

PKI VOOR HET WEB VAN DIGICERT
GEBRUIKSVOORWAARDEN VOOR CERTIFICATEN
OPENBAAR VERTROUWDE TLS/SSL

1. Toepassingsgebied en doel

Korte versie: Deze voorwaarden zijn alleen van toepassing op de openbaar vertrouwde TLS/SSL-certificaten van DigiCert (DV, OV, EV, waaronder wildcard TLS-certificaten). Ze bevatten het certificaatbeleid en de certificeringspraktijkenverklaring (“Certification Policy and Certification Practices Statement”, CP/CPS) van DigiCert en weerspiegelen de industriestandaarden (zoals de richtlijnen van het CA/Browser Forum en het beleid voor browserrootopslag) die van toepassing zijn op openbaar vertrouwde TLS-certificaten.

Deze voorwaarden (“Voorwaarden”) zijn van toepassing op openbaar vertrouwde TLS/SSL-certificaten die zijn uitgegeven door DigiCert of haar gelieerde ondernemingen onder DigiCert's Web PKI. Ze zijn niet van toepassing op andere certificaten buiten de PKI van het web van DigiCert, inclusief andere soorten certificaten of services (bijv. persoonlijke/interne certificaten, S/MIME-e-mailcertificaten, codeondertekeningscertificaten of EU-gekwadificeerde certificaten). De Voorwaarden omvatten de openbaar vertrouwde CP/CPS van DigiCert (de “CP/CPS”), die samen met deze Voorwaarden uiteenzetten hoe Web PKI-certificaten worden uitgegeven, beheerd en ingetrokken. De openbaar vertrouwde CP/CPS van DigiCert is beschikbaar op <https://www.digicert.com/legal-repository/>, en wordt van tijd tot tijd bijgewerkt (de “DigiCert Legal Repository”). Deze Voorwaarden weerspiegelen de beleidslijnen en voorschriften die zijn vastgesteld door brancheautoriteiten en de browsers, waaronder de Basiseisen van het CA/Browser Forum voor openbaar vertrouwde TLS-certificaten, beschikbaar op www.cabforum.org/working-groups/server/baseline-requirements/documents/ (de “Basiseisen”, en de Richtlijnen voor uitgebreide validatie (Extended Validation, EV) (voor EV-certificaten), beschikbaar op www.cabforum.org/working-groups/server/extended-validation/documents/ (de “EV-richtlijnen”). **Als certificeringsautoriteit (“CA”) is DigiCert verplicht om zich te houden aan deze branchenormen, waaronder zonder uitzondering indien vereist het onmiddellijk intrekken van certificaten wanneer dit vereist wordt door de toepasselijke criteria van de branchenormen.**

2. Gebruik van Web PKI-certificaten

U mag uw TLS/SSL-certificaat van DigiCert alleen gebruiken om de domeinna(m)en die u bezit of waarvoor u expliciete toestemming hebt te beveiligen. Het certificaat mag **alleen** op meerdere servers of apparaten worden geïnstalleerd als u de controle hebt over al deze systemen (bijvoorbeeld servers in de infrastructuur van uw organisatie). **Houd de persoonlijke sleutel van het certificaat vertrouwelijk.** Alleen u en uw geautoriseerde vertegenwoordigers mogen toegang hebben. Deel uw persoonlijke sleutel niet met externe partijen.

Deze openbaar vertrouwde TLS-certificaten zijn **uitsluitend bedoeld voor TLS/SSL-webserverbeveiliging**. U mag een TLS/SSL-certificaat van DigiCert niet gebruiken voor andere doelen, zoals e-mailversleuteling, codeondertekening, documentondertekening, VPN-authenticatie of enig gebruik dat niet is toegestaan voor openbare TLS-certificaten. Zelfs als de technische eigenschappen van een certificaat een bepaald gebruik mogelijk maken, is elk gebruik dat buiten deze Voorwaarden of het gedefinieerde doel van het certificaat valt, niet toegestaan en kan dit in strijd zijn met de nalevingsregels van de branche. Het gebruik van een

certificaat voor een doel buiten het toepassingsgebied of voor een verboden doel is een reden voor intrekking (raadpleeg hieronder het gedeelte **Intrekking**).

