



Datum:

27 aug. 2020

Auteur:

KPN Security

Versie:

release 7.3

Handleiding

KPN PKloverheid

Toelichting aanvraag servercertificaat

(alle typen)

Inhoudsopgave

Inhoudsopgave.....	2
1 Inleiding.....	3
1.1 Terminologie.....	3
1.2 Referenties.....	5
2 Aanvraagproces Servercertificaten.....	6
2.1 Proces stroomdiagram.....	6
2.2 Toelichting op de processtroom.....	6
3 Servercertificaataanvraag zonder KPN Self Service Portaal.....	8
3.1 Keuzescherm voor het type servercertificaat.....	8
3.2 Startscherm: checklist randvoorwaarden en validatie email.....	8
3.3 Scherm 1: Contactpersoon.....	12
3.4 Scherm 2: Certificaatbeheerder.....	13
3.5 Scherm 3: Certificaat.....	16
3.6 Scherm 4: Controle.....	22
3.7 Scherm 5: Voorwaarden.....	24
3.8 Afronding.....	27
3.8.1 Optie 1: aanvraag elektronisch ondertekenen en indienen.....	27
3.8.2 Optie 2: aanvraag op papier per post indienen.....	28
4 Servercertificaataanvraag via het KPN Self Service Portaal.....	29
4.1 Inloggen in het Self Service Portaal / MijnCertificaten.....	29
4.2 Scherm 1: Contactpersoon.....	30
4.3 Scherm 2: Certificaatbeheerder.....	31
4.4 Scherm 3: Certificaat.....	32
4.5 Scherm 4: Controle.....	33
4.6 Scherm 5: Voorwaarden.....	33
4.7 Afronding.....	34
5 Beoordeling aanvraag door KPN en vervolg.....	35
5.1 Domeincontrole.....	35
5.2 Identificatie Certificaatbeheerder en uitgifte.....	35
5.3 Certificaatvernieuwing en geldigheidsduur.....	35
6 BIJLAGEN: email en PDF formulier.....	36
6.1 Emailbericht afronding.....	36
6.2 PDF Aanvraag Servercertificaat.....	36

1 Inleiding

Dit document bevat een toelichting op de aanvraag van een PKI-overheid Servercertificaat via:

- het webformulier dat beschikbaar is op: <https://kpnpkio.managedpki.com/csr/>; of
- het Self Service Portal (SSP) dat beschikbaar is op: <https://kpnpkio.managedpki.com/ssp/>

- Met een pijltje is aangegeven welke concrete acties er nodig zijn om het formulier en de aanvraag af te ronden.

U vraagt u een PKI-overheid servercertificaat aan namens een geregistreerde Abonnee van de PKI-overheid Certificatiedienstverlening van KPN. Een (eenmalige) abonneeregistratie is nodig om Certificaten van de PKI voor de overheid die door KPN worden uitgegeven te mogen aanvragen, ontvangen en gebruiken. Als u nog geen abonneeregistratie heeft uitgevoerd ga dan eerst naar: <https://kpnpkio.managedpki.com/registratie/>.

Op dit moment zijn de volgende types servercertificaten leverbaar:

- Standaard SSL
- Digipoort Private
- Private SSL

Het servercertificaat wordt na goedkeuring van de aanvraag uitgegeven aan een eerder geregistreerde of een nieuw te identificeren Certificaatbeheerder.

1.1 Terminologie

Hieronder zijn enkele definities opgenomen die van belang zijn voor een goed begrip van dit document.

Abonnee: de natuurlijke persoon of rechtspersoon die een overeenkomst aangaat met KPN om uitgifte van PKI-overheid Certificaten aan door de Abonnee aangewezen Certificaathouders te bewerkstelligen.

Bevoegd vertegenwoordiger: Een natuurlijk persoon die bevoegd is een organisatie te vertegenwoordigen. Bevoegdheid tot vertegenwoordiging kan voortvloeien uit de wet of uit een volmacht. Er kan ook sprake zijn van meerdere natuurlijke personen, b.v. een bestuur van een vereniging, die gezamenlijk bevoegd zijn een organisatie te vertegenwoordigen.

Certificaat: Een elektronisch bestand met de publieke sleutel van een eindgebruiker, samen met aanvullende identificerende gegevens zoals een naam van een persoon of service. Een certificaat is digitaal ondertekend door de Certification Authority waardoor het certificaat onvervalsbaar is.

Certificaatbeheerder: een natuurlijke persoon die bevoegd is om namens de Abonnee en ten behoeve van de Certificaathouder een Servercertificaat of Groeps-certificaat te installeren, te beheren en/of in te trekken. De Certificaatbeheerder voert handelingen uit waartoe de Certificaathouder zelf niet in staat is.

Certificaathouder: Een entiteit die geïdentificeerd wordt in een certificaat als de houder van de private sleutel behorend bij de publieke sleutel die in het certificaat gegeven wordt.

De certificaathouder zal in het geval van persoonsgebonden certificaten een natuurlijke persoon zijn, in het geval van services certificaten zal de certificaathouder een functie of een machine/server zijn.

Certificate Signing Request (CSR): Een Certificate Signing Request is een bestand dat de publieke sleutel bevat die in het Servercertificaat komt te staan. Certificaatbeheerder dient dit aan te maken op het serversysteem waarvoor het certificaat wordt aangevraagd.

Contactpersoon: persoon die namens de Abonnee is geautoriseerd om certificaten aan te vragen en in te trekken, alsmede om andere Contactpersonen en Certificaatbeheerders te autoriseren. De Bevoegd Vertegenwoordiger heeft na registratie automatisch de autorisaties van een Contactpersoon.

FQDN (Fully Qualified Domain Name): Een Fully Qualified Domain Name is volgens de definitie van PKI-overheid een in het Internet Domain Name System (DNS) geregistreerde volledige naam waarmee een server op het Internet uniek is te identificeren en te adresseren. Een uitgebreide technische toelichting over FQDN vindt u hier:

<https://certificaat.kpn.com/aanvragen/servercertificaten/fqdn-naam-van-de-service/>

Samengevat komt dit neer op de naam die u in een browser intypt om het systeem te benaderen, bijvoorbeeld 'certificaat.kpn.com' of 'www.logius.nl'.

Public Key Infrastructure – PKI: Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Het doel is het mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

PKI voor de overheid (PKI-overheid of PKIO): De gehele PKI infrastructuur die door de Policy Authority (PA) PKI-overheid wordt beheerd. De PA PKI-overheid ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid.

De PKI voor de overheid is een afsprakenstelsel. Dit maakt generiek en grootschalig gebruik mogelijk van de elektronische handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. De PKI voor de overheid voorziet in een betrouwbaar normenkader voor PKI-diensten met een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en andere gebruikers.

SAN / Subject Alternative Name: Met het toevoegen van (optionele) additionele SAN's kunt u een servercertificaat geschikt maken voor beveiliging van meerdere domeinnamen en meerdere hostnamen binnen een domeinnaam. Naast de primaire naam van de service (FQDN) kunt u maximaal 10 aanvullende Subject Alternative Names (SAN's) in één servercertificaat toevoegen. Bij een EV SSL servercertificaat dienen de SAN's en primaire naam van de service uit hetzelfde domein te komen.

Services/server certificaat: Een certificaat waarmee een functie of apparaat, bijvoorbeeld een server, wordt gekoppeld aan een rechtspersoon of andere organisatie. In het geval van een server wordt het certificaat gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.

Veilige Omgeving: De omgeving van het systeem dat de sleutels van de Servercertificaten bevat. Binnen deze omgeving is het toegestaan de sleutels softwarematig te beschermen, in plaats van in een Hardware Security Module. De compenserende maatregelen hiervoor moeten van dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging, audit en functiescheiding.

Vertrouwende Partij: de natuurlijke persoon of rechtspersoon die ontvanger is van een Certificaat en die handelt in vertrouwen op dat Certificaat. Door te vertrouwen op een Certificaat gaat de Vertrouwende Partij impliciet akkoord met de KPN Bijzondere Voorwaarden PKI Overheid Certificaten. Voor dit "akkoord gaan" hoeft geen aparte handeling door de Vertrouwende Partij te worden verricht;

1.2 Referenties

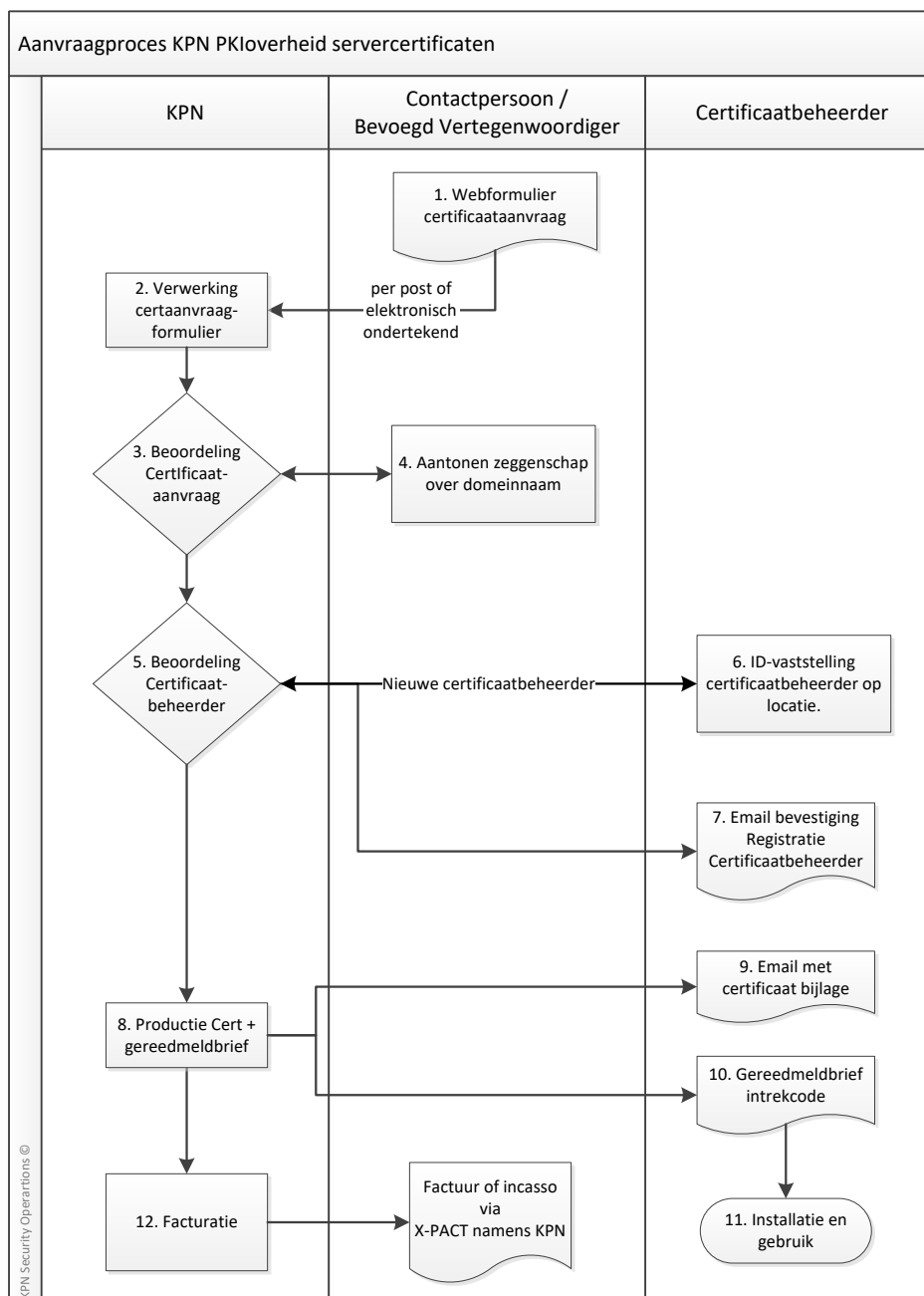
Voor meer informatie over de PKI voor de overheid en de Certificatiedienstverlening van KPN verwijzen wij u naar:

1. De documenten van de PKI voor de overheid, deze zijn beschikbaar op de site van PKIoverheid;
<https://www.logius.nl/diensten/pkioverheid/>
2. De documenten van de Certificatiedienstverlening van KPN, de belangrijkste daarvan zijn de Certificate Practice Statement en de KPN Bijzondere Voorwaarden PKI Overheid Certificaten. Deze zijn beschikbaar via <https://certificaat.kpn.com/downloads/>

2 Aanvraagproces Servercertificaten

2.1 Proces stroomdiagram

Het proces voor de aanvraag van een servercertificaat is in de volgende figuur weergegeven.



