-vragen-pkio-certificaat of neem contact op met de afdeling informatiebeveiliging van RvIG via info@rvig.nl.

Hoogachtend,

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
namens deze,

Bijlage: technische toelichting

Beveiligde verbinding (mTLS)

In dit document gaat het over de versleuteling *tussen* computers (servers) waarbij integriteit en vertrouwelijkheid onlosmakelijk met elkaar verbonden zijn. Binnen RvIG spreken we dan over versleuteling op basis van mTLS (mutual TLS), waarbij de vertrouwensrelatie voor de beveiligde verbinding tussen servers wederzijds is ingeregeld. Hiermee voldoen we ook aan het Zero Trust principe.

Partijen waar RvIG BRP-gegevens aan levert kunnen gebruikmaken van een technische aansluitpartij. Dit is een partij die gegevens namens haar klant (de geautoriseerde afnemer, bijvoorbeeld een gemeente) opvraagt. De technische aansluitpartij handelt in opdracht van de afnemer, die de eindklant is. In de context van PKIo wordt de technische aansluitpartij daarom behandeld als de 'afnemer'. Dit houdt in dat de technische aansluitpartij voor de afnemer(s) waarvoor zij gegevens opvraagt beschikt over een PKIo-certificaat of certificaten van de afnemer(s) om een mTLS-verbinding met de systemen van RvIG op te zetten. Deze verbinding wordt gebruikt voor het opvragen van gegevens of voor het ontvangen van spontane verstrekkingen wanneer een afnemerindicatie is ingesteld.

Ter verduidelijking: een technische aansluitpartij treedt op namens de afnemer en gebruikt daarvoor een PKIo-certificaat dat door de betreffende afnemer is verstrekt.

API en OAuth

Voor het gebruik van API's voor het uitwisselen van gegevens hanteren we de volgende werkwijze;

- Aan klantzijde is een API Gateway ingericht voor het afhandelen van API verkeer.
    - Een API Gateway mag meerdere afnemerID's afhandelen, dit in combinatie met een uniek PKIo-certificaat per afnemer.
- De API Gateway gebruikt een PKIo-certificaat met OIN.
    - Dit certificaat is uniek per afnemer/gemeente.
- RvIG controleert op geldigheid, hostname, OIN en status certificaat (of deze is ingetrokken bijvoorbeeld)
- Bij (cyber)incidenten kan toegang worden afgesloten door het blokkeren van AfnemerID/OIN

Voor het gebruik van de API gebruiken we de volgende informatie;

- De Scope - Deze bestaat uit:
    - AfnemerID (autorisatiebesluitnummer) en;
    - OIN van de afnemer/gemeente
- De Claims
    - Gemeentecode (voor alle gemeente accounts)
    - Endpoint= brp;brp-berichten (voor LAP met de toevoeging – lap)(uitbreidbaar met nieuwe API endpoints)
    - Berichtenboxnummer
    - Mogelijke extra informatie

Voorbeeld:

Client credentials
Client Name: 510189-00000001001808035000
Client ID: 64b3f293-ab8a-434c-83cf-37f8d34bacf0
Client Secret: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Grants Required: Client Credentials
OIN=00000001001808035000
afnemerID=510189
gemeenteCode=0441
endpoints=brp;brp-berichten;any-rvig-api

Twee-factor-authenticatie/Multi-factor authenticatie
Bovenstaande implementatie van het gebruik van een uniek PKIo-certificaat per afnemer/gemeente en het vanuit RvIG verstrekken van unieke client credentials zorgt ervoor dat we ook voldoen aan de informatiebeveiliging-eisen ten aanzien van twee-factor-authenticatie (2-FA)/ multi-factor authenticatie (MFA). Hierdoor weten we zeker dat we de gegevens leveren aan de juiste, daarvoor geautoriseerde, partij.

Meer informatie
Voor meer informatie over PKIo bekijk: logius.nl/onze-dienstverlening/toegang/pkioverheid/wat-pkioverheid

Voor het aanvragen van een PKIo-certificaat bekijk: logius.nl/onze-dienstverlening/toegang/pkioverheid/pkioverheidcertificaat-aanvragen

Voor meer informatie over BIO2 bekijk: bio-overheid.nl

Voor meer informatie over OIN bekijk: logius.nl/onze-dienstverlening/toegang/organisatie-identificatienummer

Voor het aanvragen van een OIN bekijk: logius.nl/domeinen/toegang/organisatie-identificatienummer/aanvraagformulier-oin