



**Rechtszekerheid**

## **Stappenplan aansluiting LV-WKPB**

Versie

3.1

Auteur(s)

Projectteam WKPB VROM



## Rechtszekerheid

Datum  
25 febr 2009

Titel  
Stappenplan aansluiting LV-WKPB

Versie  
3.1

Blad  
1 van 28

## Stappenplan aansluiting LV-WKPB

### Opdrachtgever

RZ/MB/PPB

### Status

Definitief

### Verspreiding

o.a. WKPB-Site

### Versiehistorie

Versie	Datum	Auteur	Opmerking
1.0	01-09-2006	Projectteam WKPB, VROM	Initiële versie
2.0	07-02-2007	Projectteam WKPB, VROM	Actualisering en aanscherping. Opname bijlage 1 t/m 4
2.1	20-02-2007	Projectteam WKPB, VROM	Bijlage 2 bijgewerkt met extra technische toegangstest
3.0	2 mei 2008	RZ/PPB	Huisstijl, actualisatie na overdracht beheer (zie inleiding), verwerken interne review, opnemen aantal veel voorkomende problemen
3.1	25 febr 2009	RZ/PPB	In URL waren ten onrechte hoofdletters opgenomen. Is hersteld.

### Recensiehistorie

Versie	Datum	Recensent	Opmerking
--------	-------	-----------	-----------

kadaster



Datum  
25 febr 2009

Titel  
Stappenplan aansluiting LV-WKPB

Versie  
3.1

Blad  
2 van 28

Versie

Datum

Recensent

Opmerking

## Inhoudsopgave

<b>1</b>	<b>Inleiding</b> .....	<b>4</b>
<b>2</b>	<b>Doorlooptijd voor aansluiting op de Landelijke Voorziening WKPB</b> .....	<b>5</b>
<b>3</b>	<b>Vorbereiden</b> .....	<b>6</b>
3.1	Vaststellen programma van eisen gemeentelijke WKPB-registratie (stap 1) .....	6
3.2	Software aanschaffen (stap 2) .....	7
3.3	Vorbereiden van de aansluiting op de LV via Gemnet (stap 3) .....	8
3.4	PKI-Overheid certificaat aanvragen (stap 4) .....	9
3.5	WKPB software installeren (stap 5) .....	10
3.6	PKI-Overheid certificaat installeren (stap 6) .....	10
<b>4</b>	<b>Beoordelen</b> .....	<b>11</b>
4.1	Interne test uitvoeren (stap 7) .....	11
4.2	Technische toegangstest LV uitvoeren (stap 8) .....	12
4.3	Autorisatieverzoek doen (stap 9) .....	13
<b>5</b>	<b>Productie</b> .....	<b>14</b>
5.1	Totaalstand percelen en beperkingen aanleveren ("initial load") (stap 10) .....	14
5.2	Controle correcte werking (stap 11) .....	15
<b>6</b>	<b>En dan echt aan de slag</b> .....	<b>16</b>
	<b>Bijlage 1: Instructie aanvraag certificaten t.b.v. WKPB</b> .....	<b>17</b>
	<b>Bijlage 2: Checklist I&amp;A</b> .....	<b>21</b>
	<b>Bijlage 3: Geconstateerde problemen met betrekking tot netwerk en certificaten</b> .....	<b>24</b>
	<b>Bijlage 4: Contactgegevens</b> .....	<b>28</b>

## 1 Inleiding

Dit stappenplan voor de aansluiting van gemeenten op de Landelijke Voorziening WKPB (LV WKPB), voorziet in een handreiking voor het juist en tijdig aansluiten op de LV WKPB. Doelgroep van het document is de beoogd WKPB gemeentelijk beheerder, de verantwoordelijke voor de implementatie van de WKPB in de gemeente en/of de ICT afdeling.

Het document heeft een focus op de technische aansluiting op de Landelijke Voorziening, de koppeling tussen de gemeentelijke WKPB registratie en de centrale Landelijk Voorziening. Het document beschrijft binnen drie onderdelen: Voorbereiden, Beoordelen en Productie, de activiteiten die uitgevoerd moeten worden. Enkele activiteiten zijn niet strikt noodzakelijk maar geadviseerd wordt een weloverwogen keuze te maken om deze wel of juist niet uit te voeren.

Het onderhanden document is een actualisatie van de versie van het document "Stappenplan aansluiting gemeenten op de landelijke voorziening" zoals het van VROM is overgenomen bij de overdracht van het beheer aan het Kadaster.

De actualisatie houdt in, naast omzetten van huisstijl, dat geschreven is vanuit de situatie dat de Wet al van kracht is (i.p.v. toekomstig), de frontoffice door het Kadaster wordt georganiseerd en de applicatie daadwerkelijk bij het Kadaster in beheer is. Met name dit laatste punt heeft technische consequenties. Zo kan de toegangstest op netwerk-niveau vanwege de beveiligingseisen niet meer worden uitgevoerd zoals in oudere versies beschreven (dus geen "ping" naar IP-adres meer); en zijn VROM-/ATOS-certificaten niet toegestaan, ook niet op de testomgevingen.

Verder:

Er is een hoofdstuk toegevoegd om partijen heel kort voor te bereiden op de nu aangebroken fase van daadwerkelijk werken conform de wet met daarbij opgave van een paar mogelijk nuttige documenten.

Het Autorisatieverzoek is niet meer als bijlage (nr 3) opgenomen omdat dit via de site beschikbaar is (zowel .PDF als .DOC) en, natuurlijk, zijn de contactgegevens aangepast.

Toegevoegd is een nieuwe bijlage 3 waarin een aantal praktijkproblemen opgesomd zijn met betrekking tot netwerken, netwerkverbindingen en certificaten. Voorzover mogelijk is daarbij aangegeven wat de oplossing is of minimaal in welke richting een oplossing gezocht zou moeten worden.

Vanuit de beheerorganisatie, het Kadaster, is geprobeerd het upgraden van dit document met eenzelfde zorg te omkleden als waarmee het oorspronkelijk door VROM is opgezet en gepubliceerd. Mocht het op enigerwijze naar uw idee tekort schieten in duidelijkheid, consistentie of anderszins, nodigen wij u graag uit dit aan ons kenbaar te maken zodat wij hier in een volgende versie rekening mee kunnen houden.

Uw reactie(s) kunt u mailen aan [kadasterwkpb@kadaster.nl](mailto:kadasterwkpb@kadaster.nl)

## 2 Doorlooptijd voor aansluiting op de Landelijke Voorziening WKPB

Onderstaand overzicht geeft een beeld van de stappen die worden verwacht voor het aansluiten van een gemeentelijk WKPB-systeem op de Landelijke Voorziening (LV) WKPB met daarvoor te plannen doorlooptijden. Voor de doorlooptijden is uitgegaan van een “gemiddelde” gemeente en er zijn geen vertragingen door onvoorziene omstandigheden ingebouwd.

Een aantal van de stappen kunnen parallel uitgevoerd worden, sommige activiteiten zijn een logische aaneenschakeling. Bij elkaar ontstaat er een kritiekpad van circa 10 weken doorlooptijd. De activiteiten zijn beschreven vanuit het theoretische oogpunt dat een gemeente nog helemaal geen activiteiten ondernomen heeft. In de praktijk zijn de meeste gemeenten al een eind op weg met verschillende activiteiten.

