Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CERTIFICATION PRACTICE STATEMENT

*TEST*certificaten binnen de PKI voor de overheid

Datum Oktober 2016

Colofon

Versienummer	3.0
Contactpersoon	Policy Authority PKIoverheid
Organisatie	Logius
	Bezoekadres Wilhelmina van Pruisenweg 52
	Postadres Postbus 96810 2509 JE DEN HAAG
	T 0900 - 555 4555 servicecentrum@logius.nl

Inhoud

Revisiegegevens

Versie	Datum	Status	Auteur	Manager	Omschrijving
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
2.0	10-02-2012	Definitief	Policy Authority	H. Verweij	Testdoeleinden opgenomen. Introductie services server type 1 en 2 testcertificaten en de daarbij behorende aanpassingen. Aanpassing commonname veld bij persoonsgebonden testcertificaten. Daarnaast enkele kleine toevoegingen en redactionele aanpassingen.
3.0	oktober 2016	Definitief	Policy Authority	Mark Janssen	CPS omgeschreven conform RFC3647. Tevens enkele correctieve wijzigingen doorgevoerd.

1 Inleiding

1.1 Overzicht

1.1.1 *Policy Authority voor de PKI voor de overheid*

De Policy Authority van de PKI voor de overheid (PA PKIoverheid) ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties (MinBZK) 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 taken van de PA PKIoverheid zijn:
1. het leveren van bijdragen voor de ontwikkeling en het beheer van het normenkader dat aan de PKI voor de overheid ten grondslag ligt, het zogeheten Programma van Eisen (PvE);
2. het proces van toetreding door Certification Service Providers (CSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
3. het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de root van de PKI voor de overheid certificaten uitgeven.

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 overheid1.

1 *Zie in dit verband de nota "De Elektronische Overheid aan het begin van de 21e eeuw" (Tweede Kamer, vergaderjaar 2000 – 2001, 26 387, nr. 9) van de Minister voor Grote Steden – en Integratiebeleid aan de Voorzitter van de Tweede Kamer der Staten – Generaal.*

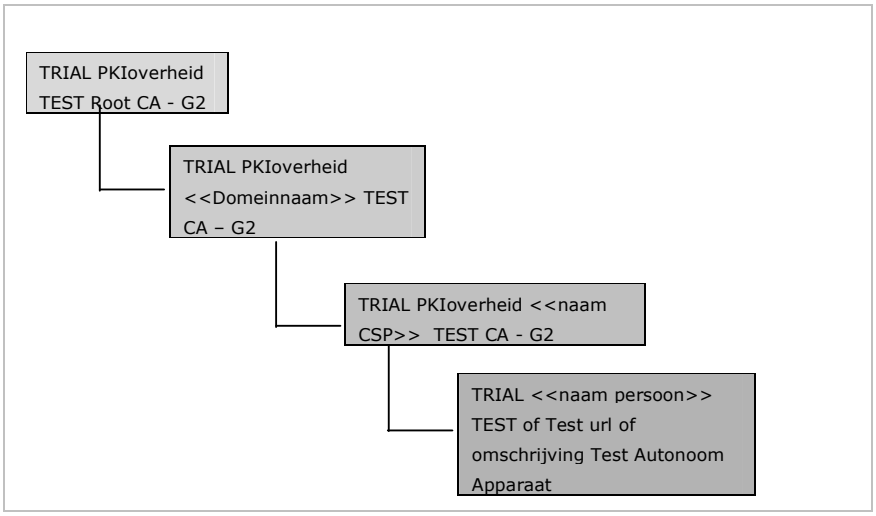
In algemene zin is de PA in het kader van PKIoverheid verantwoordelijk voor:
1. beheer van het normenstelsel van de PKI voor de overheid, het Programma van Eisen deel 3a t/m d;
2. beheer van Object Identifiers, de unieke nummers voor CSP's en hun CPS's;
3. creatie en beheer van sleutelpaar en het bijbehorende stamcertificaat;
4. intrekken van het stamcertificaat en ad hoc publicatie van de CRL;
5. periodieke publicatie van de CRL;
6. creatie en beheer van sleutelparen en de bijbehorende domeincertificaten;
7. intrekken van van domeincertificaten en ad hoc publicatie van de bijbehorende CRL;
8. voorbereiding inzake het toelaten van CSP's tot de PKIoverheid;
9. effectuering van de toelating van CSP's met inbegrip van creatie, uitgifte en beheer van CSP CA-certificaten;

10. voorbereiding inzake het intrekken van CSP CA-certificaten;
11. effectuering van het intrekken van CSP CA-certificaten;
12. houden van toezicht op toegelaten CSP's;
13. voorbereiding inzake het vernieuwen van CSP CA-certificaten;
14. effectuering van het vernieuwen van CSP CA-certificaten met inbegrip van creatie, uitgifte en beheer van nieuwe CSP CA-certifcaten;
15. registreren en beoordelen van meldingen omtrent aantasting van de PKIoverheid.

Het technisch beheer van het Staat der Nederlanden Root CA en de Staat der Nederlanden <Domein> CA en de bijbehorende Certificate Revocation Lists (CRL's) vindt plaats door KPN Corporate Market B.V.
Het beheer van stamcertificaten en domeincertificaten is opgedragen aan de Policy Authority van de PKI voor de overheid. Deze organisatie is ondergebracht bij Logius (http://www.logius.nl), dienst digitale overheid van
Naast de productie hiërarchie, zoals beschreven in het CPS Policy Authority PKIoverheid voor certificaten uit te geven door de PA van de PKI voor de overheid versie 4.0 paragraaf 1.1.2 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 een nieuwe algoritme en/of de nieuwe sleutellengte;
B. De 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.

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. Het CPS geeft géén inzicht in de werking van de operationele c.q. productie hiërarchie van de PKI voor de overheid. De algemene indeling van dit CPS volgt zoveel mogelijk het model zoals gepresenteerd in Request for Comments 3647[1].

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

CPS	Omschrijving
Naamgeving	Certification Practice Statement *TEST*certificaten binnen de PKI voor de overheid
Link	https://cps.pkioverheid.nl
OID	n.v.t.

Openbare informatie over de PA of de PKI voor de overheid is te vinden op http://www.logius.nl/pkioverheid.

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

1.2.1 Certificate Policies (CP's) (geen RFC 3647)

Dit deel heeft betrekking op de eisen die aan de dienstverlening van een Certification Service Provider (CSP) worden gesteld. Er zijn negen gebieden gedefinieerd die elk in een afzonderlijk deel worden behandeld, te weten:
Deel 3a – Certificate Policy voor Domein, Organisatie en Organisatie Persoon;
Deel 3b – Certificate Policy voor Domein Organisatie en Organisatie Services;
Deel 3c – Certificate Policy voor Domein Burger;
Deel 3d – Certificate Policy voor Domein Autonome Apparaten;
Deel 3e – Certificate Policy voor Server Certificaten.
Deel 3f – Certificate Policy voor Extended Validation
Deel 3g – Certificate Policy voor Private Services
Deel 3h – Certificate Policy voor Private server certificaten
Deel 3i – Certificate Policy voor Private personen

Dit CPS heeft alleen betrekking op CP deel 3a t/m e.

1.2.1.1 *Doel CPS(geen RFC 3647)*

Dit 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. De kwaliteit van de dienstverlening ligt ten grondslag aan het vertrouwen dat in de PKI voor de overheid gesteld kan worden. Hierbij is ook de relatie tussen de PA en Certification Service Providers (CSP's) van belang. Deze relatie en de voorwaarden waaronder CSP's kunnen deelnemen aan de PKI voor de overheid zijn op hoofdlijnen beschreven. CSP's die zijn geïnteresseerd in deelname aan de PKI voor de overheid kunnen over dit onderwerp meer gedetailleerde informatie PKIoverheid Programma van Eisen deel 2.

1.2.1.2 *Verhouding CPS en CP (geen RFC3647)*

Het CP PvE deel 3a t/m f beschrijft de minimumeisen die zijn gesteld aan de dienstverlening van een CSP binnen PKIoverheid. Dit voorliggende CPS geeft aan op welke wijze invulling wordt gegeven aan de PKIoverheid dienstverlening, voor zover dit valt onder directe verantwoordelijkheid van de PA. Genoemde eisen in het PvE zijn ook van toepassing op de TRIAL certificaten.

1.2.1.3 *Positionering Programma van Eisen (geen RFC 3647)*

Het Programma van Eisen is het uitgangspunt voor de dienstverlening van de PA. In het *Programma van Eisen* zijn de eisen geformuleerd voor de PKI voor de overheid, deze eisen zijn ontleend aan internationale standaarden en de van toepassing zijnde wetgeving. Het Programma van Eisen omvat vier delen en in ieder deel is een bepaald aspect van de PKI voor de overheid nader uitgewerkt.

1.2.1.4 *Introductie Programma van Eisen(geen RFC 3647)*

Dit deel bevat een introductie op het Programma van Eisen en de PKI voor de overheid.

1.2.1.5 *Toetreding tot en toezicht(geen RFC 3647)*
In deel 2 van het Programma van Eisen (PvE) PKIoverheid wordt beschreven op welke wijze een CSP kan toetreden tot de PKI voor de overheid, conformiteit aan de eisen kan aantonen en aan welke formaliteiten moet worden voldaan. Tevens is beschreven op welke wijze de PA toezicht houdt op de toegetreden CSP's.

1.3 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.

Onderstaand zijn voor elk van deze partijen de verantwoordelijkheden en de daarbij behorende activiteiten kort beschreven.

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* adviseert de directeur van Logius en is verantwoordelijk voor het beheer van het centrale deel3 van de PKI voor de overheid infrastructuur en het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de Staat der Nederlanden Root CA van de PKI voor de overheid, certificaten uitgeven.
Per domein van de PKI voor de overheid opereren één of meer *CSP's*. Een CSP geeft binnen een domein van de PKI voor de overheid certificaten uit aan certificaathouders. De verplichtingen van de CSP's die deel uitmaken van de PKI voor de overheid zijn gespecificeerd in het Programma van Eisen, deel 3a t/m d: Certificate Policies.

Een *abonnee* gaat een overeenkomst aan met een CSP namens één of meer certificaathouders. Hóe de levering van certificaten 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 certificaat vermeld is. Op alle niveaus in de hiërarchie van de PKI voor de overheid bevinden zich certificaathouders. Eindgebruikers ontvangen de certificaten van de CSP's. De PA geeft certificaten uit aan zichzelf (Staat der Nederlanden Root CA en Staat der Nederlanden <Domein> CA’s) en aan CSP's (CSP CA).

De *vertrouwende partij* is de ontvanger van een certificaat dat is uitgegeven binnen de PKI voor de overheid en handelt in vertrouwen op dat certificaat. De vertrouwende partij is verplicht om de geldigheid te controleren van de volledige keten van certificaten tot aan de bron (stamcertificaat) waarop wordt vertrouwd. Deze verplichting is opgenomen in het Programma van Eisen, deel 3: Certificate Policies.
Certificaatgebruik

De TRIAL PKIoverheid TEST Root CA - G2 en alle testcertificaten die daaronder worden gecreëerd en uitgegeven mogen uitsluitend worden gebruikt voor testdoeleinden.

Dit betekent dat de TRIAL PKIoverheid TEST Root CA - G2 en alle testcertificaten die daaronder zijn en worden gecreëerd en uitgegeven NIET gebruikt 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 mogen worden voor het authenticeren van de identiteit van een abonnee en/of een eindgebruiker en/of service en/of autonoom apparaat. Tevens 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.

De testdoeleinden van Server/SSL testcertificaten en Autonome Apparaten testcertificaten, zijn in ieder geval, maar niet limitatief:
- 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.

De testdoeleinden van overige Service certificaten en Persoonsgebonden certificaten, zijn in ieder geval 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.

1.4 Policy Beheer

1.4.1 Organisatie verantwoordelijk voor het beheer van het 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.

1.4.2 Contactinformatie

Voor klachten, vragen of meldingen kunnen CSP's binnen het PKIoverheid stelsel contact opnemen met medewerkers van de PA PKIoverheid via de gebruikelijke kanalen. De PA PKIoverheid is binnen kantooruren beschikbaar en zal zo spoedig mogelijk reageren. In het geval van meldingen van incidenten of calamiteiten buiten kantoren wordt verzocht contact op te nemen met het Servicecentrum van Logius dat 24 uur per dag beschikbaar is.

Abonnees die vragen hebben omtrent certificaatuitgifte worden verzocht in eerste instantie contact op te nemen met hun (potentiële) CSP.

Overige betrokken partijen kunnen contact opnemen met het servicecentrum van Logius. Het servicecentrum registreert de vraag en beantwoordt deze binnen de gestelde termijn. Indien noodzakelijk worden

vragen via het servicecentrum doorgezet naar de PA PKIoverheid of in het geval van een incident, de dienstdoende incidentmanager.

Contactgegevens:
Policy Authority PKIoverheid
Wilhelmina van Pruisenweg 52
Postbus 96810
2509 JE DEN HAAG
http://www.logius.nl/pkioverheid
Algemeen telefoonnummer: 0900-555 4555
E-mailadres: servicecentrum@logius.nl

1.4.3 *Persoon die geschiktheid beoordeelt van CPS voor het CP*
De PA PKIoverheid kent geen eigen Certificate Policy. Goedkeuring van het CPS wordt behandeld in 1.5.4.

1.4.4 *Wijzigingsprocedure CPS*
De PA van PKIoverheid heeft het recht dit CPS te wijzigen of aan te vullen. Wijzigingen gelden vanaf het moment dat het nieuwe CPS gepubliceerd is, conform het gestelde in paragraaf 9.109.10. Het management van het Logius is verantwoordelijk voor een juiste navolging van de procedure zoals beschreven in paragraaf 9.12 en voor de uiteindelijke goedkeuring van dit CPS conform deze procedure.

1.4.5 *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 52
Postbus 96810
2509 JE DEN HAAG
http://www.logius.nl/pkioverheid
Algemeen telefoonnummer: 0900-555 4555
email: servicecentrum@logius.nl

1.5 Definities en afkortingen

In deel 4 zijn de in het Programma van Eisen gehanteerde definities en afkortingen toegelicht.
Voor een overzicht van de gebruikte definities en afkortingen wordt verwezen naar http://www.logius.nl/begrippenlijst.

1.6 Waarborgen (geen RFC 3647)

Bij de uitgifte van een PKIoverheid certificaten zijn onder meer de volgende partijen te onderkennen:
A. Abonnee;
B. Eindgebruiker;
C. Organisaties die internet browser software ontwikkelen;
D. Vertrouwende partijen.

Aan deze partijen wordt kenbaar gemaakt dat:

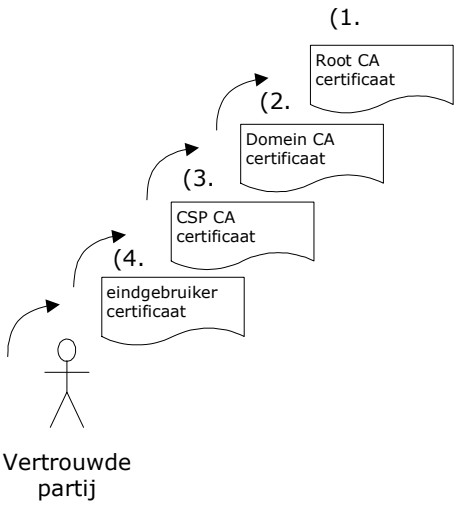
De PA van PKIoverheid waarborgt dat sub CA's binnen het PKIoverheid stelsel bekend zijn bij de PA en onder controle blijven van de CSP die een sub CA heeft gecreëerd. Tevens zullen deze sub CA's niet worden gebruikt voor man-in-the middle (*MITM)*doeleinden.

Alle sub CA certificaten die zijn uitgeven binnen de PKI voor de overheid staan vermeld op deze website:
https://cert.pkioverheid.nl

1.7 Controle betrouwbaarheid (geen RFC 3647)

In figuur 2 wordt de structuur gepresenteerd vanuit het gezichtspunt van de vertrouwende partijen. Een vertrouwende partij heeft een certificaat (4) van een ander (de certificaathouder) en wil zekerheid omtrent de betrouwbaarheid van dit certificaat. Een certificaat wordt geverifieerd door de volgende controles uit te voeren[2]:

- Is het bericht tijdens verzending niet gewijzigd, ofwel is de integriteit gewaarborgd?
- Is het gebruikte certificaat ingetrokken en op zogenaamde "zwarte lijst" geplaatst?
- Is het certificaat nog geldig?



Figuur 2 - Vertrouwensketen

Vervolgens wordt door de software vastgesteld of het certificaat door een vertrouwde instantie is uitgegeven. Om deze laatste controle te kunnen uitvoeren, moet de software beschikken over het stamcertificaat van de PKI voor de overheid. Wanneer het stamcertificaat niet aanwezig is, krijgt de gebruiker een foutmelding. Daarom heeft de PA ervoor gekozen om het stamcertificaat op te nemen in veelgebruikte besturingssystemen en (OpenSource) browsers.

[2] *Deze controles worden normaliter automatisch door de gebruikte applicatie uitgevoerd. De genoemde controles dienen voor ieder certificaat uit de vertrouwensketen te worden uitgevoerd.*

Wanneer software wordt gebruikt waarin het stamcertificaat niet is opgenomen, kan de vertrouwende partij het stamcertificaat op een betrouwbare wijze downloaden op https://cert.pkioverheid.nl

Het CSP-certificaat (3) is uitgegeven door de PA en kan worden gecontroleerd aan de hand van het domeincertificaat (2). Dit laatste certificaat is ook uitgegeven door de PA en kan worden gecontroleerd aan de hand van het stamcertificaat (1). Het vertrouwen in een certificaat hangt daarom op elk niveau van de PKI voor de overheid af van het vertrouwen dat men stelt in de partij die het certificaat heeft uitgegeven. Vanuit het gezichtspunt van een vertrouwende partij is dat bij de eerste controlestap de CSP, bij de tweede stap de PA op het niveau van de domeinen en tenslotte de PA op het hoogste niveau van de hiërarchie. Het stamcertificaat is dus het ankerpunt van vertrouwen in de hiërarchie van de PKI voor de overheid en bepaalt het vertrouwen dat in alle andere certificaten die zijn uitgegeven binnen de PKI voor de overheid wordt gesteld. Door het vertrouwen uit te spreken in het stamcertificaat, worden alle onderliggende domein-, CSP- en eindgebruikercertificaten vertrouwd. De gebruikers hoeven dus slechts één certificaat te vertrouwen. Een belangrijk aspect hierbij is het bepalen van de betrouwbaarheid van de uitgevende instantie van het certificaat.

1.7.1 Betrouwbaarheid uitgevende instantie (geen RFC 3647)

Om te kunnen vertrouwen op een certificaat moet de vertrouwende partij bepalen of hij wil vertrouwen op de uitgevende instantie (de CSP). Dit kan de vertrouwende partij doen door de Certification Practice Statement (CPS) van de CSP te beoordelen. Een verwijzing naar het CPS is opgenomen in het certificaat. Om te voorkomen dat een vertrouwende partij iedere CPS van de CSP's binnen de PKI voor de overheid in detail moeten gaan beoordelen, is de hiërarchie van de PKI voor de overheid gecreëerd. De voorwaarden voor uitgifte, beheer en ook het gebruik van eindgebruikercertificaten zijn door de PA beschreven in de zogenaamde CP. De CP is hiermee bepalend voor de CPS van de verschillende CSP's die actief zijn binnen de PKI voor de overheid.

Om van een betrouwbare hiërarchie te kunnen spreken is het dus van groot belang dat de PA op een betrouwbare wijze functioneert. De PA waarborgt de betrouwbaarheid van het stamcertificaat en de domeincertificaten door adequate beveiligingsmaatregelen toe te passen. Deze beveiligingsmaatregelen evenals de wijze waarop de PA toezicht houdt op de CSP zijn beschreven in dit CPS van de PA. Door het CPS van de PA te beoordelen kan de vertrouwende partij vaststellen of hij/zij vertrouwt op een certificaat dat is uitgegeven binnen de hiërarchie van de PKI voor de overheid. Daarnaast wordt het betrouwbaar functioneren van de PA periodiek vastgesteld door het laten uitvoeren van een audit door externe auditors.

1.8 Programma van Eisen en stelseloverleg PKIoverheid (geen RFC 3647)

Het Programma van Eisen geldt als het formele normenkader ten aanzien van de betrouwbaarheid en kwaliteit van dienstverlening binnen de PKI voor de overheid. Bij het door de PA onderhouden van dit normenstelsel is het van belang dat ook de praktijkervaringen en ideeën vanuit gebruikers worden meegewogen. Om dit draagvlak voor de toepassing van het

Programma van Eisen te kunnen realiseren is een PKIoverheid stelseloverleg ingesteld die wordt geconsulteerd bij de besluitvorming over wijzigingsvoorstellen op het Programma van Eisen. Daarnaast komen in dit overleg ook onderwerpen aan de orde die in het algemeen relevant zijn voor de PKI –ontwikkelingen.
De volledige procedures voor het wijzigingenbeheer van het Programma van Eisen van PKIoverheid zijn opgenomen in Annex B.

2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

De PA publiceert het stamcertificaat, de domeincertificaten en de CSP-certificaten op haar website. Op de website is tevens informatie beschikbaar met betrekking tot het gebruik van het stamcertificaat, de domeincertificaten en de CSP-certificaten.
Een toegelaten CSP publiceert de CSP-certificaten uitgegeven door de PA op de eigen website. Daarbij is tevens een verwijzing opgenomen naar het stamcertificaat en de domeincertificaten op de website van de PA.

Op de websites van de verschillende CSP's zijn de CRL's ten behoeve van de eindgebruiker certificaten te vinden.

2.2 Publicatie certificaat informatie

De volgende testcertificaten worden gepubliceerd:

- TRIAL PKIoverheid TEST Root CA - G2;
- TRIAL PKIoverheid Organisatie TEST CA - G2;
- TRIAL PKIoverheid Burger TEST CA - G2;
- TRIAL PKIoverheid Autonome Apparaten TEST CA - G2;
- TRIAL PKIoverheid <<naam CSP>> TEST CA - G2.

De volgende CRL's worden gepubliceerd:

- TRIAL G2 domein-certificaten;
- CSP-certificaten onder TRIAL G2 domein Organisatie;
- CSP-certificaten onder TRIAL G2 domein Burger;
- CSP-certificaten onder TRIAL G2 domein Autonome Apparaten.

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

- Ingetrokken Test domeincertificaten: http://crl.pkioverheid.nl/pkiotest/TESTRootLatestCRL-G2.crl
- 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 domein-certificaat. 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 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.

Tevens wordt in het Subject.organizationalUnitName (OU) veld de tekst: "only to be used for testing purposes" opgenomen.

Daarnaast ontbreekt bij de persoonsgebonden testcertificaten het id-etsi-qcs-QcCompliance statement (0.4.0.1862.1.1) en/of het qcp-public-with-sscd statement (0.4.0.1456.1.1).

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.

3.1.1 Noodzaak gebruik betekenisvolle namen

Er zijn geen nadere bepalingen op dit gebied voor de certificaatdienstverlening door de PA.

3.1.2 Pseudoniemen

Het gebruik van pseudoniemen of anonieme certificaten wordt niet toegestaan.

3.1.3 Regels voor het interpreteren van verschillende naamvormen

De naam van de CSP CA wordt overgenomen van het uittreksel uit het Nederlands Handelsregister.

3.1.4 Uniciteit van namen

Alle certificaten die onder dit CPS worden uitgegeven, bezitten een uniek subjectveld (*DistinguishedName*).

3.1.5 Erkenning, authenticatie en de rol van handelsmerken

De PA gaat uit van de correctheid van de naamgeving van organisaties zoals opgenomen in het Nederlands Handelsregister van de Kamer van Koophandel.

3.2 Initiële identiteitsvalidatie

3.2.1 Initieel Registratieproces

Zie voor de eisen die worden gesteld aan een initieel registratieproces het Programma van Eisen, deel 2 van PKIoverheid.

3.2.2 Authenticatie van organisatorische entiteit

Op basis van het aanvraagformulier en de aangeleverde bewijsmiddelen verifieert de PA,

- dat de CSP een bestaande organisatie is die is opgenomen in het NHR of een organisatorische entiteit behorend bij een bestaande organisatie die is opgenomen in het NHR. In het geval van een

overheidsorganisatie die niet is ingeschreven in het NHR zal de Staatsalmanak worden geraadpleegd;

- dat de door de CSP aangemelde organisatienaam en landnaam die in het certificaat wordt opgenomen juist en volledig is en dat de aanvrager bevoegd is de organisatie te vertegenwoordigen;
- de aanwezigheid van de relevante registratie-informatie van de aspirant CSP met het daarbij behorende bewijsmateriaal (uittreksel KvK etc.). Er moet sprake zijn van een origineel uittreksel dat niet ouder mag zijn dan 13 maanden.

Nota bene: Indien de toetredende partij minder dan drie jaar bestaat en niet voorkomt in de meest recente versie van genoemde registratiebronnen kan de identiteit en validiteit van de aspirant CSP eventueel worden vastgesteld aan de hand van een moedermaatschappij of kerndepartement, die wel geregistreerd zijn in de KVK of de Staatsalmanak.

3.2.3 Authenticatie van persoonlijke identiteit

Bij initiële toetreding tot het PKIoverheid stelsel verifieert de PA de opgegeven persoonsgegevens van de bevoegd vertegenwoordiger van de CSP aan de hand van een in art. 1 van de Wet op de Identificatieplicht genoemd identiteitsdocument:

- een geldig reisdocument als bedoeld in de Paspoortwet;
- een geldig rijbewijs dat is afgegeven op basis van de Wegenverkeerswet, als bedoeld in artikel 107 van de Wegenverkeerswet 1994..

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

Dikwijls zal een CSP al toegetreden zijn tot het PKIoverheid stelsel wanneer een nieuwe CSP CA aangemaakt dient te worden onder een nieuwe generatie van de reguliere root. Ook is het mogelijk dat een reeds toegetreden CSP certificaten wil uitgeven onder een nieuw domein of een andere root. In dat geval kan een verkorte procedure gehanteerd worden voor de identificatievalidatie omdat de CSP CA reeds bekend is bij de PA en is toegetreden tot het PKIoverheid stelsel.

Het is dan voldoende als de PA controleert of de organisatienaam en naam van het land opgegeven in het Naming document / CSR nog steeds correct is. Dit kan op de volgende manieren worden gecontroleerd:

1. Door het online raadplegen van het NHR om te controleren of de CSP CA een bestaande organisatie is;
2. Door het online raadplegen van een database zoals Dunn & Bradstreet die up-to-date wordt gehouden en wordt beschouwd als een betrouwbare bron.

Daarnaast dient de PA te controleren dat de aanvraag daadwerkelijk van de CSP CA afkomstig is. Een aanvraag kan op twee manieren worden ingediend:

1. De bevoegd vertegenwoordiger kan een aanvraagformulier versturen via e-mail en ondertekenen met een PKIoverheid certificaat;
2. De bevoegd vertegenwoordiger kan een aanvraagformulier ondertekenen en per post te versturen.

In het tweede geval dient tevens contact te worden opgenomen met de bij de PA PKIoverheid geregistreerde bevoegd vertegenwoordiger van de CSP CA om de aanvraag te verifieren. Ter controle kunnen identificerende gegevens van de contactpersoon of organisatie worden opgevraagd.

Deze identificatiecontrole door de PA wordt vastgelegd en gearchiveerd in het dossier van de CSP CA.

3.4 Identificatie en authenticatie bij verzoeken tot intrekking

Een verzoek tot intrekking van een certificaat kan worden ingediend door de CSP CA. Bij een verzoek tot intrekking zal altijd een opgave van redenen moeten worden gegeven. In overleg met betrokken partijen zal worden gekeken in hoeverre aan het verzoek voldaan zou kunnen worden aangezien intrekking van een CSP CA betekent dat onderliggende certificaat niet meer geldig zullen zijn.

Identificatie en authenticatie van de indiener van het verzoek tot intrekking van de CSP CA kan op één van onderstaande wijzen geschieden:

- Een verzoek per e-mail aan de PA, waarbij het verzoek digitaal wordt ondertekend met een gekwalificeerde elektronische handtekening;
- Een verzoek per ondertekende brief;

In alle drie de gevallen zal de PA telefonisch contact opnemen met de bevoegd vertegenwoordiger van de CSP CA om vast te stellen dat de aanvraag tot intrekking authenthiek is. Ter controle kunnen identificerende gegevens van de contactpersoon of organisatie worden opgevraagd.

4 Operationele eisen certificaatcyclus

4.1 Toepassingsgebied

Binnen de PKI voor de overheid zijn op vier niveaus verschillende typen certificaten gedefinieerd, te weten:

- Stamcertificaat;
- Domeincertificaat;
- CSP certificaat;
- Eindgebruikercertificaat.

Het stamcertificaat, de domeincertificaten en de CSP-certificaten kunnen uitsluitend worden gebruikt voor het verifiëren van de handtekening van de uitgever en worden uitgegeven door de Policy Authority. Het is niet toegestaan deze certificaten voor andere doeleinden te gebruiken. Het eindgebruikercertificaat wordt uitgegeven door de CSP's.

Dit CPS heeft betrekking op de betrouwbaarheid van de dienstverlening van de Policy Authority, derhalve worden in deze paragraaf enkel de procedures met betrekking tot stam-, domein- en CSP certificaten behandeld.

4.2 Aanvraag van certificaten

Het stamcertificaat, de domeincertificaten en CSP-certificaten worden in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties aangemaakt door de Policy Authority.

Opdracht tot het maken van CSP CA certificaten vindt plaats naar aanleiding van een aanvraag hiertoe door een CSP. Zie voor meer informatie PKIoverheid PvE deel 2.

De PA PKIoverheid controleert geen CAA records bij het tekenen van CSP CA’s.

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

4.2.1 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.

Het creëren van het stamcertificaat, de domeincertificaten en CSP-certificaten vindt plaats tijdens speciale creatieceremonies. Voor iedere creatieceremonie wordt een gedetailleerd draaiboek opgesteld waarin alle uit te voeren handelingen zijn vermeld. Dit draaiboek is met name bedoeld om invoerfouten tijdens de ceremonie te voorkomen.

De creatieceremonies verlopen voor alle genoemde typen certificaten op vergelijkbare wijze. Tijdens de ceremonie vinden onder meer de volgende stappen plaats:

1. opbouwen van het computersysteem;
2. installeren en configureren van de PKI-software;
3. activeren van de Hardware Security Module (HSM), waarbij meerdere sleutelhouders elk een deel van de activeringsgegevens inbrengen;

4. genereren van de sleutelparen;
5. genereren van certificaten voor elk sleutelpaar;
6. ontmantelen van het computersysteem en

veiligstellen van het computersysteem en de kritieke componenten.

4.3 Uitgifte van certificaten

Uitsluitend een CSP die 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.

De eisen waaraan een CSP dient te voldoen bij de uitgifte van de certificaten zijn geformuleerd in deel 3 (Certificate Policies) van het Programma van Eisen. De wijze waarop een CSP uitvoering geeft aan deze eisen dient door de CSP zelf beschreven te worden in een Certification Practice Statement (CPS). De beschrijving van de dienstverlening door CSP's valt derhalve buiten het bestek van dit CPS.

Voor het uitgeven van certificaten door de PA is geen separaat CP opgesteld, aangezien de PA geen eindgebruikercertificaten uitgeeft. De maatregelen die de PA heeft getroffen om de betrouwbaarheid van de door de PA uit te geven certificaten te waarborgen zijn in dit CPS beschreven.

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 Sleutelpaar 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.

Het Staat der Nederlanden Root CA, de Staat der Nederlanden <Domein> CA’s en de CSP CA’s certificaten worden primair gebruikt voor het verifiëren van de handtekening van de uitgever en worden uitgegeven door de PA. Daarnaast worden deze certificaten gebruikt voor CRL signing. Het is niet toegestaan deze certificaten voor andere doeleinden te gebruiken. Het eindgebruiker certificaat wordt uitgegeven door de CSP's.

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. Hierbij valt te denken aan het wijzigen van de naam van een CSP die in het certificaat is vermeld of, bij het verminderen van de sterkte van een cryptografisch algoritme, het opnemen van een sterker cryptografisch algoritme.
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 sleutelpaar vernieuwd.

4.7 Rekey van certificaten

Certificate Rekey waarbij de bestaande publieke sleutel in een certificaat wordt gewijzigd, wordt binnen de centrale hiërarchie van de PKI voor de Overheid niet toegepast.

4.8 Aanpassing van certificaten

Certificate Modification wordt alleen in uitzonderlijke gevallen toegepast. Normaliter zal de voorkeur worden gegeven aan het opnieuw uitgeven van een certificaat wanneer de inhoud van het certificaat (publieke sleutel) niet meer correct is.

