ESG de electronische signatuur BV

# Certification Practice Statement

Versie 7.7

**ESG de electronische signatuur BV**

**Adres:** Horselstraat 1 | 6361 HC Nuth

**Tel:** +31 (0)495 566 355

info@de-electronische-signatuur.nl
www.de-electronische-signatuur.nl

**KvK:** 12056805
**BTW:** NL8220.033.26.B01

**Rabobank:** 17.69.17.209
**Swiftadres:** RABONL2U
**IBAN:** NL96RABO0176917209

## *Colofon*

Versienummer 7.7
Contactpersoon W. Kamminga

Organisatie ESG de Electronische Signatuur B.V.

*Bezoek- en postadres*
Horselstraat 1
6361 HC Nuth

## *Inhoudsopgave*

# 1. Introductie

## 1.1 Achtergrond

PKI is een methode om via iedere vorm van digitale communicatie een bewijs te leveren. Bijvoorbeeld het bewijs dat degene waarmee je over het Internet communiceert degene is die hij beweert te zijn. PKI bewijsvoering is erop gebaseerd dat bepaalde paren van getallen via een wiskundige wetmatigheid bij elkaar horen. Zo'n getallenpaar heet een 'sleutelpaar'. Het mooie van zo'n sleutelpaar is dat je aan iedere kant van een verbinding maar een van de twee sleutels nodig hebt om te bewijzen dat aan de andere kant de juiste (de andere) sleutel gebruikt wordt. De wiskundige wet immers verbindt de twee sleutels onverbrekelijk. Sleutelparen worden in een Public Key Infrastructuur (PKI) beheerd. Een van de sleutels van een sleutelpaar wordt geheim gehouden, de 'Secret Key' of 'Private Key'. De andere wordt als 'Public Key' gepubliceerd.

**Als de identiteitsgegevens van één persoon betrouwbaar verbonden zijn aan één publieke sleutel en dat de bijbehorende privé sleutel in zijn exclusieve beheer is, kan die persoon aan de hand van zijn publieke sleutel worden geïdentificeerd.**

Om deze identificatie te bewijzen moeten alle stappen van de bewijsvoering in samenhang gecontroleerd worden. Indien het sleutelpaar, het exclusieve beheer en de betrouwbare koppeling allemaal correct zijn, is een bewijs geleverd. Dan is de persoon geauthentiseerd, onweerlegbaarheid vastgelegd of kun je erop vertrouwen dat alleen de bedoelde persoon de vertrouwelijke gegevens kan lezen.

ESG de electronische signatuur BV verzorgt als Trusted Service Provider (TSP) onder de handelsnaam 'ESG' de Services die een Public Key Infrastructuur in de praktijk bruikbaar maakt. ESG genereert in een 'veilige omgeving', 'PKI geschikte sleutelparen'. Iedere geheime sleutel wordt direct opgeslagen op een 'veilig medium'. Dit medium, waarvoor ESG de houder zelf een pin laat kiezen, beantwoordt aan de eisen van het 'exclusieve beheer'. In een 'registratie procedure' verzorgt ESG de 'betrouwbare koppeling' van een publieke sleutel aan 'betrouwbare identificerende gegevens'. Deze koppelingen worden als 'elektronische certificaten', waarbij X509 vereist is, op het Internet controleerbaar gemaakt. Daarnaast certificeert ESG publieke sleutels op basis van de door haar abonnees aangeleverde Certificate Signing Requests (CSR).

### 1.1.1 Kader van de dienstverlening (PKIoverheid)

De Staat der Nederlanden heeft onder de naam PKIoverheid een Public Key Infrastructuur opgezet. PKIoverheid is geïmplementeerd in een afsprakenstelsel dat het mogelijk maakt generiek en grootschalig gebruik te maken van 'de elektronische handtekening'. Daarnaast faciliteert het stelsel 'identificatie op afstand' (authenticatie) en 'vertrouwelijke communicatie'. De Policy Authority (PA) van PKIoverheid heeft het afsprakenstelsel beschreven in haar Programma van Eisen (PvE) en de bijbehorende Certificaat Policy (CP). ESG heeft zich bij PKIoverheid aangesloten en zich aan het PvE geconformeerd. ESG conformeert zich tevens aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid Programma van Eisen deel 3b en de

betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements. De services van ESG voldoen aan alle eisen die door de Nederlandse wet en regelgeving gesteld zijn. Zij leveren daarmee de basis voor het hoogst beschikbare beveiligingsniveau van geautomatiseerde dienstverlening, waaronder elektronische communicatie. Zij maken “dat betrouwbare authenticatie mogelijk is zonder onmiddellijke tussenkomst van natuurlijke personen” ofwel “dat machinale controle van identiteit en authenticiteit voldoende betrouwbaar is voor gebruik in het maatschappelijk verkeer”.
Op de kwaliteit van de ESG services wordt toezicht gehouden door de PA van PKIoverheid. Ieder jaar wordt de servicekwaliteit van de ESG services door een onafhankelijke auditor gecontroleerd op basis van de ETSI EN 319 411-2 en EN 319 411-1 eisen en de additionele eisen uit het PvE. Deze audit herbevestigt dat de services van ESG aan alle eisen uit de betreffende standaarden voldoen. Dit blijkt uit de afgifte van een certificaat door de onafhankelijke auditor en de ondertekening van de ESG certificaten met het Nederlandse stamcertificaat.

Naast het feit dat de services van ESG moeten voldoen aan de eisen uit ETSI EN 319 411-2, EN 319411-1 en de PvE moeten zich ook houden aan de volgende wet- en regelgeving:

- Europese Richtlijn elektronische handtekeningen (1999/93/EG)
- Uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten
- Besluit Vertrouwensdiensten
- Regeling Vertrouwensdiensten
- eIDAS verordening
- Wet elektronisch bestuurlijk verkeer van kracht per 1 juli 2004
- CA/Browser Forum: Network and Certificate System Security Requirements (Netsec).

### 1.1.2 Opzet van de Certificate Policy

Dit document is de Certification Practice Statement voor ESG en bevat de richtlijnen voor het gebruik van de door ESG uitgegeven certificaten. De indeling van deze CPS is zoveel mogelijk conform de RFC3647 standaard toegepast.
Deze CPS wordt onder verantwoordelijkheid van de directie onderhouden.

### 1.1.3 Status

| Versie | vastgesteld | gepubliceerd | wijzigingen |
|---|---|---|---|
| CPS-4.10 | 04-02-11 ESG directie | 05-02-11 | |
| CPS-5.3 | 30-03-12 ESG directie | 31-03-12 | |
| CPS-5.11 | 03-07-12 ESG directie | 03-07-12 | |
| CPS-6.2 | 21-03-13 ESG directie | 25-03-13 | |
| CPS-6.3 | 11-06-13 ESG directie | 13-06-13 | |
| CPS-6.4 | 15-07-13 ESG directie | 15-07-13 | |
| CPS-6.5 | 10-02-14 ESG directie | 14-02-14 | |
| CPS-6.6 | 27-06-2014 ESG directie | 01-07-14 | H5.2.4/ 6.4.1/ 6.5/ 6.9.2/ 8.1/ 9.3/ 9.5 |
| CPS-7.0 | 05-01-2015 ESG directie | 5-01-2015 | Herindeling document conform RFC3647 |
| CPS-7.1 | 21-04-2015 ESG directie | 21-04-2015 | Aanpassing profiel services certificaat. |
| CPS-7.2 | 08-04-2016 ESG directie | 08-04-2016 | H3.2, H4.2.1, H6.1.3, H6.2, H6.4.1 t.a.v. gebruik nieuwe smartcard, verwijdering vermelding QV als leverancier. |
| CPS-7.3 | 02-08-2016 ESG directie | 02-08-2016 | § 1.2.4 toevoeging OID zegels, H7 update profielen |
| CPS-7.4 | 06-04-2017 ESG directie | 07-04-2017 | Toevoegen einddatum dienstverlening KPN in §1.1.4 en §1.2.2 |
| CPS-7.5 | 29-06-2017 ESG directie | 30-06-2017 | Aanpassingen ivm aangepast dienstverlening per 01-07-17 |
| CPS-7.6 | 04-12-2017 ESG directie | 04-12-2017 | Intrekken van certificaten via KPN servicedesk per 4-12-2017 12:00 uur |
| CPS-7.7 | 02-04-2019 ESG directie | 02-04-2019 | Jaarlijkse cps inhoud controle |

### 1.1.4 Doelgroep en betrokken partijen

In het PvE en de CPS van PKIoverheid wordt de volgende gebruikersgemeenschap onderscheiden; abonnees, certificaatbeheerders, certificaathouders (zowel natuurlijke personen als services) en vertrouwende partijen. Naast de in de CP genoemde betrokkenen beschrijft deze CPS; de TSP, de CSO, de LRA en de LRAO. Voor al deze betrokkenen is het van belang kennis te nemen van het Programma van Eisen van PKIoverheid.

- **CSP (Certification Service Provider)**

ESG is de eindverantwoordelijke TSP. Zij verzorgt (provides) services en certificatie op basis waarvan een certificaathouder zich betrouwbaar kan identificeren en authenticeren tegenover een vertrouwende partij. Het management van ESG is verantwoordelijk voor de in dit document beschreven services, de uitvoering van de beschreven richtlijnen en de controle op naleving hiervan. ESG heeft een aantal werkzaamheden uitbesteed.

- De 'component services organisatie' (CSO),
- De registratieprocedure.

- **CSO (Component Services Organisation)**

CSO voor ESG is 'KPN B.V.'. Deze organisatie zorgt onder verantwoordelijkheid van ESG voor de certificaat generatie, het revocatie status service en de revocatie management service. Verder beheert zij het 'High Secure' rekencentrum en de infrastructuur voor de productie van

cryptografische elementen.

Tot 01-07-2017 zal zij deze diensten blijven verzorgen. Na deze datum vervalt de dienst certificaat generatie. KPN zorgt tot 23-03-2020 ervoor dat de diensten revocatie status service en revocatie management service beschikbaar blijven.

- **LRA(Local Registration Authority) en LRAO (Local Registration Authority Officer)**

Het onmiddellijke contact met aankomende certificaathouders, de registratieprocedure, is uitbesteed aan LRA's, c.q. LRAO's. De LRA is aanspreekpunt voor certificaathouders. Tevens zijn zij de partij waar een certificaathouder advies en ondersteuning voor aankoop, installatie en implementatie van software kan krijgen. Iedere LRA heeft één of meer LRA-Officers in dienst. Iedere LRAO is door de TSP opgeleid en vertegenwoordigt de TSP bij de uitvoering van de verificaties en controles voorzien in het hier beschreven stelsel.

- **Abonnee**

De abonnee is een,

- natuurlijke persoon die met ESG een overeenkomst sluit om als certificaathouder publieke sleutels te laten certificeren.
- rechtspersoon die met ESG een overeenkomst sluit om namens een of meer certificaathouders publieke sleutels te laten certificeren.

Een abonnee is verplicht certificaten met een onjuiste inhoud te laten intrekken.

- **Certificaathouder**

Een certificaathouder is 'subject' van een certificaat. Dat is een entiteit die gekenmerkt is als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is opgenomen. Een certificaathouder kan zich, binnen de grenzen van de toepasselijke regelgeving, met behulp van de ESG certificaten identificeren en authenticeren. Bij services gebonden certificaten wordt de verantwoordelijkheid van de certificaathouder gedragen door een certificaatbeheerder.
Een natuurlijk persoon die certificaathouder is verkrijgt, middels de voorgeschreven controles en procedures, het recht zijn certificaat samen met het sleutelpaar conform dit CPS te gebruiken.

Een service is een 'niet natuurlijke persoon' die certificaathouder is. Het is een apparaat of een systeem, bediend door of namens een entiteit; een persoon of een organisatie. Voor het aanvragen, of mogelijk intrekken, van een service certificaat is tussenkomst door een certificaatbeheerder, een natuurlijk persoon die de certificaathouder vertegenwoordigd, vereist.

- **Certificaatbeheerder**

Een certificaatbeheerder is een natuurlijke persoon die namens de abonnee, die contractpartij is, gemachtigd is alle handelingen uit te voeren ten aanzien van certificaten van een service. De organisatorische entiteit legt de machtiging adequaat vast en blijft verantwoordelijk.

- **Vertrouwende Partij**

Een vertrouwende partij is iedere natuurlijke of rechtspersoon die handelt in vertrouwen op een ontvangen certificaat.
Een ontvangen certificaat kan en mag alleen vertrouwd worden:

- als de status informatie van het certificaat is geverifieerd en het Certificaat:
  - niet is ingetrokken;

- niet is verlopen;

- de volledige keten van certificaten tot aan het stamcertificaat van de Staat der Nederlanden geldig is;
- en voor zover het vertrouwen dat in het certificaat gesteld mag worden, niet beperkt wordt door het certificaat zelf of door deze CPS.

## *1.2 Certificaatgebruik*

### 1.2.1 Toepassingsgebied certificaten

Het gebruik van services certificaten uitgegeven onder PKIoverheid heeft betrekking op communicatie van certificaathouders die handelen namens de abonnee.
Het gebruik van persoonsgebonden certificaten uitgegeven onder PKIoverheid heeft betrekking op communicatie van certificaathouders op persoonlijke titel.

Het is de TSP niet toegestaan om binnen het toepassingsgebied van certificaten beperkingen te aan het gebruik van certificaten of aan de waarde van de transacties waarvoor certificaten kunnen worden gebruikt.

### 1.2.2 Certificaat hiërarchie

De Certificaten worden niet onmiddellijk door het Nederlandse stamcertificaat getekend. De Public Key Infrastructuur van Nederland, is geïmplementeerd in een 'three-level certification hiërarchie'. Op het hoogste niveau, tekent het Nederlandse stamcertificaat, 'Staat der Nederlanden Root CA – G2':

1. in het domein 'Overheid en bedrijven' het 'Staat der Nederlanden Organisatie CA - G2'-certificaat. Met dit (niveau 2) certificaat is het 'ESG CA-certificaat' 2.16.528.1.1003.1.3.5.3.1 (niveau 3) getekend.
2. in het domein 'Burger' het 'Staat der Nederlanden Burger CA - G2'-certificaat. Met dit (niveau 2) certificaat is het 'ESG Burger-CA-certificaat' 2.16.528.1.1003.1.3.3.1.1 (niveau 3) getekend.

ESG tekent met deze certificaten de verschillende eindgebruikers certificaten.

Deze root zal blijven bestaan tot 23-03-2020 en daarna volledig vervangen zijn door de G3 root. ESG heeft tot 01-07-2017 certificaten onder de G2 root geproduceerd Deze certificaten hebben een maximale geldigheid van 2 jaar. Na deze datum zal zij alleen nog voorzien in de revocatie diensten die voor de G2 root beschikbaar zijn.

### 1.2.3 Certificaat gebruik

ESG is Certification Service Provider en sluit als zodanig een contract met een abonnee ten behoeve van een certificaathouder. In dit contract staat een artikel conform artikel 253 van Boek 6 BW. Dit artikel regelt de aansprakelijkheid van ESG als een vertrouwende partij kan aantonen dat hij alvorens het certificaat te vertrouwen alle vereiste controles heeft uitgevoerd.
Certificaten die onder deze CPS worden uitgegeven, kunnen niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen alleen met een in de Wet op de identificatieplicht aangewezen document mag worden vastgesteld.

### 1.2.4 Certificate Policies

Het PKIoverheid Programma van Eisen (Certificate Policy) van de door ESG uitgegeven certificaten is beschikbaar via www.logius.nl. ESG geeft de navolgende typen certificaat aan, respectievelijk ten behoeve van, de certificaathouder in gebruik.

| OID | Type |
|---|---|
| 2.16.528.1.1003.1.2.5.1 | Het persoonsgebonden authenticiteitcertificaat, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie van een persoon |
| 2.16.528.1.1003.1.2.5.2 | Het persoonsgebonden handtekeningcertificaat, dat de publieke sleutel bevat ten behoeve van de gekwalificeerde elektronische handtekening |
| 2.16.528.1.1003.1.2.5.3 | Het persoonsgebonden vertrouwelijkheidcertificaat, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid |
| 2.16.528.1.1003.1.2.5.4 | Het service gebonden authenticiteitcertificaat, wordt gebruikt voor het langs elektronische weg betrouwbaar identificeren en authentificeren van een service als behorende bij de organisatorische entiteit die verantwoordelijk is voor de betreffende service |
| 2.16.528.1.1003.1.2.5.5 | Het service gebonden vertrouwelijkheidcertificaat, wordt gebruikt voor het beschermen van de vertrouwelijkheid van gegevens die worden uitgewisseld en/of opgeslagen in elektronische vorm |
| 2.16.528.1.100.3.1.2.5.7 | Het service gebonden onweerlegbaarheid certificaat, wordt gebruikt voor het verifieren van elektronische zegels. |
| 2.16.528.1.1003.1.2.5.6 | Het servercertificaat, wordt gebruikt voor het beveiligen van een verbinding tussen een bepaalde cliënt en een server die behoort bij de organisatorische entiteit die wordt genoemd in het betreffende certificaat |
| 2.16.528.1.1003.1.2.3.1 | Het persoonsgebonden authenticiteitcertificaat wordt gebruikt voor het betrouwbaar identificeren en authenticeren van personen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen |
| 2.16.528.1.1003.1.2.3.2 | Het persoonsgebonden handtekeningcertificaat wordt gebruikt om elektronische handtekeningen te verifiëren, die “dezelfde rechtsgevolgen hebben als een handgeschreven handtekening”, zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecomwet |
| 2.16.528.1.1003.1.2.3.3 | Het persoonsgebonden vertrouwelijkheidcertificaat wordt gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm. Dit betreft zowel de uitwisseling tussen personen onderling als tussen personen en geautomatiseerde middelen |

# 2. Publicatie en verantwoordelijkheid voor elektronische opslagplaats

## 2.1 Elektronische opslagplaats

De door ESG onderhouden publicaties zijn 7 dagen in de week en 24 uur per dag bereikbaar. Desondanks kan een service door onvoorziene omstandigheden uitvallen. In een dergelijk geval zorgt ESG dat de service binnen 24 uur weer bereikbaar is.

## 2.2 Publicatie van CPS-informatie

ESG publiceert op haar website www.de-electronische-signatuur.nl :

- De volledige inhoud van dit document
- De algemene voorwaarden
- Informatie voor het verkrijgen van een certificaat
- Prijslijst/Tarieven
- Informatie met betrekking tot blokkering of intrekking van
    - een certificaat
    - een encryptie sleutel
    - een CA sleutel
- Informatie met betrekking tot wijziging van
    - een encryptie sleutel
    - een CA sleutel
- (verdenking van) Fraude met
    - een encryptie sleutel
    - een CA sleutel
- Aankondigingen van relevante wijzigingen van de Certificaat Policy

De website is beveiligd tegen het aanpassen en verwijderen van gegevens door derden. Inzage in deze informatie is niet onderhevig aan toegangscontrole.

# 3. Identificatie en authenticatie

Deze paragraaf beschrijft op welke wijze de identificatie en authenticatie van certificaataanvragers plaatsvindt tijdens de initiële registratieprocedure en welke criteria ESG stelt ten aanzien van de naamgeving.

## 3.1 Naamgeving

Geen nadere bepalingen.

## 3.2 Vaststellen van de identiteit

Geen nadere bepalingen.

### 3.2.1 Methode om bezit van Private sleutel aan te tonen

Geen nadere bepalingen.

## 3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

De I&A procedure bij een routinematige certificaat vernieuwing is gelijk aan die bij eerste registratie met uitzondering van het feit dat een aanvraag voor een routinematige certificaatvernieuwing ook kan en mag plaatsvinden met een beschikbare en geldige gekwalificeerde elektronische handtekening.

### 3.3.1 Identificatie en authenticatie bij vernieuwing van het certificaat na intrekking

ESG biedt geen mogelijkheid tot vernieuwing van gecertificeerde sleutels.

## 3.4 Identificatie en authenticatie bij intrekking van een certificaat.

Voor de authenticatie van de intrekkingsbevoegdheid wordt het telewachtwoord gebruikt. Een certificaatbeheerder, -houder kan onder telefonische vermelding van het opgegeven telewachtwoord, een verzoek tot intrekking van het desbetreffende certificaat indienen bij ESG. ESG zal na controle van het opgegeven telewachtwoord direct overgaan tot intrekking van het certificaat. Indien de certificaatbeheerder of –houder niet in de gelegenheid is om telefonisch contact op te nemen met ESG, kan het verzoek ook ingediend worden door een bevoegd vertegenwoordiger van de abonnee die geïdentificeerd is door ESG.
De reden van intrekking wordt altijd door ESG vastgelegd.

# 4. Operationele eisen certificaatlevenscyclus

## 4.1 Aanvraag

Geen nadere bepalingen.

## 4.2 Registratieprocedure

Geen nadere bepalingen.

### 4.2.1 Identificatie

Geen nadere bepalingen.

### 4.2.2 Vaststellen van de certificaatgegevens

Geen nadere bepalingen.

### 4.2.3 Vaststellen van de organisatiegegevens

Geen nadere bepalingen.

### 4.2.4 Indienen aanvraagdossier

Geen nadere bepalingen.

## 4.3 Productie & uitgifte

Geen nadere bepalingen.

## 4.4 Controle & acceptatie

Geen nadere bepalingen.

### 4.4.1 Acceptatie persoonsgebonden certificaten

Geen nadere bepalingen.

### 4.4.2 Acceptatie Server certificaten

Geen nadere bepalingen.

## 4.5 Sleutelpaar en certificaatgebruik

Normaliter zijn certificaten 3 jaar geldig, Als de levensduur van het CA certificaat dit toelaat is op verzoek een levensduur tot 5 jaar mogelijk. Dit verzoek dient echter goedgekeurd te zijn door de PA PKIoverheid. Ook een kortere levensduur kan op verzoek worden geproduceerd.

De abonnee, certificaathouder, respectievelijk de certificaatbeheerder, garanderen dat het certificaat uitsluitend wordt gebruikt conform de richtlijnen in dit CPS, de Bijzondere Voorwaarden en de AV (algemene voorwaarden) voor de dienstverlening van ESG de electronische signatuur BV. Daarnaast draagt hij de verantwoordelijkheid voor deugdelijkheid en maatregelen ter bescherming van de informatie- en communicatiesystemen waarmee hij elektronisch berichtenverkeer tot stand brengt.

De abonnee zowel als de certificaathouder, respectievelijk de certificaatbeheerder, staan garant voor de volledigheid en de juistheid van de gegevens in zijn certificaten. Hieronder wordt mede de verplichting verstaan relevante wijzigingen door middel van een intrekkingsverzoek aan de TSP kenbaar te maken.

De abonnee draagt zelf zorg voor een tijdige vervanging van het certificaat in het geval van een naderende afloop geldigheid en noodvervanging in geval van compromittatie en/of andere soorten calamiteiten met betrekking tot het certificaat of van bovenliggende certificaten. Van de

abonnee wordt verwacht dat hij zelf adequate maatregelen neemt om de continuïteit van het gebruik van certificaten te borgen.

## 4.6 Certificaat vernieuwing

ESG biedt geen mogelijkheid tot vernieuwing van PKIoverheid Certificaten.

## 4.7 Certificaat rekey

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

## 4.8 Aanpassen van certificaten

ESG biedt geen mogelijkheid tot aanpassing van de inhoud van PKIoverheid Certificaten. Indien de gegevens in het Certificaat niet meer overeenstemmen met de werkelijkheid dan is de Abonnee verplicht het betrokken Certificaat onmiddellijk in te trekken..

## 4.9 Intrekking en opschorting van certificaten

De geldigheid van een certificaat kan worden geblokkeerd. Opschorting van een certificaat is niet toegestaan. Wanneer een omstandigheid genoemd in paragraaf 4.9.1 zich voordoet is iedere bevoegde die kennis draagt van deze omstandigheid verplicht onmiddellijk een verzoek tot intrekking in te dienen. De reden voor intrekking wordt, indien bekend, vastgelegd.

### 4.9.1 Omstandigheden die leiden tot intrekking

De volgende omstandigheden leiden tot intrekking van een certificaat:

- de abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee verleent met terugwerkende kracht ook geen toestemming;
- de TSP beschikt over voldoende bewijs dat de privésleutel van de abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast of er is het vermoeden van compromittatie, of er is sprake van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel of SSCD, gestolen of vermoedelijk gestolen sleutel of SSCD of vernietigde sleutel ofSSCD;
- een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in de CP van Logius, het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft afgesloten;
- de TSP op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder;
- de TSP bepaalt dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft gesloten;
- de TSP bepaalt dat informatie in het certificaat niet juist of misleidend is;
- de TSP haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere TSP.
- De PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen).
- Daarnaast kunnen certificaten worden ingetrokken als maatregel om een calamiteit te voorkomen, c.q. te bestrijden. Als calamiteit wordt zeker de aantasting of vermeende aantasting van de private sleutel van de TSP waarmee certificaten worden ondertekend, beschouwd.

Certificaten waarvoor een van bovenstaande omstandigheden geldt, mogen niet worden gebruikt en dient er door de Abonnee of Certificaatbeheerder, -houder een intrekkingsverzoek ingediend te worden bij ESG.

#### 4.9.2 Intrekkingsbevoegdheid

De intrekking van een certificaat kan worden gelast door de:

- abonnee
- certificaathouder of zijn wettelijke vertegenwoordigers. (In het domein Burger is de certificaathouder gelijk aan de abonnee).
- een door de certificaathouder vertegenwoordigde derde waarvan de vertegenwoordiging in het certificaat vermeld staat.
- ESG.

#### 4.9.3 Procedure voor het plaatsen van een intrekkingsverzoek

Intrekking van een certificaat dient telefonisch of via email door een bevoegd persoon te worden aangevraagd.

Binnen kantooruren (ma t/m vr 9:00 – 17:00 uur):

088–6610621 (email: servicedesk.sbr@kpn.com)

Buiten kantooruren:

088–6610621 (email: esd.24x7@kpn.com)

Meld hierbij dat het gaat over het intrekken van een door ESG uitgegeven PKIoverheid certificaat. Vermeld tevens het Telewachtwoord dat is opgegeven tijdens de registratie.

Binnen maximaal vier (4) uur na een geauthentiseerd intrekkingsaanvraag zal het certificaat worden ingetrokken en een nieuwe CRL worden uitgeven.

#### 4.9.4 Herroepen van een intrekking

Een intrekking van een certificaat is definitief en kan niet herroepen worden.

### *4.10 Certificaat statusservice*

Vertrouwende partijen kunnen in redelijkheid op een certificaat vertrouwen als zij een adequate (online) controle uitvoeren. De URL's voor onderstaande services zijn opgenomen in de certificaten. De services zijn in principe 7 dagen in de week en 24 uur per dag bereikbaar. Desondanks kan een service door onvoorziene omstandigheden uitvallen. In een dergelijk geval zorgt ESG dat de service binnen 4 uur weer bereikbaar is.

#### 4.10.1 CRL (Blokkeringslijst)

Geblokkeerde certificaten worden in de blokkeringslijst (CRL) opgenomen. De CRL wordt dagelijks en binnen maximaal 4 uur na elke melding vernieuwd. De blokkeringslijst kan via de LDAP server op elk moment ingezien worden. Opname van een certificaat in de CRL is de definitieve bevestiging van een blokkering. Certificaten worden minstens tot zeven jaar, ook na afloop van de geldigheid, op de blokkeringslijst vermeld

#### 4.10.2 Geldigheidscontrole via OCSP

De geldigheid van een certificaat kan ook via het OCSP conform RFC6960, zonder 'precomputed responses', gecontroleerd worden.

#### 4.10.3 Duur overeenkomst

De duur van een overeenkomst met een abonnee is in principe onbeperkt. Echter, ESG vernieuwd de overeenkomst bij iedere certificaataanvraag die geplaatst wordt.

### *4.11 Key escrow en Recovery*

Standaard vindt er geen Escrow van Private Sleutels plaats. ESG biedt geen mogelijkheid tot het in Escrow nemen van Private Sleutels.

# 5. Management, operationele en fysieke beveiligingsmaatregelen

De omgeving van ESG is gecertificeerd tegen ETSI EN 319 411-2 en EN 319 411-1. Het kwaliteitsmanagement systeem is via de PDCA-cyclus voortdurend gericht op verbetering van het systeem. In de volgende hoofdstukken wordt beschreven welke operationele en fysieke beveiligingsmaatregelen zijn toegepast op de locatie van haar CSO KPN waar de technische omgeving van ESG is ondergebracht.

## 5.1 Fysieke beveiliging

### 5.1.1 Vestiging CSO

De CSO van de ESG is ondergebracht bij KPN B.V.. Deze organisatie onderscheidt zich met nauwkeurig vastgelegde procedures en een zeer hoge mate van veiligheid. KPN B.V. beheert en implementeert fysieke en procedurele veiligheidsmaatregelen om toegang tot hardware en software, gebruikt met betrekking tot de CA operaties, te beperken.

### 5.1.2 KPN B.V.

De certificatiedienstverlening wordt beheerd in en geleverd vanuit een streng beveiligde omgeving binnen het rekencentrum van KPN 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 een beveiligingsbedrijf.

De beveiligingssystemen signaleren automatisch pogingen tot (on)geautoriseerde toegang. De technische maatregelen worden ondersteund door verschillende procedures, onder andere door bewegingssensoren die personeel 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 o.a. 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 gebouwenbeheerdienst de in- en uitgaande goederen (op Basis van geleidedocumenten).

De beveiligde omgeving van KPN biedt standaard tot minimaal vijf fysieke barrières tot aan de productieomgeving. Voor niet-productie (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/SUD, biometrische data, begeleiding bij toegang en visuele inspectie. Additionele maatregelen zijn onder andere inbraakdetectie en video-opnames. 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 KPN.

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

- Bliksemafleiding;
- Airco voorzieningen;
- Back-up van elektriciteit met behulp van een eigen elektriciteitsvoorziening;
- Bouwkundige maatregelen (brandresistentie, waterafvoer, etc.);
- Brandpreventie door middel van automatisch en handmatige brandalarmvoorzieningen. Zulks in combinatie met gerichte, geautomatiseerde brandblussing.

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 KPN.

#### *5.1.3.1 Opslag van media*

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

#### *5.1.3.2 Afval verwijdering*

KPN heeft een overeenkomst gesloten met een professioneel afval verwijder bedrijf voor de veilige afvoer van afval, gebruikt papier en dergelijke. Het personeel van KPN is eraan gehouden al het afvalpapier te gooien in de overal in het gebouw aanwezige afgesloten papiercontainers.

#### *5.1.3.3 Externe back-up*

Media met daarop data en programmatuur worden ook opgeslagen in een ander gebouw van KPN, met een minimaal gelijkwaardige beveiligingsniveau.

## *5.2 Procedurele beveiliging*

### 5.2.1 Vestiging Nuth

De sleutel van de serverruimte is in het bezit van de directie en aanwezig in de sleutelkast. Daar bevindt zich ook de sleutel van de kluis. Toegang tot deze sleutelkast hebben de verantwoordelijke medewerk(st)er van de administratie en de binnendienst medewerker.

### 5.2.2 KPN B.V.

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 TSP functies.

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

Autorisatie van het TSP personeel vindt plaats op basis van het 'need-to-know'principe.

## 5.3 Personele beveiliging

### 5.3.1 KPN B.V.

#### 5.3.2.1 Vertrouwelijke functies

KPN heeft een Trusted Employee Policy geïmplementeerd. In deze policy staat o.a. beschreven voor welke functiecategorieën en rollen de status "vertrouwd"hebben. Het betreft voornamelijk functies die betrokken zijn bij het management van certificaten en sleutelmateriaal, functies die betrokken zijn bij systeemontwikkeling, -beheer, en –onderhoud en functies binnen Security management, Quality management en Auditing.

#### 5.3.2.2 Aantal personen benodigd per taak

Voor het uitvoeren van bepaalde, vooraf gedefinieerde, activiteiten op het gebied van sleutel -, certificaatmanagement, systeemontwikkeling, - onderhoud en - beheer zijn meerdere medewerkers nodig. De noodzaak om met meerdere mensen een bepaalde activiteit wordt afgedwongen o.a. met behulp van technische voorzieningen, autorisaties in combinatie met identificatie/ authenticatie en aanvullende procedures.

#### 5.3.2.3 Functiescheiding

KPN 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).

#### 5.3.2.4 Vakkennis, ervaring en kwalificaties

Voor de levering van PKIoverheid Certificaten zet KPN personeel in dat beschikt over voldoende vakkennis, ervaring en kwalificaties.

KPN heeft van elke functie vastgesteld welke kennis en ervaring voor een goede invulling benodigd is. Dit wordt onderhouden, omdat de ontwikkelingen in het vakgebied elkaar snel opvolgen. Daarnaast wordt van elke medewerker geregistreerd welke kennis en ervaring hij/zij bezit.

#### 5.3.2.5 Trusted Employee Policy

KPN heeft voor haar certificatiedienstverlening een Trusted Employee Policy opgesteld en geïmplementeerd. Bij het opstellen en onderhouden van deze policy is/ wordt goed gekeken naar de mogelijkheden en onmogelijkheden van algemeen geldende wet- en regelgeving. In deze policy is uitgebreid beschreven hoe wordt omgegaan met bijvoorbeeld een pre-employmentscreening, het opleveren van een Verklaring omtrent het Gedrag ingevolge de Wji en

het uitvoeren van veiligheidsonderzoeken door diensten als Algemene Inlichtingen- en Veiligheidsdienst of de Militaire Inlichtingen- en Veiligheidsdienst ter verkrijging van een Verklaring van Geen Bezwaar. In de policy is ook opgenomen welke mogelijkheden het management heeft indien een (toekomstig) medewerker niet mee wil werken dan wel de uitkomst van het onderzoek niet positief is.

#### *5.3.2.6 Beheer en Beveiliging*

KPN 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, te houden en waar mogelijk te verbeteren.
KPN heeft gescheiden systemen voor ontwikkeling, test, acceptatie en productie. Deze systemen worden beheerd met gebruikmaking van eerder genoemde ITIL procedures.
Het overbrengen van programmatuur van de ene omgeving naar de nadere vindt gecontroleerd plaats, met gebruikmaking van de procedure voor Change management. Deze procedure omvat onder andere het bijhouden en vastleggen van versies, het aanbrengen van 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, repressie en correctief van aard. Voorbeelden van getroffen maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen.

KPN heeft erin voorzien dat er in een 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.

Indien een incident of andere gebeurtenis op enigerlei wijze de betrouwbaarheid van de certificatiedienstverlening en/of het imago van de PKI voor de overheid kunnen bedreigen of beïnvloeden zal dit onmiddellijk gemeld worden aan de PKIOverheid Policy Authority.

## *5.4 Procedures ten behoeve van beveiligingsaudits*

De afzonderlijke componenten in het systeem van de CSO houden automatisch logs bij. Handmatige Protocollen worden zowel schriftelijk als in protocolbestanden vastgehouden. Logs worden regelmatig op veiligheidsrelevante gebeurtenissen onderzocht. Alle veiligheidskritische gebeurtenissen worden aan de TSP gemeld. Indien noodzakelijk via de blokkeringshotline.

### 5.4.1 Vastlegging van gebeurtenissen

ESG hanteert logging op minimaal:

- Routers, Firewalls en netwerk systeem componenten;
- Database activiteiten en events;
- Transacties;
- Operating systemen;
- Access control systemen;
- Mail servers;

Hierbij worden de volgende gebeurtenissen handmatig of automatisch gelogd:

- CA key life cycle management;
- Certificate life cycle management;
- Bedreigingen en risico's zoals:
  - Succesvolle en niet succesvolle aanvallen PKI systeem;
  - Activiteiten van medewerkers op het PKI systeem;
  - Lezen, schrijven en verwijderen van gegevens;
  - Profiel wijzigingen (Access Management);
  - Systeem uit, hardware uitval en andere abnormaliteiten;
  - Firewall en router activiteiten;
  - Betreden van- en vertrekken uit de ruimte van de CA.

De log bestanden moeten minimaal het volgende registreren:

- Bron adressen (IP adressen indien voorhanden);
- Doel adressen (IP adressen indien voorhanden);
- Tijd en datum;
- Gebruikers ID's (indien voorhanden);
- Naam van de gebeurtenis;
- Beschrijving van de gebeurtenis.

Audit logs worden regelmatig gereviewed om te bezien of er zich belangrijke security of operationele gebeurtenissen hebben voorgedaan waar eventueel nadere actie op moet worden ondernomen.

#### 5.4.2 Bewaartermijn voor logbestanden

De logbestanden worden minimaal 18 maanden opgeslagen en daarna worden ze verwijderd. De geconsolideerde (elektronische) auditlogs worden evenals de handmatige registraties 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

### *5.5 Archivering van documenten*

#### 5.5.1 Vastlegging van gebeurtenissen

Alle papieren documenten bedoeld voor aanvraag, controle en productie van een certificaat worden in het archief van KPN opgeslagen en 10 jaar na archivering bewaard. Logs en protocollen worden voor korte termijn beveiligd online bewaard. Alleen geautoriseerd personeel heeft toegang tot deze bestanden. Er worden regelmatig back-ups gemaakt. Deze back-ups worden gearchiveerd. Deze archieven zullen worden behouden en beschermd tegen wijziging of vernietiging voor een periode van 7 (zeven) jaar en daarna worden verwijderd. Enkel officers van de certificatieautoriteit, de chief security officer en auditoren mogen het gehele archief inzien. De inhoud van de archieven zal niet in zijn geheel worden vrijgegeven, behalve wanneer dit vereist is door wetgeving.

#### 5.5.2 Toegang tot het archief

Certificaathouders mogen hun eigen registratiegegevens inzien. Op verzoek zal KPN deze gegevens toegankelijk maken. Daarnaast kan KPN beslissen logs van individuele registratie transacties vrij te geven, wanneer enig belanghebbende hierom vraagt. Een redelijke handling fee zal in rekening worden gebracht om de kosten te dekken.

## 5.6 Vernieuwing CA Sleutel

De geldigheid van de CA sleutel is bepaald door PKIoverheid. Voordat met de bestaande CA sleutel geen gebruikerscertificaten met voldoende looptijd meer kunnen worden uitgegeven, zal er een nieuwe sleutel in gebruik genomen worden. Ingebruikname van een nieuwe CA sleutel heeft geen directe gevolgen voor eerder, onder een andere CA sleutel uitgegeven certificaten. Zowel de oude als nieuwe sleutelparen kunnen gelijktijdig actief zijn. Zodra alle onder een CA sleutel uitgegeven certificaten zijn verlopen, zal de CA sleutel onbruikbaar worden gemaakt.

## 5.7 Aantasting en Continuiteit

### 5.7.1 Afhandeling calamiteiten

ESG maakt onderdeel uit van het bedrijfcontinuiteitsplan van KPN B.V. De plannen omvatten onder meer:

- Procedures voor het regeren op incidenten en compromittatie van sleutels;
- Procedures voor intrekken van certificaten;
- Procedures voor optreden in geval van problemen met gegevensverwerking, software, en/ of corrupte data;
- Procedures voor het waarborgenv an de bedrijfscontinuiteit na een ramp.

De plannen zijn merkgebonden, veiligheidsgevoelig en vertrouwelijk. Derhalve zijn ze niet algemeen beschikbaar.

### 5.7.2 Informatieverspreiding

KPN zal betrokkenen zo spoedig als mogelijk op de hoogte stellen. Dit zal men doen door het versturen van e-mail en/of het publiek kenbaar maken van de calamiteit via onze website, afhankelijk van de omvang van de calamiteit. Daarnaast zal KPN de PA (Policy Authority), het NCSC en de auditor onmiddellijk op de hoogte stellen en houden van risico's, gevaren of gebeurtenissen die op enigerlei wijze de betrouwbaarheid van de dienstverlening en/of het imago van de PKI voor de overheid kunnen bedreigen of beïnvloeden.

## 5.8 Beëindiging van de service

De Certificate Service activiteiten kunnen, met in acht neming van de wettelijke bepalingen, eenzijdig door ESG stopgezet worden. Een voorgenomen stopzetting wordt, ten minste 2 maanden vóór de stopzetting, aan zowel de ACM, Logius, alsmede aan alle abonnees en certificaathouders medegedeeld. Bij het stopzetten van de Certificate Service activiteiten zal het register nog tot 6 maanden na stopzetting van de activiteiten worden voortgezet. Ingeval deze activiteiten niet door een andere certificaatdienstverlener wordt overgenomen, worden alle uitgegeven certificaten ingetrokken.

# 6. Technische beveiliging

## 6.1 Genereren en installeren van sleutelparen

### 6.1.1 Genereren van sleutelparen van de certificaathouders

Geen verdere bepalingen.

#### 6.1.2 Overdracht van Private Sleutel en SSCD aan certificaathouder

Geen nadere bepalingen.

#### 6.1.3 PIN-PUK procedure

Geen nadere bepalingen.

#### 6.1.4 Overdracht van de Publieke sleutel aan Vertrouwende partijen

Geen nadere bepalingen.

#### 6.1.5 Sleutellengte van private sleutels van certificaathouders

De sleutellengte van een certificaat is sha256RSA van minimaal 2048 bits.

#### 6.1.6 vereisten sleutellengte van private sleutels

de lengte van cryptografisch sleutels van de certificaathouders dient te voldoen aan de eisen, die daaraan zijn gesteld in de lijts van cryptografische algoritmes en sleutellengtes, zoals gedefineerd in ETSI TS 102 176-1.

#### 6.1.7 Doelen van sleutelgebruik

Geen nadere bepalingen.

### *6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen*

De aankomende certificaathouder is volledig verantwoordelijk voor de beveiliging van zijn eigen smartcard. De geleverde smartcard wordt geleverd met een gedefinieerde PIN en PUK. Deze PIN en PUK worden slechts eenmalig door ESG verstrekt. ESG hanteert geen opslag van deze gegevens. Omdat optimale beveiliging een kaartlezer met eigen PIN pad vereist wordt normaliter een numerieke PIN gebruikt. Op geen moment mag een certificaathouder het PIN aan een ander bekend maken. ESG is niet op de hoogte van het PIN en aanvaardt derhalve geen enkele aansprakelijkheid voor misbruik van een PIN.

#### 6.2.1 Veiligheid van componenten

Alle gebruikte componenten zijn conform ETSI geëvalueerd en gecertificeerd. Componenten, waarvoor de Nederlandse wet elektronische handtekening evaluatie naar ITSEC of Common Criteria vereist, zijn aanvullend conform die criteria gecertificeerd. De hardware security modules voldoen aan FIPS 140-2 niveau 3 en/of aan EAL 4+. Toegang tot de modules is beperkt met het gebruik van smartcards.

#### 6.2.2 Timestamping

ESG verzorgt geen time-stamping services.

#### 6.2.3 Escrow van Private Sleutels van Certificaathouders

ESG biedt geen mogelijkheid tot het in escrow houden van private sleutels van certificaathouders.

#### 6.2.4 Back-up van private sleutels van certificaathouders

ESG biedt geen mogelijkheid tot een back-up van de private sleutels van certificaathouders.

#### 6.2.5 Archivering van private sleutels van certificaathouders

Private sleutels van certificaten worden niet gearchiveerd.

#### 6.2.6 Toegang tot private sleutels in cryptografische module

Voor de private sleutels behorende bij CA-certificaten van ESG, die zijn opgeslagen in een cryptografische hardware modules, wordt toegangsbeveiliging gebruikt die garandeert dat de sleutels niet buiten de module kunnen worden gebruikt.

#### 6.2.7 Opslag van private sleutels in cryptografische module

CA-private sleutels worden versleuteld opgeslagen in hardware cryptografische modules.

#### 6.2.8 Activering van private sleutels

Geen nadere bepalingen.

#### 6.2.9 Deactivering van private sleutels

Onder specifieke omstandigheden kan de TSP bepalen dat de private sleutels worden gedeactiveerd, met inachtneming van de daarop van toepassing zijnde waarborgen ten behoeve van zorgvuldigheid.

Indien een SSCD door de certificaathouder wordt verloren en door een vinder wordt geretourneerd aan de TSP, zal deze SSCD door haar worden vernietigd, inclusief de daarin opgenomen private sleutels. Tevens zal de TSP controleren of de bijbehorende certificaten zijn ingetrokken. Is dit niet het geval, dan zal de TSP alsnog per direct de certificaten intrekken.

#### 6.2.10 Methode voor het vernietigen van private sleutels

De private sleutels waarmee certificaten worden ondertekend, kunnen na het einde van hun levenscyclus niet meer worden gebruikt. De TSP zorgt voor een adequate vernietiging waarbij wordt voorkomen dat het mogelijk is de vernietigde sleutels te herleiden uit de restanten. Als dergelijke sleutels worden vernietigd worden die activiteiten gelogd.

#### 6.2.11 Eisen voor veilige middelen voor opslag en gebruik van certificaten

De smartcard die wordt gebruikt voor de opslag van sleutels van certificaathouders, voldoet aan de eisen die gesteld zijn in CWA 14169 niveau EAL4+.

In plaats van gebruik te maken van een hardwarematige SUD mogen de sleutels van een services certificaat softwarematig worden beschermd indien compenserende maatregelen worden getroffen in de omgeving van het systeem dat de sleutels bevat. De compenserende maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren.

De beheerder van de services certificaten die gebruik maakt van deze mogelijkheid voor softwarematige opslag dient bij registratie ten minste een schriftelijke verklaring te overleggen dat compenserende maatregelen zijn getroffen die voldoen aan de hiervoor gestelde voorwaarde.

In de Bijzondere Voorwaarden van de TSP staat opgenomen dat ESG het recht heeft om een controle uit te voeren naar de getroffen maatregelen.

### *6.3 Andere aspecten van sleutelpaarmanagement*

Het Root certificaat van PKIoverheid is controleerbaar via de formele publicatie in het Nederlandse Staatsblad. Feitelijk wordt het certificaat meegeleverd met browsers en andere

programmatuur. Via de eigen website en die van PKIoverheid zijn de publieke sleutels van ESG te downloaden. Alle uitgegeven publieke sleutels worden 7 jaar in administratie gehouden. ESG slaat privé sleutels alleen op de SSCD/SUD op en heeft derhalve na uitreiking van de SSCD geen privé sleutels meer onder zich.

30 dagen voordat de geldigheid van een certificaat verloopt, wordt de certificaathouder of –beheerder per email genotificeerd en de mogelijkheid geboden om een nieuw certificaat aan te vragen.

## 6.4 Activeringsgegevens

### 6.4.1 Genereren en installeren van activeringsgegevens

De SSCD die de TSP levert is door de TSP voorzien van een zogenaamde PIN en PUK. (zie 6.1.3). De PIN en PUK wordt slechts eenmalig door de TSP verstrekt aan de certificaathouder. De TSP heeft verder geen opslag van deze PIN en PUK. Indien de pincode drie maal foutief wordt ingevoerd, wordt de SSCD geblokkeerd, deze kan alleen gedeblokkeerd worden door de geleverde PUK. Indien deze 5 maal foutief wordt ingevoerd, is de kaart geblokkeerd en dient deze vervangen te worden .

In het geval van een services server certificaat in de variant PKCS#12 wordt er door de TSP een eenmalige PINbrief gegeneerd. Deze PINbrief wordt separaat van het certificaat verzonden naar de certificaatbeheerder. Omdat de TSP geen opslag hanteerd van PINbrieven, zal het certificaat bij verlies van deze PINbrief, ingetrokken dienen te worden.

## 6.5 Logische toegangsbeveiliging van TSP-computers

De systemen die gebruikt worden voor de uitgifte of goedkeuring van certificaten zijn allemaal voorzien van multifactor authenticatie. Iedere TSP operator heeft een smartcard met een persoonsgebonden certificaat en heeft de smartcard voorzien van een persoonlijke pincode.

Deze systemen zijn uitsluitend toegankelijk voor de vaste medewerkers van de TSP.

## 6.6 Beheersmaatregelen technische levenscyclus

De CSO volgt de Certificate Issuing and Management Components (CIMC) Family of Protection Profiles, welke de eisen bepaalt voor componenten die X.509 (public key) certificaten uitgeven, intrekken en beheren. CIMC is gebaseerd op de Criteria EAL 4+. De Security Officer verifieert periodiek de integriteit van de componenten.

## 6.7 Netwerkbeveiliging

De gebruikte firewall en computersystemen voldoen aan de actuele stand van de techniek. Alle systemen zijn minimaal geconfigureerd, alleen de meest noodzakelijke software is geïnstalleerd. Tevens staan deze systemen in een onafhankelijk netwerk. De configuratie van de systemen en firewall werd door een onafhankelijke instantie gecontroleerd.

Minimaal maandelijks wordt, met behulp van een audittool, een security scan uitgevoerd op de PKIoverheid infrastructuur. De resultaten en maatregelen die voortkomen uit deze scans worde gedocumenteerd.
Tenslotte wordt minimaal één keer per jaar een pentest uitgevoerd op de PKIoverheid internet facing omgeving door een onafhankelijke, ervaren, externe leverancier. De bevindingen en de maatregelen die voortkomen uit deze pentesten, worden ook gedocumenteerd.

# 7. Certificaat-, CRL- en OCSP-profielen

## 7.1 CRL-profielen

### 7.1.1 CRL Burger

| CRL - Burger | | | | |
|---|---|---|---|---|
| **Base attributes** | **OID** | **Critical** | **O/F/R** | **Value** |
| Version | | | Fixed | V2 (X.509v3) |
| SignatureAlgorithm | 1.2.840.113549.1.1.11 | | Fixed | sha256withRSAEncryption |
| Issuer | | | | |
| Issuer.countryName | 2.5.4.6 | | Fixed | NL |
| Issuer.organizationName | 2.5.4.10 | | Fixed | ESG de Electronische Signatuur B.V. |
| Issuer.commonName | 2.5.4.3 | | Fixed | ESG Burger CA - G2 |
| Update | | | | |
| ThisUpdate | | | Required | yymmdd000000Z (date of issuance) |
| NextUpdate | | | Required | yymmdd000000Z (ThisUpdate + 24 hours) |
| revokedCertificates | | | Required | List of revoked certificates |
| **CRL attributes** | **OID** | **Critical** | **O/F/R** | **Value** |
| AuthorityKey Identifier | 2.5.29.35 | False | | |
| KeyIdentifier | | | Fixed | 160 bit SHA-1 hash issuerPublicKey |
| CRLNumber | 2.5.29.20 | False | | |
| CRLNumber | | | Required | sequenced number |
| CRLReason | 2.5.29.21 | False | | |
| CRLReason | | | Optional | reason of revocation |

### 7.1.2 CRL Organisatie

| CRL - Organisatie, Beroep, Services, Server | | | | |
|---|---|---|---|---|
| **Base attributes** | **OID** | **Critical** | **O/F/R** | **Value** |
| Version | | | Fixed | V2 (X.509v3) |
| SignatureAlgorithm | 1.2.840.113549.1.1.11 | | Fixed | sha256withRSAEncryption |
| Issuer | | | | |
| Issuer.countryName | 2.5.4.6 | | Fixed | NL |
| Issuer.organizationName | 2.5.4.10 | | Fixed | ESG de Electronische Signatuur B.V. |
| Issuer.commonName | 2.5.4.3 | | Fixed | ESG Organisatie CA - G2 |
| Update | | | | |
| ThisUpdate | | | Required | yymmdd000000Z (date of issuance) |
| NextUpdate | | | Required | yymmdd000000Z (ThisUpdate + 24 hours) |
| revokedCertificates | | | Required | List of revoked certificates |
| **CRL attributes** | **OID** | **Critical** | **O/F/R** | **Value** |
| AuthorityKey Identifier | 2.5.29.35 | False | | |
| KeyIdentifier | | | Fixed | 160 bit SHA-1 hash issuerPublicKey |
| CRLNumber | 2.5.29.20 | False | | |
| CRLNumber | | | Required | sequenced number |
| CRLReason | 2.5.29.21 | False | | |
| CRLReason | | | Optional | reason of revocation |

## 7.2 OCSP profielen

### 7.2.1 OCSP Burger

| OCSP Responder 1 - Burger | | | | |
|---|---|---|---|---|
| **Base attributes** | **OID** | **Critical** | **O/F/R** | **Value** |
| Version | | | Fixed | V2 (X.509v3) |
| SerialNumber | | | Required | 8 bytes Unique identifier |
| SignatureAlgorithm | 1.2.840.113549.1.1.11 | | Fixed | sha256withRSAEncryption |
| Issuer | | | | |
| Issuer.countryName | 2.5.4.6 | | Fixed | NL |
| Issuer.organizationName | 2.5.4.10 | | Fixed | ESG de Electronische Signatuur B.V. |
| Issuer.commonName | 2.5.4.3 | | Fixed | ESG Burger CA - G2 |
| Validity | | | | |
| Validity not before | | | Required | yymmdd000000Z (date of issuance) |
| Validity not after | | | Required | yymmdd000000Z (not before + 3 years) |
| Subject | | | | |
| Subject.countryName | 2.5.4.6 | | Required | NL |
| Subject.commonName | 2.5.4.3 | | Required | ESG Burger CA - G2 OCSP Responder 1 |
| Subject.organizationName | 2.5.4.10 | | Required | ESG de Electronische Signatuur B.V. |
| subjectPublicKeyInfo | 1.2.840.113549.1.1.1 | | Fixed | RSA (2048 Bits) |
| **Standard Extensions** | **OID** | **Critical** | **Optional** | **Value** |
| AuthorityKey Identifier | 2.5.29.35 | False | | |
| KeyIdentifier | | | Required | 160 bit SHA-1 hash issuerPublicKey |
| SubjectKeyIdentifier | 2.5.29.14 | False | | |
| Key Identifier | | | Required | 160 bit SHA-1 hash subjectPublicKey |
| KeyUsage | 2.5.29.15 | True | | |
| KeyUsage | | | Fixed | digitalSignature |
| certificatePolicies | 2.5.29.32 | False | | |
| CertPolicyId | | | Fixed | 2.16.528.1.1003.1.2.5.4 |
| CPS Qualifier | 1.3.6.1.5.5.7.2.1 | | Fixed | http://cps.de-electronische-signatuur.nl |
| User Notice Qualifier | 1.3.6.1.5.5.7.2.2 | | Fixed | The terms and conditions as mentioned on our website (cps.de-electronische-signatuur.nl), are applicable to all our products and services |
| BasicConstraints | 2.5.29.19 | True | | |
| cA | | | Fixed | False |
| pathlenConstraints | | | Fixed | 0 |
| CRLDistributionPoints | 2.5.29.31 | False | | |
| distributionPoint URI | | | Fixed | http://crl.de-electronische-signatuur.nl/esg/burgercag2.crl |
| extKeyUsage | 2.5.29.37 | True | | |
| extKeyUsage | | | Fixed | id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) |
| **Private Extensions** | **OID** | **Critical** | | |
| ocspNoCheck | 1.3.6.1.5.5.7.48.1.5 | | | |
| ocspNoCheck | | | Fixed | 05 00 (Null) |

### 7.2.2 OCSP Organisatie

| OCSP Responder 1 - Organisatie, Beroep, Services, Server | | | | |
|---|---|---|---|---|
| **Base attributes** | **OID** | **Critical** | **O/F/R** | **Value** |
| Version | | | Fixed | V2 (X.509v3) |
| SerialNumber | | | Required | 8 bytes Unique identifier |
| SignatureAlgorithm | 1.2.840.113549.1.1.11 | | Fixed | sha256withRSAEncryption |
| Issuer | | | | |
| Issuer.countryName | 2.5.4.6 | | Fixed | NL |
| Issuer.organizationName | 2.5.4.10 | | Fixed | ESG de Electronische Signatuur B.V. |
| Issuer.commonName | 2.5.4.3 | | Fixed | ESG Organisatie CA - G2 |
| Validity | | | | |
| Validity not before | | | Required | yymmdd000000Z (date of issuance) |
| Validity not after | | | Required | yymmdd000000Z (not before + 3 years) |
| Subject | | | | |
| Subject.countryName | 2.5.4.6 | | Required | NL |
| Subject.commonName | 2.5.4.3 | | Required | ESG Organisatie CA - G2 OCSP Responder 1 |
| Subject.organizationName | 2.5.4.10 | | Required | ESG de Electronische Signatuur B.V. |
| subjectPublicKeyInfo | 1.2.840.113549.1.1.1 | | Fixed | RSA (2048 Bits) |
| **Standard Extensions** | **OID** | **Critical** | **Optional** | **Value** |
| AuthorityKey Identifier | 2.5.29.35 | False | | |
| KeyIdentifier | | | Required | 160 bit SHA-1 hash issuerPublicKey |
| SubjectKeyIdentifier | 2.5.29.14 | False | | |
| Key Identifier | | | Required | 160 bit SHA-1 hash subjectPublicKey |
| KeyUsage | 2.5.29.15 | True | | |
| KeyUsage | | | Fixed | digitalSignature |
| certificatePolicies | 2.5.29.32 | False | | |
| CertPolicyId | | | Fixed | 2.16.528.1.1003.1.2.5.4 |
| CPS Qualifier | 1.3.6.1.5.5.7.2.1 | | Fixed | http://cps.de-electronische-signatuur.nl |
| User Notice Qualifier | 1.3.6.1.5.5.7.2.2 | | Fixed | The terms and conditions as mentioned on our website (cps.de-electronische-signatuur.nl), are applicable to all our products and services |
| BasicConstraints | 2.5.29.19 | True | | |
| cA | | | Fixed | False |
| pathlenConstraints | | | Fixed | 0 |
| CRLDistributionPoints | 2.5.29.31 | False | | |
| distributionPoint URI | | | Fixed | http://crl.de-electronische-signatuur.nl/esg/organisatiecag2.crl |
| extKeyUsage | 2.5.29.37 | True | | |
| extKeyUsage | | | Fixed | id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) |
| **Private Extensions** | **OID** | **Critical** | | |
| ocspNoCheck | 1.3.6.1.5.5.7.48.1.5 | | | |
| ocspNoCheck | | | Fixed | 05 00 (Null) |

# 8. Conformiteitsbeoordeling

## 8.1 CSO

KPN B.V. is conform ETSI gecertificeerd als CSO. Deze certificatie garandeert dat alle bedrijfsprocessen voor productie van certificaten en voor de online services precies beschreven en gecontroleerd zijn.
De relevante publicaties van KPN B.V., de controle door de auditor van BSI en het door KPN B.V. overlegde certificaat tonen dit aan.

## 8.2 Certificatie

Certificatie audits worden uitgevoerd door BSI. BSI is geaccrediteerd door de Raad van Accreditatie.

# 9. Algemene en juridische bepalingen

## 9.1 Tarieven

Geen nadere bepalingen.

## 9.2 Financiële verantwoordelijkheid en aansprakelijkheid

De aansprakelijkheid van de TSP is geregeld conform artikel 253 BW6.

## 9.3 Vertrouwelijkheid van bedrijfsinformatie

Het is medewerkers verboden op welke wijze dan ook software, documenten of correspondentie of afschriften hiervan, die hij/zij in verband met zijn/haar werkzaamheden bij de opdrachtgever onder zich heeft verkregen, in zijn/haar bezit te hebben, of te houden of te kopiëren, uitgezonderd voor zover en voor zolang dit voor de uitoefening van haar werkzaamheden voor de opdrachtgever is vereist.

Het is medewerkers zowel gedurende als tot 2 jaar na het einde van deze overeenkomst verboden financiële transacties aan te gaan, hetzij middellijk of onmiddellijk, waarmee de zaken van cliënten van opdrachtgever zijn gemoeid, hieronder begrepen het kopen of verkopen van aandelen in vennootschappen welke behoren tot de cliëntenkring van opdrachtgever, wanneer bij deze transacties gebruik wordt gemaakt van door of tijdens de uitoefening van de werkzaamheden verkregen kennis, die niet aan derden bekend is of behoort te zijn.

Indien een medewerker of (rechts-)perso(o)n(en) die namens de medewerker bij een opdrachtgever werkzaamheden verrichten, in welke functie en hoedanigheid dan ook, in strijd met de verplichtingen uit hoofde van het bepaalde in de voorgaande leden handelt, zal de medewerker de opdrachtgever zonder dat enige ingebrekestelling is vereist, voor iedere overtreding een boetesom verbeuren ten bedrage van vijfduizend Euro per overtreding en duizend Euro voor iedere dag dat de overtreding voortduurt, onverminderd het recht van opdrachtgever in plaats van boete volledige schadevergoeding te vorderen, met een maximum van vijftigduizend euro.

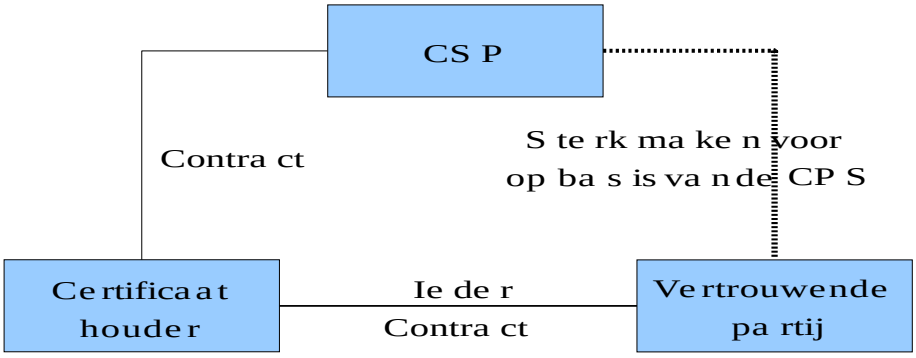
## 9.4 Privacy

ESG de electronische signatuur BV neemt bij opname, verwerking en archivering van persoonsgegevens de relevante wet- en regelgeving stipt in acht. De activiteiten en administratie van ESG zijn aangemeld bij de registratiekamer onder nummer M1321561.

## 9.5 Intellectuele eigendomsrechten

ESG de electronische signatuur BV vrijwaart de abonnee ten aanzien van aanspraken door derden vanwege schendingen van intellectuele eigendomsrechten door ESG. Alle rechten van deze CPS berusten bij ESG de electronische signatuur BV, ongewijzigde kopieën mogen met bronvermelding worden verspreid.

## 9.6 Aansprakelijkheid




### 9.6.1 Persoonsgebonden certificaten

Persoonsgebonden certificaten verlenen een vertrouwende partij zekerheid over de natuurlijke persoon waarmee zij te maken hebben.

### 9.6.2 Services certificaten

Service certificaten verlenen een vertrouwende partij vooral zekerheid over de verbondenheid van een service (apparaat of functie) met de organisatorische entiteit die de service (doet) bedienen.

**De geldigheid van een certificaat dient niet verward te worden met de bevoegdheid van de certificaathouder een bepaalde transactie namens een organisatie te doen. PKIoverheid regelt geen autorisatie; daarvan moet een vertrouwende partij zichzelf op andere wijze overtuigen.**

## 9.7 Beperkingen van garanties

In de Bijzondere voorwaarden van de TSP staat opgenomen hoe, door de TSP en de betrokken partijen, omgegaan dient te worden met de beperkingen in garanties.

## 9.8 Beperkingen van aansprakelijkheid

Geen nadere bepalingen

### 9.9 Schadevergoedingen

Geen nadere bepalingen..

### 9.10 Beëindiging

In de Bijzondere Voorwaarden van de TSP is opgenomen hoe de TSP omgaat met beëindiging.

### 9.11 Persoonlijke berichtgeving

Aanspraak op persoonlijke berichtgeving van aanpassing van enige publicatie is expliciet uitgesloten. De uitzondering hierop is de meldplicht die de TSP heeft aan de PA PKIoverheid. De meldplicht omvat incidenten als ook het verstrekken van informatie over het voornemen om de CA structuur te wijzigen

### 9.12 Wijzigingen

Om op veranderende marktvoorwaarden, veiligheidseisen, wetswijzigingen etc. te kunnen reageren, behoudt de TSP zich het recht voor om wijzigingen en aanpassingen in deze documentatie aan te brengen. Wijzigingen worden op de internetsite www.de-electronische-signatuur aangekondigd en gelden vanaf het moment waarop een nieuwe CPS van kracht wordt. Als in de publicatie van de CPS niet anders is vastgesteld treedt deze twee weken na publicatie in werking. Wijzigingen die uitsluitend betrekking hebben op schrijffouten of die uitsluitend van redactionele aard zijn, worden zonder vooraankondiging aangebracht.

De documentatie ondergaat periodiek, minimaal een keer per jaar, een evaluatie naar aanleiding van de jaarlijkse hercertificering. Iedere belanghebbende kan opmerkingen met betrekking tot de inhoud melden aan de TSP. De bevoegdheid om wijzigingen aan te brengen in de documentatie blijft voorbehouden aan de TSP. Bij elke wijziging van de CPS worden versienummer en datum vernieuwd.

### 9.13 Geschillenbeslechting

In gevallen waarin onenigheid bestaat over het gebruik van de in een certificaat op te nemen namen, beslist de TSP na afweging van de betrokken belangen, voor zover een beslissing niet wordt voorgeschreven door dwingend Nederlands recht of overige toepasselijke regelgeving. Klachten en geschillen kunnen worden voorgelegd aan de directie van de TSP. Deze beslist, gehoord de CSO en indien van toepassing de PA. Deze regeling laat toegang tot de Nederlandse rechter onverlet mits het geschil wordt voorgelegd aan de daartoe bevoegde rechter in het arrondissement Limburg.

### 9.14 Van toepassing zijnde wetgeving

Op alle overeenkomsten is het Nederlands recht van toepassing

### 9.15 Verdere juridische voorzieningen

Geen nadere bepalingen.

### *9.16 Overige bepalingen*

Als één of meerdere bepalingen van het CPS bij gerechtelijke uitspraak ongeldig of anderszins niet van toepassing wordt verklaard, laat dit de geldigheid en toepasselijkheid van alle overige bepalingen onverlet