



Logius  
*Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties*

## CERTIFICATION PRACTICE STATEMENT

TESTcertificaten binnen de PKI voor de  
overheid

Datum      11 januari 2010

## Colofon

Versienummer 1.2  
Contactpersoon Policy Authority PKIoverheid

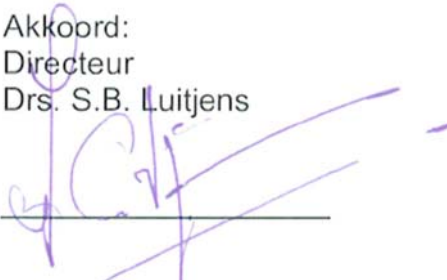
Organisatie Logius

*Bezoekadres*  
Wilhelmina van Pruisenweg 104

*Postadres*  
Postbus 84011  
2508 AA DEN HAAG

T 0900 - 555 4555  
servicecentrum@logius.nl

Akkoord:  
Directeur  
Drs. S.B. Luitjens



## Inhoud

<b>Colofon</b> .....	<b>2</b>
<b>Inhoud</b> .....	<b>3</b>
<b>1 Introductie</b> .....	<b>7</b>
1.1 <i>Introductie PKI voor de overheid</i> .....	7
1.2 <i>Documentnaam en identificatie</i> .....	8
1.3 <i>Verhouding CPS en CP</i> .....	9
1.4 <i>Betrokken partijen</i> .....	9
1.5 <i>Certificaatgebruik</i> .....	10
1.6 <i>Beheer CPS</i> .....	10
1.7 <i>Definities en afkortingen</i> .....	10
<b>2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats</b> .....	<b>11</b>
2.1 <i>Elektronische opslagplaats</i> .....	11
2.2 <i>Publicatie certificaat informatie</i> .....	11
2.3 <i>Frequentie van publicatie</i> .....	12
2.4 <i>Toegang tot publicatie</i> .....	12
<b>3 Naamgeving</b> .....	<b>13</b>
3.1 <i>Naamgeving</i> .....	13
3.2 <i>Initiële identiteitsvalidatie</i> .....	14
3.3 <i>Identificatie en authenticatie bij vernieuwing van het certificaat</i> .....	14
3.4 <i>Identificatie en authenticatie bij verzoeken tot intrekking</i> ..	14
<b>4 Operationele eisen certificaatcyclus</b> .....	<b>15</b>
4.1 <i>Aanvraag van certificaten</i> .....	15
4.2 <i>Werkwijze met betrekking tot aanvraag van certificaten</i> ....	15
4.3 <i>Uitgifte van certificaten</i> .....	15
4.4 <i>Acceptatie van certificaten</i> .....	15
4.5 <i>Sleutelbaar en certificaatgebruik</i> .....	15
4.6 <i>Vernieuwen van certificaten</i> .....	15
4.7 <i>Intrekking en opschorting van certificaten</i> .....	15
4.8 <i>Certificaat statusservice</i> .....	16

4.9	<i>Beëindiging abonnee relatie</i> .....	16
4.10	<i>Key escrow en recovery</i> .....	16
<b>5</b>	<b>Fysieke, procedurele en personele beveiliging</b> .....	<b>17</b>
5.1	<i>Fysieke beveiliging</i> .....	17
5.2	<i>Procedurele beveiliging</i> .....	17
5.3	<i>Personele beveiliging</i> .....	17
5.4	<i>Procedures ten behoeve van beveiligingsaudits</i> .....	17
5.5	<i>Archivering en back-up</i> .....	17
5.6	<i>Vernieuwen sleutels</i> .....	17
5.7	<i>Aantasting en continuïteit</i> .....	17
5.8	<i>Beëindiging PKIoverheid</i> .....	17
<b>6</b>	<b>Technische beveiliging</b> .....	<b>19</b>
6.1	<i>Genereren en installeren van sleutelparen</i> .....	19
6.2	<i>Bescherming van de signing key</i> .....	19
6.3	<i>Andere aspecten van sleutelpaar management</i> .....	19
6.4	<i>Activeringsgegevens</i> .....	19
6.5	<i>Logische toegangsbeveiliging</i> .....	19
6.6	<i>Netwerkbeveiliging</i> .....	19
6.7	<i>Time stamping</i> .....	19
<b>7</b>	<b>Certificaat- en CRL profielen</b> .....	<b>20</b>
7.1	<i>Certificaatprofielen</i> .....	20
7.2	<i>CRL profiel</i> .....	20
<b>8</b>	<b>Conformiteitbeoordeling</b> .....	<b>21</b>
<b>9</b>	<b>Algemene en juridische bepalingen</b> .....	<b>22</b>
9.1	<i>Tarieven</i> .....	22
9.2	<i>Financiële verantwoordelijkheid en aansprakelijkheid</i> .....	22
9.3	<i>Vertrouwelijkheid bedrijfsgegevens</i> .....	22
9.4	<i>Vertrouwelijkheid persoonsgegevens</i> .....	22
9.5	<i>Intellectuele eigendomsrechten</i> .....	22
9.6	<i>Aansprakelijkheid en garanties</i> .....	22
9.7	<i>Uitsluiting van garantie</i> .....	22
9.8	<i>Beperking aansprakelijkheid</i> .....	22
9.9	<i>Schadeloosstelling</i> .....	22
9.10	<i>Geldigheid CPS</i> .....	22

