



## CERTIFICATE POLICY TESTcertificaten binnen de PKI voor de overheid

Datum 11 januari 2010

Domein Test:	
Test Authenticiteit	2.16.528.1.1003.1.2.9.1
Test Onweerlegbaarheid	2.16.528.1.1003.1.2.9.2
Test Vertrouwelijkheid	2.16.528.1.1003.1.2.9.3
Test Services - Authenticiteit	2.16.528.1.1003.1.2.9.4
Test Services - Vertrouwelijkheid	2.16.528.1.1003.1.2.9.5
Test Services - Server	2.16.528.1.1003.1.2.9.6
Test Apparaten - Authenticiteit	2.16.528.1.1003.1.2.9.7
Test Apparaten - Vertrouwelijkheid	2.16.528.1.1003.1.2.9.8
Test Apparaten - Combinatie	2.16.528.1.1003.1.2.9.9

## Colofon

Versienummer 1.2  
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

*Bezoekadres*

Wilhelmina van Pruisenweg 104

*Postadres*

Postbus 84011  
2508 AA DEN HAAG

T 0900 - 555 4555  
servicecentrum@logius.nl

## Inhoud

<b>Colofon</b> .....	<b>2</b>
<b>Inhoud</b> .....	<b>3</b>
<b>1 Introductie</b> .....	<b>6</b>
1.1 <i>Introductie PKI voor de overheid</i> .....	6
1.2 <i>Documentnaam en identificatie</i> .....	6
1.3 <i>Verhouding CP en CPS</i> .....	7
1.4 <i>Gebruikersgemeenschap</i> .....	8
1.5 <i>Certificaatgebruik</i> .....	8
1.6 <i>Beheer CP</i> .....	9
1.7 <i>Definities en afkortingen</i> .....	9
<b>2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats</b> .....	<b>10</b>
2.1 <i>Publicatie certificaat informatie</i> .....	10
2.2 <i>Beschikbaarheid CRL</i> .....	10
2.3 <i>Frequentie van publicatie</i> .....	10
<b>3 Identificatie en authenticatie</b> .....	<b>11</b>
3.1 <i>Naamgeving</i> .....	11
3.2 <i>Initiële identiteitsvalidatie</i> .....	11
3.2.1 <i>Interne testdoeleinden</i> .....	11
3.2.2 <i>Bestaande abonnee</i> .....	11
3.2.3 <i>Onbekende abonnee</i> .....	11
3.2.4 <i>Server testcertificaten</i> .....	11
<b>4 Operationele eisen certificaatcyclus</b> .....	<b>12</b>
4.1 <i>Aanvraag van certificaten</i> .....	12
4.2 <i>Uitgifte van certificaten</i> .....	12
4.3 <i>Vernieuwen van certificaten</i> .....	12
4.4 <i>Re-Key van certificaten</i> .....	12
4.5 <i>Aanpassing certificaten</i> .....	12
<b>5 Fysieke, procedurele en personele beveiliging</b> .....	<b>13</b>
5.1 <i>Fysieke beveiliging</i> .....	13
5.2 <i>Procedurele beveiliging</i> .....	13

5.3	<i>Personele beveiliging</i> .....	13
<b>6</b>	<b>Technische beveiliging</b> .....	<b>14</b>
6.1	<i>Genereren en installeren van sleutelparen</i> .....	14
6.2	<i>Bescherming van de signing key</i> .....	14
6.3	<i>Andere aspecten van sleutelpaar management</i> .....	14
6.4	<i>Logische toegangsbeveiliging</i> .....	14
<b>7</b>	<b>Certificaat- en CRL profielen</b> .....	<b>15</b>
7.1	<i>Certificaatprofielen</i> .....	15
7.1.1	<i>CertificatePolicies (Certificaatbeleid)</i> .....	15
7.1.2	<i>Persoonsgebonden eindgebruiker testcertificaten</i> .....	15
7.1.3	<i>Server- en Autonome Apparaten testcertificaten</i> .....	16
7.2	<i>CRL profiel</i> .....	16
<b>8</b>	<b>Conformiteitbeoordeling</b> .....	<b>17</b>
<b>9</b>	<b>Algemene en juridische bepalingen</b> .....	<b>18</b>
9.1	<i>Financiële verantwoordelijkheid en aansprakelijkheid</i> .....	18
9.2	<i>Intellectuele eigendomsrechten</i> .....	18
9.3	<i>Geldigheid CP</i> .....	18
9.4	<i>Wijzigingen</i> .....	18
9.5	<i>Toepasselijk recht</i> .....	18
9.6	<i>Overige bepalingen</i> .....	18

