DIGITAL CERTIFICATES BY DIGICERT – TERMS OF USE

Deze Gebruiksvoorwaarden Digitale Certificaten ('**Gebruiksvoorwaarden Certificaten**') zijn van toepassing op alle digitale certificaten ('**Certificaten**') ongeacht certificaattype, zowel openbaar vertrouwde TLS/SSL-certificaten, Client Certificates (conform de definitie in artikel 9), Gekwalificeerde Certificaten (zoals gedefinieerd in artikel 10) of anderszins, die zijn uitgegeven door DigiCert, Inc., een in Utah gevestigd bedrijf of een van zijn affiliates, inclusief zijn Gekwalificeerde Verleners van Vertrouwensdiensten (gezamenlijk '**DigiCert**') aan een entiteit of persoon ('**Klant**'), conform de identificatie in de DigiCert-servicebeheerportal en/of gerelateerde API's die aan de Klant beschikbaar zijn gesteld ('**Portal**') of op het uitgegeven Certificaat. De Gebruiksvoorwaarden voor Certificaten zijn van toepassing ongeacht wanneer de Klant het Certificaat heeft aangevraagd of wanneer het Certificaat is uitgegeven. De account voor het namens de Klant verkrijgen van toegang tot de Portal en gebruiken hiervan wordt hierin de '**Portalaccount**' genoemd.

Door acceptatie of ondertekening van een overeenkomst waarin naar deze Gebruiksvoorwaarden voor Certificaten wordt verwezen (die overeenkomst afzonderlijk en gezamenlijk met deze voorwaarden, de '**Overeenkomst**'), verklaart de accepteerder of ondertekenaar (de '**Ondertekenaar**') uitdrukkelijk dat hij/zij (i) handelt in zijn hoedanigheid van bevoegd vertegenwoordiger van de Klant namens wie de Ondertekenaar deze Overeenkomst accepteert, en uitdrukkelijk bevoegd is om de Overeenkomst te ondertekenen en de Klant aan de Overeenkomst te verbinden, (ii) de bevoegdheid heeft om het digitale equivalent van een bedrijfsstempel, -zegel of handtekening van een superieur te verkrijgen om (x) de authenticiteit van de website van de Klant vast te stellen, en (y) vast te stellen dat de Klant verantwoordelijk is voor elk gebruik van het Certificaat, (iii) uitdrukkelijk door de Klant gemachtigd is tot goedkeuring van Certificaataanvragen namens de Klant, en (iv) het exclusieve recht dat de Klant heeft, of zal hebben, op het gebruik van de domein(en) die in de afgegeven Certificaten moeten worden opgenomen, zal bevestigen.

Voor alle Certificaten die door DigiCert volgens deze Overeenkomst zijn uitgegeven, zijn de partijen ervan op de hoogte en gaan zij ermee akkoord dat deze Overeenkomst een abonneeovereenkomst vormt, zoals vereist uit hoofde van de toepasselijke normen, richtlijnen en eisen in de industrie voor de uitgifte van Certificaten (waaronder de EV-richtlijnen conform de definitie hieronder).

De Klant en DigiCert komen hierbij het volgende overeen:

1. **Accountgebruikers.**

De Klant machtigt elke persoon die als beheerder in de Portalaccount wordt vermeld om op te treden als een Certificaataanvrager, Certificaatgoedkeurder en Contractondertekenaar (conform de definitie in de EV-richtlijnen) en om te communiceren met DigiCert over het beheer van de Certificaten en sleutelsets. '**EV-richtlijnen**' betekent de Extended Validation-richtlijnen die door het CA/Browser Forum ('**CAB-forum**') worden gepubliceerd en openbaar beschikbaar zijn op www.cabforum.org. De Klant is gerechtigd om deze volmacht in te trekken door DigiCert een kennisgeving te sturen. De Klant is verantwoordelijk voor het periodiek controleren en opnieuw bevestigen van de personen die bevoegd zijn om Certificaten aan te vragen en goed te keuren. Wanneer de Klant een Portalaccountgebruiker wenst te verwijderen, dient de Klant de noodzakelijke maatregelen te nemen om te voorkomen dat die gebruiker toegang krijgt tot de Portal, waaronder het wijzigen van het wachtwoord en andere verificatiemechanismen voor de Portalaccount. De Klant dient DigiCert onmiddellijk op de hoogte te brengen wanneer is vastgesteld dat er onbevoegd gebruik wordt gemaakt van de Portal of Portalaccount. De Klant bevestigt dat: (i) de Klant DigiCert machtigt om gegevens inzake de Services van DigiCert te scannen, te verzamelen en het verlengen en upgraden van Certificaten te automatiseren; (ii) de Klant de Services uitsluitend zal gebruiken voor het scannen en automatiseren van domeinen, IP-adressen en activa die het eigendom van de Klant zijn of waarover hij zeggenschap heeft; (iii) de Klant de Services uitsluitend zal gebruiken voor het beoogde doel zoals DigiCert dit heeft beschreven en op de markt brengt, in overeenstemming met het Beleid inzake aanvaardbaar gebruik van DigiCert op https://www.digicert.com/legal-repository.

2. **Aanvragen.**

De Klant is uitsluitend gerechtigd om Certificaten aan te vragen voor domeinnamen die op naam van de Klant, een affiliate van de Klant of andere entiteit is geregistreerd die DigiCert uitdrukkelijk machtigt om de Klant toe te staan Certificaten voor de domeinnaam te verkrijgen en beheren. DigiCert kan naar eigen inzicht het aantal domeinnamen beperken dat de Klant in één Certificaat mag opnemen.

3. Verificatie.

Na ontvangst van een Certificaataanvraag van de Klant controleert DigiCert de aanvraag en probeert de relevante informatie te verifiëren in overeenstemming met de Certification Practices Statement van DigiCert en toepasselijke normen, richtlijnen en eisen van de bedrijfstak, inclusief wetten en voorschriften voor de uitgifte van Certificaten ('**Industrienormen**'). De verificatie van dergelijke aanvragen gebeurt geheel naar eigen inzicht van DigiCert en DigiCert kan de uitgifte van een Certificaat al dan niet met redenen omkleed weigeren. DigiCert informeert de Klant wanneer een Certificaataanvraag is geweigerd, maar DigiCert is niet verplicht om een reden voor de weigering te geven. **'Certification Practices Statement'** betekent de toepasselijke schriftelijke verklaringen over de beleidsdocumenten en praktijken die door DigiCert worden gebruikt voor de exploitatie van zijn public key infrastructure ('**PKI'**), inclusief toepasselijke beleidsregels en verklaringen met betrekking tot tijdstempels. De Certification Practices Statements van DigiCert zijn beschikbaar op https://www.digicert.com/legal-repository. De Certification Practices Statements die zijn uitgegeven voor services die worden geleverd door een Gekwalificeerd Verlener van Vertrouwensdiensten (al dan niet handelend in zijn hoedanigheid van Gekwalificeerd Verlener van Vertrouwensdiensten) of een gelieerde entiteit zijn beschikbaar op https://www.quovadisglobal.com/repository.

4. Levenscyclus van Certificaten.

De levenscyclus van een uitgegeven Certificaat is afhankelijk van de keuze die de Klant maakt bij het bestellen van het Certificaat, de vereisten die zijn uiteengezet in de Certification Practices Statement en het beoogde gebruik van het Certificaat. DigiCert kan de levenscycli van Certificaten voor niet-uitgegeven Certificaten indien nodig wijzigen om te voldoen aan de eisen van: (i) de Overeenkomst; (ii) Industrienormen; (iii) accountants van DigiCert; of (iv) een Applicatiesoftwareleverancier. **'Applicatiesoftwareleverancier'** betekent een entiteit die Certificaten weergeeft of gebruikt in verband met een gedistribueerde root store waaraan DigiCert deelneemt of zal deelnemen. De Klant dient te stoppen met het gebruik van een Certificaat en de bijbehorende Private Key (zoals hieronder gedefinieerd) zodra de vervaldatum van het Certificaat is verstreken of DigiCert het Certificaat intrekt, zoals toegestaan uit hoofde van de Overeenkomst.

5. Uitgifte.

Wanneer de verificatie van een Certificaat naar tevredenheid van DigiCert is voltooid, wordt het aangevraagde Certificaat door DigiCert uitgegeven en geleverd aan de Klant, waarbij gebruik wordt gemaakt van een redelijke leveringswijze. In de meeste gevallen stuurt DigiCert Certificaten per e-mail naar een adres dat de Klant heeft gespecificeerd, als een elektronische download in de Portal of als reactie op een API-aanroep van de Klant via de Portal. Openbaar Vertrouwde Certificaten worden uitgegeven vanaf een Root Certificate of Intermediate Certificate dat door DigiCert is geselecteerd. DigiCert kan op ieder moment en zonder kennisgeving aan de Klant wijzigingen aanbrengen aan het Root Certificate of Intermediate Certificate dat voor de uitgifte van Certificaten wordt gebruikt. De Klant dient alle toepasselijke wetten, voorschriften en Industrienormen na te leven bij het bestellen en gebruiken van Certificaten, waaronder de Amerikaanse wetgeving op het gebied van exportcontrole en economische sancties. De Klant is ervan op de hoogte dat de Certificaten niet beschikbaar zijn in landen of regio's die verboden zijn door het Office of Foreign Assets Control van het Amerikaanse Ministerie van Financiën, het Amerikaanse Ministerie van Handel, de Europese Commissie, het Office of Financial Sanctions Implementation van het Britse Ministerie van Financiën of andere toepasselijke overheidsinstanties die jurisdictie hebben over DigiCert.

6. Certificaatlicentie.

Onmiddellijk na het starten van een aanvraag voor een Certificaat en tot het tijdstip waarop het Certificaat verloopt of wordt ingetrokken, is de Klant uitsluitend gerechtigd elk afgegeven Certificaat en de daaraan verwante services (ongeacht of die vóór of na uitgifte van het Certificaat worden geleverd) en de bijbehorende Sleutelset te gebruiken voor het doeleinde dat is beschreven in de Certification Practices Statement, in overeenstemming met alle toepasselijke wetten, voorschriften, Industrienormen en deze voorwaarden. Op alle Certificaten die worden vertrouwd door Applicatiesoftwareleveranciers zijn alle toepasselijke vereisten van de Industrienormen van toepassing, inclusief de vereisten van het toepasselijke root-storebeleid van de Applicatiesoftwareleverancier en de Certification Practices Statement, ongeacht hoe de Certificaten worden gebruikt. Elk gebruik dat niet is toegestaan volgens de toepasselijke Industrienormen of de Certification Practices Statement is verboden. DigiCert raadt ten zeerste af om certificaten en sleutels vast te zetten, Certificaten die worden vertrouwd voor het web te gebruiken met een PKI voor andere doeleinden, of Certificaten te gebruiken op een manier waardoor het voor de Klant moeilijk is ze tijdig in te trekken of te voldoen aan de andere vereisten van de Certification Practices Statement, en een dergelijk gebruik wordt niet gezien als afdoende reden om intrekking te vertragen. '**Sleutelset**'

betekent een set van twee of meer wiskundig gerelateerde sleutels, zogenaamde Private Keys die worden gecombineerd met een Public Key, waarbij (i) een bericht kan worden versleuteld met de Public Key en uitsluitend kan worden ontsleuteld met de Private Key(s), en (ii) het onhaalbaar is de Private Key(s) te berekenen, zelfs wanneer de Public Key bekend is. De Klant informeert DigiCert onmiddellijk na de vaststelling van misbruik van een Certificaat, Private Key of de Portal. De Klant is verantwoordelijk voor het verkrijgen en behouden van elke vergunning of licentie die noodzakelijk is voor het bestellen, gebruiken en distribueren van een Certificaat aan eindgebruikers en systemen, waaronder elke licentie die vereist is volgens de Amerikaanse exportwetten. Het is toegestaan SSL-certificaten tegelijkertijd te gebruiken op een of meerdere fysieke servers of apparaten , maar het staat DigiCert vrij kosten in rekening te brengen voor het gebruik van Certificaten op extra servers of apparaten.

7. Sleutelsets.

Een '**Private Key**' betekent de sleutel die de Klant geheim dient te houden en die wordt gebruikt voor het maken van digitale handtekeningen en/of ontsleutelen van elektronische records of bestanden die zijn versleuteld met de bijbehorende Public Key. Een '**Public Key**' betekent een openbaar gemaakte sleutel van een Klant die is opgenomen in het Certificaat van de Klant en die hoort bij de geheime Private Key die de Klant gebruikt. De Klant dient (i) Sleutelsets te genereren met behulp van betrouwbare systemen, (ii) Sleutelsets te gebruiken die ten minste gelijkwaardig zijn aan RSA 2048-bitssleutels en (iii) alle Private Keys vertrouwelijk te behandelen. De Klant is als enige verantwoordelijk voor het niet beschermen van zijn Private Keys. De Klant verklaart dat hij uitsluitend Sleutelsets zal genereren en opslaan voor Adobe Signing Certificates en EV Code Signing Certificates op een apparaat van FIPS 140-2 niveau 2. Alle andere Certificaattypen kunnen worden opgeslagen op beveiligde software- of hardwaresystemen. De Klant dient ervoor te zorgen dat de aanschaf, het gebruik en de acceptatie door de Klant van Sleutelsets die door DigiCert uit hoofde van deze Overeenkomst zijn gegenereerd, voldoen aan de toepasselijke wetten, regels en voorschriften, inclusief, maar niet beperkt tot, export- en importwetten, -regels en -voorschriften, in de jurisdictie waarin de Klant die Sleutelsets aanschaft, gebruikt, accepteert of anderszins ontvangt. Wanneer het de Klant is toegestaan om Private Keys (inclusief kopieën) te importeren of exporteren in verband met het gebruik van specifieke Services van DigiCert, is DigiCert niet aansprakelijk jegens de Klant voor het gebruik en de opslag door de Klant van Private Keys (inclusief kopieën) die niet zijn aangemaakt in de toepasselijke Portal of Service of die worden gebruikt buiten die Portal of Service, ook nadat ze zijn geëxporteerd uit de betreffende Portal of Service.

8. Publicatie van certificaatinformatie.

Niettegenstaande andersluidende bepalingen in deze Gebruiksvoorwaarden voor Certificaten of enige andere overeenkomst tussen de Klant en DigiCert, gaat de Klant akkoord met: (i) openbare bekendmaking door DigiCert van informatie (zoals de domeinnaam, de jurisdictie van oprichting of contactgegevens van de Klant) die in een uitgegeven Certificaat is opgenomen; en (ii) de registratie van Certificaten van de Klant en daarin opgenomen informatie door of namens DigiCert in openbaar toegankelijke Certificate Transparency-databases teneinde phishingaanvallen en andere vormen van fraude te detecteren en voorkomen, en de Klant gaat ermee akkoord dat die informatie na de registratie mogelijk niet kan worden verwijderd. Deze publicatie van certificaatinformatie zal gebeuren in overeenstemming met de toepasselijke Certification Practices Statement.

9. Client Certificates.

'**Client Certificate**' betekent een Certificaat dat een extendedKeyUsage bevat anders dan codeSigning, tijdstempel of serverAuthentication. Het gebruik van Client Certificates kan verschillen en wordt gedefinieerd in het Client Certificate-profiel. De mogelijke in een Client Certificate-profiel gedefinieerde gebruiksmogelijkheden zijn digitale handtekening, e-mailversleuteling en cryptografische authenticatie. Indien een Klant Client Certificates wil aanvragen, dient de Klant (i) de identiteit en relatie met de aanvrager te bevestigen aan de hand van passende interne documentatie zoals voorgeschreven in de Certification Practices Statement, en (ii) bevestigen dat de informatie en verklaringen die zijn verstrekt in verband met Client Certificates of zijn opgenomen in Client Certificate in elk wezenlijk opzicht waarheidsgetrouw, volledig en nauwkeurig zijn.

10. Gekwalificeerde certificaten.

'**Gekwalificeerd Certificaat**' betekent een Certificaat (i) dat is uitgegeven door een Gekwalificeerd Verlener van Vertrouwensdiensten in overeenstemming met de vereisten die voortvloeien uit de toepasselijke Europese en Zwitserse wetten met betrekking tot certificering en elektronische handtekeningen, en (ii) dat het hoogste betrouwbaarheidsniveau biedt van 'gekwalificeerd' krachtens de vereisten.

'**Gekwalificeerd Verlener van Vertrouwensdiensten**' betekent een aan DigiCert gelieerde entiteit die door overheidsinstanties is gecertificeerd voor het uitgeven van Gekwalificeerde Certificaten. De Gekwalificeerde Verleners van Vertrouwensdiensten van DigiCert zijn de volgende:

Gekwalificeerd Verlener van Vertrouwensdiensten	**Vertrouwde lijst**	**Jurisdictie toezichthoudende instantie**
QuoVadis Trustlink B.V.	Netherlands Trusted List	Nederland
DigiCert Europe Belgium B.V.	Belgium Trusted List	België
QuoVadis Trustlink Schweiz AG	Swiss Trusted List	Zwitserland

'**Services van een Gekwalificeerd Verlener van Vertrouwensdiensten**' betekent Services die worden geleverd door een Gekwalificeerd Verlener van Vertrouwensdiensten van DigiCert (zoals hierboven gedefinieerd) (al dan niet handelend in zijn hoedanigheid van Gekwalificeerd Verlener van Vertrouwensdiensten) of een van zijn Affiliates.

Wanneer de Klant Services van een Gekwalificeerd Verlener van Vertrouwensdiensten aanschaft, bevindt de toepasselijke Certification Practices Statement voor die Services zich op https://www.quovadisglobal.com/repository. Met betrekking tot Gekwalificeerde Certificaten dient de Klant (i) wanneer het gebruik van een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen (Qualified Signature Creation Device, 'QSCD') is vereist door de Industrienormen, uitsluitend gebruik te maken van Gekwalificeerde Certificaten voor elektronische handtekeningen die zijn gegenereerd met de QSCD waarop deze zijn opgeslagen; (ii) wanneer de Klant een natuurlijke persoon is, als enige zeggenschap te hebben over het bewaren en gebruiken van zijn Private Keys; en (iii) wanneer de Klant een rechtspersoon of organisatie is, als enige controle en zeggenschap te hebben over het bewaren en gebruiken van zijn Private Keys.

11. Beheer.

In het algemeen zal DigiCert een Certificaat uitgeven, beheren, verlengen en intrekken in overeenstemming met de instructies die door de Klant zijn gegeven via de Portal, en DigiCert mag erop vertrouwen dat die instructies accuraat zijn. De Klant dient juiste en volledige informatie te verstrekken bij communicatie met DigiCert en dient DigiCert binnen 5 Werkdagen te informeren wanneer informatie met betrekking tot zijn account op de Portal wijzigt. De Klant dient vragen van DigiCert over de geldigheid van de door de Klant verstrekte informatie te beantwoorden binnen 5 Werkdagen na op de hoogte te zijn gekomen van de ontvangst daarvan. De Klant dient de Certificaatgegevens op juistheid te controleren en verifiëren voordat hij het Certificaat gebruikt. Certificaten worden geacht door de Klant te zijn geaccepteerd dertig (30) dagen na uitgifte van het Certificaat of eerder, wanneer kan worden bewezen dat de Klant het Certificaat eerder heeft gebruikt. Hoewel DigiCert een herinnering over verlopende Certificaten kan sturen, is DigiCert daartoe niet verplicht en is het uitsluitend de verantwoordelijkheid van de Klant om ervoor te zorgen dat Certificaten vóór de vervaldatum worden verlengd. '**Werkdag**' betekent maandag t/m vrijdag, met uitzondering van officiële Amerikaanse feestdagen, zoals vastgelegd in paragraaf 6103 van hoofdstuk 5 van de United States Code.

12. Registration Authority.

Met uitzondering van openbaar vertrouwde TLS/SSL-certificaten en Gekwalificeerde Certificaten wordt de Klant benoemd als een Registration Authority (en de Klant accepteert hierbij die benoeming) volgens de voorwaarden van de betreffende Certification Practices Statement. Met betrekking tot openbaar vertrouwde TLS/SSL-certificaten wordt de Klant benoemd als een Enterprise RA (en de Klant accepteert hierbij die benoeming) volgens de voorwaarden van de betreffende Certification Practices Statement. Wanneer de Klant functies van een Registration Authority of Enterprise RA uitvoert, zal hij dit doen in overeenstemming met de toepasselijke Certification Practices Statement, en DigiCert kan vertrouwen op de handelingen van de Klant in zijn hoedanigheid als Registration Authority of Enterprise RA. In het geval dat een externe vordering, rechtszaak, procedure of uitspraak voortkomt uit het feit dat de Klant de verplichtingen van een Registration Authority of Enterprise RA niet strikt is nagekomen, dient de Klant DigiCert en zijn directeuren, bestuurders, tussenpersonen, werknemers, opvolgers en rechtverkrijgenden te behoeden voor en te vrijwaren tegen die vordering. Wanneer de Klant handelt als een Registration Authority of Enteprise RA, dient hij ervoor te zorgen dat zijn abonnees die de Certificaten volgens deze Overeenkomst ontvangen, zich houden aan de voorwaarden in de abonneeovereenkomst van DigiCert, die te vinden is op https://www.digicert.com/subscriber-agreement. De Abonnees van de Klant dienen de abonneeovereenkomst te accepteren voordat ze Certificaten ontvangen. '**Enterprise RA**' heeft de betekenis zoals die is toegekend in de actuele versie van de CAB Forum Baseline Requirements op https://cabforum.org/baseline-requirements-documents/, die regelmatig worden geactualiseerd.

13. Beveiliging en gebruik van sleutelsets.

De Klant dient de Sleutelsets die bij een Certificaat horen op veilige wijze te genereren en beschermen, en alle maatregelen te nemen die noodzakelijk zijn ter voorkoming van beschadiging, verlies of onbevoegd gebruik van een Private Key die bij een Certificaat hoort. De Klant dient wachtwoorden te gebruiken die tegemoetkomen aan de vereisten van het CAB Forum en andere relevante vereisten op het gebied van best practices. De Klant zal uitsluitend werknemers, tussenpersonen en onderaannemers toestemming geven voor de toegang tot en het gebruik van Private Keys wanneer de Klant antecedentenonderzoek heeft gedaan naar deze werknemer, tussenpersoon of onderaannemer (voor zover wettelijk toegestaan) en de betreffende persoon training en ervaring met PKI en andere informatiebeveiligingsonderwerpen heeft. De Klant dient DigiCert te informeren, om intrekking van een Certificaat en de bijbehorende Private Key te vragen, het gebruik van dat Certificaat en de bijbehorende Private Key te stoppen en het Certificaat van alle apparaten te verwijderen waarop het is geïnstalleerd, wanneer: (i) informatie in het Certificaat onjuist of onnauwkeurig is of wordt, of (ii) er sprake is van werkelijk of vermeend misbruik of compromittering van de Private Key die hoort bij de Public Key die in het Certificaat is opgenomen. Met betrekking tot code signing Certificates dient de Klant onmiddellijk te stoppen met het gebruik van een Certificaat en de bijbehorende Private Key en onmiddellijk om intrekking van het Certificaat te verzoeken wanneer de Klant van mening is dat (a) informatie in het Certificaat onjuist of onnauwkeurig is of wordt, (b) er sprake is van misbruik of compromittering van de Private Key die hoort bij de Public Key die in het Certificaat is opgenomen, of (c) er bewijs is dat het Certificaat is gebruikt om Verdachte Code te tekenen. '**Verdachte Code**' betekent code die schadelijke of kwaadaardige functies in welke vorm dan ook bevat of die ernstige kwetsbaarheden bevat, waaronder spyware, malware en andere code die wordt geïnstalleerd zonder toestemming van de gebruiker en/of die niet kan worden verwijderd, en code die kan worden gebruikt op manieren die niet door de ontwerpers ervan zijn bedoeld en die schade toebrengt aan de betrouwbaarheid van de platformen waarop deze wordt uitgevoerd. Het is de Klant niet toegestaan om dezelfde Private Key te gebruiken voor verschillende typen Certificaten. Zo is het de Klant niet toegestaan om een Private Key voor code signing te gebruiken voor het aanvragen van een Certificaat dat geen code signing Certificate is. Indien DigiCert vaststelt dat een Private Key die is gebruikt voor een bepaald type Certificaat of actie (zoals code signing), wordt gebruikt voor het aanvragen van een ander type Certificaat (zoals een TLS/SSL- of Client Certificate), is DigiCert verplicht tot het intrekken van alle Certificaten die zijn gekoppeld aan de betreffende Private Key of Sleutelset die zich in de Portalaccount van de Klant bevinden of die op andere wijze door DigiCert zijn uitgegeven. De Klant dient binnen 24 uur te reageren op instructies van DigiCert met betrekking tot de compromittering van Sleutelsets of misbruik van Certificaten. De Klant dient onmiddellijk te stoppen met het gebruik van de Sleutelset die bij een Certificaat hoort (I) bij intrekking van het Certificaat, of indien eerder, (II) op de datum waarop de toegestane gebruiksperiode van de Sleutelset verloopt. Het is de Klant niet toegestaan het Certificaat te gebruiken nadat het is ingetrokken.

Indien de Klant een Private Key die is gegenereerd voor een code signing Certificate opslaat in een HSM (zoals gedefinieerd in de toepasselijke Certification Practices Statement), verklaart de Klant met betrekking tot elk van deze Private Keys dat (w) de Klant zijn Private Key veilig opslaat in een HSM die verwijdering van de Private Key verhindert, (x) de Klant als enige zeggenschap heeft over de HSM of dat de HSM wordt gebruikt via een gecontroleerde cloud (zoals Azure of AWS), (y) de Klant geen reden heeft om aan te nemen dat de Private Key ooit is of zal worden gebruikt buiten de HSM, en (z) de Private Key wordt beschermd door middel van een cryptografische module van minimaal FIPS 140-2 niveau 2 (of het equivalent daarvan) of Common Criteria EAL4+.

14. Defecte Certificaten.

Het enige rechtsmiddel van de Klant bij een defect in een Certificaat ('**Defect**') is van DigiCert te eisen dat het redelijke commerciële inspanningen levert om het defect te herstellen na ontvangst van de kennisgeving over het Defect van de Klant. DigiCert is niet verplicht om een Defect te verhelpen wanneer (i) de Klant het Certificaat heeft misbruikt, beschadigd of gewijzigd, (ii) de Klant het Defect niet onmiddellijk aan DigiCert heeft gemeld of (iii) de Klant een bepaling van de Overeenkomst niet is nagekomen.

15. Garantie Vertrouwende Partij.

De Klant is ervan op de hoogte dat de Garantie Vertrouwende Partij alleen ten gunste is van Vertrouwende Partijen. '**Garantie Vertrouwende Partij**' betekent een garantie die wordt gegeven aan een Vertrouwende Partij die voldoet aan de voorwaarden uiteengezet in de Overeenkomst inzake Vertrouwende Partij en kennisgeving van beperkte aansprakelijkheid, zoals te vinden op de website van DigiCert op https://www.digicert.com/legal-repository. De Garantie Vertrouwende Partij voor Certificaten die zijn uitgegeven door een Gekwalificeerd Verlener van Vertrouwensdiensten of een affiliate van DigiCert bevindt zich op https://www.quovadisglobal.com/repository De Klant kan geen rechten ontlenen aan de Garantie

Vertrouwende Partij, inclusief het recht om de voorwaarden van de Garantie Vertrouwende Partij af te dwingen of een vordering volgens de Garantie Vertrouwende Partij in te dienen. '**Vertrouwende Partij**' heeft de betekenis zoals beschreven in de Garantie Vertrouwende Partij. Een Applicatiesoftwareleverancier is geen Vertrouwende Partij wanneer de door de Applicatiesoftwareleverancier gedistribueerde software alleen informatie over een Certificaat weergeeft of het gebruik van het Certificaat of digitale handtekening faciliteert.

16. Verklaringen.

Voor elk aangevraagd Certificaat verklaart de Klant uitdrukkelijk dat:

a. de Klant het gebruiksrecht heeft of de wettige eigenaar is van (i) een of meerdere in het Certificaat gespecificeerde domeinnamen, en (ii) elke gemeenschappelijke naam of organisatienaam die in het Certificaat is gespecificeerd;

b. de Klant het Certificaat uitsluitend gebruikt voor goedgekeurde en rechtmatige doeleinden, waaronder het niet gebruiken van het Certificaat om Verdachte Code te tekenen, en het Certificaat en de Private Key alleen gebruikt in overeenstemming met alle toepasselijke wetten en uitsluitend in overeenstemming met het doel van het Certificaat, de Certification Practices Statement, elk toepasselijk certificaatbeleid en de Overeenkomst;

c. de Klant kennis heeft genomen van de Certification Practices Statement en ermee akkoord gaat;

d. de Klant DigiCert onmiddellijk schriftelijk zal informeren over elke schending van de Certification Practices Statement of de Baseline Requirements, en

e. de in het Certificaat genoemde organisatie en de geregistreerde domeinnaamhouder op de hoogte zijn van elke Certificaataanvraag en die goedkeurt.

17. Beperkingen.

De Klant is alleen gerechtigd een TLS/SSL-certificaat te gebruiken op de servers die toegankelijk zijn op de domeinnamen die in het uitgegeven Certificaat zijn vermeld. Daarnaast is het de Klant niet toegestaan om:

a. een TLS/SSL-certificaat of Private Key te wijzigen, in sublicentie te geven of afgeleide werken ervan maken (behalve wanneer vereist voor het beoogde gebruik van het Certificaat);

b. bestanden of software te uploaden of distribueren die de werking van andermans computer kunnen beschadigen;

c. verklaringen af te geven over of gebruik te maken van een TLS/SSL-certificaat, behalve wanneer dit uit hoofde van de Certification Practices Statement is toegestaan;

d. de relatie van de Klant met een entiteit te imiteren of verkeerd voor te stellen;

e. een Certificaat of gerelateerde software of service (zoals de Portal) zodanig te gebruiken dat redelijkerwijs een civiel- of strafrechtelijke procedure zou kunnen worden aangespannen tegen de Klant of DigiCert;

f. een Certificaat of gerelateerde software te gebruiken om het vertrouwen van een derde partij te ondermijnen of om ongevraagde bulkcorrespondentie te verzenden of ontvangen;

g. code signing Certificates te gebruiken om Verdachte Code te ondertekenen;

h. een code signing Certificate aan te vragen indien de Public Key in het Certificaat is of wordt gebruikt met een Certificaat dat geen code signing Certificate is;

i. de juiste werking te verstoren van de website van DigiCert of transacties die via de website van DigiCert worden uitgevoerd;

j. te proberen een Certificaat te gebruiken voor de uitgifte van andere Certificaten;

k. de technische implementatie van de systemen of software van DigiCert te monitoren, verstoren of reverse-engineeren of anderszins willens en wetens de beveiliging van de systemen of software van DigiCert compromitteren;

l. certificaatinformatie naar DigiCert te sturen die inbreuk maakt op de intellectuele eigendomsrechten van een derde partij; of

m. opzettelijk een Private Key te maken die sterke overeenkomsten vertoont met een Private Key van DigiCert of derde partij.

n. Tenzij uitdrukkelijk schriftelijk toegestaan door DigiCert is het de Klant niet toegestaan een Certificaat voor een eind-entiteit te gebruiken voor het ondertekenen van enig Certificaat.