2.2 Toelichting op de processtroom

Het aanvraag proces van een PKIoverheid Servercertificaat bestaat uit de volgende stappen:

1. Allereerst dient u op de website het webformulier in te vullen om de aanvraag te starten.

Afronding van het webformulier resulteert in een PDF document dat ondertekend dient te worden door de Contactpersoon. Dit kan op papier of elektronisch. Vervolgens dient u het ondertekende formulier te versturen naar KPN per post of elektronisch.

Deze stap wordt uitgebreid toegelicht in de volgende hoofdstukken.

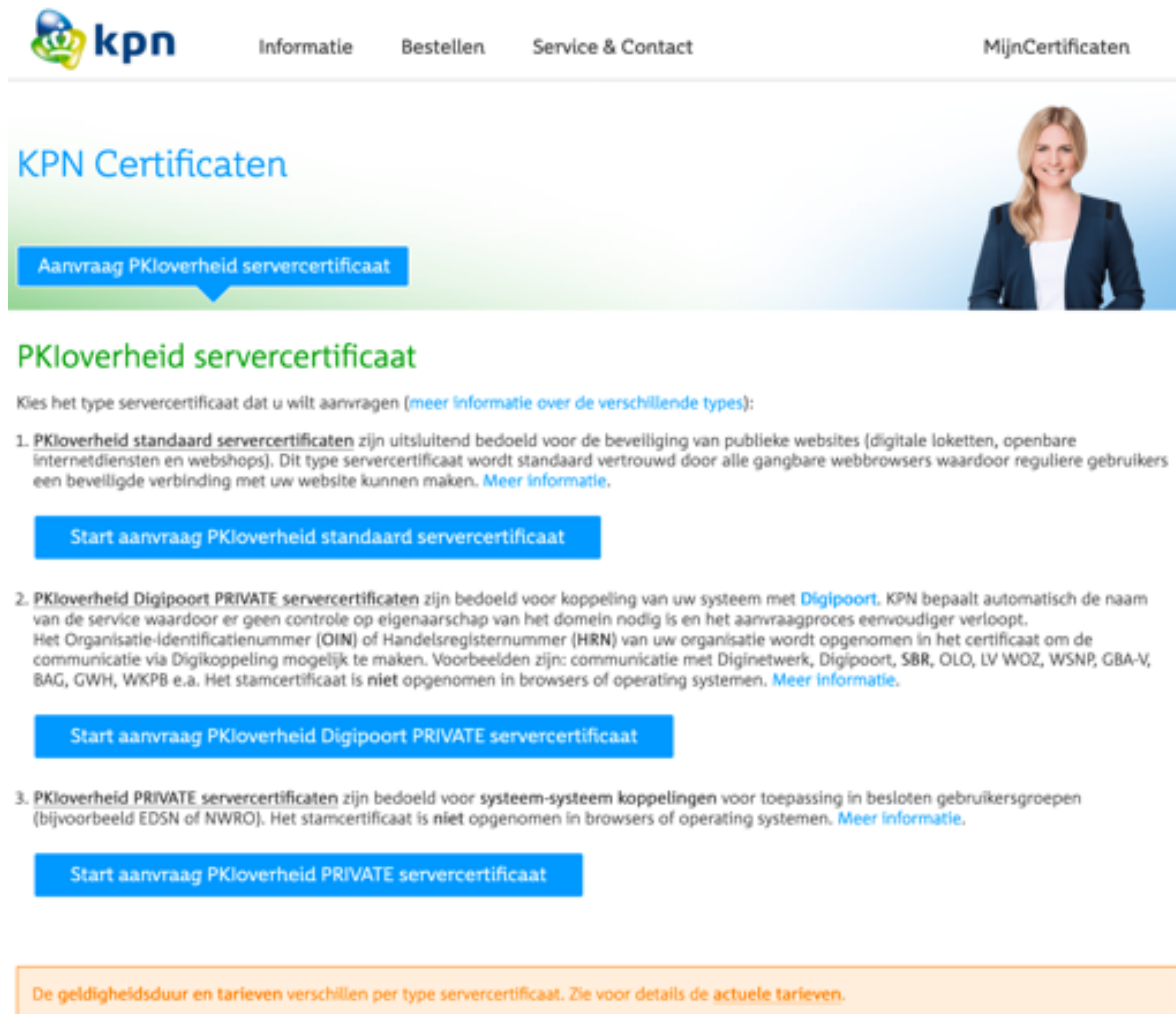
2. Na ontvangst van de aanvraag start bij KPN het validatieproces. Dit betreft allereerst het vergelijken van de gegevens van Abonnee en de Contactpersoon met gegevens die al bij KPN zijn geregistreerd.
3. Vervolgens vindt een inhoudelijke controle plaats van de certificaataanvraag. Het kan zijn dat KPN ten behoeve van de validatie nog contact opneemt voor aanvullende informatie.
4. KPN stuurt een emailbericht naar de Contactpersoon met het verzoek om aan te tonen dat deze zeggenschap heeft over de gebruikte domeinnaam. Dit kan op verschillende manieren worden aangetoond en is nader toegelicht in de toegestuurde email.
5. Indien er een nieuwe Certificaatbeheerder is opgegeven, zal KPN een identificatie laten uitvoeren.
6. Een koerier voert deze identificatie in opdracht van KPN uit op locatie van de klant. Per email ontvangt de Certificaatbeheerder een uitnodiging om een afspraak te maken voor deze identificatie.
7. KPN zal de identificatie controleren. Indien deze correct is ontvangt de Certificaatbeheerder een bevestiging van de registratie.
8. KPN produceert vervolgens het servercertificaat.
9. KPN stuurt het certificaat per email naar de Certificaatbeheerder met een kopie naar de Contactpersoon die de aanvraag doet. KPN gebruikt daarvoor het emailadres dat de contactpersoon opgeeft bij de registratie van de Certificaatbeheerder.
10. De Certificaatbeheerder ontvangt een brief met de intrekcode. Hiermee is het mogelijk om (bijvoorbeeld in geval van een beveiligingsincident) het certificaat in te trekken via een self-service portal. Zie hiervoor de *KPN Bijzondere Voorwaarden PKI Overheid Certificaten*¹. Indien gewenst kan de intrekcode ook per versleutelde email worden toegestuurd. In dat geval dient u contact op te nemen met de Servicedesk. Zie <https://certificaat.kpn.com/support/> voor contactgegevens.
11. Het certificaat is gereed voor gebruik.
12. Tot slot ontvangt de Abonnee op het opgegeven facturatieadres een factuur.

¹ Zie https://certificaat.kpn.com/files/voorwaarden/BIJZ_VW_PKI_OVERHEID_CERTIFICATEN.pdf

3 Servercertificaataanvraag zonder KPN Self Service Portaal

3.1 Keuzeschermb voor het type servercertificaat

De aanvraag van een Servercertificaat start op <https://kpnpkio.managedpki.com/csr/> als volgt:



The screenshot shows the KPN Certificaten website. At the top, there is a navigation bar with the KPN logo, 'Informatie', 'Bestellen', 'Service & Contact', and 'MijnCertificaten'. Below the navigation bar, the main heading is 'KPN Certificaten'. A blue button labeled 'Aanvraag PKIoverheid servercertificaat' is prominently displayed. Below this, the section is titled 'PKIoverheid servercertificaat'. A sub-heading asks the user to choose the type of certificate. Three options are listed, each with a blue button to start the request:

- PKIoverheid standaard servercertificaten** zijn uitsluitend bedoeld voor de beveiliging van publieke websites (digitale loketten, openbare internetdiensten en webshops). Dit type servercertificaat wordt standaard vertrouwd door alle gangbare webbrowsers waardoor reguliere gebruikers een beveiligde verbinding met uw website kunnen maken. [Meer informatie.](#)
Start aanvraag PKIoverheid standaard servercertificaat
- PKIoverheid Digipoort PRIVATE servercertificaten** zijn bedoeld voor koppeling van uw systeem met **Digipoort**. KPN bepaalt automatisch de naam van de service waardoor er geen controle op eigenaarschap van het domein nodig is en het aanvraagproces eenvoudiger verloopt. Het Organisatie-identificatienummer (OIN) of Handelsregisternummer (HRN) van uw organisatie wordt opgenomen in het certificaat om de communicatie via Digikoppeling mogelijk te maken. Voorbeelden zijn: communicatie met Diginetwerk, Digipoort, SBR, OLO, LV WOZ, WSNP, GBA-V, BAG, GWH, WKPB e.a. Het stamcertificaat is niet opgenomen in browsers of operating systemen. [Meer informatie.](#)
Start aanvraag PKIoverheid Digipoort PRIVATE servercertificaat
- PKIoverheid PRIVATE servercertificaten** zijn bedoeld voor **systeem-systeem koppelingen** voor toepassing in besloten gebruikersgroepen (bijvoorbeeld EDSN of NWRO). Het stamcertificaat is niet opgenomen in browsers of operating systemen. [Meer informatie.](#)
Start aanvraag PKIoverheid PRIVATE servercertificaat

De geldigheidsduur en tarieven verschillen per type servercertificaat. Zie voor details de [actuele tarieven.](#)

Met de blauwe knoppen kiest u het type servercertificaat dat u wilt aanvragen met een korte toelichting. Indien u al weet welk type u nodig heeft kunt u deze stap overslaan met de volgende directe links:

- Standaard SSL: <https://kpnpkio.managedpki.com/csr/standard-ssl/>
- Digipoort private: <https://kpnpkio.managedpki.com/csr/digipoort/>
- Private SSL: <https://kpnpkio.managedpki.com/csr/private-ssl/>

3.2 Startscherm: checklist randvoorwaarden en validatie email

Nadat u een keuze heeft gemaakt verschijnt een vinklijst die aangeeft wat u nodig heeft om de aanvraag volledig te doorlopen². Daarnaast wordt u gevraagd om uw email adres in te vullen.

² Getoonde schermen betreffen een aanvraag van een PKIoverheid Digipoort PRIVATE servercertificaat. Voor een ander type certificaat kan een scherm in detail verschillen. Belangrijke verschillen worden steeds in de tekst benoemd.

KPN Certificaten

Aanvraag PKIoverheid Digipoort PRIVATE servercertificaat



PKIoverheid Digipoort PRIVATE servercertificaat

Welkom bij het aanvraagformulier voor een **PKIoverheid Digipoort PRIVATE servercertificaat** van KPN. Voor meer informatie over PKIoverheid Digipoort PRIVATE servercertificaten kunt u contact opnemen met de [Servicedesk](#).

Mocht het type servercertificaat incorrect zijn, dan verzoeken we u om een nieuwe aanvraag te beginnen vanaf [het overzicht met PKIO servercertificaten](#) en daar het juiste type servercertificaat te selecteren.

Een uitgebreide toelichting en invulinstructie vindt u hier: [KPN PKIoverheid Toelichting aanvraag Servercertificaat](#).

LET OP: gebruik bij een verlenging altijd [MijnCertificaten](#) of de link uit het e-mailbericht dat KPN u toestuurt voorafgaand aan het verlopen van het certificaat. De verloopdatum van de verlenging wordt dan de verloopdatum van het oorspronkelijke certificaat plus 1 jaar voor publieke servercertificaten en plus 3 jaar voor PRIVATE servercertificaten. Bovendien komt u dan automatisch in aanmerking voor de vernieuwingskorting.

