Datum:
27 aug. 2020
Auteur:
KPN Security
Versie:
release 7.3

Handleiding

KPN PKIoverheid
Toelichting aanvraag servercertificaat (alle typen)

Inhoudsopgave

1 Inleiding

Dit document bevat een toelichting op de aanvraag van een PKIoverheid 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 PKIoverheid servercertificaat aan namens een geregistreerde Abonnee van de PKIoverheid 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 PKIoverheid 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 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 Groepscertificaat 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 PKIoverheid 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 (PKIoverheid of PKIO): De gehele PKI infrastructuur die door de Policy Authority (PA) PKIoverheid wordt beheerd. De PA PKIoverheid 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

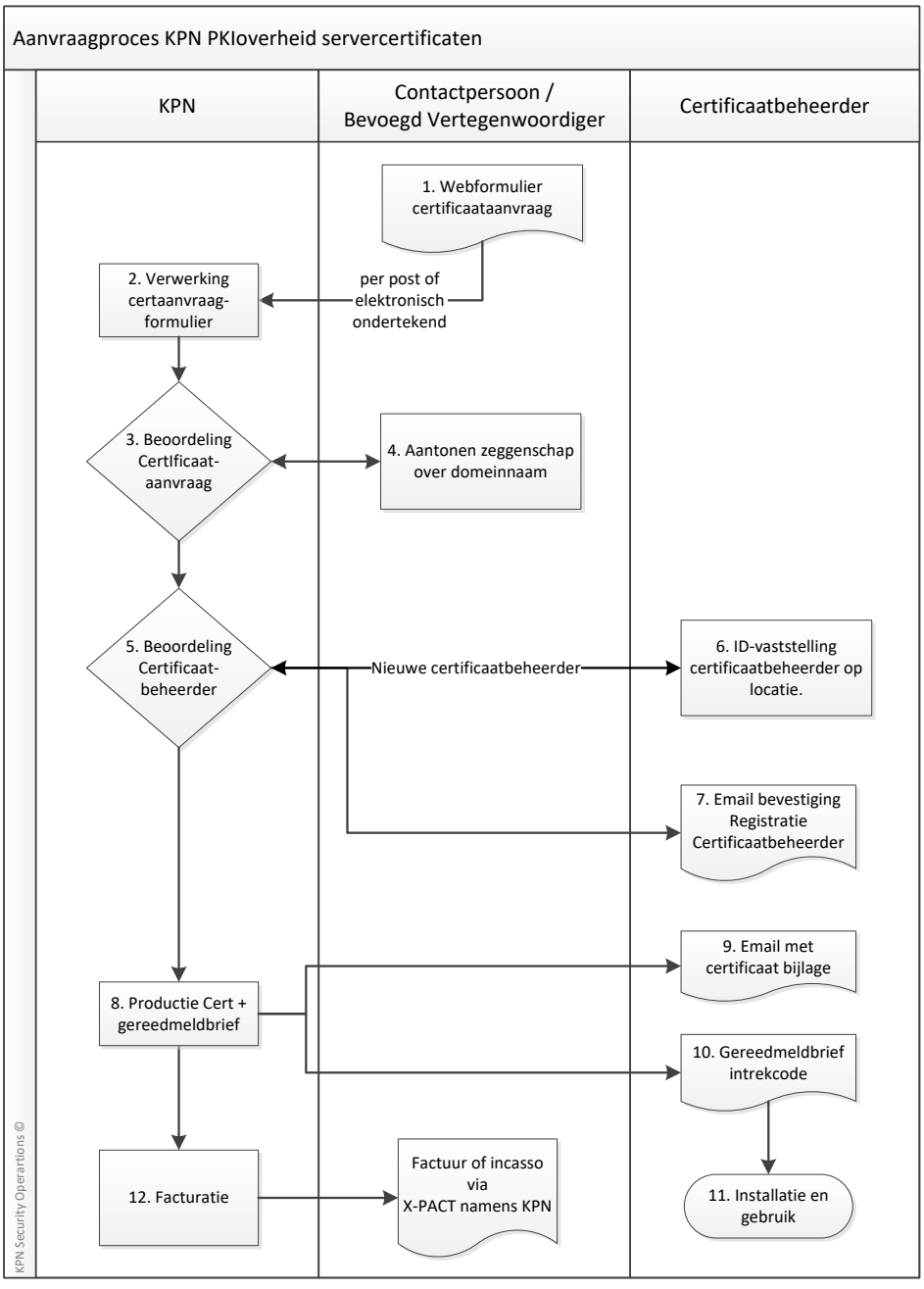
Voor meer informatie over de PKI voor de overheid en de Certificatiedienstverlening van KPN verwijzen wij u naar:

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 hoofstukken.

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.

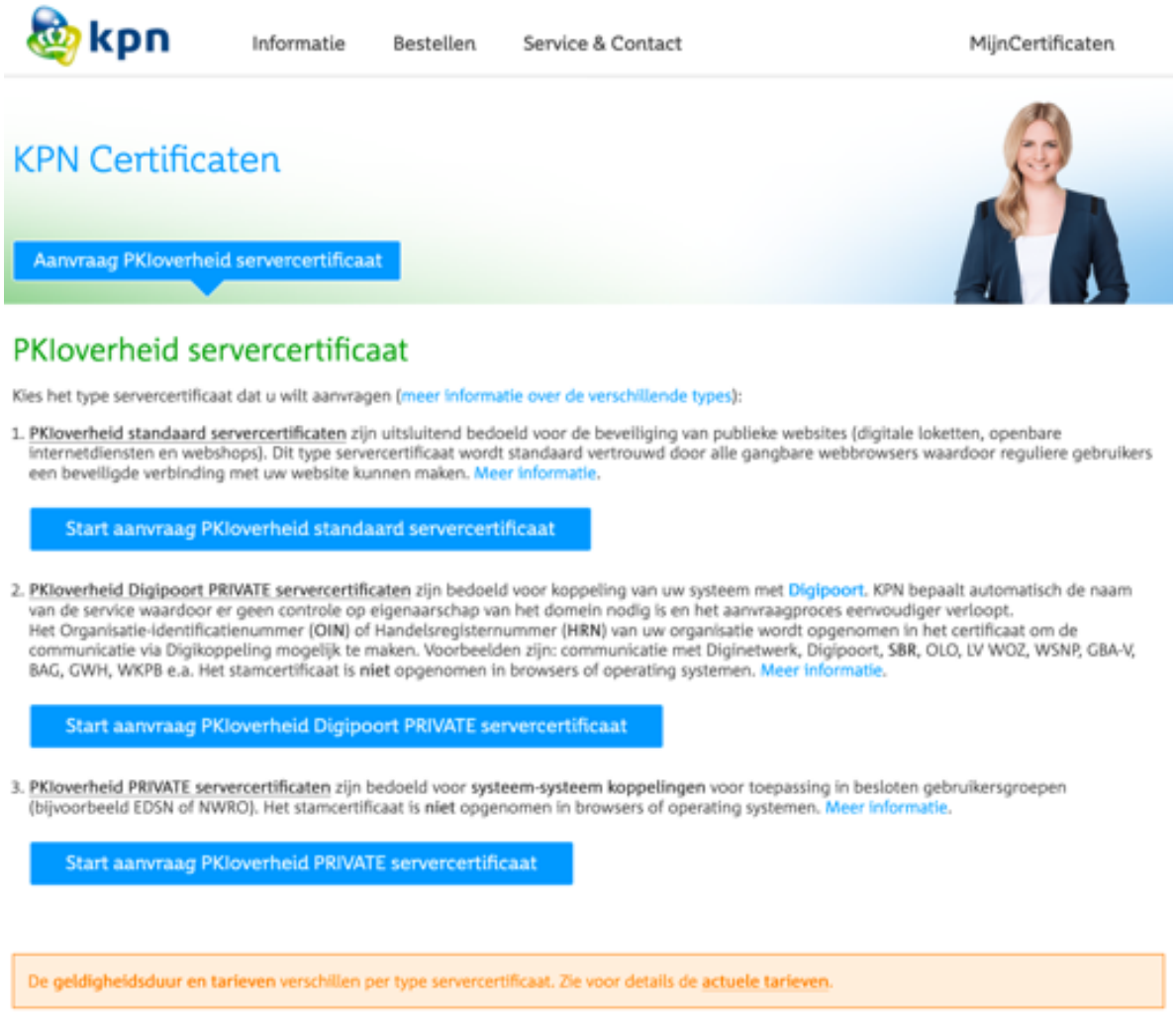
12. Tot slot ontvangt de Abonnee op het opgegeven facturatieadres een factuur.