*Revisiegegevens*

<b>Versie</b>	<b>Datum</b>	<b>Status</b>	<b>Auteur</b>	<b>Manager</b>	<b>Omschrijving</b>
1.0	28-04-2009	Definitief	Policy Authority	T. Behre	-
1.1	17-11-2009	Definitief	Policy Authority	H. Verweij	Wijzigingen naar aanleiding van creatie TEST Domein CA Autonome Apparaten
1.2	11-01-2010	Definitief	Policy Authority	H. Verweij	Wijzigingen naar aanleiding van naamswijziging GBO.Overheid in Logius

# 1 Introductie

## 1.1 **Introductie PKI voor de overheid**

De PKI voor de overheid stelt burgers, ambtenaren en medewerkers van bedrijven in staat tot betrouwbare, elektronische communicatie met de overheid. Daarvoor is een architectuur ontworpen en ingericht die bestaat uit een hiërarchie met meerdere niveaus. Op elk niveau worden diensten geleverd conform strikte normen om de betrouwbaarheid van de gehele PKI voor de overheid zeker te stellen.

De Policy Authority (PA) is verantwoordelijk voor het beheer van de gehele infrastructuur. De PKI voor de overheid is zo opgezet dat externe organisaties, de Certification Service Providers (CSP's), onder voorwaarden toe kunnen treden tot de PKI voor de overheid. Deelnemende CSP's zijn verantwoordelijk voor de dienstverlening binnen de PKI voor de overheid. De PA ziet toe op de betrouwbaarheid van de gehele PKI voor de overheid

De PA-functie wordt uitgevoerd door Logius (<http://www.logius.nl/>), is een directie binnen het Ministerie van BZK en is verantwoordelijk voor het beheer en de doorontwikkeling van een aantal overheidsbrede ICT-voorzieningen.

## 1.2 **Documentnaam en identificatie**

De Certificate Policy *TEST*certificaten binnen de PKI voor de overheid (verder te noemen CP) heeft betrekking op de eisen die aan de dienstverlening, op het gebied van testcertificaten, van een Certification Service Provider (CSP) binnen de PKI voor de overheid worden gesteld.

Formeel wordt het voorliggend document aangeduid als 'Certificate Policy *TEST*certificaten binnen de PKI voor de overheid'.

CP	Omschrijving
Naamgeving	Certificate Policy <i>TEST</i> certificaten binnen de PKI voor de overheid

PKIoverheid onderscheidt drie typen persoonsgebonden testcertificaten en zes typen niet persoonsgebonden testcertificaten, te weten:

1. het persoonsgebonden testcertificaat voor authenticiteit;
2. het persoonsgebonden testcertificaat voor onweerlegbaarheid;
3. het persoonsgebonden testcertificaat voor vertrouwelijkheid;
4. het niet persoonsgebonden services testcertificaat voor authenticiteit;
5. het niet persoonsgebonden services testcertificaat voor vertrouwelijkheid;
6. het niet persoonsgebonden server testcertificaat;
7. het niet persoonsgebonden autonome apparaten testcertificaat voor authenticiteit;
8. het niet persoonsgebonden autonome apparaten testcertificaat voor vertrouwelijkheid;
9. het niet persoonsgebonden combinatie autonome apparaten testcertificaat.

