

PKI VOOR E-MAIL VAN DIGICERT

GEBRUIKSVOORWAARDEN VOOR CERTIFICATEN

OPENBAAR VERTROUWDE S/MIME-CERTIFICATEN

1. Toepassingsgebied en doel

Korte versie: Deze voorwaarden zijn alleen van toepassing op de openbaar vertrouwde S/MIME-certificaten van DigiCert. Ze bevatten het certificaatbeleid en de certificeringspraktijkverklaring (CP/CPS) van DigiCert en weerspiegelen de industrienormen (zoals de CA/Browser Forum S/MIME Baseline Requirements en root store-beleidsregels zoals die van Mozilla) die van toepassing zijn op openbaar vertrouwde S/MIME-certificaten.

Deze voorwaarden ("Voorwaarden") zijn van toepassing op openbaar vertrouwde S/MIME-certificaten uitgegeven door DigiCert of de gelieerde ondernemingen van DigiCert. Ze zijn niet van toepassing op (browser vertrouwde) TLS/SSL-certificaten, persoonlijke/interne S/MIME-, codeondertekening-, documentondertekening- of EU-gekwalficeerde certificaten. De Voorwaarden omvatten de openbaar vertrouwde CP/CPS van DigiCert (de "CP/CPS"), beschikbaar op <https://www.digicert.com/legal-repository/>, die samen met de Voorwaarden uiteenzet hoe S/MIME-certificaten worden uitgegeven, beheerd en ingetrokken. Deze Voorwaarden weerspiegelen het beleid en de voorschriften die zijn vastgesteld door het CA/Browser Forum S/MIME Baseline Requirements, beschikbaar op www.cabforum.org/working-groups/smime/documents/ ("Baseline Requirements") en het toepasselijke beleid voor root stores (bijv. Mozilla, Microsoft, Apple). **Als certificeringsinstantie (Certification Authority, CA) is DigiCert verplicht om zich aan deze industrienormen te houden, waaronder het onmiddellijk intrekken van certificaten wanneer dat nodig is, zonder uitzondering.**

2. Gebruik van S/MIME-certificaten

U mag DigiCert S/MIME-certificaten alleen gebruiken om e-mail te beveiligen in verband met ondertekening, versleuteling en gerelateerde clientverificatie. U mag deze niet gebruiken voor TLS/SSL-webservers, codeondertekening, documentondertekening of andere niet-gerelateerde doeleinden.

Toegestaan gebruik:

- Het ondertekenen van e-mail om de afzender en integriteit van het bericht te verifiëren
- Het versleutelen van e-mail om vertrouwelijkheid te bieden
- Clientverificatie, indien in overeenstemming met de extensies en beleidslijnen van het certificaat

Verboden gebruik:

- TLS/SSL (webserververificatie)
- Codeondertekening of documentondertekening (tenzij specifiek aangewezen)
- Elk gebruik buiten het beoogde toepassingsgebied

Het gebruik van een S/MIME-certificaat van DigiCert voor een verboden doel is een reden voor intrekking (raadpleeg hieronder het gedeelte **Intrekking**).

3. Een certificaat aanvragen

Korte versie: Wanneer u een S/MIME-certificaat aanvraagt, verklaart u dat de informatie juist is en dat u bevoegd bent om het certificaat aan te vragen voor het e-mailadres/domein en (indien van toepassing) de organisatie.

Wanneer u een certificaat aanvraagt, moet u nauwkeurige, volledige en waarheidsgetrouwe informatie verstrekken. Hieronder vallen het e-mailadres, gegevens over de organisatie en alle andere gegevens die nodig zijn voor de uitgifte.