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

3 Servercertificaataanvraag zonder KPN Self Service Portaal

3.1 Keuzescherm voor het type servercertificaat

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



Met de blauwe knoppen kiest u het type servercertificaat dat u wilt aanvragen met een korte toelichting. Indien u al weet welk type uw 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 doorlopen[2]. 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.

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 PKIoverheid abonnee bij KPN geregistreerd. De bevoegd vertegenwoordiger heeft bij de bevestiging hiervan een *PKIoverheid 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 PKIoverheid Abonneeregistratie;
c. U beschikt over een *Certificate Signing Request* (CSR) gebaseerd op een uniek sleutelpaar. 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:

U ontvangt vervolgens een email waarmee KPN uw emailadres verifieert.

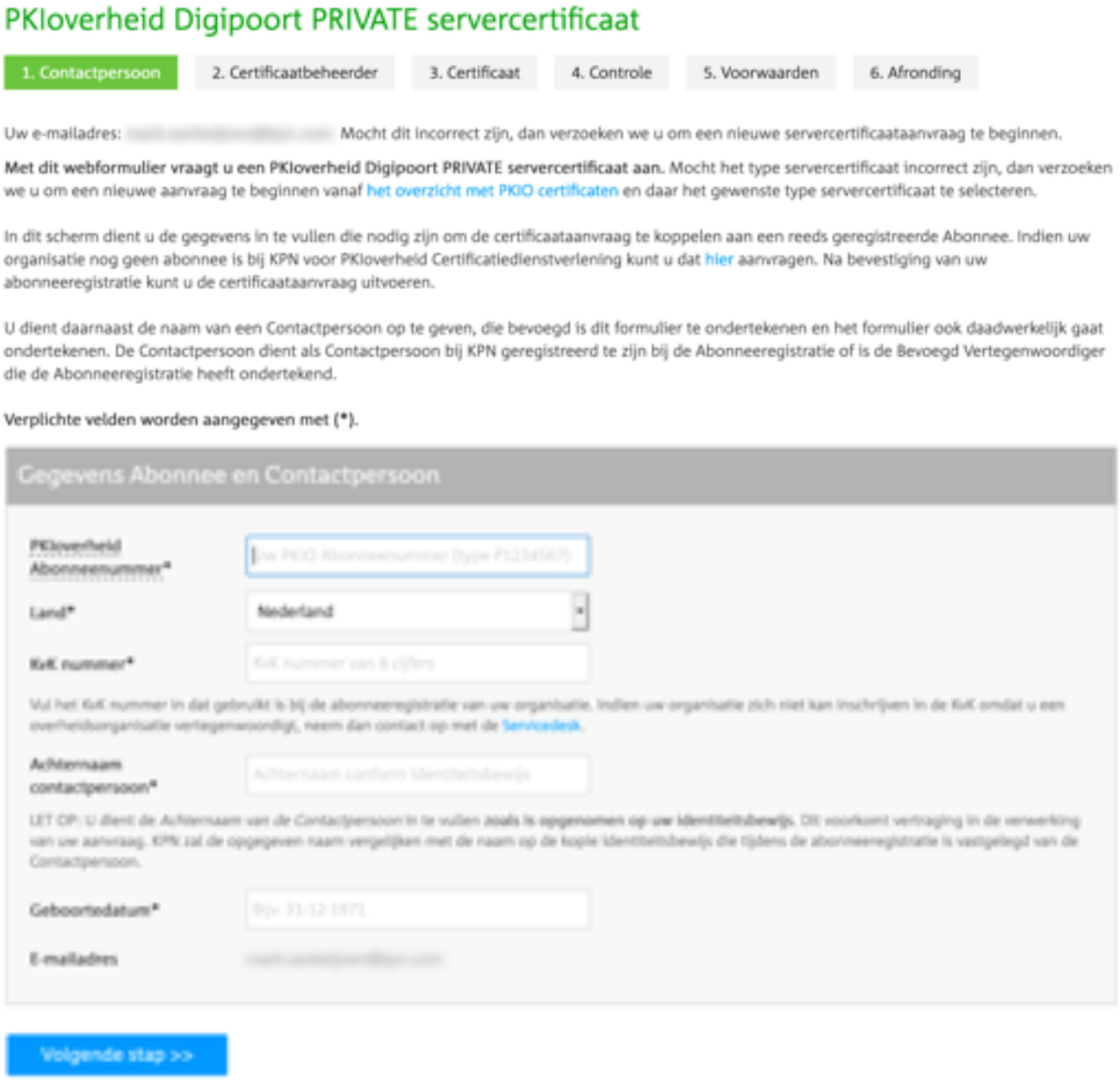
- Klik op de link in de email om het aanvraagformulier voor uw servercertificaat te starten.

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.

3.3 Scherm 1: Contactpersoon

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

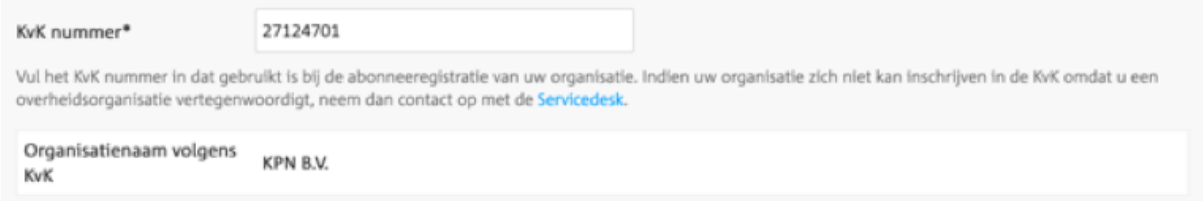


Invulinstructie en toelichting scherm 1. Contactpersoon

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 Organisatienaam en overige publieke KvK gegevens op. Als dat succesvol verloopt ziet u de handelsnaam zoals hieronder is geïllustreerd met het KvK nummer van KPN.



en verschijnt de volgende toelichting:

- 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 >>

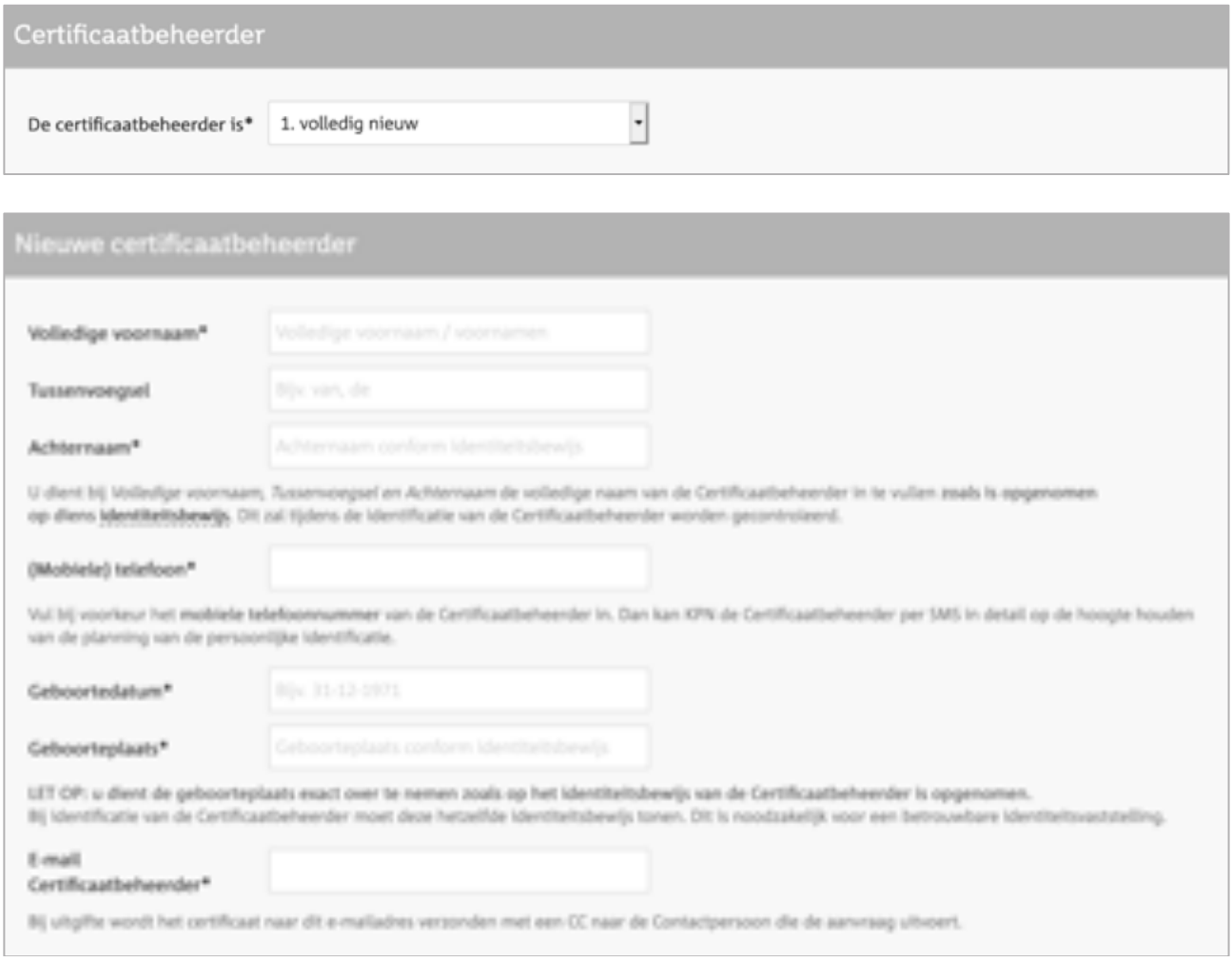
3.4 Scherm 2: Certificaatbeheerder

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

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 Certificaat-beheerder zijn voor meerdere Abonnees.

Optie 1 Certificaatbeheerder is volledig nieuw



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.

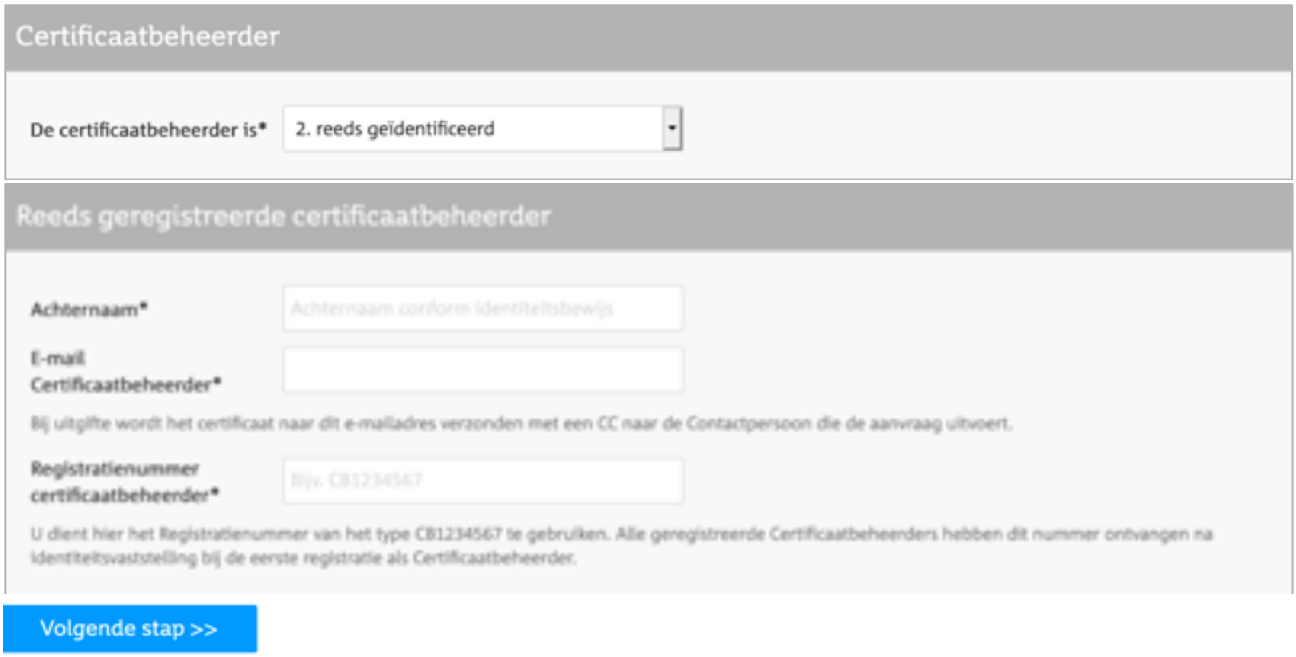
- Vul de persoonsgegevens in van de beoogde Certificaatbeheerder.
  - Naam;
  - Telefoonnummer;
  - Geboortedatum en -plaats;
  - Emailadres.

- Indien van toepassing: vul de organisatienaam 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



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 certificaatbeheerdernummer (‘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.

Invulinstructie en toelichting 3. Certificaat 1e gedeelte: Type servercertificaat

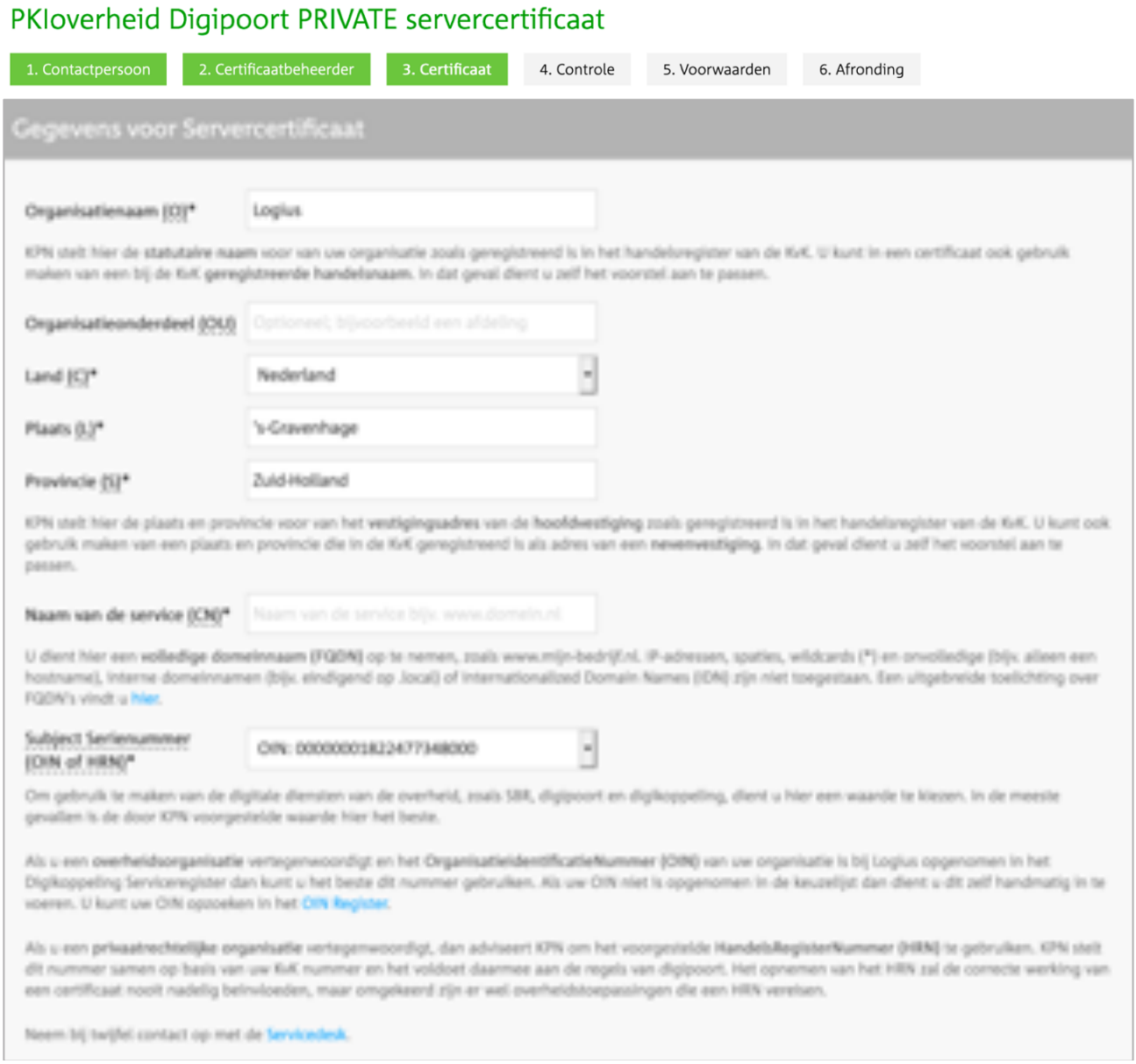
Het eerste blok geeft als eerste het type servercertificaat u aanvraagt weer. Dit is alleen te wijzigen door via de website https://certificaat.kpn.com/aanvragen/servercertificaten/ een nieuwe aanvraag te starten of vanaf het Keuzescherm voor het type servercertificaat (zie paragraaf 3.1).

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 certificaattype bestaan er kleine verschillen in de invoervelden van dit scherm en de volgende schermen.



Invulinstructie en toelichting 3. Certificaat 2e 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 (Organisatienaam, Plaats en Provincie).

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

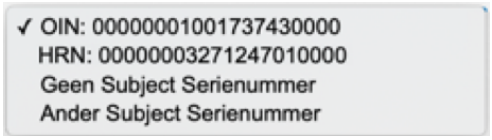
- Vul eventueel een afdelingsnaam in.

- 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 keuzescherm biedt u verder de volgende mogelijkheden[3]:

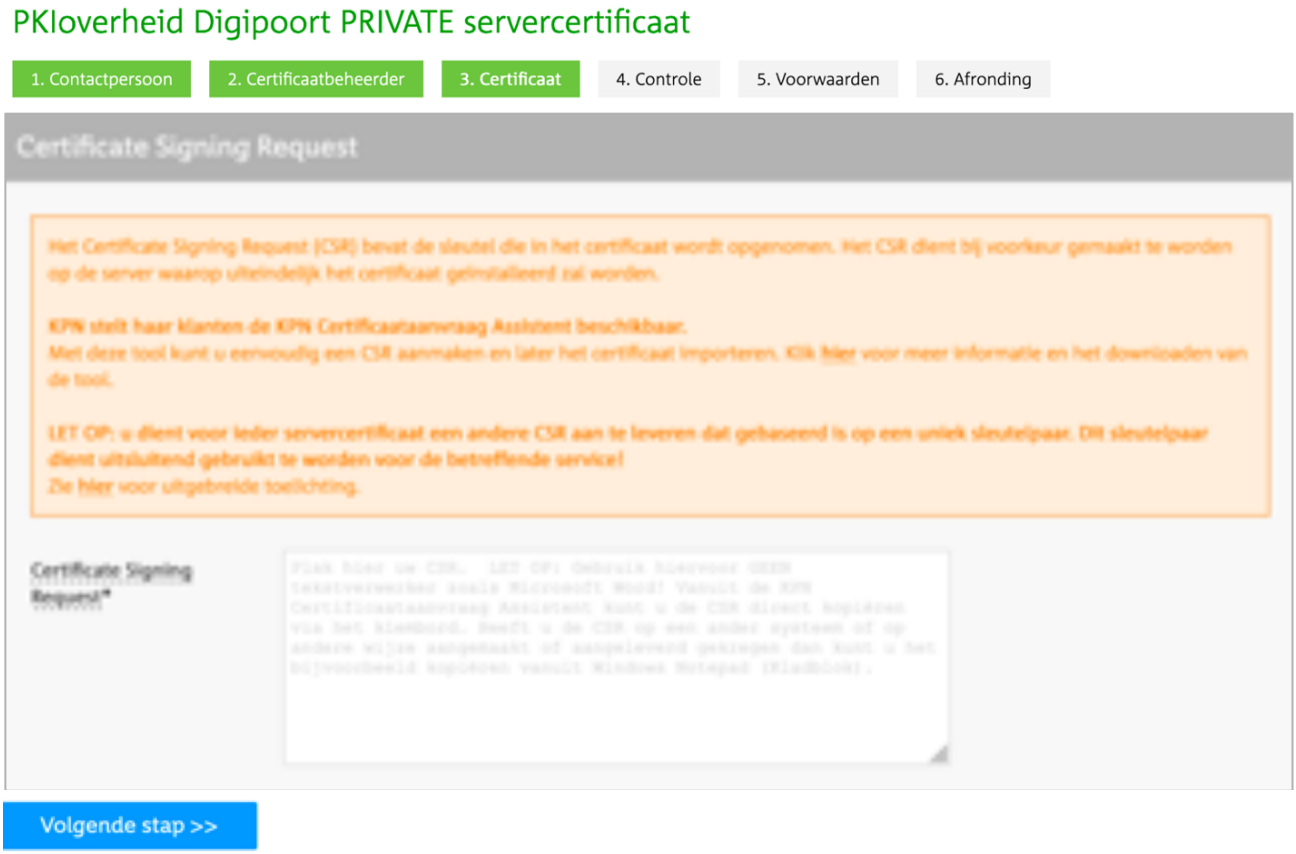
  

  Als u kiest voor 'Ander Subject Serienummer' dan krijgt u een leeg veld waarin u een 20-cijferig nummer kunt invoeren. KPN zal een ingevoerd nummer altijd controleren.

  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.



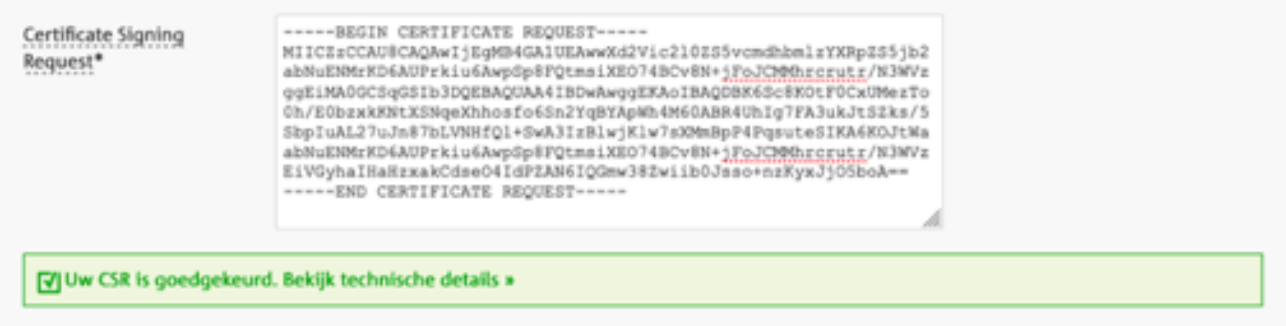
Invulinstructie en toelichting 3. Certificaat 3e gedeelte: Certificate Signing Request

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]

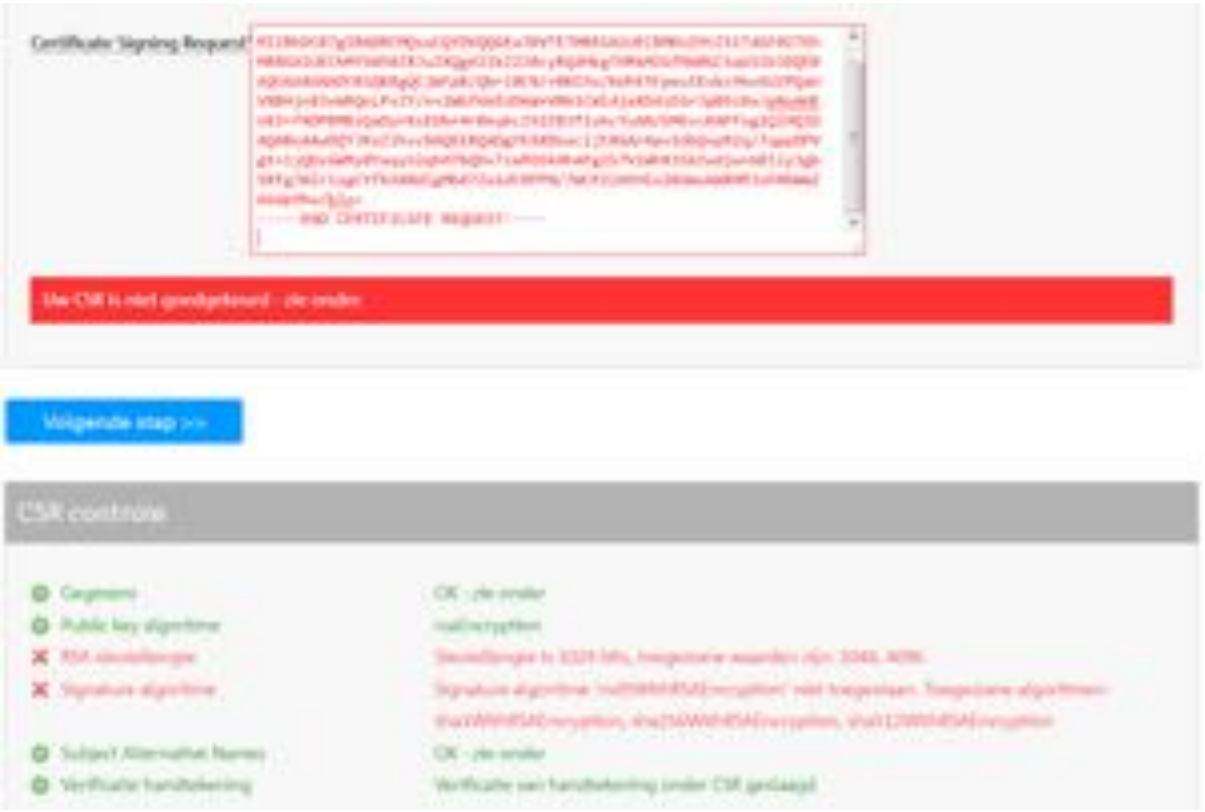
- Plak het CSR in het formulier. **LET OP: GEBRUIK HIERVOOR NOOIT EEN PROGRAMMA ALS MICROSOFT WORD MAAR GEBRUIK HET KLADBLOK (NOTEPAD).**
- Er vindt een controle plaats of het CSR technisch voldoet.

[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:



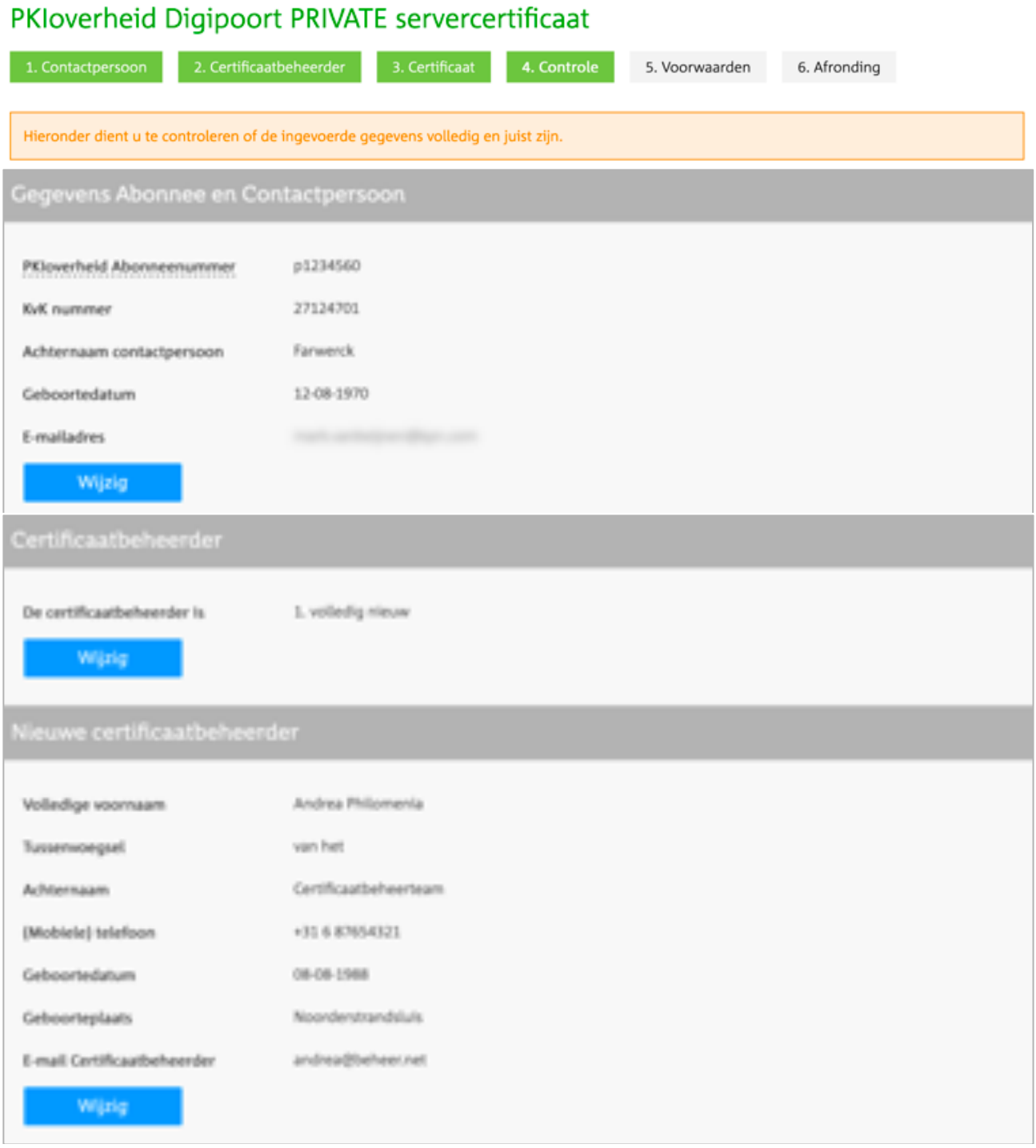
Extra naam in een PKIoverheid server certificaat (SAN / Subject Alternative Name)
U kunt tegen meerprijs maximaal 10 extra namen op laten nemen in het servercertificaat door deze aan het CSR-bestand toe te voegen[5]. Eventuele additionele namen zijn zichtbaar als u de technische details van de CSR bekijkt 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.

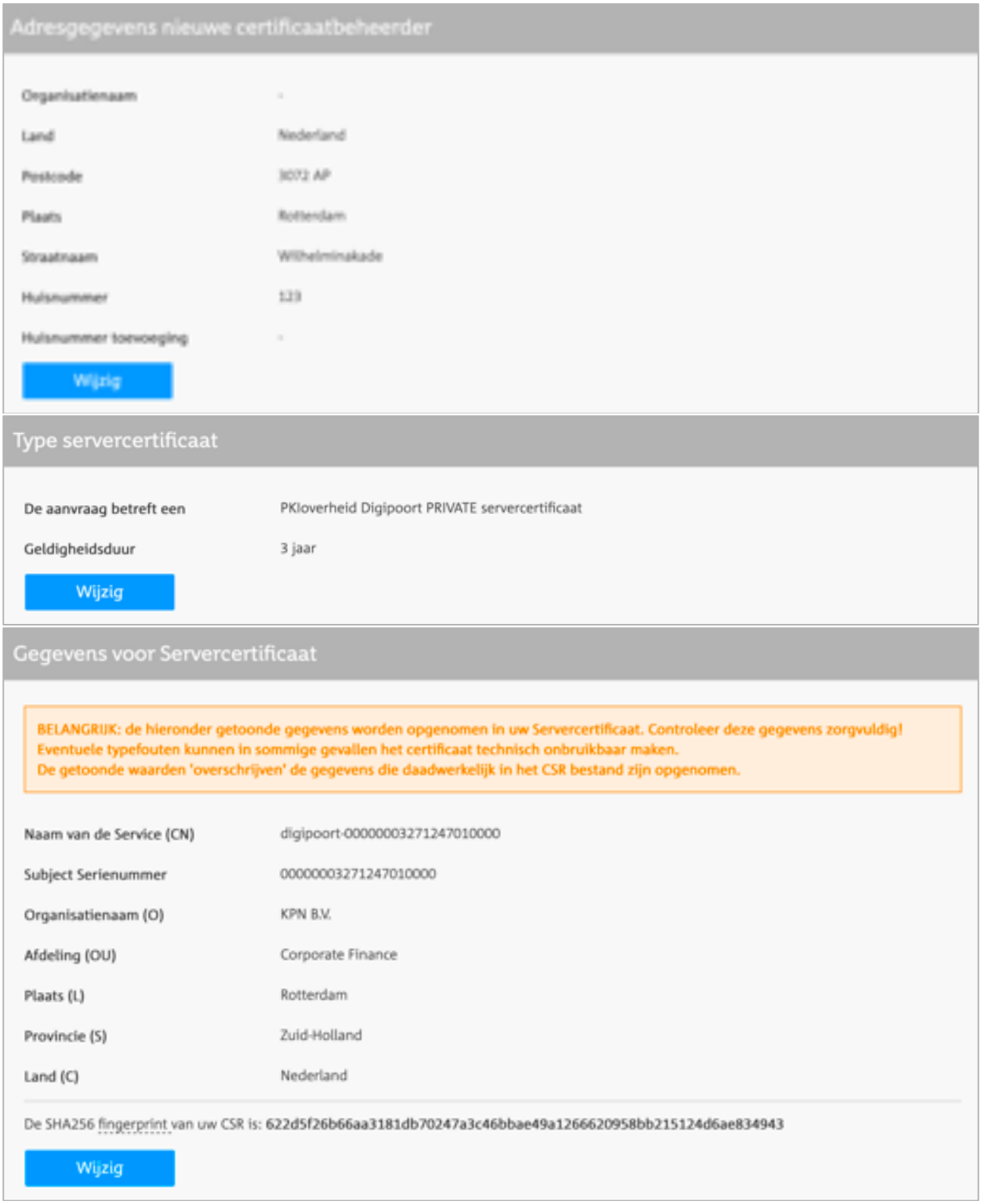
[5] Het toevoegen van extra namen is niet beschikbaar als u gebruik maakt van de certificaat aanvraag assistent. Uw systeembeheerder is in staat om een CSR aan te maken met daarin de extra namen.

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.



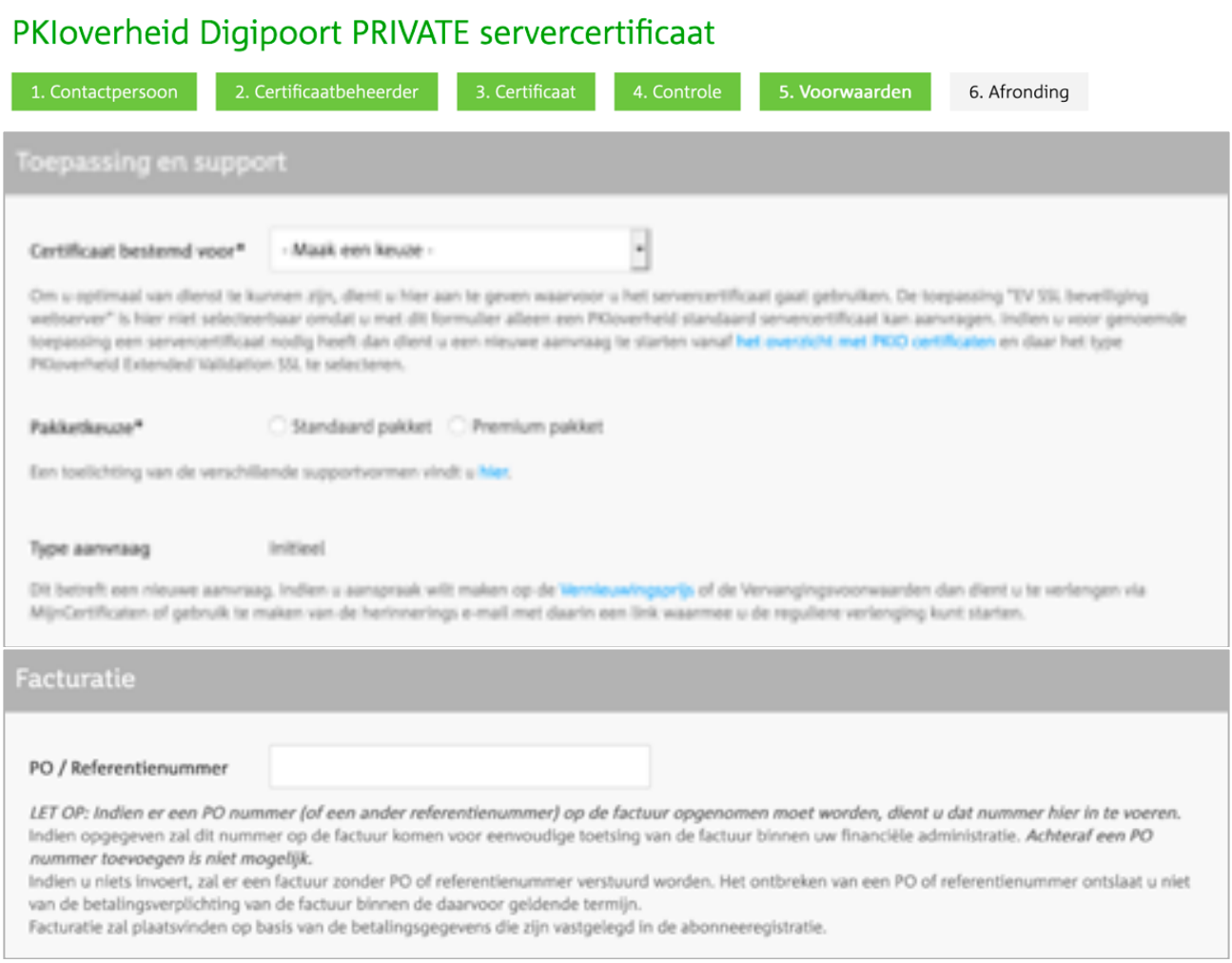

Adresgegevens nieuwe certificaatbeheerder
Organisatienaam
Land
Nederland
Postcode
3072 AP
Plaats
Rotterdam
Straatnaam
Wilhelminakade
Huisnummer
123
Huisnummer toevoeging
Wijzig
Type servercertificaat
De aanvraag betreft een
PKIoverheid Digipoort PRIVATE servercertificaat
Geldigheidsduur
3 jaar
Wijzig
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
Organisatienaam (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:



De gegevens bestaan uit drie blokken:

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

<u>Voorwaarden</u>

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 Servercertificaat[8];
- 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 Verzend Aanvraag

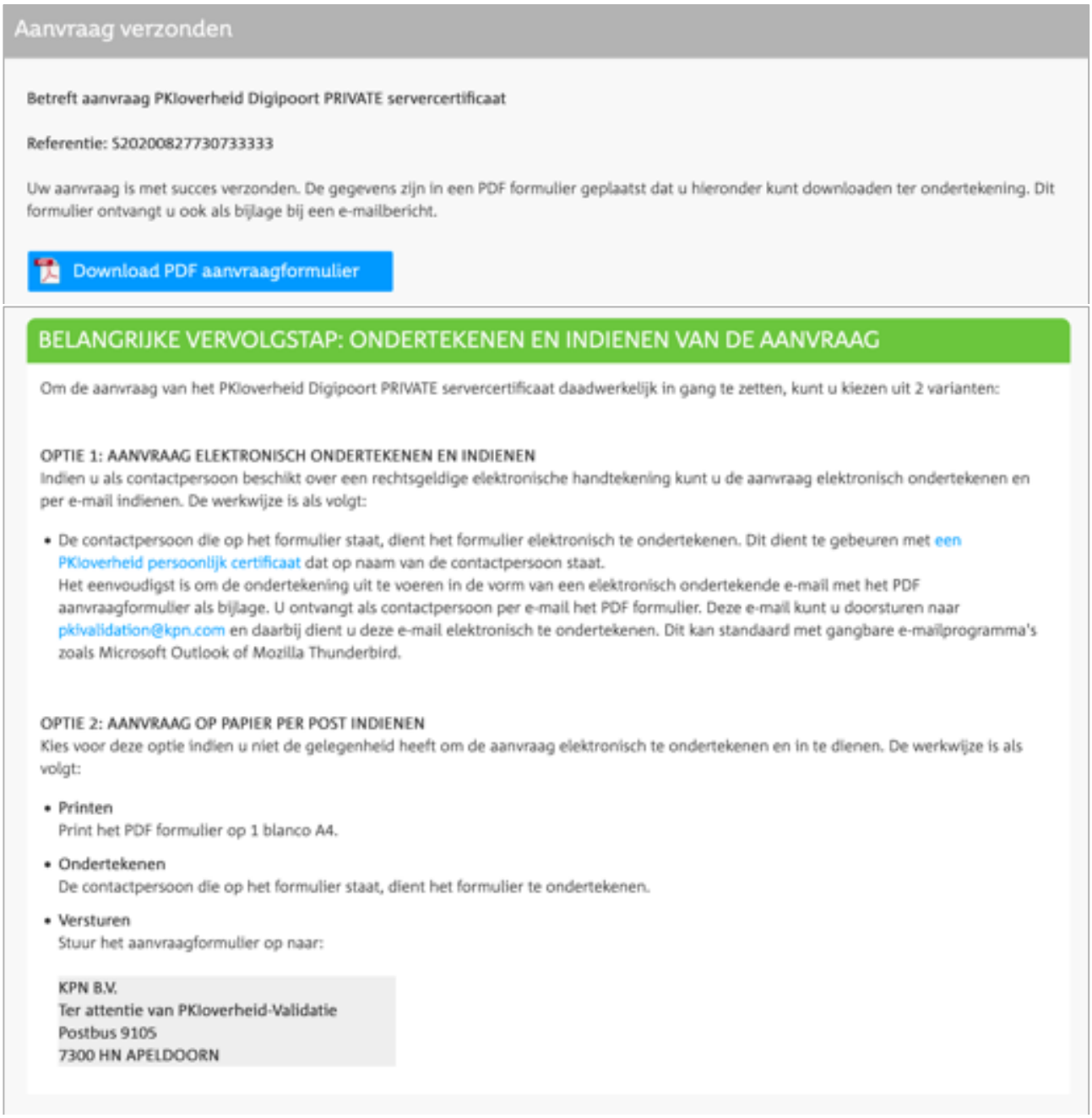
BELANGRIJK: hoewel KPN na het verzenden van de aanvraag de digitale gegevens heeft, dient de Contactpersoon die op het PDF formulier staat vermeld de afgedrukte aanvraag te ondertekenen en dient het formulier voorzien van eventuele bijlage per post opgestuurd te worden. Dit is verder uitgewerkt in Hoofdstuk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

[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



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 PKIoverheid 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 pkivalidation@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:

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:

Kies de knop Servercertificaten bovenaan de pagina om het scherm met een overzicht van alle server-certificaten 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:

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.

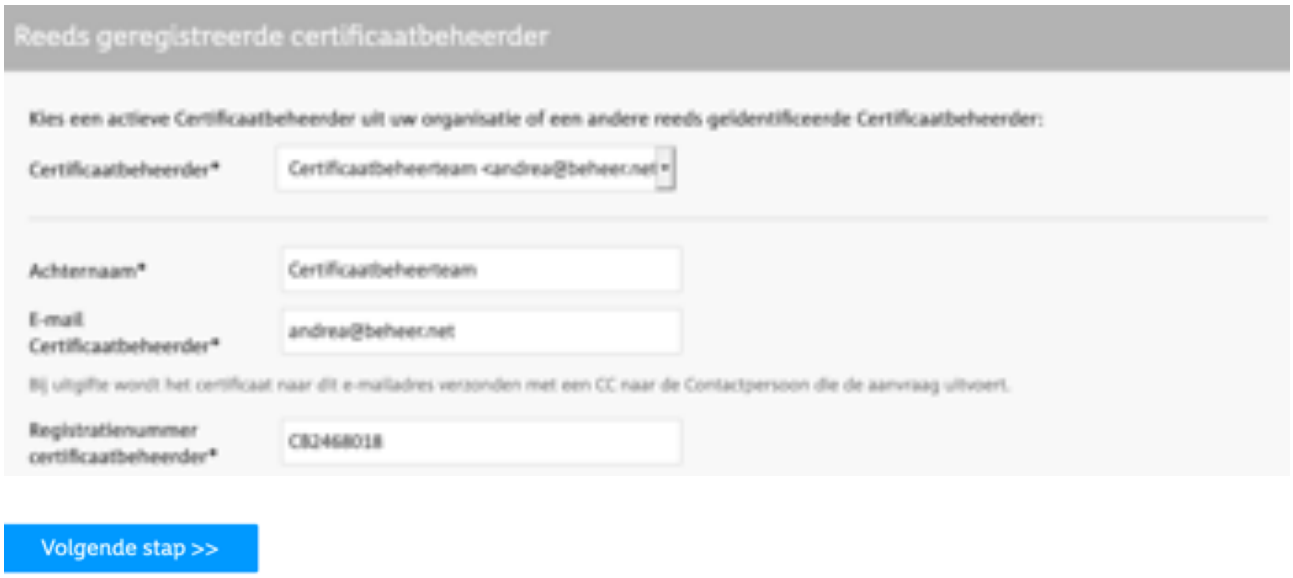
U kunt kiezen uit twee opties:

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 Certificaat-beheerder zijn voor meerdere Abonnees.

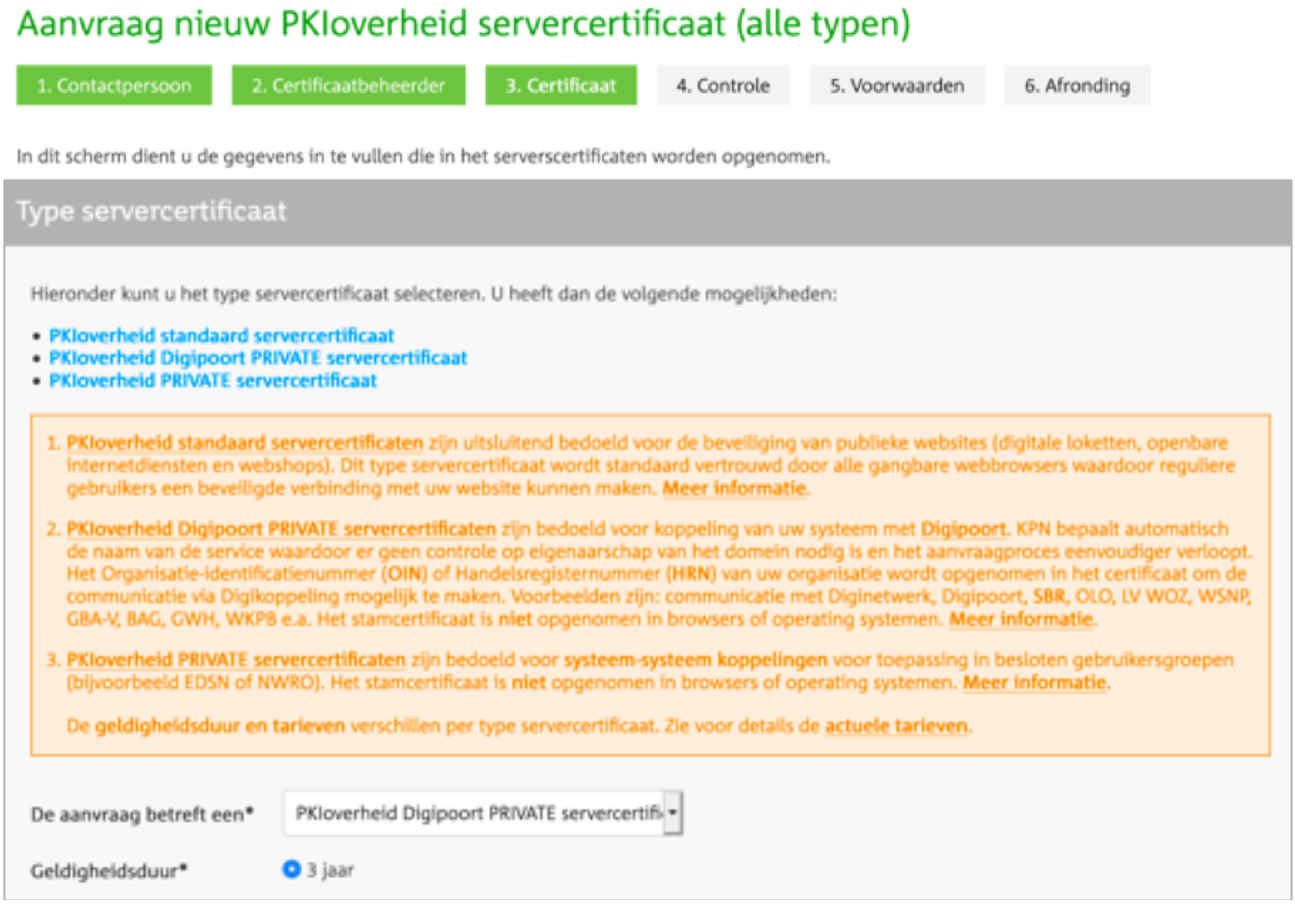
De uitleg en invulinstructies van beide opties kunt u vinden in paragraaf 3.4: Scherm 2: Certificaatbeheerder.
Als u kiest voor de 2e optie (reeds geïdentificeerd) is in het SSP de volgende keuzelijst als extra beschikbaar:

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:



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.



Invulinstructie en toelichting 3. Certificaat 1e 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.

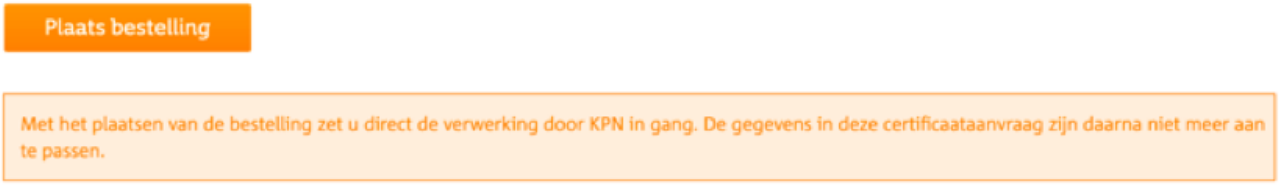
U kiest hier het servercertificaat dat geschikt is voor uw toepassing. In de oranje balk staat een korte toelichting over de verschillende types met een link 'Meer informatie' die doorverwijst naar de website waarin de verschillen uitgebreid beschreven staan.

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

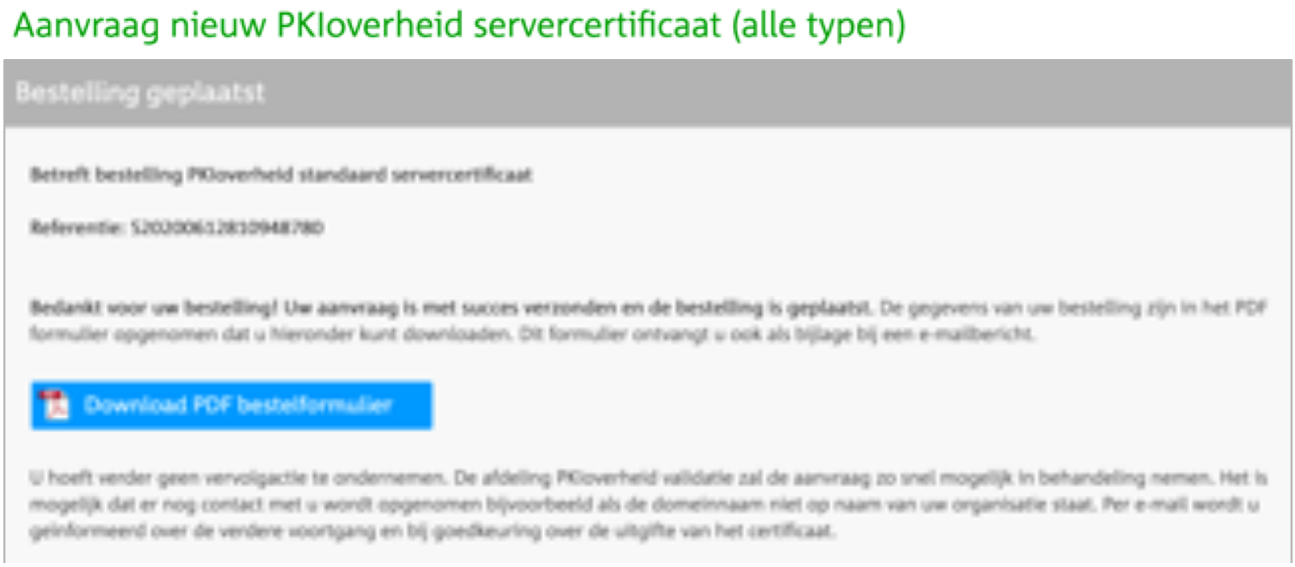
Het scherm met de voorwaarden is identiek aan hetgeen beschreven is in paragraaf 3.7: Scherm 5: Voorwaarden en wordt daarom hier niet herhaald. Als extra toevoeging wordt onderaan het formulier wel de volgende banner getoond:



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:



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 uitgeeft, 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/domein-controle/.
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 Servercertifcaat 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 Servercertifcaat 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.

KPN B.V. Afdeling PKIoverheid-Validatie <no-reply@kpn.com>
To: [redacted]
S2020082773073333... 1,2 MB

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 onderte enen 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:

KPN - Aanvraag PKIoverheid Digipoort PRIVATE servercertificaat

Referentie: S20200827730733333

Gegevens Abonnee en Contactpersoon

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

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		
Organisatienaam:	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		
Organisatienaam (O):	KPN B.V.		
Afdeling (OU):	Corporate Finance		
Plaats (L), Provincie (S), Land (C):	Rotterdam, Zuid-Holland, NL		
SHA256 fingerprint van CSR:	622d5f26b66aa3185db70247a3c46bbae49a1266620958bb215124d6ae834943		
Subject Alternative Names:			

Overige gegevens

Toepassing certificaat:	Digipoort-private	Type aanvraag:	Initieel
Support pakket:	Standaard pakket	Einddatum oude certificaat:	
Referentie tbv 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. Leveringsvoorwaarden 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.

Handtekening Contactpersoon

Farwerck Geb. 12-08-1970

Datum:
Plaats:
Handtekening:

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

ASQQ13048A - Pagina 1 van 1