Id	Taaknaam	Doorlooptijd (in werkdagen)
	<b>Vorbereiding</b>	
1	Vaststellen progr. van eisen gemeentelijke WKPB registratie	10
2	Software aanschaffen	20
3	Voorbereiden van de aansluiting op de LV via Gemnet	10
4	PKI certificaat aanvragen	30
5	WKPB software installeren	5
6	PKI certificaat installeren	5
	<b>Beoordelen</b>	
7	Interne test uitvoeren	10
8	LV-toegangstest uitvoeren	3
9	Autorisatieverzoek doen	2
	<b>Productie</b>	
10	Totaalstand percelen aanleveren aan LV	5
11	Controle correcte verwerking	1

Figuur 1: Doorlooptijd voor aansluiting op de LV WKPB

Alle stappen worden in de navolgende hoofdstukken verder uitgewerkt.

Gemeenten die mogelijk nog géén applicatie hebben geselecteerd (of alsnog willen overstappen naar andere), kunnen op [www.kadaster.nl/wkpb/](http://www.kadaster.nl/wkpb/) informatie vinden over leveranciers en applicaties die de conformiteitstoets reeds met goed gevolg hebben afgelegd.

### 3 Voorbereiden

#### 3.1 Vaststellen programma van eisen gemeentelijke WKPB-registratie (stap 1)

Beschrijving van de activiteiten	<p>Stel de eisen op voor het registratiesysteem van publiekrechtelijke beperkingen, op basis van de wettelijke vereisten voor het voeren van een WKPB administratie en de eigen gemeentelijke wensen. Het programma van eisen moet in ieder geval aandacht besteden aan zaken als:</p> <ul style="list-style-type: none"> <li>• Hoeveelheid beperkingen en percelen die aanwezig zullen zijn</li> <li>• Hoeveelheid besluiten die per maand worden genomen</li> <li>• (Het kennen van) De benodigde functionaliteit en mogelijkheden van het systeem</li> <li>• Stel vast op welke wijze het PKI-Overheid Services Certificaat moet worden verworven, dit kan via een eigen webserver of via Open SSL. De beide mogelijkheden worden beschreven in het document 'Instructie aanvraag certificaten t.b.v. WKPB' (bijlage 1)</li> </ul>
Verantwoordelijke personen/ rollen	<ul style="list-style-type: none"> <li>• Beleidsmedewerker belast met WKPB,</li> <li>• ICT-afdeling,</li> <li>• Beoogd beheerder van de WKPB,</li> <li>• Vakafdeling.</li> </ul>
Afhankelijkheden	<p>Afhankelijk van:</p> <ul style="list-style-type: none"> <li>• voldoende prioriteit en</li> <li>• kennis binnen de gemeente</li> </ul>
Informatie bronnen	<p>Wetgeving, draaiboek, opleidingsmateriaal, catalogus, berichtenspecificatie, architectuur. Deze documentatie is beschikbaar via <a href="http://www.kadaster.nl/wkpb/">www.kadaster.nl/wkpb/</a> (en <a href="http://www.vrom.nl">www.vrom.nl</a>)</p>
Aandachtspunten / tips & trics	<p>De informatiebronnen beschrijven gedetailleerd de vereisten. Als toevoeging hierop moet de eigen situatie in ogenschouw worden genomen. Hierbij moet nagedacht worden over:</p> <ul style="list-style-type: none"> <li>• De plaats in de organisatie</li> <li>• Wel of geen combinatie met de kadastrale registratie</li> <li>• Combinatie met andere trajecten als BAG en DURP</li> <li>• Combinatie met DIS</li> <li>• Wel of geen GIS</li> </ul>
Tijdsduur (doorlooptijd)	10 werkdagen

### 3.2 Software aanschaffen (stap 2)

Beschrijving van de activiteiten	<p>a. Selecteer voor het voeren van uw WKPB registratie een softwaresysteem uit de markt dat een conformiteitverklaring heeft. Als het systeem nog geen conformiteitstoets doorlopen heeft, ga dan na of en wanneer dit gaat gebeuren.</p> <p>OF</p> <p>b. Ontwikkel zelf een software systeem en doorloop daarmee de conformiteitstoets via de LV beheerorganisatie.</p>
Verantwoordelijke personen / rollen	<ul style="list-style-type: none"> <li>• ICT afdeling</li> <li>• Beoogd WKPB beheerder</li> </ul>
Afhankelijkheden	Informatie en offertes uit de markt, beschikbaar budget
Informatie bronnen	Leverancier
Aandachtspunten / tips & trics	<ul style="list-style-type: none"> <li>• Houdt rekening met mogelijkheden tot ruimtelijke vastlegging i.v.m. ruimtelijke beperkingen (GIS functionaliteit).</li> <li>• Alleen ruimtelijke vastlegging is niet voldoende aangezien er ook appartementen en deelpercelen moeten kunnen worden geregistreerd</li> <li>• Laat verschillende leveranciers de oplossing demonstreren</li> <li>• Zelf ontwikkelen is een niet te onderschatten traject</li> <li>• Maak de aanschaf en implementatie niet afhankelijk van definitieve conformiteit verklaring van het beoogde systeem. Maak hier indien van toepassing duidelijke afspraken over met de beoogde leverancier</li> </ul>
Tijdsduur (doorloop tijd)	20 Werkdagen voor optie a; voor optie b kan geen reële schatting worden afgegeven

### 3.3 Voorbereiden van de aansluiting op de LV via Gemnet (stap 3)

Beschrijving van de activiteiten	Maak afspraken voor een aansluiting van uw WKPB applicatie op Gemnet en zorg ervoor dat deze aansluiting voldoende bandbreedte heeft om het verwachte berichtenverkeer te verwerken
Verantwoordelijke personen / rollen	ICT vertegenwoordiger
Afhankelijkheden	Afhankelijk van: <ul style="list-style-type: none"> <li>• Afhandeling van de aanvraag door Gemnet</li> <li>• Beschikbare bandbreedte van Gemnet</li> </ul>
Informatie bronnen	Gemnet Document 'Checklist I&A' (bijlage 2) Evaluatie aansluittesten proefgemeenten Frontoffice WKPB
Aandachtspunten / tips & trics	<ul style="list-style-type: none"> <li>• Wees tijdig en zorg dat deze stap parallel wordt uitgevoerd</li> <li>• Vraag advies bij Gemnet over de benodigde bandbreedte en technische aansluitvoorwaarden</li> <li>• Let op dat zaken als firewall's, proxy's, DNS, IPranges goed zijn ingesteld. Let ook op dat proxy's en firewall's geschikt zijn voor HTTPS verkeer met tweezijdige SSL-authenticatie (zie ook bijlage 2)</li> </ul>
Tijdsduur (doorloop tijd)	10 werkdagen

### 3.4 PKI-Overheid certificaat aanvragen (stap 4)

Beschrijving van de activiteiten	Vraag een PKI-Overheid Services Certificaat <sup>1</sup> aan bij een certificaat uitgever of controleer of het bestaande PKI-Overheid Services Certificaat hergebruikt kan worden
Verantwoordelijke personen / rollen	ICT vertegenwoordiger
Afhankelijkheden	Afhankelijk van: <ul style="list-style-type: none"> <li>• LV WKPB (voorschrift certificaten)</li> <li>• Certificatenuitgever PKI-overheid (CSP)</li> <li>• Kennis van het werken met PKI certificaten</li> </ul>
Informatie bronnen	<ul style="list-style-type: none"> <li>• Certificaatuitgevers (CSP's)</li> <li>• Leverancier WKPB software</li> <li>• ICT afdeling</li> <li>• Website PKI-overheid (<a href="http://www.pki-overheid.nl">www.pki-overheid.nl</a>)</li> <li>• 'Instructie aanvraag certificaten t.b.v. WKPB' (bijlage 1)</li> </ul>
Aandachtspunten / tips & trics	<ul style="list-style-type: none"> <li>• Deze activiteit kan parallel aan de andere activiteiten gebeuren</li> <li>• De initiële registratie als abonnee kan een aantal weken duren en vereist het op orde hebben van mandatering</li> <li>• Als de gemeente al abonnee is (bv voor BSN, DigiD) zal uitgifte veel sneller verlopen</li> <li>• Certificaatuitgevers zijn o.a.: DigiNotar, GemnetCSP en GetronicsPinkRocade</li> <li>• Een bestaand certificaat (organisatie gebonden PKI-overheid) kan mogelijk voldoende zijn</li> </ul>
Tijdsduur (doorloop tijd)	30 werkdagen

<sup>1</sup> Een PKI SSL certificaat is een softwarematige authenticatie mechanisme (vergelijkbaar met bijvoorbeeld DigiD). Dit is een databestand die versleuteld op een computer staat. Dit bestand beschrijft op een unieke wijze de gemeente waartoe deze computer behoort. Bij communicatie wordt het PKI Overheids Services Certificaat gebruikt om eenduidig vast te stellen dat de verzendende partij ook de partij is die zij zegt dat ze is

### 3.5 WKPB software installeren (stap 5)

Beschrijving van de activiteiten	De programmatuur dient op de juiste wijze technisch te worden geïnstalleerd, daarnaast is het noodzakelijk om ook de “stamgegevens” / referentietabellen voor het systeem goed in te regelen
Verantwoordelijke personen / rollen	<ul style="list-style-type: none"> <li>• ICT afdeling</li> <li>• Leverancier</li> </ul>
Afhankelijkheden	Afhankelijk van: <ul style="list-style-type: none"> <li>• Leverancier voor levering software</li> <li>• Leverancier voor levering hardware</li> <li>• Capaciteit ICT afdeling</li> </ul>
Informatie bronnen	Leverancier
Aandachtspunten / tips & trics	Goed testen is belangrijk
Tijdsduur (doorloop tijd)	5 werkdagen

### 3.6 PKI-Overheid certificaat installeren (stap 6)

Beschrijving van de activiteiten	Het verkregen PKI-Overheid Services Certificaat moet geïnstalleerd worden op de server / werkplek die de communicatie met de LV zal gaan verzorgen. Waar en hoe dat precies is, is sterk afhankelijk van de geselecteerde software.
Verantwoordelijke personen / rollen	<ul style="list-style-type: none"> <li>• ICT afdeling</li> <li>• Certificaat uitgever</li> <li>• Leverancier</li> </ul>
Afhankelijkheden	Afhankelijk van: <ul style="list-style-type: none"> <li>• Levering van certificaat</li> <li>• Kennis hoe te werken met PKI overheid certificaten</li> <li>• Kennis van werking van de WKPB applicatie</li> </ul>
Informatie bronnen	<ul style="list-style-type: none"> <li>• Uitgever PKI-Overheid Services Certificaat (CSP)</li> <li>• Installatie documentatie WKPB applicatie</li> </ul>
Aandachtspunten / tips & trics	<ul style="list-style-type: none"> <li>• Kijk naar het gebruik van PKI overheid certificaten zoals gebruikt wordt voor andere trajecten (DigiD, BSN).</li> <li>• Mogelijk moet het van de CSP ontvangen .PEM bestand nog omgezet worden in een PKCS#12 bestand. Zie hiervoor bijlage 1</li> </ul>
Tijdsduur (doorloop tijd)	5 werkdagen

## 4 Beoordelen

### 4.1 Interne test uitvoeren (stap 7)

Beschrijving van de activiteiten	Maak een testopstelling voor de gemeentelijke WKPB applicatie zodat een implementatietest kan worden gedaan. Verzamel testdata (percelen, beperkingenbesluiten, vervallenverklaringen, rechterlijke uitspraken etc) voor een eigen interne test ten aanzien van het voldoen aan de gestelde eisen. Stel interne testscenario's op. Test de software op gebruiksaspecten in een interne test. Ga vervolgens na of ook alle berichten juist worden verstuurd door de output uit de software te vergelijken met referentie output (hier is wel IT expertise voor nodig)
Verantwoordelijke personen / rollen	<ul style="list-style-type: none"> <li>• ICT afdeling</li> <li>• WKPB beheerder</li> </ul>
Afhankelijkheden	Afhankelijk van: <ul style="list-style-type: none"> <li>• Beschikbaarheid van de software</li> <li>• Beschikbaarheid van de hardware</li> <li>• Voldoende ICT kennis beschikbaar</li> <li>• Voldoende tijd en aandacht van betrokken</li> </ul>
Informatie bronnen	<ul style="list-style-type: none"> <li>• ICT afdeling</li> <li>• Logische testcases (zie <a href="http://www.kadaster.nl/wkpb/">www.kadaster.nl/wkpb/</a>)</li> <li>• Testdata set (zie <a href="http://www.kadaster.nl/wkpb/">www.kadaster.nl/wkpb/</a>)</li> </ul>
Aandachtspunten / tips & trics	<ul style="list-style-type: none"> <li>• Deze stap is niet verplicht in het proces van aansluiten op de LV WKPB, maar wordt wel sterk aanbevolen. Dit is een binnengemeentelijke zaak</li> <li>• Maak een zo "natuurlijk" mogelijke opstelling voor de test</li> <li>• Gebruik waar mogelijk de handreikingen van VROM (logische testcases, testdata set)</li> <li>• Gebruik een weloverwogen methode om de testscenario's te beschrijven. Beschrijf minimaal: <ul style="list-style-type: none"> <li>○ -Doel van de test</li> <li>○ -Invoer data</li> <li>○ -Uitvoer voorspelling</li> </ul> </li> <li>• Maak een basis testdata set die na iedere keer als start situatie kan worden hergebruikt</li> <li>• Voor het juist kunnen interpreteren en beoordelen van de StUF berichten is behoorlijke ICT- en materiekennis nodig</li> </ul>
Tijdsduur (doorloop tijd)	10 werkdagen

#### 4.2 Technische toegangstest LV uitvoeren (stap 8)

Beschrijving van de activiteiten	<p>Een gemeente moet zich ervan vergewissen of er verbinding gemaakt kan worden met de LV. Dit kan een gemeente in principe zelfstandig doen. De test heeft niet als doel vast te stellen of er daadwerkelijk mutaties kunnen worden uitgevoerd. Het is dus een technische en geen functionele toegangstest.</p> <p>Concreet houdt een dergelijke test in het controleren of de ICT-infrastructuur tussen de gemeentelijke WKPB applicatie en de LV functioneert (via Gemnet) en er dus verbinding gemaakt kan worden met de productieomgeving van de LV bij het Kadaster. In de checklist I&amp;A (bijlage 2) staan de verschillende stappen die u als gemeente zelf kunt nemen uitgebreid beschreven.</p>
Verantwoordelijke personen / rollen	<ul style="list-style-type: none"> <li>• ICT-afdeling</li> <li>• Gemnet</li> <li>• Frontoffice WKPB</li> </ul>
Afhankelijkheden	<p>Afhankelijk van:</p> <ul style="list-style-type: none"> <li>• Beschikbaarheid van een PKI-Overheid Services Certificaat</li> <li>• Capaciteit ICT afdeling</li> <li>• Beschikbaarheid Gemnet infrastructuur</li> </ul>
Informatie bronnen	Checklist I&A (bijlage 2)
Aandachtspunten / tips & trics	Start hiermee niet voordat de interne test naar behoren is doorlopen
Tijdsduur (doorloop tijd)	3 werkdagen

