Bijzondere Voorwaarden

PKI OVERHEID CERTIFICATEN

Versie 5.6 – 24 april 2025

KPN B.V. (verder: KPN) is een certificatiedienstverlener die is toegetreden tot het stelsel van de PKI voor de overheid (verder: PKIoverheid). Dat betekent voor deze dienstverlening binnen de PKIoverheid dat alle relevante bepalingen en eisen uit het Programma van Eisen behorende bij PKIoverheid van toepassing zijn.

De in deze Bijzondere Voorwaarden PKIoverheid Certificaten vermelde bepalingen zijn, naast de Algemene Bepalingen van de Algemene Leveringsvoorwaarden van KPN, uitsluitend van toepassing indien KPN aan Opdrachtgever (Abonnee) PKIoverheid Certificaten levert. In geval van strijdigheid tussen bepalingen van deze Bijzondere Voorwaarden en bepalingen van de Algemene Voorwaarden, prevaleren de bepalingen van deze Bijzondere Voorwaarden.

1. Definities

1.1 De definities en afkortingen zoals opgenomen in de door KPN uitgegeven Certification Practice Statement PKIoverheid (hierna: PKIoverheid CPS) zijn integraal van toepassing op deze Bijzondere Voorwaarden.

2. Onderwerp

2.1 Tegen betaling van de daarvoor geldende tarieven door Opdrachtgever, zal KPN als Trust Service Provider (TSP) de overeengekomen hoeveelheid PKIoverheid Certificaten leveren aan Opdrachtgever onder de voorwaarden zoals opgenomen in deze Bijzondere Voorwaarden. Opdrachtgever geldt in dat verband als Abonnee, inclusief de daarbij behorende verplichtingen.

2.2 Indien de Abonnee niet een natuurlijk persoon is (zoals bedoeld in artt. 2:1, 2:2 en 2:3 BW), wijst Abonnee tenminste één contactpersoon aan om namens hem de uitgifte

en intrekking van PKIoverheid Certificaten te begeleiden. Alsdan garandeert Abonnee dat degene die namens hem om uitgifte verzoekt vertrouwd, ter zake kundig en voldoende bevoegd is om zo'n verzoek te doen en daarmee diens rechtspersoon te binden aan deze voorwaarden. Indien de Contactpersoon niet langer bevoegd is de Opdrachtgever te vertegenwoordigen, dan dient de Opdrachtgever dit vroegtijdig schriftelijk kenbaar te maken aan KPN.

3. Verplichtingen en garanties KPN

3.1 KPN garandeert tegenover Abonnees, Certificaathouders en Vertrouwende Partijen dat:

- de levering zal geschieden conform deze Bijzondere Voorwaarden, de PKIoverheid CPS van KPN;
- Alle gegevens in het PKIoverheid Certificaat op het tijdstip van afgifte juist zijn en dat alle noodzakelijke gegevens zijn opgenomen;
- Voor beroepsgebonden certificaten die zijn uitgegeven aan leden van Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders geldt dat het register zoals gepubliceerd in http://www.registergerechtsdeurwaarders.nl geacht wordt correct te zijn.
  De juistheid en volledigheid van de inhoud van dit register kan niet door KPN gegarandeerd worden. KPN aanvaardt derhalve geen aansprakelijkheid voor de beschikbaarheid, de juistheid en de volledigheid van dit register;
- De gegevens van de in het PKIoverheid Certificaat geïdentificeerde Certificaathouder op het tijdstip van de afgifte van het PKIoverheid Certificaat overeenkomen met de gegevens die zijn gebruikt voor het aanmaken van het PKIoverheid Certificaat;
- De gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening complementair kunnen worden gebruikt;
- Geen inhoudelijke fouten of onvolledigheden zullen worden geïntroduceerd bij de generatie en uitgifte van een PKIoverheid Certificaat door KPN.

3.2 KPN garandeert tegenover Abonnees, Certificaathouders en Vertrouwende Partijen dat in de volgende gevallen tot intrekking van de uitgegeven Certificaten zal worden overgegaan.

- De abonnee geeft aan dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee ook met terugwerkende kracht geen toestemming verleent.
- KPN over voldoende bewijs beschikt over:
    - dat de private sleutel van de abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast en/of
    - een vermoeden van compromittatie en/of
    - een inherente beveiligingszwakheid en/of
    - dat het certificaat op een andere wijze is misbruikt.
- Een sleutel wordt als aangetast beschouwd in geval van
    - ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel,
    - verloren of vermoedelijk verloren private sleutel of QSCD,
    - gestolen of vermoedelijk gestolen private sleutel
    - vernietigde private sleutel of QSCD.
- Een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in deze CP en/of het bijbehorende CPS van KPN en/of de overeenkomst die KPN met de abonnee heeft afgesloten.
- KPN op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de gegevens, die in het certificaat staat. Een voorbeeld daarvan is: verandering van de naam van de certificaathouder.
- KPN bepaalt dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van KPN of de overeenkomst die KPN met de abonnee heeft gesloten.
- KPN bepaalt dat gegevens in het certificaat niet juist of misleidend zijn.

- KPN haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere certificatiedienstverlener.
- De Policy Authority van PKIoverheid vaststelt en naar KPN toe aangeeft dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (zoals browserpartijen).

Opmerking: Daarnaast kunnen certificaten worden ingetrokken als maatregel om een calamiteit te voorkomen, danwel te bestrijden. Als calamiteit wordt zeker de aantasting of vermeende aantasting van de private sleutel van KPN, waarmee certificaten worden ondertekend, beschouwd.

Voor Servercertificaten gelden ook de volgende redenen.

- KPN op de hoogte wordt gesteld of anderszins zich er bewust van wordt dat het gebruik van de domeinnaam in het certificaat niet langer wettelijk toegestaan is (bijvoorbeeld ten gevolge van een rechterlijke uitspraak of door misbruik).
- De Abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen.

4. Verplichtingen en garanties Abonnee

4.1 De Abonnee garandeert tegenover KPN en Vertrouwende Partijen dat:

- de rol van Abonnee zal worden uitgevoerd conform deze Bijzondere Voorwaarden en conform de PKIoverheid CPS van KPN;
- alle gegevens die worden aangeboden ten behoeve van de generatie en uitgifte van een PKIoverheid Certificaat naar waarheid, actueel en correct zijn;
- alle door of namens hem aangewezen Certificaathouders en/of Certificaatbeheerders handelen conform de in deze Bijzondere Voorwaarden opgenomen verplichtingen;
- alle relevante wijzigingen in de relatie tussen de Abonnee en Certificaathouder en/of Certificaatbeheerder vroegtijdig aan KPN worden gecommuniceerd;

- alle relevante stukken op eerste verzoek van KPN, uiterlijk binnen drie weken na genoemd verzoek, worden overlegd;
- KPN zo spoedig mogelijk op de hoogte zal worden gesteld indien onjuistheden in de inhoud van het PKIoverheid Certificaat zijn ontstaan;
- KPN, in geval van beroepsgebonden certificaten, zo spoedig mogelijk op de hoogte zal worden gesteld indien het authentieke bewijs welke noodzakelijk is voor het behouden van het Certificaat voor een erkend beroep niet langer kan worden overlegd;
- QSCD's en SUD's (indien van toepassing) waarop Private Sleutels worden bewaard, zullen worden beveiligd conform de wijze waarop gevoelige gegevens en/of bedrijfskritische middelen zijn beveiligd;
- sleutelmateriaal van Certificaathouders zal worden gegenereerd in een veilig middel dat voldoet aan EAL4+ of aan gelijkwaardige beveiligingscriteria, dan wel op een softwarematige wijze in een omgeving die aldus is ingericht dat ongeoorloofde toegang tot en/of gebruik van de sleutels wordt uitgesloten, met inachtneming van het onder artikel 7 lid 1 bepaalde;
- elk op zijn verzoek uitgegeven PKIoverheid Certificaat direct en zonder vertraging wordt ingetrokken wanneer de Certificaathouder niet langer valt onder de verantwoordelijkheid van de Abonnee of indien de Certificaathouder en/of Certificaatbeheerder handelt in strijd met het onder artikel 5 bepaalde.

4.2 De Abonnee/ Certificaathouder is zelf verantwoordelijk voor een tijdige vervanging van de uitgegeven certificaten in het geval van een naderende afloop geldigheid van het Certificaat, compromittatie en/of andere soorten van calamiteiten met betrekking tot het Certificaat of van bovenliggende certificaten, gedurende de periode van geldigheid. KPN verwacht van de Abonnee dat de Abonnee zelf adequate maatregelen neemt om de continuïteit van het gebruik van de Certificaten te borgen.

5. Verplichtingen en garanties Certificaathouder

5.1 De Certificaathouder garandeert tegenover KPN, de Abonnee en Vertrouwende Partijen dat:

- geen enkele andere persoon toegang zal hebben tot de Private Sleutel die is gekoppeld aan de Publieke Sleutel in het PKIoverheid Certificaat;
- het PKIoverheid Certificaat enkel zal worden gebruikt voor de doelen waartoe deze is uitgereikt;
- de toegangscodes van QSCD en/of SUD, waarin de Private Sleutel is opgeslagen, steeds veilig en gescheiden van de QSCD of SUD bewaard zullen worden;
- direct na ontvangst van het certificaat, maar in ieder geval alvorens over te gaan tot installatie en gebruik, het certificaat op haar volledige en juiste inhoud zal worden gecontroleerd;
- direct tot intrekking van het PKIoverheid Certificaat zal worden overgaan en elk gebruik daarvan direct zal worden gestaakt wanneer:
    - er onvolledigheden en/of onjuistheden in het PKIoverheid Certificaat worden geconstateerd dan wel deze door gewijzigde omstandigheden dreigen te ontstaan of zijn ontstaan;
    - de Private sleutel is verloren, gestolen of anderszins gecompromitteerd is geraakt;
    - de QSCD, SUD, de toegangscodes van QSCD en SUD en/of andere autorisatiemiddelen dan wel activeringsgegevens in onbevoegde handen zijn gekomen of kunnen zijn gekomen;
    - de Private sleutel van KPN en/of de Staat der Nederlanden is verloren, gestolen of anderszins gecompromitteerd is geraakt.

6. Verplichtingen en garanties Vertrouwende Partij

6.1 De Vertrouwende Partij is verplicht om per geval zelfstandig te beoordelen of het gerechtvaardigd is om op een PKIoverheid Certificaat te vertrouwen. Nadrukkelijk wordt erop gewezen dat, daar waar het transacties van een substantiële financiële omvang

betreft, dan wel de transmissie van gegevens met een uitzonderlijk hoge economische waarde of gevoeligheid, een PKIoverheid Certificaat mogelijk niet voldoende betrouwbaarheid biedt, mede gezien de beperkte aansprakelijkheden van KPN.

6.2 Wil de Vertrouwende Partij in redelijkheid kunnen vertrouwen op een door de KPN uitgegeven PKIoverheid Certificaat, dan is ze verplicht om daaraan voorafgaand:

- de geldigheid van het PKIoverheid Certificaat te controleren door vast te stellen dat de datum einde geldigheid van het certificaat (voor identificatie/authenticatie en gekwalificeerde certificaten: op het moment van gebruik door de certificaathouder) nog niet voorbij was;
- de geldigheid van het PKIoverheid Certificaat te controleren door middel van de actuele Certificaten Revocatie Lijst (CRL) en/of Online Certificate Status Protocol (OCSP);
- de geldigheid van de hiërarchie te controleren waarbinnen het PKIoverheid Certificaat is uitgegeven, dat wil zeggen de geldigheid van Certificaten van bovenliggende CA's alsmede van het Stamcertificaat;
- kennis te nemen van en akkoord te gaan met deze Bijzondere Voorwaarden; en,
- Indien een Vertrouwende Partij wil vertrouwen op een certificaat dat hij/zij heeft ontvangen van een Gerechtsdeurwaarder (een lid van Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders) dient hij/zij, naast de hierboven genoemde controles, tevens te controleren of de in het certificaat genoemde Gerechtsdeurwaarder op de datum van het gebruik van het certificaat door de Gerechtsdeurwaarder vermeld is in het register waarnaar de in het certificaat opgenomen URL (http://www.registergerechtsdeurwaarders.nl) verwijst.
  Indien de Gerechtsdeurwaarder geschorst is op de datum van het gebruik van het certificaat door de Gerechtsdeurwaarder, kan en mag niet op het betreffende certificaat vertrouwd worden.
  Indien het register niet beschikbaar is, behoort de Vertrouwende Partij zelfstandig informatie in te winnen bij de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders teneinde vast te stellen of de Gerechtsdeurwaarder vermeld

is in het register dat bijgehouden wordt door de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders.

6.3 Indien een Vertrouwende Partij een redelijk vermoeden heeft van misbruik van het Certificaat waarop het wil vertrouwen, dan is het verplicht hiervan terstond melding te maken bij KPN.

7. Additionele verplichtingen servers/groepen

7.1 Indien Abonnee, in het geval van PKIoverheid Certificaten bestemd voor serverdomeinen, van de mogelijkheid gebruikmaakt om sleutels op softwarematige wijze te genereren, is Abonnee gehouden tenminste een naar het oordeel van KPN afdoende schriftelijke verklaring te overleggen inzake de (technische) maatregelen die zijn getroffen om te kunnen voldoen aan de hiervoor gestelde voorwaarde. KPN heeft te allen tijde het recht de naleving van zulke maatregelen te controleren en, indien Abonnee daarbij aantoonbaar in gebreke blijft, de dienstverlening op te schorten of te beëindigen totdat zulks is hersteld.

7.2 Voor wat betreft PKIoverheid Certificaten voor serverdomeinen of voor groepen geldt dat alle daarop van toepassing zijnde verplichtingen van de Certificaathouder eveneens integraal van toepassing zijn op de Certificaatbeheerder, inclusief maar niet beperkt tot de onder artikel 5.1 genoemde garanties.

7.3 Voor PKIoverheid Certificaten van het type Services Server geldt dat, indien de domeinnaam (FQDN), zoals vermeld in een Services Server Certificaat, identificeerbaar en adresseerbaar is via het internet, het betreffende Services Server Certificaat alleen op een server mag worden gezet [1]die bereikbaar is met één van de FQDN's, die in dat Services Server Certificaat vermeld staat.

7.4 Voor PKIoverheid Certificaten van het type Services Server geldt dat een dergelijk Certificaat alleen mag worden gebruikt in overeenstemming met de regelgeving die op de bedrijfsvoering van de Abonnee van toepassing is en alleen in relatie met de werkzaamheden van de Abonnee.

[1] Deze bepaling is niet van toepassing indien, in uitzonderingsgevallen, geen FQDN in het Certificaat wordt vermeld.

7.5 Voor PKIoverheid Certificaten van het type Services Server geldt dat de Abonnee geen gebruik meer zal en mag maken van de Private Sleutel behorende bij de Publieke Sleutel van het Certificaat, als de geldigheid van het desbetreffende Certificaat is verlopen of als het Certificaat is ingetrokken.

8. Additionele verplichtingen Beroepsgebonden Certificaten

8.1 De Beroepsgebonden Abonnee/Certificaathouder garandeert tegenover KPN en Vertrouwende Partijen dat direct tot intrekking van het PKIoverheid Certificaat zal worden overgegaan en elk gebruik daarvan direct zal worden gestaakt wanneer de Beroepsgebonden Abonnee/Certificaathouder het erkend beroep, het beroep waarvan hij/zij heeft aangetoond dat hij/zij dat uitoefent en zoals weergegeven in het Certificaat, niet langer uitoefent of niet langer mag uitoefenen en/of het authentieke bewijs voor het uitoefenen van dat beroep niet meer aanwezig of niet meer geldig is, ongeacht of dit tijdelijk of definitief is.

9. Beperkingen van gebruik

9.1 Eigendomsrechten met betrekking tot het PKIoverheid Certificaat, het QSCD en het SUD blijven ook na uitgifte berusten bij KPN en diens licentiegevers, inclusief rechten van intellectueel eigendom.

9.2 KPN verstrekt aan de Certificaathouder een niet-overdraagbaar en beperkt gebruiksrecht op het PKIoverheid Certificaat, het QSCD en het SUD gedurende de periode waarin het PKIoverheid Certificaat geldig is.

9.3 Het Persoonsgebonden en Beroepsgebonden PKIoverheid Certificaat, het voor de opslag ervan gebruikte QSCD, de toegangscodes van het QSCD, en de Private Sleutel zijn allen persoonsgebonden en op geen enkele wijze overdraagbaar aan andere natuurlijke personen of rechtspersonen.

9.4 Het Groepscertificaat wordt beheerd door een Certificaatbeheerder, deze beheert het Certificaat namens de Abonnee/Certificaathouder. Bij een Groepscertificaat is het

toegestaan dat de activeringsgegevens van de SUD door verschillende personen wordt gedeeld als het beheer en gebruik dat vereist. Echter aangeraden wordt het aantal personen dat kennis heeft van de activeringsgegevens te beperken en daartoe passende maatregelen te nemen.

9.5 Het is de Abonnee noch de Certificaathouder of Certificaatbeheerder toegestaan om het uiterlijk van het QSCD te wijzigen of anderszins aan te passen, inclusief de daarop vermelde (persoons)gegevens.

9.6 De Abonnee en de Certificaathouder zijn zelf verantwoordelijk voor applicaties en andere middelen nodig voor gebruikmaking van het PKIoverheid Certificaat, met uitzondering van het QSCD en het SUD.