De regels waaronder de hiervoor genoemde certificaten worden uitgegeven zijn gelijk. Daarom is besloten om de negen CP's voor deze negen certificaattypen op te nemen in één document. Voorliggend CP heeft derhalve betrekking op alle genoemde certificaten. Hoewel er daarmee één fysiek CP voor certificaten in de test hiërarchie van de PKI voor de overheid is, is er feitelijk sprake van negen logische CP's. De CP's kunnen via de volgende Object Identifiers (OID) worden geïdentificeerd:

OID	CP
2.16.528.1.1003.1.2.9.1	Test Authenticiteit
2.16.528.1.1003.1.2.9.2	Test Onweerlegbaarheid
2.16.528.1.1003.1.2.9.3	Test Vertrouwelijkheid
2.16.528.1.1003.1.2.9.4	Test Services – Authenticiteit
2.16.528.1.1003.1.2.9.5	Test Services – Vertrouwelijkheid
2.16.528.1.1003.1.2.9.6	Test Services - Server
2.16.528.1.1003.1.2.9.7	Test Apparaten - Authenticiteit
2.16.528.1.1003.1.2.9.8	Test Apparaten - Vertrouwelijkheid
2.16.528.1.1003.1.2.9.9	Test Apparaten - Combinatie

De OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse organisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). domein test (9). test authenticiteit (1)/test onweerlegbaarheid (2)/test vertrouwelijkheid (3)/ test services – authenticiteit (4)/ test services – vertrouwelijkheid (5)/ test services – server (6)/ test apparaten – authenticiteit (7)/ test apparaten – vertrouwelijkheid (8)/ test apparaten – combinatie (9).

### 1.3 Verhouding CP en CPS

Voorliggend CP beschrijft de minimumeisen die zijn gesteld aan de dienstverlening, op het gebied van testcertificaten, van een Certification Service Provider (CSP) binnen de PKI voor de overheid. De Certification Practice Statement *TEST*certificaten binnen de PKI voor de overheid geeft aan op welke wijze invulling is gegeven aan deze eisen, voor zover dat valt onder directe verantwoordelijkheid van de PA.

#### 1.4 **Gebruikersgemeenschap**

De gebruikersgemeenschap binnen het domein Test komt overeen met, en is beperkt tot, de gebruikersgemeenschap in het domein Organisatie en Autonome Apparaten uit de productie hiërarchie en bestaat uit abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn en uit certificaathouders, die bij deze abonnees behoren. Daarnaast zijn er vertrouwende partijen. De vertrouwende partijen dienen zich er van bewust te zijn dat het gebruik van testcertificaten alleen beperkt is tot testsituaties en hieraan dus geen vertrouwen kan worden ontleend.

Uitgifte van testcertificaten door een (aspirant) CSP in het test domein TRIAL PKIoverheid Burger TEST CA - G2 is alleen mogelijk met *expliciete toestemming* van de Policy Authority van PKIoverheid.

#### 1.5 **Certificaatgebruik**

Binnen de PKIoverheid test hiërarchie uitgegeven eindgebruiker testcertificaten mogen uitsluitend gebruikt worden voor testdoeleinden.

Testdoeleinden m.b.t. Server/SSL testcertificaten en Autonome Apparaten testcertificaten, waaronder verstaan maar niet limitatief:

- Het eindgebruiker testcertificaat wordt door de CSP gebruikt t.b.v. haar eigen testdoeleinden;
- Het eindgebruiker testcertificaat wordt gebruikt om een niet in productie zijnde applicatie, aanwezig op een test url, of een autonoom apparaat te testen op de wijze waarop deze omgaat met certificaten;
- Door middel van het aanvragen van een eindgebruiker testcertificaat wordt ervaring opgedaan met het generen van een Certificate Service Request (CSR) en implementeren van een SSL (test)certificaat.

Testdoeleinden overige Service certificaten en Persoonsgebonden certificaten, waaronder verstaan maar niet limitatief:

- Het eindgebruiker testcertificaat wordt door de CSP gebruikt t.b.v. haar eigen testdoeleinden;
- Het eindgebruiker testcertificaat wordt gebruikt om in een test- of productieomgeving ervaring op te doen met het gebruik van Persoonsgebonden certificaten.

De (aspirant) CSP's kunnen de test hiërarchie gebruiken voor interne testdoeleinden (= uitsluitend voor testdoeleinden binnen de eigen organisatie van de CSP) b.v. voor de overgang naar het nieuwe SHA256 algoritme en/of de nieuwe sleutellengte. De eisen in paragraaf 2, 3.2.2, 3.2.3, 3.2.4, 4.1 en 7.1.2 in deze CP zijn hierbij niet van toepassing.

