Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van BZK
Operatie BRP

Lange Vijverberg 11
2513 AC Den Haag
Postbus 10451
2501 HL Den Haag

www.operatiebrp.nl
support@operatiebrp.nl

Fout! Onbekende naam voor documenteigenschap. **Fout! Onbekende naam voor documenteigenschap.Fout! Onbekende naam voor documenteigenschap. Fout! Onbekende naam voor documenteigenschap.**

Fout! Onbekende naam voor documenteigenschap. Fout! Onbekende naam voor documenteigenschap.

Fout! Onbekende naam voor documenteigenschap.
14 augustus 2014

Fout! Onbekende naam voor documenteigenschap. **Fout! Onbekende naam voor documenteigenschap.**

Fout! Onbekende naam voor documenteigenschap. **Fout! Onbekende naam voor documenteigenschap.**

notitie

Operatie BRP
Authenticatie Partijen **Fout! Onbekende naam voor documenteigenschap.**

Lijnparaaf	Medeparaaf	Afschrift aan
Fout! Onbekende naam voor documenteigenschap.	**Fout! Onbekende naam voor documenteigenschap.**	**Fout! Onbekende naam voor documenteigenschap.**
Fout! Onbekende naam voor documenteigenschap.	**Fout! Onbekende naam voor documenteigenschap.**	**Fout! Onbekende naam voor documenteigenschap.**
Fout! Onbekende naam voor documenteigenschap.	**Fout! Onbekende naam voor documenteigenschap.**	**Fout! Onbekende naam voor documenteigenschap.**

Inleiding

Het programma operatie BRP (hierna oBRP) is belast met de ontwikkeling van de centrale voorziening BRP. In aanvulling op het vastgestelde Informatiebeveiligingsplan voor het ontwerp en de bouw van de centrale voorziening BRP beschrijft deze notitie de oplossingsrichting inzake de authenticatie van Partijen, zoals oBRP deze zal implementeren in de centrale voorziening BRP.

Onder Partijen worden in deze notitie de Afnemers, Bijhouders en de eventueel door hen ingeschakelde Bewerkers bedoeld.

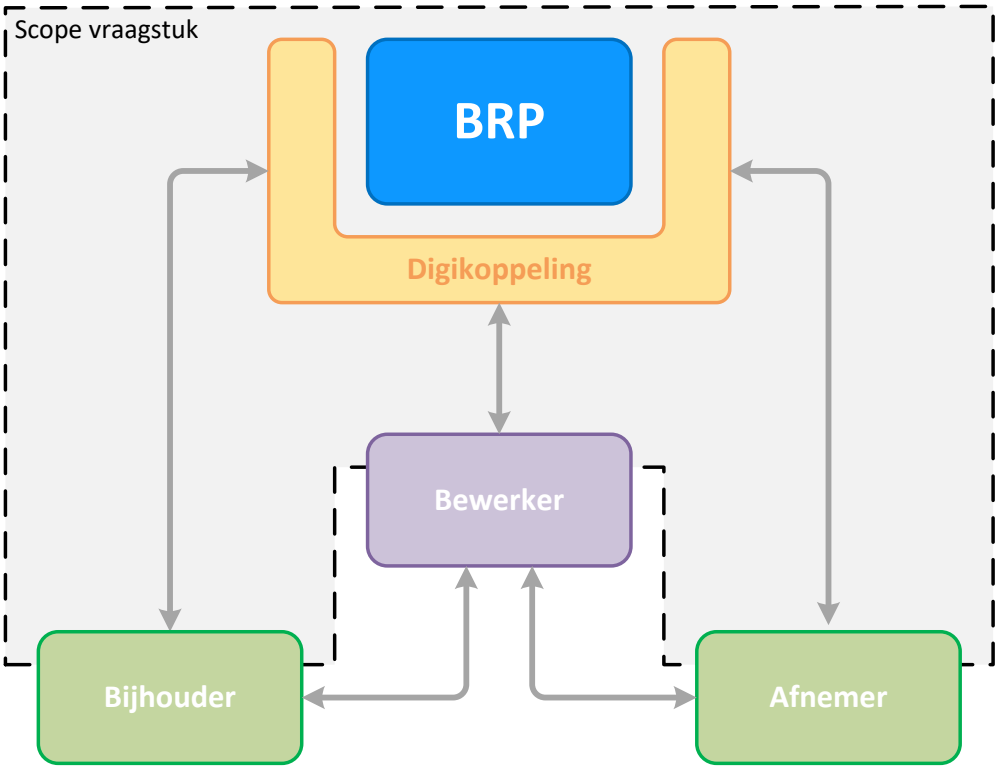
Voor authenticatie is voor de BRP in het ontwerp één methodiek voorzien die aansluit op het gebruik van de overheidsstandaard Digikoppeling versie 3.0. Binnen deze standaard is gedefinieerd dat partijen zich identificeren met PKIO-certificaten.

Voor gebruik binnen de centrale voorzieningen BRP betreft het de volgende Digikoppeling-profielen:

a. "2W-be-s": WUS met 2 zijdige TLS met signing voor synchrone berichten (Digikoppeling 3.0)
b. "2W-R-S": Ws-rm reliable messaging met signing voor asynchrone berichten (Digikoppeling 3.0)
c. "osb-rm-s": Ebms reliable messaging met signing voor asynchrone berichten (Digikoppeling 3.0)[1];

[1] Momenteel vinden op basis van ervaringen bij andere basisregistraties (NHR) gesprekken plaats over het al dan niet opnemen van eBMS in de scope van oBRP. De uitkomst hiervan is nog niet bekend.

Onderstaande figuur schetst het BRP-communicatielandschap in globale zin en geeft via de stippellijn het bereik van het 'Authenticatie'-vraagstuk aan.



Nadere toelichting vraagstuk

De BRP ontvangt en levert uitsluitend berichten van en aan juridisch geautoriseerde overheidsorganen en derden; dit betreft Afnemers en Bijhouders. De aldus met de BRP communicerende bevoegden worden in de centrale voorziening BRP als een zogenaamde 'Partij' geregistreerd.

Afnemers en Bijhouders kunnen rechtstreeks met de BRP communiceren of zij kunnen hiervoor een Bewerker inschakelen. Ook Bewerkers worden in de centrale voorzieningen BRP als 'Partij' geregistreerd. De communicatie tussen de centrale voorziening BRP en de Partijen volgt de Digikoppeling 3.0-standaard en geschiedt op basis van PKIO-certificaten.

Hierbij wordt onderscheid gemaakt in certificaten voor de versleuteling (encryptie) van de communicatie en ondertekening (signing) van het bericht.

Een Bewerker kan voor een Afnemer of Bijhouder verschillende rollen vervullen;
- alleen die van Transporteur (versleuteling)
- alleen die van Ondertekenaar (signing)
- of die van Transporteur en Ondertekenaar.

Voor wat betreft de berichtuitwisseling zelf wordt in de uitwerking van de oplossingsrichting onderscheid gemaakt tussen de volgende vormen van communicatie:

1. Synchrone communicatie; de Afnemer/Bijhouder/Bewerker doet een verzoek aan de centrale voorziening BRP ('request-response'-berichten; bv. bevraging, bijhouding)
2. Asynchrone communicatie; de centrale voorziening BRP informeert de Afnemer/Bijhouder/Bewerker ('push'-berichten; bv. mutatie- en vulberichten, notificaties)

NB. De vorm 'Asynchrone communicatie' waarbij het initiatief niet bij de centrale voorzieningen BRP ligt maar bij de Afnemer cq. Bijhouder is tot op heden nog niet onderkend en valt buiten de scope van deze notitie.

Voorgestelde oplossingsrichting oBRP …

De door oBRP voorgestelde oplossingsrichting is gebaseerd op de volgende uitgangspunten en regels:

1. Er geldt een hoog beveiligingsniveau voor toegang tot en gebruik van de centrale voorziening BRP;

2. Vanuit oBRP wordt hiervoor één methodiek gehanteerd; hiervoor wordt aangesloten op de overheidsstandaard Digikoppeling versie 3.0 met de eerder genoemde profielen.

3. Een Afnemer of Bijhouder kan zelfstandig aansluiten op de centrale voorziening van de BRP door zelf een versleutelde verbinding met de centrale voorzieningen BRP op te zetten en de berichten zelf te ondertekenen. Hiermee vult de Afnemer cq. Bijhouder de rollen Transporteur en Ondertekenaar zelf in;

4. Een Afnemer of Bijhouder kan één of meer Bewerkers machtigen om namens hem op te treden als Transporteur en te communiceren met de centrale BRP voorziening voor het opzetten van een versleutelde verbinding;

5. Een Afnemer of Bijhouder kan één of meer Bewerkers machtigen om namens hem op te treden als Ondertekenaar en de berichten digitaal te ondertekenen;

6. Een Afnemer, Bijhouder of Bewerker dient aan te geven met welke IP-adressen gecommuniceerd wordt, zodat deze in de whitelist van de centrale voorzieningen BRP kunnen worden opgenomen. Voor de asycnhrone communicatie zal tevens het zogenaamde adres van de ontvangstservice (het zogenaamde endpoint) moeten worden opgegeven;

7. Andersom geldt dat de Beheerder van de centrale voorziening BRP de IP-adressen door geeft, waarvandaan de berichten vanuit de centrale voorziening worden gecommuniceerd.

Zo kan een Afnemer, Bijhouder of Bewerker deze ook in de eigen whitelist opnemen;

8. Een Afnemer of Bijhouder moet bij machtigingen van Bewerkers bij de Beheerder van de centrale voorziening BRP aangeven welke combinaties van Transport- en Ondertekeningmachtigingen bij een Bewerker zijn toegestaan;

9. Indien door een Afnemer of Bijhouder een Bewerker als Ondertekenaar wordt gemachtigd, dient ten behoeve van de Diensten binnen het koppelvlak Levering en de Administratieve handelingen binnen het koppelvlak Bijhouding een Bewerker apart te worden gemachtigd[2];

10. Machtigingen en de gemachtigde partijen (Bewerkers) worden binnen de centrale voorzieningen BRP geregistreerd. Bij het opzetten van de communicatie en de verwerking van binnenkomende berichten valideert de centrale BRP voorziening of sprake is van een geldige machtiging;

11. Conform Digikoppeling 3.0 identificeren Afnemers, Bijhouders en Bewerkers zich bij de communicatie (Transporteur) met de centrale voorzieningen BRP met hun ***eigen*** PKIOverheid-certificaat inclusief het unieke OverheidsIdentificatieNummer (OIN)[3];

12. Conform Digikoppeling 3.0 ondertekenen Afnemers, Bijhouders en Bewerkers (Ondertekenaar) berichten met de centrale voorzieningen met hun ***eigen*** PKIOverheid-certificaat (PKIO-certificaat) inclusief het unieke OverheidsIdentificatieNummer (OIN);

13. Het in het PKIO-certificaat opgenomen OverheidsIdentificatieNummer (OIN) wordt door de centrale BRP voorziening gebruikt om te identificeren met welke Afnemer, Bijhouder of Bewerker wordt gecommuniceerd en welke Afnemer, Bijhouder of Bewerker berichten heeft ondertekend;

14. In de centrale voorziening BRP worden geen afzonderlijke certificaat-gegevens opgenomen. Nadat is vastgesteld dat het certificaat een PKIO-certificaat is, gaat de voorgestelde oplossingsrichting er namelijk vanuit dat het in het certificaat opgenomen OIN vertrouwd kan worden en vanaf dat moment in het proces gebruikt kan worden voor de identificatie van de betreffende Partij in de verdere BRP-verwerking.

15. In alle gevallen geldt dat de Partijcode van de juridisch geautoriseerde overheidsorganen en derden (Afnemers en Bijhouders) in de stuurgegevens van het bericht (berichtinhoud) als formele zender en ontvanger zijn opgenomen;

16. Voor de verdere autorisatie binnen de BRP spelen de volgende gegevens een rol:
    a. Overheidsidentificatienummer (OIN); via PKIO-certificaat Ondertekenaar
    b. Partijcode; via binnenkomende bericht
    c. Abonnementnaam (koppelvlak Levering); via binnenkomende bericht
    d. Administratieve handeling (koppelvlak Bijhouding); via binnenkomende bericht

[2] Machtigingen op bijhoudingen nader uit te werken in BOP-stap 4.3

[3] Afnemers of Bijhouders stellen dus niet hun eigen PKIO-certificaat ter beschikking aan een Bewerker. De Bewerker gebruikt zijn eigen PKIO-certificaat met het eigen 20-cijferige OIN. Ook private partijen kunnen een op het KvK nummer gebaseerd OIN toegewezen krijgen.

