



Datum
mei 2022

Auteur
KPN

Versie
1.1

KPN certSIGN Toelichting en instructie Aanvraag servercertificaat

OV SSL

Documentnummer: ASC-220704

Inhoudsopgave

1	Inleiding	3
1.1	<i>Introductie</i>	3
1.2	<i>Terminologie</i>	3
1.3	<i>Referenties</i>	5
2	certSIGN servercertificaataanvraag	6
2.1	<i>Toelichting proces certificaataanvraag</i>	6
2.2	<i>Startscherm: checklist randvoorwaarden en validatie e-mail</i>	8
2.3	<i>Scherf 1: Aanvraag</i>	12
2.4	<i>Scherf 2: Controleren en bestellen</i>	21
3	Scherf 3: Afronding	24
3.1	<i>Optie 1: aanvraag elektronisch ondertekenen en indienen</i>	24
3.2	<i>Optie 2: aanvraag op papier per post indienen</i>	25
4	Beoordeling aanvraag door KPN en vervolg	26
4.1	<i>Controle Abonneeregistratie</i>	26
4.2	<i>Identificatie Certificaatbeheerder</i>	26
4.3	<i>Domeinvalidatie</i>	26
4.4	<i>Uitgifte en gebruik</i>	26
5	BIJLAGEN: e-mail en PDF formulier	27
5.1	<i>E-mailbericht afronding</i>	27
5.2	<i>PDF Aanvraag Servercertificaat</i>	27

1 Inleiding

1.1 Introductie

Dit document bevat een uitgebreide toelichting en invulinstructie voor de aanvraag van een certSIGN Servercertificaat via het webformulier dat beschikbaar is op:

<https://kpnpkio.managedpki.com/certsigncsr/>

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

Met dit webformulier kunt u de volgende typen servercertificaten aanvragen:

- certSIGN OV SSL servercertificaat.

Voordat u certSIGN servercertificaten kunt aanvragen, ontvangen en gebruiken, dient u zich eenmalig te registreren als Abonnee van KPN Certificatiedienstverlening. Dit kan via:

<https://kpnpkio.managedpki.com/registratie/>

Het certificaat zal na goedkeuring van de aanvraag worden uitgegeven aan een reeds geregistreerde of nieuw geïdentificeerde Certificaatbeheerder.

1.2 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 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 natuurlijk personen, b.v. een bestuur van een vereniging, die 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 en de identificerende gegevens van de certificaathouder 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 namens de Abonnee 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 (FQDN) is 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'.

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

OV (Organisation Validated): publiek vertrouwd servercertificaat dat uitsluitend bedoeld is 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. OV staat voor 'Organisation Validated' en houdt in dat KPN uw organisatie zal controleren en dat deze organisatie naam ook in het servercertificaat komt. Dit biedt bezoekers van uw site de zekerheid dat zij met de juiste organisatie communiceren.

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.

Services/servercertificaat: 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.

1.3 Referenties

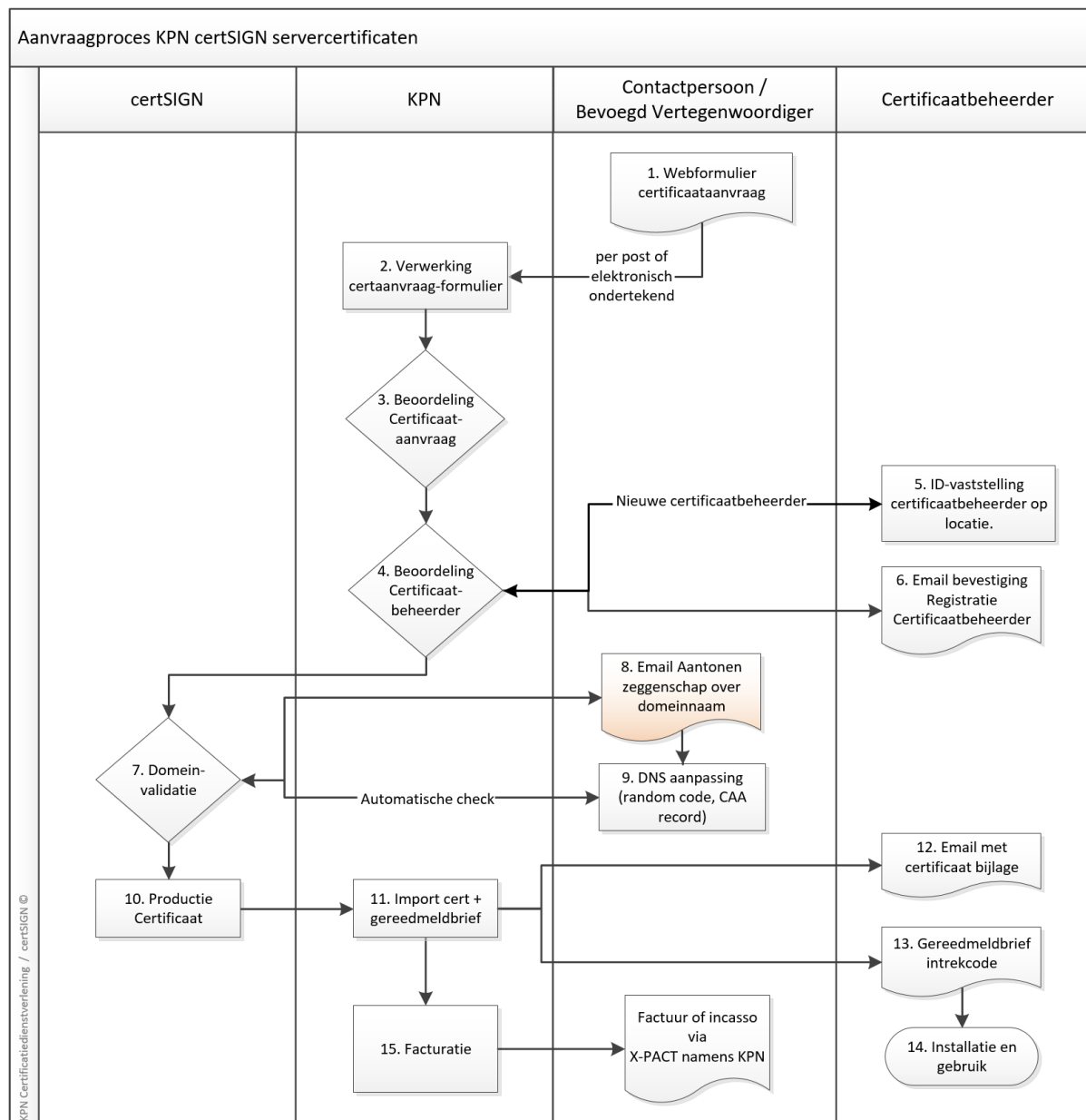
Voor meer informatie over de Certificatiedienstverlening van KPN verwijzen wij u naar

<https://certificaat.kpn.com>

2 certSIGN servercertificaataanvraag

2.1 Toelichting proces certificaataanvraag

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



Het aanvraag proces van een KPN certSIGN servercertificaat bestaat uit de volgende stappen:

1. Allereerst dient u op de website het webformulier in te vullen op <https://kpnpkio.managedpki.com/certsigncsr/> Hierin geeft u gegevens op over:
 - a. de Contactpersoon die de aanvraag doet namens een Abonnee. Zowel de Contactpersoon als de Abonnee dienen reeds bij KPN geregistreerd te zijn;

- b. de Certificaatbeheerder die verantwoordelijk is voor het beheer van het Certificaat en die KPN (eenmalig) persoonlijk zal identificeren;
- c. de identificerende gegevens die in het Servercertificaat opgenomen dienen te worden.

Afronding van het webformulier resulteert in een PDF document die ondertekend dient te worden door de Contactpersoon. Dit kan op papier of elektronisch. Vervolgens dient u het ondertekende formulier op te sturen naar KPN per post of e-mail of via het selfservice portal MijnCertificaten, zie <https://certificaat.kpn.com/support/mijn-registratie/mijncertificaten/>

2. Na ontvangst van het aanvraagformulier start bij KPN het validatieproces. Dit betreft allereerst het vergelijken van de gegevens van Abonnee en Contactpersoon met gegevens die bij KPN zijn geregistreerd tijdens de eenmalige Abonneeregistratie voor de certificatie-dienstverlening van KPN, zie <https://certificaat.kpn.com/aanvragen/abonneeregistratie/>
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. Indien er een nieuwe Certificaatbeheerder is opgegeven, zal KPN een identificatie laten uitvoeren.
5. Een koerier van AMP voert deze identificatie in opdracht van KPN uit op locatie van de klant. Per e-mail ontvangt de Certificaatbeheerder een uitnodiging om een afspraak te maken voor deze identificatie.
6. KPN zal de identificatie controleren. Indien deze correct is, ontvangt de Certificaatbeheerder een bevestiging van de registratie en een identificatienummer dat bij volgende aanvragen te gebruiken is.
KPN stuurt de minimaal vereiste aanvraaggegevens door naar certSIGN.
7. **certSIGN** voert de zogenaamde domeinvalidatie uit.
8. **certSIGN** stuurt daarvoor een e-mailbericht naar de Contactpersoon met het verzoek om aan te tonen dat deze zeggenschap heeft over de gebruikte domeinnaam. Dit is nader toegelicht in de toegestuurde e-mail.
9. De IT beheerorganisatie van het betreffende domein voert de wijzigingen door die de zeggenschap over het domein aantonen via een random code in een DNS TXT record. Indien nodig autoriseert men certSIGN om voor het domein een certificaat uit te geven door "**certsign.ro**" toe te voegen in een DNS CAA record.
10. **certSIGN** checkt automatisch of de aanpassingen zijn doorgevoerd en stuurt na 1 week een herinnering. Als de wijzigingen correct zijn doorgevoerd, produceert certSIGN vervolgens het servercertificaat en stuurt dit naar KPN.
11. KPN importeert het certificaat in voor verder verwerking.
12. KPN stuurt het certificaat per e-mail naar de Certificaatbeheerder met een kopie naar de Contactpersoon die de aanvraag doet. KPN gebruikt daarvoor het e-mailadres dat de Contactpersoon opgeeft bij de registratie van de Certificaatbeheerder.

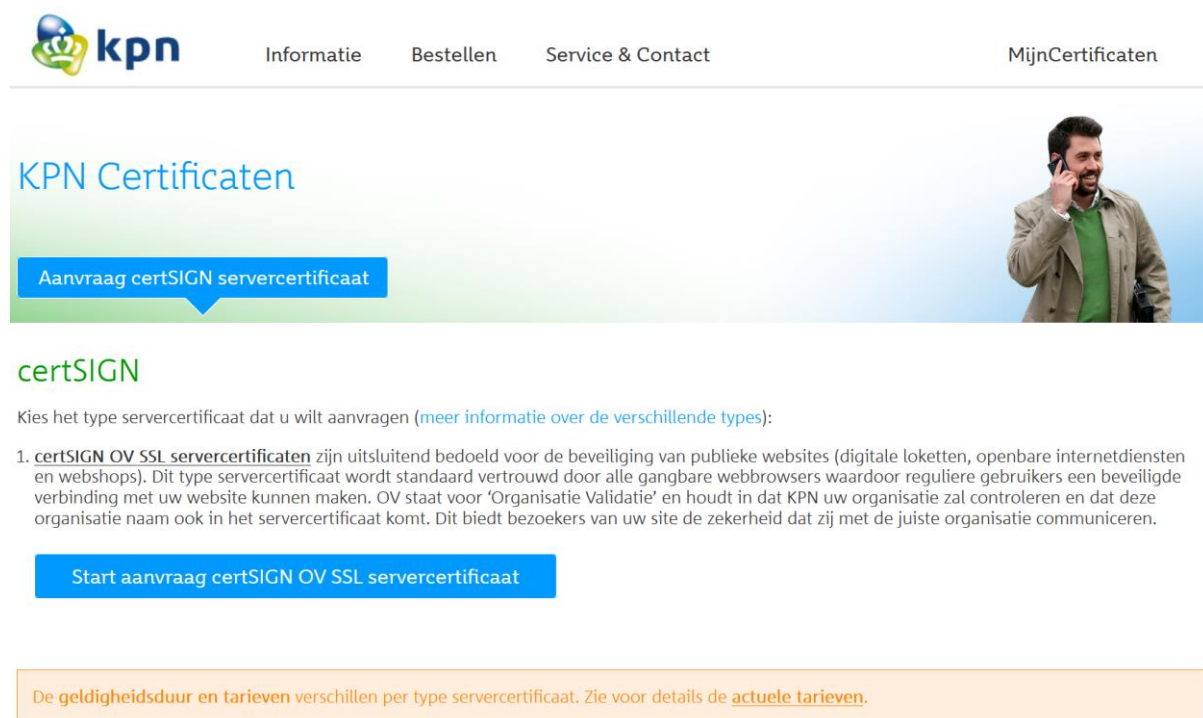
13. De Certificaatbeheerder ontvangt per PIN-mailer brief een intrekingscode. Hiermee is het mogelijk om (bijvoorbeeld in geval van een beveiligingsincident) het certificaat in te trekken via een self-service portal. Zie <https://certificaat.kpn.com/support/mijn-registratie/intrekken/>

Indien gewenst kunnen de PIN-mailers per versleutelde e-mail worden toegestuurd. In dat geval dient u contact op te nemen met de Servicedesk. Zie <https://certificaat.kpn.com/support/> voor contactgegevens.

14. Het certificaat is na installatie gereed voor gebruik. Zie voor toelichting: <https://certificaat.kpn.com/installatie-en-gebruik/installatie/servercertificaten/>
15. Tot slot ontvangt de Abonnee op het opgegeven facturatieadres een factuur.

2.2 Startscherm: checklist randvoorwaarden en validatie e-mail

De aanvraag van een Servercertificaat start op <https://kpnpkio.managedpki.com/certsigncsr/> met het onderstaande scherm:



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, there is a large banner with the text 'KPN Certificaten' and a blue button labeled 'Aanvraag certSIGN servercertificaat'. To the right of the banner is an image of a man talking on a mobile phone. Below the banner, the text 'certSIGN' is displayed, followed by a paragraph: 'Kies het type servercertificaat dat u wilt aanvragen (meer informatie over de verschillende types):'. Below this paragraph is a list item: '1. certSIGN OV SSL 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. OV staat voor 'Organisatie Validatie' en houdt in dat KPN uw organisatie zal controleren en dat deze organisatie naam ook in het servercertificaat komt. Dit biedt bezoekers van uw site de zekerheid dat zij met de juiste organisatie communiceren.' Below this list item is a blue button labeled 'Start aanvraag certSIGN OV SSL servercertificaat'. At the bottom of the screenshot, there is an orange box with the text: 'De geldigheidsduur en tarieven verschillen per type servercertificaat. Zie voor details de actuele tarieven.'

Momenteel is er één type beschikbaar.

- Klik op de knop 'Start aanvraag certSIGN OV SSL servercertificaten'

Aanvraag certSIGN OV SSL servercertificaat

certSIGN OV SSL servercertificaat

Welkom bij het aanvraagformulier voor een [certSIGN OV SSL servercertificaat](#) bij KPN.

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

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

Checklist aanvraag certSIGN OV SSL servercertificaataanvraag

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

- Uw organisatie is reeds als [abonnee van de PKI dienstverlening](#) bij KPN geregistreerd.
- Uw organisatie heeft een [actieve registratie bij de Kamer van Koophandel](#) en de geregistreerde gegevens zijn correct.
- U bent [bevoegd](#) om een certificaat aan te vragen.
- U beschikt over een [Certificate Signing Request \(CSR\)](#) gebaseerd op een uniek sleutelbaar. De CSR bevat de juiste gegevens die ook in het servercertificaat opgenomen zullen worden.
- U heeft een [domeinnaam](#) om op te laten nemen in het Servercertificaat.

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*

[Vernieuw captcha](#)De tekst is *niet* hoofdlettergevoelig[Volgende stap >>](#)

Type certificaat

Met dit formulier kunt u alleen een certSIGN OV SSL servercertificaat aanvragen. Zie voor meer informatie over de verschillende type servercertificaten:

<https://certificaat.kpn.com/pkioverheidcertificaten/servercertificaten/>

Toelichting

De eerste stap bestaat uit twee delen:

1. een checklist om vooraf te controleren of alle benodigde gegevens beschikbaar is en aan de randvoorwaarden is voldaan. Het doel van de checklist is om te voorkomen dat u halverwege het formulier 'vastloopt' omdat bepaalde informatie ontbreekt of dat uw aanvraag vertraging oploopt. De eerste twee punten zijn organisatorisch de laatste twee punten zijn meer technisch van aard;
 - a. Uw organisatie is reeds als abonnee voor de PKI dienstverlening bij KPN geregistreerd. De bevoegd vertegenwoordiger heeft bij de bevestiging van de registratie een PKI(overheid) abonneenummer ontvangen. Dit is nodig tijdens het invullen van het certificaataanvraagformulier.
 - b. Uw organisatie heeft een actieve registratie bij de Kamer van Koophandel en de geregistreerde gegevens zijn correct. Bij het invullen van het formulier zal KPN een online controle uitvoeren bij de KvK. LET OP: Het is niet mogelijk om afwijkende gegevens in de certificaataanvraag door te voeren. Als de KvK gegevens niet meer actueel zijn dan dient u deze eerst bij de KvK te wijzigen.
 - c. U bent bevoegd om een certificaat aan te vragen. Bevoegd zijn de Bevoegd Vertegenwoordiger of een door de Bevoegd Vertegenwoordiger gevolmachtigde Contactpersoon die bij KPN is geregistreerd als onderdeel van de PKI Abonneeregistratie.
 - d. U heeft een zogenaamd Certificate Signing Request (CSR) gebaseerd op een uniek sleutelpaar. Dit bestand bevat de sleutel én de naamgeving die certSIGN in het certificaat gaat opnemen.

BELANGRIJK: alle informatie in de CSR dient overeen te komen met de informatie die in de KvK is vermeld, anders kan het certificaat niet worden uitgegeven.

Zie voor uitgebreide technische toelichting:

<https://certificaat.kpn.com/aanvragen/servercertificaten/csr-genereren/>

- e. U heeft een domeinnaam om op te laten nemen in het Servercertificaat, zie <https://certificaat.kpn.com/aanvragen/servercertificaten/fqdn-naam-van-de-service/>. Deze zal opgenomen worden 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 naam van een derde partij. Het kan zijn dat uw domeinnaam op naam staat van een ICT dienstverlener of ingeval van een overheidsorganisatie 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.

2. het vaststellen het valideren van uw e-mailadres. Het doel hiervan is om zeker te zijn dat de eigenaar van het e-mailadres zelf de aanvraag doet -danwel minimaal op de hoogte is- en dat het e-mailadres ook correct is ingevoerd. Naar dit e-mailadres 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 e-mailadres van de Contactpersoon te gebruiken. Verder zal KPN dit e-mailadres gebruiken om u te informeren over de voortgang van uw registratie.

Invulinstructie

- Verifieer of u alle informatie beschikbaar heeft en vink alle checkboxes aan.
- Voer uw e-mailadres in.
- Type de Verificatiecode over van het plaatje (een zogenaamde CAPTCHA).
- Klik op 'VOLGENDE STAP'.

Vervolgens verschijnt het onderstaande bevestigingsscherm:

certSIGN OV SSL servercertificaat

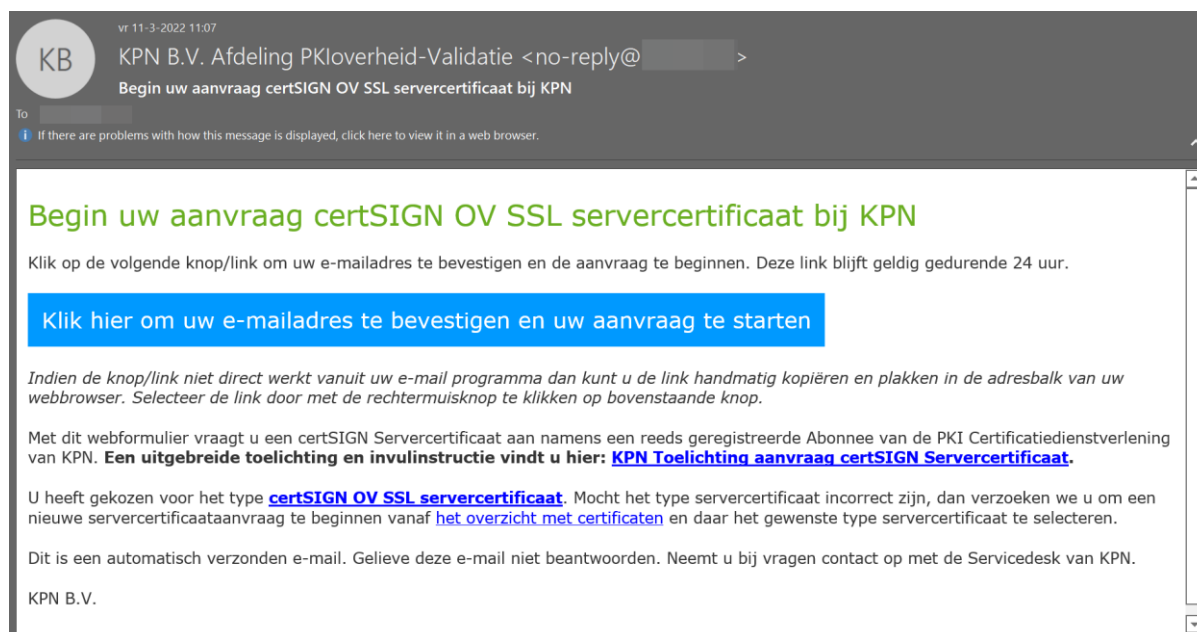
E-mail verzonden

Er is een e-mail verstuurd aan [REDACTED]

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

Deze link blijft geldig gedurende 24 uur (tot 2022-05-07 10:17:55). Daarna dient u opnieuw het proces te starten.

U ontvangt per omgaande de volgende e-mail waarmee KPN uw e-mailadres verifieert.



- Klik op de bovenste link in de e-mail om het aanvraagformulier voor een Servercertificaat te starten.

LET OP:

1. Indien de link niet direct werkt vanuit uw e-mail 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 dient u opnieuw uw e-mailadres in te voeren ter validatie.

2.3 Scherm 1: Aanvraag

Na het klikken op de link in de e-mail opent het eerste invoerscherm:

certSIGN OV SSL servercertificaat

1. Aanvraag

2. Controleren en Bestellen

3. Afronding

U vraagt met dit formulier een [certSIGN OV SSL servercertificaat](#) aan.

certSIGN OV SSL 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.

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

Verplichte velden worden aangegeven met (*).

Invulinstructie en toelichting sectie 1: Gegevens Abonnee en Contactpersoon

Gegevens Abonnee en Contactpersoon

PKI(overheid) Abonneenummer*

In dit blok 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 PKI Certificatiedienstverlening kunt u dat [hier](#).

Land*

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](#).

Uw E-mailadres

LET OP: Naar dit e-mailadres zal KPN het PDF formulier sturen. Mocht dit incorrect zijn, dan verzoeken we u om een nieuwe servercertificaataanvraag te beginnen.

Achternaam contactpersoon*

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. De Contactpersoon dient bevoegd te zijn dit formulier te ondertekenen en het formulier ook daadwerkelijk te gaan ondertekenen. De Contactpersoon dient als Contactpersoon bij KPN geregistreerd te zijn bij de Abonneeregistratie of is de Bevoegd Vertegenwoordiger die de Abonneeregistratie heeft ondertekend.

Geboortedatum*

Deze sectie 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 PKI(overheid) 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 dat is gebruikt in de Abonneeregistratie. U kunt alleen een certSIGN OV SSL servercertificaat aanvragen als uw organisatie een KvK registratie heeft.
- Na het invullen 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

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

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

Gegevens in KvK

Bij het succesvol opvragen van de gegevens bij de Kamer van Koophandel is het tweede blok in deze sectie automatisch gevuld. Er zal een controle plaatsvinden tussen deze gegevens en de gegevens in het Certificate Signing Request (CSR).

Gegevens in KvK

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

Organisatienaam*	Koninklijke KPN N.V.
------------------	----------------------

Dit is de statutaire naam van uw organisatie zoals geregistreerd is in het handelsregister van de KvK. Deze statutaire naam (of een geregistreerde handelsnaam) dient u in de CSR op te nemen.

Land*	NL
Provincie*	Zuid-Holland
Plaats*	Rotterdam

Dit is het vestigingsadres van de hoofdvestiging zoals geregistreerd is in het handelsregister van de KvK. Dit adres dient u in de CSR op te nemen.

Invulinstructie en toelichting sectie 2: Certificaatbeheerder

Certificaatbeheerder

De certificaatbeheerder is*

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. 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.

In deze sectie 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.

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 certificaatbeheerder al eerder bij KPN als Certificaatbeheerder is

aangemeld **en een nieuw Registratienummer heeft van het type CB1234567**. Die situatie kan optreden bij een tweede certificaat aanvraag maar een persoon kan ook Certificaatbeheerder zijn voor meerdere Abonnees.

- Kies de optie die voor u van toepassing is.

Optie 1 Certificaatbeheerder is volledig nieuw

Indien u kiest voor een nieuwe Certificaatbeheerder dan dient u van deze persoon de persoons- en adresgegevens op te geven in de twee secties met invoervelden die verschijnen na selectie in de dropdown.

Nieuwe certificaatbeheerder

Volledige voornaam*	<input type="text" value="Volledige voornaam / voornamen"/>
Tussenvoegsel	<input type="text" value="Bijv. van, de"/>
Achternaam*	<input type="text" value="Achternaam conform identiteitsbewijs"/>

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*	<input type="text"/>
----------------------------	----------------------

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*	<input type="text" value="Bijv. 31-12-1971"/>
Geboorteplaats*	<input type="text" value="Geboorteplaats conform identiteitsbewijs"/>

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*	<input type="text"/>
-------------------------------------	----------------------

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

Adresgegevens nieuwe certificaatbeheerder

Organisatiename

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

Land*

Nederland



Postcode*

3072AP

Plaats*

Rotterdam

Straatnaam*

Wilhelminakade

Huisnummer*

123

Huisnummer toevoeging

Optioneel, bijv. a, b, c

De brief met daarop de intrekcode van het certificaat wordt naar het opgegeven adres van de certificaatbeheerder gestuurd.

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 de naam van die organisatie (ICT dienstverlener) op te geven.

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 aanpassen.

- Vul de persoonsgegevens in van de beoogde Certificaatbeheerder.
- Indien van toepassing: vul de organisatiename in.
- Indien van toepassing: pas de adresgegevens van de certificaatbeheerder aan.

Optie 2: Een reeds geïdentificeerde 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 waarna de volgende invoervelden verschijnen.

Reeds geregistreeerde certificaatbeheerder

Achternaam*

Achternaam conform identiteitsbewijs

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*

Bijv. CB1234567

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

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 e-mailadres 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.

Invulinstructie en toelichting sectie 3: Certificaat

In deze sectie dient u gegevens in te vullen die daadwerkelijk in het certificaat komen te staan. Deze sectie bestaat uit de volgende blokken die hierna in detail aan de orde komen:

1. Type servercertificaat (*informatief, read-only*)
2. Certificate Signing Request (*in te voeren door contactpersoon*)
3. CSR Gegevens op te nemen in servercertificaat (*automatisch itgelezen uit CSR, read-only*)

Type servercertificaat

Het eerste blok geeft aan welk type servercertificaat u aanvraagt.

Type servercertificaat	
De aanvraag betreft een	certsign_ov_ssl
Geldigheidsduur*	<input checked="" type="radio"/> 1 jaar

Dit is alleen te wijzigen door vanaf <https://certificaat.kpn.com/aanvragen/servercertificaten/> de aanvraag te starten. Zie ook par. 2.2 onder kopje Type certificaat.

Momenteel is er (naast PKIoverheid servercertificaten) maar 1 optie mogelijk en dat is een certSIGN OV SSL servercertificaat met een geldigheidsduur van 1 jaar.

Certificate Signing Request:

Het Certificate Signing Request (CSR) bevat het publieke gedeelte van het sleutelpaar en de identificerende gegevens van de server/service en is bij voorkeur op de server gegenereerd waarop uiteindelijk het certificaat komt te staan.

Certificate Signing Request

Het is noodzakelijk dat de CSR alle gegevens bevat die in het certificaat worden opgenomen en dat de organisatiernaam, vestigingsplaats en provincie overeenkomen met de KvK registratie van uw organisatie.

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

Plak hier uw CSR. LET OP: Gebruik hiervoor GEEN tekstverwerker zoals Microsoft Word maar een tekstverwerker die geen opmaak codes toevoegt zoals Notepad (Kladblok)!

Certificate Signing Request*

Het is noodzakelijk dat de CSR alle gegevens bevat die in het certificaat worden opgenomen en dat de organisatiernaam, vestigingsplaats en provincie overeenkomen met de KvK registratie van uw organisatie.

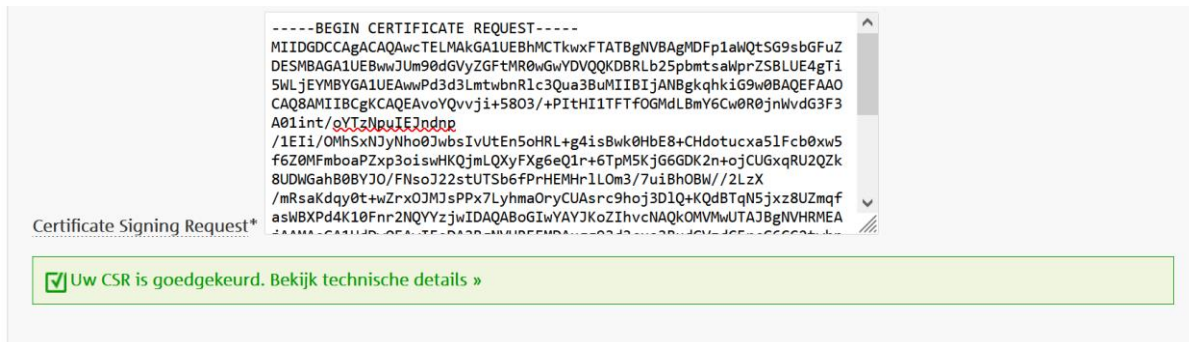
Verder dient u voor ieder servercertificaat een andere CSR aan te leveren dat gebaseerd is op een uniek sleutelpaar. Dit sleutelpaar dient uitsluitend gebruikt te worden voor de betreffende service!

Zie voor een toelichting over het genereren van een CSR en de eisen die daaraan zijn gesteld:

<https://certificaat.kpn.com/aanvragen/servercertificaten/csr-genereren/>

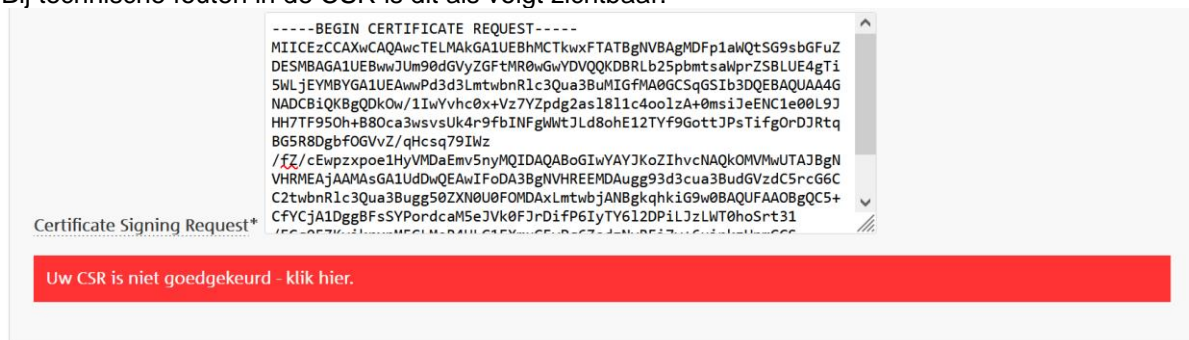
- Plak de CSR in het formulier. LET OP: GEBRUIK HIERVOOR NOOIT EEN PROGRAMMA ALS MS-WORD MAAR GEBRUIK HET KLADBLOK (NOTEPAD).
- Er vindt controle plaats of het CSR technisch voldoet.

Als de CSR technisch correct is verschijnt de volgende melding:



Bij klikken op *Bekijk technische details* krijgt u een pop-up scherm te zien met de uitgevoerde controles.

Bij technische fouten in de CSR is dit als volgt zichtbaar.



Het detailscherm geeft in dat geval aan welke technische controles niet succesvol zijn uitgevoerd.

CSR Gegevens op te nemen in servercertificaat

Deze read-only sectie van het scherm laat alle gegevens zien die in de CSR zijn opgenomen.

CSR gegevens op te nemen in servercertificaat	
Organisatiennaam (O)*	Koninklijke KPN N.V.
Land:*	NL
Provincie/staat:*	Zuid-Holland
Plaatsnaam:*	Rotterdam
Naam van de service (CN)*	www.kpntest.kpn
Subject Alternative Names:	www.kpntest.kpn, kpntest.kpn, testSAN001.kpn (3)

- Organisatiennaam dient de statutaire naam of een geregistreerde handelsnaam te zijn.
- Land, Provincie/staat en Plaatsnaam zullen worden vergeleken met de gegevens die bij de KvK zijn opgehaald op basis van het KvK nummer dat u heeft ingegeven bij de Abonneegegevens.

- De Naam van de service (CN) dient een zogenaamde FQDN te zijn. Een uitgebreide technische toelichting over FQDN vindt u hier:
<https://certificaat.kpn.com/aanvragen/servercertificaten/fqdn-naam-van-de-service/>
- Subject Alternative Names (SAN). U kunt tegen meerprijs maximaal 10 additionele namen opnemen in het servercertificaat door deze op te nemen in het CSR bestand. Alle additionele namen zijn zichtbaar bij de CSR Gegevens op te nemen in servercertificaat. Indien in de CSR een SAN is opgenomen die gelijk is aan de ingevulde Naam van de service (Common Name), 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. Op de PDF zijn alleen de additionele SAN's opgenomen die tegen meerprijs in het servercertificaat worden opgenomen.

2.4 Scherm 2: Controleren en bestellen

Dit scherm is bedoeld voor controle van de ingevoerde gegevens, vereist een akkoord met de voorwaarden en biedt de optie om een PO / Referentienummer op te geven voor de facturatie.

Invulinstructie en toelichting sectie 2: Certificaatbeheerder

In deze sectie ziet u een overzicht van alle ingevoerde gegevens ter controle en kunt u indien nodig nog gegevens wijzigen.

certSIGN OV SSL servercertificaat

1. Aanvraag 2. Controleren en Bestellen 3. Afronding

Controleren

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

Certificaatbeheerder

De certificaatbeheerder is volledig nieuw

Volledige voornaam	Johannes Gerardus
Tussenvoegsel	van het
Achternaam	Certificaatbeheer
E-mail Certificaatbeheerder	beheerder@organisatie.nl
Organisatiennaam	-
Postcode	3072AP
Plaats	Rotterdam

Type servercertificaat

De aanvraag betreft een	certSIGN OV SSL servercertificaat
Geldigheidsduur	1 jaar

CSR Gegevens op te nemen in 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.

Naam van de Service	www.kpntest.kpn
Organisatiennaam	Koninklijke KPN N.V.
Plaats	Rotterdam
Provincie	Zuid-Holland
Land	NL

SUBJECT ALTERNATIVE NAMES (SAN)

Subject Alternative Name 1	kpntest.kpn
Subject Alternative Name 2	testSAN001.kpn

NIET GEFACTUREERDE SUBJECT ALTERNATIVE NAMES (SAN)

Subject Alternative Name	www.kpntest.kpn
--------------------------	-----------------

De SHA256 fingerprint van uw CSR is: d179fc990f1bcc233ef1378c448e0db2d09d81a4ff72fd836606a5523c7b3e7

[Wijzig](#)

- Controleer uw gegevens.
- Klik op 'Wijzig' om gegevens aan te passen.

Sectie 2: Voorwaarden

Deze sectie vraagt expliciet om een akkoord op de voorwaarden die van toepassing zijn:

Voorwaarden

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

- Ik ben akkoord met de [KPN Algemene Leveringsvoorwaarden](#) en het [certSIGN Web CA OV - Certification Practice Statement](#).
- 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](#).
- Ik ben akkoord dat de certificaten worden gepubliceerd in de KPN online certificaten database en openbare transparency logs.
- Het **sleutel**materiaal van het Servercertificaat is gegenereerd en wordt bewaard in een Veilige Omgeving.
- Ik verklaar dat de **domeinnaam**(*) ten behoeve waarvan een Servercertificaat wordt aangevraagd onder mijn controle is, en dat ik dat kan aantonen door het toevoegen van een nog te ontvangen code aan het DNS TXT record.
() Dit is inclusief alle eventueel gebruikte additionele SAN's.*

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

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

- Akkoord met de *KPN Algemene Leveringsvoorwaarden*¹ en het *certSIGN Web CA OV - Certification Practice Statement*². 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;
 - Bij de aanvraag gaat u akkoord met de *kosten* die KPN in rekening zal brengen voor een certSIGN servercertificaat³;
 - 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.
- Vink de checkbox aan dat alle gegevens volledig, juist en naar waarheid zijn ingevuld.

¹ Zie <https://www.kpn.com/algemeen/algemene-voorwaarden/zakelijk/algemeen.htm>

² Zie <https://www.certsig.ro/en/repository/>

³ Zie <https://certificaat.kpn.com/pkioverheidcertificaten/tarieven/>

Sectie 3: Facturatie

Optioneel kan u hier een PO / Referentienummer opgeven. Deze referentie komt als PO nummer terug op de factuur die u van KPN ontvangt. U kunt dit gebruiken om de factuur te relateren aan uw eigen administratie.

Facturatie	
PO / Referentienummer	<input type="text"/>
<p><i>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.</i></p> <p>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.</p> <p>Facturatie zal plaatsvinden op basis van de betalingsgegevens die zijn vastgelegd in de abonneeregistratie.</p>	

Verzend Aanvraag

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

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.

3 Scherm 3: Afronding


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

Aanvraag verzonden

Betreft aanvraag certSIGN OV SSL servercertificaat

Referentie: S20220411677670255

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 certSIGN OV SSL 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 PKI-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.

3.1 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 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 persoonsgebonden PKI-overheid 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-mail programma's zoals Microsoft Outlook of Mozilla Thunderbird.

3.2 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 B.V.
t.a.v. PKI-Validatie
Postbus 9105
7300 HN APELDOORN

4 Beoordeling aanvraag door KPN en vervolg

KPN zal de aanvraag in behandeling nemen zodra het ondertekende aanvraagformulier -of de bestelling vanuit MijnCertificaten- is ontvangen. De belangrijkste stappen die de doorlooptijd bepalen zijn hieronder nader toegelicht. Zie voor een compleet overzicht van de stappen de procesbeschrijving in par. 2.1.

4.1 Controle Abonneeregistratie

KPN zal de gegevens van de abonnee en contactpersoon controleren. Dit is zoveel mogelijk geautomatiseerd in het webformulier.

4.2 Identificatie Certificaatbeheerder

KPN zal de Certificaatbeheerder identificeren indien dat nog niet eerder is gedaan. Hiervoor zal de Certificaatbeheerder per email een uitnodiging ontvangen van AMP. Een koerier van AMP voert deze identificatie in opdracht van KPN uit op locatie van de klant.

Na identificatie ontvangt de Certificaatbeheerder een bevestiging van de registratie en een identificatienummer dat bij volgende aanvragen te gebruiken is.

4.3 Domeinvalidatie

Een belangrijke controle 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 zogenaamde 'domeinvalidatie' of 'domein controle'.

certSIGN stuurt daarvoor een e-mailbericht naar de Contactpersoon. De IT beheerorganisatie van het betreffende domein voert de wijzigingen door die de zeggenschap over het domein aantonen.

Hiervoor dient men een random code in een DNS TXT record toe te voegen.

Indien nodig autoriseert men certSIGN om voor het domein een certificaat uit te geven door "certsign.ro" toe te voegen in een DNS CAA record.

Deze stappen zijn nader toegelicht in de toegestuurde e-mailberichten en op de pagina <https://certificaat.kpn.com/aanvragen/servercertificaten/domein-controle/>.

certSIGN checkt automatisch of de aanpassingen zijn doorgevoerd.