#### 4.3 Autorisatieverzoek doen (stap 9)

Beschrijving van de activiteiten	Dien bij het Frontoffice WKPB uw aanvraag in om toegang te krijgen tot de productie omgeving op basis van het Verzoek tot autorisatie LV WKPB (beschikbaar op de site). Vermeld hierbij welke (getoetste) applicatie gebruikt wordt en stuur de publieke sleutel mee van het PKI-Overheid Services Certificaat mee (.PEM of .CER-bestand). Eindresultaat van deze stap is dat: a) de gemeente geautoriseerd is in de LV b) bevestiging heeft ontvangen van Frontoffice WKPB
Verantwoordelijke personen / rollen	WKPB beheerder
Afhankelijkheden	Afhankelijk van: <ul style="list-style-type: none"> <li>• Front Office WKPB</li> <li>• Beschikbaarheid van een PKI-Overheid Services Certificaat</li> </ul>
Informatie bronnen	Format autorisatie aanvraag (is beschikbaar op de site: <a href="http://www.kadaster.nl/wkpb/">www.kadaster.nl/wkpb/</a> )
Aandachtspunten / tips & trics	Voor samenwerkingsverbanden is aanvullende informatie nodig. Vermeld deze ook op het format
Tijdsduur (doorloop tijd)	2 werkdagen

## 5 Productie

### 5.1 Totaalstand percelen en beperkingen aanleveren (“initial load”) (stap 10)

Beschrijving van de activiteiten	<p>De gemeentelijke WKPB registratie dient een volledige en actuele set met percelen te bevatten. Gebruik hiervoor zonodig een nieuwe “Totaal-stand” van het Kadaster of verwerk de actuele massale output. Deze totaalstand moet aangeleverd worden aan de Landelijke Voorziening WKPB. Naast de percelen kunnen ook de reeds door de gemeente geregistreerde beperkingen meegeleverd worden, voorzover deze natuurlijk al door de gemeente in haar eigen systeem zijn ingevoerd. Met behulp van de dienst “VoegTotaalStandToe” kunnen de percelen (eventueel in combinatie met de beperkingen) initieel worden aangeleverd. Randvoorwaarde is dat de autorisatie aanvraag (zie 4.3) al succesvol uitgevoerd is. De LV kan op vier wijzen gevuld worden.</p> <ol style="list-style-type: none"> <li>1. Online via synchroon berichtenverkeer</li> <li>2. Offline aanleveren op CD/DVD</li> <li>3. Offline aanleveren via de upload service</li> <li>4. Het Kadaster de LV initieel te laten vullen met percelen per overeengekomen peildatum. Voor deze dienst wordt een bedrag in rekening gebracht. Meer informatie hierover kunt u opvragen bij het frontoffice: <a href="mailto:kadasterwkpb@kadaster.nl">kadasterwkpb@kadaster.nl</a>.</li> </ol> <p>Optie 1 kan geheel zelfstandig worden uitgevoerd. De grens is maximaal enkele Mb's. E.e.a. hangt ook af van de capaciteit van de gemeentelijke Gemnet aansluiting. Voor opties 2 en 3 zijn aanleverinstructie en formulier op de site beschikbaar (<a href="http://www.kadaster.nl/wkpb/">www.kadaster.nl/wkpb/</a>)</p>
Verantwoordelijke personen / rollen	WKPB beheerder en/of ICT afdeling
Afhankelijkheden	<p>Afhankelijk van:</p> <ul style="list-style-type: none"> <li>• Kadaster voor aanleveren van Totaal-stand percelen aan gemeente (indien geen correcte en actuele Totaal-stand bij de gemeente aanwezig)</li> <li>• Indiening van de modelverklaring bij het Kadaster</li> <li>• Correcte interne registratie van beperkingen</li> </ul> <p>Voor volledige invoering “oude” beperkingen heeft de gemeente de tijd tot 2 jaar na invoeringsdatum 1-7-2007.</p>
Informatie bronnen	Kadaster (Frontoffice WKPB)
Aandachtspunten / tips & trics	Randvoorwaarde voor het uitvoeren van deze activiteit is

	dat de gemeentelijke registratie helemaal ingericht is. De wijze van aanlevering is mede afhankelijk van de omvang van de totaalstand.
Tijdsduur (doorloop tijd)	5 werkdagen

## 5.2 Controle correcte werking (stap 11)

Beschrijving van de activiteiten	Na de initiële vulling van de LV kan gestart worden met het toevoegen van nieuwe en vigerende beperkingen via de gemeentelijke WKPB software. Check met behulp van de WKPB applicatie (via de beheerdiensten) of de eerst geregistreerde beperkingen goed in de LV staan
Verantwoordelijke personen / rollen	WKPB beheerder
Afhankelijkheden	<ul style="list-style-type: none"> <li>• Lesmateriaal LV</li> <li>• Draaiboek LV</li> </ul>
Informatie bronnen	
Aandachtspunten / tips & trics	<p>Dit is een standaard beheertaak voor de WKPB-beheerder ter verificatie van het synchroon houden van de WKPB registratie enerzijds en de landelijke voorziening anderzijds.</p> <p>Indien uw gemeentelijk applicatie deze raadpleegfunctionaliteit niet biedt, kunt u via uw gemeenteloket of rechtstreeks via Kadaster OnLine (KOL) de stand (steekproefsgewijs) controleren.</p>
Tijdsduur (doorloop tijd)	1 werkdag



## 6 En dan echt aan de slag .....

Als alle voornoemde stappen succesvol doorlopen zijn, bent u geautoriseerd om te communiceren met de LV en heeft u een initiële vulling geplaatst. Maar eigenlijk gaat het echte werk nu pas beginnen.

Alle nieuwe besluiten moeten binnen 4 dagen op de LV zijn opgevoerd. U moet er voor zorgen dat de massale output (ook wel was/wordt mutaties) maandelijks wordt verwerkt. En u moet ook de oude, nog geldige besluiten op uiterlijk 1 juli 2009 op de LV hebben opgevoerd.

En dat allemaal om er voor te zorgen dat alle vigerende beperkingen die vallen onder de WKPB, via Kadaster OnLine (KOL) aan geïnteresseerden kenbaar worden gemaakt.

De praktijk heeft ondertussen uitgewezen dat de nieuwe fase die u gaat betreden, niet altijd probleemloos zal zijn. Daarom graag uw aandacht voor een paar documenten die op de Kadaster-site zijn gepubliceerd. Mogelijk kunnen zij u bij deze nieuwe uitdagingen helpen.

**Gevolgen perceelsmutaties voor LV-WKPB** : aan de hand van een aantal scenario's wordt in dit document de massale output verklaard. Met name vragen over de "actualiteit" van percelen, splitsen in deelpercelen en splitsen in appartementen, zullen hiermee mogelijk duidelijk(er) worden.

**Ondersteuning bij voorbereidingen Wkpb** : een paar diensten die het Kadaster u kan bieden om u te helpen uw beperkingenregistratie op orde te krijgen volgens de WKPB

**Modelverklaring verwijderen gemeentelijke beperkingen uit kadastrale registratie** : een door u in te vullen verklaring om, *nadat* u *alle* oude nog vigerende beperkingen hebt opgevoerd op de LV, met één opdracht alle beperkingen uit de kadastrale registratie kunt laten verwijderen, zodat deze niet dubbel getoond worden op de KOL-berichten.



## **Bijlage 1: Instructie aanvraag certificaten t.b.v. WKPB**

### ***Inleiding***

In deze bijlage wordt beschreven hoe PKI-overheid Services certificaten<sup>2</sup>, en de bijbehorende publieke en private sleutels, gebruikt dienen te worden om te communiceren met de Landelijke Voorziening (LV). Er wordt beschreven hoe systeembeheerders / ontwikkelaars van gemeenten zelf een aanvraag voor een PKI-overheid Services certificaat kan doen.