18. Intrekking van Certificaten.

DigiCert is gerechtigd om zonder kennisgeving een Certificaat in te trekken om de redenen die zijn vermeld in de Certification Practices Statement, inclusief wanneer DigiCert reden heeft om aan te nemen dat:

a. de Klant intrekking van het Certificaat heeft aangevraagd of geen toestemming heeft gegeven voor de uitgifte van het Certificaat;

b. de Klant de Services gebruikt voor het plaatsen of anderszins beschikbaar maken van materiaal dat een inbreuk vormt op de rechten van DigiCert of een derde partij;

c. de Klant de Overeenkomst of een verplichting uit hoofde van de Certification Practices Statement niet is nagekomen;

d. een bepaling of een overeenkomst met de Klant met daarin een verklaring of verplichting wat betreft de uitgifte, het gebruik, het beheer of de intrekking van het Certificaat verloopt of ongeldig wordt verklaard;

e. de Klant wordt toegevoegd aan een lijst met door de overheid verboden personen of entiteiten, of activiteiten uitvoert vanuit een bestemming die uit hoofde van de Amerikaanse wetgeving is verboden;

f. het Certificaat onjuiste of misleidende informatie bevat;

g. het Certificaat zonder toestemming of niet volgens het beoogde gebruik is gebruikt of is gebruikt voor het tekenen van Verdachte Code;

h. de Private Key die is gekoppeld aan het Certificaat openbaar is gemaakt of is gecompromitteerd;

i. het Certificaat is (i) misbruikt; (ii) gebruikt of uitgegeven in strijd met de wet, de Certification Practices Statement of de Industrienormen; of (iii) gebruikt, op directe of indirecte wijze, voor illegale of frauduleuze doeleinden zoals phishingaanvallen, fraude of de verspreiding van malware, andere illegale of frauduleuze doeleinden of andere schendingen zoals uiteengezet in het Beleid inzake aanvaardbaar gebruik van DigiCert; of

j. intrekking van het Certificaat is vereist op basis van Industrienormen of de Certification Practices Statement van DigiCert, of noodzakelijk is om de rechten, vertrouwelijke informatie, activiteiten of reputatie van DigiCert of een derde partij te beschermen.

19. Delen van informatie.

De Klant is ervan op de hoogte en gaat ermee akkoord dat wanneer (i) het Certificaat of de Klant als een bron van een Verdachte Code wordt vastgesteld, (ii) de bevoegdheid voor het aanvragen van het Certificaat niet kan worden geverifieerd of (iii) het Certificaat wordt ingetrokken om een andere reden dan een verzoek van de Klant (bijv. vanwege compromittering van een Private Key, ontdekking van malware etc.), DigiCert bevoegd is informatie over de Klant, over alle applicaties en objecten die met het Certificaat zijn getekend, over het Certificaat zelf en de omstandigheden te delen met andere certificeringsinstantie of groepen in de industrie, waaronder het CAB Forum.

20. Industrienormen**.**

Beide partijen zijn gebonden tot naleving van alle Industrienormen en wetten die op de Certificaten van toepassing zijn; indien een toepasselijke wet of Bedrijfstaknorm wijzigt en die wijziging gevolgen heeft voor de Certificaten of andere Services die uit hoofde van de Overeenkomst worden geleverd, is DigiCert gerechtigd de Services te wijzigen of de Overeenkomst te wijzigen of beëindigen voor zover dit noodzakelijk is om aan deze wijzigingen te voldoen.

21. Apparatuur.

De Klant is verantwoordelijk, voor eigen rekening, voor (i) alle computers, telecommunicatieapparatuur, software, internettoegang en communicatienetwerken (indien van toepassing) die vereist zijn voor het gebruik van de Certificaten en gerelateerde software of Services van DigiCert; en (ii) het gedrag van de Klant en het onderhoud en de exploitatie, ontwikkeling en inhoud van zijn website.

22. Certificaatbegunstigden.

Vertrouwende Partijen en Applicatiesoftwareleveranciers zijn uitdrukkelijke externe begunstigden van de verplichtingen en verklaringen van de Klant ten aanzien van het gebruik of de uitgifte van een Certificaat. De Vertrouwende Partijen en Applicatiesoftwareleveranciers zijn geen uitdrukkelijke externe begunstigden met betrekking tot de software van DigiCert.

23. Intermediate Certificates.

Dit artikel 23 is uitsluitend van toepassing wanneer de Klant een eigen Root Certificate en/of Intermediate Certificate aanschaft voor de uitgifte van Persoonlijke Certificaten of openbaar vertrouwde Certificaten, zoals gespecificeerd op een Bestelformulier.

a. Aanmaak. Binnen 60 dagen na ontvangst van de toepasselijke betaling conform de Overeenkomst en de informatie die DigiCert nodig heeft voor het maken van het Root Certificate en/of Intermediate Certificate zoals beschreven in subparagraaf (b) hieronder, maakt DigiCert een Root Certificate en/of Intermediate Certificate voor de uitgifte van (i) niet openbaar vertrouwde Certificaten via de Portal of (ii) openbaar vertrouwde Certificaten, zoals aangegeven in een Bestelformulier. '**Persoonlijk Certificaat**' betekent een Certificaat dat niet is opgenomen in een vertrouwensarchief. '**Root Certificate**' betekent een zelfondertekend Certificaat dat op een beveiligde offlinelocatie is opgeslagen en wordt gebruikt voor de uitgifte van andere Certificaten. '**Intermediate Certificate**' betekent een Certificaat dat is ondertekend door een Private Key en overeenkomt met een Root Certificate en wordt gebruikt voor de uitgifte van Certificaten voor gebruik door de Klant.

b. Inhoud. DigiCert en de Klant werken te goeder trouw samen om de juiste inhoud van het Root Certificate en/of Intermediate Certificate te bepalen. De Klant moet DigiCert voorzien van alle informatie die DigiCert nodig heeft voor het maken van het Root Certificate en/of Intermediate Certificate binnen twaalf (12) maanden na het sluiten van een overeenkomst voor het maken van dat Root Certificate en/of Intermediate Certificate. Indien de Klant nalaat om binnen die tijd alle vereiste informatie te verschaffen, vervalt het recht van de Klant om het Root Certificate en/of Intermediate Certificate aan te vragen en zal DigiCert de vergoedingen inhouden die zijn betaald voor het maken van het Root Certificate en/of Intermediate Certificate. Nadat een Intermediate Certificate is gemaakt, is het de Klant niet toegestaan de inhoud van dat Intermediate Certificate te wijzigen, maar is de Klant wel gerechtigd om, indien nodig, net zoveel identieke kopieën van het Intermediate Certificate te maken als gewenst. Intermediate Certificates hebben een vaste levenscyclus van tien jaar, waarna ze zonder verlenging verlopen. De Klant is ervoor verantwoordelijk dat alle op basis van een Intermediate Certificate uitgegeven Certificaten ten minste twee jaar vóór het verlopen van het Intermediate Certificate verlopen. DigiCert heeft het recht om Certificaten in te trekken die zijn uitgegeven op basis van de Intermediate Certificates en die nog geldig zijn tot maximaal twee jaar na het verlopen van het Intermediate Certificate.

c. Eigendom. DigiCert blijft de enige eigenaar van het Intermediate Certificate, maar gebruikt het in verband met deze Overeenkomst afgegeven Intermediate Certificate uitsluitend in overeenstemming met de instructies die de Klant via de Portal heeft gegeven, tenzij anders is bepaald in deze overeenkomst. Het is de Klant toegestaan om kopieën van het Intermediate Certificate te maken en kopieën van het Intermediate Certificate te verspreiden onder zijn eigen eindgebruikers en klanten.

d. Hosting. DigiCert host de Private Key van het Intermediate Certificate in de beveiligde PKI-systemen van DigiCert. Het is de Klant niet toegestaan de Private Key van het Intermediate Certificate om welke reden dan ook uit de PKI-systemen van DigiCert te verwijderen of door een derde partij te laten verwijderen. DigiCert levert en host CRL/OCSP-services voor de Klant. DigiCert blijft de CRL/OCSP-services ook na beëindiging van de Overeenkomst leveren totdat alle uit hoofde van deze Overeenkomst uitgegeven Certificaten zijn verlopen of ingetrokken. Een Intermediate Certificate op basis waarvan openbaar vertrouwde Certificaten worden uitgegeven, omdat openbaar vertrouwde Certificaten kunnen worden uitgegeven op basis van het Intermediate Certificate, dat wordt gehost in de PKI van DigiCert en dat wordt beheerd door medewerkers van DigiCert, valt onder de WebTrust-audit van DigiCert. Wanneer de Industrienormen of het beleid van een Applicatiesoftwareleverancier zodanig wijzigen dat een afzonderlijke controle nodig is van het Intermediate

Certificate, dienen DigiCert en de Klant in goed vertrouwen samen te werken aan het uitvoeren van de gewenste controle.

e. Intrekking. DigiCert is gerechtigd om het Intermediate Certificate in te trekken indien: (i) de Klant DigiCert schriftelijk om intrekking verzoekt vanwege een specifieke schending van Industrienormen; (ii) DigiCert reden heeft om aan te nemen dat het Intermediate Certificate is gecompromitteerd; (iii) de Klant de Overeenkomst wezenlijk niet nakomt en de niet-nakoming niet herstelt binnen 30 dagen na ontvangst van de kennisgeving van de niet-nakoming; of (iv) de Klant het Intermediate Certificate blijft gebruiken nadat het recht van de Klant op het gebruik daarvan eindigt, of (v) DigiCert redelijkerwijs van mening is dat de intrekking noodzakelijk is op basis van Industrienormen.

f. Beperkingen. Het is de Klant niet toegestaan om: (i) aanvullende intermediate certificates te maken of proberen te maken op basis van het Intermediate Certificate; (ii) het Intermediate Certificate te verkopen, distribueren, verhuren, leasen, in licentie te geven, toe te wijzen of anderszins aan een derde partij over te dragen; (iii) een door DigiCert verstrekt Intermediate Certificate te gebruiken nadat het is verlopen, ingetrokken of de onderhavige Overeenkomst is beëindigd; (iv) een door DigiCert verstrekt Intermediate Certificate te veranderen, wijzigen of herzien; of (v) het Intermediate Certificate te gebruiken wanneer de Klant reden heeft om aan te nemen dat de Private Key van het Intermediate Certificate is gecompromitteerd.

24. Merklicentie en Voorwaarden van Derden.

a. DigiCert kan bepaalde van zijn merken en logo's (ieder afzonderlijk een '**Merk**') beschikbaar stellen voor weergave door de Klant om te tonen dat een bepaald Certificaat is uitgegeven door DigiCert voor een bepaald eigendom van de Klant. Vanaf de uitgifte van het betreffende Certificaat en alleen zolang dat Certificaat geldig is en de Klant alle toepasselijke voorwaarden daarvoor volledig nakomt, verleent DigiCert de Klant een beperkte, herroepbare licentie voor de geldigheidsperiode van het betreffende Certificaat voor weergave van het betreffende Merk (in de door DigiCert aan de Klant verstrekte vorm) om het betreffende Certificaat op de juiste en niet-misleidende manier op de producten, domeinnamen of services van de Klant te laten zien. De Klant verklaart dat hij Merken op geen enkele manier zal wijzigen (inclusief het niet verwijderen of wijzigen van handelsmerktekens die DigiCert mogelijk aanbrengt op dergelijke Merken) of Merken voor een ongeschikt doel of op een wijze weer zal geven waardoor de relatie van de partijen verkeerd zou worden voorgesteld of de reputatie of goodwill die aan een Merk van DigiCert of andere handelsmerken of servicemerken van DigiCert is gekoppeld, zou verminderen of beschadigen, waaronder het gebruik van een Merk of Certificaat op een website die in verband zou kunnen worden gebracht met misdaad, fraude, misleiding, laster, smaad, obsceniteit, verduistering of inbreuk of waartegen DigiCert anderszins redelijkerwijs bezwaar zou kunnen hebben. Alle goodwill die voortvloeit uit het gebruik van Merken komt ten goede aan DigiCert en indien de Klant rechten, aanspraken of belangen op of in een Merk verkrijgt vanwege het gebruik van dat Merk, wijst de Klant hierbij al die rechten, aanspraken en belangen erin of erop onherroepelijk toe aan DigiCert.
b. De Klant is ervan op de hoogte en gaat ermee akkoord dat, wanneer het Certificaat van de Klant een wettelijke entiteitsidentificatie (Legal Entity Identifier of '**LEI**') bevat die wordt geleverd door Ubisecure Oy, de Servicevoorwaarden van Ubisecure Oy op https://rapidlei.com/documents/global-lei-system-terms van toepassing zijn op de LEI van de Klant en het gebruik van het RapidLEI Legal Entity Identifier Management System of opvolgende service.
c. De Klant is ervan op de hoogte en gaat ermee akkoord dat op zijn gebruik van de toolkit voor post-quantumcryptografie van DigiCert (de '**PQC-toolkit**') de volgende voorwaarden van toepassing zijn, naast alle andere voorwaarden van toepasselijke licentieovereenkomsten: (i) de aan de Klant toegekende licentie voor de PQC-toolkit is een niet-exclusieve, opzegbare licentie die alleen dient te worden gebruikt in verband met een DigiCert-certificaat met een handtekening en een openbare sleutel die is gegenereerd door of met de PQC-toolkit of verwante test- en configuratieactiviteiten; (ii) de Klant verkrijgt geen intellectueel eigendom of andere eigendomsrechten met betrekking tot de PQC-toolkit of daaraan verwant intellectueel eigendom; (iii) het is de Klant niet toegestaan de PQC-toolkit te reverse-engineeren, vertalen, demonteren, decompileren, ontsleutelen of ontmantelen; (iv) de Klant stopt met het gebruik van de PQC-toolkit bij beëindiging van de verwante Services van DigiCert; (v) ISARA Corporation kan op geen enkele wijze door de Klant aansprakelijk worden gesteld voor enige schade; (vi) de Klant is gerechtigd om de PQC-toolkit te importeren, exporteren en opnieuw te gebruiken uitsluitend in overeenstemming met de toepasselijke wetgeving in de landen of gebieden waarin de PQC-toolkit wordt gebruikt of geïmporteerd, of van waaruit de PQC-toolkit wordt geëxporteerd of wederuitgevoerd; (vii) DigiCert biedt namens ISARA Corporation geen expliciete of impliciete garanties met

betrekking tot het gebruik van de PQC-toolkit; en (viii) de Klant brengt geen wijzigingen aan in enig copyright-, handelsmerk- of patentteken in of bij de PQC-toolkit of daaraan verwante materialen.

25. Eisen omtrent overdracht van rechten en plichten Het is de Klant niet toegestaan om de technische implementatie van de systemen of software van DigiCert te monitoren, verstoren of reverse-engineeren of anderszins willens en wetens de beveiliging van de systemen of software van DigiCert te compromitteren, en de Klant dient dezelfde beperking op te leggen aan zijn aangewezen fabrikanten, indien van toepassing.

26. Door Microsoft vereiste aanvullende verplichtingen.

a. Indien de Klant het Microsoft-onderdeel Automatische Inschrijving gebruikt, zijn de volgende DOOR MICROSOFT VEREISTE AANVULLENDE VERPLICHTINGEN van toepassing:

b. Afwijzing van garanties. MICROSOFT EN ZIJN AFFILIATES GEVEN GEEN GARANTIE, EXPLICIET, IMPLICIET OF WETTELIJK VOOR DE UIT HOOFDE VAN DEZE OVEREENKOMST GELEVERDE SERVERSOFTWARE ('**SERVERSOFTWARE**'), EN ZIJN NIET VERANTWOORDELIJK VOOR DE PRESTATIES EN WERKING ERVAN. WAT MICROSOFT BETREFT, WORDT DE SERVERSOFTWARE GELEVERD IN DE HUIDIGE STAAT EN MET ALLE FOUTEN, EN MICROSOFT EN ZIJN AFFILIATES WIJZEN HIERBIJ ALLE ANDERE EXPLICIETE, IMPLICIETE OF WETTELIJKE GARANTIES, PLICHTEN EN VOORWAARDEN AF, INCLUSIEF, MAAR NIET BEPERKT TOT, ALLE (EVENTUELE) IMPLICIETE GARANTIES, VOORWAARDEN MET BETREKKING TOT COMMERCIËLE BRUIKBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL, BETROUWBAARHEID OF BESCHIKBAARHEID, ALLEMAAL MET BETREKKING TOT DE SERVERSOFTWARE. OOK GEVEN MICROSOFT EN ZIJN AFFILIATES GEEN GARANTIE MET BETREKKING TOT EIGENDOMSRECHTEN, ONGESTOORD GEBRUIK, OVEREENKOMSTIGHEID MET BESCHRIJVING OF NIET-INBREUK AF WAT BETREFT DE SERVERSOFTWARE.

c. Uitsluiting van bepaalde schade. IN DE VOLGENS DE TOEPASSELIJKE WETGEVING MAXIMAAL TOEGESTANE MATE IS MICROSOFT IN GEEN GEVAL AANSPRAKELIJK VOOR SPECIALE, INCIDENTELE, PUNITIEVE, INDIRECTE OF GEVOLGSCHADE IN WELKE VORM DAN OOK (WAARONDER, MAAR NIET BEPERKT TOT, SCHADE DOOR WINSTDERVING OF VERLIES VAN (VERTROUWELIJKE) INFORMATIE, BEDRIJFSONDERBREKING, PERSOONLIJK LETSEL, INBREUK OP PRIVACY, NIET-NAKOMING VAN EEN PLICHT INCLUSIEF TE GOEDER TROUW OF REDELIJKE ZORG, NALATIGHEID EN ENIG ANDER (GELDELIJK) VERLIES IN WELKE VORM DAN OOK) DIE VOORTVLOEIT UIT OF OP EEN OF ANDERE MANIER VERBAND HOUDT MET HET AL DAN NIET KUNNEN GEBRUIKEN VAN DE SERVERSOFTWARE, HET AL DAN NIET VERLENEN VAN ONDERSTEUNING OF ANDERE DIENSTEN, INFORMATIE, SOFTWARE EN GERELATEERDE INHOUD VIA DE SERVERSOFTWARE OF DIE ANDERSZINS VOORTVLOEIT UIT HET GEBRUIK VAN SERVERSOFTWARE, OF ANDERSZINS VOLGENS OF IN VERBAND MET EEN VAN DEZE VOORWAARDEN VOOR DE SERVICEBESCHRIJVING, ZELFS IN HET GEVAL VAN SCHULD, ONRECHTMATIGE DAAD (WAARONDER NALATIGHEID), RISICOAANSPRAKELIJKHEID, CONTRACTBREUK OF SCHENDING VAN GARANTIE VAN MICROSOFT; ZELFS ALS MICROSOFT OVER DE MOGELIJKHEID VAN DIE SCHADE IS INGELICHT.

d. Serversoftwarevereisten. De Klant is gerechtigd om slechts één (1) exemplaar (tenzij anderszins gespecificeerd in de betreffende Bestelling) van de uit hoofde van deze Overeenkomst geleverde Serversoftware te gebruiken zoals gespecificeerd in de bij deze software geleverde documentatie, en alleen voor samenwerking en communicatie met de besturingssystemen Microsoft Windows 2000 Professional, Windows XP Home of Professional of Vista Client (of opvolgers daarvan). Het is de Klant niet toegestaan om de Serversoftware op een Personal Computer te gebruiken. In het kader van het voorgaande betekent een '**Personal Computer**' elke computer die is geconfigureerd om primair te worden gebruikt door één persoon tegelijk, en die is voorzien van beeldscherm en toetsenbord.

e. Externe begunstigde. Niettegenstaande eventuele tegenstrijdige voorwaarden in de Overeenkomst gaat de Klant er hierbij mee akkoord dat Microsoft Corporation, als licentiegever van het intellectuele eigendom dat deel uitmaakt van de Serversoftware, wordt beschouwd als externe begunstigde van de voorwaarden in dit artikel 26 met het recht om alle voorwaarden hierin af te dwingen die gevolgen hebben voor het ingesloten intellectuele eigendom van Microsoft of andere Microsoft-belangen met betrekking tot de voorwaarden hiervan.

f. Serverklasse 2. Indien de Klant Serverklasse 2 heeft gekozen, is de Klant gerechtigd om de Serversoftware te gebruiken op een server (a) die niet meer dan vier (4) processoren bevat, waarbij elke processor maximaal

tweeëndertig (32) bits en vier (4) gigabytes RAM-geheugen heeft, en (b) waarvan het geheugen niet kan worden uitgebreid, gewijzigd of verwijderd zonder dat de server waarop deze draait opnieuw moet worden gestart ('**Hot-swappingmogelijkheden**'). De Klant mag de Serversoftware niet gebruiken in combinatie met software die Hot-swappingmogelijkheden of Clusteringmogelijkheden ondersteunt, waarbij met '**Clusteringmogelijkheden**' de mogelijkheid wordt aangeduid om een groep servers te laten functioneren als één platform met hoge beschikbaarheid voor het uitvoeren van applicaties met applicatie-failover tussen Serverknooppunten in de groep.

g. Controlerechten. Om naleving van al deze voorwaarden door de Klant te toetsen, is DigiCert gerechtigd op locatie bij de Klant tijdens normale kantooruren een controle uit te voeren en de faciliteiten en procedures van de Klant te inspecteren, na een vooraankondiging van niet minder dan veertien (14) dagen. Niettegenstaande eventuele tegenstrijdige voorwaarden in de Overeenkomst (inclusief, maar niet beperkt tot, geheimhoudingsbepalingen), gaat de Klant ermee akkoord dat, indien de Klant een dergelijke controle weigert en DigiCert reden heeft om aan te nemen dat de Klant de voorwaarden van de Servicebeschrijving niet naleeft, DigiCert het recht heeft (i) de identiteit van de Klant bekend te maken aan Vertrouwende Partijen en Applicatiesoftwareleveranciers, alsmede (ii) de basis voor de aanname van DigiCert wat betreft de niet-nakoming.