Checklist aanvraag PKIoverheid Digipoort PRIVATE servercertificaataanvraag

Om het formulier voor een servercertificaataanvraag met succes te kunnen doorlopen, zijn de volgende zaken noodzakelijk:

- Uw organisatie is reeds als PKIoverheid abonnee bij KPN geregistreerd.
- U bent [bevoegd](#) om een certificaat aan te vragen.
- U beschikt over een Certificate Signing Request (CSR) gebaseerd op een uniek sleutelpaar. U kunt eenvoudig een CSR genereren met de [KPN Certificaataanvraag Assistent](#).

E-mail validatie

Als alle punten uit bovenstaande checklist zijn geregeld, vult u hieronder uw e-mailadres in tezamen met de verificatiecode (captcha) die hieronder als plaatje zichtbaar is. U ontvangt vervolgens een e-mail met daarin een link waarmee u met uw certificaataanvraag kunt beginnen.

E-mailadres*

Verificatie code*



De tekst is niet hoofdlettergevoelig

[Volgende stap >>](#)

Toelichting

Dit formulier bestaat uit de volgende twee delen:

1. Een vinklijst om vooraf te controleren of u alle benodigde gegevens beschikbaar heeft en of aan de randvoorwaarden is voldaan. Deze lijst zorgt ervoor dat u het aanvraagproces succesvol kunt

doorlopen en zo vertraging voorkomt. De eerste twee punten zijn organisatorisch de laatste twee punten zijn meer technisch van aard;

- a. Uw organisatie is als PKloverheid abonnee bij KPN geregistreerd. De bevoegd vertegenwoordiger heeft bij de bevestiging hiervan een PKloverheid abonneenummer ontvangen. Dit nummer heeft u nodig tijdens het invullen van het aanvraagformulier;
 - b. U bent bevoegd om een certificaat aan te vragen. Bevoegd zijn de Bevoegd Vertegenwoordiger of een door hem/haar gevolmachtigde Contactpersoon die bij KPN is geregistreerd als onderdeel van de PKloverheid Abonneeregistratie;
 - c. U beschikt over een Certificate Signing Request (CSR) gebaseerd op een uniek sleutelbaar. Dit bestand bevat de publieke sleutel die KPN in het certificaat zal opnemen. Zie voor uitgebreide toelichting:
<https://certificaat.kpn.com/aanvragen/servercertificaten/csr-genereren/>
 - d. U heeft een domeinnaam om op te laten nemen in het Servercertificaat. Dit kan een eigen domeinnaam zijn van uw organisatie of u bent geautoriseerd om een domeinnaam van een andere organisatie te gebruiken. Het advies is om een eigen domeinnaam te gebruiken. De volgende opties zijn van belang:
 - i. Eigen domein, nieuw. U kunt eenvoudig een nieuwe domeinnaam registreren bij KPN via de volgende site: <https://www.kpn.com/zakelijk/domeinnaam.htm>
 - ii. Eigen domein, bestaand. Bij gebruik van een bestaande domeinnaam is het belangrijk dat de registratiegegevens van dit domein overeenkomen met de gegevens van uw abonneeregistratie. U kunt de registratiegegevens in het zogenaamde WHOIS register opvragen. Voor .nl domeinen kan dit via <https://www.sidn.nl/>. Raadpleeg bij vragen uw internet provider.
 - iii. Domein van KPN t.b.v. SBR. Indien u niet over een domeinnaam beschikt kunt u ook eenvoudig gebruik maken van een domeinnaam van KPN. Dit geldt met name voor het gebruik t.b.v. SBR. Neem hiervoor contact op met de KPN helpdesk:
088 – 661 06 21
 - iv. Domein naam van een derde partij. Het kan zijn dat uw domeinnaam op naam staat van een ICT-dienstverlener of, in het geval van een organisatie van de rijksoverheid, op naam van het Ministerie van Algemene Zaken. In dat geval hebt u toestemming nodig van deze partij om de domeinnaam te mogen gebruiken. Voor een niet overheid bedrijf zal KPN zelf bij deze partij om een domein autorisatie vragen. Voor een overheidsorganisatie zal deze toestemming vastgelegd moeten worden in de vorm van het zogenaamde Domeinautorisatieformulier.
2. Het vaststellen van uw emailadres. Het doel hiervan is om zeker te zijn dat de eigenaar van het email adres zelf de aanvraag doet – danwel minimaal op de hoogte is – en dat het emailadres ook correct is ingevoerd. Naar dit emailadres zal KPN uiteindelijk het aanvraagformulier in PDF formaat sturen, evenals het certificaat na succesvolle verwerking van de aanvraag. Het advies is om hiervoor het zakelijke emailadres van de Contactpersoon te gebruiken.
KPN gebruikt dit emailadres om u te informeren over de voortgang van uw aanvraag.

Invulinstructie

- Verifieer of u alle informatie beschikbaar heeft en vink alle vakjes aan;

- Voer uw emailadres in;
- Type de Verificatiecode over van het plaatje (een CAPTCHA);
- Klik op [Volgende stap >>](#)

Vervolgens verschijnt het onderstaande bevestigingsscherm:

E-mail verzonden

Er is een e-mail verstuurd aan [\[email address\]](#).

Open de link in deze e-mail om het aanvraagproces voor een PKIoverheid servercertificaat te vervolgen.

Deze link blijft geldig gedurende 24 uur (tot 2020-06-10 10:48:12). Daarna dient u opnieuw het proces te starten.

U ontvangt vervolgens een email waarmee KPN uw emailadres verifieert.

Begin uw aanvraag PKIoverheid Digipoort PRIVATE servercertificaat bij KPN

 KPN B.V. Afdeling PKIoverheid-Validatie <no-reply@kpn.com>
To: [email address]

Begin uw aanvraag PKIoverheid Digipoort PRIVATE servercertificaat bij KPN

Klik op de volgende knop/link om uw e-mailadres te bevestigen en de aanvraag te beginnen. Deze link blijft geldig gedurende 24 uur.

[Klik hier om uw e-mailadres te bevestigen en uw aanvraag te starten](#)

Indien de knop/link niet direct werkt vanuit uw e-mail programma dan kunt u de link handmatig kopiëren en plakken in de adresbalk van uw webbrowser. Selecteer de link door met de rechtermuisknop te klikken op bovenstaande knop.

Met dit webformulier vraagt u een PKIoverheid Servercertificaat aan namens een reeds geregistreerde Abonnee van de PKIoverheid Certificatiedienstverlening van KPN. Een uitgebreide toelichting en invulinstructie vindt u hier: [KPN PKIoverheid Toelichting aanvraag Servercertificaat](#).

U heeft gekozen voor het type PKIoverheid Digipoort PRIVATE servercertificaat. Mocht het type servercertificaat incorrect zijn, dan verzoeken we u om een nieuwe servercertificaataanvraag te beginnen vanaf [het overzicht met PKIO certificaten](#) en daar het gewenste type servercertificaat te selecteren.

Dit is een automatisch verzonden e-mail. Gelieve deze e-mail niet beantwoorden. Neemt u bij vragen contact op met de Servicedesk van KPN.

KPN B.V.

- Klik op de link in de email om het aanvraagformulier voor uw servercertificaat te starten.

LET OP:

1. Indien de link niet direct werkt vanuit uw email programma dan kunt u deze handmatig kopiëren en plakken in de adresbalk van uw webbrowser
2. De link is 24 uur geldig. Als de link is verlopen verschijnt onderstaande melding met daaronder het formulier om uw email adres opnieuw in te voeren.

PKIoverheid standaard servercertificaat

De gebruikte link voor de e-mail validatie is niet meer geldig. Start de e-mail validatie opnieuw.

3.3 Scherm 1: Contactpersoon

Na het klikken op de link in de email opent het eerste invoerscherm:

PKIoverheid Digipoort PRIVATE servercertificaat

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Uw e-mailadres: Mocht dit incorrect zijn, dan verzoeken we u om een nieuwe servercertificaataanvraag te beginnen.

Met dit webformulier vraagt u een PKIoverheid Digipoort PRIVATE servercertificaat aan. Mocht het type servercertificaat incorrect zijn, dan verzoeken we u om een nieuwe aanvraag te beginnen vanaf [het overzicht met PKIO certificaten](#) en daar het gewenste type servercertificaat te selecteren.

In dit scherm dient u de gegevens in te vullen die nodig zijn om de certificaataanvraag te koppelen aan een reeds geregistreerde Abonnee. Indien uw organisatie nog geen abonnee is bij KPN voor PKIoverheid Certificatiedienstverlening kunt u dat [hier](#) aanvragen. Na bevestiging van uw abonneeregistratie kunt u de certificaataanvraag uitvoeren.

U dient daarnaast de naam van een Contactpersoon op te geven, die bevoegd is dit formulier te ondertekenen en het formulier ook daadwerkelijk gaat ondertekenen. De Contactpersoon dient als Contactpersoon bij KPN geregistreerd te zijn bij de Abonneeregistratie of is de Bevoegd Vertegenwoordiger die de Abonneeregistratie heeft ondertekend.

Verplichte velden worden aangegeven met (*).

Gegevens Abonnee en Contactpersoon

PKIoverheid Abonneenummer*	<input type="text" value="Uw PKIO Abonneenummer (type P1234567)"/>
Land*	<input type="text" value="Nederland"/>
KvK nummer*	<input type="text" value="KvK nummer van 8 cijfers"/>
Vul het KvK nummer in dat gebruikt is bij de abonneeregistratie van uw organisatie. Indien uw organisatie zich niet kan inschrijven in de KvK omdat u een overheidsorganisatie vertegenwoordigt, neem dan contact op met de ServiceDesk .	
Achternaam contactpersoon*	<input type="text" value="Achternaam conform Identiteitsbewijs"/>
LET OP: U dient de Achternaam van de Contactpersoon in te vullen zoals is opgenomen op uw Identiteitsbewijs. Dit voorkomt vertraging in de verwerking van uw aanvraag. KPN zal de opgegeven naam vergelijken met de naam op de kopie Identiteitsbewijs die tijdens de abonneeregistratie is vastgelegd van de Contactpersoon.	
Geboortedatum*	<input type="text" value="Bijv. 31-12-1971"/>
E-mailadres	<input type="text" value="naam.vertegenwoordiger@kpn.nl"/>

[Volgende stap >>](#)

Invulinstructie en toelichting scherm **1. Contactpersoon**

Dit scherm heeft als doel om de gegevens van de Abonnee vast te leggen waarvoor het Servercertificaat wordt aangevraagd en van de Contactpersoon die de aanvraag doet.

- Voer in uw PKIoverheid Abonneenummer dat u heeft ontvangen bij de bevestiging van uw abonneeregistratie. Het nummer begint met een 'P' gevolgd door 7 cijfers.
- Voer uw KvK-nummer in indien dat is gebruikt in de Abonneeregistratie.

- Bij gebruik van het KvK-nummer haalt KPN automatisch de Organisatiennaam en overige publieke KvK gegevens op. Als dat succesvol verloopt ziet u de handelsnaam zoals hieronder is geïllustreerd met het KvK nummer van KPN.



KvK nummer*

Vul het KvK nummer in dat gebruikt is bij de abonneeregistratie van uw organisatie. Indien uw organisatie zich niet kan inschrijven in de KvK omdat u een overheidsorganisatie vertegenwoordigt, neem dan contact op met de [ServiceDesk](#).

Organisatiennaam volgens KvK

en verschijnt de volgende toelichting:



Uw handelsnaam en adresgegevens zijn online opgevraagd bij de KvK op basis van het ingevoerde KvK nummer.

Indien deze gegevens niet actueel of onjuist zijn dan dient u eerst uw KvK registratie te actualiseren. Indien u andere gegevens wenst te gebruiken dan opgehaald uit de KvK —bijvoorbeeld vanwege meerdere geregistreerde handelsnamen of vestigingsadressen— dan kunt u de gegevens wijzigen.

- Vul de Achternaam en de Geboortedatum in van de Contactpersoon die de certificaataanvraag doet zoals is opgenomen op het ID bewijs.

