



Wijziging LO BES 2025.Q1: W186 LO beveiligingseisen conform IB-richtlijnen

Versie 0.3

Datum 26-08-2024
Status Concept

Wijziging LO BES 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.

B.5.1 PKI

PIVA-V bevat een kopie van de PIVA-gegevens in de onderscheiden eilandelijke basisadministraties. De inhoud en toegang tot PIVA-V dienen derhalve adequaat beveiligd te zijn.

Voor de beveiliging van het gegevensverkeer van afnemers met PIVA-V wordt versleuteling toegepast. Sleutelmetaal wordt ook gebruikt voor de authenticatie van afnemers. Gebruikers van de PIVA-V online service moeten beschikken over een gekwalificeerd PKI-overheid certificaat (zie www.pkioverheid.nl).

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

- PIVA-V is alleen benaderbaar voor systemen van afnemers van PIVA-V.
- Uitgangspunt is dat een afnemer alleen een koppeling met PIVA-V kan realiseren met een eigen server en via een besloten netwerk (huurlijn). De koppeling is gebaseerd op HTTP, SOAP en SSL. De aansluiting van afnemers op PIVA-V verloopt via een PKI. Hiervoor wordt dezelfde invulling gebruikt als bij het datatransport voor het 'reguliere' BRP-berichtenverkeer: TCP/IP met SSL. PIVA-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 PIVA-V opzetten. Een afnemer kan de berichtafhandeling met PIVA-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 PIVA-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. PIVA-V accepteert alleen geldige certificaten. De certificatedienstverlener (CSP) kan de geldigheid van een certificaat door middel van een Certificate Revocation List (CRL) intrekken.
- ~~Hot certificaat geldt zowel voor de testomgeving als voor de productieomgeving.~~