Zonder het gebruik van public en private keys, kunnen derden zich mogelijk voordoen als een gemeente die gerechtigd is om de LV te gebruiken. Een 'man-in-the-middle' attack is een voorbeeld hiervan. Om ervoor te zorgen dat alleen geautoriseerde gemeenten toegang kunnen krijgen, is een geldig PKI-overheid Services certificaat bij de gemeente nodig om toegang te verkrijgen tot de LV.

In dit document zal niet ingegaan worden op de procedures voor het opzetten van een eigen CA of CSP.

Om een PKI-overheid services certificaat te kunnen aanvragen moet eerst een certificaataanvraag worden aangemaakt, oftewel een CSR<sup>3</sup>, welke men indient bij de certificaatuitgever (CSP)<sup>4</sup>. Normaliter kan dit met de gebruikelijke webserver, hierover is meer informatie te vinden op: <https://pkioverheid.gemnetcsp.nl/help/csr/index.htm>.

Voor een WKPB applicatie is het echter niet vanzelfsprekend dat deze een webserver gebruikt of op eenzelfde server/URL als een webserver draait. In dit document wordt daarom instructie gegeven hoe met een algemeen verkrijgbare open source tool een dergelijke CSR gedaan kan worden. In principe is gebruik hiervan slechts eenmalig nodig bij de aanvraag van een certificaat.

### ***Richtlijnen voor de naamgeving van het certificaat***

Bij aanvraag van het PKI-overheid services certificaat moeten een aantal gegevens worden ingevoerd over de gemeente. Om de herbruikbaarheid (bijvoorbeeld voor BAG) te vergroten en te voldoen aan de PKI-overheid eisen, dient aan een aantal randvoorwaarden voldaan te worden:

- Voor de naamgeving van Organisation (O) in het certificaat wordt de (unieke / officiële) naam gebruikt waaronder de gemeente is geregistreerd.
- Let er verder op dat de Common Name (CN) ingevuld is.

<sup>2</sup>De hier gehanteerde term "Services certificaat" is equivalent aan een organisatiegebonden c.q. SSL c.q. server certificaat, echter uitdrukkelijk geen persoonsgebonden certificaat

<sup>3</sup> Certificate signing request: aanvraag voor digitale ondertekening van een certificaat.

<sup>4</sup> CSP = certificate service provider. Dit zijn op dit moment: PinkRocadeCSP, GemnetCSP, DigiNotar, Centraal Instituut voor de Gezondheidszorg (CIGZ)

Één certificaatuitgever hanteert een afwijkende werkwijze: deze maakt zelf de private sleutel aan van het certificaat. De CSP heeft dan een kopie van de private sleutel. Het is wel zaak dat de aanvrager contractueel goed vastlegt met de CSP dat deze de private sleutel vernietigt. Zo niet dan is misbruik mogelijk en zijn verantwoordelijkheden niet helder



Datum  
25 febr 2009

Titel  
Stappenplan aansluiting LV-WKPB

Versie  
3.1

Blad  
18 van 28

- Indien u het certificaat voor meerdere doeleinden denkt te gaan gebruiken, dan is het verstandig de zogenaamde Common Name (CN) zo algemeen mogelijk te kiezen, dus bijvoorbeeld geen afdelingsnaam hierin opnemen.
- Als er voor de Common Name geen Fully Qualified Domain Name gebruikt wordt, maar er een certificaat wordt aangevraagd op een servernaam dan is er een Eigen Verklaring nodig. Deze Eigen Verklaring houdt in dat de contactpersoon op briefpapier van de gemeente verklaart dat het een eigen server betreft voor intern gebruik; u kunt hiervoor een template gebruiken dat te verkrijgen is bij uw CSP.
- Let erop dat het ontvangen certificaat goed beveiligd is om de server / PC waar deze uiteindelijk op komt te staan. Zorg daarom door adequate technische, fysieke en organisatorische beveiligingsmaatregelen dat onbevoegden hier geen toegang tot kunnen krijgen.

### ***Installatie en gebruik OpenSSL***

Er zijn meerdere pakketten, waarmee CSR's gegenereerd kunnen worden. In dit document wordt uitgegaan van OpenSSL, omdat dit programma voor bijna elk platform beschikbaar is en vrij te downloaden is via de website [openssl.org](http://openssl.org). De voorbeelden gaan uit van een versie 0.9.7g van openssl.

### ***OpenSSL***

Meestal is OpenSSL al meegeleverd bij de distributie van Linux. Als dit niet het geval is, kan het meestal met een packet-manager geïnstalleerd worden. Voor Windows is een installer beschikbaar via de website van openssl.

Controleer (na installatie) of openssl al geïnstalleerd is:

```
> openssl version
```

Hiermee wordt gelijk de versie van openssl getoond. Standaard wordt alles onder /usr/local/ssl geïnstalleerd, dus het pad moet eventueel aangepast worden.

Onder Windows wordt openssl standaard geïnstalleerd in C:\OpenSSL\bin. Het pad kan via de "system properties" (rechter muisknop op "deze computer") aangepast worden, bovendien kan het volledige pad opgegeven worden om het commando aan te roepen.

```
(C:\OpenSSL\bin\openssl.exe).
```

### ***Aanvragen en ondertekenen van certificaten***

Voor de productieomgeving, is een PKI-overheid Services certificaat vereist. Dit certificaat is via een PKI-overheid certificaatuitgever (CSP) via een CSR aan te vragen.

### ***Aanvragen certificaat bij CSP***



In deze paragraaf wordt beschreven, hoe gemeenten een CSR kunnen indienen bij een CSP. Gemeenten moeten eerst zelf een private-key genereren, door middel van:

```
> openssl genrsa -out priv.key 1024
```

Vervolgens kan er een request aangemaakt worden, die naar de eigen CSP's opgestuurd kan worden:

```
> openssl req -new -key priv.key -out newreq.pem
```

Er zal een aantal vragen gesteld worden voor het opstellen van het request. Let hierbij op de richtlijnen genoemd in de paragraaf 'Richtlijnen voor de naamgeving van het certificaat'.

Met bovenstaande commando's wordt er overigens geen passphrase (wachtwoord) gevraagd, wat beveiligingstechnisch niet sterk is. Om de beveiliging hieromtrent te verbeteren is het verstandig om het aanmaken van een private-key en het genereren van een CSR te combineren:

```
> openssl req -newkey 1024 -out newreq.pem \  
-keyout priv.key
```

Na het uitvoeren van dit commando wordt een passphrase gevraagd die goed bewaard moet worden. De CSP heeft deze passphrase ook nodig om een certificaat te kunnen aanmaken. Deze passphrase wordt meestal ook gevraagd tijdens het importeren van een p12 bestand in een client (browser).

Als de CSP een controle uitgevoerd heeft voor de gemeente in kwestie, zal het request ondertekend worden en zal er een ondertekend certificaatbestand (newcert.pem) teruggestuurd worden. Op basis van dit bestand kan de autorisatieaanvraag voor de LV gedaan worden.

Om het ondertekende certificaat in de eigen WKPB applicatie te kunnen gebruiken, is er mogelijk een PKCS#12 bestand nodig. De gemeente kan dit bestand met het volgende commando het genereren:

```
> openssl pkcs12 -in newcert.pem -inkey priv.key -export \  
-out mycert.p12
```

Dit bestand kan overigens beveiligd worden met een wachtwoord. Zie hiervoor de documentatie van openssl.