Het emailadres is het gevalideerde emailadres dat in het Startscherm is opgegeven. Mocht dit incorrect zijn, dan verzoeken we u om een nieuwe servercertificaataanvraag te beginnen.

- Klik op [Volgende stap >>](#)

3.4 Scherm 2: Certificaatbeheerder

In dit scherm geeft u aan wie de Certificaatbeheerder is voor deze certificaataanvraag.

PKIoverheid Digipoort PRIVATE servercertificaat



1. Contactpersoon 2. Certificaatbeheerder 3. Certificaat 4. Controle 5. Voorwaarden 6. Afronding

In dit scherm kunt u aangeven wie als Certificaatbeheerder op zal treden voor deze certificaataanvraag. De Certificaatbeheerder zal namens de Abonneeorganisatie dit Servercertificaat in ontvangst (gaan) nemen en beheren.

BELANGRIJK: u kunt kiezen uit twee opties:

Kies 1 als u een nieuwe Certificaatbeheerder wilt aanmelden die niet eerder is geregistreerd bij KPN. In dit geval zal KPN -voorafgaande aan de uitgifte van het certificaat- de identiteit van de Certificaatbeheerder (laten) verifiëren en vergelijken met de aangeleverde persoonsgegevens.

Kies 2 als de Certificaatbeheerder al eerder door KPN is geïdentificeerd voor een eerdere certificaataanvraag.



Certificaatbeheerder

De certificaatbeheerder is*

[Volgende stap >>](#)

U kunt kiezen uit twee opties:

1. *volledig nieuw*
Kies deze optie als u een nieuwe Certificaatbeheerder wilt aanmelden die niet eerder is geregistreerd en geïdentificeerd door KPN.
2. *reeds geïdentificeerd*
Kies deze optie als de gewenste certificaatbeheerder al bij KPN bekend is, bijvoorbeeld bij een volgende certificaataanvraag voor dezelfde organisatie. Daarnaast kan een persoon Certificaatbeheerder zijn voor meerdere Abonnees.

Optie 1 Certificaatbeheerder is volledig nieuw

Certificaatbeheerder

De certificaatbeheerder is*

Nieuwe certificaatbeheerder

Volledige voornaam*

Tussenvoegsel

Achternaam*

U dient bij Volledige voornaam, Tussenvoegsel en Achternaam de volledige naam van de Certificaatbeheerder in te vullen zoals is opgenomen op diens **identiteitsbewijs**. Dit zal tijdens de identificatie van de Certificaatbeheerder worden gecontroleerd.

(Mobiele) telefoon*

Vul bij voorkeur het mobiele telefoonnummer van de Certificaatbeheerder in. Dan kan KPN de Certificaatbeheerder per SMS in detail op de hoogte houden van de planning van de persoonlijke identificatie.

Geboortedatum*

Geboorteplaats*

LET OP: u dient de geboorteplaats exact over te nemen zoals op het identiteitsbewijs van de Certificaatbeheerder is opgenomen. Bij identificatie van de Certificaatbeheerder moet deze hetzelfde identiteitsbewijs tonen. Dit is noodzakelijk voor een betrouwbare identiteitsvaststelling.

E-mail Certificaatbeheerder*

Bij uitgifte wordt het certificaat naar dit e-mailadres verzonden met een CC naar de Contactpersoon die de aanvraag uitvoert.

Adresgegevens nieuwe certificaatbeheerder

Organisatiernaam

U hoeft de organisatiernaam alleen in te vullen indien de Certificaatbeheerder geen onderdeel uitmaakt van de Abonneeorganisatie

Land*

Postcode*

Plaats*

Straatnaam*

Huisnummer*

Huisnummer toevoeging

De brief met daarpin de Inrekkode van het certificaat wordt naar het opgegeven adres van de certificaatbeheerder gestuurd.

[Volgende stap >>](#)

Invulinstructie en toelichting **2. Certificaatbeheerder** (optie 1: nieuwe certificaatbeheerder)

Indien u kiest voor een nieuwe Certificaatbeheerder dan dient u van deze persoon de persoonsgegevens op te geven.

- Vul de persoonsgegevens in van de beoogde Certificaatbeheerder.
 - Naam;
 - Telefoonnummer;
 - Geboortedatum en -plaats;
 - Emailadres.

- Indien van toepassing: vul de organisatiernaam in.
Het is niet noodzakelijk dat de Certificaatbeheerder werkt bij de organisatie van de Abonnee. Het kan bijvoorbeeld ook een medewerker zijn van een ICT-dienstverlener die diensten levert aan uw organisatie. In dat geval dient u hier de naam van die organisatie (ICT-dienstverlener) op te geven.

- Indien van toepassing: vul de adresgegevens in van de certificaatbeheerder.
Als adresgegevens van de Certificaatbeheerder stelt het webformulier het adres voor dat in het handelsregister van de KvK is opgehaald. Als de Certificaatbeheerder werkzaam is op een andere vestiging of voor een andere organisatie kunt u het adres hier aanpassen.

- Klik op [Volgende stap >>](#)

Optie 2: Een reeds geïdentificeerde Certificaatbeheerder

Certificaatbeheerder

De certificaatbeheerder is*

Reeds geregistreerde certificaatbeheerder

Achternaam*

E-mail
Certificaatbeheerder*

Bij uitgifte wordt het certificaat naar dit e-mailadres verzonden met een CC naar de Contactpersoon die de aanvraag uitvoert.

Registratienummer
certificaatbeheerder*

U dient hier het Registratienummer van het type CB1234567 te gebruiken. Alle geregistreerde Certificaatbeheerders hebben dit nummer ontvangen na Identiteitsvaststelling bij de eerste registratie als Certificaatbeheerder.

[Volgende stap >>](#)

Invulinstructie en toelichting **2. Certificaatbeheerder** (optie 2: bestaande certificaatbeheerder)

Als de Certificaatbeheerder al voor een andere certificaataanvraag –voor uw organisatie of voor een andere abonnee- is geïdentificeerd dan kiest u voor optie 2. De Certificaatbeheerder heeft na zijn identificatie van KPN een registratienummer ontvangen. Dit registratienummer dient u met enkele andere identificerende gegevens van de Certificaatbeheerder op te geven.

- Vul de achternaam van de Certificaatbeheerder in.
- Vul het emailadres van de Certificaatbeheerder in.
- In dit geval moet u ook het certificaatbeheerdersnummer ('CB' gevolgd door 7 cijfers) hebben van een certificaatbeheerder die reeds eerder bij KPN is geregistreerd en van wie de identiteit is vastgesteld.
- Klik op [Volgende stap >>](#)

3.5 Scherm 3: Certificaat

In dit scherm vult u de gegevens in die daadwerkelijk in het certificaat komen te staan.

PKIoverheid Digipoort PRIVATE servercertificaat

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Type servercertificaat

U vraagt met dit formulier een PKIoverheid Digipoort PRIVATE servercertificaat aan.

PKIoverheid Digipoort PRIVATE servercertificaten zijn bedoeld voor koppeling van uw systeem met Digipoort. KPN bepaalt automatisch de naam van de service, deze is niet te wijzigen. Hierdoor is er geen controle van domeinnaam nodig.

Het Organisatie-identificatienummer (OIN) of Handelsregisternummer (HRN) van uw organisatie wordt opgenomen in het certificaat om de communicatie via Digikoppeling mogelijk te maken. Voorbeelden zijn: communicatie met Diginetwerk, Digipoort, SBR, OLO, LV WOZ, WSNP, GBA-V, BAG, GWH, WKPB e.a. Het stamcertificaat is niet opgenomen in browsers of operating systemen.

Mocht het type servercertificaat incorrect zijn, dan verzoeken we u om een nieuwe aanvraag te beginnen vanaf [het overzicht met PKIO servercertificaten](#) en daar het gewenste type servercertificaat te selecteren.

De aanvraag betreft een* PKIoverheid Digipoort PRIVATE servercertificaat

Geldigheidsduur* 3 jaar

Invulinstructie en toelichting **3. Certificaat** 1^e gedeelte: [Type servercertificaat](#)

Het eerste blok geeft als eerste het type servercertificaat u aanvraagt weer. Dit is alleen te wijzigen door via de website <https://certificaat.kpn.com/aanvragen/servercertificaten/> een nieuwe aanvraag te starten of vanaf het Keuzescherf voor het type servercertificaat (zie paragraaf 3.1).

Generatie en geldigheidsduur

Een PKIoverheid Digipoort PRIVATE servercertificaat wordt uitgegeven worden onder de G1 Private Root en is 3 jaar geldig. Generatie en geldigheidsduur verschillen per type servercertificaat. Op dit moment zijn de volgende varianten leverbaar:

Type servercertificaat	Generatie CA (PKIoverheid Hiërarchie)	Geldigheidsduur
Standaard SSL	Staat der Nederlanden EV Root CA	1 jaar
Digipoort private	Staat der Nederlanden Private Root CA - G1	3 jaar
Private SSL	Staat der Nederlanden Private Root CA - G1	3 jaar

Afhankelijk van het certificaattpe bestaan er kleine verschillen in de invoervelden van dit scherm en de volgende schermen.

PKI-overheid Digipoort PRIVATE servercertificaat

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Gegevens voor Servercertificaat

Organisatiernaam [O]*

KPN stelt hier de statutaire naam voor van uw organisatie zoals geregistreerd is in het handelsregister van de KvK. U kunt in een certificaat ook gebruik maken van een bij de KvK geregistreerde handelsnaam. In dat geval dient u zelf het voorstel aan te passen.

Organisatieonderdeel [OU]

Land [C]*

Plaats [L]*

Provincie [U]*

KPN stelt hier de plaats en provincie voor van het vestigingsadres van de hoofdvestiging zoals geregistreerd is in het handelsregister van de KvK. U kunt ook gebruik maken van een plaats en provincie die in de KvK geregistreerd is als adres van een nevestiging. In dat geval dient u zelf het voorstel aan te passen.

Naam van de service [CN]*

U dient hier een volledige domeinnaam (FQDN) op te nemen, zoals www.mijn-bedrijf.nl. IP-adressen, spaties, wildcards (*) en onvolledige (bijv. alleen een hostname), interne domeinnamen (bijv. eindigend op .local) of Internationalized Domain Names (IDN) zijn niet toegestaan. Een uitgebreide toelichting over FQDN's vindt u [hier](#).

Subject Serienummer [DN of HRN]*

Om gebruik te maken van de digitale diensten van de overheid, zoals SBR, digipoort en digikoppeling, dient u hier een waarde te kiezen. In de meeste gevallen is de door KPN voorgestelde waarde hier het beste.

Als u een overheidsorganisatie vertegenwoordigt en het Organisatieidentificatienummer (OIN) van uw organisatie is bij Logius opgenomen in het Digikoppeling Serviceregister dan kunt u het beste dit nummer gebruiken. Als uw OIN niet is opgenomen in de keuzelijst dan dient u dit zelf handmatig in te voeren. U kunt uw OIN opzoeken in het [OIN Register](#).

Als u een privaatrechtelijke organisatie vertegenwoordigt, dan adviseert KPN om het voorgestelde Handelsregisternummer (HRN) te gebruiken. KPN stelt dit nummer samen op basis van uw KvK nummer en het voldoet daarmee aan de regels van digipoort. Het opnemen van het HRN zal de correcte werking van een certificaat nooit nadelig beïnvloeden, maar omgekeerd zijn er wel overheids toepassingen die een HRN vereisen.

Neem bij twijfel contact op met de [ServiceDesk](#).

Invulinstructie en toelichting **3. Certificaat** 2^e gedeelte: Gegevens voor Servercertificaat

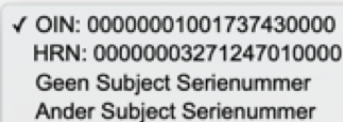
Het tweede blok bevat de identificerende gegevens van de 'service' en de Abonnee waarvoor het Servercertificaat is uitgegeven. Deze gegevens worden door KPN in het certificaat opgenomen. Indien u een KvK nummer heeft opgegeven in het scherm '1: Contactpersoon' zijn vanuit de publieke KvK gegevens al enkele gegevens opgenomen (Organisatiernaam, Plaats en Provincie).

