ESG de electronische signatuur BV

Bijzondere Voorwaarden

Versie 1.9

ESG de electronische signatuur BV

ESG de electronische signatuur B.V. (ESG) is een certificatiedienstverlener die is toegetreden tot het stelsel van de PKIoverheid. Dat betekent voor deze dienstverlening dat alle relevant bepalingen en eisen uit het Programma van Eisen behorende bij PKIoverheid van toepassing zijn.

De in deze Bijzondere Voorwaarden PKIoverheid Certificaten vermelde bepalingen zijn, naast de Algemene Bepalingen van de Algemene Leveringsvoorwaarden van ESG, uitsluitend van toepassing indien ESG aan Opdrachtgevers (Abonnee) PKIoverheid Certificaten levert. In geval van strijdigheid tussen bepalingen van deze Bijzondere Voorwaarden en bepalingen van de Algemene Voorwaarden, prevaleren de bepalingen van deze Bijzondere Voorwaarden.

Documentbeheer

Datum	Versie	Auteur	Wijzigingen
25-03-2013	1.1	Hilde Oomen	
11-04-2014	1.2	Hilde Oomen	
26-06-2014	1.3	Hilde Oomen	
21-07-2014	1.4	Hilde Oomen	Toevoeging PvE eis 9.6.1 in artikel 10
17-03-15	1.5	Hilde Oomen	Aanpassing versie nummer nav review, toevoeging richtlijn NCSC in H12
10-04-15	1.5	Hilde Oomen	Toevoeging par 10.9 n.a.v audit.
16-11-15	1.6	Hilde Oomen	Toevoeging H9 t.a.v. gebruik POC in HSM.
07-07-16	1.7	Hilde Oomen	Toevoeging bepalingen H9, aanpassing titel H7 en H9.
21-10-2016	1.8	Hilde Oomen	Aanpassing website in H13, aanpassing layout
28-10-2016	1.9	Hilde Oomen	Toevoeging punt in §11.5

1. Definities

1.1 de definities en afkortingen zoals opgenomen in de door ESG uitgegeven Certification Practice Statement PKIoverheid (hierna: CPS van ESG) zijn integraal van toepassing op deze Bijzondere Voorwaarden.

2. Onderwerp

2.1 Tegen betaling van de daarvoor geldende tarieven door Opdrachtgever, zal ESG als Certification Service Provider (CSP) de overeengekomen hoeveelheid PKIoverheid Certificaten leveren aan Opdrachtgever onder de voorwaarden zoals opgenomen in deze Bijzonder Voorwaarden. Opdrachtgever geldt in dat verband als Abonnee, inclusief de daarbij gehorende verplichtingen.

2.2. Indien de Abonnee een niet natuurlijk persoon is, wijst Abonnee ten minste één contactpersoon aan om namens hem de uitgifte en intrekking van PKIoverheid Certificaten te begeleiden. Alsdan garandeert Abonnee dat degene die namens hem om uitgifte verzoekt vertrouwd, ter zake kundig en voldoende bevoegd is om zo'n verzoek te doen en daarmee diens rechtspersoon te binden aan deze voorwaarden. Indien de Contactpersoon niet langer

bevoegd is de Opdrachtgever te vertegenwoordigen, dan dient de Opdrachtgever dit vroegtijdig schriftelijk kenbaar de maken aan ESG.

3. Verplichtingen & Garanties ESG

3.1 ESG garandeert tegenover Abonnees, Certificaathouders en Vertrouwende Partijen dat:

- De levering zal geschieden conform deze Bijzondere Voorwaarden, de CPS van ESG;
- ESG conformeert zich aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates (verder: Requierments) zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid Programma van Eisen deel 3b en 3E en de betreffende Requirements, waardoor niet ten minste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de Policy Authority van PKIoverheid, dan prevaleert het gestelde in de Requirements.
- Alle gegevens in het PKIoverheid Certificaat op het tijdstip van afgifte juist zijn en dat alle noodzakelijke gegevens zijn opgenomen;
- De gegevens van de in het PKIoverheid Certificaat geïdentificeerde Certificaathouder op het tijdstip van de afgifte van het PKIoverheid Certificaat overeenkomen met de gegevens die zijn gebruikt voor het aanmaken van het PKIoverheid Certificaat;
- De gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening complementair kunnen worden gebruikt;
- Geen inhoudelijke fouten of onvolledigheden zullen worden geïntroduceerd bij de generatie en uitgifte van een PKIoverheid Certificaat door ESG.

3.2 ESG garandeert tegenover Abonnees, Certificaathouders en Vertrouwende Partijen dat in de volgende gevallen tot intrekking van de uitgegeven Certificaten zal worden overgegaan.

- De abonnee geeft aan dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee ook met terugwerkende kracht geen toestemming verleent.
- ESG over voldoende bewijs beschikt over:
  - Dat de private sleutel van de abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast en/of
  - Een vermoeden van compromittatie en/of
  - Een inherente beveiligingszwakheid en/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 private sleutel,
  - Vernietigde private sleutel of SSCD.
- Een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in deze CP en/of het bijbehorende CPS van ESG en/of de overeenkomst die ESG met de abonnee heeft afgesloten.
- ESG op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de gegevens, die in het certificaat staat. Een voorbeeld daarvan is: verandering van de naam van de certificaathouder.
- ESG bepaalt dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van ESG of de overeenkomst die ESG met de abonnee heeft gesloten.
- ESG bepaalt dat gegevens in het certificaat niet juist of misleidend zijn.
- ESG haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere certificatiedienstverlener.

- De Policy Authority van PKIoverheid vaststelt en naar ESG toe aangeeft dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (zoals browserpartijen).

Opmerking: 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 ESG, waarmee certificaten worden ondertekend, beschouwd.

Voor Server certificaten gelden ook de volgende redenen.

- ESG op de hoogte wordt gesteld of anderszins zich er bewust van wordt dat het gebruik van de domeinnaam in het certificaat niet langer wettelijk toegestaan is (bijvoorbeeld ten gevolge van een rechterlijke uitspraak of door misbruik).
- De Abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen.

4. Verplichtingen & garanties Abonnee

4.1 De Abonnee garandeert tegenover ESG en Vertrouwende Partijen dat:

- De rol van Abonnee zal worden uitgevoerd conform deze Bijzondere Voorwaarden en conform de CPS van ESG;
- Alle gegevens die worden aangeboden ten behoeve van de generatie en uitgifte van een PKIoverheid Certificaat naar waarheid, actueel en correct zijn;
- Alle door of namens hem aangewezen Certificaathouders en/of Certificaatbeheerders handelen conform de in deze Bijzonder Voorwaarden opgenomen verplichtingen;
- Alle relevante wijzigingen in de relatie tussen de Abonnee en Certificaathouder en/of Certificaatbeheerder vroegtijdig aan ESG worden gecommuniceerd;
- Alle relevante stukken op eerste verzoek van ESG, uiterlijk binnen drie weken na genoemd verzoek, worden overlegd;
- ESG zo spoedig mogelijk op de hoogte zal worden gesteld indien onjuistheden in de inhoud van het PKIoverheid Certificaat zijn ontstaan;
- ESG, in geval van beroepsgebonden certificaten, zo spoedig mogelijk op de hoogte zal worden gesteld indien het authentieke bewijs welke noodzakelijk is voor het behouden van het Certificaat voor een erkend beroep niet langer kan worden overlegd;
- SSCD’s en SUD’s (indien van toepassing) waarop Private Sleutels worden bewaard, zullen worden beveiligd conform de wijze waarop gevoelige gegevens en/of bedrijf kritische middelen zijn beveiligd;
- Sleutelmateriaal van Certificaathouders zal worden gegenereerd in een veilig middel dat voldoet aan EAL4+ of aan gelijkwaardige beveiligingscriteria, dan wel op een softwarematige wijze in een omgeving die aldus is ingericht dat ongeoorloofde toegang en/of gebruik van de sleutels wordt uitgesloten, met inachtneming van het onder artikel 7 lid 1 bepaalde;
- Elk op zijn verzoek uitgegeven PKIoverheid Certificaat direct en zonder vertraging wordt ingetrokken wanneer de Certificaathouder niet langer valt onder de verantwoordelijkheid van de Abonnee of indien de Certificaathouder en/of Certificaatbeheerder handelt in strijd met het onder artikel bepaalde;
- De werkgever van de Abonnee/ Certificaathouder van het Certificaat toestemming heeft gegevens voor het opnemen van het door of vanwege genoemde werkgever verstrekte e-mailadres op het Certificaat en dat voornoemde toestemming te allen tijde aangetoond kan worden.

4.2 De Abonnee is zelf verantwoordelijk voor een tijdige vervanging van de aan zijn organisatie uitgegeven certificaten in het geval van een naderende afloop geldigheid van het Certificaat, compromittatie en/of andere soorten van calamiteiten met betrekking tot het Certificaat of van bovenliggende certificaten, gedurende de periode van geldigheid. ESG verwacht van de Abonnee dat de Abonnee zelf adequate maatregelen neemt om de continuïteit van het gebruik van de Certificaten te borgen.

5. Verplichtingen & Garanties Certificaathouder

5.1 De Certificaathouder garandeert tegenover ESG, de Abonnee en Vertrouwende Partijen dat:

- Geen enkele andere persoon toegang zal hebben tot de Private Sleutel die is gekoppeld aan de Publieke Sleutel in het PKIoverheid Certificaat;
- Het PKIoverheid Certificaat enkel zal worden gebruikt voor de doelen waartoe deze is uitgereikt;
- De toegangscodes van SSCD en/of SUD, waarin de Private Sleutel is opgeslagen, steeds veilig en gescheiden van de SSCD of SUD bewaard zullen worden;
- Direct na ontvangst van het certificaat, maar in ieder geval alvorens over te gaan tot installatie en gebruik, het certificaat op haar volledige en juiste inhoud zal worden gecontroleerd;
- Direct tot intrekking van het PKIoverheid Certificaat zal worden overgaan en elk gebruik daarvan direct zal worden gestaakt wanneer:
    - Er onvolledigheden en/of onjuistheden in het PKIoverheid Certificaat worden geconstateerd dan wel deze door gewijzigde omstandigheden dreigen te ontstaan of zijn ontstaan;
    - De Private sleutel is verloren, gestolen of anderszins gecompromitteerd is geraakt;
    - De SSCD, SUD, de toegangscodes van SSCD en SUD en/of andere autorisatiemiddelen dan wel activeringsgegevens in onbevoegde handen zijn gekomen of kunnen zijn gekomen;
    - De Private sleutel van ESG en/of de Staat der Nederlanden is verloren, gestolen of anderszins gecompromitteerd is geraakt.

6. Verplichtingen & Garanties Vertrouwende Partij

6.1 De Vertrouwende Partij is verplicht om per geval zelfstandig te beoordelen of het gerechtvaardigd is om op een PKIoverheid Certificaat te vertrouwen. Nadrukkelijk wordt erop gewezen dat, daar waar het transacties van een substantiële financiële omvang betreft, dan wel de transmissie van gegevens met een uitzonderlijk hoge economische waarde of gevoeligheid, een PKIoverheid Certificaat mogelijk niet voldoende betrouwbaarheid biedt, mede gezien de beperkte aansprakelijkheden van ESG.

6.2 Wil de Vertrouwende Partij in redelijkheid kunnen vertrouwen op een door ESG uitgegeven PKIoverheid Certificaat, dan is ze verplicht om daaraan voorafgaand:

- De geldigheid van het PKIoverheid Certificaat te controleren door middel van de actuele Certificaten Revocatie Lijst (CRL):
- De geldigheid van de hiërarchie te controleren waarbinnen het PKIoverheid Certificaat is uitgegeven, dat wil zeggen de geldigheid van Certificaten van bovenliggende CA's alsmede van het Stamcertificaat; en,
- Kennis te nemen van en akkoord te gaan met deze Bijzonder Voorwaarden.

7. Additionele verplichtingen server certificaten

7.1 Indien Abonnee, in het geval van PKIoverheid Certificaten bestemd voor server domeinen, van de mogelijkheid gebruikt maakt om sleutels op softwarematige wijze te genereren, verklaart de Abonnee dat passende maatregelen zullen worden genomen om de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PIN-code), behorende bij de publieke sleutel in het betreffende services server certificaat, onder zijn controle en geheim te houden en te beschermen; indien Abonnee daarbij aantoonbaar in gebreke blijft, de dienstverlening op te schroten of te beëindigen totdat zulks is hersteld.

7.2 De abonnee verklaart dat het niet het services server certificaat zal installeren en gebruiken alvorens het op juistheid en volledigheid gecontroleerd te hebben;

7.3 De abonnee verklaart dat het per direct geen gebruik meer zal maken van het services server certificaat als duidelijk is dat de gegevens in het services server certificaat onjuist of onvolledig zijn of als er aanwijzingen zijn dat de private sleutel, behorend bij de publieke sleutel van het betreffende services server certificaat, gecompromitteerd is geraakt;

7.4 De abonnee verklaart te reageren op instructies van de CSP binnen de door de CSP gestelde termijn in geval van aantasting van de private sleutel of certificaatmisbruik;

7.5 De abonnee aanvaard dat de CSP gerechtigd is om het certificaat in te trekken indien de abonnee de gebruiksovereenkomst heeft geschonden of de CSP heeft ontdekt dat het certificaat wordt gebruikt voor criminele activiteiten zoals phishing, fraude of het verspreiden van malware;

7.6 Voor wat betreft PKIoverheid Certificaten voor server domeinen of voor groepen geldt dat alle daarop van toepassing zijnde verplichtingen van de Certificaathouder eveneens integraal van toepassing zijn op de Certificaatbeheerder, inclusief maar niet beperkt tot onder artikel 5.1 genoemde garanties.

7.7 Voor PKIoverheid Certificaten van het type Services Server geldt dat een dergelijk Certificaat alleen op die server mag worden gezet die bereikbaar is met de domeinnaam (FQDN zoals vermeld in dat Services Server Certificaat.

7.8 Voor PKIoverheid Certificaten van het type Services Server geldt dan een dergelijk Certificaat alleen mag worden gebruikt in overeenstemming met de regelgeving die op de bedrijfsvoering van de Abonnee van toepassing is en alleen in relatie met de werkzaamheden van de Abonnee.

7.9 Voor PKIoverheid Certificaten van het type Services Server geldt dat de Abonnee geen gebruik meer zal en mag maken van de Private Sleutel behorende bij de Publieke Sleutel van het Certificaat, als de geldigheid van het desbetreffende Certificaat is verlopen of als het Certificaat is ingetrokken.

8. Additionele verplichtingen Beroepsgebonden Certificaten

8.1 De (Beroepsgebonden) Abonnee/ Certificaathouder garandeert tegenover ESG dat het bij de aanvraag opgegeven mailadres behoort aan de Abonnee/ Certificaathouder en dat deze, en deze alleen, toegang heeft tot dit e-mail adres. Het e-mail adres dient te zijn voorzien van een passende toegangsbeveiliging.

8.2 De beroepsgebonden Abonnee/ Certificaathouder garandeert tegenover ESG en Vertrouwende Partijen dat direct tot intrekking van het PKIoverheid Certificaat zal worden overgegaan en elk gebruik daarvan direct zal worden gestaakt wanneer de Beroepsgebonden Abonnee/ Certificaathouder het erken beroep, het beroep waarvan hij/ zij heeft aangetoond dat hij/ zij dat uitoefent en zoals weergegeven in het Certificaat, niet langer uitoefent of niet langer mag uitoefenen en/ of het authentieke bewijs voor het uitoefenen van dat beroep niet meer aanwezig of niet meer geldig is, ongeacht of dit tijdelijk of definitief is.

9. Additionele verplichtingen Persoonsgebonden/ Services onweerlegbaarheid certificaten op een gekwalificeerd middel voor elektronische handtekeningen.

9.1 De abonnee verklaart aan ESG dat de private sleutel gegenereerd, opgeslagen en gebruikt wordt op een signature creation device zoals een HSM, dat voldoet aan de eisen genoemd in CWA 14169 Secure signature-creation device “EAL 4+” of gelijkwaardige beveiligingscriteria zoals FIPS 140-2 level 3.

9.2 De abonnee dient bij de aanvraag bewijs te overhandigen door middel van het overleggen van de certificering van het veilig middel en, indien nodig, een screenshot van de instelling van het veilige middel op FIPS 140-2 level 3.

9.3 De abonnee verklaart dat de private sleutel en de daarbij behoren toegangsinformatie, behorend bij de publieke sleutel in het betreffende signature creation device, is gegenereerd en in de toekomst geheim wordt gehouden en beschermd voor anderen dan de certificaathouder.

9.4 De abonnee verklaart dat de certificaathouder, systeembeheerders van het gekwalificeerd middel voor elektronische handtekeningen expliciet heeft gemandateerd voor het beheer en dat altijd sprake is van dual control voor toegang tot dit middel.

9.5 De abonnee verklaart aantoonbaar te voldoen aan de eisen en/of de voorwaarden die het gekwalificeerde middel voor elektronische handtekeningen stelt aan het gebruik ervan dan wel de certificering van het middel stelt aan de omgeving waarbinnen het geheel wordt beheerd en het beheer zelf.

9.6 ESG houdt zich het recht voor om een controle uit te voeren naar de getroffen beveiligingsmaatregelen.

9.7 De CSP dient aanwezig te zijn bij de PKI ceremonie voor in gebruik name van het gekwalificeerde middel voor elektronische handtekeningen en het genereren van het sleutelpaar. Hiermee kan de CSP zich ook vergewissen van de effectiviteit van getroffen beveiligingsmaatregelen.

10. Beperkingen van gebruik

10.1 Eigendomsrechten met betrekking tot het PKIoverheid Certificaat, het SSCD en het SUD blijven ook na uitgifte berusten bij ESG en diens licentiegevers, inclusief rechten van intellectueel eigendom.

10.2 ESG verstrekt aan de Certificaathouder een niet-overdraagbaar en beperkt gebruiksrecht op het PKIoverheid Certificaat, het SSCD en het SUD gedurende de periode waarin het PKIoverheid Certificaat geldig is.

10.3 het Persoonsgebonden en Beroepsgebonden PKIoverheid Certificaat, het voor de opslag ervan gebruikte SSCD, de toegangscodes van het SSCD, en de Private Sleutel zijn allen persoonsgebonden en op geen enkele wijze overdraagbaar aan andere natuurlijker personen of rechtspersonen.

10.4 het is de Abonnee noch de Certificaathouder of Certificaatbeheerder toegestaan om het uiterlijk van het SSCD te wijzigen of anderszins aan te passen, inclusief de daarop vermelde (persoons)gegevens.

10.5 De Abonnee en de Certificaathouder zijn zelf verantwoordelijk voor applicaties en andere middelen nodig voor gebruikmaking van het PKIoverheid Certificaat, met uitzondering van het SSCD en het SUD.

10.6 Het authenticiteitscertificaat is niet in de Wet op de identificatieplicht (Wid) aangewezen als identiteitsdocument en kan derhalve niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen met een in de Wet op de identificatieplicht aangewezen document wordt vastgesteld.

11 Aansprakelijkheid

11.1 ESG is aansprakelijk voor schade die Abonnees en/of Vertrouwende Partijen ondervinden die in redelijkheid op een door ESG uitgegeven PKIoverheid Certificaat vertrouwen, doch enkel voor wat betreft schade ontstaan door toerekenbare tekortkomingen in de uitvoering van het navolgende:

- De garantie dat, op het tijdstip van uitgifte, alle gegevens in het PKIoverheid Certificaat juist zijn en dat daarin alle voorgeschreven gegevens zijn opgenomen;
- De garantie dat een verzoek tot intrekking van een PKIoverheid Certificaat tijdig wordt verwerkt, waarbij inbegrepen het bijwerken en publiceren van de status informatie van het PKIoverheid Certificaat;
- De garantie dat de in het PKIoverheid Certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het Certificaat, houder was van de gegevens voor het aanmaken van de handtekening die met de in het PKIoverheid Certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van de handtekening overeenstemmen; of,
- De garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening, veronderstellende dat zij beide door ESG worden gegenereerd, complementair kunnen worden gebruikt; of,
- De garantie dat de dienstverlening van ESG ten aanzien van het PKIoverheid Certificaat voldoet en blijft voldoen aan de relevante wet- en regelgeving in zijn algemeenheid en in het bijzonder ten aanzien van de hierboven genoemde punten, waarbij partijen vaststellen dat, indien ten gevolge van een omstandigheid toerekenbaar aan ESG, deze dienstverlening gecompromitteerd wordt, ESG geacht wordt niet aan alle bovengenoemde garanties (meer) te kunnen voldoen.

11.2 ESG maakt zich sterk voor een op het certificaat vertrouwende derde. Dit beding strekt zich tot een aansprakelijkheid van ESG overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:

11.2.1
a) Voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet” gelezen wordt: “een authenticiteitcertificaat”;
b) Voor “ondertekenaar” gelezen wordt: “certificaathouder”;
c) Voor “elektronische handtekeningen” gelezen wordt: “authenticiteitskenmerken”.

11.2.2
a) Voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet” gelezen wordt: “een vertrouwelijkheidcertificaat”;
b) Voor “ondertekenaar” gelezen wordt: “certificaathouder”;
c) Voor “aanmaken van elektronische handtekeningen” gelezen wordt: “aanmaken van vercijferde data”;
d) Voor “verifiëren van elektronische handtekeningen” gelezen wordt: “ontcijferen van authenticiteitskenmerken en vercijferde data”.

11.2.3
a) Voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet” gelezen wordt: “een servercertificaat”;
b) Voor “ondertekenaar” gelezen wordt: “certificaathouder”;
c) Voor “aanmaken van elektronische handtekeningen” gelezen wordt: ‘” verifiëren van authenticiteitskenmerken en aanmaken van vercijferde data:’
d) Voor “verifiëren van elektronische handtekeningen” gelezen wordt: “ontcijferen van authenticiteitskenmerken en vercijferde data”.

11.3 ESG sluit alle aansprakelijkheid uit voor schade indien het certificaat niet conform het beschreven certificaatgebruik wordt gebruikt.

11.4 De aansprakelijkheid van ESG tegenover Abonnees en Vertrouwende Partijen voor het onder artikel 10.1 genoemde is beperkt tot een gezamenlijk bedrag van één miljoen (€ 1.000.000) per jaar. Onder geen enkele omstandigheid zal ESG gehouden zijn tot schadevergoeding boven deze limiet, tenzij aantoonbaar sprake is van grove nalatigheid dan wel opzet van de zijde van ESG.

11.5 ESG aanvaardt jegens Abonnees en Vertrouwende Partijen geen aansprakelijkheid voor andere schade dan onder artikel 9.1 genoemd, waaronder begrepen doch niet beperkt tot:

- Schade ten gevolge van niet-toerekenbare tekortkomingen in de nakoming (overmacht);
- Schade die voortvloeit uit de niet-nakoming van de in deze voorwaarden beschreven verplichtingen van Abonnees, Certificaathouders, Certificaatbeheerders en/of Vertrouwende Partijen;
- Schade ten gevolge van het verlies of anderszins verdwijnen van het PKIoverheid Certificaat, het Persoonlijk Identificatie Nummer, het SSCD, het SUD of de Private Sleutel;
- Schade die voortvloeit uit gebruik van een PKIoverheid Certificaat buiten het daarvoor beschreven toepassingsgebied of buiten de in het PKIoverheid Certificaat aangegeven beperkingen.
- Schade die ontstaan is bij verblijf in de Verenigde Staten en Canada.

11.6 ESG aanvaardt geen enkele aansprakelijkheid jegens andere partijen of personen dan Abonnees en Vertrouwende Partijen, inclusief maar niet beperkt tot Certificaathouders en Certificaatbeheerders. In geval de handelingen van een derde partij leiden tot aansprakelijkstelling van ESG door een Certificaathouder, Certificaatbeheerder en/of

Vertrouwende Partij, vrijwaart Abonnee ESG voor alle daaruit voortvloeiende schade, inclusief maar niet beperkt tot de kosten van verweer van de zijde van ESG.

11.7 ESG zal toereikende regelingen onderhouden om de aansprakelijkheden die verband houden met dit artikel af te dekken, onder andere in de vorm van verzekeringen.

11.8 De ondersteuning en afhandeling van de online financiële transactie wordt door ESG de Electronische Signatuur B.V. uitbesteed aan Dynagroup B.V. Dynagroup B.V. draagt hiervoor de gehele verantwoordelijkheid.

11.9 Ondanks eventuele beperkingen inzake de aansprakelijkheid voor Abonnees en Vertrouwende Partijen, begrijpt en erkent de CA dat de Applicatie Software Leveranciers die een Root Certificaat distributieovereenkomst hebben afgesloten met de Root CA, geen enkele verplichting of potentiële aansprakelijkheid van de CA op grond van onderhavige eisen erkennen of die anders zou kunnen bestaan als gevolg van de uitgifte of het onderhoud van Certificaten of het vertrouwen daarop door Vertrouwende Partijen of anderen. Dus, behalve in het geval dat de CA een overheidsinstanties is, zal de CA elke Application Software Leverancier verdedigen, schadeloos stellen en vrijwaren voor alle claims, schade en verlies geleden door een Applicatie Software Leverancier met betrekking tot een door de CA uitgegeven certificaat ongeacht de oorzaak of juridische theorie. Echter, dit is niet van toepassing op claims, inbreuk op of verlies dat direct is veroorzaakt door de software van de applicatie leverancier waarbij een geldig certificaat als onbetrouwbaar wordt weergegeven of als betrouwbaar indien: (1) een certificaat is verlopen, of (2) een certificaat is ingetrokken (maar alleen in de gevallen waarbij de revocatie status service online beschikbaar is bij de CA en de software applicatie verzaakt heeft om een status check uit te voeren of de indicatie dat een certificaat is ingetrokken heeft genegeerd).

12 Privacy

12.1 In zoverre relevant gaan de Abonnee, Certificaathouder en de Certificaatbeheerder ermee akkoord dat:

- ESG de door haar getrainde en gecontracteerde LRA's inzet voor het uitvoeren van de registratieprocedure en de daarbij behorende controle en verzending van persoonsgegevens;
- ESG door de Abonnee, Certificaathouder en de Certificaatbeheerder verstrekte persoonsgegevens mag gebruik voor de uitgifte van het PKIoverheid Certificaat; en,
- ESG de inhoud van het PKIoverheid Certificaat openbaar mag maken voor zover dit nodig is voor het gebruik daarvan.

13 Additionele documentatie

13.1 De PKIoverheid CPS van ESG kan worden verkregen via https://cps.de-electronische-signatuur.nl.

13.2 De CPS van de PKI voor de Overheid kan worden verkregen via http://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/

13.3 Het Programma van Eisen van PKIoverheid kan worden verkregen via https://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/

13.4 De Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zijn te verkrijgen via https://www.cabforum.org.

13.5 ICT beveiligingsrichtlijnen voor de transport layer security (TLS) van het NCSC. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html