9.11	<i>Communicatie binnen betrokken partijen</i>	23
9.12	<i>Wijzigingen</i>	23
9.13	<i>Conflictoplossing</i>	23
9.14	<i>Toepasselijk recht</i>	23
9.15	<i>Naleving relevante wetgeving</i>	23
9.16	<i>Overige bepalingen</i>	23

<b>Bijlage A. Inhoud velden test stamcertificaten en test domeincertificaten</b>	<b>25</b>
--	-----------

<b>Bijlage B. Inhoud velden CRL voor test domeincertificaten en test CSP-certificaten</b>	<b>28</b>
---	-----------

*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 n.a.v. 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.

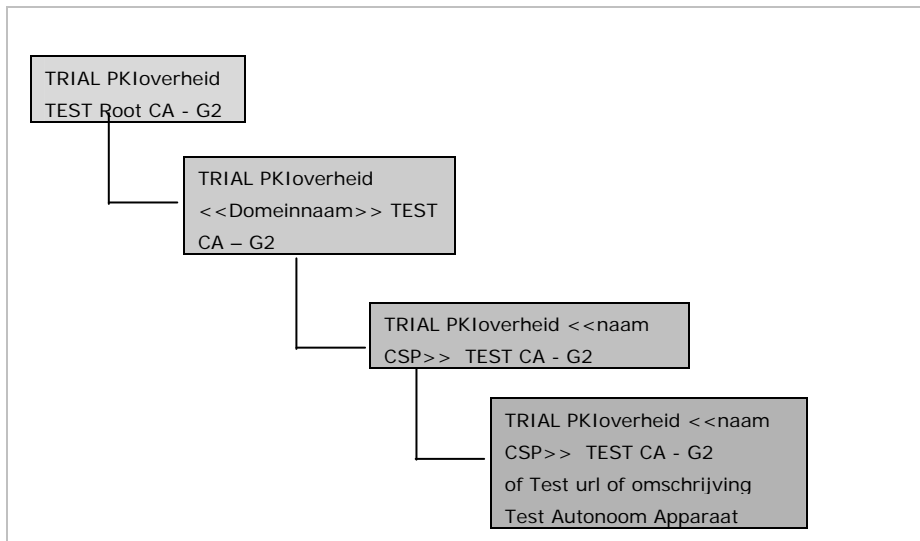
De Policy Authority (PA) is verantwoordelijk voor het beheer van de gehele infrastructuur. De PKI voor de overheid is zo opgezet dat externe organisaties, de Certification Service Providers (CSP's), onder voorwaarden toe kunnen treden tot de PKI voor de overheid. Deelnemende CSP's zijn verantwoordelijk 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>), onderdeel van het Directoraat-Generaal Bestuur en Koninkrijksrelaties, is een directie binnen het Ministerie van BZK en is verantwoordelijk voor het beheer en de doorontwikkeling van een aantal overheidsbrede ICT-voorzieningen.

Naast de productie hiërarchie, zoals beschreven in PKIoverheid PvE deel 1 bij paragraaf 2.4 "Inrichting PKI voor de overheid", ten behoeve van uitgifte van PKI voor de overheid certificaten, is er ook een test hiërarchie met meerdere niveaus gecreëerd. Deze test hiërarchie, met een vergelijkbare structuur als de productie hiërarchie, heeft twee doelstellingen:

- A. De (aspirant) CSP kan 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;
- B. 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) uitgeven.

Binnen de test hiërarchie van de PKI voor de overheid is als algoritme voor de handtekening sha256WithRSAEncryption van toepassing. De test hiërarchie bestaat uit de volgende niveaus:



## 1.2 Documentnaam en identificatie

De Certification Practice Statement TESTcertificaten binnen de PKI voor de overheid (verder te noemen CPS) biedt informatie aan *CSP's, abonnees, vertrouwende partijen en certificaathouders* over de procedures en getroffen maatregelen ten aanzien van de dienstverlening van de PA met betrekking tot testcertificaten. Het CPS beschrijft de processen, procedures en beheersingsmaatregelen voor het aanvragen, produceren, verstrekken, beheren en intrekken van testcertificaten. Voor zover dat valt onder directe verantwoordelijkheid van de PA. Het CPS geeft geén inzicht in de werking van de operationele c.q. productie hiërarchie van de PKI voor de overheid. De algemene indeling van dit CPS volgt het model zoals gepresenteerd in Request for Comments 3647<sup>1</sup>.

Formeel wordt het voorliggend document aangeduid als 'Certification Practice Statement TESTcertificaten binnen de PKI voor de overheid'.

CPS	Omschrijving
Naamgeving	Certification Practice Statement TESTcertificaten binnen de PKI voor de overheid
Link	<a href="http://www.pkioverheid.nl/policies/TESTroot-policy-G2">http://www.pkioverheid.nl/policies/TESTroot-policy-G2</a> <a href="http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2">http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2</a> <a href="http://www.pkioverheid.nl/policies/TESTdom-bu-policy-G2">http://www.pkioverheid.nl/policies/TESTdom-bu-policy-G2</a> <a href="http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2">http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2</a>
OID	n.v.t.

<sup>1</sup> <http://www.ietf.org/rfc/rfc3647.txt?number=3647>

### 1.3 **Verhouding CPS en CP**

Voorliggend CPS beschrijft op welke wijze invulling is gegeven aan de eisen, zoals beschreven in de Certificate Policy TESTcertificaten binnen de PKI voor de overheid. Voor zover dat valt onder directe verantwoordelijkheid van de PA.

### 1.4 **Betrokken partijen**

Bij de PKI voor de overheid kennen wij de navolgende betrokken partijen:

1. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK);
2. PA;
3. CSP;
4. Abonnee;
5. Certificaathouder;
6. Vertrouwende partij.

*Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)* is verantwoordelijk voor de PKI voor de overheid. BZK neemt beslissingen met betrekking tot de inrichting van de infrastructuur en de deelname van CSP's aan de PKI voor de overheid. De directeur van Logius vertegenwoordigt BZK in deze.

De *PA* is verantwoordelijk voor het beheer van het centrale deel<sup>2</sup> van de PKIoverheid test infrastructuur en het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de TESTroot van de PKI voor de overheid testcertificaten uitgeven.

Een *CSP* heeft als functie het verstrekken en beheren van testcertificaten en sleutel informatie, met inbegrip van de hiervoor voorziene dragers (bijvoorbeeld smartcards). De CSP heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatediensten.

Een *abonnee* gaat een overeenkomst aan met een CSP namens één of meer certificaathouders.

Hoe de levering van testcertificaten door de CSP aan die certificaathouders plaatsvindt, regelen de abonnee en de CSP onderling.

De *certificaathouder* is de houder van de private sleutel behorend bij de publieke sleutel die in het testcertificaat vermeld is. Op alle niveaus in de test hiërarchie van de PKI voor de overheid bevinden zich certificaathouders. Binnen de domeinen ontvangen eindgebruikers (personen) de testcertificaten van de CSP's. De PA geeft testcertificaten uit aan zichzelf (teststamcertificaat en testdomeincertificaten) en aan CSP's (test CSP-certificaten).

De *vertrouwende partij* is de ontvanger van een testcertificaat dat is uitgegeven binnen de PKI voor de overheid. 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.

---

<sup>2</sup> Het centrale deel betreft de Test Root CA, Test Domeinen CA's en de Test CSP CA's

### **1.5 Certificaatgebruik**

De TRIAL PKIoverheid TEST Root CA - G2 en alle testcertificaten die daaronder worden gecreëerd en uitgegeven kunnen en mogen NIET gebruikt worden voor andere doeleinden dan testdoeleinden.

Dit betekent dat de TRIAL PKIoverheid TEST Root CA - G2 en alle testcertificaten die daaronder zijn en worden gecreëerd en uitgegeven NIET gebruikt kunnen en mogen worden voor de elektronische handtekening (onweerlegbaarheid) in het kader van de Wet elektronische handtekeningen.

Dit betekent tevens dat de TRIAL PKIoverheid TEST Root CA - G2 en alle testcertificaten die daaronder zijn en worden gecreëerd en uitgegeven NIET gebruikt kunnen en mogen worden voor het authenticeren van de identiteit van een abonnee en/of een eindgebruiker en/of service en/of autonoom apparaat. Tevens kunnen en mogen de testcertificaten NIET gebruikt worden voor het beschermen van de vertrouwelijkheid van gegevens en het beveiligen van een verbinding tussen een bepaalde client en een server.

### **1.6 Beheer CPS**

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

Contactgegevens:

Policy Authority PKIoverheid  
Wilhelmina van Pruisenweg 104  
Postbus 84011  
2508 AA DEN HAAG

<http://www.pkioverheid.nl>

Algemeen telefoonnummer: (070) 888 75 00

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.pkioverheid.nl/begrippenlijst/>.

## 2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

### 2.1 Elektronische opslagplaats

Op de website van de PA, [www.pkioverheid.nl](http://www.pkioverheid.nl), zullen de volgende zaken worden gepubliceerd:

1. De test stam- en domeincertificaten;
2. De test CSP certificaten;
3. De CP;
4. Dit CPS;

De CRL's van de test stam- en domeincertificaten zijn te vinden op <http://crl.pkioverheid.nl/pkiotest>

Op de websites van de verschillende CSP's zijn de CRL's t.b.v. de eindgebruiker testcertificaten te vinden.

### 2.2 Publicatie certificaat informatie

De volgende testcertificaten worden gepubliceerd:

5. TRIAL PKIoverheid TEST Root CA - G2;
6. TRIAL PKIoverheid Organisatie TEST CA - G2;
7. TRIAL PKIoverheid Burger TEST CA - G2;
8. TRIAL PKIoverheid Autonome Apparaten TEST CA - G2;
9. TRIAL PKIoverheid <<naam CSP>> TEST CA - G2.

De volgende CRL's worden gepubliceerd:

10. TRIAL G2 domein-certificaten;
11. CSP-certificaten onder TRIAL G2 domein Organisatie;
12. CSP-certificaten onder TRIAL G2 domein Burger;
13. CSP-certificaten onder TRIAL G2 domein Autonome Apparaten.

Dit CPS is te vinden op de volgende url's:

14. <http://www.pkioverheid.nl/policies/TESTroot-policy-G2>
15. <http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2>
16. <http://www.pkioverheid.nl/policies/TESTdom-bu-policy-G2>
17. <http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2>

Url 1 is te vinden in het veld "Certificaatbeleid" van het TRIAL PKIoverheid TEST Root CA - G2 certificaat. Url 2 is te vinden in het veld "Certificaatbeleid" van het TRIAL PKIoverheid Organisatie TEST CA - G2 certificaat en de Level 3 en 4 testcertificaten die onder dit domein worden uitgegeven. Url 3 is te vinden in het veld "Certificaatbeleid" van het TRIAL PKIoverheid Burger TEST CA - G2 certificaat en de Level 3 en 4 testcertificaten die onder dit domein worden uitgegeven. Url 4 is te vinden in het veld "Certificaatbeleid" van het TRIAL PKIoverheid Autonome Apparaten TEST CA - G2 certificaat en de Level 3 en 4 testcertificaten die onder dit domein worden uitgegeven.

De CRL's zijn te vinden op de volgende url's:

18. Ingetrokken Test domeincertificaten:

<http://crl.pkioverheid.nl/pkiotest/TESTRootLatestCRL-G2.crl>

19. Ingetrokken Test CSP certificaten:

<http://crl.pkioverheid.nl/pkiotest/TESTDomOrganisatieLatestCRL-G2.crl>

<http://crl.pkioverheid.nl/pkiotest/TESTDomBurgerLatestCRL-G2.crl>

<http://crl.pkioverheid.nl/pkiotest/TESTDomAutonomeApparatenLatestCRL-G2.crl>

### **2.3 Frequentie van publicatie**

De PA publiceert de lijsten met ingetrokken certificaten, de Certificate Revocation Lists (CRL's). Er is een CRL met ingetrokken test domeincertificaten. Deze CRL wordt jaarlijks opnieuw gepubliceerd. Ad hoc publicatie van deze CRL vindt plaats na intrekking van een test domeincertificaat. Per domein is er een CRL met ingetrokken test CSP-certificaten binnen dat domein. De CRL met ingetrokken test CSP-certificaten wordt standaard elke drie maanden opnieuw gepubliceerd. Ad hoc publicatie van de CRL met ingetrokken test CSP-certificaten vindt plaats na intrekking van een test CSP-certificaat. Elke CRL bevat het tijdstip van de volgende geplande CRL-uitgifte.

Op de websites van de verschillende CSP's zijn de CRL's t.b.v. de eindgebruiker testcertificaten te vinden. M.b.t. de beschikbaarheid en frequentie van publicatie voor deze CRL's zijn geen nadere eisen gesteld.

### **2.4 Toegang tot publicatie**

Gepubliceerde informatie is publiek van aard en vrij toegankelijk.