- Controleer de organisatiernaam. Indien van toepassing dient u zelf:
 - De naam in te korten tot maximaal 64 karakters;
 - Eventuele speciale karakters te verwijderen.
- Vul eventueel een afdelingsnaam in.

- Vul de volledige domeinnaam in, de Fully Qualified Domain Name (FQDN). Een uitgebreide toelichting over FQDN vindt u hier: <https://certificaat.kpn.com/aanvragen/servercertificaten/fqdn-naam-van-de-service/>. Kort gezegd is dit de naam die u in een browser intypt om het systeem te benaderen, bijvoorbeeld 'certificaat.kpn.com' of 'www.logius.nl'
- Het veld Subject Serienummer wordt gebruikt voor communicatie met overheidsdiensten.

KPN adviseert om hier altijd uw Organisatie-Identificatienummer (OIN) of Handelsregisternummer (HRN) te gebruiken. Een OIN wordt uitgegeven door Logius en is beschikbaar voor organisaties met een publieke taak. Uw OIN nummer is te vinden via <https://portaal.digikoppeling.nl/registers/>. Een HRN geldt voor bedrijven en privaatrechtelijke instellingen zonder publieke taak en wordt afgeleid van het KvK nummer van de betreffende organisatie.

De geadviseerde waarde wordt voor-ingevuld en wordt gebruikt als u niets wijzigt. Het keuzeschermbiedt u verder de volgende mogelijkheden³:



✓ OIN: 00000001001737430000
HRN: 00000003271247010000
Geen Subject Serienummer
Ander Subject Serienummer

Als u kiest voor 'Ander Subject Serienummer' dan krijgt u een leeg veld waarin u een 20-cijferig nummer kunt invoeren. KPN zal een ingevoerd nummer altijd controleren.

LET OP: voor een standaard SSL servercertificaat is dit invoerveld niet beschikbaar. Dit type servercertificaat is dan ook niet geschikt voor communicatie met SBR / digipoort / digikoppeling.

Neem bij twijfel contact op met de Servicedesk: zie <https://certificaat.kpn.com/support/> voor contactgegevens.

³ Indien er geen OIN gevonden wordt voor uw organisatie op basis van het opgegeven KvK nummer dan zal dit uiteraard niet in de keuzelijst verschijnen. In dat geval is de bovenste (default) waarde in de lijst het HRN.

PKIoverheid Digipoort PRIVATE servercertificaat

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Certificate Signing Request

Het Certificate Signing Request (CSR) bevat de sleutel die in het certificaat wordt opgenomen. Het CSR dient bij voorkeur gemaakt te worden op de server waarop uiteindelijk het certificaat geïnstalleerd zal worden.

KPN stelt haar klanten de KPN Certificaataanvraag Assistent beschikbaar.
Met deze tool kunt u eenvoudig een CSR aanmaken en later het certificaat importeren. [Klik hier](#) voor meer informatie en het downloaden van de tool.

LET OP: u dient voor ieder servercertificaat een andere CSR aan te leveren dat gebaseerd is op een uniek sleutelpaar. Dit sleutelpaar dient uitsluitend gebruikt te worden voor de betreffende service!
[Zie hier](#) voor uitgebreide toelichting.

Certificate Signing Request*

Plaak hier uw CSR. LET OP! Gebruik hiervoor **NIET** tekstverwerker zoals Microsoft Word vanuit de KPN Certificaataanvraag Assistent. Kunt u de CSR direct kopiëren via het kladblok, past u de CSR op een ander systeem of op andere wijze aangeemaakt of aangeleverd gekregen dan kunt u het bijvoorbeeld kopiëren vanuit Windows Notepad (Kladblok).

[Volgende stap >>](#)

Invulinstructie en toelichting

3. Certificaat

3^e gedeelte: Certificate Signing Request

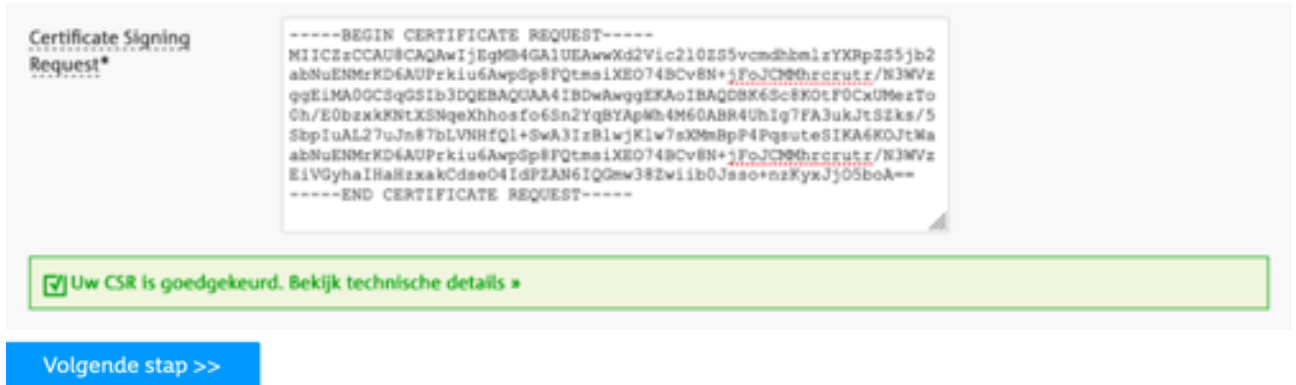
In het derde blok vult u de publieke cryptografische sleutel in die in het Servercertificaat wordt opgenomen. Het Certificate Signing Request (CSR) bevat het publieke gedeelte van het sleutelpaar dat bij voorkeur op de server is gegenereerd waarop uiteindelijk het certificaat komt te staan. Om dit proces zo goed mogelijk te ondersteunen stelt KPN software ter beschikking:

<https://certificaat.kpn.com/certificaataanvraag-assistent/>⁴

- Plak het CSR in het formulier. **LET OP: GEBRUIK HIERVOOR NOOIT EEN PROGRAMMA ALS MICROSOFT WORD MAAR GEBRUIK HET KLADBLOK (NOTEPAD).**
- Er vindt een controle plaats of het CSR technisch voldoet.

⁴ De certificaat aanvraag assistent werkt uitsluitend op Microsoft windows systemen. Instructies voor het aanmaken van een CSR op andere systemen vindt u op de website: <https://certificaat.kpn.com/aanvragen/servercertificaten/csr-genereren/>.

Als het CSR technisch correct is verschijnt de volgende melding:



Bij fouten in het CSR wordt dit direct terug gemeld, inclusief de reden waarop het CSR is afgekeurd. Bij gebruik van de *KPN SBR Certificaataanvraag assistent* zullen de juiste technische randvoorwaarden aan de CSR automatisch in orde zijn:



Extra naam in een PKlooverheid server certificaat (SAN / Subject Alternative Name)

U kunt tegen meerprijs maximaal 10 extra namen op laten nemen in het servercertificaat door deze aan het CSR-bestand toe te voegen⁵. Eventuele additionele namen zijn zichtbaar als u de technische details van de CSR bekijkt en staan ook in het controle scherm en op het PDF formulier.

LET OP: indien in de CSR een SAN is opgenomen die gelijk is aan de ingevulde Naam van de service, dan is deze SAN wel zichtbaar in het controlescherm. Daarbij is expliciet aangegeven dat deze SAN niet als 'additioneel' geldt en dus ook niet tot extra kosten leidt.

⁵ Het toevoegen van extra namen is niet beschikbaar als u gebruik maakt van de certificaat aanvraag assistent. Uw systeembeheerder is in staat om een CSR aan te maken met daarin de extra namen.

In de PDF worden alleen de additionele SAN's getoond die tegen meerprijs in het servercertificaat worden opgenomen.

3.6 Scherm 4: Controle

In dit scherm krijgt u een overzicht van alle ingevoerde gegevens ter controle en kunt u indien nodig nog gegevens wijzigen.

PKIoverheid Digipoort PRIVATE servercertificaat

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Hieronder dient u te controleren of de ingevoerde gegevens volledig en juist zijn.

Gegevens Abonnee en Contactpersoon

PKIoverheid Abonneenummer	p1234560
KvK nummer	27124701
Achternaam contactpersoon	Fanwerck
Geboortedatum	12-08-1970
E-mailadres	fanwerck@kpn.com

Wijzig

Certificaatbeheerder

De certificaatbeheerder is	1. volledig nieuw
----------------------------	-------------------

Wijzig

Nieuwe certificaatbeheerder

Volledige voornaam	Andrea Philomenia
Tussenvoegsel	van het
Achternaam	Certificaatbeheerteam
[Mobiele] telefoon	+31 6 87654321
Geboortedatum	08-08-1988
Geboorteplaats	Noordenstrandsluis
E-mail Certificaatbeheerder	andrea@beheer.net

Wijzig

Adresgegevens nieuwe certificaatbeheerder

Organisatiernaam	-
Land	Nederland
Postcode	3072 AP
Plaats	Rotterdam
Straatnaam	Wilhelminakade
Huisnummer	123
Huisnummer toevoeging	-

[Wijzig](#)

Type servercertificaat

De aanvraag betreft een	PKIoverheid Digipoort PRIVATE servercertificaat
Geldigheidsduur	3 jaar

[Wijzig](#)

Gegevens voor Servercertificaat

BELANGRIJK: de hieronder getoonde gegevens worden opgenomen in uw Servercertificaat. Controleer deze gegevens zorgvuldig! Eventuele typefouten kunnen in sommige gevallen het certificaat technisch onbruikbaar maken. De getoonde waarden 'overschrijven' de gegevens die daadwerkelijk in het CSR bestand zijn opgenomen.

Naam van de Service (CN)	digipoort-00000003271247010000
Subject Serienummer	00000003271247010000
Organisatiernaam (O)	KPN B.V.
Afdeling (OU)	Corporate Finance
Plaats (L)	Rotterdam
Provincie (S)	Zuid-Holland
Land (C)	Nederland

De SHA256 fingerprint van uw CSR is: 622d5f26b66aa3181db70247a3c46bbae49a1266620958bb215124d6ae834943

[Wijzig](#)[Volgende stap >>](#)

Invulinstructie en toelichting **4. Controle**

- Controleer uw gegevens.
- Klik op 'Wijzig' om gegevens in een bepaalde rubriek aan te passen.
- Als alle gegevens kloppen: klik op [Volgende stap >>](#)

3.7 Scherm 5: Voorwaarden

Het laatste invoerscherm vraagt expliciet om een akkoord op de voorwaarden die van toepassing zijn:

PKIoverheid Digipoort PRIVATE servercertificaat

1. Contactpersoon**2. Certificaatbeheerder****3. Certificaat****4. Controle****5. Voorwaarden**

6. Afronding

Om de aanvraag van uw PKIoverheid Servercertificaat af te ronden, dient u de volgende voorwaarden te accepteren:

Voorwaarden

- Ik ben akkoord met de Algemene Leveringsvoorwaarden (*) en de KPN Bijzondere Voorwaarden PKIoverheid Certificaten.
() De Algemene Leveringsvoorwaarden vindt u door op de bovenstaande link te klikken. Vervolgens selecteert u de categorie Zakelijk, het product ICT en daarna het document Algemene Leveringsvoorwaarden.*
- De opgegeven Certificaatbeheerder is geïnformeerd, is bevoegd en ter zake kundig om namens de Abonnee Servercertificaten te installeren, te beheren en in te trekken.
- Ik ben akkoord met de tarieven.
- Het sleutelmateriaal van het Servercertificaat is gegenereerd en wordt bewaard in een Veilige Omgeving.

- Ik ga akkoord met alle bovenstaande voorwaarden en heb namens de Abonnee alle gegevens volledig, juist en naar waarheid ingevuld.

PKIoverheid Digipoort PRIVATE servercertificaat

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Toepassing en support

Certificaat bestemd voor*

Om u optimaal van dienst te kunnen zijn, dient u hier aan te geven waarvoor u het servercertificaat gaat gebruiken. De toepassing "TV SSL beveiliging webserver" is hier niet selecteerbaar omdat u met dit formulier alleen een PKIoverheid standaard servercertificaat kan aanvragen. Indien u voor genoemde toepassing een servercertificaat nodig heeft dan dient u een nieuwe aanvraag te starten vanaf [het overzicht met PKI certificaten](#) en daar het type PKIoverheid Extended Validation SSL te selecteren.

Pakketkeuze* Standaard pakket Premium pakket

Een toelichting van de verschillende supportvormen vindt u [hier](#).

Type aanvraag Initieel

Dit betreft een nieuwe aanvraag. Indien u aanspraak wilt maken op de [Vernieuwingsprijs](#) of de Vervangingsvoorwaarden dan dient u te verlenen via MijnCertificaten of gebruik te maken van de herinnerings e-mail met daarin een link waarmee u de reguliere verlenging kunt starten.

Facturatie

PO / Referentienummer

LET OP: Indien er een PO nummer (of een ander referentienummer) op de factuur opgenomen moet worden, dient u dat nummer hier in te voeren. Indien opgegeven zal dit nummer op de factuur komen voor eenvoudige toetsing van de factuur binnen uw financiële administratie. **Achteraf een PO nummer toevoegen is niet mogelijk.** Indien u niets invoert, zal er een factuur zonder PO of referentienummer verstuurd worden. Het ontbreken van een PO of referentienummer ontslaat u niet van de betalingsverplichting van de factuur binnen de daarvoor geldende termijn. Facturatie zal plaatsvinden op basis van de betalingsgegevens die zijn vastgelegd in de abonneeregistratie.

[Verzend Aanvraag](#)

De gegevens bestaan uit drie blokken:

1. Voorwaarden;
2. Toepassing en support;
3. Facturatie.

Voorwaarden

U dient akkoord te gaan met de volgende voorwaarden om de aanvraag af te kunnen ronden:

- Akkoord met de *Algemene Leveringsvoorwaarden*⁶ en de *KPN Bijzondere Voorwaarden PKI Overheid Certificaten*⁷. Deze voorwaarden gelden zowel voor Abonnees, Contactpersonen, Certificaathouders, Certificaatbeheerders en Vertrouwende Partijen. Hierdoor is het voor alle betrokkenen duidelijk wat de rechten en plichten zijn;
- Verklaring dat de opgegeven Certificaatbeheerder geïnformeerd, bevoegd en ter zake kundig is om namens de Abonnee Servercertificaten te installeren, te beheren en in te trekken;

⁶ Zie: <https://www.kpn.com/algemeen/alle-voorwaarden.htm> Vervolgens selecteert u de categorie Zakelijk, het product ICT en daarna het document Algemene Leveringsvoorwaarden.

⁷ Zie https://certificaat.kpn.com/files/voorwaarden/BIJZ_VW_PKI_OVERHEID_CERTIFICATEN.pdf

- Bij de aanvraag gaat u akkoord met de *kosten* die KPN in rekening zal brengen voor een PKIO Servercertificaat⁸;
- U dient het sleutelpaar van het Servercertificaat te genereren en gebruiken in een Veilige Omgeving;
- U verklaart dat de domeinnaam of valt onder de directe verantwoordelijkheid van de Abonnee of dat u geautoriseerd bent om een domeinnaam van een andere organisatie te gebruiken.

Als u een domeinnaam van een andere organisatie gebruikt, dient de eigenaar van het domein uw organisatie te autoriseren tot het aanvragen van een certificaat voor het betreffende domein. KPN zal daartoe de domein eigenaar om deze autorisatie vragen. U dient daarom rekening te houden met extra doorlooptijd van uw certificaataanvraag.

- Vink het vakje aan als alle gegevens volledig, juist en naar waarheid zijn ingevuld.

Toepassing en support

- Kies de toepassing waarvoor u het servercertificaat gaat gebruiken. Bij EV SSL / QWAC is deze waarde niet aan te passen en staat deze waarde op 'EV SSL / QWAC beveiliging webserver'.

Met deze informatie kan KPN u optimaal van dienst zijn mocht u nog vragen hebben over het servercertificaat.


Bij sommige toepassingen kunt u kiezen voor premium support. Door te kiezen voor premium support garandeert KPN dat het certificaat in uw omgeving correct wordt geïnstalleerd. Een nadere toelichting van de verschillende supportvormen vindt u op:

<https://certificaat.kpn.com/support/faq/veelgestelde-vragen-sbr/>

- Vink de keuze aan van de gewenste support vorm.
- Het type aanvraag -initieel, vroegtijdige vervanging of reguliere vernieuwing- wordt automatisch in het formulier vastgesteld en is niet te wijzigen. Een nieuwe aanvraag is altijd 'initieel'. Als u gebruikt maakt van een link voor vernieuwing, wordt de waarde op 'reguliere vernieuwing' gezet. Zie ook par. 5.3.

Facturatie

De referentie die u hier opgeeft komt als terug op de factuur die u van KPN ontvangt. U kunt dit gebruiken om de factuur te relateren aan uw eigen administratie.

- Vul optioneel een PO/referentienummer in voor de factuur.
- Klik op 

BELANGRIJK: hoewel KPN na het verzenden van de aanvraag de digitale gegevens heeft, dient de Contactpersoon die op het PDF formulier staat vermeld de afgedrukte aanvraag te ondertekenen en dient het formulier voorzien van eventuele bijlage per post opgestuurd te worden. Dit is verder uitgewerkt in Hoofdstuk 3.8.

⁸ Zie <https://certificaat.kpn.com/pkioverheidcertificaten/tarieven/>

3.8 Afronding

Als de aanvraag digitaal met succes is verzonden, verschijnt het volgende scherm:


PKIoverheid Digipoort PRIVATE servercertificaat

Aanvraag verzonden

Betreft aanvraag PKIoverheid Digipoort PRIVATE servercertificaat

Referentie: 520200827730733333

Uw aanvraag is met succes verzonden. De gegevens zijn in een PDF formulier geplaatst dat u hieronder kunt downloaden ter ondertekening. Dit formulier ontvangt u ook als bijlage bij een e-mailbericht.

 [Download PDF aanvraagformulier](#)

BELANGRIJKE VERVOLGSTAP: ONDERTEKENEN EN INDIENEN VAN DE AANVRAAG

Om de aanvraag van het PKIoverheid Digipoort PRIVATE servercertificaat daadwerkelijk in gang te zetten, kunt u kiezen uit 2 varianten:

OPTIE 1: AANVRAAG ELEKTRONISCH ONDERTEKENEN EN INDIENEN
Indien u als contactpersoon beschikt over een rechtsgeldige elektronische handtekening kunt u de aanvraag elektronisch ondertekenen en per e-mail indienen. De werkwijze is als volgt:

- De contactpersoon die op het formulier staat, dient het formulier elektronisch te ondertekenen. Dit dient te gebeuren met [een PKIoverheid persoonlijk certificaat](#) dat op naam van de contactpersoon staat. Het eenvoudigst is om de ondertekening uit te voeren in de vorm van een elektronisch ondertekende e-mail met het PDF aanvraagformulier als bijlage. U ontvangt als contactpersoon per e-mail het PDF formulier. Deze e-mail kunt u doorsturen naar pkivalidation@kpn.com en daarbij dient u deze e-mail elektronisch te ondertekenen. Dit kan standaard met gangbare e-mailprogramma's zoals Microsoft Outlook of Mozilla Thunderbird.

OPTIE 2: AANVRAAG OP PAPIER PER POST INDIENEN
Kies voor deze optie indien u niet de gelegenheid heeft om de aanvraag elektronisch te ondertekenen en in te dienen. De werkwijze is als volgt:

- **Printen**
Print het PDF formulier op 1 blanco A4.
- **Ondertekenen**
De contactpersoon die op het formulier staat, dient het formulier te ondertekenen.
- **Versturen**
Stuur het aanvraagformulier op naar:

KPN B.V.
Ter attentie van PKIoverheid-Validatie
Postbus 9105
7300 HN APELDOORN

Om de aanvraag van het PKIoverheid standaard servercertificaat daadwerkelijk in gang te zetten, kunt u kiezen uit 2 varianten. Die zijn toegelicht in de volgende paragrafen.

3.8.1 Optie 1: aanvraag elektronisch ondertekenen en indienen

Indien u als contactpersoon beschikt over een rechtsgeldige elektronische handtekening kunt u de aanvraag elektronisch ondertekenen en per email indienen. De werkwijze is als volgt:

PDF aanvraagformulier elektronisch ondertekenen en toezenden

De contactpersoon die op het formulier staat, dient het formulier elektronisch te ondertekenen. Dit dient te gebeuren met een persoonsgebonden PKloverheid certificaat dat op naam van de contactpersoon staat.

Het eenvoudigst is om de ondertekening uit te voeren in de vorm van een elektronisch ondertekende email met het PDF aanvraagformulier als bijlage. U ontvangt als contactpersoon per email het PDF formulier. Deze email kunt u doorsturen naar pkvalidation@kpn.com en daarbij dient u deze email elektronisch te ondertekenen. Dit kan standaard met gangbare email programma's zoals Microsoft Outlook of Mozilla Thunderbird.

3.8.2 Optie 2: aanvraag op papier per post indienen

Kies voor deze optie indien u niet de gelegenheid heeft om de aanvraag elektronisch te ondertekenen en in te dienen. De afronding van uw aanvraag bestaat dan uit de volgende stappen:

Printen

Het printen van het PDF formulier op blanco A4 papier;

Ondertekenen

De Contactpersoon van de Abonnee dient de aanvraag met de hand te ondertekenen.

Opsturen

Het formulier (en bijlage) dient u op te sturen naar:

KPN Corporate Market B.V.
t.a.v. Afdeling Validatie
Postbus 9105
7300HN APELDOORN

4 Servercertificaataanvraag via het KPN Self Service Portaal

Het aanvragen van servercertificaten kan eenvoudig vanuit het KPN PKIoverheid Self Service Portaal (SSP). De aanvraag verloopt in principe hetzelfde als bij een aanvraag zonder SSP, echter zijn de meeste gegevens al voor u ingevuld in de verschillende webformulieren en kunt u de aanvraag na de controle direct elektronisch indienen. Dit maakt het aanvragen nog gemakkelijker voor u en voorkomt bovendien fouten en daarmee ongewenste vertraging.

In dit hoofdstuk wordt de aanvraag van een servercertificaat via het SSP verder toegelicht.

4.1 Inloggen in het Self Service Portaal / MijnCertificaten

Het KPN PKIoverheid Self Service Portaal (SSP) is ook bekend onder de naam MijnCertificaten. Om in te loggen in het SSP heeft u een persoonsgebonden certificaat (via Mobiel, Pas of USB-stick) nodig en uw organisatie dient (eenmalig) aangemeld te zijn voor het gebruik van MijnCertificaten. Het SSP is bereikbaar via de volgende URL: <https://kpnpkio.managedpki.com/ssp/>.

Het volgende scherm wordt getoond:

Welkom bij MijnCertificaten

U bent niet ingelogd.

Er is geen geldige Pas/USB-stick gevonden of u bent niet ingelogd met de Ubiqu Authenticate App (Foutcode 001). Indien u met een Pas/USB-stick wilt inloggen, controleer dan of de juiste software hiervoor is geïnstalleerd, de Pas in de kaartlezer of de USB-stick in uw PC zit, en u de juiste pincode heeft opgegeven.

Meer informatie over aanmelding voor gebruik van MijnCertificaten vindt u bij de [Veelgestelde vragen MijnCertificaten](#).

Indien u desondanks problemen met inloggen ondervindt, kunt u contact opnemen met de [ServiceDesk](#).

Inloggen met Pas/USB-stick

Inloggen met Ubiqu Authenticate App

Kies de inlogmethode die voor u van toepassing is en log in met uw persoonlijke certificaat. Het startscherm van het SSP ziet er als volgt uit:



Welkom bij MijnCertificaten

MijnCertificaten biedt u een overzicht van uw Servercertificaten, Passen, Mobilele certificaten en Organisatiegegevens. U kunt bestaande certificaten verlengen of nieuwe certificaten aanvragen. Uw aanvraag verloopt volledig digitaal.