De (voorlopig) toegetreden CSP's kunnen en mogen onder de test hiërarchie ook eindgebruiker testcertificaten, t.b.v. testdoeleinden, aan derden (= buiten de eigen organisatie van de CSP) uitgegeven. Alle eisen in deze CP zijn hierbij onverkort van toepassing.

## **1.6 Beheer CP**

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor dit CP. Het ministerie heeft deze taak gedelegeerd aan Logius. Dit omvat ook het goedkeuren van wijzigingen op dit CP.

Contactgegevens:

Policy Authority PKIoverheid

Wilhelmina van Pruisenweg 104

Postbus 84011

2508 AA DEN HAAG

<http://www.logius.nl/pkioverheid>

Algemeen telefoonnummer: 0900-555 4555

Algemeen faxnummer: (070) 888 78 82

## **1.7 Definities en afkortingen**

Voor een overzicht van de gebruikte definities en afkortingen wordt verwezen naar <http://www.logius.nl/begrippenlijst/>.

## 2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

### 2.1 **Publicatie certificaat informatie**

De CSP moet in ieder geval gebruik maken van een CRL om de test certificaatstatus informatie beschikbaar te stellen.

### 2.2 **Beschikbaarheid CRL**

Geen nadere eisen.

### 2.3 **Frequentie van publicatie**

Geen nadere eisen.

## 3 Identificatie en authenticatie

### 3.1 **Naamgeving**

Om duidelijk te maken dat het gaat om testcertificaten, worden bij de naamformatie die wordt gehanteerd de woorden TRIAL en TEST gebruikt. Dit geldt voor alle certificaten in de test hiërarchie. Zie verder hoofdstuk 7 in deze CP.

### 3.2 **Initiële identiteitsvalidatie**

#### 3.2.1 *Interne testdoeleinden*

Wanneer de CSP testcertificaten aanvraagt en maakt voor zichzelf, is identiteitsvalidatie niet noodzakelijk.

#### 3.2.2 *Bestaande abonnee*

Als de abonnee en diens contactpersoon (degene die namens de abonnee de certificaten aanvraagt en dergelijke) al bekend zijn bij de CSP dan hoeft er geen nieuwe identiteitsvalidatie plaats te vinden.

#### 3.2.3 *Onbekende abonnee*

Als de abonnee en diens contactpersoon niet bekend zijn bij de CSP en testcertificaten wil aanvragen, dan moet de CSP de volgende activiteiten verrichten:

- De CSP dient te verifiëren dat de abonnee een bestaande organisatie is;
- De CSP dient te verifiëren dat de door de abonnee aangemelde organisatiename die in het certificaat wordt opgenomen juist en volledig is;
- De CSP dient een overeenkomst af te sluiten met de abonnee;
- De CSP dient een kopie geldig identiteitsbewijs van de vertegenwoordiger van de abonnee te ontvangen.

#### 3.2.4 *Server testcertificaten*

Bij test servercertificaten moet de CSP een controle uitvoeren bij de erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) of de abonnee de eigenaar is van de domeinnaam.

## 4 Operationele eisen certificaatcyclus

### 4.1 **Aanvraag van certificaten**

De CSP dient de abonnee te laten verklaren dat het testcertificaat alleen wordt gebruikt ten behoeve van testdoeleinden.

### 4.2 **Uitgifte van certificaten**

Uitsluitend een CSP die (voorlopig) is toetreden tot de PKI voor de overheid kan en mag testcertificaten aan derden uitgeven onder de testhiërarchie van de PKI voor de overheid.

Aspirant CSP's mogen, nadat de Policy Authority van de PKI voor de overheid hiervoor expliciet toestemming heeft gegeven, uitsluitend voor interne testdoeleinden (= binnen de eigen organisatie van de CSP), gebruik maken van de testhiërarchie van de PKI voor de overheid.

### 4.3 **Vernieuwen van certificaten**

Certificaten dienen te worden vernieuwd wanneer (een deel van) de informatie die aan het certificaat ten grondslag ligt is veranderd of verouderd. Sleutels van certificaathouders mogen niet opnieuw worden gebruikt na het verstrijken van de geldigheidsduur of na het intrekken van het bijbehorende testcertificaat. Met het vernieuwen van testcertificaten wordt ook het sleutelbaar vernieuwd.