4.4 Uitgifte en gebruik

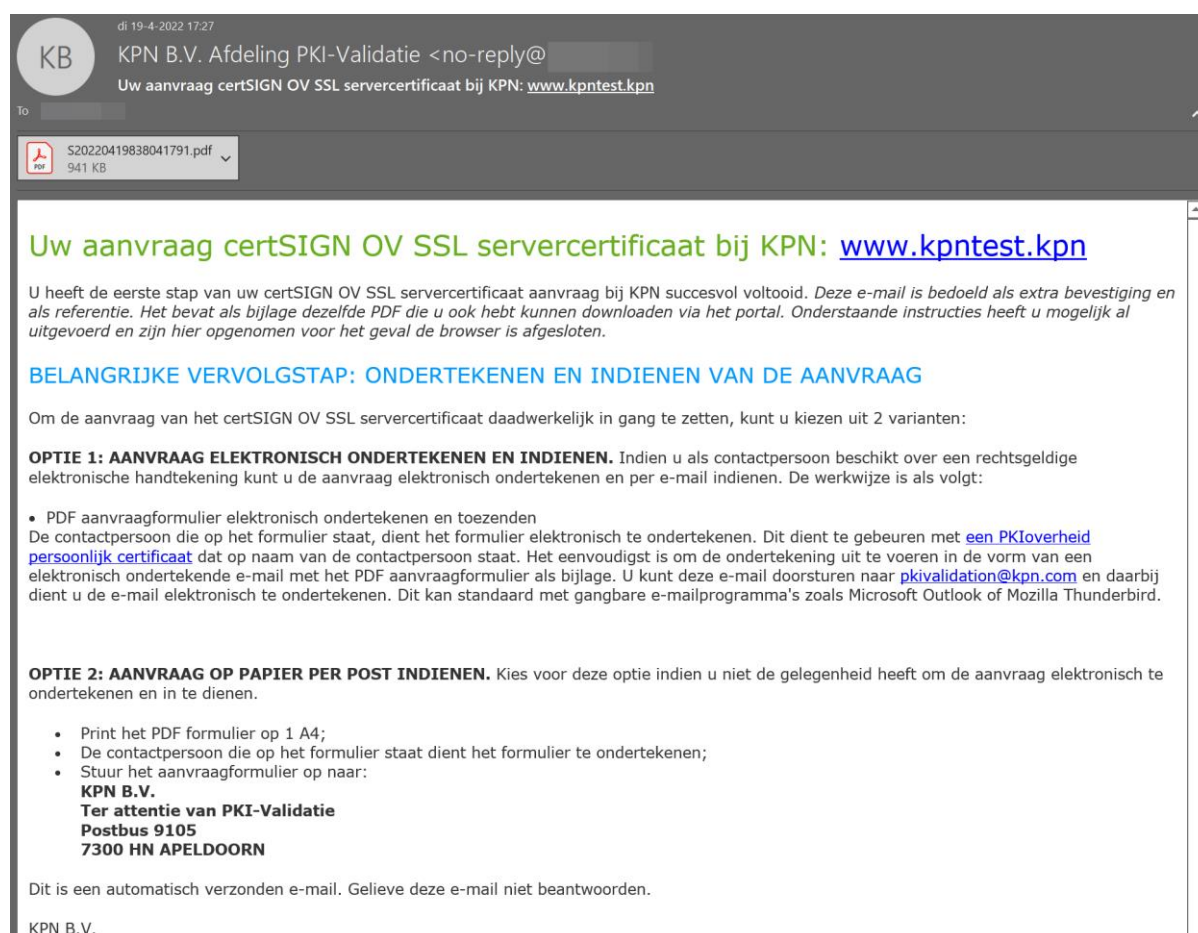
Na succesvolle domeinvalidatie zal certSIGN het certificaat produceren en KPN zal het certificaat per e-mail versturen naar de Certificaatbeheerder en de Contactpersoon. De Certificaatbeheerder ontvangt per brief een intrekingscode. U dient het Servercertificaat pas te gebruiken als de Certificaatbeheerder de intrekingscode per brief heeft ontvangen.

5 BIJLAGEN: e-mail en PDF formulier

Voor de volledigheid bevat deze bijlage de e-mail en het PDF formulier die de aanvrager per e-mail ontvangt.

5.1 E-mailbericht afronding


Na afronding van het webformulier ontvangt de aanvrager op het gevalideerde e-mailadres de volgende e-mail. 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.



di 19-4-2022 17:27

KB KPN B.V. Afdeling PKI-Validatie <no-reply@kpn.nl>
Uw aanvraag certSIGN OV SSL servercertificaat bij KPN: [www.kpntest.kpn](http://www.kpntest.kpn.nl)

To: [Redacted]

 S20220419838041791.pdf
941 KB

Uw aanvraag certSIGN OV SSL servercertificaat bij KPN: [www.kpntest.kpn](http://www.kpntest.kpn.nl)

U heeft de eerste stap van uw certSIGN OV SSL 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 certSIGN OV SSL 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 PKI-overheid 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.

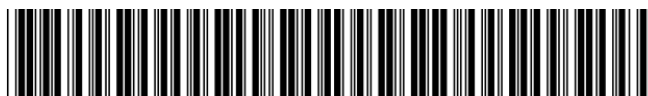
- Print het PDF formulier op 1 A4;
- De contactpersoon die op het formulier staat dient het formulier te ondertekenen;
- Stuur het aanvraagformulier op naar:
KPN B.V.
Ter attentie van PKI-Validatie
Postbus 9105
7300 HN APELDOORN

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

KPN B.V.

5.2 PDF Aanvraag Servercertificaat

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



S20220502100324972

KPN - Aanvraag certSIGN OV SSL servercertificaat

Referentie: S20220502100324972

Gegevens Abonnee en Contactpersoon

Abonneenummer: P1470329 Handelsnaam volgens KvK: Koninklijke KPN N.V.
Achternaam Contactpersoon: Aanvraeger E-mail: [REDACTED]

Certificaatbeheerder

De certificaatbeheerder is: 1. volledig nieuw Registratienummer:
Voornaam: Johannes Gerardus Geboorteplaats: Apeldoorn
Tussenvoegsel: van het E-mail: beheerder@organisatie.nl
Achternaam: Certificaatbeheer (Mobiel) telefoonnummer: 0606060606
Geboren: 01-12-1971
Organisatiename:
Adresgegevens: Wilhelminakade 123, 3072AP Rotterdam, Nederland

Gegevens voor Servercertificaat

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

Naam van de Service (CN): www.kpntest.kpn
Organisatiename (O): Koninklijke KPN N.V.
Plaats (L): Rotterdam
Provincie (S): Zuid-Holland
Land (C): NL
Subject Alternative Names: kpntest.kpn, testSAN001.kpn
SHA256 fingerprint van CSR: d179fc990f1bcca233ef1378c448e0db2d09d81a4ff72fd836606a5523c7b3e7

Overige gegevens

Geldigheidsduur: 1 jaar
Type aanvraag: initieel
Referentie tbv facturatie: Mijn PO nummer 001

Akkoordverklaringen

Ondergetekende verklaart namens Abonnee:

- dat alle gegevens volledig, juist en naar waarheid zijn ingevuld.
- akkoord met KPN Algemene Leveringsvoorwaarden en certSIGN Web CA OV - CPS.
- dat opgegeven Certificaatbeheerder geïnformeerd, bevoegd en ter zake kundig is om namens abonnee Servercertificaten te installeren, beheren en in te trekken.
- dat het sleutel materiaal is gegenereerd en wordt bewaard in een Veilige Omgeving.
- akkoord te zijn met de tarieven.
- akkoord te zijn dat de certificaten worden gepubliceerd in de KPN online certificaten database en transparancy logs.
- dat de domeinnaam ten behoeve waarvan een Servercertificaat wordt aangevraagd onder de directe verantwoordelijkheid (blijft) vallen van de Abonnee of verklaart geautoriseerd te zijn om een domeinnaam van een andere organisatie te gebruiken.

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 PKI-Validatie

Postbus 9105 , 7300 HN APELDOORN

Handtekening Contactpersoon

Aanvraeger Geb. 01-12-1971

Datum:	
Plaats:	
Handtekening:	