10. Aansprakelijkheid

10.1 KPN is aansprakelijk voor directe schade die Abonnees en/of Vertrouwende Partijen ondervinden die in redelijkheid op een door KPN uitgegeven PKIoverheid Certificaat vertrouwen, doch enkel voor wat betreft schade ontstaan door toerekenbare tekortkomingen in de uitvoering van het navolgende:

- de garantie dat, op het tijdstip van uitgifte, alle gegevens in het PKIoverheid Certificaat juist zijn en dat daarin alle voorgeschreven gegevens zijn opgenomen;
- de garantie dat een verzoek tot intrekking van een PKIoverheid Certificaat tijdig wordt verwerkt, waarbij inbegrepen het bijwerken en publiceren van de status informatie van het PKIoverheid Certificaat;
- de garantie dat de in het PKIoverheid Certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het Certificaat, houder was van de gegevens voor het aanmaken van de handtekening die met de in het PKIoverheid Certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van de handtekening overeenstemmen; of,
- de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening, veronderstellende dat zij beide door KPN worden gegenereerd, complementair kunnen worden gebruikt; of

- de garantie dat de dienstverlening van KPN ten aanzien van het PKIoverheid Certificaat voldoet en blijft voldoen de relevante wet- en regelgeving in zijn algemeenheid en in het bijzonder ten aanzien van de hierboven genoemde punten, waarbij partijen vaststellen dat, indien ten gevolge van een omstandigheid toerekenbaar aan KPN, deze dienstverlening gecompromitteerd wordt, KPN geacht wordt niet aan alle bovengenoemde garanties (meer) te kunnen voldoen.

10.2 De aansprakelijkheid van KPN tegenover Abonnees en Vertrouwende Partijen voor het onder artikel 10.1 genoemde is beperkt tot een gezamenlijk bedrag van één miljoen euro (€ 1.000.000) per jaar, ongeacht het aantal incidenten. Onder geen enkele omstandigheid zal KPN gehouden zijn tot schadevergoeding boven deze limiet, tenzij aantoonbaar sprake is van grove nalatigheid danwel opzet van de zijde van KPN.

10.3 KPN aanvaardt jegens Abonnees en Vertrouwende Partijen geen aansprakelijkheid voor andere schade dan onder artikel 10.1 genoemd, waaronder begrepen doch niet beperkt tot:

- schade ten gevolge van niet-toerekenbare tekortkomingen in de nakoming (overmacht);
- schade die voortvloeit uit de niet-nakoming van de in deze voorwaarden beschreven verplichtingen van Abonnees, Certificaathouders, Certificaatbeheerders en/of Vertrouwende Partijen;
- schade ten gevolge van het verlies of anderszins verdwijnen van het PKIoverheid Certificaat, het Persoonlijk Identificatie Nummer, het QSCD, het SUD of de Private Sleutel;
- schade die voortvloeit uit gebruik van een PKIoverheid Certificaat buiten het daarvoor beschreven toepassingsgebied of buiten de in het PKIoverheid Certificaat aangegeven beperkingen;
- schade die voortvloeit uit het opnemen van grote aantallen domeinnamen (FQDN’s) in servercertificaten.

10.4 KPN aanvaardt jegens Abonnees en Vertrouwende Partijen geen aansprakelijkheid voor het gebruik dat KPN maakt van externe registers. KPN is

verantwoordelijk voor het zorgvuldig gebruik van deze registers, bijvoorbeeld bij het beoordelen van een aanvraag, maar is niet verantwoordelijk voor de juistheid en volledigheid ervan.

10.5 KPN aanvaardt geen enkele aansprakelijkheid jegens andere partijen of personen dan Abonnees en Vertrouwende Partijen, inclusief maar niet beperkt tot Certificaathouders en Certificaatbeheerders. In geval de handelingen van een derde partij leiden tot aansprakelijkstelling van KPN door een Certificaathouder, Certificaatbeheerder en/of Vertrouwende Partij, vrijwaart Abonnee KPN voor alle daaruit voortvloeiende schade, inclusief maar niet beperkt tot de kosten van verweer van de zijde van KPN.

10.6 KPN zal toereikende regelingen onderhouden om de aansprakelijkheden die verband houden met dit artikel af te dekken, onder andere in de vorm van verzekeringen.

11. Privacy

11.1 In zoverre relevant gaan de Abonnee, Certificaathouder en de Certificaatbeheerder ermee akkoord dat:

- KPN de door de Abonnee, Certificaathouder en de Certificaatbeheerder verstrekte persoonsgegevens mag gebruiken voor de uitgifte van het PKIoverheid Certificaat; en,
- KPN de inhoud van het PKIoverheid Certificaat openbaar mag maken voorzover dit nodig is voor het gebruik daarvan.

12. Additionele documentatie

12.1 De PKIoverheid CPS van KPN kan worden verkregen via https://certificaat.kpn.com/support/downloads of per email via pkio.servicedesk@kpn.com.

12.2 De Programma van Eisen en CPS van de PKI voor de Overheid kan worden verkregen via https://cps.pkioverheid.nl/