17. Er wordt gestreefd naar een zo laag mogelijke beheer- en kostenlast aan zowel BRP-, Afnemer-, Bijhouder- als Bewerkerzijde.

Het voordeel van hierboven geschetste oplossingsrichting is dat (naast de besloten verbinding en versleutelde berichten) we met zekerheid kunnen vaststellen dat het berichtenverkeer naar of van de afnemer/bijhouder/bewerker, daadwerkelijk naar de bewerker/bijhouder/afnemer gaat.

Dit enerzijds gebaseerd op de PKIO-certificaten en deels op de door de Beheerder van de BRP vastgelegde configuraties per Partij, waarbij het via het PKIO-certificaat verkregen OIN de verbindende schakel vormt tussen enerzijds de Digikoppeling v3.0-voorschriften en anderzijds de door de Beheerder ingevoerde BRP-configuraties.

Voor een schematische weergave van het gebruik van certificaten door Afnemers, Bijhouders en/of Bewerkers wordt verwezen naar bijlage A.

Voor een eerste uitwerking van de controles zoals deze door de centrale voorozieningen van de BRP worden uitgevoerd wordt verwezen naar bijlage B.

Gevraagd besluit …

Van de gedelegeerd opdrachtgever cq. de stuurgroep oBRP wordt het volgende besluit gevraagd:

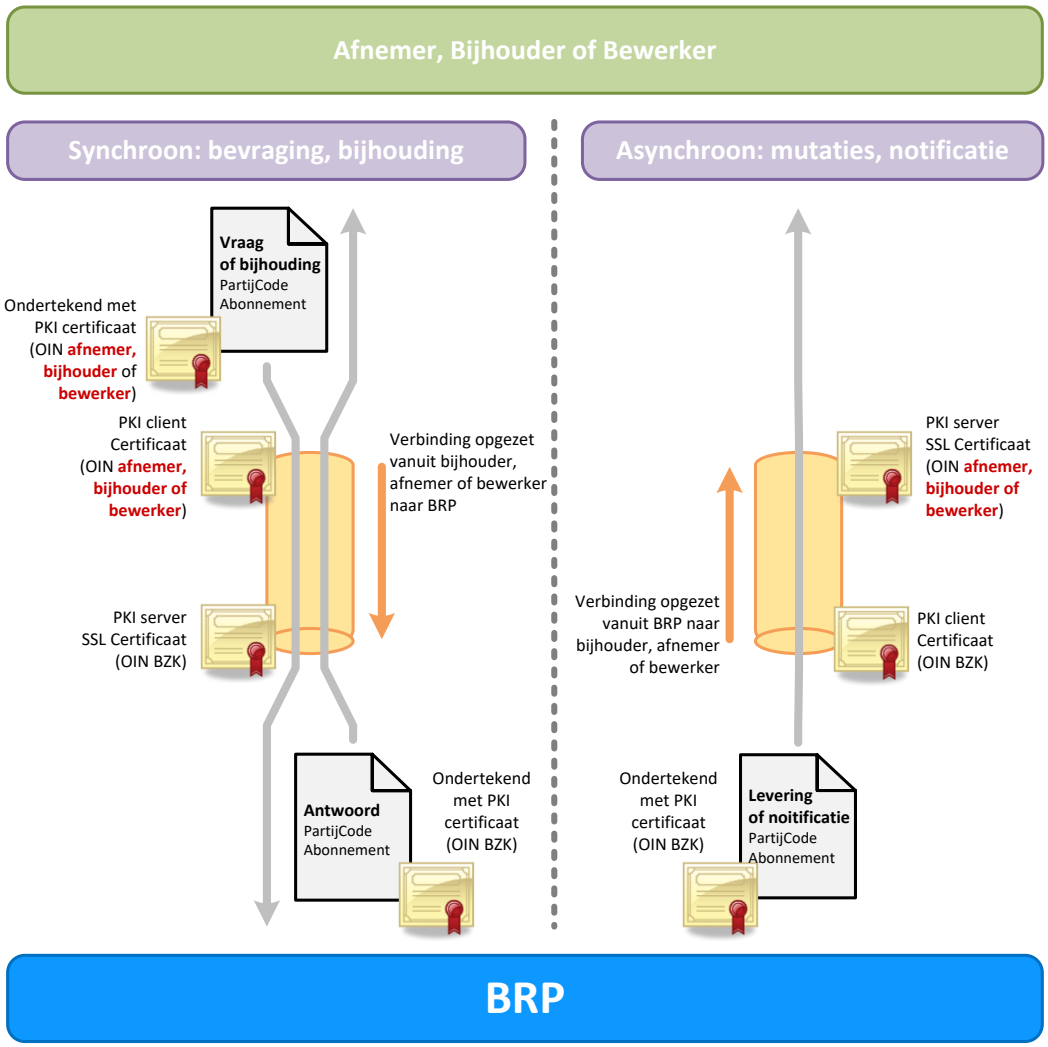
1. Akkoord te gaan met de beschreven oplossingsrichting van oBRP voor Authenticatie van Partijen, zoals deze is gebaseerd op het gebruik van de overheidsstandaard Digikoppeling 3.0