### 4.4 **Re-Key van certificaten**

Indien na het verstrijken van de geldigheidsduur of na het intrekken, nieuwe testcertificaten worden aangevraagd, dan moeten hiervoor nieuwe sleutelparen en nieuwe testcertificaten worden aangemaakt.

### 4.5 **Aanpassing certificaten**

Indien aanpassing van certificaten noodzakelijk is, moeten de testcertificaten worden ingetrokken en moeten nieuwe testcertificaten met gewijzigde gegevens worden aangevraagd.

## 5 Fysieke, procedurele en personele beveiliging

### 5.1 Fysieke beveiliging

Er dienen passende maatregelen te worden genomen op basis van een risicoanalyse waarbij rekening wordt gehouden met de van toepassing zijnde risicofactoren.

### 5.2 Procedurele beveiliging

Er dienen passende maatregelen te worden genomen op basis van een risicoanalyse waarbij rekening wordt gehouden met de van toepassing zijnde risicofactoren.

### 5.3 Personele beveiliging

Er dienen passende maatregelen te worden genomen op basis van een risicoanalyse waarbij rekening wordt gehouden met de van toepassing zijnde risicofactoren.

## 6 Technische beveiliging

### 6.1 Genereren en installeren van sleutelparen

Binnen de test hiërarchie van de PKI voor de overheid moet als algoritme voor de handtekening sha256WithRSAEncryption worden gebruikt.

De volgende sleutellengtes zijn van toepassing:

Eindgebruiker testcertificaten	2048 bit RSA sleutels
CSP testcertificaten	4096 bit RSA sleutels
Sub CA testcertificaten	4096 bit RSA sleutels
Domein testcertificaten	4096 bit RSA sleutels
Test stamcertificaat	4096 bit RSA sleutels

### 6.2 Bescherming van de signing key

Er dienen passende maatregelen te worden genomen op basis van een risicoanalyse waarbij rekening wordt gehouden met de van toepassing zijnde risicofactoren.

### 6.3 Andere aspecten van sleutelpaar management

Alle testcertificaten hebben een maximale periode van geldigheid:

Eindgebruiker testcertificaten	6 maanden
Interne Eindgebruiker testcertificaten <sup>1</sup>	Geen bepalingen
CSP testcertificaten	12 jaar minus 2 dagen
Domein testcertificaten	12 jaar minus 1 dag
Test stamcertificaat	12 jaar

### 6.4 Logische toegangsbeveiliging

Er dienen passende maatregelen te worden genomen op basis van een risicoanalyse waarbij rekening wordt gehouden met de van toepassing zijnde risicofactoren.

---

<sup>1</sup> Deze testcertificaten mogen uitsluitend gebruikt worden door de (aspirant) CSP zelf voor het testen van wijzigingen voordat deze in de productieomgeving van de (aspirant) CSP worden geïmplementeerd. Deze testcertificaten mogen niet aan derden worden verstrekt.

## 7 Certificaat- en CRL profielen

### 7.1 Certificaatprofielen

#### 7.1.1 *CertificatePolicies (Certificaatbeleid)*

Het veld/attribuut *CertificatePolicies* (Certificaatbeleid) in de eindgebruiker testcertificaten moet de van toepassing zijnde OID bevatten van deze CP en de URI van het Certification Practice Statement *TEST*certificaten binnen de PKI voor de overheid:

- Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in deze CP, zie hiervoor paragraaf 1.2;
- URI Certification Practice Statement *TEST*certificaten binnen de PKI voor de overheid:
- Domein TRIAL PKIoverheid Organisatie TEST CA - G2 moet als URI <http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2> worden aangehouden.
- Domein TRIAL PKIoverheid Autonome Apparaten TEST CA - G2 moet als URI <http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2> worden aangehouden.

De (aspirant) CSP hoeft niet zelf een TEST CPS te schrijven en te publiceren.

