Getronics PinkRoccade Nederland BV

Fauststraat 1
Postbus 9105
7300 HN Apeldoorn

T +31[0]55 577 88 22
F +31[0]55 577 84 60
I www.getronicspinkroccade.nl

Certification Practice Statement PKIoverheid Certificaten

Datum 29 september 2006
Versie 3.1
Doc nr. TS-2004-0020

Inhoudsopgave

Lijst met afkortingen

Afkorting	Betekenis
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
CSP	Certification Service Provider ofwel certificatiedienstverlener
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
LRA	Lokale Registratie Autoriteit
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Persoonlijk Unlock Kengetal
RA	Registratie Autoriteit (Registration Authority)
SSCD	Secure Signature Creation Device
SUD	Secure User Device
VPN	Virtual Private Network
WBP	Wet Bescherming Persoonsgegevens
WID	Wet op de Identificatieplicht

Begrippenlijst

Aanvrager: een natuurlijke of rechtspersoon die een aanvraag tot uitgifte van een Certificaat indient bij Getronics PinkRoccade. De Aanvrager hoeft niet dezelfde partij te zijn als de Abonnee of de Certificaathouder, maar is wel één van beide.

Abonnee: de natuurlijke persoon of rechtspersoon die zich aanmeldt bij Getronics PinkRoccade om uitgifte van PKIoverheid Certificaten aan door hem aangewezen Certificaathouders te bewerkstelligen.

Algemene Voorwaarden: de Algemene Voorwaarden PKIoverheid Certificaten, zoals van toepassing op alle bij de uitgifte en het gebruik van PKIoverheid Certificaten betrokken partijen.

Asymmetrisch Sleutelpaar: een Publieke Sleutel en Private Sleutel binnen de public key cryptografie die wiskundig zodanig met elkaar zijn verbonden dat de publieke sleutel en de private sleutel elkaars tegenhanger zijn. Wordt de ene sleutel gebruikt om te versleutelen, dan móet de andere gebruikt worden om te ontsleutelen en omgekeerd.

Authenticatie: (1) Het controleren van een identiteit voordat informatieoverdracht plaatsvindt; (2) het controleren van de juistheid van een boodschap of afzender.

Authentificatie: zie Authenticatie.

CA-Certificaat: een Certificaat van een Certification Authority.

Certificaat: de Publieke Sleutel van een Eindgebruiker, samen met aanvullende informatie. Een Certificaat is vercijferd met de Private Sleutel van de Certification Authority die de Publieke Sleutel heeft uitgegeven, waardoor het Certificaat onvervalsbaar is.

Certificaataanvraag: de door een Aanvrager ingediend verzoek om uitgifte van een Certificaat door Getronics PinkRoccade.

Certificaatbeheerder: een natuurlijke persoon die bevoegd is om namens de Abonnee en ten behoeve van de Certificaathouder een Servercertificaat of Groepscertificaat aan te vragen, te installeren, te beheren en/of in te trekken. De Certificaatbeheerder voert handelingen uit waartoe de Certificaathouder zelf niet in staat is.

Certificaathouder: een entiteit die geïdentificeerd wordt in een Certificaat als de houder van de Private Sleutel behorende bij de Publieke Sleutel die in het Certificaat gegeven wordt.

Certificaatprofiel: een beschrijving van de inhoud van een Certificaat. Ieder soort Certificaat (handtekening, vertrouwelijkheid, e.d.) heeft een eigen invulling en daarmee een eigen beschrijving – hierin staan bijvoorbeeld afspraken omtrent naamgeving e.d.

Certificate Policy (CP): een benoemde verzameling regels die de toepasbaarheid van een Certificaat aangeeft voor een bepaalde gemeenschap en/of toepassingsklasse met

gemeenschappelijke beveiligingseisen. Met behulp van een CP kunnen Abonnees en Vertrouwende Partijen bepalen hoeveel vertrouwen zij kunnen stellen in het verband tussen de Publieke Sleutel en de identiteit van de houder van de Publieke Sleutel.

Certificate Revocation List: zie Certificaten Revocatie Lijst.

Certificaten Revocatie Lijst (CRL): een openbaar toegankelijke en te raadplegen lijst van ingetrokken Certificaten, ondertekend en beschikbaar gesteld door de uitgevende CSP.

Certificatie Autoriteit (CA): een organisatie die Certificaten genereert en intrekt. Het functioneren als CA is een deelactiviteit die onder de verantwoordelijkheid van de CSP wordt uitgevoerd. In dit verband opereert Getronics PinkRoccade derhalve als CA.

Certificatiediensten: het afgeven, beheren en intrekken van Certificaten door Certificatiedienstverleners.

Certification Practice Statement (CPS): een document dat de door een CSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de dienstverlening beschrijft. Het CPS beschrijft daarmee op welke wijze de CSP voldoet aan de eisen zoals gesteld in de van toepassing zijnde Certificate Policy.

Certification Practice Statement PKIoverheid (CPS PKIoverheid): de onderhavige Certification Practice Statement, zoals van toepassing op de uitgifte door Getronics PinkRoccade van PKIoverheid Certificaten alsmede het gebruik daarvan.

Certificatiedienstverlener: een natuurlijke persoon of rechtspersoon die als functie heeft het verstrekken en beheren van Certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (SSCD, SUD). De Certificatiedienstverlener heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatiediensten waarbij het niet uit maakt of hij de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen.

Certification Service Provider (CSP): zie Certificatiedienstverlener.

Digitale Handtekening: zie Geavanceerde Elektronische Handtekening.

Directory Dienst: een dienst van (of met medewerking van) een CSP die de door de CA uitgegeven Certificaten online beschikbaar en toegankelijk maakt ten behoeve van raadplegende of vertrouwende partijen.

Eindgebruiker: een natuurlijke persoon of rechtspersoon die binnen de PKI voor de overheid één of meer van de volgende rollen vervult: Abonnee, Certificaathouder of Vertrouwende Partij. Gezien het geringe onderscheidende vermogen van deze term wordt ze in de CPS niet gebezigd, behalve daar waar het de voorgeschreven structuur van het document betreft (d.w.z. headings e.d.)

Elektronische Handtekening: elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. De Elektronische Handtekening wordt ingezet om ervoor te zorgen dat

elektronische correspondentie en transacties op twee belangrijke punten kunnen wedijveren met de aloude “handtekening op papier”. Door het plaatsen van een Elektronische Handtekening staat vast dat iemand die zegt een document te hebben ondertekend, dat ook daadwerkelijk heeft gedaan.

Elektronische Opslagplaats: locatie waar relevante informatie ten aanzien van de dienstverlening van Getronics PinkRoccade is te vinden. Zie: https://www.pki.getronicspinkroccade.nl/pkioverheid.

Escrow (Key-escrow): Een methode om tijdens uitgifte van een certificaat een kopie te genereren van de Private Sleutel ten behoeve van toegang tot versleutelde gegevens door daartoe bevoegde partijen, alsmede de beveiligde bewaarneming daarvan.

Geavanceerde Elektronische Handtekening: een Elektronische Handtekening die voldoet aan de volgende eisen:

a) Zij is op unieke wijze aan de ondertekenaar verbonden;
b) Zij maakt het mogelijk de ondertekenaar te identificeren;
c) Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d) Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

Gegevens voor het aanmaken van Elektronische Handtekeningen: zie Signature Creation Data.

Gegevens voor het verifiëren van een Elektronische Handtekening: zie Signature Verification Data.

Gekwalificeerd Certificaat: een Certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een Certificatiedienstverlener die voldoet aan de eisen gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet. Het Certificaat dient tevens te strekken tot toepassing van de Gekwalificeerde Elektronische Handtekening.

Gekwalificeerde Elektronische Handtekening: een elektronische handtekening die voldoet aan de volgende eisen:

a) Zij is op unieke wijze aan de ondertekenaar verbonden;
b) Zij maakt het mogelijk de ondertekenaar te identificeren;
c) Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d) Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
e) Zij is gebaseerd op een Gekwalificeerd Certificaat als bedoeld in artikel 1.1 onderdeel dd van de Telecommunicatiewet;
f) Zij is gegenereerd door een veilig middel voor het aanmaken van Elektronische Handtekeningen als bedoeld in artikel 1.1 onderdeel gg van de Telecommunicatiewet.

Groepscertificaat : een op een SUD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van vertrouwelijkheid en authenticiteit ondersteunen en die voldoen aan de volgende vereisten:

1) Ze zijn uitgegeven aan een dienst of een functie door Getronics PinkRoccade, en
2) Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Services' (PvE deel 3b)

Hardware Security Module: De randapparatuur dat wordt gebruikt aan de server kant om cryptografische processen te versnellen. Met name dient hierbij gedacht te worden aan het aanmaken van sleutels.

Lokale Registratie Autoriteit (LRA): de organisatieeenheid of functie aan wie de uitvoering van de taak van Registratie Autoriteit is opgedragen en die fysiek de identificatie gegevens van een aanvrager verzamelt, controleert, registreert en doorstuurt ten behoeve van de Certificaat uitgifte.

Middel voor het vervaardigen van handtekeningen: zie Signature Creation Device.

Niet-Gekwalificeerd Certificaat: een Certificaat dat niet voldoet aan de voor een Gekwalificeerd Certificaat gestelde eisen.

Object Identifier: een rij van getallen die op unieke wijze en permanent een object aanduidt.

Online Certificate Status Protocol: een methode om de geldigheid van Certificaten online (en real time) te controleren. Deze methode kan worden gebruikt als alternatief voor het raadplegen van de CRL.

Onweerlegbaarheid: de eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.

Overheids-CA: een CA die binnen de hiërarchie van de PKI voor de overheid de stam-CA is. Ze vormt in technische zin het centrale punt voor het vertrouwen binnen de hiërarchie en wordt aangestuurd door de Overheids-Policy Authority.

Overheids-Policy Authority: de hoogste beleidsbepalende autoriteit binnen de hiërarchie van de PKI voor de overheid die de regie over de Overheids-CA voert.

Persoonlijk Certificaat: een op een SSCD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen, alsmede een Gekwalificeerd Certificaat dat de functie van onweerlegbaarheid ondersteunt, en die voldoen aan de volgende vereisten:

1) Ze zijn uitgegeven aan een natuurlijke persoon door Getronics PinkRoccade, en
2) Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Domein Overheid en Bedrijven" (PvE deel 3a).

PKI voor de overheid: een afsprakenstelsel dat generiek en grootschalig gebruik mogelijk maakt van de Elektronische Handtekening, en faciliteert voorts identificatie op afstand en

vertrouwelijke communicatie. Het afsprakenstelsel is eigendom van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en wordt beheerd door de Policy Authority PKIoverheid.

PKIoverheid Certificaat: een onder de PKI voor de Overheid door Getronics PinkRoccade uitgegeven Persoonlijk Certificaat, Servercertificaat of Groepscertificaat .

PKI voor de overheid: de Public Key Infrastructure van de Staat der Nederlanden.

Policy Management Authority: de organisatorische entiteit binnen Getronics PinkRoccade die verantwoordelijk is voor ontwikkelen, onderhouden en formeel vaststellen van aan de dienstverlening verwante documenten, inclusief de CPS.

Private key: zie Private Sleutel.

Private Sleutel: de sleutel van een asymmetrisch sleutelpaar die alleen bekend dient te zijn bij de houder ervan en strikt geheim moet worden gehouden. In het kader van de PKI voor de overheid wordt de Private Sleutel door de Certificaathouder gebruikt om zich elektronisch te identificeren, zijn Elektronische Handtekening te zetten of om een vercijferd bericht te ontcijferen.

Public key: zie Publieke Sleutel.

Public Key Infrastructure (PKI): het geheel van organisatie, procedures en techniek, benodigd voor het uitgeven, gebruiken en beheer van Certificaten.

Publieke Sleutel: de sleutel van een asymmetrisch sleutelpaar die publiekelijk kan worden bekendgemaakt. De publieke sleutel wordt gebruikt voor de controle van de identiteit van de eigenaar van het asymmetrisch sleutelpaar, voor de controle van de Elektronische Handtekening van de eigenaar van het asymmetrisch sleutelpaar en voor het vercijferen van informatie voor een derde.

Qualified Certificate Policy (QCP): Een Certificate Policy die een uitwerking van de vereisten bevat die zijn omschreven in artikel 18.15, eerste en tweede lid van de Telecommunicatiewet.

Registratie Autoriteit (RA): een Registratie Autoriteit zorgt voor de verwerking van Certificaataanvragen en alle daarbij behorende taken waarbij de verificatie van de identiteit van de Certificaathouder de belangrijkste is. In dit verband opereert PinkRoccade CPS als RA.

Root: het centrale gedeelte van een (PKI-)hiërarchie waaraan de gehele hiërarchie en haar betrouwbaarheidsniveau is opgehangen.

Root Certificate: zie Stamcertificaat.

Root Certification Authority (Root-CA): een Certificatie Autoriteit die het centrum van het gemeenschappelijk vertrouwen in een PKI-hiërarchie is. Het Certificaat van de Root-CA (de Root Certificate of Stamcertificaat) is self-signed, waardoor het niet mogelijk is de bron van de handtekening op dit Certificaat te authenticeren, alleen de integriteit van de inhoud van het

Certificaat. De Root-CA wordt echter vertrouwd op basis van bijvoorbeeld de CP en andere documenten. De Root-CA hoeft niet noodzakelijkerwijs aan de top van een hiërarchie te zijn gepositioneerd.

Secure Signature Creation Device (SSCD): een middel voor het aanmaken van Elektronische Handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet. Dit kan bijvoorbeeld een smartcard of een USB token zijn.

Secure User Device (SUD): Een middel dat de gebruikers private sleutel(s) bevat, deze sleutel(s) tegen compromittatie beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert namens de gebruiker.

Servercertificaat: een binnen de Veilige Omgeving van de Abonnee opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen en die voldoen aan de volgende vereisten:

1) Ze zijn door Getronics PinkRoccade uitgegeven aan een server, en
2) Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Services' (PvE deel 3b).

Services Certificaat: een Servercertificaat of een Groepscertificaat .

Signature Creation Data: unieke gegevens, zoals codes of private cryptografische sleutels, die door de ondertekenaar worden gebruikt om een Elektronische Handtekening te maken.

Signature Creation Device: geconfigureerde software of hardware die wordt gebruikt voor het implementeren van de gegevens voor het aanmaken van Elektronische Handtekeningen.

Signature Verification Data: gegevens, zoals codes of cryptografische publieke sleutels, die worden gebruikt voor het verifiëren van een Elektronische Handtekening.

Stamcertificaat: het Certificaat van de Root-CA. Dit is het Certificaat behorend bij de plek waar het vertrouwen in alle binnen de PKI voor de overheid uitgegeven Certificaten zijn oorsprong vindt. Er is geen hoger liggende CA waaraan het vertrouwen wordt ontleend. Dit Certificaat wordt door de Certificaathouder (binnen de PKI voor de overheid is dat de Overheids-CA) zelf ondertekend. Alle onderliggende Certificaten worden uitgegeven door de houder van het stamcertificaat.

Veilig middel voor het aanmaken van Elektronische Handtekeningen: zie Secure Signature Creation Device.

Veilige Omgeving: De omgeving van het systeem dat de sleutels van de Servercertificaten bevat. Binnen deze omgeving is het toegestaan de sleutels softwarematig te beschermen, in plaats van in een SUD. De compenserende maatregelen hiervoor moeten van dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging, audit en functiescheiding.[i]

Vertrouwelijkheidcertificaat: Certificaat waarin de Publieke Sleutel wordt gecertificeerd van het sleutelpaar dat voor vertrouwelijkheidsdiensten wordt gebruikt.

Vertrouwende partij: de natuurlijke persoon of rechtspersoon die ontvanger is van een Certificaat en die handelt in vertrouwen op dat Certificaat.

X.509: een ISO standaard die een basis voor de elektronische opmaak van Certificaten definieert.

1 Introductie

1.1 Achtergrond

Getronics PinkRoccade is een Certificatiedienstverlener (CSP) die PKIoverheid Certificaten uitgeeft binnen het Domein Overheid en Bedrijven van de PKI voor de overheid.

De PKIoverheid Certificaten van Getronics PinkRoccade ondersteunen samen vier functies:

- Authenticiteit (identificatie);
- Onweerlegbaarheid (Elektronische Handtekening);
- Vertrouwelijkheid van berichten (emails); en,
- Vertrouwelijkheid van server verbindingen (Secure Socket Layer)

Certificaten voor authenticiteit kunnen worden gebruikt ten behoeve van het betrouwbaar identificeren en authenticeren van personen, organisaties en middelen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en middelen. Ten behoeve van authenticiteit wordt steeds gebruik gemaakt van Niet-Gekwalificeerde Certificaten.

Certificaten voor onweerlegbaarheid kunnen worden gebruikt om Geavanceerde Elektronische Handtekeningen te zetten, die ten aanzien van gegevens in elektronische vorm voldoen aan alle wettelijke vereisten voor een handtekening, net zoals een handgeschreven handtekening dat doet voor gegevens op papier. Ten behoeve van onweerlegbaarheid wordt steeds gebruik gemaakt van Gekwalificeerde Certificaten.

Certificaten voor vertrouwelijkheid van berichten of server verbindingen kunnen worden gebruikt ten behoeve van het beschermen van de vertrouwelijkheid van gegevens die worden uitgewisseld en/of opgeslagen in elektronische vorm. Dit betreft zowel de uitwisseling van gegevens tussen services onderling als tussen personen en services. Ten behoeve van vertrouwelijkheid wordt steeds gebruik gemaakt van Niet-Gekwalificeerde Certificaten.

Op basis van de hiervoor genoemde functies levert Getronics PinkRoccade drie typen PKIoverheid Certificaten, te weten:

1. Persoonlijke Certificaten
2. Servercertificaten
3. Groepscertificaten

Onderstaande tabel geeft aan welke functies door welke PKIoverheid Certificaten worden ondersteund:

	Persoonlijk Certificaat	Servercertificaat	Groepscertificaat
Authenticiteit	•	•	•
Onweerlegbaarheid	•		
Vertrouwelijkheid berichten	•		•
Vertrouwelijkheid server verbindingen		•	

1.1.1 Doel van de CPS

De CPS PKIoverheid vormt de beschrijving van de wijze waarop Getronics PinkRoccade invulling geeft aan haar dienstverlening rondom PKIoverheid Certificaten. De CPS bevat onder meer een beschrijving van de procedures die Getronics PinkRoccade hanteert bij de aanmaak, de uitgifte en het intrekken van Certificaten.

1.1.2 Positionering van de CPS

De CPS PKIoverheid is opgesteld conform de voorwaarden opgenomen in de CP van PKIoverheid – Domein Overheid en Bedrijven.

De Certificate Policy kan via de volgende Object Identifiers (OID) worden geïdentificeerd:

Persoonlijke Certificaten:

2.16.528.1.1003.1.2.2.1	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van identificatie of authenticatie
2.16.528.1.1003.1.2.2.2	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van onweerlegbaarheid (Gekwalificeerde Elektronische Handtekening)
2.16.528.1.1003.1.2.2.3	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van vertrouwelijkheid

Servercertificaten:

2.16.528.1.1003.1.2.2.4	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van identificatie of authenticatie.
2.16.528.1.1003.1.2.2.6	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van de vertrouwelijkheid van server verbindingen

Groepscertificaten:

2.16.528.1.1003.1.2.2.4	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van identificatie of authenticatie.

2.16.528.1.1003.1.2.2.5	voor het Certificaat dat de Publieke Sleutel bevat ten behoeve van vertrouwelijkheid.

1.1.3 Status

Formeel wordt dit document als volgt aangeduid: ‘Certification Practice Statement PKIoverheid’. In het kader van dit document wordt ze ook wel aangeduid als ‘CPS PKIoverheid’ of kortweg als ‘CPS’. Daar waar van die afkorting sprake is, wordt dit document bedoeld.

De CPS PKIoverheid kan via de volgende Object Identifier (OID) worden geïdentificeerd:

2.16.528.1.1005.1.1.1.2

De CPS PKIoverheid is geldig vanaf de datum van uitgifte, (zoals vermeld op het titelblad) voor zolang als de Getronics PinkRoccade dienstverlening voortduurt, danwel totdat de CPS wordt vervangen door een nieuwere versie (aan te duiden in het versienummer met +1 bij ingrijpende wijzigingen en +0.1 bij redactionele aanpassingen).

Getronics PinkRoccade aanvaardt geen enkele aansprakelijkheid voor schade als gevolg van onjuistheden of onvolkomenheden in de CPS noch voor schade die wordt veroorzaakt door het gebruik of de verspreiding van deze CPS buiten het toepassingsgebied.

1.1.4 Doelgroep en leeswijzer

Primaire doelgroep	Getronics PinkRoccade Abonnees Getronics PinkRoccade Contactpersonen van de Abonnee Certificaathouders & Certificaatbeheerders Vertrouwende Partijen
Achtergrond voor	Andere betrokken partijen

Voor informatie aangaande de opzet van dit document wordt verwezen naar 1.1.7.

1.1.5 Verhouding tussen CP en CPS

De CP beschrijft welke eisen er aan uitgifte en gebruik van een Certificaat binnen het Domein Overheid en Bedrijven van de PKI voor de overheid worden gesteld, terwijl de CPS beschrijft op welke wijze Getronics PinkRoccade aan deze eisen tegemoet is gekomen.

1.1.6 Normatieve referenties

Getronics PinkRoccade is gecertificeerd tegen het Scheme for Certification of Certification Authorities against ETSI TS 101 456. De volledige naam van dit document is ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates. Getronics PinkRoccade voldoet daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners in de Wet Elektronische Handtekening. Getronics PinkRoccade voldoet tevens aan de relevante onderdelen van het normenkader van de PKI voor de overheid zoals gesteld in het Programma van Eisen (zie hiervoor http://www.pkioverheid.nl).

1.1.7 Opzet van dit document

De indeling van deze CPS is conform de RFC2527 standaard (voluit: 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework', RFC 2527 van de Internet Engineering Task Force). Voor meer informatie zie http://www.ietf.org.

1.1.8 Definities en afkortingen

De in deze CPS gehanteerde begrippen en afkortingen worden verklaard in de voorafgaand aan hoofdstuk 1 opgenomen begrippenlijst en lijst van afkortingen

1.2 Verwijzingen naar deze CPS

Op alle PKIoverheid Certificaten die door Getronics PinkRoccade worden uitgegeven is de CPS volledig van toepassing.

1.3 Gebruikersgemeenschap en toepassingsgebied

1.3.1 Gebruikersgemeenschap

De gebruikersgemeenschap voor de PKIoverheid Certificaten bestaat uit Abonnees, Certificaathouders, Certificaatbeheerders en Vertrouwende Partijen.

Op de gebruikersgemeenschap zijn de Algemene Voorwaarden van toepassing (zie https://www.pki.getronicspinkroccade.nl/pkioverheid). De Algemene Voorwaarden zijn bindend voor alle bij de dienstverlening betrokken partijen. In geval van strijd tussen de CPS PKIoverheid en de Algemene Voorwaarden genieten laatstgenoemde voorrang.

1.3.2 Toepassingsgebied

Geen nadere bepalingen.

1.4 Contactgegevens

Informatie met betrekking tot dit CPS en commentaar daarop kan worden gericht aan:

Getronics PinkRoccade Nederland B.V.
t.a.v. BSS, Policy Management Authority
Postbus 9105
7300 HN Apeldoorn
pkisupport@getronics.com

Commerciële vragen inzake PKIoverheid Certificaten en daarmee verwante dienstverlening kunnen worden gericht aan: pkisales@getronics.com.

Overige documenten die verband houden met de dienstverlening rondom PKIoverheid Certificaten door Getronics PinkRoccade zijn te vinden via de algemene website: https://www.pki.getronicspinkroccade.nl/pkioverheid. Meer informatie over de PKI voor de overheid is te vinden op http://www.pkioverheid.nl.

De PKIoverheid Certificaten zijn een dienst van Getronics PinkRoccade Nederland B.V. Voor meer informatie over Getronics PinkRoccade, zie: http://www.getronicspinkroccade.nl. De onderhavige dienst werd voorheen in de markt gezet onder de naam ‘PinkRoccade CSP’ door PinkRoccade Infrastructure Services BV.

2 Algemene bepalingen

2.1 Verplichtingen

In dit hoofdstuk worden de verplichtingen van de diverse partijen gespecificeerd.

2.1.1 Verplichtingen van de CSP

Als Certificatiedienstverlener garandeert Getronics PinkRoccade tegenover Abonnees, Certificaathouders en Vertrouwende Partijen dat ze zich zal houden aan de Algemene Voorwaarden, de CPS PKIoverheid en de Certificate Policy Domein Overheid en Bedrijven van PKIoverheid.

2.1.2 Verplichtingen van de Abonnee

De Abonnee garandeert tegenover Getronics PinkRoccade en Vertrouwende Partijen dat hij zich zal houden aan de Algemene Voorwaarden en de CPS PKIoverheid.

2.1.3 Verplichtingen van de Certificaathouder

De Certificaathouder (inclusief, in geval van een Servercertificaat of Groepscertificaat , de Certificaatbeheerder) garandeert tegenover Getronics PinkRoccade, de Abonnee en Vertrouwende Partijen dat hij zich zal houden aan de Algemene Voorwaarden en de CPS PKIoverheid.

2.1.4 Verplichtingen van de Vertrouwende Partij

De Vertrouwende Partij garandeert tegenover Getronics PinkRoccade, de Abonnee en de Certificaathouder dat hij zich zal houden aan de Algemene Voorwaarden en de CPS PKIoverheid.

2.2 Aansprakelijkheid

2.2.1 Aansprakelijkheid van Getronics PinkRoccade

Getronics PinkRoccade aanvaardt de aansprakelijkheid voor PKIoverheid Certificaten zoals opgenomen in de Algemene Voorwaarden.

2.2.2 Beperkingen van aansprakelijkheid jegens de Vertrouwende Partij

De aansprakelijkheid van Getronics PinkRoccade jegens Vertrouwende Partijen is beperkt op de wijze zoals beschreven in de Algemene Voorwaarden.

2.3 Financiële verantwoordelijkheid

Getronics PinkRoccade heeft adequate regelingen getroffen, onder andere in de vorm van verzekeringen, om aansprakelijkheden die verband houden met de onderhavige dienstverlening af te dekken. Daarnaast bezit Getronics PinkRoccade de financiële stabiliteit en middelen die nodig zijn voor een gezonde bedrijfsvoering.

2.3.1 Vertrouwensrelaties

Geen nadere bepalingen.

2.3.2 Bestuurlijke processen

De financiële jaarrekening van Getronics PinkRoccade Nederland BV is geïntegreerd in de jaarrekening van Getronics NV. Als beursgenoteerd bedrijf is het Getronics NV niet toegestaan om, buiten de reguliere verslagen en officiële kanalen, financiële gegevens te verstrekken.

2.4 Interpretatie en handhaving

2.4.1 Van toepassing zijnde wetgeving

Op de diensten van Getronics PinkRoccade is bij uitsluiting Nederlands recht van toepassing.

2.4.2 Geldigheid en toepasselijkheid

Geen nadere bepaling.

2.4.3 Geschillenbeslechting

Geschillen die uit de diensten van Getronics PinkRoccade mochten voortvloeien of daarmee verband houden, zullen in eerste instantie tussen partijen onderling worden opgelost, eventueel met behulp van tussenpersonen. In zoverre dit het geschil niet beslecht, wordt ze bij uitsluiting voorgelegd aan de bevoegde rechter te Amsterdam.

2.5 Tarieven

Geen nadere bepalingen.

2.6 Publicatie en elektronische opslagplaats

2.6.1 Publicatie van CSP informatie

Via de Elektronische Opslagplaats (https://www.pki.getronicspinkroccade.nl/pkioverheid) is tenminste het volgende online beschikbaar:

1. Stamcertificaat
2. Certificate Revocation List
3. Algemene voorwaarden
4. CPS PKIoverheid
5. Certificate Policy – Domein Overheid en Bedrijven
6. Directory Dienst
7. Afschrift ETSI-certificaat

2.6.2 Publicatie van Certificaat

Certificaten worden gepubliceerd via de Directory Dienst, als onderdeel van de uitgifteprocedure. Via de Directory Dienst kan het Certificaat worden geraadpleegd door Abonnees, Certificaatbeheerders, Certificaathouders en Vertrouwende Partijen.

De Directory Dienst is op adequate wijze beveiligd tegen manipulatie en is online toegankelijk. Informatie over de intrekkingstatus is vierentwintig uur per dag en zeven dagen per week te raadplegen.

In geval van systeemdefecten, serviceactiviteiten, of andere factoren die buiten het bereik van Getronics PinkRoccade liggen, zal Getronics PinkRoccade al het mogelijke doen om ervoor te zorgen dat de Directory Dienst zo snel mogelijk weer bereikbaar is. Getronics PinkRoccade is niet verantwoordelijk voor de niet-beschikbaarheid van de Directory Dienst vanwege natuurrampen of andere omstandigheden waar Getronics PinkRoccade niet verantwoordelijk voor kan worden gehouden.

Behoudens het ETSI certificaat worden afschriften en rapportages betrekking hebbende op de normatieve referenties van Getronics PinkRoccade niet in de Elektronische Opslagplaats opgeslagen.

2.6.3 Publicatie frequentie

Geen nadere bepalingen.

2.6.4 Toegang tot gepubliceerde informatie

Informatie in de Elektronische Opslagplaats is publiek van aard en vrij toegankelijk. De Elektronische Opslagplaats kan vierentwintig uur per dag en zeven dagen per week worden geraadpleegd.

2.6.5 Elektronische opslagplaats

Getronics PinkRoccade zorgt voor de beschikbaarheid van de informatie in de Elektronische Opslagplaats.

In geval van systeemdefecten, serviceactiviteiten of andere factoren die buiten het bereik van Getronics PinkRoccade liggen, zal Getronics PinkRoccade al het redelijkerwijs mogelijke doen om ervoor te zorgen dat de Elektronische Opslagplaats binnen vierentwintig uur weer bereikbaar is.

2.7 Conformiteitbeoordeling

Getronics PinkRoccade Nederland bv is gecertificeerd tegen het "Scheme for Certification of Certification Authorities against ETSI TS 101 456:2000" op 1 november 2002 door KPMG Certification en voldoet daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners in de Wet Elektronische Handtekening.

Getronics PinkRoccade voldoet tevens aan het Programma van Eisen, de delen 3a en 3b. Een externe, ter zake gekwalificeerde auditor heeft hiervoor auditverklaringen afgegeven.

Getronics PinkRoccade is als certificatiedienstverlener geregistreerd bij de OPTA, onder registratienummer 901278, als getoetste uitgever van Gekwalificeerde Certificaten aan het publiek.

2.8 Vertrouwelijkheid

2.8.1 Vertrouwelijke informatie

Tenminste de volgende informatie wordt als vertrouwelijk beschouwd en niet aan derden verstrekt:

- Aanvraagformulieren (inclusief bijgevoegde informatie)
- Overeenkomsten met Abonnees
- Overeenkomsten met LRA's
- Interne beveiligingsprocedures en maatregelen
- Interne procedures Administratieve Organisatie (AO)
- Audit rapporten
- Private sleutels

2.8.2 Niet-vertrouwelijke informatie

De gegevens in het Certificaat zijn niet vertrouwelijk. De Certificaathouder, de Certificaatbeheerder en de Abonnee hebben toestemming voor publicatie gegeven door instemming met de Algemene Voorwaarden. Het voltooien van een aanvraagprocedure door de Certificaathouder wordt door Getronics PinkRoccade beschouwd als toestemming voor publicatie van de gegevens in het Certificaat.

2.8.3 Openbaarmaking informatie intrekking Certificaat

Informatie met betrekking tot intrekking van Certificaten is beschikbaar via de CRL. De daar gegeven informatie betreft slechts het Certificaatnummer, het moment van intrekking en de status (geldig/ingetrokken) van het Certificaat. Indien Getronics PinkRoccade eigenhandig een Certificaat intrekt, zal deze via de CRL worden gepubliceerd.

2.8.4 Verstrekking aan opsporingsambtenaren

Getronics PinkRoccade verstrekt vertrouwelijke gegevens niet aan opsporingsambtenaren, behoudens voor zover Nederlandse wet- en regelgeving Getronics PinkRoccade daartoe dwingt en enkel na overhandiging van een rechtsgeldige sommatie.

2.8.5 Verstrekking in verband met privaatrechtelijke bewijsvoering

Het Certificaat en de bij de Certificaataanvraag verstrekte gegevens zullen blijven opgeslagen gedurende een nader aan de Abonnee en/of Certificaathouder opgegeven periode (zie paragraaf 4.6) en voor zover nodig voor het leveren van bewijs van certificatie in de rechtsgang. Vertrouwelijke gegevens zullen slechts ter bewijsvoering aan andere partijen dan de Abonnee en de Certificaathouder worden verstrekt met voorafgaande schriftelijke toestemming van de Abonnee danwel de Certificaathouder.

2.8.6 Verstrekking op verzoek van de eigenaar

Getronics PinkRoccade verstrekt de Abonnee en/of Certificaatbeheerder of Certificaathouder desgevraagd de hem betreffende persoonsgegevens. Getronics PinkRoccade verstrekt de Abonnee desgevraagd persoonsgegevens van een Certificaatbeheerder of Certificaathouder die in aanvraag van de betreffende Abonnee een Certificaat heeft ontvangen.

Getronics PinkRoccade is gerechtigd per verstrekking een passende vergoeding te vragen.

2.8.7 Andere omstandigheden die kunnen leiden tot informatieverstrekking

Geen nadere bepalingen.

2.9 Intellectueel eigendom

Het intellectueel eigendomsrecht van deze CPS berust bij Getronics PinkRoccade.

Eigendomsrechten met betrekking tot het Certificaat, de SSCD en de SUD blijven ook na uitgifte berusten bij Getronics PinkRoccade en diens licentiegevers, inclusief rechten van intellectueel eigendom. Hetzelfde geldt voor documentatie verstrekt vanwege de dienstverlening van Getronics PinkRoccade, inclusief deze CPS PKIoverheid.

3 Identificatie en authenticatie

3.1 Initiële registratie

3.1.1 Soorten naamformaten

De in Certificaten gebruikte namen voldoen aan de X.501 naam standaard. De namen bestaan uit de volgende onderdelen:

Attribuut	Waarde
Country (C)	NL
Organization (O)	Naam van de Abonnee
Organizational Unit (OU)	Naam van organisatieonderdeel van de Abonnee
State or Province (S)	Niet gebruikt
Locality (L)	Niet gebruikt
Common Name (CN)	Voor- en achternaam van de Certificaathouder
E-Mail Address (E)	E-mail adres

Namen van personen opgenomen in het Certificaat voldoen aan de eisen die aan naamformaten zijn gesteld in het Programma van Eisen, deel 3 – bijlage A Certificaat-, CRL- en OCSP-profielen (Naamconventie Subject.commonName).

De in Servercertificaten en Groepscertificaten gebruikte namen voldoen aan de X.501 naam standaard. De namen bestaan uit de volgende onderdelen:

Attribuut	Waarde
Country (C)	NL
Organization (O)	Naam van de Abonnee-organisatie
Common Name (CN)	Naam van de Certificaathouder
Optioneel:	
Organizational Unit (OU)	Afdeling van de organisatie van Abonnee
State or Province (S)	Provincie waar de Abonnee gevestigd is
Locality (L)	Plaats waar de Abonnee gevestigd is
E-Mail Address (E)	E-mail adres (niet voor Servercertificaten)

3.1.2 Noodzaak van betekenisvolle namen

Naamgeving die in de door Getronics PinkRoccade uitgegeven Certificaten wordt gehanteerd, is ondubbelzinnig, zodanig dat het voor de Vertrouwende Partij mogelijk is de identiteit van de Certificaathouder onomstotelijk vast te stellen.

Getronics PinkRoccade neemt geen pseudoniemen in de door haar uitgegeven Certificaten op.

3.1.3 Richtlijnen voor het interpreteren van de diverse naamvormen

Geen nadere bepalingen.

3.1.4 Uniciteit van namen

De gebruikte namen identificeren de Certificaathouder op unieke wijze. Uniciteit van namen binnen de X.501 name space is daarbij het uitgangspunt.

3.1.5 Geschillenbeslechting inzake naam claims

In gevallen waarin partijen het oneens zijn over het gebruik van namen, beslist Getronics PinkRoccade na afweging van de betrokken belangen, voorzover hierin niet wordt voorzien door dwingend Nederlands recht of overige toepasselijke regelgeving.

3.1.6 Erkenning, authenticatie en de rol van handelsmerken

Abonnees dragen de volledige verantwoordelijkheid voor eventuele juridische gevolgen van het gebruik van de door hen opgegeven naam.

De naam van een organisatorische entiteit zoals deze wordt genoemd in het uittreksel van een erkend register, dan wel in de wet of het besluit waarbij de organisatorische entiteit is ingesteld, wordt gebruikt in het Certificaat.

Getronics PinkRoccade is niet gehouden een onderzoek in te stellen naar mogelijke inbreuken op handelsmerken die ontstaan als gevolg van het gebruik van een naam die deel uitmaakt van de in het Certificaat opgenomen gegevens.

Getronics PinkRoccade heeft het recht wijzigingen aan te brengen in naamattributen wanneer deze in strijd blijken met een handelsmerk of met andere rechten van intellectueel eigendom.

3.1.7 Methode om bezit van Private Sleutel aan te tonen

Getronics PinkRoccade kan, met het oog op de gebruikmaking van veilige en betrouwbare systemen en ter controle van correct werkende processen, aan Abonnee en/of Certificaathouder de verplichting opleggen om aan te tonen dat de voor het Certificaat noodzakelijke sleutelparen correct werken. Deze verplichting geldt niet als dit van de Abonnee en/of Certificaathouder een onevenredige inspanning vergt.

De Certificaathouder kan het bezit van de Private Sleutel aantonen door een daartoe bestemd bericht te ondertekenen. Een geslaagde verificatie door Getronics PinkRoccade bewijst vervolgens afdoende dat de Private Sleutel in het bezit van de Certificaathouder is.

3.1.8 Authenticatie van organisatorische identiteit

Ten behoeve van de aanvraag van een organisatie die als Abonnee aangemerkt wil worden binnen de PKI voor de overheid dient het volgende te worden overlegd:

- Volledige naam en wettelijke status van de betreffende organisatie;
- Bewijs dat de organisatie past binnen of onderdeel uitmaakt van het Domein Overheid en Bedrijven, zoals een overheidsbesluit, een bewijs van inschrijving in de Kamer van Koophandel, een recent uittreksel uit een ander erkend register, of een oprichtingsakte;
- Bewijs dat de naam van de organisatorische entiteit juist ,en volledig en actueel is;
- Naam en de functie van de medewerker die de organisatie vertegenwoordigt bij het aanvragen en intrekken van (Services) Certificaten, alsmede schriftelijk bewijs van diens vertegenwoordigingsbevoegdheid en een duidelijke kopie van een geldig en wettelijk erkende identiteitsbewijs.

De betreffende bevoegde vertegenwoordiger dient het aanvraagformulier te ondertekenen. Getronics PinkRoccade zal het formulier plus de bijgevoegde stukken controleren op echtheid, volledigheid en juistheid.

3.1.9 Authenticatie van persoonlijke identiteit

3.1.9.1 Authenticatie ten behoeve van Persoonlijk Certificaat

Ten behoeve van de aanvraag van een Persoonlijk Certificaat dienen de navolgende gegevens verstrekt te worden op een door of namens de Abonnee ondertekend aanvraagformulier:

- Abonneenummer en naam Abonnee
- Persoonlijke gegevens Certificaathouder
- Email-adres Certificaathouder
- Universal Principal Name (UPN)

Een fotokopie van het identiteitsbewijs van de Certificaathouder dient met de aanvraag te worden meegestuurd. Het identiteitsbewijs moet voldoen aan de eisen uit de Wet op de Identificatie (WID) en mag op de (beoogde) datum van uitgifte van het Persoonlijk Certificaat niet zijn verstreken.

De vaststelling van de identiteit van de Certificaathouder geschiedt op het moment van uitgifte in persoonlijke aanwezigheid van die Certificaathouder, danwel met gebruikmaking van middelen die eenzelfde mate van bewijskracht opleveren als in geval van verschijning in persoon.

3.1.9.2 Authenticatie ten behoeve van Servercertificaat

Ten behoeve van de aanvraag van een Servercertificaat dienen de navolgende gegevens verstrekt te worden op een door of namens de Abonnee ondertekend aanvraagformulier:

Van de Abonnee:

- Naam en abonneenummer
- Naam en email-adres contactpersoon
- CSR nummer

Van de Certificaathouder tenminste:

- CSR gegevens van de server
- Identifier server

Van de Certificaatbeheerder:

- Volledige namen en andere persoonsgegevens
- Postadresgegevens
- Email-adres

Indien de Certificaatbeheerder niet tot de organisatie van de Abonnee behoort, dient zulks eveneens te worden aangegeven ten behoeve van authenticatie.

Met de aanvraag dient een fotokopie van het identiteitsbewijs van de Certificaatbeheerder meegestuurd de worden. Het identiteitsbewijs moet voldoen aan de eisen uit de WID en mag niet zijn verstreken.

3.1.9.3 Authenticatie ten behoeve van Groepscertificaat

Ten behoeve van de aanvraag van een Groepscertificaat dienen de navolgende gegevens verstrekt te worden op een door of namens de Abonnee ondertekend aanvraagformulier:

Van de Abonnee:
- Naam en abonneenummer
- Naam en email-adres contactpersoon

Van de Certificaathouder:
- Naam van de groep of service
- Email-adres
- Universal Principal Name

Van de Certificaatbeheerder:
- Volledige namen en andere persoonsgegevens
- Postadresgegevens
- Email-adres

Indien de Certificaatbeheerder niet tot de organisatie van de Abonnee behoort, dient zulks eveneens te worden aangegeven ten behoeve van authenticatie.

Met de aanvraag dien een fotokopie van het identiteitsbewijs van de Certificaatbeheerder meegestuurd de worden. Het identiteitsbewijs moet voldoen aan de eisen uit de WID en mag op de datum van uitgifte niet zijn verstreken.

Na ontvangst van het aanvraagformulier zal Getronics PinkRoccade beoordelen of de aanvraag volledig (onvolledige aanvragen worden niet in behandeling genomen) en juist is. Getronics PinkRoccade zal de abonnee informeren over de uitkomst van de beoordeling.

3.1.10 Autorisatie van Certificaathouder

De autorisatie van de Certificaathouder om een Certificaat van de organisatie te mogen ontvangen en te gebruiken blijkt uit de ondertekening van de aanvraag door of namens de Abonnee.

Indien sprake is van een Servercertificaat, dient door de Abonnee het bewijs te worden geleverd van de identifier van het apparaat of systeem, waardoor er naar kan worden verwezen.

Na ontvangst van het aanvraagformulier zal Getronics PinkRoccade beoordelen of de aanvraag volledig en juist is. Getronics PinkRoccade zal de abonnee informeren over de uitkomst van de beoordeling. Onvolledige aanvragen worden niet in behandeling genomen.

3.1.11 Authenticatie van intrekkingsverzoeken

Voor het op elektronische wijze indienen van een intrekkingsverzoek voor een Persoonlijk Certificaat geldt, dat zulke verzoeken worden geautoriseerd met de Private Sleutel die wordt gebruikt ten behoeve van onweerlegbaarheid (Gekwalificeerde Elektronische Handtekening) in combinatie met de bij het Persoonlijk Certificaat behorende intrekkingscode.

Voor het op elektronische wijze indienen van een intrekkingsverzoek voor een Servercertificaat en Groepscertificaat geldt, dat zulke verzoeken worden geautoriseerd met de daarbij behorende intrekkingscode.

De Certificaathouder kan zijn verzoek online indienen via de website van Getronics PinkRoccade (www.pki.getronicspinkroccade.nl/intrekking). Tevens kan hij een intrekkingsverzoek indienen met behulp van het formulier 'Intrekkingsverzoek Certificaten' of met behulp van de Abonnee.

Indien Getronics PinkRoccade gerede aanleiding heeft om te twijfelen over de authenticiteit van een intrekkingsverzoek, kan van diegene die het verzoek heeft ingediend worden verlangd dat hij zich persoonlijk legitimeert tegenover Getronics PinkRoccade voordat aan de intrekking uitvoering wordt gegeven.

3.2 Routinematige vernieuwing van het Certificaat

Getronics PinkRoccade biedt momenteel geen mogelijkheid tot routinematige vernieuwing van PKIoverheid Certificaten.

Getronics PinkRoccade zal de Abonnee minimaal twee maanden voor het verlopen van de geldigheidsduur van op zijn verzoek uitgegeven Certificaten informeren over het verstrijken van de geldigheidstermijn.

3.3 Vernieuwing van sleutels na intrekking van het Certificaat

Getronics PinkRoccade certificeert bestaande sleutels niet na intrekking van het Certificaat.

3.4 Verzoeken tot intrekking

Alle conform de daartoe gestelde procedure, zoals beschreven in paragraaf 4.4.3, gedane verzoeken tot intrekking worden door Getronics PinkRoccade in behandeling genomen.

Getronics PinkRoccade is eveneens gerechtigd zelfstandig tot intrekking over te gaan indien:

- De Abonnee en/of Certificaathouder handelt in strijd met de aan hem opgelegde voorwaarden voor gebruik, zoals onder meer vastgelegd in deze CPS PKIoverheid en in de Algemene Voorwaarden, of
- De Private sleutel van de CA van Getronics PinkRoccade of van de Staat der Nederlanden verloren raakt, wordt gestolen of anderszins wordt gecompromitteerd.

4 Operationele eisen

4.1 Aanvraag van Certificaten

Er zijn twee soorten procedures:

1. Aanvragen van Persoonlijke Certificaten en Groepscertificaten, waarbij het sleutelpaar wordt aangemaakt door Getronics PinkRoccade; en,
2. Aanvragen van Servercertificaten, waarbij het sleutelpaar wordt aangemaakt door de Abonnee in de Veilige Omgeving van de Abonnee.

4.1.1 Aanvraag Persoonlijke Certificaten en Groepscertificaten

Voor het aanvragen van een Persoonlijk Certificaat of Groepscertificaat dienen de volgende stappen te worden doorlopen.

1. De Abonnee vult een aanvraagformulier in en verklaart zich daarin onder andere akkoord met de Algemene Voorwaarden.
2. De Abonnee ondertekent het aanvraagformulier, voorziet deze van een kopie van het identiteitsbewijs van de (beoogd) Certificaathouder en verstuurt het naar Getronics PinkRoccade.
3. Getronics PinkRoccade neemt de aanvraag in ontvangst en beoordeelt de volledigheid en de juistheid.
4. Indien Getronics PinkRoccade de aanvraag goedkeurt, wordt het Certificaat aangemaakt en op een SSCD geplaatst. Tevens genereert Getronics PinkRoccade de geheime toegangscodes voor de SSCD en de intrekkingscodes voor het Certificaat.
5. Alvorens de uitgifte plaats kan vinden, dient de Certificaathouder of Certificaatbeheerder zich te identificeren tegenover Getronics PinkRoccade conform het in de paragrafen 3.1.9 en 3.1.10 gestelde.
6. Indien de identificatie slaagt, geeft Getronics PinkRoccade het Persoonlijk Certificaat of Groepscertificaat uit aan de Certificaathouder of Certificaatbeheerder. Zie hiervoor 4.2.1.

4.1.2 Aanvraag Servercertificaten

De aanvraag voor een Servercertificaat verloopt hetzelfde als onder 4.1.1 genoemd, met inachtneming van de volgende verschillen.

- Certificaatbeheerders van Servercertificaten dienen voorafgaand aan de aanvraagprocedure als zodanig te worden geïdentificeerd door en geregistreerd bij Getronics PinkRoccade, met gebruikmaking van het daartoe bestemd formulier.
- Is een Certificaatbeheerder eenmaal geïdentificeerd en geregistreerd, dan kunnen daarna alle Servercertificaten resulterende uit aanvragen gedaan voor diezelfde Certificaatbeheerder per mail aan de betreffende Certificaatbeheerder worden verstuurd.
- De Certificaatbeheerder maakt in de Veilige Omgeving van de Abonnee het sleutelpaar aan en stuurt de Private Sleutel, samen met een Certificate Signing Request (CSR-nummer), naar Getronics PinkRoccade.
- De Certificaatbeheerder bedenkt een intrekkingscode en registreert deze bij Getronics PinkRoccade.

4.2 Uitgifte van Certificaten

4.2.1 Uitgifte van Persoonlijke Certificaten en Groepscertificaten

Indien identificatie van de Certificaathouder conform artikel 4.1.1 slaagt, gaat Getronics PinkRoccade over tot uitgifte van het Certificaat. De Certificaathouder of Certificaatbeheerder tekent voor ontvangst, waarbij datum en tijdstip van uitgifte worden geregistreerd. Getronics PinkRoccade neemt het Certificaat vervolgens op in de Directory Dienst en stuurt de toegangscodes tot de SSCD en de intrekkingscodes in een zogenaamde PIN-mail aan de Certificaathouder (of Certificaatbeheerder). Tenslotte bevestigt Getronics PinkRoccade de uitgifte aan de Abonnee, in welke bevestiging ook de intrekkingscode staat vermeld.

4.2.2 Uitgifte van Servercertificaten

Bij aanvragen door reeds geregistreerde Certificaatbeheerders verstuurt Getronics PinkRoccade de aangemaakte Certificaten per mail naar het adres van de Certificaatbeheerder. De Certificaatbeheerder dient de ontvangst van de Certificaten per omgaande te bevestigen door invulling en ondertekening van de daartoe meegestuurde ontvangstbevestiging.

Getronics PinkRoccade bewaakt de retournering van de bevestigingen. Is na drie weken geen bevestiging retour ontvangen, dan verstuurt Getronics PinkRoccade een herinnering aan de Certificaatbeheerder en de Abonnee. Is na zes weken geen bevestiging retour ontvangen, dan trekt Getronics PinkRoccade de Certificaten zonder nadere aankondiging in. De met de uitgifte gepaarde kosten van de zijde van Getronics PinkRoccade komen alsdan voor rekening van de Abonnee.

4.3 Acceptatie van Certificaten

4.3.1 Acceptatie van Persoonlijke Certificaten en Groepscertificaten

Het Persoonlijke Certificaat of Groepscertificaat wordt geacht te zijn uitgereikt en geaccepteerd zodra de Certificaathouder of Certificaatbeheerder ze heeft ontvangen en de ontvangst heeft bevestigd.

4.3.2 Acceptatie van Servercertificaten

Het Servercertificaat wordt geacht te zijn uitgereikt en geaccepteerd zodra de Certificaatbeheerder het verkregen Servercertificaat in gebruik neemt.

4.4 Intrekking van Certificaten

Getronics PinkRoccade zorgt ervoor dat datum en tijdstip van intrekking van Certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door Getronics PinkRoccade vastgestelde tijdstip als moment van intrekking.

Als een Certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

4.4.1 Omstandigheden die leiden tot intrekking

In de volgende gevallen is de Abonnee en/of de Certificaathouder gehouden per direct en zonder vertraging een verzoek om intrekking van het Certificaat in te dienen bij Getronics PinkRoccade:

- Verlies, diefstal of compromittering van het Certificaat, de SSCD, de SUD, de PIN-code en/of PUK-code;
- Onjuistheden in de inhoud van het Certificaat;
- Wijziging van de in het Certificaat vermelde gegevens (naam, email, etc)
- Wijziging van de voor de betrouwbaarheid van het Certificaat noodzakelijke gegevens, bijvoorbeeld de beëindiging van het dienstverband of beroepsuitoefening;
- Overlijden van de Certificaathouder;
- Beëindiging van de organisatorische eenheid (bij Groepscertificaten);
- Ontbinding of faillissement van de rechtspersoon van Abonnee (indien van toepassing)

Certificaten kunnen door Getronics PinkRoccade zonder nadere tussenkomst worden ingetrokken indien de Abonnee, de Certificaathouder en/of de Certificaatbeheerder zich niet houdt aan de verplichtingen in de Algemene Voorwaarden. De beweegreden voor elke door Getronics PinkRoccade zelfstandig uitgevoerde intrekking wordt door haar geregistreerd.

4.4.2 Wie een verzoek tot intrekking mag doen

Getronics PinkRoccade zal een Certificaat intrekken na een verzoek daartoe van de Abonnee, de Certificaathouder of de Certificaatbeheerder.

Een Vertrouwende Partij kan geen verzoek tot intrekking doen, maar kan wel melding maken van het vermoeden van een omstandigheid die aanleiding kan zijn tot het intrekken van een Certificaat. Getronics PinkRoccade zal zo'n melding onderzoeken en zal, als daar aanleiding toe is, het Certificaat intrekken.

4.4.3 Procedure voor een verzoek tot intrekking

De melding van een verzoek tot intrekking, danwel van een omstandigheid die kan leiden tot de intrekking van een Certificaat, kan geschieden langs de volgende wegen:

Schriftelijk:	Getronics PinkRoccade Nederland B.V. t.a.v. PKIoverheid BSS Validatie Postbus 9105 7300 HN Apeldoorn
Fax:	+31 55 577 8460
Elektronisch:	pkivalidation@getronics.com (e-mail) https://www.pki.getronicspinkroccade.nl/pkioverheid/intrekking (WWW)

Nadrukkelijk wordt erop gewezen dat, in geval met de intrekking een spoedeisend belang gediend is, dit via de online intrekkingspagina's dient te geschieden. Deze vorm van intrekking is zeven dagen per week vierentwintig uur per dag beschikbaar, waarbij intrekking in beginsel steeds plaatsvindt binnen vier uur na ontvangst van het verzoek daartoe. Verzoeken om

intrekkingen per fax en e-mail worden pas op zijn vroegst de volgende werkdag na ontvangst in behandeling genomen en worden niet gegarandeerd binnen vier uur na ontvangst verwerkt.

4.4.4 Opschorting

Opschorting van Certificaten ('suspension') wordt niet ondersteund door Getronics PinkRoccade.

4.4.5 CRL-uitgifte frequentie

De CRL-uitgifte frequentie is vier uur, een CRL heeft een geldigheidsduur van vierentwintig uur.

Maximaal vier uur nadat een geautoriseerd online verzoek om intrekking is ontvangen, zal Getronics PinkRoccade het Certificaat intrekken en een nieuwe CRL uitgeven.

4.4.6 CRL-controlevoorwaarden

Vertrouwende Partijen zijn verplicht de actuele status (ingetrokken/niet ingetrokken) van een Certificaat te controleren door naslag van de CRL. Tevens zijn Vertrouwende Partijen gehouden om de Elektronische Handtekening waarmee de CRL is getekend, inclusief het bijbehorende certificatiepad, te controleren.

Ingetrokken Certificaten blijven op de CRL staan zolang hun oorspronkelijke geldigheidsdatum niet is verstreken. Nadien is de status van dat Certificaat voor vertrouwende partijen enkel nog online te verifiëren via de webdirectory van Getronics PinkRoccade of via OCSP.

4.4.7 Online intrekking/statuscontrole

De status van de uitgegeven Certificaten kan naast consultatie van de betreffende CRL tevens worden gecontroleerd via de OCSP service. De OCSP service geeft een realtime vermelding van de geldigheid van het Certificaat.

4.5 Procedures ten behoeve van beveiligingsaudits

4.5.1 Vastlegging van gebeurtenissen

Getronics PinkRoccade houdt voor audit-doeleinden overzichten bij van:

- Aanmaak van accounts;
- Installatie van nieuwe software of software updates;
- Datum en tijd en andere beschrijvende informatie betreffende backups;
- Datum en tijd van alle hardware wijzigingen;
- Datum en tijd van auditog dumps;
- Afsluiting en (her)start van systemen.

Getronics PinkRoccade houdt de volgende gebeurtenissen handmatig of automatisch bij:

- Levenscyclus gebeurtenissen ten aanzien van de CA sleutel, waaronder:
  - Genereren van sleutels, backup, opslag, herstel, archivering en vernietiging;
  - Levenscyclus gebeurtenissen ten aanzien van de cryptografische apparatuur.
- Levenscyclus gebeurtenissen ten aanzien van het beheer van Certificaten, waaronder:
  - Certificaataanvragen, heruitgifte en intrekking;
  - Geslaagde of niet-geslaagde verwerking van aanvragen;

- Genereren en het uitgeven van Certificaten en CRL's.
- Beveiligingsincidenten, waaronder:
  - Geslaagde en niet-geslaagde pogingen om toegang tot het systeem te verkrijgen
  - PKI en beveiligingsactiviteiten ondernomen door personeel;
  - Lezen, schrijven of verwijderen van beveiligingsgevoelige bestanden of records;
  - Veranderingen in het beveiligingsprofiel;
  - Systeem crashes, hardware uitval, en andere onregelmatigheden;

De onderdelen van de logs bevatten de volgende elementen:

- Datum en tijd;
- Volgnummer;
- Identiteit invoerder;
- Soort.

4.5.2 Bewaartermijn auditlog

De geconsolideerde auditlogs worden tijdens de geldigheidsduur van het Certificaat en bovendien gedurende een periode van ten minste zeven jaar na de datum waarop de geldigheid van het Certificaat is verlopen bewaard.

4.5.3 Bescherming van auditlog

Gebeurtenissen die op elektronische en handmatige wijze worden opgenomen in audit logfiles, worden door middel van een passende combinatie van verschillende soorten beveiligingsmaatregelen beschermd tegen niet-geautoriseerde inzage, wijziging, verwijdering of andere ongewenste aanpassingen.

4.5.4 Auditlog backup procedure

Incrementele backups van audit logs worden op dagelijkse basis gecreëerd, volledige backups worden op wekelijkse basis uitgevoerd en worden ook gearchiveerd op een externe locatie.

4.6 Archivering van documenten

4.6.1 Vastlegging van gebeurtenissen

Getronics PinkRoccade legt alle relevante registratieinformatie vast, waaronder tenminste:

- Soort identiteitsdocument dat door de Certificaathouder of Certificaatbeheerder is getoond;
- Bestand met uniek identificerende data, nummers of een combinatie daarvan (bijvoorbeeld het paspoortnummer) van identiteitsdocumenten, indien van toepassing;
- Opslaglocatie van kopieën van aanvragen en identiteitsdocumenten;
- Identiteit van degene die de aanvraag heeft goedgekeurd;
- Methode om identiteitsdocumenten te valideren.

4.6.2 Bewaartermijn archief

Getronics PinkRoccade bewaart alle relevante documentatie en informatie van een Certificaat tijdens de geldigheidsduur daarvan, alsmede gedurende een periode van tenminste zeven jaar na de datum waarop de geldigheidsduur van het Certificaat is verlopen.

4.6.3 Bescherming van archieven

Getronics PinkRoccade zorgt voor de integriteit en toegankelijkheid van de gearchiveerde gegevens. Alle noodzakelijke apparatuur en programmatuur voor het ontsluiten van de informatie wordt gedurende dezelfde periode bewaard. Getronics PinkRoccade zorgt voor een zorgvuldige en beveiligde wijze van opslag en archivering.

4.6.4 Archief backup procedure

Geen nadere bepalingen.

4.6.5 Voorwaarden aan tijdsaanduiding van vastgelegde gebeurtenissen

Geen nadere bepalingen.

4.7 Vernieuwen van sleutels

Sleutels van Certificaathouders zullen na het verstrijken van de geldigheidsduur of na het intrekken van de bijbehorende Certificaten niet opnieuw worden gebruikt.

Getronics PinkRoccade zal de Abonnee minimaal twee maanden voor het verstrijken van de geldigheidsduur van (alsdan niet ingetrokken) Certificaten informeren over de mogelijkheid tot vernieuwing van het sleutelpaar, mits van toepassing. Getronics PinkRoccade laat een dergelijke vernieuwing van sleutels altijd vooraf gaan door een controle of is voldaan aan de eisen die in paragraaf 3.1 zijn gesteld.

4.8 Aantasting en continuïteit

Getronics PinkRoccade heeft procedures geïmplementeerd om de gevolgen van eventuele calamiteiten zoveel mogelijk te minimaliseren.

Compromittering van de Private Sleutel van Getronics PinkRoccade wordt beschouwd als een calamiteit. Getronics PinkRoccade stelt Vertrouwende Partijen, Abonnees, Certificaathouders en Certificaatbeheerders zo spoedig mogelijk op de hoogte van de compromittering van de Private Sleutel van Getronics PinkRoccade door informatie daaromtrent te publiceren op haar website (https://www.pki.getronicspinkroccade.nl/pkioverheid). Daarnaast zal Getronics PinkRoccade aan Abonnees, Certificaathouders en Certificaatbeheerders een e-mailbericht sturen en de Overheids-Policy Authority onmiddellijk op de hoogte brengen.

4.9 CSP beëindiging

In geval Getronics PinkRoccade de certificatiedienstverlening beëindigt zal door haar het CA Termination Plan worden uitgevoerd. Alsdan zullen Abonnees, Certificaathouders en Certificaatbeheerders tenminste drie maanden van tevoren worden ingelicht. over de beëindiging en zal Getronics PinkRoccade per direct stoppen met het uitgeven van nieuwe Certificaten.

Getronics PinkRoccade zal waar redelijkerwijs mogelijk maatregelen nemen om schade te beperken die voor Abonnees en Certificaathouders kan ontstaan vanwege de beëindiging van de dienstverlening. Alsdan zal Getronics PinkRoccade aangeven welke voorzieningen zijn

getroffen met betrekking tot de overdracht van de verplichtingen aan andere Certificatiedienstverleners, inzoverre dit redelijkerwijs mogelijk is.

Getronics PinkRoccade zorgt ervoor dat het bewijs van certificatie, nodig om in rechte bewijs te kunnen leveren, blijft bestaan. Tevens zal de revocation status service (inclusief de CRL's) tenminste in stand worden gehouden totdat de geldigheidsduur van het laatste uitgegeven Certificaat verlopen is. Zodra dit het geval is, zal Getronics PinkRoccade alle ten behoeve van de onderhavige dienstverlening door haar gebruikte Private Sleutels vernietigen of permanent buiten werking stellen.

5 Fysieke, procedurele en personele beveiliging

5.1 Fysieke beveiliging

5.1.1 Fysieke beveiliging Getronics PinkRoccade

De onderhavige dienstverlening wordt beheerd in en geleverd vanuit een streng beveiligde omgeving binnen het rekencentrum van Getronics PinkRoccade in Apeldoorn. Deze omgeving voldoet aan de voor de overheid in deze geldende wet- en regelgeving, waaronder onder meer begrepen de Wet Bescherming Staatsgeheimen 1951.

De fysieke toegang tot de beveiligde omgeving wordt gerealiseerd door een combinatie van procedurele en (bouw)technische maatregelen. Toegang tot het gebouw en de beveiligde omgeving wordt bewaakt middels elektronische (biometrische) en visuele middelen. Het toegangssysteem van het gebouw registreert het in- en uitgaan van personeel en bezoekers. Het gebouw wordt 7*24 uur bewaakt door eigen beveiligingsbeambten.

De beveiligingssystemen signaleren automatisch pogingen tot (on)geautoriseerde toegang. De technische maatregelen worden ondersteund door verschillende procedures, onder andere door bewegingssensoren die personen en materialen (voor cryptografisch sleutelbeheer) monitoren. De technische infrastructuur inclusief de beveiligingssystemen bevindt zich in beschermde ruimten met een daarvoor benoemde beheerder. Toegang tot deze ruimten wordt geregistreerd voor audit-doeleinden.

Huishoudelijke regels zijn van kracht voor het registreren en begeleiden van bezoekers en servicepersoneel van derden. Met servicebedrijven zijn afspraken gemaakt voor toegang tot bepaalde ruimten. Daarnaast controleert de gebouwbeheerdienst de in- en uitgaande goederen (op basis van geleidedocumenten).

De beveiligde omgeving van Getronics PinkRoccade biedt standaard tot minimaal vijf fysieke barrières tot aan de productieomgeving. Voor niet-produktie (offline) opslag van bijvoorbeeld cryptografische hardware en materiaal gelden zes niveaus.

Het oneigenlijke verkrijgen van toegang tot de beveiligde omgeving vereist het compromitteren van meerdere systemen. Afhankelijk van de ruimte kan dit een combinatie zijn van kennis, SSCD, biometrische data, begeleiding bij toegang en visuele inspectie. Additionele maatregelen zijn onder andere inbraakdetectie en videoopnames. De verschillende toegangscontrolesystemen zijn van elkaar gescheiden en bewaken de toegang tot de beveiligde omgeving. Functiescheiding in combinatie met vijf of zes fysieke barrières zorgen ervoor dat niet één individu toegang kan krijgen tot kritische apparatuur van Getronics PinkRoccade.

Getronics PinkRoccade heeft tal van maatregelen getroffen om noodsituaties in de beveiligde omgeving te voorkomen en/of schade te beperken. Voorbeelden daarvan zijn:

- Bliksemafleiding;
- Volcontinue eigen energie voorziening;
- Bouwkundige maatregelen (brandresistentie, waterafvoer, etc.);
- Brandpreventie door middel van automatisch brandalarm.

De maatregelen worden op reguliere basis getest. In geval van uitzonderingssituaties treedt een escalatieplan in werking. Politie en brandweer zijn bekend met de specifieke situatie met betrekking tot de beveiligde omgeving van Getronics PinkRoccade.

5.1.2 Fysieke beveiliging Certificaathouders

Geen nadere bepalingen indien sprake is van Persoonlijke Certificaten of Groepscertificaten.

Indien sprake is van een Servercertificaat, dan geldt dat deze in een Veilige Omgeving moet zijn ondergebracht. Zie hiervoor het gestelde onder paragraaf 2.1.2 (Verplichtingen Abonnee).

5.2 Procedurele beveiliging

- Getronics PinkRoccade draagt zorg voor procedurele beveiliging door de toepassing van ITIL management processen. ITIL is een methodologie voor het standaardiseren van IT beheerprocessen met als doel de kwaliteit van deze processen op een vastgesteld niveau te brengen en te houden.

5.2.1 Vertrouwelijke functies

Personeel met toegang tot cryptografisch materiaal, of personen die daarbij een rol spelen, hebben een functie die als vertrouwelijk wordt gekwalificeerd. Zij hebben in het verleden en zolang dat mogelijk was een AIVD-B-screening ondergaan, uitgevoerd door de (toenmalige) Binnenlandse Veiligheidsdienst (nu AIVD). Overig bij de certificatiedienstverlening betrokken personeel is tenminste voorzien van een Verklaring omtrent het Gedrag, conform de Wet Justitiële Informatie.

5.2.2 Aantal personen benodigd per taak

Geen nadere bepalingen.

5.2.3 Identificatie en authenticatie met betrekking tot CSP-functies

Geen nadere bepalingen.

5.2.4 Beheer en beveiliging

Getronics PinkRoccade heeft gescheiden systemen voor tests, acceptatie en productie. Deze systemen worden beheerd met gebruikmaking van ITIL procedures.

Het overbrengen van programmatuur van de ene omgeving naar de andere vindt gecontroleerd plaats, met gebruikmaking van de procedure voor change management. Deze procedure omvat onder andere het bijhouden en vastleggen van versies, wijzigingen en noodreparaties van alle operationele software.

De integriteit van alle systemen en informatie gebruikt voor PKIoverheid Certificaten wordt beschermd tegen virussen, schadelijke software en andere mogelijke verstoringen van de dienstverlening door middel van een passende combinatie van fysieke, logische en organisatorische maatregelen. Deze maatregelen zijn preventief, repressief en correctief van aard. Voorbeelden van getroffen maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen.

Opslagmedia van systemen die worden gebruikt voor PKIoverheid Certificaten, worden op een veilig manier behandeld om ze te beschermen tegen schade, diefstal en niet-geautoriseerde toegang. Opslagmedia worden zorgvuldig verwijderd wanneer zij niet langer nodig zijn.

Getronics PinkRoccade heeft erin voorzien dat er tijdige en gecoördineerde wijze actie wordt ondernomen om snel te reageren op incidenten en om de invloed van inbreuk op de beveiliging te beperken. Alle incidenten worden zo snel mogelijk gemeld nadat zij zich hebben voorgedaan.

Incidenten van een tevoren door de Overheids-Policy Authority bepaalde categorie worden door Getronics PinkRoccade aan hen gerapporteerd.

5.3 Personele beveiligingsmiddelen

Alle bij de dienstverlening van Getronics PinkRoccade betrokken medewerkers bezitten ruime kennis en ervaring op gebied van certificatiedienstverlening, inclusief kennis van de wijze waarop de echtheidskenmerken worden gecontroleerd van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten.

Pre-employment screening en ‘Verklaring omtrent het gedrag’ conform Wet justitiële gegevens zijn onderdeel van het antecedentenonderzoek. Al het personeel dat direct is betrokken bij de operationele uitvoering van de onderhavige dienstverlening, is gescreend op het aanwezig zijn van tegengestelde belangen die de onpartijdigheid van de activiteiten van Getronics PinkRoccade zouden kunnen beïnvloeden.

Getronics PinkRoccade hanteert functiescheiding tussen uitvoerende, beslissende en controlerende taken. Daarnaast is er sprake van functiescheiding tussen systeembeheer en bediening van de systemen gebruikt voor PKIoverheid Certificaten, alsmede tussen Security Officer(s), Systeem auditor(s), systeembeheerder(s) en operator(s).

Beveiligingstaken en –verantwoordelijkheden, waaronder vertrouwelijke functies, zijn gedocumenteerd in functieomschrijvingen. Deze zijn opgesteld op basis van de scheiding van taken en bevoegdheden en waarin de gevoeligheid van de functie is vastgesteld. Waar dat van toepassing is, is in de functieomschrijvingen onderscheid gemaakt tussen algemene functies en specifieke CSP-functies.

Personeel werkzaam voor Getronics PinkRoccade (zowel tijdelijk als vast) is onderwerp van antecedentenonderzoek, training en bewustwording voor de uitvoering van hun taak. Autorisatie van het CSP personeel vindt in beperkte mate plaats op basis van het ‘need-to-know’ principe.

Voor alle vertrouwelijke en administratieve taken, die invloed hebben op de levering van certificatiediensten, zijn procedures opgesteld en geïmplementeerd.

5.3.1 Vakkennis, ervaring en kwalificaties

Voor de levering van PKIoverheid Certificaten zet Getronics PinkRoccade personeel in dat beschikt over voldoende vakkennis, ervaring en kwalificaties. Voor bepaalde functies is het volgen van specifieke trainingen verplicht.

Het voor de onderhavige dienstverlening verantwoordelijk management participeert actief in de bewaking en bevordering van de kwaliteit en betrouwbaarheid van de PKIoverheid Certificaten.

5.3.2 Antecedentenonderzoek

Zie 5.2.1 voor screening en antecedentenonderzoek.

Getronics PinkRoccade conformeert zich aan bepaling art. 2, lid in, sub s van het Besluit Elektronische Handtekening omtrent het benoemen van personen. Personeel betrokken bij PKIoverheid Certificaten zal niet worden benoemd voordat de noodzakelijke onderzoeken zijn afgerond.

5.3.3 Trainingseisen

Geen nadere bepalingen.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

Bij het genereren van sleutelparen maakt Getronics PinkRoccade gebruik van veilige middelen en betrouwbare systemen. Getronics PinkRoccade zorgt ervoor dat de betrouwbaarheid en de veiligheid van de systemen in ieder geval voldoen aan internationaal erkende standaards.

Het genereren van de sleutels geschiedt in apparatuur dat voldoet aan EAL 4+ of hoger in overeenstemming met ISO 15408 (‘Cryptographic module for CSP Signing Operations’).

Alle Certificaten, met uitzondering van Servercertificaten, worden in een SSCD gegenereerd. Op de SSCD kunnen meerdere Certificaten worden opgeslagen. Voor de Servercertificaten geldt dienaangaande het gestelde onder paragraaf 2.1.2 Verplichtingen Abonnee.

6.1.1 Genereren van sleutelparen

Bij het genereren van sleutelparen maakt Getronics PinkRoccade gebruik van betrouwbare procedures die worden uitgevoerd binnen een beveiligde omgeving die voldoet aan objectieve en internationaal erkende standaards.