4.9 Intrekking en opschorting van certificaten

Intrekking van het stamcertificaat, een domeincertificaat of een CSP-certificaat zal in ieder geval worden overwogen als de signing key behorende bij het certificaat is gecompromitteerd of daarvan wordt verdacht. Van compromittatie is onder meer sprake als ongeautoriseerd toegang is verkregen tot deze signing key of wanneer dragers hiervan zijn gestolen of verloren gegaan. Om dit te bewerkstelligen houdt de PA een registratie bij van de meldingen die kunnen leiden tot intrekking van het stamcertificaat, een domeincertificaat of een CSP-certificaat. Alle meldingen worden door de PA geregistreerd en in behandeling genomen. De Wet bescherming persoonsgegevens is van toepassing en wordt in acht genomen.

De PA merkt compromittatie van de signing key binnen de TEST/TRIAL hiërarchie aan als een incident. Doet zich een incident voor, dan treedt de incidentenregeling in werking en worden alle relevante partijen op de hoogte gesteld.

Voorafgaand aan het intrekken van een stamcertificaat, een domeincertificaat of een CSP-certificaat en de bij dat certificaat behorende sleutels wordt een zorgvuldig beoordelingsproces doorlopen. De PA zal deze beoordeling uitvoeren en zal eventuele hieruit voortvloeiende activiteiten (laten) initiëren.

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 CSP-certificaat. De intrekking van een certificaat kan binnen één dag worden geëffectueerd. De PA informeert de CSP vooraf over het intrekken van het certificaat.

In geval van het intrekken van het stamcertificaat informeert de PA de CSP's waarmee samenwerking is overeengekomen.

In geval van het intrekken van een domeincertificaat informeert de PA de onderliggende CSP's.

Het besluit het stamcertificaat of een domeincertificaat in te trekken zal gepaard gaan met een uitspraak over het al dan niet uitgeven van een nieuw certificaat ter vervanging van het ingetrokken certificaat.

Het intrekken van een domeincertificaat of een CSP-certificaat leidt altijd tot ad hoc publicatie van de betreffende gewijzigde CRL. Het intrekken van certificaten en het uitgeven van CRL's geschiedt conform een vooraf

opgesteld draaiboek Maximaal 24 uur na intrekking van domein of CSP CA zal de nieuwe CRL worden gepubliceerd.

Opschorting van certificaten wordt binnen de PKI voor de overheid niet ondersteund.

4.10 Certificaat statusservice

4.10.1 Operationele eigenschappen van de certificaat statusservice
De geldigheid van certificaten is raadpleegbaar middels de gepubliceerde CRL die verkrijgbaar is via de elektronische opslagplaats (zie 2.1). De PA hanteert voor de CRL's het X.509 versie 2 formaat.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.

4.10.2 Beschikbaarheid certificaat statusservice
Er zijn geen eisen gesteld aan de beschikbaarheid van de CRL

4.10.3 Optionele kenmerken van de certificaat statusservice
Geen nadere bepalingen voor de certificaatdienstverlening van CSP.

4.11 Beëindiging

Indien BZK besluit de dienst PKIoverheid te beëindigen, dan zullen de volgende stappen worden gevolgd:

1. Alle betrokken partijen (abonnees, cross certifying CA's, hoger gelegen CA's en vertrouwenspartijen) van de dienst PKIoverheid, zullen een half jaar voor het beëindigen van de dienst worden geïnformeerd.
2. Alle certificaten die zijn uitgeven na bekendmaking van het beëindigen van de dienst, zullen in het certificaat een einddatum bevatten gelijk aan de geplande einddatum van PKIoverheid.
3. Bij het beëindigen van de dienst zullen alle nog geldige certificaten worden ingetrokken.
4. PKIoverheid stopt op de einddatum met het distribueren van certificaten en CRL's.

4.11.1 Overdracht PKIoverheid

Indien BZK besluit de dienst PKIoverheid over te dragen aan een andere organisatie, dan zullen alle betrokken partijen (abonnees, cross certifying CA's, hoger gelegen CA's en vertrouwenspartijen) van de dienst PKIoverheid minimaal 3 maanden van tevoren worden geïnformeerd over de overdracht. De nieuwe organisatie zal de bepalingen uit deze CPS in haar eigen CPS overnemen.

4.12 Key escrow en recovery

Niet van toepassing.

4.13 Registratie van certificaathouders (geen RFC 3647)

De PA geeft in tegenstelling tot de CSP geen certificaten uit aan natuurlijke personen. Een registratie met persoonsgegevens van certificaathouders is derhalve niet aanwezig.

5 Fysieke, procedurele en personele beveiliging

In dit CPS zijn de door de PA getroffen beveiligingsmaatregelen op hoofdlijnen beschreven.

De PA heeft beheersmaatregelen geïmplementeerd om verlies, diefstal, beschadiging of compromittatie van infrastructurele middelen en onderbreking van de activiteiten te voorkomen. Daarbij is onder meer voorzien in fysieke toegangscontrole. De fysieke inrichting kent verschillende lagen die aparte toegangscontrole vereisen met steeds een hoger niveau van beveiliging. Daarnaast is een reeks van maatregelen getroffen ter bescherming tegen brand, natuurrampen, uitval van ondersteunende faciliteiten (zoals elektriciteit en telecommunicatie-voorzieningen), instortingsgevaar, lekkages, et cetera.

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 Audit logging 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 sleutelpaar vernieuwd.