2. oBRP opdracht te geven voor de nadere uitwerking van deze oplossingsrichting in termen van een ontwerp.

3. oBRP opdracht te geven voor het op basis van dit ontwerp uit te voeren impactanalyse; deze analyse samen met het ontwerp in de vorm van een wijzigingsvoorstel ter goedkeuring voor te leggen aan de Stuurgroep oBRP.

Bijlage A Weergave communicatie met BRP

Onderstaand schema laat het gebruik van certificaten zien bij het opzetten van een verbinding tussen Afnemers, Bijhouders en/of Bewerkers en de centrale voorzieningen BRP.



Bijlage B Eerste uitwerking controleregels BRP …

Onderstaand volgt een eerste uitwerking van controleregels zoals deze door de centrale voorziening BRP voor de afhandeling van Authenticatie worden uitgevoerd. Nadat een Partij is geauthenticeerd (en geïdentificeerd) volgen de autorisatiecontroles, waarna een bericht vervolgens door de centrale voorziening kan worden verwerkt. Deze controleregels worden bij nadere uitwerking verder aangevuld en aangescherpt.

Synchrone communicatie (WUS)

Nr	Controle	Waar
1	Check of IP-adres is opgenomen in de whitelist	BPR (BigIP F5)
2	Valideer transport PKIO certificaat (Transporteur): * check de certificate chain (is het een PKI-O certificaat) * check vervaldatum * check CRL van de certificate chain online * check of certificaat OIN bevat	BPR (BigIP F5)
3	Check of 'Transporteur'- OIN als partij bekend en geldig is	BRP stack
4	Check of combinatie 'Transporteur'-OIN en IP-adres geldig is	BRP stack
5	Check of bericht signature overeenkomt met bericht	BRP stack
6	Valideer signing PKIO certificaat (Ondertekenaar): * check de certificate chain (is het een PKI-O certificaat) * check vervaldatum * check CRL van de certificate chain online * check of certificaat OIN bevat	BRP stack
7	Check of 'Ondertekenaar'-OIN als partij bekend en geldig is	BRP stack
8	Check of combinatie 'Ondertekenaar'-OIN en 'Transporteur'-OIN valide is	BRP stack
9	Check of PartijCode uit bericht als Afnemer of Bijhouder bekend is	BRP stack
10	Check of Abonnementnaam/Administratieve handeling uit bericht bekend en geldig is	BRP stack
11	Check of er een Toegang is gedefinieerd met PartijCode, 'Ondertekenaar'-OIN en Abonnementnaam/Administratieve handeling	BRP stack
12	Autorisatie, zoals validatie op abonnement	BRP stack

Asynchrone communicatie (WSRM)

Nr	Controle	Waar
1	Autorisatie, zoals filtering op abonnement	BRP stack
2	Check of IP-nummer is opgenomen in whitelist	BPR (BigIP F5)
3	Valideer transport (server) certificaat van ontvangende partij: * check de certificate chain (is het een PKI-O certificaat) * check vervaldatum * check CRL van de certificate chain online * check of certificaat OIN bevat	BPR (BigIP F5)
4	Check of transport (server) OIN overeenkomt met de verwachte OIN bij de Afleverwijze, zoals in de BRP is geregistreerd (nog afstemmen hoe)	BPR (BigIP F5)