3. Een certificaat aanvragen

Korte versie: Wanneer u een certificaat aanvraagt, belooft u dat de informatie waar is en dat u bevoegd bent om het certificaat aan te vragen voor het domein en (indien van toepassing) de organisatie.

Wanneer u een certificaat aanvraagt, moet u **nauwkeurige, volledige en waarheidsgetrouwe informatie verstrekken**. Hieronder vallen de domeinnamen, gegevens over de organisatie en alle andere gegevens die nodig zijn voor de uitgifte. U mag **alleen certificaten aanvragen voor domeinnamen waarvan u de eigenaar bent of waarover u de controle hebt**, of waarvoor u de uitdrukkelijke toestemming van de eigenaar hebt. Neem geen namen, handelsmerken of andere informatie op die u niet mag gebruiken.

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 zal uw controle over het/de domein(en) verifiëren en, voor OV- en EV-certificaten, ook uw organisatie verifiëren. EV-certificaten vereisen aanvullende documentatie en controles. Als de validatie niet succesvol is of als er waarschuwingen verschijnen, zal DigiCert het certificaat pas uitgeven als aan de eisen is voldaan.

Voordat een openbaar vertrouwd TLS-certificaat wordt uitgegeven, voert DigiCert de nodige identiteits- en autorisatiecontroles uit, in overeenstemming met de CP/CPS van DigiCert. Alle certificaataanvragen zijn onderhevig aan definitieve beoordeling en goedkeuring door DigiCert.

- **Domeininvalidatie (DV, OV, EV):** Voor alle certificaattypes moet u aantonen dat u controle hebt over het/de domein(en) die in het certificaat moeten worden opgenomen. Dit kan bestaan uit oproepen per e-mail, het aanmaken van DNS-records, het uploaden van bestanden of andere goedgekeurde methoden voor domeincontrole.
- **Organisatievalidatie (OV, EV):** Voor OV- en EV-certificaten moet DigiCert het wettelijke bestaan, de operationele status en de bevoegdheid van uw organisatie om het certificaat aan te vragen, verifiëren. Dit proces kan bestaan uit het controleren van officiële bedrijfsregisters, adresverificatie, validatie van telefoonnummers en het vergelijken van gegevens met die van gezaghebbende externe bronnen.
- **Uitgebreide validatie (EV):** EV-aanvragen zijn onderworpen aan strengere criteria, waaronder de aanwijzing van specifieke bevoegde rollen (zoals EV-aanvrager, goedkeurder en contractondertekenaar) en aanvullende documentatie, zoals bewijs van

wettelijke registratie of professionele adviesbrieven. DigiCert zal deze rollen verifiëren, exclusieve domeinrechten bevestigen en een uitgebreide fraudecontrole uitvoeren.

DigiCert kan weigeren een certificaat uit te geven als u niet reageert op validatieverzoeken, de vereiste documentatie niet verstrekt of als DigiCert een risico op fraude, verkeerde voorstelling van zaken of niet-naleving van branchenormen constateert. Alle validatiestappen moeten voor uitgifte naar tevredenheid van DigiCert worden voltooid. Als een aanvraag niet kan worden gevalideerd of niet aan de eisen voldoet, zal DigiCert het certificaat niet uitgeven.

5. De geldigheid van certificaten

Korte versie: *Certificaten hebben een korte levensduur. U bent verantwoordelijk voor het vervangen ervan voordat ze verlopen. Het gebruik van automatisering voor certificaatvernieuwing wordt sterk aanbevolen.*

Openbare TLS/SSL-certificaten zijn bedoeld om na een beperkte tijd te verlopen. Op dit moment is **de maximale geldigheid** voor een openbaar vertrouwd TLS/SSL-certificaat 398 dagen (ongeveer 13 maanden). Het beleid van de branche verandert en vereist de komende jaren een nog kortere levensduur (bijvoorbeeld een vermindering tot ongeveer 200 dagen in 2026, 100 dagen in 2027 en 47 dagen in 2029). Deze veranderingen worden ingegeven door best practices op het gebied van beveiliging en de consensus van het CA/Browser Forum om de levensduur van certificaten te beperken, waardoor automatisering essentieel is geworden. DigiCert kan voor het gemak jaarabonnementen of langere bundels aanbieden, maar certificaten worden nog steeds opnieuw uitgegeven op door de branche voorgeschreven tussenpozen (d.w.z. dat u het bijgewerkte certificaat opnieuw moet valideren en installeren wanneer dat vereist wordt).

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 eerste aan om automatisering voor certificaatbeheer (zoals ACME-protocollen, DigiCert CertCentral® API's, DigiCert Trust Lifecycle Manager of andere geautomatiseerde vernieuwingstools) te gebruiken voor het afhandelen van verlengingen en vervangingen.

6. Uw verantwoordelijkheden als abonnee

Korte versie: *Door een DigiCert-certificaat 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 de domeinen en beoogde doelen 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 **(g)** onmiddellijk reageren op vragen van DigiCert over beveiligingskwesaties, 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 het 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 begunstigen 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 certificaten. U zult alle informatie onmiddellijk bijwerken als deze tijdens het validatieproces verandert. Als de door u verstrekte informatie aan DigiCert verouderd of onjuist is geworden (bijvoorbeeld als de naam van de organisatie of het adres is gewijzigd, of als u niet langer de controle hebt over een domein in het certificaat), dient u die informatie onmiddellijk bij DigiCert bij te werken of DigiCert op de hoogte te stellen van de wijziging.
- b. **Bescherming van 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 van gelijkwaardige sterkte, tenzij er strengere eisen gelden). U moet de persoonlijke sleutel te allen tijde vertrouwelijk en volledig onder uw controle houden. Dit omvat het gebruik van alle noodzakelijke maatregelen om verlies, openbaarmaking of ongevoegd gebruik van de persoonlijke sleutel te voorkomen.
- c. **Acceptatie van certificaat:** Nadat DigiCert uw certificaat heeft uitgegeven, controleert u de gegevens van het certificaat (zoals de naam van de aanvrager, de domeinnamen, gegevens van de organisatie, enz.) 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 installeert en gebruikt het certificaat alleen op de server(s) of apparaat(en) die toegankelijk zijn via de domeinnaam(en) die in het certificaat wordt/worden vermeld (d.w.z. de subjectAltName entries van het certificaat). 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 op een systeem waarvoor u geen gebruiksrechten hebt, en u mag het certificaat niet gebruiken voor andere doelen dan waarvoor het bedoeld is (zie het gedeelte Gebruik van Web PKI-certificaten hierboven).
- 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, 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, 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 al uw systemen verwijderen en elk gebruik van het certificaat en van die persoonlijke

sleutel staken. Het gebruik van een verlopen of ingetrokken certificaat voor enig doel is ten strengste verboden. Nadat een certificaat is ingetrokken of verlopen, stemt u er ook mee in om de bijbehorende persoonlijke sleutel niet te gebruiken om de intrekking 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 intrekkingen:** 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 CPS van DigiCert, 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 wordt uitgevoerd. ***Volgens de branchenormen moeten Certificeringsautoriteiten certificaten soms op korte termijn intrekken, bijvoorbeeld binnen 24 uur voor bepaalde kritieke incidenten en binnen 5 dagen voor andere gebeurtenissen. U erkent dat DigiCert zich aan deze niet-onderhandelbare termijnen moet houden en u stemt ermee in om in dergelijke gevallen dienovereenkomstig te handelen.***

7. 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 domein). In andere gevallen moet DigiCert een certificaat zelfs zonder uw aanvraag vaak op korte termijn intrekken. Deze intrekkingen zijn niet onderhandelbaar en worden vereist door branchenormen, waaronder de Basiseisen en de browser root store-beleidslijnen. 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 de domeinautorisatie of controle van een domeinnaam of IP-adres 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 voorgeschreven technische normen (bijvoorbeeld, de cryptografische of sleutelgrootte is niet langer toegestaan op grond van de Basiseisen of het browser 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 wordt ervan op de hoogte gesteld dat het gebruik van een domeinnaam of IP-adres in het certificaat niet langer wettelijk is toegestaan (bijvoorbeeld omdat een rechtbank of arbiter het recht van een domeinnaamhouder om de domeinnaam te gebruiken heeft ingetrokken).
- e. DigiCert bevestigt dat er een wildcardcertificaat is gebruikt om een frauduleuze of misleidende ondergeschikte domeinnaam te verifiëren.
- f. DigiCert wordt op de hoogte gebracht van een wezenlijke wijziging in de informatie die oorspronkelijk in het certificaat is opgenomen.
- g. DigiCert wordt erop gewezen dat het certificaat niet is afgegeven in volledige overeenstemming met de Basiseisen of de CP/CPS.
- h. DigiCert stelt vast dat de informatie in het certificaat onnauwkeurig is.
- i. 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.
- j. Intrekking is vereist door de CP/CPS van DigiCert om een reden die hierboven niet wordt vermeld.
- k. 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 intrekkingregisters 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.

8. Transparantie van certificaten en openbaarmaking

Korte versie: Wanneer DigiCert een openbaar vertrouwd TLS/SSL-certificaat uitgereikt, kunnen bepaalde details over het certificaat (waaronder uw domein en mogelijk de naam van de organisatie) openbaar worden geregistreerd in de Certificate Transparency-logboeken. Dit is een door de branche gepromote veiligheidsmaatregel. Door certificaten van DigiCert te gebruiken, stemt u in met deze openbaarmaking van certificaatinformatie. Er zijn geen gevoelige persoons- of accountgegevens opgenomen in deze logboeken, maar certificaatgegevens (zoals domein en bedrijfsnaam) zijn openbaar en permanent.

DigiCert kan alle uitgegeven TLS/SSL-certificaten registreren in openbare Certificate Transparency (CT)-logboeken in overeenstemming met de branchevoorschriften en de beleidslijnen van DigiCert. CT-logboeken zijn openbare databases met certificaten die worden gebruikt om de uitgifte van certificaten in de hele branche te controleren en te auditen. Wanneer uw certificaat wordt geregistreerd, wordt de volgende informatie voor iedereen zichtbaar (via CT-zoekfuncties of datafeeds): het serienummer van het certificaat, de volledig gekwalificeerde domeinna(m)en (SAN's) in het certificaat, de uitgiftedatum, de vervaldatum, de uitgevende CA en, voor OV/EV-certificaten, de naam en locatie van uw organisatie zoals vermeld in het certificaat. Er worden geen vertrouwelijke persoonsgegevens (zoals contact-e-mailadressen, betalingsgegevens of account-ID's) opgenomen in CT-logboeken, alleen de informatie die daadwerkelijk in het certificaat zelf aanwezig is.

Het aanmaken van een CT-logboek kan plaatsvinden als onderdeel van het uitgifteproces (voor of onmiddellijk nadat het certificaat aan u is geleverd). **Na het aanmaken kunnen de gegevens van een certificaat niet met terugwerkende kracht uit openbare logboeken worden verwijderd.** Certificate Transparency-gegevens zijn in feite onveranderlijk en blijven voor onbepaalde tijd toegankelijk voor het publiek. Het doel van CT is om de veiligheid te verbeteren door domeineigenaren en de bredere gemeenschap in staat te stellen om verkeerd uitgegeven of frauduleuze certificaten snel op te sporen. Door een certificaat aan te vragen bij DigiCert, erkent u dat de certificaatgegevens worden gepubliceerd in CT-logboeken en stemt u in met die publicatie. Als u zich zorgen maakt over het openbaar maken van bepaalde informatie (bijvoorbeeld de officiële naam van uw organisatie), houd er dan rekening mee dat als deze informatie in het certificaat moet worden vermeld, deze via CT **openbaar wordt** gemaakt. U zou **niet moeten vragen om optionele informatie in een certificaat op te nemen als u het niet prettig vindt dat deze informatie openbaar zichtbaar is.** Als u bijvoorbeeld een e-mailadres opneemt in de subjectAltName van een certificaat, betekent dit dat dit e-mailadres openbaar wordt geregistreerd. Over het algemeen bevatten certificaten van DigiCert voor TLS alleen informatie die noodzakelijk en niet erg gevoelig is (domeinen en organisatienamen).

DigiCert kan ook eigen repositories en statusservices onderhouden waar certificaatinformatie en intrekingsstatus beschikbaar zijn (bijvoorbeeld OCSP-respondenten, CRL's en websites met certificaatstatus), zoals toegestaan door de CPS en de Basiseisen. Deze zijn ook 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.

9. 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 TLS/SSL (webbeveiliging) *als* een ander doel, zoals S/MIME-e-mailversleuteling, 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.

10. Diversen

Integratie met andere overeenkomsten: Deze Voorwaarden, samen met de CP/CPS, regelen uw gebruik van TLS/SSL-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 TLS/SSL-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 websitebezoekers 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 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 Web PKI-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 Web PKI-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.