Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Wijziging LO BRP 2025.Q1: W186 LO Beveiligingseisen conform IB-richtlijnen

Versie	0.3
Datum	30-08-2024
Status	Concept

Wijziging LO BRP 2025.Q1:
W186 LO Beveiligingseisen conform IB-richtlijnen

De volgende wijzigingen worden doorgevoerd in het Logisch Ontwerp BRP (LO BRP). Voor niet genoemde paragrafen en hoofdstukken uit het LO BRP geldt dat daarin geen wijzigingen optreden.

6.4.4.1 PKI

BRP-V bevat een kopie van de BRP-gegevens in de onderscheiden gemeentelijke basisregistraties en de RNI. De inhoud en toegang tot BRP-V dienen derhalve adequaat beveiligd te zijn.

Voor de beveiliging van het gegevensverkeer van afnemers met BRP-V wordt versleuteling toegepast. Sleutelmateriaal wordt ook gebruikt voor de authenticatie van afnemers. Gebruikers van de Ad hoc webservice en API's moeten beschikken over een gekwalificeerd PKI-overheid certificaat (zie www.pkioverheid.nl).

Met betrekking tot de beveiliging van BRP-V gelden de volgende eisen.

- BRP-V is alleen benaderbaar voor systemen van gemeenten, RNI en afnemers van BRP-V.
- Uitgangspunt is dat een afnemer alleen een koppeling met BRP-V kan realiseren met een eigen server en via een besloten netwerk (Diginetwerk). De koppeling is gebaseerd op HTTP, SOAP dan wel REST/JSON en TLS. De aansluiting van afnemers op BRP-V verloopt via een PKI. Hiervoor wordt dezelfde invulling gebruikt als bij het datatransport voor het ‘reguliere’ BRP-berichtenverkeer: TCP/IP met TLS. BRP-V fungeert in het PKI-stelsel als een server.
- Een geautoriseerde afnemer kan met behulp van een geldig certificaat vanuit zijn systemen een beveiligde verbinding met BRP-V opzetten. Een afnemer kan de berichtafhandeling met BRP-V laten uitvoeren door een derde partij, een bewerker. Een bewerker die voor een of meerdere afnemers de berichtafhandeling uitvoert, kan voor de communicatie met BRP-V zijn eigen certificaat of dat van een van de betreffende afnemers gebruiken. Als de beveiligde verbinding tot stand is gekomen, dient een autorisatie plaats te vinden van de afnemer waarvoor de verbinding wordt opgezet. Dat gebeurt middels een afnemernaam/wachtwoord combinatie.
- In een PKI worden certificaten alleen voor een bepaalde duur uitgegeven. Een afnemer of bewerker kan derhalve beschikken over nul, een of meerdere geldige certificaten. BRP-V accepteert alleen geldige certificaten. De certificatiedienstverlener (CSP) kan de geldigheid van een certificaat door middel van een Certificate Revocation List (CRL) intrekken.
- ~~Het certificaat geldt zowel voor de testomgeving als voor de productieomgeving.~~

[…]

A.6.2.2 Wachtwoordbeheer

De afnemer, gemeente en RNI krijgen toegang tot BRP-V met een naam/wachtwoord-combinatie. Dit wachtwoord moet eenmaal per drie maanden worden gewijzigd. Bij het verkrijgen van toegang mag het wachtwoord niet verlopen zijn. Is het wachtwoord wel verlopen, dan wordt een foutbericht met reden “X” verstuurd.

De afnemer, gemeenten en RNI kunnen het wachtwoord wijzigen met de service changePassword. Daartoe worden het nieuwe wachtwoord als parameter meegestuurd.

In het wachtwoord van de ~~LO3 Ad hoc~~ webservices van BRP-V zijn de volgende tekens toegestaan:

- 'Letters': de tekens A-Z (decimaal 065 t/m 090) en de tekens a..z (decimaal 097 t/m 122).
- 'Cijfers': de tekens 0-9 (decimaal 048 t/m 057).
- ~~'Spatie': het teken met decimale waarde 32.~~
- 'Overige tekens': alle overige tekens met een decimale waarde groter ~~of gelijk a~~dan 32 en kleiner dan 127.

Er wordt gecontroleerd of elk gebruikt teken ~~in~~ ligt in de (ASCII/UTF-8) reeks: 32 <= x < 127 (hexadecimaal: 20 <= x ~~>~~< 7f). De complete reeks is dan:

a-z, A-Z, 0-9~~, <spatie>~~, !@#$%^&*()_-+={}[]"'|/\?.,:><,~`

A.6.2.3 Regels voor de samenstelling van het wachtwoord:

- Het wachtwoord bestaat uit minimaal 10~~8~~ tekens en maximaal ~~12~~ 64 tekens.
- ~~Een teken mag maximaal 2 keer in het wachtwoord voorkomen.~~
- ~~De decimale waarden van e~~Een opeenvolgende reeks van ~~3~~4 tekens ~~mogen~~ mag niet met 1 oplopen (bijvoorbeeld "ABCD") of aflopen (bijvoorbeeld "8765").
- ~~Spaties mogen alleen voorkomen vanaf de 7e positie: de eerste 6 posities bevatten geen spatie.~~
- ~~Als in het wachtwoord letters worden gebruikt, geldt dat deze of losstaand (dus in de vorm van 1 enkele letter) of in een reeks van 3 letters mogen voorkomen. Reeksen van 2, 4 of meer letters mogen dus niet worden gebruikt.~~
- ~~Als in het wachtwoord cijfers worden gebruikt, geldt dat deze of losstaand (dus in de vorm van 1 enkel cijfer) of in een reeks van 3 cijfers mogen voorkomen. Reeksen van 2, 4 of meer cijfers mogen dus niet worden gebruikt.~~
- ~~Als in het wachtwoord 3 of meer tekens anders dan letters, cijfers of spaties voorkomen, komen de regels onder punt 4, 5 en 6 te vervallen.~~
- Het wachtwoord bevat altijd minstens 3 van de 4 van de volgende eigenschappen:
  - Minimaal 1 hoofdletter;
  - Minimaal 1 kleine letter;
  - Minimaal 1 cijfer;
  - Minimaal 1 'speciaal teken'. ~~Een speciaal teken is in dit geval elk teken dat geen spatie, hoofd- of kleine letter, cijfer of underscore is.~~
- Het wachtwoord mag niet gelijk zijn aan 1 van de 10 voorafgaande wachtwoorden.