5.7 Compromittatie 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.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

Het genereren van de sleutelparen van de PA vindt plaats tijdens de verschillende creatieceremonies. Daarbij worden slechts stand-alone computersystemen gebruikt. Deze computersystemen hebben geen verbinding met een netwerk, alle communicatie tussen systemen vindt plaats via media als USB stick of smartcard. Omdat het genereren en het gebruik van de signing key van de PA incidenteel plaatsvindt, zijn de computersystemen uitsluitend voor dit doel in gebruik. De meeste tijd zijn de kritische componenten van de computersystemen opgeborgen in een kluis.
De volgende sleutellengtes zijn van toepassing:

Eindgebruikerscertificaten	2048 bit RSA sleutels
CSP testcertificaten	4096 bit RSA sleutels
Sub CA testcertificaten	4096 bit RSA sleutels
Domein testcertifcaten	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 sleutelpaar management

Alle testcertificaten hebben een maximale periode van geldigheid:

Testcertificaten algemeen	6 maanden
Server type 1 testcertificaten	3 jaar
Server type 2 testcertificaten	1 maand
Interne Eindgebruiker testcertificaten[3]	Geen bepalingen
CSP testcertificaten	12 jaar minus 2 dagen
Domein testcertifcaten	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 Beheersingsmaatregelen technische levenscyclus

De hard- en software die wordt gebruikt in de centrale hiërarchie t.b.v. het keymanagement komt overeen met de systemen die gebruikt worden in het centrale deel van de productie hiërarchie van de PKI voor de overheid.

3 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.

6.7 Netwerkbeveiliging

De netwerkbeveiliging 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.

6.8 Tijdstempelen

De PA ondersteunt geen tijdstempeldienst als onderdeel van haar dienstverlening.

6.9 Cryptografische algoritmes (geen RFC 3647)

Binnen de PKI voor de overheid is, met het oog op de betrouwbaarheid van de PKI voor de overheid, een beperkt aantal cryptografische algoritmes toegestaan. De PA zal, gelet op de te verwachten ontwikkelingen, regelmatig nagaan of de gehanteerde standaarden nog voldoen volgens ETSI TS 119 312. Mocht een overstap naar een ander algoritme noodzakelijk zijn dan zal hierover vooraf ook advies worden gevraagd aan het Nationaal Bureau voor Verbindingsbeveiliging (NBV-AIVD). Op basis van de ETSI standaard is in de certificaatprofielen, die zijn opgenomen in deel 3 van het Programma van Eisen, aangegeven welke algoritmes zijn toegestaan.

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.

De CRL voor statuscontrole van de domein CA’s is een jaar geldig. De CRL voor statuscontrole van de CSP CA’s is een half jaar geldig.

Er is een overgangsperiode van twee weken voordat de CRL verloopt, waarbinnen een nieuwe CRL wordt gepubliceerd.

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, een baten- en lastendienst van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, en haar certificatendienstverleners aanvaarden geen enkele aansprakelijkheid voor schade die voorvloeit 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

De PA PKIoverheid geeft in tegenstelling tot de CSP geen certificaten uit aan natuurlijke personen. Een registratie met persoonsgegevens van certificaathouders is derhalve niet aanwezig.

9.5 Intellectuele eigendomsrechten

Voorliggend CPS is eigendom van Logius. Ongewijzigde kopieën van dit CPS mogen zonder toestemming verspreid en gepubliceerd worden mits dit met bronvermelding geschiedt.

9.6 Aansprakelijkheid en garanties

In aanvulling op het gestelde in paragraaf 9.2:
Logius, een baten- en lastendienst van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, én haar certificatiedienstverleners geven geen zekerheid over, en garanderen op geen enkele wijze de nauwkeurigheid, authenticiteit, integriteit, of de betrouwbaarheid van de informatie in testcertificaten waarop dit voorliggende CPS van toepassing is.

9.7 Verwerping van aansprakelijkheid

Geen nadere bepalingen in aanvulling op het gestelde in paragraaf 9.2 en 9.6.

9.8 Beperking van aansprakelijkheid

Geen nadere bepalingen in aanvulling op het gestelde in paragraaf 9.2 en 9.6.

9.9 Vrijwaring

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

9.10 Geldigheid CPS

Dit is versie 3.0 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, september 2016.

Dit CPS is geldig vanaf de datum inwerkingtreding. Het CSP is geldig zolang de dienstverlening van de PKI voor de overheid voortduurt of tot dat 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 volgende website (https://cps.pkioverheid.nl).

9.11 Afspraken en communicatie tussen entiteiten uit de PKIoverheid-hiërarchie

Indien CSP's vragen hebben kan contact worden opgenomen met de PA PKIoverheid.

Er wordt op regelmatige basis gecommuniceerd via e-mail met de contactpersonen van de aan het PKIoverheid stelsel deelnemende CSP's. CPS's worden terstond op de hoogte gesteld van de publicatie van een nieuwe versie van het CPS of Programma van Eisen. Ook worden voorgenomen wijzigingen zo snel mogelijk kenbaar gemaakt.

Naast communicatie met de CSP's is er tevens geregeld contact met de ACM en de auditor(s) van de deelnemende CSP's.

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 Geschillenbeslechting

Geen nadere bepalingen.

9.14 Van toepassing zijnde wetgeving

Het Nederlands recht is van toepassing.

9.15 Naleving relevante wetgeving

De PA-functie wordt uitgevoerd door Logius. Logius is een baten- en lastendienst van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 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 http://www.pkioverheid.nl/policies/TESTroot-policy-G2	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS http://www.pkioverheid.nl/policies/TESTdom-org-policy-G2	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS http://www.pkioverheid.nl/policies/TESTdom-bu-policy-G2	ID=2.5.29.32.0 Beleidskwalificatie-ID=CPS http://www.pkioverheid.nl/policies/TESTdom-aa-policy-G2
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= http://crl.pkioverheid.nl/pkiotest/TESTRootLatestCRL-G2.crl		
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