## 3 Naamgeving

### 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. Binnen de test hiërarchie is de naamformatie van de Common name (CN) als volgt:

(Level 1)	Issuer/verlener:	TRIAL	PKIoverheid		TEST	Root	CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid		TEST	Root	CA - G2
(Level 2)	Issuer/verlener:	TRIAL	PKIoverheid		TEST	Root	CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid	Organisatie	TEST		CA - G2
(Level 2)	Issuer/verlener:	TRIAL	PKIoverheid		TEST	Root	CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid	Burger	TEST		CA - G2
(Level 2)	Issuer/verlener:	TRIAL	PKIoverheid		TEST	Root	CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid	Autonome Apparaten	TEST		CA - G2
(Level 3)	Issuer/verlener:	TRIAL	PKIoverheid	Organisatie	TEST		CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid	<<naam CSP>>	TEST		CA - G2
(Level 3)	Issuer/verlener:	TRIAL	PKIoverheid	Burger	TEST		CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid	<<naam CSP>>	TEST		CA - G2
(Level 3)	Issuer/verlener:	TRIAL	PKIoverheid	Autonome Apparaten	TEST		CA - G2
	Subject/onderwerp:	TRIAL	PKIoverheid	<<naam CSP>>	TEST		CA - G2
(Level 4)	Issuer/verlener:	TRIAL	PKIoverheid	<<naam CSP>>	TEST		CA - G2
	Persoonsgebonden testcertificaten:						
	Subject/onderwerp:	TRIAL	PKIoverheid	<<naam CSP>>	TEST		CA - G2
	<u>Server testcertificaten:</u>						
	Subject/onderwerp:	<a href="http://www.testurl.nl">www.testurl.nl</a>					
	<u>Autonome Apparaten</u>						

	<u>testcertificaten</u>						
	Subject/onderwerp:	Het typegoedkeurings-nummer van het betreffende test apparaat of een (korte) omschrijving van het specifieke soort test autonoom apparaat					

Daarnaast ontbreekt bij de persoonsgebonden testcertificaten het id-etsiqcs-QcCompliance statement.

Zie verder Bijlage A voor de certificaatprofielen van de TRIAL PKIoverheid TEST Root CA - G2, TRIAL PKIoverheid Organisatie TEST CA - G2, TRIAL PKIoverheid Burger TEST CA - G2 en TRIAL PKIoverheid Autonome Apparaten TEST CA - G2.

**3.2 Initiële identiteitsvalidatie**

De vertegenwoordiger van de abonnee dient een kopie geldig identiteitsbewijs te verstrekken aan de CSP, indien de CSP hierover nog niet de beschikking heeft. Bij test servercertificaten moet de abonnee een test domeinnaam of IP adres opgeven waarover hij/zij de volledige controle heeft.

**3.3 Identificatie en authenticatie bij vernieuwing van het certificaat**

Niet van toepassing.

**3.4 Identificatie en authenticatie bij verzoeken tot intrekking**

Alle verzoeken tot intrekking worden in behandeling genomen.

## 4 Operationele eisen certificaatcyclus

### 4.1 **Aanvraag van certificaten**

Bij de aanvraag dient de abonnee te verklaren dat het testcertificaat alleen wordt gebruikt ten behoeve van testdoeleinden.

### 4.2 **Werkwijze met betrekking tot aanvraag van certificaten**

Aanvragen kunnen alleen worden gedaan bij CSP's die, onder de PKIoverheid testhiërarchie, testcertificaten aan eindgebruikers (waaronder ook services en/of autonome apparaten) uitgeven.

### 4.3 **Uitgifte van certificaten**

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

### 4.4 **Acceptatie van certificaten**

Het draaiboek behorende bij de creatieceremonies bevat tevens de procedure voor het vaststellen van de juistheid en het accepteren van de gecreëerde testcertificaten. De PA stelt de juistheid van de test stamcertificaat, de test domeincertificaten en test CSP-certificaten vast. De CSP accepteert vervolgens de test CSP-certificaten.

### 4.5 **Sleutelbaar en certificaatgebruik**

Het gebruik van de certificaten, uitgegeven onder de testhiërarchie van de PKI voor de overheid, is uitsluitend beperkt tot testsituaties. Vertrouwende partijen dienen zich hiervan bewust te zijn.

### 4.6 **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.

### 4.7 **Intrekking en opschorting van certificaten**

Intrekking van het test stamcertificaat, een test domeincertificaat of een test CSP-certificaat zal in ieder geval worden overwogen als de signing key behorende bij het certificaat is gecompromitteerd of daarvan wordt verdacht.

Indien een CSP niet langer voldoet aan de voorwaarden voor deelname aan de PKI voor de overheid, dan kan de PA overgaan tot het intrekken van het betreffende test CSP-certificaat. De intrekking van een testcertificaat kan binnen één dag worden geëffectueerd. De PA informeert de CSP vooraf over het intrekken van het testcertificaat.

In geval van het intrekken van het test stamcertificaat en/of een test domeincertificaat informeert de PA de onderliggende CSP's.

#### **4.8 Certificaat statusservice**

Er is een CRL met ingetrokken test domeincertificaten. Deze CRL wordt jaarlijks opnieuw gepubliceerd. Ad hoc publicatie van deze CRL vindt plaats na intrekking van een test domeincertificaat. Per domein is er een CRL met ingetrokken test CSP-certificaten binnen dat domein. De CRL met ingetrokken test CSP-certificaten wordt standaard elke drie maanden opnieuw gepubliceerd. Ad hoc publicatie van de CRL met ingetrokken test CSP-certificaten vindt plaats na intrekking van een test CSP-certificaat.

CSP's die testcertificaten aanbieden onder de test hiërarchie van de PKI voor de overheid stellen ook een CRL beschikbaar. Aan de beschikbaarheid van deze CRL en de frequentie van publicatie zijn verder geen eisen gesteld.

#### **4.9 Beëindiging abonnee relatie**

Niet van toepassing.

#### **4.10 Key escrow en recovery**

Niet van toepassing.

## 5 Fysieke, procedurele en personele beveiliging

### 5.1 Fysieke beveiliging

De fysieke beveiliging voor het centrale deel van de test hiërarchie van de PKI voor de overheid komt overeen met de fysieke beveiliging van het centrale deel van de productie hiërarchie van de PKI voor de overheid.

### 5.2 Procedurele beveiliging

De procedurele beveiliging voor het centrale deel van de test hiërarchie van de PKI voor de overheid komt overeen met de procedurele beveiliging van het centrale deel van de productie hiërarchie van de PKI voor de overheid.

### 5.3 Personele beveiliging

De personele beveiliging voor het centrale deel van de test hiërarchie van de PKI voor de overheid komt overeen met de personele beveiliging van het centrale deel van de productie hiërarchie van de PKI voor de overheid.

### 5.4 Procedures ten behoeve van beveiligingsaudits

Niet van toepassing.

### 5.5 Archivering en back-up

Van alle signing keys is een back-up gemaakt. Deze back-ups zijn opgeslagen in een andere ruimte dan waar de operationele signing keys zijn opgeslagen. Op de back-ups zijn dezelfde beveiligingsmaatregelen van toepassing als op de operationele signing keys.

De signing keys van de PA worden nimmer ter bewaring in handen gegeven van een derde partij.

### 5.6 Vernieuwen sleutels

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.

### 5.7 Aantasting en continuïteit

De PA treft voorzieningen om de continuïteit van de eigen dienstverlening zodanig te waarborgen, dat mogelijke verstoringen minimaal blijven.

Hiertoe behoort het in stand houden van kritieke diensten, waaronder het aanbieden van de revocation management service, de revocation status service en het via de gebruikelijke kanalen beschikbaar stellen van certificate status information.

### 5.8 Beëindiging PKIoverheid

Indien Logius besluit het product PKIoverheid te beëindigen, dan zullen de volgende stappen worden gevolgd:

1. Alle betrokken partijen van het product PKIoverheid, zullen een half jaar voor het beëindigen van het product worden geïnformeerd;
2. Alle testcertificaten die zijn uitgegeven na bekendmaking van het beëindigen van het product, zullen in het certificaat

een einddatum bevatten gelijk aan de geplande einddatum van PKIoverheid;

3. Bij het beëindigen van het product zullen alle nog geldige testcertificaten worden ingetrokken;
4. PKIoverheid stopt op de einddatum met het distribueren van testcertificaten en de daarbij behorende CRL's.

## 6 Technische beveiliging

### 6.1 Genereren en installeren van sleutelparen

De procedures voor het genereren en installeren van sleutelparen in de test hiërarchie zijn in beginsel gelijk aan die voor het genereren en installeren van sleutelparen in de productie hiërarchie. 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

De bescherming van de actieve signing keys van de testcertificaten van de PA komt overeen met de bescherming van de actieve signing keys van de productiecertificaten.

### 6.3 Andere aspecten van sleutelbaar management

Alle testcertificaten hebben een maximale periode van geldigheid:

Eindgebruiker testcertificaten	6 maanden
Interne Eindgebruiker testcertificaten <sup>3</sup>	Geen bepalingen
CSP testcertificaten	12 jaar minus 2 dagen
Domein testcertificaten	12 jaar minus 1 dag
Test stamcertificaat	12 jaar

### 6.4 Activeringsgegevens

Niet van toepassing.

### 6.5 Logische toegangsbeveiliging

De logische toegangsbeveiliging voor het centrale deel van de test hiërarchie van de PKI voor de overheid komt overeen met de logische toegangsbeveiliging van het centrale deel van de productie hiërarchie van de PKI voor de overheid.

### 6.6 Netwerkbeveiliging

Niet van toepassing.

### 6.7 Time stamping

Niet van toepassing.

---

<sup>3</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**

De PA hanteert voor het formaat van het test stamcertificaat, de test domeincertificaten en de CSP-testcertificaten de standaard ITU-T Rec. X.509 (1997).

In bijlage A is in een overzicht de inhoud weergegeven van de velden van het test stamcertificaat en van de test domeincertificaten

### 7.2 **CRL profiel**

De PA hanteert voor de CRL ten behoeve van het test stamcertificaat en de test domeincertificaten en de CSP-testcertificaten het X.509 versie 2 formaat voor CRL's.

In bijlage B is in een overzicht de inhoud weergegeven van de velden van de CRL's.

## 8 Conformiteitbeoordeling

Voor de test hiërarchie vindt geen conformiteitbeoordeling plaats.

## 9 Algemene en juridische bepalingen

### 9.1 **Tarieven**

Het test stamcertificaat, de test domeincertificaten en de test CSP-certificaten bevatten een verwijzing naar dit CPS. Er worden geen kosten in rekening gebracht voor het raadplegen van deze certificaten of de informatie waarnaar wordt verwezen. Dit geldt voor:

- het raadplegen van de certificaten;
- het raadplegen van de revocation status information (CRL's) en;
- het raadplegen van de CP;
- het raadplegen van dit CPS.

### 9.2 **Financiële verantwoordelijkheid en aansprakelijkheid**

Logius aanvaardt geen enkele aansprakelijkheid voor schade die voortvloeit uit het gebruik van testcertificaten uitgegeven onder de test hiërarchie van de PKI voor de overheid.

### 9.3 **Vertrouwelijkheid bedrijfsgegevens**

Geen nadere bepalingen.

### 9.4 **Vertrouwelijkheid persoonsgegevens**

Geen nadere bepalingen.

### 9.5 **Intellectuele eigendomsrechten**

Voorliggend CPS is eigendom van Logius.

### 9.6 **Aansprakelijkheid en garanties**

Geen nadere bepalingen in aanvulling op het gestelde in paragraaf 9.2.

### 9.7 **Uitsluiting van garantie**

Geen nadere bepalingen in aanvulling op het gestelde in paragraaf 9.2.

### 9.8 **Beperking aansprakelijkheid**

Geen nadere bepalingen in aanvulling op het gestelde in paragraaf 9.2.

### 9.9 **Schadeloosstelling**

Geen nadere bepalingen in aanvulling op het gestelde in paragraaf 9.2.

### 9.10 **Geldigheid CPS**

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

Het CPS is geldig vanaf de datum van uitgifte. Het CSP is geldig zolang de dienstverlening van de PKI voor de overheid voortduurt of totdat het CPS 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 overige minder ingrijpende aanpassingen wordt het versienummer opgehoogd met 0.1. Nieuwere versies worden gepubliceerd op de website van PKIoverheid.

**9.11 Communicatie binnen betrokken partijen**

Geen nadere bepalingen.

**9.12 Wijzigingen**

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

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

**9.13 Conflictoplossing**

Geen nadere bepalingen.

**9.14 Toepasselijk recht**

Het Nederlands recht is van toepassing.

**9.15 Naleving relevante wetgeving**

De PA-functie wordt uitgevoerd door Logius. Logius onderdeel van het Directoraat-Generaal Bestuur en Koninkrijksrelaties, is een directie binnen het Ministerie van BZK. Op Logius is de Awb van toepassing.

**9.16 Overige bepalingen**

Geen nadere bepalingen.



## Bijlage A. Inhoud velden test stamcertificaten en test domeincertificaten

Attribuut	Test Stamcertificaat	Test Domein Organisatie	Test Domein Burger	Test Domein Autonome Apparaten
Versie	V3			
Serienummer	01 31 05 f1	01 31 05 ff	01 31 05 fe	01 31 07 84
Algoritme voor handtekening	sha256WithRSAEncryption (1.2.840.113549.1.1.11)			
Verlener	CN = TRIAL PKIoverheid TEST Root CA - G2 O = PKIoverheid TEST C = NL			
Geldig van / tot	woensdag 29 oktober 2008 13:38:44 woensdag 25 maart 2020 14:27:19	woensdag 29 oktober 2008 17:01:22 dinsdag 24 maart 2020 17:00:39	woensdag 29 oktober 2008 16:33:57 dinsdag 24 maart 2020 16:33:01	donderdag 15 oktober 2009 14:41:04 dinsdag 24 maart 2020 15:38:59
Onderwerp	CN = TRIAL PKIoverheid TEST Root CA - G2 O = PKIoverheid TEST C = NL	TRIAL PKIoverheid Organisatie TEST CA - G2 PKIoverheid TEST NL	TRIAL PKIoverheid Burger TEST CA - G2 PKIoverheid TEST NL	TRIAL PKIoverheid Autonome Apparaten TEST CA - G2 PKIoverheid TEST NL
Openbare sleutel	RSA (4096 Bits) Betreft cijferreeks.	RSA (4096 Bits) Betreft cijferreeks.	RSA (4096 Bits) Betreft cijferreeks.	RSA (4096 Bits) Betreft cijferreeks.

Attribuut	Test Stamcertificaat	Test Domein Organisatie	Test Domein Burger	Test Domein Autonome Apparaten
	Bevat o.a. de publieke sleutel.	Bevat o.a. de publieke sleutel.	Bevat o.a. de publieke sleutel.	Bevat o.a. de publieke sleutel.
Certificate Policies	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS <a href="http://www.pkioverheid.nl/policies/TESTroot-policy-G2">http://www.pkioverheid.nl/policies/TESTroot-policy-G2</a>	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS <a href="http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2">http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2</a>	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS <a href="http://www.pkioverheid.nl/policies/TESTdom-bu-policy-G2">http://www.pkioverheid.nl/policies/TESTdom-bu-policy-G2</a>	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS <a href="http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2">http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2</a>
Sleutel ID van CA	N.V.T.	Sleutel-ID= 11 56 07 49 a3 36 0b cf 99 8d f7 c7 04 94 f3 9b 06 a9 ee 79 Certificaatverlener: CN= TRIAL PKIoverheid TEST Root CA - G2 O= PKIoverheid TEST C=NL Serienummer van certificaat=01 31 05 f1		
CRL distributie	N.V.T.	URL= <a href="http://crl.pkioverheid.nl/pkiotest/TESTRootLatestCRL-G2.crl">http://crl.pkioverheid.nl/pkiotest/TESTRootLatestCRL-G2.crl</a>		
Sleutel ID van onderwerp	11 56 07 49 a3 36 0b cf 99 8d f7 c7 04 94 f3 9b 06 a9 ee 79	60 5b 87 e8 90 85 8d ad ca 36 a3 d7 00 ca 81 d0 e1 36 97 1b	34 24 e1 4c f9 0a fb f7 b4 39 e8 ba f2 5b b7 ac 87 3b 1f 7c	e4 87 99 cd 7d 79 75 60 87 47 cb 2b 4b e1 dc 80 f7 24 36 63
Essentiële beperkingen	Subjecttype=CA Beperking voor padlengte=Geen			
Sleutelgebruik	Certificaatondertekening , Off line CRL-ondertekening , CRL-ondertekening(06)			

Attribuut	Test Stamcertificaat	Test Domein Organisatie	Test Domein Burger	Test Domein Autonome Apparaten
Vingerafdruk algoritme	sha1			
Vingerafdruk	fb c4 7c 0b bc 87 73 14 43 d2 db 46 9d b6 98 f6 af 2a 9d de	d4 37 19 b5 1b 57 ca 4b b8 74 16 7d 47 95 23 1d 34 34 fd a8	ce cc 35 8e 51 55 40 ac e6 9a e6 1e 69 c3 45 9b cd 65 78 68	0a 90 ac 45 18 1c f8 67 26 4b e5 8b c2 d1 c9 9e 64 00 e2 6d

## Bijlage B. Inhoud velden CRL voor test domeincertificaten en test CSP-certificaten

Attribuut	CRL Test domeincertificaten	CRL CSP-Testcertificaten Organisatie	CRL CSP-Testcertificaten Burger	CRL CSP-Testcertificaten Autonome Apparaten
Versie	V2			
Verlener	CN = TRIAL PKIoverheid TEST Root CA - G2 O = PKIoverheid TEST C = NL	TRIAL PKIoverheid Organisatie TEST CA - G2 PKIoverheid TEST NL	TRIAL PKIoverheid Burger TEST CA - G2 PKIoverheid TEST NL	TRIAL PKIoverheid Autonome Apparaten TEST CA - G2 PKIoverheid TEST NL
Ingangsdatum	donderdag 30 oktober 2008 13:08:00	donderdag 30 oktober 2008 13:13:37	donderdag 30 oktober 2008 13:10:43	donderdag 15 oktober 2009 15:46:20
Datum volgende publicatie	vrijdag 30 oktober 2009 13:13:00	woensdag 28 januari 2009 13:18:37	woensdag 28 januari 2009 13:15:43	woensdag 13 januari 2010 15:51:20
Algoritme voor handtekening	sha256WithRSAEncryption (1.2.840.113549.1.1.11)			
Volgnummer CRL	2	2	2	2