

Registratieformulier PKIoverheid Certificaatbeheerders – v1.12

Domein Organisatie

Met behulp van dit formulier kunt u, namens de hieronder genoemde Abonnee, binnen het Domein Organisatie van de PKI voor de overheid, Certificaatbeheerders laten registreren. Een Certificaatbeheerder kan namens de Abonneeorganisatie één of meerdere Servercertificaten of Groepslicenties in ontvangst (gaan) nemen en beheren.

KPN Corporate Market BV
Fauststraat 1
7323 BA Apeldoorn
Postbus 9105
7300 HN Apeldoorn
T +31 (0) 31 08 86 61 00 00
<http://certificaat.kpn.com>
K.v.K. Amsterdam nr. 52959597
NL850684481B01

Belangrijk: Lees eerst de bijgevoegde toelichting voor het invullen van dit formulier.

1) Gegevens Contactpersoon

Organisatiename Abonnee

Abonneenummer

Naam Contactpersoon

Telefoonnummer Contactpersoon

2) Gegevens Certificaatbeheerder(s)

In bijlage A kunnen de gegevens van de beoogde Certificaatbeheerder(s) worden ingevuld.

3) Checklist bijlagen

- Bijlage A: gegevens Certificaatbeheerder(s)
- Kopie geldig identiteitsbewijs Certificaatbeheerder(s)

4) Verklaring

Ondergetekende verklaart namens Abonnee:

- I. dat alle gegevens volledig, juist en naar waarheid zijn ingevuld;
- II. akkoord te gaan met de KPN Bijzondere Voorwaarden PKI Overheid Certificaten.

Handtekening Contactpersoon:

.....

ondertekend te:

d.d. / /(dag/maand/jaar)

Bijlage A: Gegevens Certificaatbeheerder(s)

1)

Volledige namen
Organisatiennaam*
Geboortedatum
Geboorteplaats
Telefoonnummer
E-mail adres
postadres privé	Straatnaam: Postcode: Plaatsnaam:
postadres zakelijk	Straatnaam: Postbus: Postcode: Plaatsnaam:
Enmalige identificatie via	<input type="checkbox"/> een GWK Travelex vestiging (standaard) <input type="checkbox"/> identificatie op lokatie (meerprijs)
Kan KPN steunen op een eerdere identificatie?	<input type="checkbox"/> Ja <input type="checkbox"/> Nee
	Abonneenaam en -nummer

2)

Volledige namen
Organisatiennaam*
Geboortedatum
Geboorteplaats
Telefoonnummer
E-mail adres
postadres privé	Straatnaam: Postcode: Plaatsnaam:
postadres zakelijk	Straatnaam: Postbus: Postcode: Plaatsnaam:
Enmalige identificatie via	<input type="checkbox"/> een GWK Travelex vestiging (standaard) <input type="checkbox"/> identificatie op lokatie (meerprijs)
Kan KPN steunen op een eerdere identificatie?	<input type="checkbox"/> Ja <input type="checkbox"/> Nee
	Abonneenaam en -nummer

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

Toelichting en instructie Registratieformulier PKIoverheid Certificaatbeheerders

Domein Organisatie

Algemeen

Voor het registreren van Certificaatbeheerders in het Domein Organisatie van de PKI voor de overheid gelden een aantal voorwaarden en dient u een aantal gegevens te verstrekken.

Dit document is een toelichting op het formulier 'Registratieformulier PKIoverheid Certificaatbeheerders'.

Een Services certificaat is een niet-persoonsgebonden certificaat. Dat betekent dat het certificaat kan worden gebonden aan enerzijds een apparaat of een systeem of anderzijds aan een functie of een groep van mensen. In het eerste geval is sprake van Servercertificaten, in het tweede geval spreekt men van Groepslicenties. Voor de aanvraag van een Servercertificaat of een Groepslicentie verwijzen wij u naar: http://www.pki.getronics.nl/PKI_osc.html.

Met behulp van dit formulier kunt u namens uw organisatie binnen het Domein Organisatie van de PKI voor de overheid, één of meer Certificaatbeheerders laten registreren die namens uw organisatie Services licenties in ontvangst mogen nemen en (gaan) beheren. De registratie is eenmalig. Hierbij zal de Certificaatbeheerder persoonlijk worden geïdentificeerd. Aangevraagde Services licenties worden vervolgens naar de geregistreerde Certificaatbeheerder verzonden. Een Servercertificaten wordt naar het opgegeven e-mail adres van de Certificaatbeheerder verstuurd, een Groepslicentie naar zijn privé postadres.

Voorwaarden en handreikingen bij het invullen van het formulier

Ad 1) Gegevens Contactpersoon

U dient de volgende gegevens in te vullen:

- organisatiename Abonnee;
- Abonneenummer;
- naam van de Contactpersoon;
- emailadres van de Contactpersoon;
- telefoonnummer van de Contactpersoon.

Organisatiename Abonnee en Abonneenummer

U dient de naam van de Abonneeorganisatie op te geven, zoals deze bij KPN is geregistreerd met behulp van het formulier 'Abonnee Registratie'. U dient tevens het Abonneenummer in te vullen. Het Abonneenummer is na de registratie van uw organisatie als Abonnee aan u teruggekoppeld (brief acceptatie Abonnee).

Naam en telefoonnummer van de Contactpersoon

U dient de naam en het telefoonnummer 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 zijn één of meerdere Contactpersonen geregistreerd. Indien de Contactpersoon nog niet als zodanig is geregistreerd bij KPN, dient u het formulier 'Wijziging

Contactpersoon' te gebruiken en mee te zenden met deze wijziging.

Ad 2) Gegevens beoogde Certificaatheerder

U dient de gegevens van de Certificaatheerder in te vullen in Bijlage A ten behoeve van de registratie van de certificaatheerder.

U kunt het aantal Certificaatheeders waarvoor u een aanvraag doet, aanpassen in Bijlage A, door de benodigde gegevensvelden te kopiëren of te verwijderen.

De Certificaatheerder is de persoon die namens en onder verantwoordelijkheid van de Abonnee het Servercertificaat beheert. Beheren betekent dat hij/zij o.a. het certificaat installeert en indien nodig zorgt voor tijdige intrekking. De gegevens van de Certificaatheerder betreffen:

- volledige naam;
- geboortedatum;
- geboorteplaats;
- e-mail adres;
- postadres (zakelijk en privé);
- organisatiename Certificaatheerder;
- eenmalige identificatie voorkeur;
- of gesteund kan worden op een eerder uitgevoerde identificatie.

Volledige naam

U dient de volledige naam van de Certificaatheerder in te vullen. De naam van de Certificaatheerder moet overeenkomen met de naam op diens identiteitsbewijs (zie Ad 4).

Geboortedatum en -plaats

U dient hier de geboortedatum en -plaats van de Certificaatheerder in te vullen. Deze gegevens moeten uiteraard ook overeenkomen met de betreffende gegevens op diens identiteitsbewijs.

E-mail adres

U dient hier het e-mail adres van de Certificaatheerder in te vullen. Dit dient het e-mail adres te zijn dat de Certificaatheerder namens uw organisatie toegewezen heeft gekregen.

De in het e-mail adres gebruikte domeinnaam moet behoren tot het domein van de Abonnee of tot het domein van de organisatie van de Certificaatheerder. Dit betekent dat de Abonnee of de organisatie van de Certificaatheerder als eigenaar van de domeinnaam geregistreerd moet staan bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA). Ook voor het e-mail adres geldt dat het niet meer dan 63 posities mag bevatten.

Dit e-mail adres wordt gebruikt om het meldverzoek voor identificatie bij GWK Travelex en het Servercertificaat naar toe te zenden.

Postadressen

U dient hier het postadres (zakelijk en privé) van de Certificaatheerder in te vullen. Bij aanvragen voor Groepslicenties wordt de smartcard naar het privé adres verzonden. De PIN-mailer wordt naar het zakelijke adres verzonden. Het zakelijke adres wordt tevens gehanteerd voor eventuele correspondentie met gegevens die benodigd zijn voor het beheren van de licenties.

Organisatiename Certificaatheerder

Het is mogelijk dat de Certificaatheerder geen onderdeel uitmaakt van uw organisatie (de Abonneeorganisatie). Dat kan bijvoorbeeld het geval zijn indien u (delen van het beheer van) uw ICT-infrastructuur heeft uitbesteed. In dat geval dient u hier in te vullen van welke organisatie de

Certificaatbeheerder onderdeel uitmaakt.

Eenmalige identificatie voorkeur

Als gevolg van de voorschriften van PKloverheid, dient de Certificaatbeheerder persoonlijk geïdentificeerd te worden. Standaard vindt deze identificatie plaats op een vestiging van GWK Travelex. De identificatie op de GWK vestiging is kosteloos.

Voor de identificatie ontvangt de Certificaatbeheerder een meldverzoek. Met dit meldverzoek en het identiteitsbewijs, dat gebruikt is om de Certificaatbeheerder te registreren (dwz. het identiteitsbewijs waarvan u een kopie bij deze aanvraag dient te sluiten), dient de Certificaatbeheerder zich zo spoedig mogelijk, doch uiterlijk binnen 6 weken te melden bij GWK Travelex. Het meldverzoek dient hiertoe afgedrukt te worden.

Een overzicht van de GWK Travelex vestigingen is te vinden op: <http://www.travelex.com/nl/store-locator/?lang=NLD>.

Let op: U kunt voor uw identificatie alleen terecht bij de GWK Travelex vestigingen. U kunt hiervoor niet terecht bij een Servicepunt van GWK Travelex.

Het is tevens mogelijk om, tegen meerprijs, op een nader te bepalen locatie te worden geïdentificeerd.

Kan KPN steunen op een eerdere identificatie.

U kunt deze vraag positief beantwoorden indien de betreffende Certificaatbeheerder al eerder door of namens KPN als Certificaatbeheerder is geïdentificeerd. In dat geval dient u de naam en het nummer van de Abonnee te vermelden voor welke de identificatie destijds is uitgevoerd. Hierbij geldt de beperking dat KPN (of voor deze GWK Travelex) de identificatie moet hebben uitgevoerd en het daarbij gebruikte identiteitsbewijs nog steeds geldig moet zijn tot minimaal 6 weken na indiening van de aanvraag. De datum van ontvangst van de aanvraag bij KPN is daarbij leidend. KPN zal in deze gevallen nagaan of uw identiteitsbewijs als 'gestolen' of 'vermist' geregistreerd staat.

Ad 3) Checklist bijlagen

Met deze aanvraag dient u een kopie van een geldig identiteitsbewijs van de Certificaatbeheerder mee te sturen.

Kopie van een geldig identiteitsbewijs

Het te gebruiken identiteitsbewijs moet een identiteitsbewijs zijn conform de Wet op de Identificatie (Wid). Voorbeelden van een dergelijk identiteitsbewijs zijn een paspoort of een identiteitskaart. Het gebruikte identiteitsbewijs moet geldig zijn op de datum van identificatie van de Certificaatbeheerder, op die dag mag de geldigheidstermijn van het identiteitsbewijs niet zijn verstreken.

Deze kopie van het identiteitsbewijs moet voor KPN voldoende leesbaar zijn. Duidelijk moet zijn:

- het documentnummer;
- datum einde geldigheid;
- de gegevens van de beoogde Certificaatbeheerder;
- de handtekening van de beoogde Certificaatbeheerder;
- de foto van de beoogde Certificaatbeheerder.

Ad 4) Verklaring

U, als de bij 1) genoemde Contactpersoon, dient het formulier te ondertekenen. Dat kan met behulp van een handgeschreven handtekening, maar dat kan ook met een elektronische handtekening. Deze elektronische handtekening dient te voldoen aan de eisen van de Wet elektronische handtekeningen en het Gekwalificeerde Certificaat dat u gebruikt om de elektronische handtekening te zetten dient binnen het Domein Organisatie van de PKI voor de overheid namens de Abonnee aan u te zijn uitgereikt.

Door de aanvraag van een (elektronische) handtekening te voorzien geeft u onder andere aan dat u instemt met de KPN Bijzondere Voorwaarden PKI Overheid Certificaten.

Nota Bene: De KPN Bijzondere Voorwaarden PKI Overheid Certificaten gelden zowel voor Abonnees, Contactpersonen, Certificaathouders, Certificaatbeheerders en vertrouwende partijen. Hierdoor is het voor alle betrokkenen duidelijk wat de rechten en plichten zijn. Door te vertrouwen op het Services 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.

Vervolg

U dient het ingevulde (en met de hand ondertekende) registratieformulier en bijlagen te versturen naar:

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

U kunt het registratieformulier ook per mail versturen naar KPN. U dient dan het registratieformulier en de bijlagen te hechten aan een mail, deze te voorzien van een elektronische handtekening en de mail te versturen naar pkivalidation@getronics.com.

KPN zal de aanvraag in behandeling nemen. Indien de aanvraag leidt tot registratie van de Certificaatbeheerder, zal een meldverzoek worden verzonden naar het opgegeven privé adres van de Certificaatbeheerder. Met dit meldverzoek en zijn/haar identiteitsbewijs dient de Certificaatbeheerder zich persoonlijk te laten identificeren. Het te gebruiken identiteitsbewijs moet hetzelfde zijn als gebruikt tijdens de Aanvraag en dient geldig te zijn op de datum van identificatie. Indien bij identificatie voorkeur is aangegeven 'identificatie op locatie', zal KPN contact opnemen om een afspraak te maken over de identificatiedatum en locatie. Nadat de Certificaatbeheerder geïdentificeerd is zullen zijn gegevens in het Certificaatbeheerdersregister worden opgenomen.

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; <http://www.pkioverheid.nl>
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 <http://certificaat.kpn.com/>.