### ***Het importeren van een p12 bestand***

Het importeren van een p12 bestand met Internet Explorer gaat als volgt:

- Dubbelklik op het bestand mycert.p12
- Doorloop de certificaat import wizard
- Indien het bestand met een wachtwoord beveiligd is, moet dit hier ingegeven worden

- Kies vervolgens voor automatisch selectie van de plaatsing van het certificaat.
- Na het importeren van dit certificaat, dient de CA hiërarchie geïnstalleerd te worden.

Voor PKI-overheid Services certificaten kan deze gedownload worden via:

[http://www.pkioverheid.nl/fileadmin/PKI/PKI\\_certificaten/pkioverheid.p7b](http://www.pkioverheid.nl/fileadmin/PKI/PKI_certificaten/pkioverheid.p7b)

Voor test PKI-overheid-certificaten (door GemnetCSP geleverd) is de CA-hiërarchie te vinden op:

<https://pkioverheid.gemnetcsp.nl/test-certificate-chain.p7b>

### **Afkortingen en bronnen**

Certificate Signing Requests (CSR)

Certificate Authority (CA)

Certificate Service Provider (CSP)

Wet Kenbaarheid Publiek Rechtelijke Beperkingen (WKPB)

Public-key Infrastructure (PKI)

Certificate Revocation List (CRL)

Private Enhanced Mail (PEM)

Public-key Cryptography Standards (PKCS)

Personal Information Exchange Syntax Standard (PKCS#12)

### **Bronnen:**

<http://www.openssl.org/docs/HOWTO/certificates.txt>

<http://sial.org/howto/openssl/>

Manual Page openssl

## **Bijlage 2: Checklist I&A**

Deze checklist is bedoeld ter voorbereiding op de aansluiting met de Landelijke Voorziening. De checklist biedt houvast om te controleren of de infrastructuur tussen de gemeente en de Landelijke Voorziening juist werkt. De hieronder genoemde punten beschrijven wat u zelf ter voorbereiding kan en moet doen om de Landelijke Voorziening te kunnen benaderen via Gemnet.

### ***Technische toegangstest***

Als u al over een PKI-overheid Services certificaat beschikt, kan ook de authenticatie en eventueel ook de autorisatie getest worden. Dit kan door met een gebruikelijke webbrowser (IE, Firefox) de URL via Gemnet te benaderen: <https://www.wkpblv.nl/wkpb/cert.jsp>.

Nota bene: het PKI-certificaat moet hiervoor wel beschikbaar zijn in de certificate store van uw browser (IE: klik in het menu Extra van Internet Explorer op Internet-opties. Klik op het tabblad Inhoud. Klik onder Certificaten op de knop Certificaten of Uitgevers om de lijst met certificaten weer te geven die u vertrouwt, hier kunt u ook het certificaat toevoegen). Als dat niet zo is, dan krijgt u een foutmelding bij het benaderen van de bovengenoemde URL.

Indien een gemeente nog geen autorisatieaanvraag heeft gedaan met een PKI-overheid Services certificaat krijgt ment het onderstaande bericht op het scherm:

```
-----  
LV WKPB -Controle van client-certificaat pagina 1 van 1  
Certificaat:CN=<gemeentenaam>, O=<gemeentenaam>, L=<plaatsnaam>, C=NL  
Geen gebruiker gevonden bij certificaat  
-----
```

Indien een gemeente al wel een PKI-certificaat aangeboden heeft en het door het Kadaster is geautoriseerd, krijgt u de volgende melding:

```
-----  
LV WKPB -Controle van client-certificaat  
https://www.wkpblv.nl/wkpb/cert.jsp  
Certificaat: CN=<gemeentenaam>, O=<gemeentenaam>, L=<plaatsnaam>, C=NL  
Gebruiker: Gemeente <gemeentenaam>  
Beschouwingsgebied: [<gemeentenaam>(1708), Virtueel 1(9001)]  
Diensten: [<voor de gemeente beschikbare diensten binnen de Landelijke  
Voorziening>]  
-----
```

Bij de regel "Beschouwingsgebied" vindt u als het goed is uw eigen gemeentenaam: dit betekent dat uw PKI-certificaat is geautoriseerd voor betreffende gemeente in de LV WKPB.

Samenwerkende gemeenten met 1 PKI-certificaat zullen hier meerdere gemeentenamen vinden.

Als de toegangstest niet is gelukt kunt u om technische ondersteuning vragen via Frontoffice WKPB ([kadasterwkpb@kadaster.nl](mailto:kadasterwkpb@kadaster.nl)).

### ***Gekoppelde server of cliënt***

Zorg voor een server/cliënt die gekoppeld is via de Gemnet-router.

Deze server/cliënt moet een IP-adres krijgen uit de IP-reeks die overeenkomt met de IP-reeks die op de Gemnet router staat of een IP-adres uit het eigen LAN.

In het laatste geval zal uw organisatie er zelf voor moeten zorgen dat dit IP-adres omgeNat wordt naar een IP-adres uit de Gemnet reeks.

### ***Routing via Gemnet***

Indien uw organisatie internet via Gemnet afneemt, hoeft er qua routing niets te worden veranderd.

Wanneer dit niet het geval is, zal uw organisatie ervoor moeten zorgen dat het IP-adres of -reeks dat wordt gebruikt voor de WKPB via het eigen netwerk gerouteerd wordt naar de Gemnet router door middel van een statische route. De Gemnet routes kunt u vinden op hun klantenportaal; Statische routing Gemnet.

### ***Dns-server aanpassen, updaten en host-files***

Wanneer uw organisatie gebruik maakt van de dns-server van Gemnet, krijgt u de juiste gegevens voor deze verbinding.

Mocht dit niet het geval zijn, moet uw organisatie ervoor zorgen dat zij secundair draaien voor de websites die op Gemnet bekend zijn.

Indien uw organisatie met host-files werkt, moet ervoor worden gezorgd dat deze ook zijn aangepast.

### ***Firewall aanpassingen***

Als uw organisatie in het bezit is van een eigen firewall moet er worden nagekeken of deze firewall de benodigde IP-adressen en poorten ( poort 80 voor http en 443 voor https ) open heeft staan naar Gemnet toe.

### ***Proxyserver***

Proxy server (authenticatie)

Wanneer de communicatie met Gemnet (of internet) via een proxy verloopt, moet de te gebruiken client een voorziening hebben om deze proxy in te stellen. Tevens moet deze client dan ondersteuning hebben voor de authenticatie mechanismen die eventueel gebruikt worden door de proxy server.

In het bijzonder moet er opgelet worden indien er gebruik gemaakt wordt van open source software in combinatie met een proxy server die gebruik maakt van NTLM authenticatie. Het NTLM protocol is een closed source oplossing van Microsoft en de kans is daardoor aanwezig dat de open source software hiervoor geen ondersteuning biedt.

### ***Workaround***



Datum  
25 febr 2009

Titel  
Stappenplan aansluiting LV-WKPB

Versie  
3.1

Blad  
23 van 28

Gebruik maken van een IIS proxy server die gebruik maakt van NTLM authenticatie gaat niet zonder meer in combinatie met de Workaround SSL Authenticatie v1.1, zoals deze gepubliceerd staat op [www.kadaster.nl/wkpb/](http://www.kadaster.nl/wkpb/). De software die gebruikt wordt voor deze workaround heeft namelijk geen ondersteuning voor proxies met NTLM authenticatie, met als gevolg dat het niet mogelijk is om met de LV WKPB te communiceren.

Om dit euvel te verhelpen kan de workaround uitgebreid worden met een lokale proxy (NTLM Authorization Proxy Server, <http://www.geocities.com/rozmanov/ntlm/>) die de NTLM authenticatie voor zijn rekening neemt. Middels deze oplossing is het mogelijk met de LV-WKPB te communiceren.

### ***HTTPS verbindingen met tweezijdige SSL authenticatie***

De LV WKPB maakt gebruik van SOAP-over-HTTPS met tweezijdige SSL authenticatie. De netwerk configuratie aan de kant van de client moet dus toestaan dat er een HTTPS connectie opgezet wordt dmv tweezijdige SSL.

In het bijzonder moet daarbij gelet worden op firewalls en proxies. Deze moeten verbindingen naar het adres van de LV WKPB op poort 443 toestaan. Daarnaast moet de proxy/firewall toestaan dat de client tijdens de SSL-handshake met de LV WKPB zijn eigen certificaat opstuurt.

### ***PKI-overheid Services certificaat***

Verkrijgen van het benodigde PKI-overheid Services Certificaat (c.q. server/SSL/organisatiegebonden):

Op het moment dat uw gemeente aangesloten wil worden op de Landelijke Voorziening, of u als leverancier wil testen op een van beide testomgevingen, moet u op uw WKPB-systeem over een PKI-overheid Services Certificaat beschikken voor de PKI-authenticatie. Houdt u hierbij rekening met een doorlooptijd van een aantal weken. Zie ook bijlage 1 van dit stappenplan.

### ***Waar kan ik PKI-overheid certificaten kopen?***

Dit kan bij verschillende leveranciers; voor een overzicht zie <http://www.pkioverheid.nl/voor-certificaatverleners/toegetreden-certificaatverleners/>.

### ***Meer informatie***

Overzichtelijke informatie over PKI-overheidcertificaten en WKPB met relevante links vindt u op de sites van de certificaatuitgevers

<http://www.gemnetcsp.nl/?page=wkpb> (GemnetCSP) en

<https://www.servercertificaat.nl/common.asp?id=287> (DigiNotar).



Datum

25 febr 2009

Titel

Stappenplan aansluiting LV-WKPB

Versie

3.1

Blad

24 van 28

### **Bijlage 3: Geconstateerde problemen met betrekking tot netwerk en certificaten**

#### **Verbinding met de landelijke voorzieningen WKPB (en BAG) opzetten**

Alleen beveiligde (SSL) verbindingen zijn toegestaan om vanuit een toepassing te communiceren met een landelijke voorziening WKPB of BAG. Verbinding opzetten met de productie landelijke voorziening WKPB kan op dit moment alleen via Gemnet. Beveiligde verbindingen met de conformiteit en test landelijke voorzieningen voor WKPB kunnen zowel via Internet als via Gemnet worden opgezet. SSL beveiligde verbindingen met een van de landelijke voorzieningen BAG kunnen via Internet worden opgezet. Voor het kunnen opzetten van een beveiligde SSL verbinding met een van de landelijke voorzieningen dient een applicatie zich te authenticeren met behulp van een PKI Overheid service certificaat. Een dergelijk certificaat kan worden aangevraagd bij een van de hiertoe bevoegde certificaat uitgevende instanties (Certificate Service Provider, CSP). PKI Overheid certificaten worden op dit moment uitgegeven door GemnetCSP, GetronicsPinkRocade en Diginotar.

#### **Certificaten en autorisatie voor gebruik van de landelijke voorzieningen WKPB (en BAG)**

Om geautoriseerd te kunnen worden voor toegang tot de landelijke voorziening moet het publieke deel van een door een PKI Overheid CSP ondertekend certificaat worden opgestuurd naar Kadaster (samen met het autorisatieverzoek).

#### **Gebruik van test-certificaten**

PKI Overheid test-certificaten uitgegeven door GemnetCSP, GetronicsPinkRocade en Diginotar kunnen worden gebruikt voor het opzetten van een verbinding met de landelijke voorziening in de conformiteits- en testomgevingen van de landelijke voorzieningen WKPB en BAG. Gebruik van testcertificaten voor toegang tot de productieomgevingen van de landelijke voorzieningen WKPB en BAG is niet mogelijk.

#### **Problemen bij het opsturen van certificaten bij aanvraag voor autorisatie**

Regelmatig worden de verkeerde gegevens opgestuurd bij het aanvragen van autorisaties voor een van de landelijke voorzieningen WKPB en BAG. Hieronder worden een aantal van in de praktijk voorkomende vergissingen beschreven.

In plaats van het publieke deel van het certificaat wordt per abuis een certificaat ondertekening verzoek opgestuurd (Certificate Signing Request, CSR). Een CSR dient echter te worden opgestuurd naar de PKI Overheid certificaat verstrekende instantie (Certificate Service Provider, CSP) ter ondertekening. Het door een CSP ondertekende (publieke deel van een) certificaat dient vervolgens te worden opgestuurd naar Kadaster bij het aanvragen van autorisatie voor toegang tot de landelijke voorzieningen van WKPB en BAG (samen met autorisatieverzoek).

Een CSR ziet er ongeveer uit als onderstaand voorbeeld en is te herkennen aan het feit dat de tekst begint met de regel -----BEGIN NEW CERTIFICATE REQUEST----- en eindigt met de regel -----END NEW CERTIFICATE REQUEST-----

-----BEGIN NEW CERTIFICATE REQUEST-----



Datum  
25 febr 2009

Titel  
Stappenplan aansluiting LV-WKPB

Versie  
3.1

Blad  
25 van 28

```
MIICFDCCAX0CAQAwgdUxCzAJBgNVBAYTAm5sMQ0wCwYDVQQKEwRURXN0MQ0wCwYDVQQHEwRUZXN0MSUwIwYDVQQLExxCZWRyaWpmc2NjYWF0IC16aWUgQ1BTMRAwDgYDVQQLEwdCZXBlcmt0MQkwBwYDVMBgNVBAMTBUtsYWFzMSUwHwYJKoZIhvcJrbGFhc0BkaWdpbm90YXlubmwxEjAQBgNVBAwTCURpcmVjdGV1cjEdMBsGA1UECRMUamhka2hkYWtmZCBja2xkamwgMzIwZDQYJKoZIhvcNjMVhw1Pm53M=
-----END NEW CERTIFICATE REQUEST-----
```

Voor het aanvragen van een certificaat moet eerst een sleutelpaar worden gegenereerd waarbij een privé sleutel en een publieke sleutel worden gegenereerd. In plaats van het publieke deel van het certificaat wordt de bijbehorende privé sleutel opgestuurd. Hiermee is de privé sleutel echter gecompromitteerd en dient een nieuw certificaat te worden aangeschaft. De houder van het certificaat kan namelijk niet meer zeker zijn dat deze privé sleutel niet door derden gebruikt wordt. Het certificaat is hiermee waardeloos geworden.

De generatie van het sleutelpaar kan zelf worden gedaan m.b.v. bijvoorbeeld Microsoft IIS of m.b.v. de opensource programmatuur OpenSSL. In dat geval beschikt de aanvrager van een PKI Overheid certificaat reeds zelf over de privé sleutel. Het publieke deel moet naar de PKI Overheid CSP worden gestuurd ter ondertekening.

Het genereren van het sleutelpaar kan vaak ook door de PKI Overheid CSP worden gedaan. In dat geval zal de aanvrager in het algemeen een ondertekend publiek certificaat, een privé sleutel en vaak ook nog het bijbehorende rootcertificaat van de CSP en eventueel tussenliggende (intermediate) certificaten van de CSP ontvangen. Alleen het door een PKI Overheid CSP ondertekende publieke certificaat moet naar Kadaster worden gestuurd bij het aanvragen van autorisatie voor toegang tot de landelijke voorzieningen van WKPB en BAG. Stuur nooit de privé sleutel toe!!!

Een door RDW uitgegeven certificaat is geen PKI Overheid certificaat en kan niet worden gebruikt voor authenticatie bij het opzetten van een verbinding met een landelijke voorziening WKPB en BAG of voor autorisatiedoeleinden.

#### **Certificaat formaten en bestandextensies**

Een ondertekend certificaat dat wordt geleverd door een CSP in de vorm van een bestand kan op verschillende manieren zijn gecodeerd. Hierbij maakt de CSP gebruik van een van de beschikbare coderingsstandaarden. Ondersteund worden certificaten die zijn gecodeerd in CER (standaardformaat DER) en PEM (base64-gecodeerde DER) formaat. Als extensie van het certificaatbestand wordt meestal .CER of .PEM gebruikt.

#### **Installatieproblemen certificaten**

Bij het opzetten van een SSL verbinding met een van de landelijke voorzieningen dient geverifieerd te kunnen worden dat het service certificaat dat door de landelijke voorziening wordt gestuurd ter authenticatie is ondertekend door een vertrouwde derde partij die PKI Overheid certificaten uit mag geven. Hiervoor moet de applicatie toegang hebben tot het stamcertificaat, domeincertificaten en CSP-certificaten van PKI Overheid.



Datum

25 febr 2009

Titel

Stappenplan aansluiting LV-WKPB

Versie

3.1

Blad

26 van 28

Waar deze certificaten geïnstalleerd dienen te worden voor uw applicatie kan verschillen per toepassing en omgeving. Raadpleeg hiervoor uw leverancier. Het stamcertificaat, domeincertificaten en CSP-certificaten van PKI Overheid kunnen worden gedownload van de website van PKI Overheid. Deze is te bereiken via de URL <https://www.pkioverheid.nl/>

De WKPB (of BAG) toepassing moet ook bij de privé sleutel kunnen komen die bij het service certificaat hoort dat wordt gebruikt om de betreffende gemeente te authenticeren. Deze sleutel dient dus net als het ondertekende PKI Overheid certificaat eveneens te worden geïnstalleerd zodat de gemeentetoepassing bij de sleutel kan. De gemeente dient daarbij er voor zorg te dragen dat de privé sleutel niet gecompromitteerd raakt.

#### **Waarde Subject.commonName**

Het Subject Name veld van een certificaat dient uniek te zijn. De naamsgegevens van een X509 certificaat zijn gerelateerd aan het X500 directory datamodel. Bij voorkeur wordt als Subject Name van een certificaat de X.500 Distinguished Name gehanteerd. Een DN is in feite een combinatie van attributen die samen uniek moeten zijn. De belangrijkste attributen die worden gebruikt zijn o.a. de Common Name (CN), Organization Name (O), Organizational Unit (OU) en Country (C).

Bijvoorbeeld: CN="wkpserver.gemeenteapeldoorn.nl", O="Gemeente Apeldoorn", C="NL"

In het PvE deel 3b van PKI Overheid wordt beschreven welke attributen van o.a. het Subject gevoerd mogen worden in het certificaat en welke eisen gesteld worden. Daarnaast worden in paragraaf 2.9 van het document 'PKI Overheid-certificaten voor BAG v1.0' (een ICT-handreiking die is opgesteld door het ministerie van VROM), aanbevelingen gedaan ten aanzien van de gegevens die in een certificaat opgenomen dienen te worden. Deze aanbevelingen zijn zowel van toepassing voor certificaten voor BAG als ook voor certificaten voor WKPB. Voor het attribuut CommonName wordt aanbevolen om de volgende waarde in te vullen:

- 1) indien de server van de gemeente waarop het certificaat geïnstalleerd wordt een unieke DNS naam heeft dan is het advies om voor de CommonName de Fully Qualified Domain Name (FQDN) in te vullen (de volledige Internetdomein naam). PKI Overheid geeft zelfs aan dat indien een service een DNS naam heeft dat deze MOET worden vermeld in de commonName als FQDN.
- 2) indien de server geen unieke Internet DNS naam heeft dan wordt aanbevolen de unieke naam van de server zoals deze binnen de gemeente infrastructuur bekend is te gebruiken.
- 3) als derde variant kan gekozen worden om de organisatienaam plus uniek serienummer te hanteren voor de CommonName.
- 4) als laatste variant is het mogelijk om het ip adres van de server waarop het certificaat geïnstalleerd wordt op te geven voor de commonName. Deze variant wordt in de praktijk echter afgeraden.



Datum  
25 febr 2009

Titel  
Stappenplan aansluiting LV-WKPB

Versie  
3.1

Blad  
27 van 28

## **Routeringsproblemen**

De servers van de landelijke voorziening WKPB hebben officiële Internet adressen. De conformiteit en testservers zijn behalve via Gemnet ook via Internet toegankelijk. Indien een gemeente wel verbinding kan opzetten met de conformiteit en testomgeving van WKPB maar niet met de productieomgeving van WKPB dan kan een mogelijke oorzaak zijn dat de WKPB servers via Gemnet worden benaderd vanuit het lokale gemeentenetwerk maar dat in werkelijkheid de verbinding via Internet gerouteerd worden vanuit het lokale gemeentenetwerk (ervan uitgaande dat er ook een Internetaansluiting beschikbaar is naast een gemeenteaansluiting).

### **Oplossing:**

Om te zorgen dat het netwerkverkeer vanaf het gemeentenetwerk naar de wkpb servers via Gemnet loopt zal de routing binnen het gemeentenetwerk aangepast dienen te worden. Er zullen expliciet routes gedefinieerd moeten worden die aangeven dat de productie wkpb host (145.77.103.50) via de gemnet router verbinding moet opzetten met de LV. Voor de overzichtelijkheid is het aan te bevelen ook de routes naar de conformiteit (145.77.103.51) en de test (145.77.103.52) WKPB servers naar de Gemnet router te laten wijzen. De netwerkbeheerder van de gemeente heeft als het goed is het overzicht waar de route het beste kan worden gedefinieerd binnen het gemeentenetwerk.

Traceroute is niet bruikbaar voor het uitvoeren van een netwerk connectiviteit test omdat door de firewall alleen SSL verkeer wordt toegestaan tot de landelijke voorzieningen. Wel kan gecontroleerd worden of vanaf het gemeente systeem een TCP/IP verbinding met een landelijke voorziening server gelegd kan worden door met het telnet commando te proberen vanaf het gemeente systeem een tcp ip connectie te maken naar de betreffende landelijke voorziening server op TCP poortnummer 443. Voor WKPB kan dit bijvoorbeeld als volgt:

```
telnet <omgeving>.wkpblv.nl 443
```

Meestal zal niet meer dan een leeg venster te zien als het lukt de verbinding tot stand te brengen. In geval van een foutmelding door de telnet toepassing dat er geen verbinding tot stand kan worden gebracht of dat een timeout optreedt is dit een aanwijzing dat de netwerkverbinding niet tot stand gebracht kan worden. Er kunnen diverse oorzaken zijn waarom de verbinding niet tot stand komt. Veel voorkomende oorzaken zijn niet goed geconfigureerde routeringstabellen en firewalls die netwerkverkeer tegenkomen.



#### **Bijlage 4: Contactgegevens**

Nadere informatie, ondersteuning, autorisatieaanvragen etc:

Frontoffice WKPB Kadaster.

Email: [kadasterwkpb@kadaster.nl](mailto:kadasterwkpb@kadaster.nl)

Site/pagina: [www.kadaster.nl/wkpb/](http://www.kadaster.nl/wkpb/)

Formulieren e.d. die teruggestuurd moeten worden, zijn voorzien van een retouradres. Om onnodige vertraging te voorkomen: graag de adressering aanhouden die op het formulier is aangegeven (niet alle acties worden op dezelfde locatie uitgevoerd).