De sleutelgeneratie van de voor PKIoverheid Certificaten gebruikte CA’s van Getronics PinkRoccade heeft plaatsgevonden in een EAL4+ gecertificeerde Hardware Security Module. Hierbij is gebruikt gemaakt van het signature algoritme ‘SHA1RSA’. De sleutels van de sleutelparen zijn 2048 bits asymmetrisch RSA en het gebruikte hashing algoritme is ‘SHA1’.

De sleutelgeneratie voor Persoonlijke Certificaten vindt plaats in SSCD’s. Hierbij wordt gebruik gemaakt van het signature algoritme ‘SHA1RSA’. De sleutels van de sleutelparen zijn 1024 bits of hoger asymmetrisch RSA en het gebruikte hashing algoritme is ‘SHA1’.

6.1.2 Overdracht van private sleutel en SSCD/SUD aan Certificaathouder

Persoonlijke Certificaten of Groepscertificaten worden op twee manieren overgedragen aan de Certificaathouder:

1) Overhandiging van de SSCD of SUD via een commercieel postbedrijf, waarbij de benodigde PIN voor de SSCD of SUD gescheiden wordt verstrekt aan de Certificaathouder (‘out of band’); of,
2) Persoonlijk overhandiging van de SSCD of SUD aan de Certificaathouder, inclusief overhandiging van de PIN behorende bij de SSCD of SUD.

Servercertificaten worden op een geschikt opslagmedium (bijvoorbeeld een CD) persoonlijk overhandigd aan de Certificaathouder. De Private Sleutel behorende bij het Servercertificaat wordt gegenereerd in de Veilige Omgeving van de Abonnee of de Certificaathouder en hoeft derhalve niet te worden overgedragen door Getronics PinkRoccade. Zie hiervoor het gestelde onder paragraaf 2.1.2 (Verplichtingen Abonnee).

6.1.3 Overdracht van de publieke sleutel van CSP aan Vertrouwende Partijen

De Publieke Sleutels van Getronics PinkRoccade gebruikt voor PKIoverheid Certificaten worden aan Vertrouwende Partijen beschikbaar gesteld via de speciaal hiertoe ingerichte website van Getronics PinkRoccade (https://www.pki.getronicspinkroccade.nl/pkioverheid).

6.1.4 Sleutellengten

De sleutellengte van een Certificaat is minstens 1024 bits RSA. De sleutellengte van een CA-Certificaat is 2048 bits RSA.

6.1.5 Genereren van sleutels in hardware/software

Getronics PinkRoccade genereert sleutels in SSCD's of HSM's die voldoen aan de EAL 4+ normering.

6.1.6 Doelen van sleutelgebruik (zoals bedoeld in X.509v3)

De Certificaten, inclusief de daarbij behorende sleutelparen, zijn uitsluitend bedoeld voor de doeleinden die beschreven zijn in deze CPS en die zijn opgenomen in (de extensies van) het Certificaat.

6.2 Bescherming van de Private Sleutel

6.2.1 Standaarden voor cryptografische module

Voor operationeel gebruik worden de cryptografische gegevens opgeslagen in een Hardware Security Module (HSM). De HSM is EAL4+ gecertificeerd..

6.2.2 Controle op Private Sleutel door meerdere personen

De Private Sleutels van bijbehorende bij de CA-Certificaten van Getronics PinkRoccade zijn niet in één stuk leesbaar.

6.2.3 Escrow van Private Sleutels

Standaard vindt er geen escrow van Private Sleutels plaats. Desgewenst kan een Abonnee een verzoek indienen tot escrow van Private Sleutels van Certificaten voor vertrouwelijkheid. Er is geen mogelijkheid tot escrow van Private Sleutels gerelateerd aan Certificaten voor onweerlegbaarheid en identificatie.

6.2.4 Backup van Private Sleutels

Er wordt een backup gemaakt van de Private Sleutels behorende bij de CA-Certificaten van Getronics PinkRoccade. De backup wordt in versleutelde vorm bewaard in cryptografische modules en bijbehorende opslagapparatuur.

Van de Private Sleutels behorende bij Certificaten wordt in beginsel geen backup gemaakt, tenzij de Abonnee daartoe nadrukkelijk heeft verzocht voor wat betreft vertrouwelijkheidscertificaten. Indien een Private Sleutel van een vertrouwelijkheidscertificaat geen backup is gemaakt, zal verlies, vernietiging of het anderszins onbruikbaar raken van de Private Sleutel tot gevolg hebben dat de hiermee versleutelde gegevens definitief niet meer te ontsleutelen zijn.

6.2.5 Archivering van Private Sleutels

Private Sleutels van Certificaten voor onweerlegbaarheid en authenticiteit worden niet gearchiveerd, behoudens in gevallen onder 6.2.3 bepaald.

6.2.6 Toegang tot Private Sleutels in cryptografische module

Voor de Private Sleutels behorende bij CA-Certificaten van Getronics PinkRoccade, die zijn opgeslagen in een cryptografische hardware module, wordt toegangsbeveiliging gebruikt die garandeert dat de sleutels niet buiten de module kunnen worden gebruikt.

6.2.7 Activering van de Private Sleutels van Getronics PinkRoccade

Door middel van een sleutelceremonie, ten overstaan van de daarvoor noodzakelijk aanwezige functionarissen, worden de Private Sleutels behorende bij CA-Certificaten van Getronics PinkRoccade geactiveerd.

6.2.8 Deactivering van de Private Sleutels van Getronics PinkRoccade en Certificaathouders

Onder omstandigheden kan Getronics PinkRoccade bepalen dat de Private Sleutels worden gedeactiveerd, met inachtneming van de daarop van toepassing zijnde waarborgen ten behoeve van zorgvuldigheid.

Indien een SSCD of SUD door de Certificaathouder wordt verloren en door een vinder wordt geretourneerd aan Getronics PinkRoccade, zal deze SSCD of SUD door haar worden vernietigd, inclusief de daarin opgenomen Private Sleutels. Alsdan zal Getronics PinkRoccade tevens controleren of de bijbehorende Certificaten zijn ingetrokken en zoniet, dan zal ze daar per direct toe overgaan.

6.2.9 Methode voor het vernietigen van Private Sleutels

De Private Sleutels waarmee Certificaten worden ondertekend, kunnen na het einde van hun levenscyclus niet meer kunnen worden gebruikt. Getronics PinkRoccade zorgt voor een adequate vernietiging waarbij wordt voorkomen dat het mogelijk is de vernietigde sleutels te herleiden uit de restanten.

6.3 Andere aspecten van sleutelaarmanagement

Alle aspecten van sleutelaarmanagement worden door Getronics PinkRoccade uitgevoerd met inachtneming van zorgvuldige procedures die in overeenstemming zijn met het beoogde doel.

6.3.1 Archiveren van publieke sleutels

Publieke sleutels worden gearchiveerd door Getronics PinkRoccade voor tenminste zeven jaar na het verstrijken van de oorspronkelijke geldigheidsduur van een Certificaat. Archivering zal plaatsvinden in een fysiek beveiligde omgeving.

6.3.2 Gebruiksduur voor Publieke en Private Sleutels

Voor het CA-Certificaat, inclusief het bijbehorende sleutelpaar, wordt een maximale geldigheidsduur van zes jaar na de uitgiftedatum gehanteerd.

Voor het Certificaat, inclusief het bijbehorende sleutelpaar, wordt een maximale geldigheidsduur van drie jaar na de uitgiftedatum gehanteerd.

6.4 Activeringsgegevens

6.4.1 Genereren en installeren van activeringsgegevens

De toepassing van activeringsgegevens is verbonden aan het gebruik van een SSCD of SUD. Deze gegevens worden op veilige wijze voorbereid en gedistribueerd (gescheiden van de SSCD of SUD).

Ten behoeve van de activering van de SSCD of SUD wordt gebruik gemaakt van zowel een PIN-code als een PUK-code, welke steeds uit tenminste vijf tekens bestaan.

6.4.2 Bescherming activeringsgegevens

Activeringsgegevens (PIN-code en PUK-code) worden zodanig overgedragen aan de Certificaathouder dat het voor derden niet mogelijk is kennis te nemen van de activeringsgegevens. Na overdracht van de activeringsgegevens is de Certificaathouder exclusief verantwoordelijk voor de bescherming daarvan.

Indien de PIN-code driemaal onjuist is ingevoerd, wordt de SSCD of SUD automatisch geblokkeerd. Alsdan kan SSCD of SUD enkel worden gedeblokkeerd met de PUK-code.

Indien de PUK-code driemaal onjuist wordt ingevoerd, is de SSCD of SUD definitief geblokkeerd en daardoor onbruikbaar geworden.

6.5 Logische toegangsbeveiliging van computers Getronics PinkRoccade

6.5.1 Specifieke technische vereisten aan computerbeveiliging

Getronics PinkRoccade beveiligt op passende wijze de voor PKIoverheid Certificaten gebruikte computersystemen tegen ongeautoriseerde toegang en andere bedreigingen.

6.5.2 Beheer en classificatie van middelen

Getronics PinkRoccade classificeert op basis van een risicoanalyse de gebruikte middelen.

6.6 Beheersmaatregelen technische levenscyclus

Bij het gebruik van technische middelen hanteert Getronics PinkRoccade procedures die in ieder geval garanderen dat de veiligheid en betrouwbaarheid van systemen gewaarborgd is, hetgeen op objectieve wijze via een audit wordt vastgesteld.

6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling

Geen nadere bepaling, aangezien Getronics PinkRoccade geen systeemontwikkeling uitvoert.

6.6.2 Management van maatregelen ten behoeve van beveiliging

Geen nadere bepaling.

6.6.3 Levenscyclus beveiligingsclassificatie

Getronics PinkRoccade beoordeelt (jaarlijks) de classificatie van informatie periodiek en past zonodig de classificatie aan.

6.6.4 Levenscyclus cryptografische hardware voor het ondertekenen van Certificaten

De CA-Certificaten zijn gegenereerd en opgeslagen in Hardware Security Modules (HSM) die EAL4+ gecertificeerd zijn. De HSM's worden door de leverancier aangeleverd in tamper evident bags, zijnde een verpakking die elke vorm van corruptie daarvan toonbaar maken. Elke zending wordt direct na binnenkomst gecontroleerd op eventuele compromittering aan de hand van de bijbehorende out-of-band list.

Getronics PinkRoccade hanteert Key Management procedures voor het installeren, het activeren, backup en herstel van de Private Sleutels behorende bij de CA-Certificaten van Getronics PinkRoccade. Deze acties worden door tenminste twee werknemers gelijktijdig uitgevoerd. De Private Sleutels worden vernietigd op het moment dat ze buiten gebruik worden gesteld.

6.6.5 Levenscyclus cryptografische software van de CSP

Zie 5.2.4 Beheer en beveiliging.

6.7 Netwerkbeveiliging

Getronics PinkRoccade neemt maatregelen om de stabiliteit, de betrouwbaarheid en de veiligheid van het netwerk te waarborgen. Dit omvat bijvoorbeeld maatregelen om gegevensverkeer te reguleren en ongewenst gegevensverkeer onmogelijk te maken, alsmede de plaatsing van firewalls om de integriteit en exclusiviteit van het netwerk te garanderen.

6.8 Beheersmaatregelen cryptografische module engineering

Bij de ontwikkeling en het gebruik van cryptografische onderdelen zorgt Getronics PinkRoccade ervoor dat deze onderdelen voldoen aan alle eisen die kunnen worden gesteld op het gebied van beveiliging, betrouwbaarheid, toepassingsbereik en beperking van de storingsgevoeligheid. Ter beoordeling van de toepasselijke procedures kan worden uitgegaan van internationaal erkende standaards.

7 Certificaatprofielen en CRL

7.1 Certificaatprofielen

De PKIoverheid Certificaten zijn opgebouwd volgens de PKIX X.509 v3 standaard, waarbij de mogelijkheid bestaat dat extensies worden gebruikt.

Certificaten voor onweerlegbaarheid worden opgebouwd volgens het Qualified Certificate Profile van EESSI/ETSI. Eventuele extensies in dat kader worden ook in de overige Certificaten opgenomen.

Certificaatprofielen zijn opgemaakt volgens Deel 3 van het Programma van Eisen van de PKI voor de Overheid, conform het profiel van het Certificaat voor het Domein Overheid en Bedrijven.

7.1.1 Persoonlijk Certificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek serienummer
Signature	Het gebruikte algoritme is sha-1 WithRSAEncryption
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA certificaten in omloop voorzien van de volgende kenmerken; • De OrganizationName is ingesteld op ‘PinkRoccade Infrastructure Services BV’. De CommonName bevat ‘PinkRoccade CSP - Overheid – ‘ en de aanduiding ‘Onweerlegbaarheid CA’ of ‘Vertrouwelijkheid CA’ of ‘Authenticiteit CA’, afhankelijk van het type certificaat. De CountryName is ingesteld op ‘NL’. • De OrganizationName is ingesteld op ‘Getronics PinkRoccade Nederland B.V.’. De CommonName is ingesteld op ‘Getronics PinkRoccade PKIoverheid CA – Overheid en Bedrijven’. De CountryName is ingesteld op ‘NL’.
Validity	De geldigheidsperiode van het Certificaat is ingesteld op 3 of 5 jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: CountryName, CommonName, OrganizationName en

	SerialNumber. De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. Het CountryName attribuut is ingesteld op de tweeletterige landcode “NL” volgens ISO 3166.
subjectPublicKeyInfo	Bevat de PublicKey van de Subject

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
KeyUsage	Ja	In authenticiteitcertificaten is het digitalSignature bit opgenomen. In vertrouwelijkheidcertificaten zijn de keyEncipherment, dataEncipherment en de keyAgreement bits opgenomen. In Certificaten voor de Elektronische Handtekening is het non-Repudiation bit op unieke wijze zijn opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op ‘False’ en pathLenConstraint op ‘none’
CertificatePolicies	Nee	Certificaten voor authenticiteit bevatten het OID voor de CP Domein Overheid en Bedrjiven Authenticiteit (2.16.528.1.1003.1.2.2.1). Certificaten voor onweerlegbaarheid bevatten het OID voor de CP Domein Overheid en Bedrijven Onweerlegbaarheid (2.16.528.1.1003.1.2.2.2). Certificaten voor vertrouwelijkheid bevatten het OID voor de CP Domein Overheid en Bedrijven Vertrouwelijkheid (2.16.528.1.1003.1.2.2.3). Alle typen Certificaten bevatten en link naar de CPS PKIoverheid en een gebruikerstekst.
SubjectAltName	Nee	Hierin is het e-mail adres van de Subject, het OID van de betreffende CA • PinkRoccade CSP CA behorend bij het type Certificaat; - authenticiteit 2.16.528.1.1003.1.3.2.2.1, - onweerlegbaarheid 2.16.528.1.1003.1.3.2.2.2, - vertrouwelijkheid 2.16.528.1.1003.1.3.2.2.3 • of de Getronics PinkRoccade PKIoverheid CA – Overheid en Bedrijven CA; 2.16.528.1.1003.1.3.2.2.5 en het Subjectserienummer van de Certificaathouder opgenomen. Certificaten voor authenticiteit kunnen tevens een UPN bevatten ten behoeve van Windows Smartcard Logon bevatten.
CrlDistributionPoints	Nee	Bevat de URI waarde waar de CRL, die behoort bij het

		type Certificaat, kan worden opgehaald.
ExtendedKeyUsage	Nee	Certificaten voor authenticiteit kunnen deze extensie bevatten, dit maakt het mogelijk om het Certificaat onder andere voor Windows Smartcard Logon te gebruiken.
AuthorityInfoAccess	Nee	Bevat de URI waarde waar de OCSP responder, die behoort bij het type Certificaat, waar real-time status informatie over het betreffende certificaat kan worden opgevraagd.

Private extensies

Veld	Essentieel	Waarde
QCStatements	Nee	Certificaten voor onweerlegbaarheid bevatten de indicatie dat deze zijn uitgegeven in overeenstemming met de Europese Richtlijn 99/93/EG.

7.1.2 Servercertificaten en Groepscertificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek Certificaatnummer
Signature	Het gebruikte algoritme is sha-1 WithRSAEncryption
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA behorend bij het type Certificaat en wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA certificaten in omloop voorzien van de volgende kenmerken; • De OrganizationName is ingesteld op ‘PinkRoccade Infrastructure Services BV’. De CommonName bevat ‘PinkRoccade CSP - Overheid – Services CA’. De CountryName is ingesteld op ‘NL’. • De OrganizationName is ingesteld op ‘Getronics PinkRoccade Nederland B.V.’. De CommonName is ingesteld op ‘Getronics PinkRoccade PKIoverheid CA – Overheid en Bedrijven’. De CountryName is ingesteld op ‘NL’.
Validity	De geldigheidsperiode van het Services Certificaat is ingesteld op 3 of 5 jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: CountryName, CommonName en OrganizationName. Optioneel kunnen tevens de attributen OrganizationUnit, State en

	Locality worden gebruikt. De CommonName bevat de naam van de Service, dit kan bijvoorbeeld een DNS- of een groepsnaam zijn. De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. Het CountryName attribuut is ingesteld op de tweeletterige landcode “NL” volgens ISO 3166.
subjectPublicKeyInfo	Bevat de PublicKey van de Subject

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
KeyUsage	Ja	In certificaten voor authenticiteit is het digitalSignature bit opgenomen. In certificaten voor vertrouwelijkheid zijn de keyEncipherment, dataEncipherment en de keyAgreement bits opgenomen. In servercertificaten zijn de digitalSignature- en Key Encipherment bits op unieke wijze opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op ‘False’ en pathLenConstraint op ‘none’
CertificatePolicies	Nee	Certificaten voor authenticiteit bevatten het OID voor de CP Services Bijlage bij CP Domein Overheid en Bedrijven Authenticiteit (2.16.528.1.1003.1.2.2.4). Certificaten voor vertrouwelijkheid van berichten bevatten het OID voor de CP Services Bijlage bij CP Domein Overheid en Bedrijven Vertrouwelijkheid (2.16.528.1.1003.1.2.2.5). Certificaten voor vertrouwelijkheid van server verbindingen bevatten het OID voor de CP Services Bijlage bij CP Domein Overheid en Bedrijven Server (2.16.528.1.1003.1.2.2.6). Alle typen certificaten bevatten een link naar de CPS PKIoverheid en een gebruikerstekst.
SubjectAltName	Nee	Hierin is het OID van de CA: • PinkRoccade CSP Services CA; 2.16.528.1.1003.1.3.2.2.4 • of de Getronics PinkRoccade PKIoverheid CA – Overheid en Bedrijven CA; 2.16.528.1.1003.1.3.2.2.5 en het Subjectnummer van de Certificaathouder opgenomen. Bij Certificaten voor vertrouwelijkheid en authenticiteit is tevens het e-mail adres van de Subject opgenomen.
CrlDistributionPoints	Nee	Bevat de URI waarde van de betreffende CRL, die behoort bij het type Certificaat, kan worden opgehaald.

ExtendedKeyUsage	Nee	Groepscertificaten kunnen deze extensie bevatten, dit maakt het mogelijk om het Certificaat onder andere voor Windows Smartcard Logon of Codesigning te gebruiken.
AuthorityInfoAccess	Nee	Bevat de URI waarde waar de OCSP responder, die behoort bij het type Certificaat, waar real-time status informatie over het betreffende certificaat kan worden opgevraagd.

7.2 CRL-profielen

De CRL (of meer recente statusinformatie) gebruikt voor de PKIoverheid Certificaten is aldus opgebouwd dat ze makkelijk onderwerp kan vormen voor validatieprocessen.

De inrichting van de CRL en het formaat van de CRL, alsmede het aan de CRL ten grondslag liggende principe, kunnen door Getronics PinkRoccade worden aangepast, zulks in overeenstemming met de belangen van betrokken partijen.

7.2.1 Persoonlijke Certificaten

Attributen

Veld	Waarde
Version	1 (X.509 versie 2)
signatureAlgorithm	sha-1 WithRSAEncryption
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA's in omloop voorzien van de volgende kenmerken; • De OrganizationName is ingesteld op 'PinkRoccade Infrastructure Services BV'. De CommonName bevat 'PinkRoccade CSP - Overheid – ' en de aanduiding 'Onweerlegbaarheid CA' of 'Vertrouwelijkheid CA' of 'Authenticiteit CA', afhankelijk van het type certificaat. De CountryName is ingesteld op 'NL'. • De OrganizationName is ingesteld op 'Getronics PinkRoccade Nederland B.V.'. De CommonName is ingesteld op 'Getronics PinkRoccade PKIoverheid CA – Overheid en Bedrijven'. De CountryName is ingesteld op 'NL'.
effective date	datum van uitgifte
next update	is datum van uitgifte plus 24 uur
revoked certificates	de ingetrokken Certificaten met certificaatserienummer en datum

	van intrekking en mogelijk reden van intrekking.

Extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	Bevat 160 bit SHA-1 hash

7.2.2 Server Certificaten en Groepscertificaten

Attributen

Veld	Waarde
Version	1 (X.509 versie 2)
signatureAlgorithm	sha-1 WithRSAEncryption
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA en wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA's in omloop voorzien van de volgende kenmerken; • De OrganizationName is ingesteld op 'PinkRoccade Infrastructure ServicesBV'. De CommonName bevat 'PinkRoccade CSP - Overheid – Services CA'. De CountryName is ingesteld op 'NL'. • De OrganizationName is ingesteld op 'Getronics PinkRoccade Nederland B.V.'. De CommonName is ingesteld op 'Getronics PinkRoccade PKIoverheid CA – Overheid en Bedrijven'. De CountryName is ingesteld op 'NL'.
effective date	datum van uitgifte
next update	is datum van uitgifte plus 24 uur, effectief wordt een nieuwe CRL 4 uur na de datum van uitgifte gegenereerd en gepubliceerd
revoked certificates	de ingetrokken Certificaten met certificaatserienummer en datum van intrekking en mogelijk reden van intrekking.

Extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	Bevat 160 bit SHA-1 hash

8 Specificatie van onderhoud op CPS

8.1 Wijzigingsprocedure CPS

Getronics PinkRoccade heeft het recht de CPS te wijzigen of aan te vullen. Wijzigingen worden op de website (https://www.pki.getronicspinkroccade.nl/pkioverheid) aangekondigd en gelden vanaf het moment dat de nieuwe CPS ingaat. De ingangsdatum is gesteld op twee weken na publicatie van wijziging, tenzij anders aangegeven bij publicatie.

De werking van de geldende CPS wordt ten minste jaarlijks beoordeeld door de Policy Management Authority (PMA) van Getronics PinkRoccade. Abonnees, Certificaathouders, Certificaatbeheerders en Vertrouwende Partijen kunnen opmerkingen plaatsen met betrekking tot de inhoud van de CPS en deze indienen bij het PMA van Getronics PinkRoccade (pkisupport@getronics.com). Indien op grond hiervan wordt vastgesteld dat wijzigingen in het CPS noodzakelijk zijn, zal het PMA deze wijzigingen conform het daartoe ingerichte proces voor change management doorvoeren.

Wijzigingen van de CPS worden vastgesteld door de PMA van Getronics PinkRoccade. Wijzigingen van redactionele aard of correcties van kennelijke schrijf- en/of spelfouten kunnen zonder voorafgaande bekendmaking in werking treden en zijn herkenbaar doordat het versienummer met 0.1 wordt opgehoogd (1.1 > 1.2). Bij ingrijpende veranderingen zal een nieuwe versie worden vervaardigd, herkenbaar doordat het versienummer met 1 wordt opgehoogd (1.0 > 2.0).

9 Noten

[i] *Volgens het Programma van Eisen deel 2d Certificate Policy – Services dienen de door de CSP uitgegeven of aanbevolen SUD's te voldoen aan de eisen gesteld in het document CWA 14169 "Secure Electronic Signature Devices, version EAL4+. Echter hiervoor geldt op dit moment een tijdelijke omgangsregeling (paragraaf 2.2 van de Objectieve verhinderingen Programma van Eisen PKI voor de overheid, versie 1.4 d.d. maart 2004). Deze tijdelijk omgangsregeling houdt in dat er kan worden afgeweken van de eisen die in het Programma van Eisen worden gesteld aan een veilig middel indien compenserende maatregelen worden getroffen in de van het systeem dat de sleutels van de services certificaten bevat. Er is dan sprake van een Veilige Omgeving, zoals hierboven gedefinieerd.*