#### 7.1.2 *Persoonsgebonden eindgebruiker testcertificaten*

Bij de persoonsgebonden eindgebruiker testcertificaten (2.16.528.1.1003.1.2.9.1, 2.16.528.1.1003.1.2.9.2 en 2.16.528.1.1003.1.2.9.3) moet bij het subject/onderwerp veld de Common name van de CSP worden opgenomen en niet de naam van de eindgebruiker. Dit betekent dat bij de invulling van het subject/onderwerp veld de *Subject.commonName* overeenkomt met de *Issuer.commonName*. Bij de *Subject.organizationName* (O) en, indien van toepassing, de *Subject.organizationunit* (OU) moet de naam van de organisatie worden opgenomen met daarvoor de vermelding TRIAL en daarachter TEST.

Voorbeeld persoonsgebonden testcertificaat:

CN = TRIAL PKIoverheid <<naam CSP>> TEST CA - G2

O = TRIAL <<Naam organisatie>> TEST

OU = TRIAL <<Naam organisatieonderdeel>> TEST

C = NL

Bij de persoonsgebonden testcertificaten mag het *id-etsi-qcs-QcCompliance* statement niet worden opgenomen.

### 7.1.3 *Server- en Autonome Apparaten testcertificaten*

Bij server testcertificaten moet bij het subject/onderwerp veld bij Common name de test url worden opgenomen. Bij server- en Autonome Apparaten testcertificaten moet bij het O veld en, indien van toepassing, het OU veld de naam van de organisatie worden opgenomen met daarvoor de vermelding TRIAL en daarachter TEST.

Voorbeeld test servercertificaat:

CN = [www.testurl.nl](http://www.testurl.nl)

O = TRIAL <<Naam organisatie>> TEST

OU = TRIAL <<Naam organisatieonderdeel>> TEST

C = NL

Voorbeeld test autonome apparatencertificaat:

CN = Het type goedkeuringsnummer van het betreffende test apparaat of een (korte) omschrijving van het specifieke soort test Autonoom Apparaat;

O = TRIAL <<Naam organisatie>> TEST

OU = TRIAL <<Naam organisatieonderdeel>> TEST

C = NL

## 7.2 **CRL profiel**

Moet duidelijk zijn dat het om een TEST c.q. TRIAL CRL gaat.

## 8 Conformiteitbeoordeling

Voor de test hiërarchie vindt geen conformiteitbeoordeling plaats.

## 9 Algemene en juridische bepalingen

### 9.1 Financiële verantwoordelijkheid en aansprakelijkheid

Bepalingen omtrent aansprakelijkheid, m.b.t. de test hiërarchie, van BZK jegens een (aspirant) CSP zijn opgenomen in een overeenkomst dan wel convenant tussen BZK en de (aspirant) CSP.

### 9.2 Intellectuele eigendomsrechten

Voorliggend CP is eigendom van Logius.

### 9.3 Geldigheid CP

Dit is versie 1.1 van het document "Certificate Policy TESTcertificaten binnen de PKI voor de overheid" uit te geven door de Policy Authority van de PKI voor de overheid, november 2009.

Het CP is geldig vanaf de datum van uitgifte. Het CP is geldig zolang de dienstverlening van het PKIoverheid voortduurt of totdat het CP wordt vervangen door een nieuwere versie. Nieuwere versies worden aangeduid met een hoger versienummer (vX.x). Bij ingrijpende wijzigingen wordt het versienummer opgehoogd met 1, bij redactionele aanpassingen wordt het versienummer opgehoogd met 0.1. Nieuwere versies worden gepubliceerd op de website van PKIoverheid.

### 9.4 Wijzigingen

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor dit CP. Het ministerie heeft deze taak gedelegeerd aan Logius. Dit omvat ook het goedkeuren van wijzigingen op dit CP.

Alle wijzigingen die niet tot de categorie van wijzigingen van redactionele aard behoren worden bekend gesteld en leiden tot een nieuwe versie van het CP. Wijzigingen van redactionele aard zijn geen aanleiding een nieuwe versie van het CP te publiceren.

### 9.5 Toepasselijk recht

Op de overeenkomst dan wel het convenant tussen BZK en de CSP is het Nederlands recht van toepassing.

### 9.6 Overige bepalingen

Tussen BZK en de CSP's is een overeenkomst dan wel convenant gesloten met betrekking tot het leveren van test certificaten onder de test hiërarchie van de PKI voor de overheid.