Door een certificaat aan te vragen, verklaart en garandeert u dat: **(a)** u de wettelijke rechten of bevoegdheden hebt om de domeinnamen (en eventuele organisatienamen of persoonsnamen, indien van toepassing) die in de certificaataanvraag worden vermeld, te gebruiken en te beheren, en **(b)** uw certificaataanvraag en beoogd gebruik **geen inbreuk maken** op de intellectuele eigendoms- of wettelijke rechten van derden. Misbruik van het inschrijvingsproces of het verstrekken van valse, misleidende of onbevoegde informatie vormt een wezenlijke schending van deze Voorwaarden. DigiCert zal elke certificaataanvraag die in strijd is met deze regels weigeren, en **elk certificaat dat op basis van valse of misleidende informatie is uitgegeven, kan onmiddellijk worden ingetrokken.**

4. Verificatie vóór uitgifte

Korte versie: DigiCert verifieert of u controle hebt over het e-mailadres (of het domein) en voor bepaalde certificaattypen verifieert het ook de persoon of organisatie.

Voordat een openbaar vertrouwd S/MIME-certificaat wordt uitgegeven, voert DigiCert de voorgeschreven validatiestappen uit in overeenstemming met de CP/CPS en de Basiseisen. Dit zijn:

- **Mailbox-gevalideerd (MV):** DigiCert verifieert of het e-mailadres dat in het certificaat wordt opgenomen onder uw controle staat. Dit kan gebeuren door een verificatie-e-mail te sturen, een DNS-record voor het domein te vragen of andere goedgekeurde methoden voor mailboxcontrole te gebruiken. DigiCert controleert ook DNS CAA-records op eventuele 'issuemail'-eigenschappen die uitgifte toestaan of verbieden.
- **Organisatie gevalideerd (OV):** Naast de e-mailcontrole verifieert DigiCert ook het wettelijke bestaan, de operationele status en de bevoegdheid van de organisatie om het e-maildomein te gebruiken. Dit kan onder meer bestaan uit het verifiëren van officiële registergegevens, het controleren van adressen en telefoonnummers en het vergelijken van gegevens met die van externe bronnen.
- **Sponsor gevalideerd (SV):** DigiCert valideert het e-mailadres en bevestigt dat de organisatie de individuele certificaathouder heeft gesponsord. De sponsororganisatie moet worden geverifieerd en moet de aanvrager aanwijzen.
- **Persoon gevalideerd (IV):** DigiCert verifieert de identiteit van de natuurlijke persoon, doorgaans aan de hand van een door de overheid uitgegeven identiteitsbewijs met foto, notariële akte of gelijkwaardige methode, en controleert of de persoon de controle heeft over het e-mailadres.

Als DigiCert de validatie niet naar tevredenheid kan voltooien, zal er geen certificaat worden uitgegeven. DigiCert kan ook weigeren een certificaat uit te geven als er een risico bestaat op fraude of niet-naleving van branchenormen of processen.

5. Verklaringen, garanties en vrijwaring van de registratie-instantie (“RA”)

Als uw organisatie optreedt als een RA, verklaart en garandeert u dat:

- a. u alle functies voor identiteitsvalidatie en certificaataanvraag uitvoert in volledige overeenstemming met de CP/CPS, Basiseisen en deze Voorwaarden;
- b. u over getraind personeel beschikt, passende antecedentenonderzoeken hebt uitgevoerd en een veilige infrastructuur onderhoudt om uw RA-taken te vervullen; en
- c. u nauwkeurige gegevens bijhoudt en auditrechten ondersteunt zoals voorgeschreven op grond van de CP/CPS en Basiseisen.

U gaat ermee akkoord om DigiCert, en de gelieerde ondernemingen ervan, en hun respectieve directeuren, functionarissen, agents, werknemers, rechtsopvolgers en rechtverkrijgenden te vrijwaren, te verdedigen en schadeloos te stellen van claims, schade, verliezen, verplichtingen of kosten (met inbegrip van redelijke advocatenhonoraria) die voortvloeien uit of verband houden met uw handelingen of nalatigheden als een RA, waaronder, maar niet beperkt tot: (i) het niet uitvoeren van identiteitsverificatie in overeenstemming met de CP/CPS, Basiseisen en deze Voorwaarden, (ii) het uitgeven van of een verkeerde voorstelling, geven van certificaatinformatie, of (iii) het onbevoegd gebruik of de onbevoegde openbaarmaking van persoonlijke sleutels of gegevens van sollicitanten.

6. De geldigheid van certificaten

Korte versie: *Certificaten hebben een beperkte levensduur. Het toegestane maximum is 825 dagen (ongeveer 27 maanden). U moet ze vervangen voordat ze verlopen.*

Openbaar vertrouwde S/MIME-certificaten verliezen na beperkte tijd hun geldigheid. Op dit moment is de maximum toegestane geldigheid op grond van de Basiseisen 825 dagen. De praktijken in de branche kunnen in de toekomst leiden tot kortere levensduur. DigiCert kan voor het gemak abonnementsvoorwaarden aanbieden, maar certificaten worden nog steeds opnieuw uitgegeven op door de branche voorgeschreven tussenpozen.

Het is uw verantwoordelijkheid om de vervaldatum van elk certificaat in de gaten te houden en voordat het verloopt een vervangend certificaat aan te schaffen en te installeren. Als een certificaat verloopt, zullen alle systemen die ervan afhankelijk zijn fouten vertonen of geen veilige verbinding meer kunnen maken. Verlopen certificaten mogen niet meer worden gebruikt. Het blijven gebruiken van een verlopen certificaat is onveilig en schendt deze Voorwaarden. U moet ervoor zorgen dat certificaten onmiddellijk na het verlopen worden verwijderd of vervangen.

DigiCert raadt u ten zeerste aan om automatisering (zoals CertCentral® API's, Trust Lifecycle Manager of andere geautomatiseerde tools) te gebruiken voor het afhandelen van verlengingen en vervangingen.

7. Uw verantwoordelijkheden als abonnee

Korte versie: Door een S/MIME-certificaat van DigiCert te gebruiken of aan te vragen, verbindt u zich ertoe bepaalde verplichtingen na te komen. Samengevat: moet u **(a)** nauwkeurige informatie verstrekken, **(b)** uw persoonlijke sleutel beschermen, **(c)** de inhoud van het certificaat controleren en accepteren, **(d)** het certificaat alleen gebruiken zoals toegestaan (voor het gevalideerde e-mailadres en in overeenstemming met de wetgeving en het beleid), **(e)** onmiddellijk verzoeken om intrekking en het gebruik staken als de persoonlijke sleutel is aangetast of als de certificaatinformatie onjuist wordt, **(f)** het gebruik van het certificaat (en de sleutel ervan) staken bij het verlopen of intrekken (behalve dat u de sleutel uitsluitend mag behouden om eerder ontvangen e-mail te decoderen wanneer dat is toegestaan), **(g)** onmiddellijk reageren op vragen van DigiCert over beveiligingskwesties, en **(h)** het recht van DigiCert om het certificaat indien nodig in te trekken erkennen en ermee akkoord gaan. Deze verplichtingen komen voort uit branchenormen die alle abonnees moeten naleven.

Als abonnee (certificaathouder) hebt u belangrijke verplichtingen om ervoor te zorgen dat uw S/MIME-certificaat veilig en in overeenstemming met deze Voorwaarden, de CP/CPS en de toepasselijke normen wordt gebruikt. U verklaart en garandeert hierbij aan DigiCert en aan de begunstigten van het certificaat dat u het volgende zult doen:

a. Nauwkeurigheid van informatie. U verstrekt te allen tijde nauwkeurige en volledige informatie in uw certificaataanvraag en in alle communicatie met DigiCert met betrekking tot uw S/MIME-certificaten. U zult alle informatie onmiddellijk bijwerken als deze tijdens de validatie verandert. Als de door u verstrekte informatie verouderd of onjuist is geworden (bijvoorbeeld als uw officiële naam, de naam van de organisatie of het adres is gewijzigd, of als u niet langer de controle hebt over of rechtmatig gebruikmaakt van een e-mailadres dat in het certificaat is opgenomen), dient u die informatie onmiddellijk bij DigiCert bij te werken of DigiCert op de hoogte te stellen van de wijziging.

b. Bescherming van de persoonlijke sleutel. U genereert de persoonlijke sleutel van uw certificaat op veilige wijze met behulp van betrouwbare systemen en sterke cryptografische normen (**minimaal een 2048-bits RSA-sleutel of een ECC-sleutel met een gelijkwaardige sterkte die is toegestaan volgens de Basiseisen**). U moet de persoonlijke sleutel te allen tijde vertrouwelijk en onder uw exclusieve controle houden, met behulp van maatregelen die voldoende zijn om verlies, openbaarmaking of ongevoegd gebruik te voorkomen (bijvoorbeeld sterke wachtwoordzinnen, beveiligde sleutelopslagplaatsen of tokens, geschikte apparaat- en accountcontroles). U bent verantwoordelijk voor het behouden van toegang tot persoonlijke sleutels die worden gebruikt voor het **ontsleutelen van e-mails**, zodat u eerder ontvangen versleutelde berichten kunt lezen. Indien toegestaan door het beleid en de wetgeving, wordt het aanbevolen om een veilige back-up/escrow voor sleutels voor het ontsleutelen aan te houden. (Deel uw persoonlijke sleutel niet met derden, behalve zoals toegestaan door de CPS, zoals via een goedgekeurd mechanisme voor het beheer van bedrijfsleutels.)

c. Acceptatie van een certificaat. Nadat DigiCert uw certificaat heeft uitgegeven, controleert u de gegevens van het certificaat (zoals de naam van de aanvrager, het/de e-mailadres(sen) van rfc822Name en eventuele gegevens van de organisatie) om er zeker van te zijn dat alle informatie correct is. U mag het certificaat alleen gebruiken als u hebt geverifieerd dat de gegevens erin juist zijn en u deze accepteert. Door het certificaat te gebruiken, geeft u aan dat u het accepteert. Als u onjuistheden constateert, dan moet u contact opnemen met DigiCert om het certificaat in te trekken of opnieuw uit te geven voordat u het gebruikt.

d. Gebruik van een certificaat. U mag het certificaat alleen installeren en gebruiken op uw eigen e-mailclients, apparaten en systemen (of die u gemachtigd bent om te gebruiken) die e-mail verzenden en/of ontvangen voor het/de gevalideerde e-mailadres(sen) die in het certificaat worden vermeld. U stemt ermee in het certificaat uitsluitend te gebruiken in overeenstemming met deze Voorwaarden (met inbegrip van de CP/CPS). Het certificaat mag **niet** worden gebruikt voor andere doelen dan waarvoor het bedoeld is (d.w.z. **e-mailondertekening en -versleuteling** en gerelateerde clientverificatie) en mag **niet** worden gebruikt voor server-TLS/SSL, codeondertekening, documentondertekening (tenzij expliciet geprofileerd) of enig ander gebruik dat buiten het beoogde toepassingsgebied valt.

e. Melding en intrekking. Als u vermoedt of constateert dat de persoonlijke sleutel van het certificaat daadwerkelijk of mogelijk is gecompromitteerd, of dat er misbruik wordt gemaakt van het certificaat (waaronder phishing, fraude of ander onwettig gebruik), moet u DigiCert **onmiddellijk** op de hoogte stellen en direct verzoeken om intrekking van het certificaat. Evenzo moet u, als enige informatie in het certificaat op enig moment onjuist, onnauwkeurig of misleidend is of wordt (bijvoorbeeld als een e-mailadres wordt toegewezen aan iemand anders/niet meer bestaat of als de gegevens van de organisatie veranderen), onmiddellijk stoppen met het gebruik van het certificaat en DigiCert verzoeken om het certificaat in te trekken.

f. Beëindiging van het gebruik. Als een certificaat om welke reden dan ook wordt ingetrokken of als de vervaldatum ervan is bereikt, moet u het certificaat onmiddellijk van alle systemen verwijderen en **elk gebruik van** het certificaat en van die persoonlijke sleutel voor het ondertekenen of presenteren van vertrouwen aan vertrouwende partijen staken. Het gebruik van een **verlopen of ingetrokken** certificaat voor enig doel dat voortdurend vertrouwen vereist, is ten strengste verboden. *Voor alle duidelijkheid:* het bewaren van de persoonlijke sleutel **uitsluitend om eerder ontvangen e-mails te ontsleutelen** (of voor wettelijke archiverings-/registratieverplichtingen) is toegestaan indien dit door het beleid en de wet wordt toegestaan; u mag de sleutel niet gebruiken om e-mails te blijven ondertekenen of om op andere wijze intrekking of verval te omzeilen.

g. Reactie. U zult onmiddellijk reageren op vragen of instructies van DigiCert met betrekking tot uw certificaat of de bijbehorende sleutel. Tijdige samenwerking kan van cruciaal belang zijn om veiligheidsrisico's te beperken of om te voldoen aan de **intrekkingseisen** van de branche. Het niet tijdig reageren op beveiligingsvragen of aanwijzingen van DigiCert vormt een schending van deze Voorwaarden en kan leiden tot intrekking van het certificaat.

h. Erkenning van intrekkingsrechten. U erkent en accepteert dat DigiCert, als certificeringsautoriteit, het recht heeft om uw certificaat op elk moment en zonder voorafgaande kennisgeving in te trekken als u deze Voorwaarden schendt, of als intrekking vereist is om te voldoen aan de CP/CPS van DigiCert, de toepasselijke wetgeving of branchenormen. U gaat ermee akkoord dat u geen bezwaar zult maken tegen een dergelijke intrekking of deze zult belemmeren, en u doet afstand van enig recht om schadevergoeding of rechtsmiddelen te eisen van DigiCert voor een intrekking die in overeenstemming met deze Voorwaarden is uitgevoerd. ***Volgens de branchenormen moeten CA's certificaten op korte termijn intrekken (bijvoorbeeld binnen 24 uur voor bepaalde kritieke incidenten en binnen 5 dagen voor andere genoemde gebeurtenissen). U erkent dat DigiCert zich aan deze niet-onderhandelbare termijnen moet houden en stemt ermee in om in dergelijke gevallen dienovereenkomstig te handelen.***

8. Intrekking (wanneer en waarom)

Korte versie: Voor sommige gebeurtenissen moet een certificaat worden ingetrokken voordat het normaal verloopt. DigiCert moet snel handelen om de veiligheid te waarborgen en te voldoen aan de branchenormen. U bent verplicht om te helpen en mag de intrekking niet belemmeren.

In sommige gevallen moet u om intrekking verzoeken (bijvoorbeeld als uw persoonlijke sleutel is gecompromitteerd of als u geen controle meer hebt over een e-mailadres). In andere gevallen moet DigiCert een certificaat zelfs zonder uw aanvraag vaak op korte termijn intrekken. Deze intrekkingsverplichtingen zijn niet onderhandelbaar en worden vereist door branchenormen, waaronder de Basiseisen en toepasselijke root store-beleidsregels (bijv. het beleid van Mozilla). De onderstaande termijnen zijn van toepassing.

Intrekking binnen 24 uur (vereist)

DigiCert zal certificaten binnen 24 uur intrekken als één van de volgende situaties zich voordoet:

- a. U verzoekt DigiCert schriftelijk het certificaat in te trekken.
- b. U informeert DigiCert dat de oorspronkelijke certificaataanvraag niet geautoriseerd was.
- c. DigiCert heeft bewijs dat uw persoonlijke sleutel is gecompromitteerd.
- d. DigiCert is op de hoogte gebracht van een aangetoonde of bewezen methode waarmee uw persoonlijke sleutel eenvoudig kan worden berekend op basis van de openbare sleutel in het certificaat.
- e. DigiCert verkrijgt bewijs dat de validatie van domeinautorisatie of -controle voor identiteitsinformatie van onderwerpen in het certificaat niet betrouwbaar is.

Intrekking binnen 5 dagen (verplicht)

DigiCert zal certificaten binnen 5 dagen intrekken als één van de volgende situaties zich voordoet:

- a. Het certificaat voldoet niet langer aan de vereiste technische normen (bijvoorbeeld, de cryptografische of sleutelgrootte is niet langer toegestaan op grond van de Basiseisen of het toepasselijke root store-beleid).
- b. DigiCert heeft bewijs dat het certificaat is misbruikt.
- c. DigiCert wordt erop gewezen dat u een wezenlijke verplichting van deze Voorwaarden hebt geschonden.
- d. DigiCert verkrijgt bewijs dat de validatie van controle voor een e-mailadres of domeinonderdeel in het certificaat niet betrouwbaar is.
- e. DigiCert wordt op de hoogte gebracht van een wezenlijke wijziging in de informatie die oorspronkelijk in het certificaat is opgenomen.
- f. DigiCert wordt erop gewezen dat het certificaat niet is afgegeven in volledige overeenstemming met de Basiseisen of de CP/CPS.
- g. DigiCert stelt vast dat de informatie in het certificaat onnauwkeurig is.
- h. Het recht van DigiCert om certificaten uit te geven op grond van de Basiseisen vervalt of wordt ingetrokken of beëindigd, tenzij DigiCert regelingen heeft getroffen om het CRL/OCSP-repository te blijven onderhouden.
- i. Intrekking is vereist door de CP/CPS van DigiCert om een reden die hierboven niet wordt vermeld.
- j. DigiCert wordt op de hoogte gebracht van een aangetoonde of bewezen methode die uw persoonlijke sleutel blootstelt aan compromittering, of als er duidelijk bewijs is dat de specifieke methode die is gebruikt om de persoonlijke sleutel te genereren, gebrekkig was.

Als DigiCert vaststelt dat intrekking om één van de bovenstaande redenen noodzakelijk is, zal het zo snel mogelijk overgaan tot intrekking van het certificaat. Bepaalde ernstige bedreigingen vereisen intrekking op korte termijn. DigiCert houdt zich aan de branchevoorschriften dat het bij kritieke gebeurtenissen binnen 24 uur moet intrekken en bij andere genoemde gebeurtenissen binnen 5 dagen moet intrekken. In overeenstemming met de CP/CPS- en branche-eisen zal DigiCert probleemrapporten onmiddellijk onderzoeken en de **intrekking niet langer uitstellen** dan de toegestane termijn. Als uw certificaat wordt ingetrokken of is ingetrokken, stuurt DigiCert doorgaans zo snel mogelijk een bericht naar het geregistreerde e-mailadres van de contactpersoon, met een korte uitleg van de reden. Zodra een certificaat is ingetrokken, wordt het als ingetrokken gepubliceerd in de intrektingsregisters van DigiCert (CRL en/of OCSP) en moet het worden vervangen door een nieuw certificaat om de dienstverlening te kunnen voortzetten. U gaat ermee akkoord dat DigiCert het recht heeft om uw certificaat in te trekken en u accepteert de gevolgen van een dergelijke intrekking. DigiCert is niet aansprakelijk voor eventuele verliezen of schade die u ondervindt als gevolg van een intrekking die wordt opgelegd door deze Voorwaarden, de CP/CPS of branchenormen.

9. Openbaarmaking

DigiCert kan eigen repositories en statusservices onderhouden waar certificaatinformatie en intrektingsstatus beschikbaar zijn (bijvoorbeeld OCSP-respondenten, CRL's en websites met certificaatstatus), zoals toegestaan door de CPS en de Basiseisen. Deze zijn bedoeld voor publiek gebruik. Door het certificaat te gebruiken, erkent u dat de status ervan (geldig/ingetrokken/verlopen) via dergelijke mechanismen openbaar kan worden gemaakt.

10. Niet-ondersteunde praktijken (gebruiken op eigen risico)

*Korte versie: Sommige praktijken met betrekking tot certificaatgebruik worden **sterk afgeraden en worden niet ondersteund** door DigiCert. Als u deze praktijken toepast, doet u dit op eigen risico en is het mogelijk dat DigiCert u geen ondersteuning kan bieden of niet kan ingaan op speciale aanvragen die voortvloeien uit deze keuzes. Vermijd met name het hardcoderen (vastzetten) van certificaten of sleutels in applicaties en probeer niet één certificaat voor meerdere onverenigbare doeleinden te gebruiken. Dergelijke praktijken kunnen leiden tot onderbrekingen of niet-naleving.*

Bepaalde praktijken worden **sterk afgeraden of niet ondersteund** bij het gebruik van certificaten van DigiCert. Deelname aan deze praktijken is op **eigen risico**, en de verplichtingen van DigiCert om u te ondersteunen of tegemoet te komen kunnen beperkt zijn als u dit doet:

- **Het vastzetten van certificaten/sleutels:** DigiCert ondersteunt geen **hardcoden of “vastzetten”** van certificaten van DigiCert of openbare sleutels in applicaties, firmware of apparaten. Vastzetten betekent dat uw app of systeem is geconfigureerd om alleen een specifiek certificaat te vertrouwen. Het vastzetten van een certificaat kan starheid veroorzaken. Dit kan leiden tot uitval of veiligheidsrisico's (als u het vastgezette certificaat niet snel kunt vervangen). Als u ervoor kiest om een certificaat van DigiCert vast te zetten, neemt u de volledige verantwoordelijkheid voor eventuele serviceonderbrekingen die daaruit voortvloeien. **DigiCert zal de vereiste maatregelen** (waaronder intrekking) **niet uitstellen** om tegemoet te komen aan een vastgezette omgeving.
- **Dubbel gebruik/misbruik van certificaten:** Vertrouw niet op één enkel certificaat van DigiCert voor meerdere verschillende gebruiksscenario's waarvoor het niet is ontworpen. Het gebruik van één certificaat voor zowel S/MIME-e-mailversleuteling *en een ander doel*,

zoals TLS/SSL (webbeveiliging) en codeondertekening, of clientverificatie wordt bijvoorbeeld niet ondersteund. Elk certificaat is bedoeld voor een specifieke gebruikssituatie, zoals aangegeven door het type en de extensies. Het gebruik van certificaten op een niet-beoogde manier (zelfs als dit technisch mogelijk is) **wordt afgeraden** en kan leiden tot beveiligingsrisico's of niet-naleving van richtlijnen. Als u een certificaat op een **niet-goedgekeurde manier** gebruikt, doet u dat op eigen risico. DigiCert is niet verantwoordelijk voor de gevolgen van dergelijk gebruik.

- **Onherstelbare insluiting:** Vermijd het insluiten van certificaten in een context waarin ze niet makkelijk kunnen worden vervangen of ingetrokken. Het is bijvoorbeeld riskant om een certificaat in hardware/firmware te branden of op een manier te verspreiden waarna het niet meer kan worden bijgewerkt. Als dat certificaat verloopt of moet worden ingetrokken, kunnen die apparaten defect raken en is er mogelijk geen manier om dit ter plaatse te verhelpen.

U mag certificaten van DigiCert alleen gebruiken in overeenstemming met de richtlijnen van DigiCert, de CP/CPS en de best practices in de branche. Elk gebruik van een certificaat dat het voor u of DigiCert moeilijk maakt om het certificaat in te trekken of te vervangen (zoals het diep insluiten van certificaten in hardware of het op grote schaal vastzetten zonder het plannen van back-ups) gebeurt op eigen risico. Zorg altijd voor een plan voor snelle vervanging van certificaten.

11. Diversen

Integratie met andere overeenkomsten: Deze Voorwaarden, samen met de CP/CPS, regelen uw gebruik van S/MIME-certificaten die door DigiCert verstrekt worden. Ze zijn opgenomen in en vormen een aanvulling op de Raamovereenkomst voor services van DigiCert (beschikbaar op <https://www.digicert.com/master-services-agreement>) of andere toepasselijke serviceovereenkomst tussen u en DigiCert. In het geval van tegenstrijdigheid tussen deze Voorwaarden en de CP/CPS, prevaleren de bepalingen van de CP/CPS. In het geval van tegenstrijdigheid tussen deze Voorwaarden en andere overeenkomsten, servicecontracten of voorwaarden die van toepassing zijn op het aanbod van DigiCert, prevaleren deze Voorwaarden met betrekking tot zaken die specifiek verband houden met uw gebruik van S/MIME-certificaten van DigiCert.

Garantie van vertrouwende partij en derde begunstigden: Vertrouwende partijen en leveranciers van applicatiesoftware (zoals gedefinieerd in het CP/CPS, en elk een “**certificaatbegunstigde**”) zijn uitdrukkelijk derde begunstigden van uw verplichtingen en verklaringen hierin. DigiCert kan een beperkte garantie bieden aan personen die te goeder trouw vertrouwen op een certificaat van DigiCert (bijvoorbeeld e-mailontvangers of gebruikers die schade lijden als gevolg van een onjuist uitgegeven certificaat). Een dergelijke garantie is geen garantie voor u als abonnee, maar voor derden die erop vertrouwen, zoals gedefinieerd in de CPS of garantiedocumentatie. U bent geen derde begunstigde van een dergelijke garantie van vertrouwende partij. Afgezien van wat uitdrukkelijk in deze Voorwaarden wordt vermeld, worden er door deze Gebruiksvoorwaarden geen andere rechten aan derden toegekend.

Wijzigingen in de Voorwaarden: DigiCert kan deze Voorwaarden van tijd tot tijd bijwerken of wijzigen om ze aan te passen aan wijzigingen in services, technologie, wettelijke of regelgevende voorschriften, of wijzigingen in de branchenormen. Bijgewerkte versies van deze Voorwaarden worden gepubliceerd op de website van DigiCert (en/of via een klikbare link in het product, een

repository of een communicatiekanaal) en worden aangeduid met een bijgewerkte datum onder “Laatste update”. Daarnaast kan DigiCert abonnees op de hoogte brengen van belangrijke wijzigingen via bijvoorbeeld e-mailberichten of accountmeldingen. Door S/MIME-certificaten of gerelateerde services te blijven gebruiken nadat deze Voorwaarden zijn bijgewerkt, geeft u aan dat u akkoord gaat met de herziene Voorwaarden. Als u niet akkoord gaat met de wijzigingen in de Voorwaarden, dient u het gebruik van de S/MIME-certificaten en gerelateerde services te staken (onder voorbehoud van eventuele overgangsbepalingen of respijtperiodes die DigiCert mogelijk aankondigt). Het is uw verantwoordelijkheid om deze Voorwaarden regelmatig te controleren op updates. Deze Voorwaarden blijven van kracht totdat alle certificaten die hieronder zijn uitgegeven zijn verlopen of ingetrokken en niet langer in gebruik zijn, of totdat de Voorwaarden worden vervangen door een nieuwere versie.

Disclaimer met betrekking tot duidelijke taal: Voor het gemak bevatten sommige delen van deze Voorwaarden een “korte versie” met samenvattingen of vereenvoudigde uitleg om de betekenis van het betreffende deel te verduidelijken. Deze samenvattingen in duidelijke taal worden uitsluitend verstrekt om het begrip te verbeteren en zijn geen wettelijk bindende bepalingen. In geval van onduidelijkheid of tegenstrijdigheid tussen een samenvatting en de volledige tekst van de Voorwaarden, prevaleert de volledige, gedetailleerde tekst (en de opgenomen CP/CPS). Het gebruik van duidelijke taal in deze Voorwaarden is bedoeld om de Voorwaarden begrijpelijker te maken, maar doet geen afbreuk aan de juridische afdwingbaarheid van de bepalingen. De bindende verplichtingen van zowel u als DigiCert zijn zoals vermeld in de volledige tekst van de Voorwaarden.