



Datum
januari 2024

Auteur
KPN

Versie
7.0

Handleiding

KPN PKloverheid

Aanvraag van een Groepscertificaat

Inhoudsopgave

1	Inleiding	3
1.1	<i>Toelichting Groepscertificaat</i>	3
1.2	<i>Terminologie</i>	3
1.3	<i>Referenties</i>	5
2	Aanvraag Groepscertificaten	6
2.1	<i>Toelichting proces aanvraag Groepscertificaten</i>	6
2.1.1	<i>Eenmalige abonneeregistratie</i>	6
2.1.2	<i>Aanvragen Groepscertificaten</i>	6
2.1.3	<i>Eenmalige identificatie Certificaatbeheerder</i>	6
2.2	<i>Startscherm: checklist randvoorwaarden en validatie e-mail</i>	6
2.3	<i>Scherm 1: Gegevens bijbehorende Abonnee en Contactpersoon</i>	9
2.4	<i>Scherm 2: Certificaatbeheerder</i>	11
2.5	<i>Scherm 3: Certificaat</i>	14
2.6	<i>Scherm 4: Controle</i>	16
2.7	<i>Scherm 5: Voorwaarden</i>	17
3	Afronding	19
4	Beoordeling aanvraag door KPN en vervolg	21
4.1	<i>Indien van toepassing: eenmalige identificatie Certificaatbeheerder</i>	21
4.2	<i>Beoordelen aanvraag. Toezending smartcard</i>	21
4.3	<i>Elektronische ontvangstbevestiging smartcard</i>	21
5	BIJLAGEN: e-mail en PDF formulier	22
5.1	<i>E-mailbericht afronding</i>	22
5.2	<i>PDF Aanvraag Groepscertificaten</i>	23

1 Inleiding

Dit document bevat een toelichting en invulinstructie voor de aanvraag van PKIoverheid Groeps certificaten via het webformulier dat beschikbaar is op:

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

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

Met dit webformulier vraagt u PKIoverheid Groeps certificaten aan namens een reeds geregistreerde Abonnee van de PKI Certificatiedienstverlening van KPN. De Groeps certificaten zullen na goedkeuring van de aanvraag worden uitgegeven aan een reeds geregistreerde of nieuw geïdentificeerde Certificaatbeheerder.

Voordat u Certificaten in het domein Organisatie van de PKI voor de overheid kunt aanvragen, ontvangen en gebruiken, dient u zich eenmalig te registreren als Abonnee van KPN PKIoverheid Certificatiedienstverlening. Dit kan via: <https://kpnpkio.managedpki.com/registratie/>

1.1 Toelichting Groeps certificaat

De PKI voor de overheid kent zogenaamde Services certificaten. Dit zijn niet-persoonsgebonden Certificaten. Dat betekent dat het Certificaat kan worden gebonden aan enerzijds een functie of een groep van mensen of anderzijds aan een apparaat of een systeem. In het eerste geval is sprake van Groeps certificaten. Deze aanvraag betreft een aanvraag voor Groeps certificaten. In het tweede geval is sprake van Servercertificaten. Voor de aanvraag van een Servercertificaat verwijzen wij u naar: <https://kpnpkio.managedpki.com/csr/>.

In het geval van Groeps certificaten is feitelijk sprake van twee verschillende soorten certificaten:

- een certificaat voor vertrouwelijkheid;
- een certificaat voor authenticiteit.

Deze Certificaten kunnen aan een functie (bijvoorbeeld secretaris) of een groep mensen (bijvoorbeeld een afdeling) worden gekoppeld. Als de Certificaten aan een functie gekoppeld zijn, zijn deze niet direct afhankelijk van de medewerker die de functie vervuld. Als de medewerker wordt opgevolgd door een andere medewerker, kan het Certificaat worden overgedragen aan de opvolger van de vertrekkende medewerker. Als de Certificaten zijn gekoppeld aan een afdeling kunnen de Certificaten worden gebruikt door alle medewerkers van die afdeling (bijvoorbeeld het secretariaat). Zolang de afdeling, onder dezelfde naam, blijft bestaan kan het Certificaat worden gebruikt. Dit alles binnen de geldigheidsduur van het Certificaat.

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-overheid Certificaten aan door de Abonnee aangewezen Certificaathouders te bewerkstelligen.

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.

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.

Organisatiennaam: De naam van de rechtspersoonlijke entiteit waarvoor een abonnee de contracterende partij is. De organisatiennaam wordt aangetoond middels een uittreksel van het Handelsregister of een ander officieel stuk waaruit de naam blijkt. In het geval van een uittreksel uit het Handelsregister kan bij een vestiging de handelsnaam van de betreffende vestiging worden gebruikt.

Public key cryptografie: Het systeem waarbij een mechanisme van publieke sleutels en private sleutels wordt gebruikt. Dit houdt in dat er twee sleutels worden gebruikt. Eén sleutel wordt geheim gehouden (de private sleutel) en de andere sleutel mag publiekelijk worden verspreid (de publieke sleutel). Alles wat met de publieke sleutel gecijferd wordt is alleen met de private sleutel te ontcijferen en andersom. Het is een vorm van asymmetrische encryptie.

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.

PKI voor de overheid (PKI-overheid of PKIO): De gehele PKI infrastructuur die door de Policy Authority PKI-overheid (PA) wordt beheerd. De PA van de PKI voor de overheid ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid. De PKI voor de overheid is een afsprakenstelsel. Dit maakt generiek en grootschalig gebruik mogelijk van de elektronische handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. De PKI voor de overheid voorziet in een betrouwbaar normenkader voor PKI-diensten

met een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en andere gebruikers.

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.

Publieke sleutel: De sleutel van een asymmetrisch sleutelbaar die publiekelijk kan worden bekendgemaakt. De publieke sleutel wordt gebruikt voor de controle van de identiteit van de eigenaar van het asymmetrisch sleutelbaar, voor de controle van de elektronische handtekening van de eigenaar van het asymmetrisch sleutelbaar en voor het versleutelen van informatie voor een derde. Ook wordt de term "openbare sleutel" (Onder andere in de Europese Richtlijn) gebruikt. In de wet EH wordt echter "publieke sleutel" gebruikt.

USB-token: Een USB-token is een token vergelijkbaar met een smartcard, maar heeft een andere vorm. Het is een medium om certificaten op te slaan. Het verschil is dat voor een USB-token geen extra smartcardreader hoeft te worden geïnstalleerd. Daarentegen is het niet mogelijk om eindgebruikerkenmerken op de USB-token op te slaan, zoals een foto of persoonsgegevens.

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.

1.3 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 Certification Practice Statement en de KPN Bijzondere Voorwaarden PKI Overheid Certificaten. Deze zijn beschikbaar via <https://certificaat.kpn.com/downloads/>

2 Aanvraag Groeps certificaten

2.1 Toelichting proces aanvraag Groeps certificaten

Het proces voor de aanvraag van een groeps certificaat bestaat uit de volgende stappen:

2.1.1 Eenmalige abonneeregistratie

Abonneeregistratie kan middels deze link gestart worden: <https://kpnpkio.managedpki.com/registratie/>

2.1.2 Aanvragen Groeps certificaten

Dit is uitgebreid in dit document beschreven en bestaat uit de volgende stappen:

- Ga naar het aanvraagformulier PKloverheid groeps certificaat <https://kpnpkio.managedpki.com/groeps/>
- Vul alle vereiste gegevens in. Dit resulteert in een PDF formulier met alle aanvraaggegevens.
- Als de bij de aanvraag opgegeven Certificaatbeheerder nog niet als Certificaatbeheerder is geregistreerd, dient u een kopie Identiteitsbewijs van de Certificaatbeheerder toe te voegen.
- Onderteken het formulier en dien het in bij KPN. Hiervoor zijn de volgende opties beschikbaar:
 - Aanvraag elektronisch ondertekenen en indienen
 - Aanvraag op papier per post indienen

Verdere toelichting wordt gegeven in hoofdstuk 3.

2.1.3 Eenmalige identificatie Certificaatbeheerder

- Als de bij de aanvraag opgegeven Certificaatbeheerder nog niet als Certificaatbeheerder is geregistreerd, ontvangt de Certificaatbeheerder een verzoek voor identificatie.
- KPN laat deze identificatie uitvoeren door een gecontracteerde partij. Die zal per e-mail contact opnemen met de Certificaatbeheerder om de identificatie plaats te laten vinden op een door de Certificaatbeheerder te kiezen locatie en tijdstip.
- De smartcard met daarop de Certificaten zal met de ontvangstbevestiging worden verstuurd naar het geregistreerde adres van de Certificaatbeheerder. Na terugontvangst van de ontvangstbevestiging wordt de PIN-mailer verstuurd naar dit geregistreerde adres gestuurd.

2.2 Startscherm: checklist randvoorwaarden en validatie e-mail

De aanvraag van Groeps certificaten start op <https://kpnpkio.managedpki.com/groeps/> met het onderstaande scherm:

Aanvraag PKIoverheid Groepscertificaat

Aanvraag PKIoverheid Groepscertificaten

Welkom bij de aanvraag PKIoverheid Groepscertificaten van KPN.

Met dit webformulier vraagt u PKIoverheid Groepscertificaten aan voor een groep mensen en/of een functie namens een reeds geregistreerde Abonnee van de PKIoverheid Certificatiedienstverlening van KPN.

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

Checklist aanvraag PKIoverheid Groepscertificaten

Om het aanvraagformulier voor PKIoverheid Groepscertificaten met succes te kunnen doorlopen, zijn de volgende zaken noodzakelijk:

- Uw organisatie is reeds als PKIoverheid abonnee bij KPN geregistreerd.
- U bent bevoegd om een certificaat aan te vragen.

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*

Voer uw e-mailadres in

Verificatie code*



 Vernieuw captcha

Typ de tekst hierboven over

De tekst is *niet* hoofdlettergevoelig

[Volgende stap >>](#)

Toelichting

De eerste stap bestaat uit twee delen:

1. een checklist om vooraf te controleren of aan alle 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:
 - a. Uw organisatie is reeds als PKIoverheid abonnee bij KPN geregistreerd. De bevoegd vertegenwoordiger heeft bij de bevestiging van de registratie een PKIoverheid

abonneenummer ontvangen. Dit nummer is nodig tijdens het invullen van het aanvraagformulier voor Groeps certificaten.

- b. 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 PKIoverheid Abonneeregistratie.
2. 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. 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 aanvraag.

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). Indien de CAPTCHA slecht leesbaar is, kunt u deze vernieuwen door op de link te klikken.
- Klik op 'VOLGENDE STAP'.

Vervolgens verschijnt het onderstaande bevestigingsscherm:

E-mail verzonden

Er is een e-mail verstuurd aan contactpersoon@abonnee.lan.

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

Deze link blijft geldig gedurende 24 uur (tot 2023-10-18 08:22:59). Daarna dient u opnieuw het proces te starten.

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

Begin uw aanvraag van PKIoverheid Groeps certificaten bij KPN

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

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

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

Met behulp van dit webformulier vraagt u PKIoverheid Groeps certificaten aan. Het certificaat zal -na goedkeuring van de aanvraag en identiteitsvaststelling van de Certificaatbeheerder- worden uitgegeven aan de Certificaatbeheerder.

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

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

KPN B.V.

- Klik op de bovenste link in de e-mail om het aanvraagformulier voor Groeps certificaten 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: Gegevens bijbehorende Abonnee en Contactpersoon

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

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

Uw e-mailadres: **contactpersoon@abonnee.lan**. Mocht dit incorrect zijn, dan verzoeken we u om een nieuwe aanvraag voor Groeps certificaten te beginnen.

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

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

Verplichte velden worden aangegeven met (*).

Gegevens Abonnee en Contactpersoon

**PKIoverheid
Abonneenummer***

Uw PKIO Abonneenummer (type P1234567)

Land*

Nederland

KvK nummer*

KvK nummer van 8 cijfers

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

**Achternaam
contactpersoon***

Achternaam conform identiteitsbewijs

LET OP: U dient de *Achternaam van de Contactpersoon* in te vullen **zoals is opgenomen op uw identiteitsbewijs**. Dit voorkomt vertraging in de verwerking van uw aanvraag. KPN zal de opgegeven naam vergelijken met de naam op de kopie identiteitsbewijs die tijdens de abonneeregistratie is vastgelegd van de Contactpersoon.

Geboortedatum*

Bijv. 31-12-1971

E-mailadres

contactpersoon@abonnee.lan

[Volgende stap >>](#)

Invulinstructie en toelichting Scherm 1: Gegevens Abonnee en Contactpersoon

Dit scherm heeft als doel om de gegevens van de Abonnee vast te leggen waarvoor de Groeps-certificaat 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. Indien uw organisatie zich niet heeft ingeschreven in de KvK omdat u een overheidsorganisatie vertegenwoordigt, neem dan contact op met de Servicedesk.
- Bij gebruik van het KvK-nummer haalt KPN automatisch de Organisatiennaam en overige publieke KvK gegevens op. Als dat succesvol verloopt ziet u de handelsnaam zoals hieronder is geïllustreerd met het KvK nummer van KPN.

KvK nummer*	02045200
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	Koninklijke KPN N.V.

en verschijnt de volgende toelichting:

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

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

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

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 aanvraag Groepslicenties te beginnen.

- Klik op 'VOLGENDE STAP'

2.4 Scherm 2: Licentiebeheerder

In dit scherm kunt u aangeven wie als Licentiebeheerder op zal treden voor deze aanvraag Groepslicenties.

1. Contactpersoon 2. **Licentiebeheerder** 3. Licentie 4. Controle 5. Voorwaarden 6. Afronding

In dit scherm kunt u aangeven wie als Licentiebeheerder op zal treden voor deze aanvraag van Groepslicenties. De Licentiebeheerder zal namens de Abonneeorganisatie de Groepslicenties in ontvangst (gaan) nemen en beheren.

BELANGRIJK: u kunt kiezen uit twee opties:

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

Kies 2 als de Licentiebeheerder al eerder door KPN is geïdentificeerd voor een eerdere licentia aanvraag.

Certificaatbeheerder

De certificaatbeheerder is*

[Volgende stap >>](#)

U kunt kiezen uit twee opties:

1. *volledig nieuw*

Kies deze optie als u een nieuwe Licentiebeheerder 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.

Optie 1 Certificaatbeheerder is volledig nieuw

Nieuwe certificaatbeheerder

Volledige voornaam*

Tussenvoegsel

Achternaam*

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

(Mobiele) telefoon*

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

Geboortedatum*

Geboorteplaats*

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

E-mail Certificaatbeheerder*

Dit dient het e-mail adres te zijn dat de Certificaatbeheerder **namens uw organisatie** toegewezen heeft gekregen. Dit e-mail adres wordt gebruikt om een afspraak voor identificatie te maken.

Adresgegevens nieuwe certificaatbeheerder

Organisatiename

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

Land*

Postcode*

Plaats*

Straatnaam*

Huisnummer*

Huisnummer toevoeging

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

Invulinstructie en toelichting Scherm 2 (optie 1)

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

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. Dit e-mailadres wordt gebruikt om het uitnodiging voor identificatie naar toe te zenden.
Let op: De in het e-mailadres gebruikte domeinnaam moet behoren tot het domein van de Abonnee of tot het domein van de organisatie van de Certificaatbeheerder. Dit betekent dat de Abonnee of de organisatie van de Certificaatbeheerder als eigenaar van de domeinnaam geregistreerd moet staan bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA).
- Indien van toepassing: vul de organisatienaam in.
- Indien van toepassing: vul de adresgegevens in van de certificaatbeheerder. Bij een KvK geregistreerde organisatie zijn de adresgegevens al ingevuld vanuit de publieke KvK gegevens.
- Klik op 'VOLGENDE STAP'

Optie 2: Een reeds geïdentificeerde certificaatbeheerder

Reeds geregistreerde certificaatbeheerder

Achternaam*	<input type="text" value="Achternaam conform identiteitsbewijs"/>
E-mail Certificaatbeheerder*	<input type="text"/>
Registratienummer certificaatbeheerder*	<input type="text" value="Bijv. CB1234567"/>

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

[Volgende stap >>](#)

Invulinstructie en toelichting Scherm 2 (optie 2)

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 e-mailadres van de Certificaatbeheerder in.
- In dit geval moet u ook het Registratienummer hebben van een certificaatbeheerder die reeds eerder bij KPN is geregistreerd en van wie de identiteit is vastgesteld.
- Klik op 'VOLGENDE STAP'

2.5 Scherm 3: Certificaat

In dit scherm dient u gegevens in te vullen die daadwerkelijk in het certificaat komen te staan.

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

In dit scherm dient u de gegevens in te vullen die in de Groeps certificaten worden opgenomen.

Invulinstructie en toelichting Scherm 3

Pasaanvraag

Pasaanvraag

Aantal passen*

U kunt meerdere passen tegelijkertijd aanvragen. Indien u meer passen wilt aanvragen dan hier selecteerbaar zijn, verzoeken wij u contact op te nemen met de [Servicedesk](#).

- Indien u meer dan één pas tegelijk wilt aanvragen kunt u hier het aantal passen selecteren. Indien u meer passen wilt aanvragen dan hier selecteerbaar zijn in het formulier, verzoeken wij u contact op te nemen met de Servicedesk.

Gegevens voor Groeps certificaat

Gegevens voor Groeps certificaat 1

GEGEVENS CERTIFICAATHOUDER (PAS 1)

Naam van de service (CN)*

Organisatiennaam (O)*

Land (C)*

E-mailadres*

- Vul de naam van de service in. U dient hier de naam van de Certificaathouder in te vullen die in het certificaat moet worden opgenomen. De naam van de Certificaathouder is de naam van de functie of de groep mensen die het certificaat gaan gebruiken en waaraan u het Groeps certificaat wenst te koppelen.

- Controleer de organisatiename. Het webformulier stelt deze voor zoals in het handelsregister van de KvK is opgehaald. Indien van toepassing dient u zelf:
 - de naam in te korten tot maximaal 64 karakters
 - eventuele speciale karakters te verwijderen.
- Het land is altijd al correct ingevuld op basis van de ingevulde abonnee.
- Vul het e-mailadres in. U kunt slechts één e-mailadres opgeven per Groepscertificaat. Dit e-mailadres dient het e-mailadres van de Certificaathouder/service te zijn, dat door de Abonnee is toegewezen aan de Certificaathouder.

Let op: De in het e-mailadres gebruikte domeinnaam moet behoren tot het domein van de Abonnee. Dit betekent dat de Abonnee als eigenaar van de domeinnaam geregistreerd moet staan bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA).

Product formaat en Referentienummer

PRODUCT FORMAAT EN REFERENTIENUMMER (PAS 1)

Gewenste product*

Geldigheidsduur* 3 jaar

Vanwege aangepaste regelgeving hebben PKloverheid groeps certificaten een maximale geldigheidsduur van 3 jaar.

PO / Referentienummer

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

[Volgende stap >>](#)

Tot slot zijn er nog enkele gegevens nodig m.b.t. product formaat en facturatie:

- Maak een keuze voor het product formaat (smartcard, USB) en of u een starterspakket nodig heeft inclusief smartcard reader.
- Groeps certificaten zijn alleen leverbaar met een geldigheidsduur van 3 jaar.
- Vul optioneel een PO / Referentienummer. 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.
- Klik op 'VOLGENDE STAP'

2.6 Scherm 4: Controle

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

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

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

Gegevens Abonnee en Contactpersoon

PKIoverheid Abonneenummer	P1234560
KvK nummer	02045200
Achternaam contactpersoon	Groepkens
Geboortedatum	01-12-1971
E-mailadres	contactpersoon@abonnee.lan

Wijzig

Certificaatbeheerder

De certificaatbeheerder is	2. reeds geïdentificeerd
----------------------------	--------------------------

Wijzig

Reeds geregistreerde certificaatbeheerder

Achternaam	Beheerdernaam
E-mail Certificaatbeheerder	beheerder@beheerorganisatie.lan
Registratienummer certificaatbeheerder	CB4473175

Wijzig

Pasaanvraag

Aantal passen	1
---------------	---

Wijzig

Gegevens voor Groepscertificaat 1

GEGEVENS CERTIFICAATHOUDER (PAS 1)

De volgende gegevens worden in de Groeps certificaten opgenomen. **BELANGRIJK: Controleer deze gegevens zorgvuldig! Eventuele typfouten kunnen in sommige gevallen het certificaat technisch onbruikbaar maken.**

Naam van de service (CN)	Testgroep
Organisatiennaam (O)	Koninklijke KPN N.V.
Land (C)	Nederland
E-mailadres	groepsemail@abonnee.lan

PRODUCT FORMAAT EN REFERENTIENUMMER (PAS 1)

Gewenste product	certificaat op Pas (met lezer)
Geldigheidsduur	3 jaar
PO / Referentienummer	PO nummer 1

Wijzig

Volgende stap >>

Invulinstructie en toelichting Scherm 4 Controle

- Controleer uw gegevens.
- Klik op 'Wijzig' om gegevens in een bepaalde rubriek aan te passen.
- Indien de gegevens kloppen: klik op 'VOLGENDE STAP'

2.7 Scherm 5: Voorwaarden

Het laatste invoerscherm vraagt u om akkoord te gaan met de voorwaarden die van toepassing zijn.

1. Contactpersoon

2. Certificaatbeheerder

3. Certificaat

4. Controle

5. Voorwaarden

6. Afronding

Om uw aanvraag PKIoverheid Groeps certificaten af te ronden, dient u de volgende voorwaarden te accepteren:

Voorwaarden

- Ik ben akkoord met de [Algemene Leveringsvoorwaarden](#) en de [KPN Bijzondere Voorwaarden PKIoverheid Certificaten](#).
 - De 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.
- Ik ga akkoord met alle bovenstaande voorwaarden en heb namens de Abonnee alle gegevens volledig, juist en naar waarheid ingevuld.**

Verzend Aanvraag

Voorwaarden

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

- Akkoord met de [Algemene Leveringsvoorwaarden van KPN | KPN](#) en de [KPN Bijzondere Voorwaarden PKI Overheid Certificaten](#). 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 Groeps certificaten te beheren en in te trekken;
 - Verklaring dat u akkoord gaat met de [tarieven](#) die samenhangen met de PKIO Groeps certificaten;
 - Verklaring dat u akkoord gaat met de publicatie van de certificaten in de online certificaten database van KPN.
- Vink de checkbox aan dat u akkoord bent met alle voorwaarden en dat alle gegevens volledig, juist en naar waarheid zijn ingevuld;
- Klik op 'VERZEND AANVRAAG'.

BELANGRIJK: hoewel KPN na het verzenden van de aanvraag de digitale gegevens heeft, dient de Contactpersoon die de aanvraag doet de aanvraag rechtsgeldig te ondertekenen en in te dienen. Dit is verder toegelicht in Hoofdstuk 3.


3 Afronding

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

Aanvraag verzonden

Referentie: GRP202310171362156481

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 van pas 1 van 1](#)

BELANGRIJKE VERVOLGSTAP: ONDERTEKENEN EN INDIENEN VAN DE AANVRAAG

Om aanvraag van PKIoverheid Groeps certificaten 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 ondertekenen is eenvoudig uit te voeren in de meest actuele versie van de [Adobe Reader](#). Uitleg over het elektronisch ondertekenen staat in [KPN PKIoverheid Toelichting elektronisch ondertekenen aanvraagformulier](#). Een alternatief is 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 formulier op naar:

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

Voor de afronding van uw aanvraag zijn er twee opties:

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.

Dit dient te gebeuren met een [Persoonlijke certificaat](#) dat op naam van de contactpersoon staat.

Voor het elektronisch ondertekenen van het PDF aanvraagformulier met de Adobe Reader is een aparte toelichting beschikbaar: [KPN PKIO Toelichting elektronisch ondertekenen aanvraagformulieren](#)

U kunt de elektronisch ondertekende PDF vervolgens e-mailen naar: pkivalidation@kpn.com

OPTIE 2: AANVRAAG OP PAPIER PER POST INDIENEN.

Kies voor deze optie indien u niet de gelegenheid heeft om de aanvraag elektronisch in te dienen. De werkwijze is als volgt:

- Print het PDF formulier op blanco A4 papier.
- De Contactpersoon van de Abonnee dient de aanvraag met de hand te ondertekenen.
- Stuur het formulier op naar:

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

LET OP: Indien u meer dan één aanvraag voor Groeps certificaten heeft ingevoerd is er per aanvraag een PDF formulier gemaakt. U dient alle formulieren te ondertekenen en in te dienen.

4 Beoordeling aanvraag door KPN en vervolg

4.1 Indien van toepassing: eenmalige identificatie Certificaatbeheerder

Als gevolg van de voorschriften van PKI-overheid, dient de Certificaatbeheerder eenmalig persoonlijk geïdentificeerd te worden.

KPN laat deze identificatie uitvoeren door een gecontracteerde partij. Zie verder de toelichting in par. 2.1.3.

4.2 Beoordelen aanvraag. Toezending smartcard

Na succesvolle identificatie en verdere controles zal KPN de smartcard (of USB-token) met daarop de Certificaten met een ontvangstbevestiging versturen naar het opgegeven adres van de Certificaatbeheerder.

4.3 Elektronische ontvangstbevestiging smartcard

Om zeker te zijn dat u als Certificaathouder de smartcard heeft ontvangen, dient de Certificaatbeheerder de ontvangst elektronisch te bevestigen. De Certificaatbeheerder ontvangt een e-mail met daarin een unieke link. Als u hierop klikt kunt u de Activatiecode ingeven die op de begeleidende brief staat die u bij de smartcard heeft ontvangen.

Voor de elektronische ontvangstbevestiging is nog een aparte toelichting beschikbaar:

[Toelichting elektronische ontvangstbevestiging smartcards](#)

BELANGRIJK: deze ontvangstbevestiging dient **binnen 6 weken** na ontvangst door u uitgevoerd te zijn. Indien niet binnen deze 6 weken de ontvangst bevestigd wordt zullen de certificaten ingetrokken worden.

1. Toezenden PINcode voor gebruik

Na succesvolle ontvangstbevestiging wordt de brief met de PIN-, PUK-, en intrekingscode nagezonden naar het geregistreerde adres van de Certificaatbeheerder.

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 onderstaande 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.

From "KPN B.V. Afdeling PKI-Validatie" <no-reply@devkpnki.local>
Subject **Uw aanvraag PKIoverheid Groeps certificaten bij KPN [1/1]: Testgroep**
To contactpersoon@abonnee.lan

Show headers ▼

HTML Plain text Source MIME

Uw aanvraag PKIoverheid Groeps certificaten bij KPN

U heeft de eerste stap van uw aanvraag PKIoverheid Groeps certificaten 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 ook al uitgevoerd maar zijn hier voor de zekerheid herhaald voor het geval de browser is afgesloten.

BELANGRIJKE VERVOLGSTAP: ONDERTEKENEN EN INDIENEN VAN DE AANVRAAG

Om uw aanvraag PKIoverheid Groeps certificaten 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 e-mailen naar pkivalidation@kpn.com

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 ondertekenen is eenvoudig uit te voeren in de meest actuele versie van de [Adobe Reader](#). Uitleg over het elektronisch ondertekenen staat in [KPN PKIoverheid Toelichting elektronisch ondertekenen aanvraagformulier](#).

Een alternatief is 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 formulier 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 Groeps certificaten

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



GRP202310171362156481

KPN aanvraag PKloverheid Groeps certificaat - Pas 1 van 1

Referentie: GRP202310171362156481

Gegevens Abonnee en Contactpersoon

Abonneenummer: P1234560
Handelsnaam volgens KvK: Koninklijke KPN N.V.
Achternaam Contactpersoon: Groepkens Geboortedatum: 01-12-1971
E-mail: contactpersoon@abonnee.lan

Certificaatbeheerder

De certificaatbeheerder is: 2. reeds geïdentificeerd Registratienummer: CB4473175
Voornaam: Geboorteplaats:
Tussenvoegsel: E-mail: beheerder@beheerorganisatie.lan
Achternaam: Beheerdernaam (Mobiel) telefoonnummer:
Geboren:
Organisatiennaam:
Adresgegevens:

Gegevens voor Groeps certificaat

BELANGRIJK: De hieronder getoonde gegevens worden onwrijzigbaar opgenomen in de Groeps certificaten. Controleer deze gegevens zorgvuldig! Typfouten kunnen in sommige gevallen de certificaten technisch onbruikbaar maken.

Naam van de Service (CN): Testgroep
Organisatiennaam (O): Koninklijke KPN N.V.
Land (C): NL
E-mailadres: groepsemail@abonnee.lan

Overige gegevens

Product: certificaat op Pas (met lezer) Referentie tbv facturatie: PO nummer 1
Geldigheidsduur: 3 jaar

Akkoordverklaringen

Ondergetekende verklaart namens Abonnee:

- dat alle gegevens volledig, juist en naar waarheid zijn ingevuld.
- akkoord te gaan met de KPN Algemene Leveringsvoorwaarden en de Bijzondere Voorwaarden PKI Overheid Certificaten.
- dat opgegeven Certificaatbeheerder geïnformeerd, bevoegd en ter zake kundig is om namens abonnee Groeps certificaten te beheren en in te trekken.
- akkoord te zijn met de tarieven.
- akkoord te zijn dat de certificaten worden gepubliceerd in de KPN online certificaten database.

Vervolg stappen

Om de aanvraag van de Groeps certificaten 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

Groepkens Geb. 01-12-1971

Datum:
Plaats:
Handtekening: