Dit document is de **Certification Practice Statement** (CPS) voor *ESG-CSP* en bevat de richtlijnen voor het gebruik van de door *ESG-CSP* uitgegeven certificaten. Voor het correct functioneren van het afsprakenstelsel 'PKI voor de overheid' dienen alle betrokkenen zich aan de eisen van het stelsel te conformeren. Op last van de Certificate Policy (CP) van PKI-Overheid is deze CPS-ESG derhalve een onderdeel van de contractuele afspraken over verstrekking, intrekking en gebruik van certificaten en is een aanvulling op de AV (algemene voorwaarden) voor de dienstverlening van *ESG de electronische signatuur BV*.

Inhoudsopgave

1 Dit document

1.1 Naam en identificatie

Dit document is de Certification Practice Statement(CPS-4/04-02-11/10) voor ESG-CSP en bevat de richtlijnen voor het gebruik van de door ESG-CSP uitgegeven certificaten.

1.2 Toegankelijkheid

Inzage in deze informatie is niet onderhevig aan toegangscontrole.

1.3 Beheer

Deze CPS wordt, onder verantwoordelijkheid van de directie, onderhouden door de Chief Security Officer van ESG.

1.3.1 Contactgegevens

Voor informatie over en commentaar op deze CPS kunt u bij deze terecht:

ESG, de Chief Security Officer
Pelmersheideweg 16
6005 PK Weert
CSO@esg4.eu

2 Publicatie en elektronische opslag

De door ESG onderhouden publicaties 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 24 uur weer bereikbaar is.

2.1 www.esg4.eu

ESG-CSP publiceert:

- De volledige inhoud van dit document
- De algemene voorwaarden
- Informatie voor het verkrijgen van een certificaat
- Prijslijst/Tarieven
- Certificaatprofielen
- Informatie met betrekking tot blokkering of intrekking van
  - een certificaat[1]
  - een encryptie sleutel
  - een CA sleutel
- Informatie met betrekking tot wijziging van
  - een encryptie sleutel
  - een CA sleutel

1 Intrekking wordt via email aangekondigd aan betrokkene

- (verdenking van) Fraude met
  - een encryptie sleutel
  - een CA sleutel
- Aankondigingen van relevante wijzigingen[2] van de Certificaat Policy

3 Achtergronden & Overzicht

3.1 PKI (Public Key Infrastructuur)

PKI is een methode om via een willekeurig medium[3] 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 geauthenticeerd, onweerlegbaarheid vastgelegd of kun je erop vertrouwen dat alleen de bedoelde persoon de vertrouwelijke gegevens kan lezen.

3.2 Dienstverlening van ESG

ESG de electronische signatuur BV verzorgt als Certificate Service Provider (CSP) onder de handelsnaam 'ESG-CSP' de Services die een Public Key Infrastructuur in de praktijk bruikbaar maakt. ESG-CSP genereert in een 'veilige omgeving' 'PKI geschikte sleutelparen'. Iedere geheime sleutel wordt direct opgeslagen op een 'veilig medium'. Dit medium, waarvoor ESG-CSP de houder zelf een pin laat kiezen, beantwoordt aan de eisen van het 'exclusieve beheer'. In een 'registratie[4] procedure' verzorgt ESG-CSP de 'betrouwbare koppeling' van een publieke sleutel aan 'betrouwbare identificerende gegevens'. Deze koppelingen worden als 'elektronische certificaten[5]' op het Internet controleerbaar gemaakt.

3.3 Kader van 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 gebruiken te maken van 'de elektronische handtekening'. Daarnaast faciliteert het stelsel 'identificatie op afstand' (authentificatie) 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-CSP heeft zich bij PKIOverheid aangesloten en zich aan het PvE geconformeerd. De services van ESG-CSP voldoen aan alle eisen die door de Nederlandse wet en regelgeving[6] gesteld zijn. Zij leveren daarmee de basis voor het hoogst beschikbare beveiligingsniveau van geautomatiseerde dienstverlening[7]. Zij maken “dat betrouwbare authentificatie mogelijk is zonder onmiddellijke tussenkomst van natuurlijke personen” ofwel “dat machinale controle van identiteit en authenticiteit voldoende

2 Zie ook paragraaf 10.9
3 Iedere vorm van digitale communicatie.
4 Ook wel certificatieprocedure genoemd.
5 Het PvE vereist X509 voor alle uitgegeven certificaten.
6 PvE van PKIOverheid, de wet op de elektronische handtekening;
- SSCD (v1.3.1, 2005-05);
- SUD (v1.2.1, 2005-05) NCP+[2]
- ETSI TS 101 456

7 Waaronder elektronische communicatie

betrouwbaar is voor gebruik in het maatschappelijk verkeer”.
Op de kwaliteit van de ESG-CSP services wordt toezicht gehouden door de PA van PKIOverheid. Ieder jaar wordt de servicekwaliteit van de ESG-CSP services door een onafhankelijke auditor gecontroleerd op basis van de ETSI TS 101 456 eisen en de additionele eisen uit het PvE. Deze audit herbevestigt dat de services van ESG-CSP 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-CSP certificaten met het Nederlandse stamcertificaat.

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

PvE 3a paragraaf 1.4

Het gebruik van certificaten uitgegeven onder deze CP heeft betrekking op communicatie van certificaathouders op persoonlijke titel.

PvE 3c paragraaf 1.4

3.3.1 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-CSP CA-certificaat' 2.16.528.1.1003.1.3.5.3.1(niveau 3) getekend.
2. in het domein 'Burger' het 'staatdernederlandenburgerca-g2'-certificaat. Met dit (niveau 2) certificaat is het 'ESG-CSP Burger-CA-certificaat' 2.16.528.1.1003.1.3.3.1.1 (niveau 3) getekend.

ESG-CSP tekent met deze certificaten de verschillende eindgebruikers certificaten.

3.4 Betrokken Partijen

In het PvE en de CPS van PKIoverheid wordt de volgende gebruikers-gemeenschap onderscheiden; abonnees, certificaatbeheerders, certificaathouders (zowel natuurlijke personen als services) en vertrouwende partijen. Naast de in de CP genoemde betrokkenen beschrijft deze CPS; de CSP, 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.

3.4.1 CSP (Certification Service Provider)

ESG-CSP is de eindverantwoordelijke CSP. Zij verzorgt (provides) services en certificatie op basis waarvan een certificaathouder zich betrouwbaar kan identificeren en authentificeren tegenover een vertrouwende partij. ESG-CSP 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 certificatieprocedure.

3.4.2 CSO (Component Services Organisatie)

CSO voor ESG-CSP is QuoVadis. Deze organisatie zorgt onder verantwoordelijkheid van ESG-CSP voor de certificaat generatie, het revocatie status service en de disseminatie service. Verder beheert zij het 'High Secure' rekencentrum en de infrastructuur voor de productie van cryptografische elementen.

3.4.3 LRA (Local Registration Authority)

Het onmiddellijke contact met aankomende certificaathouders, de certificatieprocedure, is uitbesteed aan LRA's, cq 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.

3.4.4 LRAO (LRA-Officer)

Iedere LRAO is door de CSP opgeleid en vertegenwoordigt de CSP bij de uitvoering van de verificaties en controles voorzien in het hier beschreven stelsel.

3.4.5 Abonnee

De abonnee een,

- natuurlijke persoon die met ESG-CSP een overeenkomst sluit[8] om als certificaathouder publieke sleutels te laten certificeren.
- rechtspersoon die met ESG-CSP een overeenkomst sluit[9] om namens een of meer certificaathouders publieke sleutels te laten certificeren.

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

3.4.6 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 authentificeren. Bij servicegebonden certificaten wordt de verantwoordelijkheid van de certificaathouder gedragen door een certificaat-beheerder.

3.4.6.1 Persoon

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.

3.4.6.2 Service

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.

3.4.7 Certificaatbeheerder[10]

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.

3.4.8 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.

3.5 Certificaat gebruik

ESG-CSP is Certificaat Service Provider en sluit als zodanig een contract met een abonnee ten behoeve van een certificaathouder[11]. In dit contract staat een artikel conform artikel 253 van Boek 6 BW. Dit artikel regelt de aansprakelijkheid van ESG-CSP 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.

8 In het domein 'Burger'
9 In het domein 'Overheid en organisatie'
10 In het domein 'Burger' komt certificaatbeheer niet voor.
11 In het domein 'Burger' zijn abonnee en certificaathouder dezelfde.

3.6 Certificate Policies

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

OID[12]	Type
2.16.528.1.1003.1.2.5.1	Het persoonsgebonden authenticiteitscertificaat, 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 vertrouwelijkheidscertificaat, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid
2.16.528.1.1003.1.2.5.4	Het service gebonden authenticiteitscertificaat, 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 vertrouwelijkheidscertificaat, wordt gebruikt voor het beschermen van de vertrouwelijkheid van gegevens die worden uitgewisseld en/of opgeslagen in elektronische vorm
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

4 Identificatie and Authenticatie (I&A)

4.1 Namen[13]

Een in het certificaat opgenomen naam moet de certificaathouder eenduidig identificeren en begrijpelijk zijn. Pseudoniemen zijn niet toegestaan.

- De schrijfwijze van een Persoonsnaam moet met de schrijfwijze in het legitimatiebewijs overeenkomen en mag niet met leestekens, bijvoorbeeld trema, gewijzigd zijn.
- De naam die in een certificaat aan een Certificaathouder wordt toegekend zal te allen tijde uniek zijn voor deze Certificaathouder en niet worden uitgegeven aan andere certificaat-houders. De rechten op deze naam dienen te worden aangetoond.
- Indien dezelfde naam vaker voorkomt, wordt met een numeriek achtervoegsel het onderscheid kenbaar gemaakt.

12 Een OID (Object Identifier) is een rij getallen die op ondubbelzinnige wijze en permanent een object aanduiden

13 Zie ook paragraaf 10.11

4.2 Vaststellen van de identiteit

ESG-CSP stelt, op basis van een aanvraag conform het contract met de abonnee, een LRAO aan middels een opdracht voor een registratieprocedure. De LRAO zal de voorgeschreven verificaties en controles uitvoeren.

De certificaathouder, respectievelijk beheerder, dient in een face2face procedure door een LRAO geïdentificeerd te worden. De LRAO dient alle relevante gegevens te controleren en vast te stellen dat geplaatste handtekeningen in overeenstemming zijn met de handtekening op het overlegde identiteitsbewijs. Dit identiteitsbewijs, een geldig paspoort of vergelijkbaar document dat voldoet aan de eisen uit de Wet op de Identificatieplicht(WID), wordt door de LRAO gecontroleerd en gekopieerd.

4.3 I&A bij vernieuwing van een 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.

4.4 I&A bij intrekking van een certificaat

Voor het authentificeren van de intrekkingsbevoegdheid wordt het tele-password gebruikt.

5 Certificaat

5.1 Aanvraag

Certificaatdienstverlening is gebaseerd op een contract van ESG-CSP met een abonnee. Een abonnee die dit contract heeft gesloten kan bij ESG-CSP kan een aanvraag doen een certificatieprocedure te starten.

5.2 Certificatieprocedure

De Certificatieprocedure moet face2face worden gevolgd bij een door ESG-CSP aan te stellen LRAO (Local Registration Authority Officer). Een aankomende certificaathouder, respectievelijk beheerder, kan zijn voorkeur voor een LRAO kenbaar maken.

5.2.1 Identificatie

Na vaststelling van de identiteit van de aanvrager door de LRAO(zie 4.2) worden gezamenlijk de formulieren[14] ingevuld. Waar mogelijk worden de vereiste originele documenten als bijlagen in het dossier opgenomen. In gevallen waar dit onmogelijk is (identiteitsbewijs en dergelijke) wordt een door de LRAO gewaarmerkte kopie gebruikt.

5.2.2 Vaststellen van de certificaatgegevens

Na deze identificatie worden de gegevens voor het certificaat vastgesteld en geverifieerd. De gegevens die in een certificaat moeten, respectievelijk kunnen, worden opgenomen zijn gespecificeerd in de certificaatprofielen.

5.2.3 Vaststellen van de organisatie gegevens

Bij certificaten in de domeinen 'Overheid en bedrijven' en 'Organisatie' dienen de gegevens van de abonnee expliciet in het certificaat te worden opgenomen in een daartoe aangewezen veld. In het domein 'Burger' is de abonnee gelijk aan de certificaathouder en komt dat veld in de certificaten niet voor.

5.2.4 Uitgifte keymateriaal

Tijdens de face2face certificatieprocedure wordt aan de aanvrager een smartcard[15] uitgereikt waarop de sleutel-paren ten behoeve van PKI aanwezig zijn. De smartcard is gelocked en kan alleen worden ontsloten door personificatie, dat wil zeggen het initialiseren van een PIN. De aankomende certificaathouder bevestigt bij ontvangst de overdracht van het privé sleutelmateriaal en het feit dat hij de controle en verantwoordelijkheid voor de SSCD op zich

14 Zie de set Formulieren

15 Deze smartcard is gecertificeerd als SSCD (Secure Signature Creation Divice)

neemt.

5.2.5 Indienen aanvraagdossier[16]

De LRAO verzorgt het indienen van het dossier, in een verzegelde envelop beveiligd[17], bij ESG-CSP. Deze controleert de documenten-set op compleetheid, geloofwaardigheid en zonodig op authenticiteit en verwerkt de gegevens ten behoeve van van certificaatproductie en disseminatie. Bij aanvraag van servercertificaten met een domeinnaam, controleert de LRAO bij de erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) of de certificaatbeheerder gemachtigd is te handelen inzake de domeinnaam.

5.2.6 Productie & uitgifte

Na acceptatie van de aanvraag worden de op de formulieren bevestigde gegevens via een, met een SSCD, beveiligde verbinding in het CA systeem ingebracht. Na controle van deze gegevens wordt een certificaat geproduceerd. Dit certificaat wordt adequaat versleuteld (in ondermeer de public key van het certificaat) aan de aanvrager per E-mail toegezonden. Pas als de CSO (Certificaat Service Organisatie) een correct ondertekende ontvangstbevestiging van, respectievelijk namens, de certificaathouder heeft ontvangen neemt de CSO het certificaat in de registers op en verleent het daarmee zijn geldigheid.

5.3 Controle & acceptatie

De certificaathouder, respectievelijk certificaatbeheerder, moet een ontvangen certificaat, met daartoe geëigende middelen, op juistheid en volledigheid controleren. Hij moet ontvangst en acceptatie van het certificaat aan de CSP bevestigen met een handtekening. Certificaten zijn pas geldig nadat zij in het on-line register geactiveerd zijn en worden pas geactiveerd wanneer de officiële acceptatie binnen is. De CSP dient onverwijld via een intrekkingsverzoek van een onjuist certificaat op de hoogte te worden gebracht.

5.4 Sleutelpaar en Certificaat gebruik

Normaliter zijn certificaten 3 jaar geldig, Als de levensduur van het CA-certificaat dit toelaat is op verzoek een levensduur tot 5 jaar mogelijk. 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 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 CSP kenbaar te maken.

5.5 Vernieuwen

zie paragraaf 4.3.

5.6 Re-key

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

5.7 Aanpassen

ESG-CSP 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

16 Zie de set Formulieren

17 Alle persoonlijke gegevens worden conform de Wet Bescherming Persoonsgegevens verwerkt, verzonden en bewaard.

Abonnee verplicht het betrokken Certificaat onmiddellijk in te trekken. Indien gewenst kan de Abonnee daarna een nieuw Certificaat aanvragen.

5.8 Intrekking en Opschorting

De geldigheid van een certificaat kan worden geblokkeerd. Opschorting van een certificaat is niet toegestaan. Wanneer een omstandigheid genoemd onder 5.8.2 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.

5.8.1 Intrekkinghotline +31 800 ESGKEYS (+31 800 3745397)

Intrekking van een certificaat dient telefonisch door een bevoegd persoon te worden aangevraagd. Dit kan via de Intrekkinghotline die 7 dagen per week, 24 uur per dag bereikbaar is: +31 800 ESGKEYS (+31 800 3745397 of +31 495 566355).

Binnen maximaal vier (4) uur na een geauthentificeerde intrekkingsaanvraag zal de CSP ESG BV het certificaat intrekken en een nieuwe CRL uitgeven.

5.8.2 Omstandigheden die leiden tot Intrekken

De volgende omstandigheden leiden tot intrekking van een certificaat:

1. Wettelijk voorschrift;
2. Compromittering van de CA.
3. Verlies (mogelijke diefstal) of compromittering van de SSCD en/of SUD;
4. Verlies (mogelijke diefstal) of compromittering van het PIN;
5. Het certificaat is niet meer correct (kwalificaties zijn niet meer juist);
6. De gecertificeerde (privé)sleutel of de daarvoor gebruikte algoritmen voldoen niet meer aan de actuele eisen;
7. De privé sleutel is aangetast;
8. Overlijden van de Certificaathouder;
9. De relatie tussen abonnee en certificaathouder is veranderd[18].
10. Ontbinding of faillissement van de rechtspersoon van abonnee[19];

Certificaten waarvoor een van bovenstaande omstandigheden geldt mogen niet worden gebruikt.

5.8.3 Intrekkingsbevoegdheid

De intrekking van een certificaat kan worden gelast door de:

- abonnee
- certificaathouder[20] (of zijn wettelijke vertegenwoordigers)
- een door de certificaathouder vertegenwoordigde derde waarvan de vertegenwoordiging in het certificaat vermeld staat.
- ESG-CSP.

5.8.4 Herroepen van een Intrekking

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

5.9 Online controleservices

Vertrouwende partijen kunnen in redelijkheid op een certificaat vertrouwen als zij een adequate (on-line) 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.

5.9.1 CRL[21] (Blokkeringslijst)

Geblokkeerde certificaten worden in de blokkeringslijst (CRL) opgenomen. De CRL wordt dagelijks en binnen maximaal 4 uur na elke blokkering 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.

---

18 In het domein 'Burger' kan deze situatie zich niet voordoen.
19 In het domein 'Burger' is deze situatie voor de certificaten irrelevant.
20 In het domein 'Burger' is de abonnee gelijk aan de certificaathouder.
21 Specificaties van deze CRL zijn via de ESG-website beschikbaar.

5.9.2 Geldigheidscontrole via OCSP[22]

De geldigheid van een certificaat kan ook via het OCSP conform RFC2560, zonder 'precomputed responses', gecontroleerd worden.

5.10 Duur overeenkomst

De duur van een overeenkomst met een abonnee is in principe onbeperkt.

5.11 Sleutelbewaring en herstel

CSP ESG biedt deze dienst niet aan.

6 Veiligheid

6.1 Fysieke veiligheid

6.1.1 Vestiging Weert

ESG-CSP heeft de navolgende maatregelen genomen voor de veiligheid van haar vestiging in Weert.

6.1.1.1 Terrein

ESG-CSP is gevestigd op een terrein in het bedrijvenpark Kampershoek te Weert. Dit park is beveiligd d.m.v. slagbomen met een meldsysteem. Dit meldsysteem is verbonden met een meldkamer. De slagbomen zijn maandag t/m zaterdag tussen 6:30 en 22:00 uur open. Zondag is het bedrijven terrein gesloten. Uitsluitend personen die door het Bestuur Kampershoek zijn aangemeld bij de meldkamer kunnen buiten de genoemde tijden het park op.
Het terrein is beveiligd d.m.v. een elektrische rolpoort en een stalen omheining rondom. De rolpoort is aan de voorzijde en voorzien van een zogenaamde Myfare antenne. De poort is geopend tussen 7:45 en 18:15 uur en is in het weekend gesloten. D.m.v. een speciale druppel, alleen uitgegeven aan de directie, kan deze rolpoort buiten de normale kantoor uren geopend en gesloten worden. De code om de toegangspoort handmatig te openen is uitsluitend bij de directie bekend.

6.1.1.2 Gebouw

De hoofdingang van het gebouw is 24 uur per dag 7 dagen in de week op slot. Personeel en bezoekers kunnen zich melden bij het console rechts naast de ingang. De deur is op afstand elektrische te openen. Bezoekers krijgen slechts toegang indien vooraf een afspraak is gemaakt en bevestigd. Het gebouw is dusdanig geconstrueerd dat er slechts twee toegangen zijn; Directie en bezoekers en een personeelsingang. Alle wegen naar buiten zijn kort en direct gericht op de hoofdingang. De ramen zijn voorzien van dubbel speciaal glas.
Het gebouw is voorzien van een alarmsysteem met bewegingsmelders. Elke ruimte op de begane grond is voorzien van een aparte bewegingsmelder. Het alarmsysteem is direct aangesloten op een meldkamer d.m.v. een telefoonlijn en wordt door middel van een code in- en uitgeschakeld. Deze code is uitsluitend bij de directie bekend. ESG-CSP heeft een eigen code en kan daarmee de bewegingsmelder op de 4de etage uitschakelen. In het gebouw is een tweede alarmsysteem, een zogenaamd schreeuwalarm. Bij een overval kan het personeel d.m.v. een drukknop dit alarm inschakelen. Bij het inschakelen wordt de meldkamer gealarmeerd en meteen een microfoon in werking gesteld zodat de meldkamer direct kan horen wat er aan de hand is en gericht actie ondernemen.

6.1.1.3 Kantoor

De toegang naar de kantoren is via afgesloten toegangsdeuren. De sloten op deze deuren zijn anders dan de sloten op de andere deuren in het gebouw. Slechts de directie en één persoon van het secretariaat heeft een sleutel van deze sloten. De Serverruimte met daarin de apparatuur en brandkast is voorzien van een apart slot met een aparte sleutel. De directie heeft één sleutel. De andere sleutels zijn in een sleutelkast opgeborgen. Deze kast wordt na 18:00 afgesloten en blijft ook in het weekend en gedurende feestdagen gesloten. Er is een sleutelprocedure voor het gebruik en opslag van de sleutels. De sleutel van de sleutelkast ligt in een afgesloten archiefkast.

22 Specificaties van deze dienst zijn op de ESG-website beschikbaar.

Deze archiefkast wordt beheerd door het secretariaat.

6.1.1.4 Serverruimte

De Serverruimte, waar de registratie van de personen en de opslag van documenten plaats vindt wordt de toegangsdeur voorzien van een elektronisch slot met een keypad. Nu is deze deur voorzien van een apart slot met een eigen sleutel. Gedurende de kantooruren is deze deur geopend. Na deze tijd, in het weekend en feestdagen is deze deur gesloten. De code van het keypad is uitsluitend bij de directie bekend. In dit kantoor is tevens de kluis geplaatst.

6.1.1.5 Documenten

Alle documenten die met registratie en uitgifte van certificaten te maken hebben, alsmede alle contracten met LRA's en toeleveranciers, handleidingen, beschrijvingen, CPS en aanverwante documenten worden in de kluis opgeslagen. De kluis is altijd gesloten en uitsluitend te openen d.m.v. een sleutel. Slechts twee personen hebben toegang tot deze kluis, de sleutel wordt in aparte sleutelkast opgeborgen. Digitale documenten worden opgeslagen op een individuele ESG Server, uitsluitend ESG Personeel heeft toegang tot deze Server.

6.1.1.6 Voorraad

Alle door ESG gehouden voorraad van kaartlezers en SSCD[23] is opgeslagen in een afgesloten kast in de serverruimte.

6.1.2 Vestiging CSO

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

6.1.2.1 Locatie en constructie

De CSO voert haar CA dienstverlening uit vanaf een beveiligd datacenter, gevestigd in een gebouwencomplex te Bermuda. Dit centrum voldoet aan de strikte regels en hoge eisen opgesteld door een onafhankelijk gecertificeerde partij. Normen omvatten: Gecertificeerde BS-EN 1047 toepassing, gesteund door ISO9000/1/2 aansprakelijkheidsverzekering; brand (volgens DIN 4102 F90 standaard) met een automatisch FM200 blussysteem; rook en vochtigheid (volgens DIN 18095 standaard); overval en vandalisme (ET2 volgens DIN 18103 standaard); en bescherming tegen elektromagnetische invloeden en straling (zoals een elektromagnetische puls).

6.1.2.2 Toegang

QuoVadis staat toegang tot haar beveiligde operationele omgeving enkel toe aan bevoegde personen, wiens bewegingen binnen de instelling worden opgeslagen in een log-file dat regelmatig wordt ge-audit. De toegang wordt gecontroleerd door een combinatie van passen en biometrische identificatie.

6.1.2.3 Power- en Airconditioning

De QuoVadis beveiligde operationele omgeving is aangesloten aan een standaard energievoorziening. Alle kritieke componenten zijn aangesloten aan een UPS-unit, om tijdens de eventuele uitval van elektra de ongecontroleerde shutdown van een systeem te voorkomen.

6.1.2.4 Blootstelling aan water

De QuoVadis beveiligde operationele omgeving biedt bescherming tegen water. Het is gevestigd op een hoger gelegen etage waar de vloeren zijn verhoogd. Ook zijn de muren gesealed en houdt het centrum zich aan de veiligheidseisen opgesteld in DIN 18095.

6.1.2.5 Bescherming en preventie tegen brand

De QuoVadis beveiligde operationele omgeving biedt bescherming tegen brand volgens de richtlijnen van DIN 4102 F9 met een automatisch FM200 blussysteem.

6.1.2.6 Media opslag

Alle magnetische media die informatie betreffende QuoVadis PKI bevatten, waaronder back-up files, worden opgeslagen in opslagvoorzieningen, kasten en brandvrije kluizen met beschermings-

23 SSCD zijn beveiligd met de NULLPIN.

mogelijkheden betreffende vuur en elektromagnetische onderbreking (EMI) en deze bevinden zich in de QuoVadis operationele omgeving of op een externe beveiligde locatie.

6.1.2.7 Afval verwerking

Papieren documenten en magnetische media welke vertrouwelijke QuoVadis of commercieel gevoelige informatie bevatten, worden beveiligd vernietigd door middel van:

- In het geval van magnetische media
  - fysieke schade of gehele vernietiging van de betreffende informatiebron;
  - gebruik van een goedgekeurd apparaat voor het wissen of overschrijven van de informatie; en
- In het geval van gedrukte informatie, wordt het document versnipperd of vernietigd door op een daarvoor goedgekeurde manier.

6.1.2.8 Externe back-up

Een externe locatie (CSO) wordt gebruikt voor opslag en behoud van back-up software en data (registratiegegevens). De externe locatie:

- is 24 uur per dag en 7 dagen per week beschikbaar voor geautoriseerd personeel, met als doel het terughalen van software en data. De data blijft 7 jaar beschikbaar.
- heeft geschikte niveaus van fysieke beveiligingsmaatregelen getroffen (software en data zijn bijvoorbeeld opgeslagen in vuurvaste kluizen en opslagmogelijkheden die zich bevinden achter toegangsgecontroleerde deuren in omgevingen die alleen toegankelijk zijn voor geautoriseerd personeel).

6.2 Procedurele veiligheid

6.2.1 Vestiging Weert

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.

6.2.2 Vestiging Bermuda

Om zeker te stellen dat geen enkel individu de beveiliging kan omzeilen, zijn verant-woordelijkheden verdeeld over meerdere rollen. Dit geeft een systeem van “checks and balances”. Bijvoorbeeld CA sleutelpaargeneratie, initialisatie van een Root CA of initialisatie van een uitgevende CA vereist de actieve participatie van ten minste twee vertrouwde individuen. Bijzonder gevoelige handelingen vereisen tevens de actieve participatie van hoger management.

De gedefinieerd rollen zijn:

- Toezichthouder die verantwoordelijk is voor het houden van toezicht en het geven van een onafhankelijk oordeel over de wijze waarop de bedrijfsprocessen zijn ingericht en over de wijze waarop aan de eisen ten aanzien van de betrouwbaarheid is voldaan.
- Chief Security Officer, verantwoordelijk voor het verifiëren van de integriteit van de Certificatieautoriteiten en hun verrichtingen en configuraties.
- Certification Authority Officer, verantwoordelijk voor CA hardware en software zowel als de generatie en ondertekening van CA sleutels.
- Registration Authority Officer, verantwoordelijk voor het uitvoeren van acties voor de registratieautoriteit en de interface met de uitgevende CA.
- Systeembeheerder, verantwoordelijk voor het beheer van de systemen.

Elk individu dat een vertrouwelijke rol vervult dient een adequaat Certificaat, opgeslagen op een SSCD, te gebruiken om zichzelf te authenticeren aan de Certificaat-server of -repository. Er zijn per vertrouwelijke rol minstens twee personen beschikbaar, met uitzondering van de rol die audit logs verifieert en analyseert. De volledige procedurele beveiliging wordt beschreven in interne documenten.

6.3 Personele veiligheid

De betrouwbaarheid van het personeel dat bij ESG-CSP of haar CSO werkzaam is, wordt gecontroleerd. Personeel wordt regelmatig bijgeschoold. Bij kritische processen wordt een strikte rollenscheiding in acht genomen en naar alle personen die een vertrouwelijke rol vervullen is antecedentenonderzoek verricht. ESG-CSP is desondanks niet aansprakelijk voor gedrag van

werknemers dat buiten hun aanstelling ligt en waarover ESG-CSP geen controle heeft, inclusief, maar niet beperkt tot, spionage, sabotage, misdadig gedrag of kwaadwillige tussenkomst. Ongeoorloofd gedrag door personeel van ESG word van geval tot geval doorde directie beoordeeld . Zonodig worden disciplinaire maatregelen getroffen .

6.3.1 Kwalificaties

Personeel is gecontroleerd op:

- Werkervaring
- Professionele referenties
- Strafblad

ESG-CSP en haar CSO voorzien alle personeel van de benodigde materialen om functie en plichten te kunnen vervullen.

6.3.2 Geheimhoudingsverklaring

ESG-CSP doet al het mogelijke om te zorgen dat het personeel vertrouwelijke informatie adequaat behandelt. Teneinde het personeel hiervan bewust te laten zijn, worden geheimhoudings-verklaringen ondertekend.

6.4 Logs & Protocollen

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 CSP gemeld. Indien noodzakelijk via de blokkeringshotline.

6.4.1 Geregistreerde gebeurtenissen

De data die worden gelogd omvatten, maar zijn niet beperkt tot;

- Alle gebeurtenissen relevant bij de generatie van CA sleutelparen, inclusief alle gebruikte configuratiegegevens bij dit proces
- Alle gebeurtenissen relevant bij het registratieproces van een Certificaat
- Alle gebeurtenissen relevant bij de verspreiding van een Certificaat
- Alle gegevens relevant voor de publicatie van de Digitale Certificaten
- Alle gegevens relevant voor de publicatie van intrekkingslijsten
- Alle herroepingdetails van een Certificaat, inclusief de reden van intrekking
- Alle gebeurtenissen relevant bij beheer van de beveiligde omgeving
- Alle netwerkverkeer van en naar vertrouwde machines
- Alle wijzigingen in de configuratie van de back-up
- Alle gebeurtenissen relevant bij het back-upproces
- Alle aspecten van de installatie van nieuwe of bijgewerkte software.
- Alle aspecten van hardware updates.
- Alle aspecten van shutdown en restart.
- Tijd en datum van log dumps.
- Tijd en datum van de dump van transactiearchieven.
- Veranderingen van het beveiligingsprofiel.

Alle log-entries worden van een time-stamp voorzien. Deze is gebaseerd op een betrouwbare tijdbron. De integriteit van de logs wordt beschermd door het maken van een dagelijkse back-up on-site en regelmatige opslag op een afzonderlijke locatie.

6.5 Archivering

Alle papieren documenten bedoeld voor aanvraag, controle en productie van een certificaat worden in het archief van ESG-CSP opgeslagen en 35 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 backups worden gearchiveerd. Deze archieven zullen worden behouden en beschermd tegen wijziging of vernietiging voor een periode van 11 (elf) jaar. 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.

6.5.1 Toegang tot het archief

Certificaathouders mogen hun eigen registratiegegevens inzien. Op verzoek zal ESG-CSP deze gegevens toegankelijk maken. Daarnaast kan ESG-CSP 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.

6.6 Vernieuwing CA-sleutel

De geldigheid van de CA-sleutel is bepaald door PKIoverheid. Voordat met de bestaande CA-sleutel geen gebruikerscertificaten met voldoende looptijd[24] meer kunnen worden uitgegeven, zal ESG-CSP een nieuwe sleutel in gebruik nemen. 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.

6.7 Sleutel-compromittatie & calamiteiten

ESG-CSP heeft een calamiteitenplan, waarvan het QuoVadis bedrijfscontinuïteitsplan deel uitmaakt, en zal eventuele calamiteiten zoveel mogelijk minimaliseren. De plannen omvatten ondermeer:

- Procedures voor het reageren 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 waarborgen van de bedrijfscontinuïteit na een ramp.

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

6.7.1 Informatieverspreiding

ESG-CSP 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 ESG-CSP de PA (Policy Authority) 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.

6.8 Beëindiging van de service

De Certificate Service activiteiten kunnen, met in achtneming van de wettelijke bepalingen, eenzijdig door ESG-CSP stopgezet worden. Een voorgenomen stopzetting wordt, tenminste 2 maanden vóór de stopzetting, aan zowel de OPTA, GBOoverheid, 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 geblokkeerd.

6.9 Technische veiligheid

6.9.1 Sleutelparen

De ESG-CSP gebruikte sleutelparen worden geproduceerd op een gecertificeerd systeem in een afgeschermde ruimte bij de kaartleverancier. Privé-sleutels worden direct op een SSCD[25], respectievelijk een SUD, opgeslagen, er worden geen kopieën achtergehouden. Sleutels zijn sha256RSA van tenminste 2048 bits. 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.

24 Normaliter drie jaar; er kan sprake zijn van een afwijkende looptijd.
25 Meestal een smartcard

6.9.2 Veiligheid van privé sleutels

De privesleutels van de CA bestaan uitsluitend in de HSM, FIPS 140-2 niveau 3. Zij zijn sha256RSA sleutels van minimaal 2048 bits. De veiligheid van uit te geven prive-sleutels wordt beschermd door ze uitsluitend[26] op smartcard te leveren. Sleutellengte wordt bepaald door de certificaat profielen, maar is minimaal 2048 bits.

6.9.2.1 SSCD (Smartcard)

Persoonsgebonden certificaten mogen uitsluitend gebruikt worden in combinatie met een SSCD, een 'geschikt device'. Voor service certificaten kunnen ook ten behoeve van een HSM (High Secure Module) geleverd worden. Tijdens de 'certificatie-bijeenkomst' wordt aan de aankomende certificaathouder een smartcard uitgereikt. Deze smartcard voldoet aan alle eisen van een 'geschikt device' en bevat de privé sleutels die de basis vormen voor de beveiliging. De privésleutels staan in het beveiligde deel van de kaart, de publieke sleutels zijn op de kaart beschikbaar in een dummy-certificaat en zijn tevens opgenomen in de administratie van de CSP[27].

6.9.2.2 Zero- of NULL-PIN procedure

Bij levering van de smartcard is de zogenaamde Zero- of NULL- PIN procedure geactiveerd. Dit patent van de Duitse Telesec maakt het mogelijk vast te stellen dat de beveiligde functies van de kaart die door de PIN worden beschermd, nog nooit zijn gebruikt. Bij de productie van de kaart is een PIN met een default initiële waarde gegenereerd. Om reden van backward-compatibiliteit heeft deze PIN 6 bytes '00' (hexadecimaal), hier komt de naam Zero-PIN vandaan. Om de beveiligde functies van de kaart te gebruiken moet de gebruiker allereerst het commando ' CHANGE REFERENCE DATA' uitvoeren om de PIN te wijzigen ic te initialiseren. Dit commando is natuurlijk beschermd met de PIN maar deze is in dit stadium '000000000000' (hexadecimaal). Vanaf het moment dat de PIN is gezet, kan hij niet meer naar de initiële waarde worden teruggezet. Dit alles betekent dat de gebruiker kan vaststellen dat de beveiligde functies nooit waren gebruikt als de Zero-PIN geldig was bij ingebruikname. Deze procedure maakt het verzenden van een PIN-brief overbodig, en bespaart zo de kosten en de tijd van administratieve inspanning.

6.9.3 Overige aspecten van sleutelbeheer

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-CSP downloadable. Alle uitgegeven publieke sleutels worden 7 jaar in administratie gehouden. ESG-CSP slaat privé sleutels alleen op de SSCD/SUD op en heeft derhalve na uitreiking van de SSCD geen private keys meer onder zich.

6.9.4 PIN

De aankomende certificaathouder is volledig verantwoordelijk voor de beveiliging van zijn eigen smartcard. De geleverde smartcard kent de zogenaamde 'Zero- of NULL-PIN procedure[28]'. Het bij de eerste activering van de kaart gebruikte PIN wordt het geldende PIN van de smartcard. De aankomende certificaathouder dient te zorgen dat hij deze eerste activering direct en persoonlijk met een zelfbedachte PIN uitvoert. Deze PIN is minimaal 6 alfanumerieke karakters groot. Omdat optimale beveiliging een kaartlezer met eigen PINpad vereist wordt normaliter een numerieke PIN gebruikt. Door het uitvoeren van de personificatie neemt de aankomende certificaathouder de controle over en de verantwoordelijkheid voor de beveiliging van zijn smartcard. Op geen moment mag een certificaathouder het PIN aan een ander bekend maken. ESG-CSP is niet op de hoogte van het PIN en aanvaardt derhalve geen enkele aansprakelijkheid voor misbruik van een PIN. De gebruikte SSCD kent de mogelijkheid voor specifieke functies een SUB-PIN te definiëren. De certificaathouder kan daarmee een deblokkeringscode van de gebruikscode scheiden. ESG-CSP ondersteunt deze mogelijkheid echter niet.

6.9.5 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

26 In bijzondere gevallen kan voor service sleutels een uitzondering worden gemaakt.
27 De Public key is daar gekenmerkt met kaartnummer en container-id.
28 Zie paragraaf 6.9.2.2.

voldoen aan FIPS 140-2 niveau 3 en/of aan EAL 4. Toegang tot de modules is beperkt met het gebruik van smartcards .

6.9.6 Life Cycle Security Controls

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/ISO IS15408 normen. De Chief Security Officer verifieert periodiek de integriteit van de componenten.

6.9.7 Netwerktechnische veiligheidsmaatregelen

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. De configuratie van de systemen en firewall werd door een onafhankelijke instantie gecontroleerd.

6.9.8 Timestamping

De structuur en de inhoud van de Time-Stamp Policy zijn in overeenstemming met ETSI TS 101.023, Elektronische handtekeningen en infrastructuren (ESI) en de beleidsvereisten voor Time-Stamping Authorities.

7 Certificaat Profielen

7.1 Overheid & Bedrijven – Authenticiteit

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS (certificaat creatie datum / tijd)	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Bedrijfsnaam	O=	Var
Organizational Unit (OU)	Afdeling	OU=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Digital signature (1000 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.1	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our	Fixed

		products and services.	
Subject Altname			
Othername SSO	Microsoft UPN voor single sign on	user@domain	Var
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Extended Key Usage	AnyExtendedKeyUsage	OID 2.5.29.37.0	Var
msSmartcardLogin	Microsoft smartcard logon	OID 1.3.6.1.4.1.311.20.2.2	Var
codesigning	Code signering	OID 1.3.6.1.5.5.7.3.3	Var
emailprotection	Email beveiliging	OID 1.3.6.1.5.5.7.3.4	Var
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

7.2 Overheid & Bedrijven – Onweerlegbaarheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Bedrijfsnaam	O=	Var
Organizational Unit (OU)	Afdeling	OU=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Subject Key Identifier van CA certificaat	SubjectKeyIdentifier of ESG CA – G2 certificate	Fixed
Subject Key Identifier	ID van sleutel certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Non-Repudiation (0100 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.2	Fixed
Webadres		http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of	Fixed

		certificate request	
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var
QcStatement	Verklaring Gekwalificeerd certificaat	0.4.0.1862.1.1	Fixed

7.3 Overheid & Bedrijven – Vertrouwelijkheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Bedrijfsnaam	O=	Var
Organizational Unit (OU)	Afdeling	OU=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Subject Key Identifier van CA certificaat	SubjectKeyIdentifier of ESG CA – G2 certificate	Fixed
Subject Key Identifier	ID van sleutel certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	• KeyEncipherment • dataEncipherment • keyAgreement (0011 1000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.3	Fixed
Webadres		http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed

Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

7.4 Services – Authenticiteit

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Bedrijfsnaam	O=	Var
Organizational Unit (OU)	Afdeling	OU=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Digital signature (1000 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.4	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
User Notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername SSO	Microsoft UPN voor single sign on	user@domain	Var
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Extended Key Usage			
Smartcard Logon	Microsoft smartcard logon	(OID 1.3.6.1.4.1.311.20.2.2)	Var
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

7.5 Services – Vertrouwelijkheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Bedrijfsnaam	O=	Var
Organizational Unit (OU)	Afdeling	OU=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)		• KeyEncipherment • dataEncipherment • keyAgreement (0011 1000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.5	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
User Notice	Gebruikersmelding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Extended Key Usage			
Authority Info Acces	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Acces	Extra info over de certificaathouder	OID, Generalname	Var

7.6 Services – Server

Veld	Inhoud		
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed

Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Bedrijfsnaam	O=	Var
Organizational Unit (OU)	Afdeling	OU=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	Sleutelgebruik	• DigitalSignature • keyEncipherment • keyAgreement (1010 1000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.6	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
User notice	Gebruikersmelding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Extended Key Usage			
Authority Info Acces	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Acces	Extra info over de certificaathouder	OID, Generalname	Var

7.7 Burger – Authenticiteit

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG Persoonlijk CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed

Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS (certificaat creatie datum / tijd)	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG Persoonlijk CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Digital signature (1000 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.3.1	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.3.1.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgpersooncag2.crl	Fixed
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

7.8 Burger – Onweerlegbaarheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG Persoonlijk CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280,	Fixed

		RFC 3279	
Extensions			
Authority Key Identifier	Subject Key Identifier van CA certificaat	SubjectKeyIdentifier of ESG Persoonlijk CA – G2 certificate	Fixed
Subject Key Identifier	ID van sleutel certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Non-Repudiation (0100 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.3.2	Fixed
Webadres		http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.3.1.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgpersooncag2.crl	Fixed
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var
QcStatement	Verklaring Gekwalificeerd certificaat	0.4.0.1862.1.1	Fixed

7.9 Burger – Vertrouwelijkheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG Persoonlijk CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Subject Key Identifier van CA certificaat	SubjectKeyIdentifier of ESG Persoonlijk CA – G2 certificate	Fixed
Subject Key Identifier	ID van sleutel certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	• KeyEncipherment • dataEncipherment • keyAgreement (0011 1000)	Fixed
Certificate Policies			

OID	Object Identifier	2.16.528.1.1003.1.2.3.3	Fixed
Webadres		http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.3.1.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgpersooncag2.crl	Fixed
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

7.10 Beroeps – Authenticiteit

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS (certificaat creatie datum / tijd)	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Naam Abonnee	O=	Var
Title (T)	Beroepstitel	T=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Digital signature (1000 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.1	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services. The certificate holder acts on behalf of his profession.	Fixed
Subject Altname			

Othername SSO	Microsoft UPN voor single sign on	user@domain	Var
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Extended Key Usage	AnyExtendedKeyUsage	OID 2.5.29.37.0	Var
msSmartcardLogin	Microsoft smartcard logon	OID 1.3.6.1.4.1.311.20.2.2	Var
codesigning	Code signering	OID 1.3.6.1.5.5.7.3.3	Var
emailprotection	Email beveiliging	OID 1.3.6.1.5.5.7.3.4	Var
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

7.11 Beroeps – Onweerlegbaarheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Naam abonnee	O=	Var
Title (T)	Beroepstitel	T=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Subject Key Identifier van CA certificaat	SubjectKeyIdentifier of ESG CA – G2 certificate	Fixed
Subject Key Identifier	ID van sleutel certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	Non-Repudiation (0100 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.2	Fixed
Webadres		http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services. The certificate holder acts on behalf of his profession.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed

rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed
Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var
QcStatement	Verklaring Gekwalificeerd certificaat	0.4.0.1862.1.1	Fixed

7.12 Beroeps – Vertrouwelijkheid

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	CN=	Var
Country (C)	Land	C=NL	Fixed
Organization (O)	Naam abonnee	O=	Var
Title (T)	beroepstitel	T=	Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Subject Key Identifier van CA certificaat	SubjectKeyIdentifier of ESG CA – G2 certificate	Fixed
Subject Key Identifier	ID van sleutel certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	sleutelgebruik	• KeyEncipherment • dataEncipherment • keyAgreement (0011 1000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.3	Fixed
Webadres		http://cps.csp4.eu	Fixed
User notice	Gebruikers melding	The general terms and conditions as mentioned on our website (cps.csp4.eu), are applicable to all our products and services. The certificate holder acts on behalf of his profession.	Fixed
Subject Altname			
Othername	Universal Principal Name (uniek nummer)	2.16.528.1.1003.1.3.5.3.1-number of certificate request	Fixed
rfc822name	e-mailadres	E-mailadres of subject	Var
Basic Constraints (Critical)	(False)	empty	Fixed
CRL Distribution Points	Adres CRL	http://crl.csp4.eu/esgcag2.crl	Fixed

Authority Info Access	URI van de OCSP Responder	http://ocsp.csp4.eu	Fixed
Subject Info Access	Extra info over de certificaathouder	OID, Generalname	Var

8 CRL en OCSP Profielen

8.1 CRL (Organisatie)

Veld	Inhoud		
Version	Versie	1	
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS (certificaat creatie datum / tijd)	Certificate production date & time	Fixed
Valid to	Valid from + 24 uur	Certificate production date & time + 24 uur	Fixed
Revoked certificates	Overzicht van ingetrokken certificaten	List revoked certificates (time, date, serialnumber of certificate)	Fixed
Serialnumber	Serienummer van ingetrokken certicaat	Serialnumber of certificate	
Daytime	Datum en tijd van intrekking van het certificaat	Date and time of revocation of certificate	
CRL Entry Extensions			
CRL Reason	Reden van revocation van het certificaat	Reason revocation of certificate	
CRL Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
CRL number	Opvolgend nummer (systeem gegenereerd)	Serialnumber of crl	Fixed

8.2 CRL (Burger)

Veld	Omschrijving	Inhoud	
Version	Versie	1	
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG Persoonlijk CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS (certificaat creatie datum / tijd)	Certificate production date & time	Fixed
Valid to	Valid from + 24 uur	Certificate production date & time + 24 uur	Fixed
Revoked certificates	Overzicht van ingetrokken certificaten	List revoked certificates (time, date, serialnumber of certificate)	Fixed
Serialnumber	Serienummer van ingetrokken certificaat	Serialnumber of certificate	
Daytime	Datum en tijd van intrekking van het certificaat	Date and time of revocation of certificate	
CRL Entry Extensions			
CRL Reason	Reden van revocation van het certificaat	Reason revocation of certificate	
CRL Extensions			

Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG Persoonlijk CA – G2 certificate	Fixed
CRL number	Opvolgend nummer (systeem gegenereerd)	Serialnumber of crl	Fixed

OCSP

Veld	Omschrijving	Inhoud	
Version	Versie	2	Fixed
Serialnumber	Uniek nummer systeem gegenereerd	Serialnumber of certificate	Fixed
Signature Algorithm	algoritme	OID of sha256RSA	Fixed
Issuer			
Common name (CN)	Autoriteit naam certificaat uitgever	ESG CA - G2	Fixed
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Fixed
Country (C)	Land	NL	Fixed
Validity			
Valid from	DD-MM-JJJJ UU:MM:SS	Certificate production date & time	Fixed
Valid to	Valid from + 3 jaar	Certificate production date & time + 3 jaar	Fixed
Subject			
Common name	Naam certificaathouder	ESG OCSP - G2	Var
Country (C)	Land	NL	Var
Organization (O)	Bedrijfsnaam	ESG de electronische signatuur BV	Var
Organizational Unit (OU)	Afdeling		Var
Serialnumber	Uniek nummer (opvolgend)	Serialnumber of subject	Fixed
Public Key info	RSA (2048 Bits) (systeem gegenereerd)	PublicKeyInfo conform ETSI TS 102280, RFC 3279	Fixed
Extensions			
Authority Key Identifier	Sleutel ID CA	SubjectKeyIdentifier of ESG CA -G2 certificate	Fixed
Subject Key Identifier	Sleutel ID certificaathouder	SubjectKeyIdentifier	Fixed
Key Usage (Critical)	Sleutelgebruik	Digital Signature (1000 0000)	Fixed
Certificate Policies			
OID	Object Identifier	2.16.528.1.1003.1.2.5.4	Fixed
Webadres	webadres	http://cps.csp4.eu	Fixed
Basic Constraints (Critical)	(False)	empty	Fixed
Extended Key Usage (Critical)			
OCSPSigning (Critical)	OCSPSigning	id-kp-OCSPSigning (OID 1.3.6.1.5.5.7.3.9)	Fixed

9 Conformiteit

9.1 CSO

Het management van ESG-CSP is conform het PvE van PKIoverheid eindverantwoordelijk voor de controle van methodes, processen en procedures die in het Trust Center voor de veiligheid zijn genomen. QuoVadis is conform ETSI gecertificeerd als CSO. Deze certificatie garandeert dat alle bedrijfsprocessen voor productie van certificaten en voor de on-line services precies beschreven en gecontroleerd zijn.

ESG-CSP baseert zich hierop middels de relevante publicaties van QuoVadis, de controle door de auditor van BSI en het door QuoVadis overlegde certificaat.

9.2 Certificatie

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

10 Algemene en juridische bepalingen

10.1 Tarieven

Alle tarieven van ESG-CSP zijn beschikbaar via de website: www.esg4.eu.

10.2 Financiële aansprakelijkheid

De aansprakelijkheid van ESG de electronische signatuur BV is geregeld conform artikel 253 BW6.

10.3 Vertrouwelijkheid van bedrijfsinformatie

Geen specifieke bepalingen.

10.4 Privacy

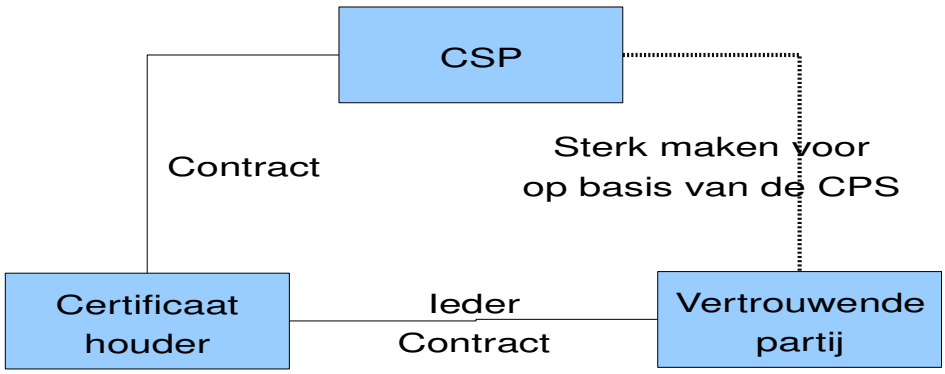
ESG de electronische signatuur BV neemt bij opname, verwerking en archivering van persoonsgegevens de relevante wet- en regelgeving stipt in acht. De activiteiten en administratie van ESG-CSP zijn aangemeld bij de registratiekamer onder nummer M1321561. LRAO respectievelijk LRA dienen ingevulde formulieren direct na beëindiging van een controle in een gesealde en genummerde enveloppe te versturen aan ESG. Opslag van deze enveloppen is alleen toegestaan als de LRA(O) beschikt over daartoe geëigende voorzieningen. Noch de LRAO noch de LRA zijn gerechtigd kopieën van bij de RA-controle gebruikte documenten na beëindiging daarvan in bezit te hebben.

10.5 Intellectuele eigendomsrechten

ESG de electronische signatuur BV vrijwaart haar klanten van aansprakelijkheid als gevolg van schending van intellectuele eigendomsrechten door ESG-CSP. De door ESG-CSP verstrekte Digiseal Reader is zogenaamde 'KostenFreie VersuchsSoftware'. Voor de Aloaha smartcard-connector wordt een specifieke gebruikerssleutel ter beschikking gesteld.

Alle rechten van deze CPS berusten bij ESG de electronische signatuur BV, ongewijzigde kopieën mogen met bronvermelding worden verspreid.

10.6 Zekerheden & garanties



Afbeelding 1: artikel 253 van Boek 6 BW.

10.6.1 Persoonsgebonden certificaten

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

10.6.2 Service-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.

10.7 Garantieuitsluiting

In geval van systeemdefecten of andere factoren die buiten de invloedssfeer van ESG-CSP liggen, zal ESG-CSP al het mogelijke doen om de dienstverlening zo snel mogelijk bereikbaar te maken. ESG-CSP is niet verantwoordelijk voor uitval van de dienstverlening vanwege natuurrampen of andere omstandigheden waarvoor ESG-CSP niet verantwoordelijk kan worden gehouden.

10.8 Aansprakelijkheidsbeperking

De aansprakelijkheid van ESG de electronische signatuur BV is beperkt tot haar aansprakelijkheid conform artikel 253 van Boek 6 BW. ESG de electronische signatuur BV is niet aansprakelijk voor schade indien het certificaat niet conform de PKIoverheid regelgeving is gebruikt. De aansprakelijkheid van ESG is beperkt tot 1 miljoen euro per gebeurtenis.

10.9 Persoonlijke berichtgeving[29]

Aanspraak op persoonlijke berichtgeving van aanpassing van enige publicatie is expliciet uitgesloten.

10.10 Wijzigingen & aanpassingen CPS

Om op veranderende marktvoorwaarden, veiligheidseisen, wetswijzigingen etc. te kunnen reageren, behoudt ESG de electronische signatuur BV zich het recht voor om wijzigingen en aanpassingen in deze documentatie aan te brengen. Wijzigingen worden op de internetsite www.esg4.eu 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 ESG de electronische signatuur BV. De bevoegdheid om wijzigingen aan te brengen in de documentatie blijft voorbehouden aan ESG de electronische signatuur BV. Bij elke wijziging van de CPS worden versienummer en datum vernieuwd.

10.11 Geschillen

In gevallen waarin onenigheid bestaat over het gebruik van de in een certificaat op te nemen namen, beslist ESG-CSP 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 ESG-CSP. 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 Roermond.

10.12 Toepasselijke wetgeving

Op alle overeenkomsten is het Nederlands recht van toepassing.

10.13 Compliance

ESG De Electronische Signatuur BV voldoet aan de voorwaarden van ETSI TS 101 456 en de

29 Zie ook paragraaf 2.1.

aanvullende eisen van PKIOverheid. Zij verzorgt de volgende diensten:

1. Registratie Service
2. Certificate Generatie Service
3. Dissemination Service
4. Revocation Management & Status Service
5. Subject Device Provision Service (SSCD & SUD)

10.14 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.