h. Multiplexingapparaten. Hardware of software die het aantal gebruikers vermindert dat direct toegang heeft tot door de Serversoftware geleverde services of daarvan gebruikmaakt, vermindert niet het aantal gebruikers dat geacht wordt toegang te krijgen tot door de Serversoftware geleverde services of dat geacht wordt daarvan gebruik te maken. Het aantal gebruikers dat toegang heeft tot de Serversoftware of daarvan gebruikmaakt, is gelijk aan het aantal gebruikers dat, hetzij direct, hetzij via een Multiplexingapparaat, toegang heeft tot services, of daarvan gebruikmaakt, die worden geleverd door (a) de Serversoftware of (b) elk(e) ander(e) software of systeem waarbij de authenticatie of autorisatie voor die software of dat systeem wordt geleverd door de Serversoftware (een '**Ander Geauthenticeerd Systeem**'). Zoals hier gebruikt, betekent '**Multiplexingapparaat**' elke hardware of software die (in)direct toegang biedt of verkrijgt tot services die worden geleverd door de Serversoftware of elk Ander Geauthenticeerd Systeem aan of namens meerdere andere gebruikers via een beperkt aantal verbindingen.

i. Windows CAL-vereiste. De Klant moet een aparte Windows CAL aanschaffen en toewijzen voor elke gebruiker die, direct of via of vanaf een Multiplexingapparaat, toegang krijgt tot services, of daarvan gebruikmaakt, die worden geleverd door de Serversoftware of elk Ander Geauthenticeerd Systeem. '**Windows CAL**' betekent (a) een Client Access License voor een Windows-apparaat ('**CAL**'), of een CAL voor een Windows-gebruiker, in beide gevallen voor een serverbesturingssysteem van Microsoft Windows Server 2003 (Standard Edition, Enterprise Edition of Datacenter Edition) (of opvolgers daarvan) ('**Windows-server**'); of (b) een Microsoft Core CAL die een individuele persoon of elektronisch apparaat rechten op toegang tot een Windows-server en gebruik daarvan biedt, in een van beide gevallen (a) of (b) hierboven die de Klant heeft gekocht voor gebruik met een of meer van dergelijke Microsoft Windows Server-besturingssystemen en die per gebruiker of per apparaat wordt gebruikt.

27. Door Adobe vereiste aanvullende verplichtingen.

Indien er Adobe Signing Certificates worden uitgegeven aan de Klant, gaat de Klant akkoord met:

a. naleving van de Adobe Systems Inc. AATL Certificate Policy 2.0, die momenteel beschikbaar is op https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf, inclusief, maar niet beperkt tot: (1) het uitsluitend genereren en opslaan van Sleutelsets voor Adobe Signing Certificates op een apparaat van FIPS 140-2 niveau 2; en (2) bij de registratie van een nieuwe account, of op ieder moment dat een nieuwe registratie van een AATL-certificaat wordt gestart voor een abonnee: het verstrekken van nauwkeurige en waarheidsgetrouwe informatie aan DigiCert, waarvoor is vereist dat (A) een accountbeheerder een grondige identiteitscontrole uitvoert, tijdens een persoonlijke ontmoeting met DigiCert of op basis van een procedure die dezelfde mate van zekerheid biedt (bijv. via beveiligde videocommunicatie); (B) een accountbeheerder een grondige identiteitscontrole uitvoert tijdens een persoonlijke ontmoeting met de abonnees (oftewel de eindgebruikers), en de opname lokaal opslaat voor controledoeleinden, totdat DigiCert de beheerder een online mechanisme biedt voor het uploaden van verklaringen en opnames; en (C) de identiteitscontrole, ongeacht of die van een beheerder of een abonnee is, een opname van de abonnee omvat waarop zowel de persoon als een

geldig, door de overheid uitgegeven identiteitsbewijs (zoals een rijbewijs, paspoort, identiteitskaart) met een overeenkomende pasfoto van de abonnee zichtbaar is; en

b. de voorwaarden van de toepasselijke Certification Practices Statement.

28. **Aanvullende beperkingen voor Code Signing Certificates.** Het is de Klant niet toegestaan een code signing Certificate te gebruiken: (i) voor of namens een andere organisatie dan de organisatie van de Klant; (ii) voor de uitvoering van activiteiten met een Private Key of Public Key die betrekking hebben op een ander domein en/of de naam van een andere organisatie dan die de Klant bij de Certificaataanvraag heeft vermeld; (iii) voor het verspreiden van Verdachte Code; of (iv) op een zodanige manier dat controle wordt overdragen of toestemming wordt gegeven voor toegang tot de Private Key die bij de Public Key van een Certificaat hoort, aan iemand anders dan een werknemer die de Klant heeft gemachtigd (een dergelijke overdracht moet op een beveiligde manier plaatsvinden ter bescherming van de Private Key).

    Voor alle OV code signing Certificates die zijn uitgegeven op of na 1 juni 2023, inclusief verlengde of opnieuw uitgegeven Certificaten, geldt dat alle Private Keys dienen te zijn opgeslagen op hardware die is gecertificeerd voor FIPS 140 niveau 2, Common Criteria EAL 4+ of het equivalent daarvan. Voor alle OV code signing Certificates die zijn uitgegeven voor 1 juni 2023, inclusief verlengde of opnieuw uitgegeven Certificaten, geldt dat alle Private Keys dienen te zijn opgeslagen op hardwaretokens.

29. **Aanvullende beperkingen voor niet-openbare TLS/SSL-certificaten.** TLS/SSL-certificaten die aan een Persoonlijk Root Certificate zijn gekoppeld, dienen alleen te worden gebruikt met intranetdomeinen. Het is niet toegestaan deze toe te wijzen aan apparaten die vanaf het internet openbaar toegankelijk zijn. DigiCert behoudt zich het recht voor de openbaar toegankelijke internetservers en/of apparaten te monitoren om te garanderen dat persoonlijke TLS/SSL-certificaten voldoen aan de bepalingen in deze clausule. Indien DigiCert ontdekt dat een of meerdere persoonlijke TLS/SSL-certificaten niet in overeenstemming met deze clausule worden gebruikt, informeert DigiCert de Klant onmiddellijk over deze niet-nakoming. De Klant moet, binnen vierentwintig (24) uur, (i) het persoonlijke TLS/SSL-certificaat naar een intranetdomein verplaatsen; of (ii) het persoonlijke TLS/SSL-certificaat van de servers van de Klant verwijderen en intrekken. Indien de Klant het Certificaat dat niet aan de voorwaarden voldoet niet intrekt of verwijdert, is DigiCert gerechtigd om het Certificaat in te trekken.

30. **Hulpmiddelen voor elektronische communicatie/kennisgeving.** Wanneer de Klant gebruikmaakt van e-mail of andere hulpmiddelen voor elektronische communicatie of kennisgeving ('**Kennisgevingshulpmiddelen**') die door DigiCert worden geleverd voor het verzenden van communicatie-uitingen of kennisgevingen ('**Communicatie-uitingen**') gaat de Klant ermee akkoord dat (1) de inhoud van dergelijke Communicatie-uitingen strikt beperkt is tot communicatie of kennisgevingen over producten of services van DigiCert; (2) de Klant de toepasselijke wetgeving (inclusief toepasselijke wetgeving op het gebied van elektronische communicatie en wetgeving op het gebied van gegevensprivacy/gegevensbescherming) naleeft in de rechtsgebieden van de ontvangers van de Communicatie-uitingen; (3) de Klant als enige verantwoordelijk is voor de inhoud van de Communicatie-uitingen die de Klant verzendt met de Kennisgevingshulpmiddelen; en (4) de Klant DigiCert schadeloosstelt, behoedt voor en vrijwaart tegen claims van derde partijen, maatregelen of boetes van de overheid en alle aansprakelijkheid, schade en kosten, inclusief redelijke advocaatkosten die voortvloeien uit het gebruik van de Klant van de Kennisgevingshulpmiddelen of uit de inhoud van Communicatie-uitingen die door de Klant zijn verzonden met de Kennisgevingshulpmiddelen.

31. **Survivalclausule en beëindiging.** De Gebruiksvoorwaarden voor Certificaten blijven van toepassing na de beëindiging van de Overeenkomst, totdat alle uitgegeven Certificaten zijn verlopen of ingetrokken.