Bij het afronden van een aanvraagformulier plaatst u direct een bestelling bij KPN.

MijnCertificaten biedt u de volgende mogelijkheden:

- Onder het menu **Servercertificaten** vindt u alle typen Servercertificaten van uw organisatie en kunt u Servercertificaten verlengen, intrekken of een nieuw Servercertificaat aanvragen.
- Onder het menu **Passen** vindt u de Persoonlijke en/of Groeps-certificaten van uw organisatie die zijn uitgegeven op een Pas, USB-stick of als Mobilele certificaten. U kunt Persoonlijke en/of Groeps-certificaten verlengen, intrekken of nieuwe certificaten aanvragen.
- Onder het menu **Organisatiegegevens** vindt u de Bedrijfsgegevens van uw organisatie, Facturatie gegevens en de gerechtigde Bevoegd Verleggenwoordigden, Contactpersonen en Certificaatbeheerders van uw organisatie. Via wijzigingsformulieren kunt u volledig digitaal wijzigingverzoeken indienen.

Een uitgebreide toelichting bij het gebruik van MijnCertificaten vindt u hier: [KPN PKI-overheid Toelichting MijnCertificaten](#)

Kies de knop **Servercertificaten** bovenaan de pagina om het scherm met een overzicht van alle servercertificaten van uw organisatie te openen. U ziet direct over welke certificaten uw organisatie beschikt en tot wanneer deze geldig zijn. Vanuit dit scherm kunt u uw certificaten beheren en eenvoudig verlengen. Met de knop **Nieuw servercertificaat** kunt u direct een nieuwe aanvraag starten. Omdat u bent ingelogd is uw email adres reeds bekend. De stap waarin uw emailadres wordt geverifieerd is daarom nu niet nodig.

4.2 Scherm 1: Contactpersoon

Na het klikken op de aanvraagknop opent het eerste scherm:

Aanvraag nieuw PKI-overheid servercertificaat (alle typen)

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Hieronder is een overzicht van de Abonnee gegevens en uw gegevens getoond. Indien deze gegevens niet meer correct zijn, is het belangrijk om deze eerst aan te passen om te voorkomen dat uw aanvraag tijdens de behandeling vertraging oploopt.

LET OP: KPN zal het getoonde e-mailadres gebruiken voor verdere communicatie over deze aanvraag.

Gegevens Abonnee en Contactpersoon	
PKIoverheid Abonneenummer	P1234560
Land	Nederland
KvK nummer	27124701
Organisatiernaam	KPN B.V.
Achternaam contactpersoon	Molentje
E-mailadres	martine.intmolentje@kpn.net

[Volgende stap >>](#)

Toelichting bij scherm **1. Contactpersoon**

Dit scherm stelt u in staat om de gegevens van de Abonnee waarvoor het Servercertificaat wordt aangevraagd te controleren. Als contactpersoon wordt automatisch de persoon genomen die is ingelogd in het SSP.

- Klik op [Volgende stap >>](#) om verder te gaan.

4.3 Scherm 2: Certificaatbeheerder

In dit scherm geeft u aan wie de Certificaatbeheerder is voor deze certificaataanvraag.

Aanvraag nieuw PKIoverheid servercertificaat (alle typen)

1. Contactpersoon 2. Certificaatbeheerder 3. Certificaat 4. Controle 5. Voorwaarden 6. Afronding

In dit scherm kunt u aangeven wie als Certificaatbeheerder op zal treden voor deze certificaataanvraag. De Certificaatbeheerder zal namens de Abonneeorganisatie dit Servercertificaat in ontvangst (gaan) nemen en beheren.

BELANGRIJK: u kunt kiezen uit twee opties:

Kies 1 als u een nieuwe Certificaatbeheerder wilt aanmelden die niet eerder is geregistreerd bij KPN. In dit geval zal KPN -voorafgaande aan de uitgifte van het certificaat- de identiteit van de Certificaatbeheerder (laten) verifiëren en vergelijken met de aangeleverde persoonsgegevens.

Kies 2 als de Certificaatbeheerder al eerder door KPN is geïdentificeerd voor een eerdere certificaataanvraag.

Certificaatbeheerder	
De certificaatbeheerder is*	<input type="text" value="- Maak een keuze -"/>

[Volgende stap >>](#)

U kunt kiezen uit twee opties:

1. *volledig nieuw*
Kies deze optie als u een nieuwe Certificaatbeheerder wilt aanmelden die niet eerder is geregistreerd en geïdentificeerd door KPN.

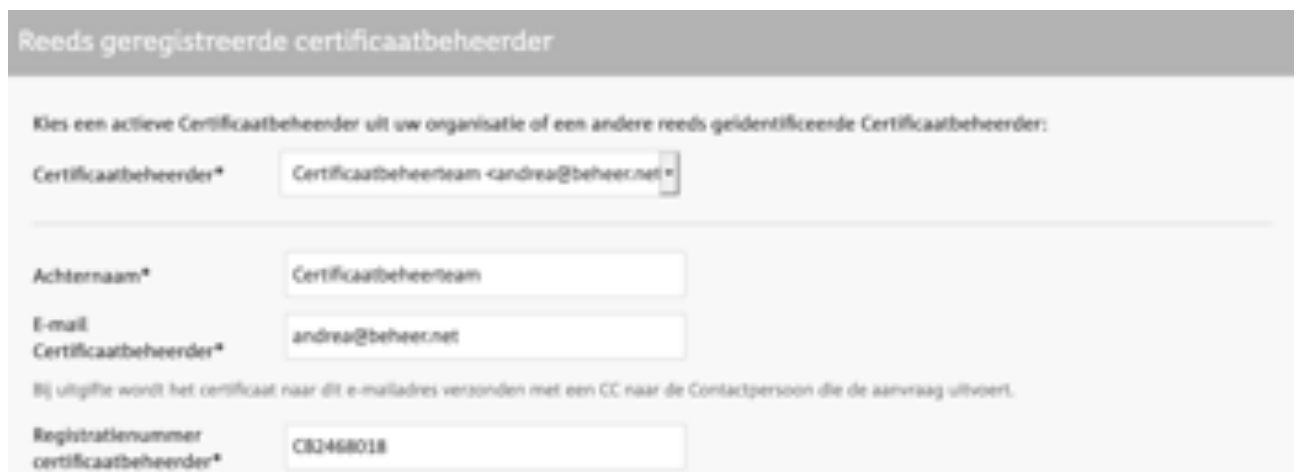
2. *reeds geïdentificeerd*

Kies deze optie als de gewenste certificaatbeheerder al bij KPN bekend is, bijvoorbeeld bij een volgende certificaataanvraag voor dezelfde organisatie. Daarnaast kan een persoon Certificaatbeheerder zijn voor meerdere Abonnees.

De uitleg en invulinstructies van beide opties kunt u vinden in paragraaf 3.4: Scherm 2: Certificaatbeheerder. Als u kiest voor de 2^e optie (reeds geïdentificeerd) is in het SSP de volgende keuzelijst als extra beschikbaar:



Hiermee kunt u kiezen uit de bestaande certificaatbeheerders van uw organisatie. Als u een bestaande certificaatbeheerder kiest dan worden de bijbehorende velden automatisch voor u ingevuld:



[Volgende stap >>](#)

4.4 Scherm 3: Certificaat

In dit scherm vult u de gegevens in die daadwerkelijk in het certificaat komen te staan. Dit deel is grotendeels hetzelfde als bij een aanvraag zonder SSP (zie paragraaf 3.5: Scherm 3: Certificaat), met uitzondering van het eerste blok. Daarom wordt hier alleen het eerste blok getoond en verder toegelicht.

Aanvraag nieuw PKIoverheid servercertificaat (alle typen)

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

In dit scherm dient u de gegevens in te vullen die in het serverscertificaten worden opgenomen.

Type servercertificaat

Hieronder kunt u het type servercertificaat selecteren. U heeft dan de volgende mogelijkheden:

- [PKIoverheid standaard servercertificaat](#)
- [PKIoverheid Digipoort PRIVATE servercertificaat](#)
- [PKIoverheid PRIVATE servercertificaat](#)

1. **PKIoverheid standaard servercertificaten** zijn uitsluitend bedoeld voor de beveiliging van publieke websites (digitale loketten, openbare internetdiensten en webshops). Dit type servercertificaat wordt standaard vertrouwd door alle gangbare webbrowsers waardoor reguliere gebruikers een beveiligde verbinding met uw website kunnen maken. [Meer informatie.](#)
 2. **PKIoverheid Digipoort PRIVATE servercertificaten** zijn bedoeld voor koppeling van uw systeem met Digipoort. KPN bepaalt automatisch de naam van de service waardoor er geen controle op eigenaarschap van het domein nodig is en het aanvraagproces eenvoudiger verloopt. Het Organisatie-identificatienummer (OIN) of Handelsregisternummer (HRN) van uw organisatie wordt opgenomen in het certificaat om de communicatie via Digikoppeling mogelijk te maken. Voorbeelden zijn: communicatie met Diginetwerk, Digipoort, SBR, OLO, LV WOZ, WSNP, GBA-V, BAG, GWH, WKP8 e.a. Het stamcertificaat is niet opgenomen in browsers of operating systemen. [Meer informatie.](#)
 3. **PKIoverheid PRIVATE servercertificaten** zijn bedoeld voor systeem-systeem koppelingen voor toepassing in besloten gebruikersgroepen (bijvoorbeeld EDSN of NWRO). Het stamcertificaat is niet opgenomen in browsers of operating systemen. [Meer informatie.](#)
- De geldigheidsduur en tarieven verschillen per type servercertificaat. Zie voor details de [actuele tarieven.](#)

De aanvraag betreft een*

Geldigheidsduur* 3 jaar

Invulinstructie en toelichting **3. Certificaat** 1^e gedeelte: [Type servercertificaat](#)

In het eerste blok kiest u het type servercertificaat dat u wenst aan te vragen. Het blok begint met een korte toelichting op de mogelijke keuzes, gevolgd door de keuzelijst. De keuzelijst bevat de volgende 3 opties:

- 1 PKIoverheid standaard servercertificaat;
- 2 PKIoverheid Digipoort PRIVATE servercertificaat;
- 3 PKIoverheid PRIVATE servercertificaat.

U kiest hier het servercertificaat dat geschikt is voor uw toepassing. In de oranje balk staat een korte toelichting over de verschillende types met een link 'Meer informatie' die doorverwijst naar de website waarin de verschillen uitgebreid beschreven staan.

4.5 Scherm 4: Controle

De controle is identiek aan hetgeen beschreven is in paragraaf 3.6: Scherm 4: Controle en wordt daarom hier niet herhaald.

4.6 Scherm 5: Voorwaarden

Het scherm met de voorwaarden is identiek aan hetgeen beschreven is in paragraaf 3.7: Scherm 5: Voorwaarden en wordt daarom hier niet herhaald. Als extra toevoeging wordt onderaan het formulier wel de volgende banner getoond:

Plaats bestelling

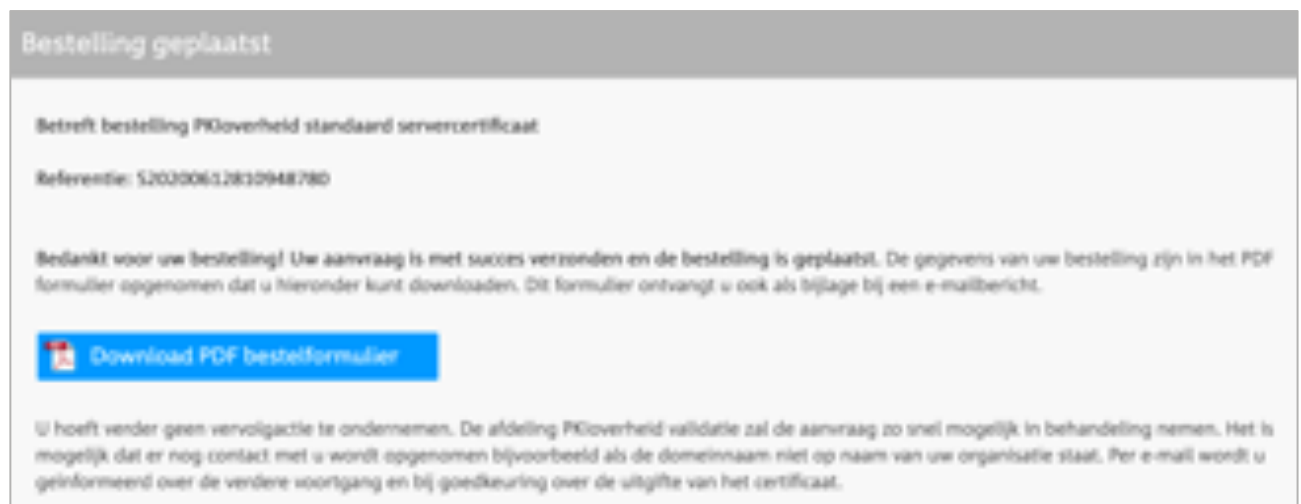
Met het plaatsen van de bestelling zet u direct de verwerking door KPN in gang. De gegevens in deze certificaataanvraag zijn daarna niet meer aan te passen.

De knop **Verzend Aanvraag** is vervangen met **Plaats bestelling** en er wordt een waarschuwing gegeven dat wijzigingen niet meer mogelijk zijn. Dit is omdat bij een aanvraag via het SSP de aanvraag direct automatisch verzonden wordt en daarmee de bestelling is gedaan door de contactpersoon die op dat moment is ingelogd in het SSP.

4.7 Afronding

Als de bestelling digitaal met succes is geplaatst, verschijnt het volgende scherm:

Aanvraag nieuw PKIoverheid servercertificaat (alle typen)



Het is in dit geval niet nodig om het bestelformulier uit te printen, te ondertekenen en via de post te versturen.

U kunt vanuit het scherm een kopie van het bestelformulier downloaden. Het formulier wordt bovendien altijd per email verzonden aan de aanvrager (contactpersoon).

5 Beoordeling aanvraag door KPN en vervolg

5.1 Domeincontrole

KPN neemt de aanvraag in behandeling. Een belangrijke controle voordat KPN een servercertificaat uit geeft, is het vaststellen dat de aanvrager daadwerkelijk de zeggenschap over de Naam van de service (FQDN) heeft die in de aanvraag van het servercertificaat is opgenomen. Dit is de 'domein controle'. KPN neemt per email contact met u op of de beheerder van uw domein om deze controle uit te voeren. Dit wordt toegelicht in het toegestuurde emailbericht en op de pagina <https://certificaat.kpn.com/aanvragen/servercertificaten/domeincontrole/>.

In het geval van een Digipoort PRIVATE servercertificaat wordt de domeinnaam vastgesteld volgens de regels van digipoort. Er vindt voor dergelijke certificaten daarom geen domeincontrole plaats.

5.2 Identificatie Certificaatbeheerder en uitgifte

Indien de zeggenschap over het domein is aangetoond en aanvraag wordt goedgekeurd, zal KPN de Certificaatbeheerder identificeren als dat nog niet eerder is gedaan. Na succesvolle identificatie zal KPN het certificaat per email versturen naar de Certificaatbeheerder en de Contactpersoon. De Certificaatbeheerder ontvangt per brief een intrekcode. U dient het Servercertificaat pas te gebruiken als de Certificaatbeheerder de intrekcode per brief heeft ontvangen.

Zie ook de procesbeschrijving in par. 2.1.

5.3 Certificaatvernieuwing en geldigheidsduur

KPN stuurt een emailbericht met een gepersonaliseerde link een aantal weken voor het verlopen van een Servercertificaat. Via de link in zo'n emailberichten kunt u het aanvraagproces voor het vernieuwen van een Servercertificaat eenvoudig opstarten en zijn zoveel mogelijk gegevens al voor u ingevuld. Bij vernieuwing zal de geldigheidsduur van het nieuwe Servercertificaat gebaseerd zijn op de oorspronkelijke geldigheidsdatum van het verlopende Servercertificaat, uiteraard verhoogd met 1 of 3 jaar, afhankelijk van het type. U kunt daarmee tijdig verlengen om de continuïteit te garanderen én tegelijkertijd gebruik maken van de effectieve geldigheidsduur van 1 of 3 jaar. Daarnaast ontvangt u automatisch de vernieuwingskorting zoals vermeld bij de tarieven.

LET OP: u dient daarvoor gebruik te maken van de link in het emailbericht dat KPN u toestuurt voorafgaand aan het verlopen van het certificaat of via MijnCertificaten een Servercertificaat te verlengen.

Overige aandachtspunten:

- De geldigheidsduur van een standaard Servercertificaat is 397 dagen (1 jaar).
- Als u gebruik maakt van het openbare aanvraagformulier (zonder de link in het emailbericht dat KPN u toestuurt) of een nieuw Servercertificaat aanvraagt via MijnCertificaten is de productiedatum de ingangsdatum van de geldigheid van het Servercertificaat. U maakt dan geen aanspraak op een vernieuwingskorting ook als u een Servercertificaat heeft met dezelfde FQDN/Naam van de Service. U kunt in het formulier niet zelf meer kiezen of het een vernieuwing betreft, dit is alleen mogelijk door de toegestuurde link te gebruiken of via MijnCertificaten te verlengen.

6 BIJLAGEN: email en PDF formulier

Voor de volledigheid bevat deze bijlage de email en het pdf-formulier die de aanvrager per email ontvangt.

6.1 Emailbericht afronding

Na afronding van het webformulier ontvangt de aanvrager op het gevalideerde emailadres de volgende email. De tekst en bijlage is identiek aan het afrondingsscherm in hoofdstuk 3. Het is bedoeld als backup voor het geval de browser wordt afgesloten en de download link naar de PDF niet meer voorhanden is.



Uw aanvraag PKIoverheid Digipoort PRIVATE servercertificaat bij KPN: digipoort-00000003271247010000

U heeft de eerste stap van uw PKIoverheid Digipoort PRIVATE servercertificaat aanvraag bij KPN succesvol voltooid. Deze e-mail is bedoeld als extra bevestiging en als referentie. Het bevat als bijlage dezelfde PDF die u ook hebt kunnen downloaden via het portal. Onderstaande instructies heeft u mogelijk al uitgevoerd en zijn hier opgenomen voor het geval de browser is afgesloten.

BELANGRIJKE VERVOLGSTAP: ONDERTEKENEN EN INDIENEN VAN DE AANVRAAG

Om de aanvraag van het PKIoverheid Digipoort PRIVATE servercertificaat daadwerkelijk in gang te zetten, kunt u kiezen uit 2 varianten:

OPTIE 1: AANVRAAG ELEKTRONISCH ONDERTEKENEN EN INDIENEN.

Indien u als contactpersoon beschikt over een rechtsgeldige elektronische handtekening kunt u de aanvraag elektronisch ondertekenen en per e-mail indienen. De werkwijze is als volgt:

- PDF aanvraagformulier elektronisch ondertekenen en toezenden

De contactpersoon die op het formulier staat, dient het formulier elektronisch te ondertekenen. Dit dient te gebeuren met [een PKIoverheid persoonlijk certificaat](#) dat op naam van de contactpersoon staat.

Het eenvoudigst is om de ondertekening uit te voeren in de vorm van een elektronisch ondertekende e-mail met het PDF aanvraagformulier als bijlage. U kunt deze e-mail doorsturen naar pkivalidation@kpn.com en daarbij dient u de e-mail elektronisch te ondertekenen. Dit kan standaard met gangbare e-mailprogramma's zoals Microsoft Outlook of Mozilla Thunderbird.

OPTIE 2: AANVRAAG OP PAPIER PER POST INDIENEN.

Kies voor deze optie indien u niet de gelegenheid heeft om de aanvraag elektronisch te ondertekenen en in te dienen.

- Print het PDF formulier op 1 A4;
- De contactpersoon die op het formulier staat dient het formulier te ondertekenen;
- Stuur het aanvraagformulier op naar:
KPN B.V.
Ter attentie van PKIoverheid-Validatie
Postbus 9105
7300 HN APELDOORN

Dit is een automatisch verzonden e-mail. Gelieve deze e-mail niet beantwoorden.

KPN B.V.

6.2 PDF Aanvraag Servercertificaat

Het pdf-formulier dat de Contactpersoon moet ondertekenen ziet er als volgt uit:



S2020082773073333

KPN - Aanvraag PKIoverheid Digipoort PRIVATE servercertificaatReferentie: **S20200827730733333****Gegevens Abonnee en Contactpersoon**

Abonneenummer:	p1234560	Geboortedatum:	12-08-1970
Handelsnaam volgens KvK:	KPN B.V.	E-mail:	mark.vanbeijnen@kpn.com
Achternaam Contactpersoon:	Farwerck		

Certificaatbeheerder

De certificaatbeheerder is:	1. volledig nieuw	Registratienummer:	
Voornaam:	Andrea Philomenia	Geboorteplaats:	Ijsberg
Tussenvoegsel:	van het	E-mail:	andrea@beheer.net
Achternaam:	Certificaatbeheerteam	(Mobiel) telefoonnummer:	+31 6 87654321
Geboren:	08-08-1988		
Organisatiename:	KPN BV		
Adresgegevens:	Wilhelminakade 123 , 3072 AP Rotterdam, Nederland		

Gegevens voor Servercertificaat

BELANGRIJK: De hieronder getoonde gegevens worden opgenomen in uw Servercertificaat. Controleer deze gegevens zorgvuldig! Typefouten kunnen in sommige gevallen het Servercertificaat technisch onbruikbaar maken en zijn na uitgifte niet meer te wijzigen.

Naam van de Service (CN):	digipoort-00000003271247010000	Geldigheidsduur:	3 jaar
Subject Serienummer:	00000003271247010000		
Organisatiename (O):	KPN B.V.		
Afdeling (OU):	Corporate Finance		
Plaats (L), Provincie (S), Land (C):	Rotterdam, Zuid-Holland, NL		
SHA256 fingerprint van CSR:	622e5f26b66aa3181db70247a3c460bae49a12666209580b215124d6ae834943		
Subject Alternative Names:			

Overige gegevens

Toepassing certificaat:	Digipoort-private	Type aanvraag:	Indieel
Support pakket:	Standaard pakket	Einddatum oude certificaat:	
Referentie (bv facturatie):	CF-Belasting-08-003a	Serienummer oude certificaat:	

Akkoordverklaringen

Ondergetekende verklaart namens Abonnee:

- dat alle gegevens volledig, juist en naar waarheid zijn ingevuld.
- akkoord met KPN Alg. Leveringvoorwaarden en Bijz. Voorwaarden PKIoverheid certificaten.
- dat opgegeven Certificaatbeheerder geïnformeerd, bevoegd en ter zake kundig is om namens abonnee Servercertificaten te installeren, beheren en in te trekken.
- dat het sleutelmateriaal is gegenereerd en wordt bewaard in een Veilige Omgeving.
- akkoord te zijn met de tarieven.

Vervolgstappen

Om de aanvraag van het Servercertificaat daadwerkelijk in gang te zetten dient u de volgende vervolgstappen uit te voeren:

- De contactpersoon die op het formulier staat, dient het formulier te ondertekenen.
- Het formulier indienen bij KPN. Hiervoor heeft u twee opties.

Optie 1: Aanvraag per e-mail elektronisch ondertekenen en indienen. Dit is voor u de eenvoudigste en snelste optie. Toelichting heeft u per e-mail ontvangen met dit formulier.

Optie 2: Aanvraag op papier per post indienen. Formulier opsturen naar:

KPN B.V.**Ter attentie van PKIoverheid-Validatie****Postbus 9105, 7300 HN APELDOORN****Handtekening Contactpersoon****Farwerck Geb. 12-08-1970**

Datum:
Plaats:
Handtekening: