digicert®

DIGITALE ZERTIFIKATE VON DIGICERT – CERTIFICATE TERMS OF USE

Diese Nutzungsbedingungen für digitale Zertifikate („**Certificate Terms of Use**“) gelten für jedes digitale Zertifikat („**Zertifikat**“), und zwar unabhängig vom Zertifikatstyp und ob es sich um ein öffentlich vertrauenswürdiges TLS/SSL-Zertifikat, Client Certificate (gemäß Definition in Abschnitt 9), qualifiziertes Zertifikat (gemäß Definition in Abschnitt 10) oder anderweitiges Zertifikat handelt, das von der DigiCert, Inc., einem Unternehmen mit Sitz in Utah, oder von einem Affiliate, einschließlich deren qualifizierte Vertrauensdienstanbieter (zusammen als „**DigiCert**“ bezeichnet), für eine natürliche oder juristische Person („**Kunde**“) ausgestellt wird, und zwar gemäß der Kennung im Serviceverwaltungsportal von DigiCert und/oder einer damit verbundenen API, die dem Kunden zur Verfügung gestellt wird (das „**Portal**“), oder im ausgestellten Zertifikat. Die Certificate Terms of Use gelten ungeachtet des Zeitpunkts, zu dem der Kunde das Zertifikat beantragt hat oder dieses ausgestellt wurde. Das Konto für den Zugriff und die Nutzung des Portals im Auftrag des Kunden wird in diesem Dokument als das „**Portalkonto**“ bezeichnet.

Durch Annahme oder Unterzeichnung eines Agreements, in das diese Certificate Terms of Use durch Bezugnahme eingeschlossen sind (und dieses Agreement wird zusammen mit diesen Bedingungen als das „**Agreement**“ bezeichnet) versichert und garantiert die annehmende Partei oder der Unterzeichner (der „**Unterzeichner**“), dass (i) er/sie als berechtigter Vertreter des Kunden handelt, in dessen Auftrag der Unterzeichner dieses Agreements annimmt, und ausdrücklich bevollmächtigt ist, das Agreement zu unterzeichnen und den Kunden an das Agreement zu binden, (ii) er/sie bevollmächtigt ist, das digitale Pendant eines Firmenstempels, Siegels oder der Unterschrift eines Zeichnungsberechtigten entgegenzunehmen, um (x) die Echtheit der Website des Kunden festzustellen und (y) festzustellen, dass der Kunde für alle Nutzungen des Zertifikats verantwortlich ist, (iii) er/sie ausdrücklich vom Kunden bevollmächtigt ist, Zertifikatsanforderungen im Auftrag des Kunden zu genehmigen, und (iv) er/sie das ausschließliche Nutzungsrecht des Kunden an der/den Domain(s) bestätigt hat oder bestätigen wird, die auf ausgegebenen Zertifikaten angegeben wird/werden.

In Bezug auf Zertifikate, die von DigiCert im Rahmen dieses Agreements an den Kunden ausgestellt werden, bestätigen und vereinbaren die Parteien, dass die Certificate Terms of Use zusammen mit dem Agreement den Abonnentenvertrag darstellen, der gemäß den entsprechenden Branchenstandards, Richtlinien und Anforderungen an die Ausstellung von Zertifikaten erforderlich ist (einschließlich den EV-Richtlinien gemäß der Definition unten).

Der Kunde und DigiCert vereinbaren hiermit das Folgende:

1. **Kontonutzer.**

Der Kunde bevollmächtigt jede natürliche Person, die als Administrator im Portalkonto aufgeführt ist, dazu, als Zertifikatanforderer, Zertifikatgenehmiger und Vertragsunterzeichner (gemäß der Definition in den EV-Richtlinien) zu handeln und mit DigiCert bezüglich der Verwaltung der Zertifikate und Schlüsselsätze zu kommunizieren. „**EV-Richtlinien**“ bedeutet die Extended-Validation-Richtlinien, die vom CA/Browser Forum („**CA/B Forum**“) veröffentlicht werden und öffentlich unter www.cabforum.org zur Verfügung stehen. Der Kunde kann diese Bevollmächtigung revozieren, indem eine entsprechende Benachrichtigung an DigiCert gesandt wird. Der Kunde ist dafür verantwortlich, regelmäßig zu prüfen und erneut zu bestätigen, welche natürlichen Personen bevollmächtigt sind, Zertifikate anzufordern und zu genehmigen. Wenn der Kunde einen Portalkonto-Nutzer entfernen möchte, wird der Kunde die notwendigen Schritte unternehmen, um zu verhindern, dass der Nutzer auf das Portal zugreifen kann, einschließlich der Änderung des Passwortes und sonstiger Authentifizierungsmechanismen für ein Portalkonto. Der Kunde muss DigiCert unverzüglich benachrichtigen, wenn eine unautorisierte Nutzung des Portals oder Portalkontos entdeckt wird. Der Kunde bestätigt das Folgende: (i) Der Kunde genehmigt DigiCert, Daten zu scannen, sammeln und zu erfassen, die für die DigiCert-Services relevant sind, und die Erneuerung und Upgrades von Zertifikaten zu automatisieren; (ii) der Kunde wird die Services nur dazu verwenden, die Domains, IP-Adressen oder Objekte zu automatisieren, die der Kunde besitzt oder über die er die Kontrolle hat; (iii) der Kunde wird die Services nur für die Zwecke verwenden, die von DigiCert beschrieben und für die sie vermarktet werden, und zwar gemäß der DigiCert-Richtlinie zu zulässigen Nutzungen, die Sie hier finden: https://www.digicert.com/legal-repository.

2. **Anforderung.**

Der Kunde kann Zertifikate nur für Domainnamen anfordern, die auf den Kunden, einen Affiliate des Kunden oder eine sonstige juristische Person registriert sind, die es DigiCert ausdrücklich genehmigt hat, es dem Kunden zu erlauben,

Zertifikate für den Domainnamen ausstellen zu lassen und zu verwalten. DigiCert kann im eigenen und alleinigen Ermessen die Anzahl der Domainnamen begrenzen, die der Kunde in ein einzelnes Zertifikat einschließen kann.

3. Verifizierung.

Nach Eingang einer Anforderung für ein Zertifikat vom Kunden überprüft DigiCert die Anfrage und versucht, die entsprechenden Angaben gemäß dem Certification Practices Statement von DigiCert sowie den geltenden Branchenstandards, Richtlinien und Voraussetzungen zu verifizieren, einschließlich von Gesetzen und Vorschriften, die sich auf die Ausstellung von Zertifikaten beziehen („**Branchenstandards**"). Die Verifizierung dieser Anfragen liegt ganz im eigenen Ermessen von DigiCert und DigiCert kann die Ausstellung eines Zertifikats mit oder ohne Angabe von Gründen verweigern. DigiCert wird den Kunden benachrichtigen, wenn eine Zertifikatsanforderung abgelehnt wird, aber DigiCert ist nicht dazu verpflichtet, Gründe für die Ablehnung anzugeben. „**Certificate Practices Statement**" oder „**CPS**" bedeutet die geltende schriftliche Erklärung zu den Richtlinien und Praktiken, einschließlich der jeweiligen Zeitstempelrichtlinien und Erklärungen, die DigiCert nutzt, um seine Public Key Infrastructure („**PKI**") zu betreiben. Das CPS von DigiCert steht unter https://www.digicert.com/legal-repository zur Verfügung. Die CPS für Services, die von einem qVDA (ob in der Eigenschaft als qVDA oder anderweitig handelnd) oder einem Affiliate ausgegeben werden, sind verfügbar unter https://www.quovadisglobal.com/repository.

4. Zertifikat-Lebenszyklus.

Der Lebenszyklus eines ausgestellten Zertifikats hängt von der vom Kunden getroffenen Auswahl bei der Bestellung des Zertifikats ab, von den Anforderungen gemäß des CPS und der beabsichtigten Nutzung des Zertifikats. DigiCert kann die Zertifikat-Lebenszyklen von nicht ausgestellten Zertifikaten so anpassen, wie dies nötig ist, um folgende Anforderungen zu erfüllen: (i) des Agreements, (ii) der Branchenstandards, (iii) der Wirtschaftsprüfer von DigiCert oder (iv) eines Verkäufers von Anwendungssoftware. „**Verkäufer von Anwendungssoftware**" bedeutet eine juristische Person, die Zertifikate in Verbindung mit einem Distributed Root Store anzeigt oder nutzt, an dem DigiCert beteiligt ist oder sich beteiligen wird. Der Kunde stimmt zu, das Zertifikat und den zugehörigen Private Key (siehe Definition unten) nach dem Ablaufdatum des Zertifikats bzw. nach der Revozierung eines Zertifikats durch DigiCert gemäß dem Agreement nicht mehr zu nutzen.

5. Ausstellung.

Wenn die Verifizierung eines Zertifikats zur Zufriedenheit von DigiCert abgeschlossen wurde, stellt DigiCert dem Kunden das angeforderte Zertifikat aus und liefert es über angemessene Mittel aus. In der Regel wird DigiCert den Kunden entweder per E-Mail an die vom Kunden angegebene Adresse dazu auffordern, das Zertifikat per Download über Portal abzurufen, oder dem Kunden den Zugriff auf das Zertifikat über einen API-Aufruf im Portal ermöglichen. Öffentlich vertrauenswürdige Zertifikate werden von einem von DigiCert ausgewählten Root oder Intermediate Certificate ausgestellt. DigiCert kann jederzeit und ohne Nachricht an den Kunden ändern, von welchem Root oder Intermediate Certificate ein Zertifikat ausgestellt wird. Der Kunde wird sich an alle geltenden Gesetze, Vorschriften und Branchenstandards halten, wenn er Zertifikate bestellt oder nutzt, unter anderem auch an die US-Gesetze zur Exportkontrolle und Gesetze zu Wirtschaftssanktionen und -vorschriften. Der Kunde bestätigt, dass die Zertifikate nicht in Ländern oder Regionen verfügbar sind, für die es vom Finanzministerium der Vereinigten Staaten von Amerika zur Kontrolle ausländischer Vermögen (OFAC), vom US-Wirtschaftsministerium, von der Europäischen Kommission, dem Finanzministerium des Vereinigten Königreichs oder sonstigen staatlichen Stellen mit Zuständigkeit für DigiCert Beschränkungen gibt.

6. Zertifikatslizenz.

Mit sofortiger Wirkung ab Antragstellung für ein Zertifikat und bis das Zertifikat abläuft oder revoziert wird, kann der Kunde jedes ausgestellte Zertifikat und die damit verbundenen Services (ob vor oder nach Ausstellung des Zertifikats ausgeführt) und entsprechenden Schlüsselsätze nur für die im CPS beschriebenen Zwecke nutzen, und zwar zugunsten der Identitätseinheit (Subjekt) des Zertifikats und gemäß allen geltenden Gesetzen, Vorschriften, Branchenstandards und den Bedingungen in diesem Dokument. Alle Zertifikate, die von Verkäufern von Anwendungssoftware für vertrauenswürdig gehalten werden, unterliegen allen geltenden Vorschriften der Branchenstandards, unter anderem solchen, die sich in den Root-Store-Richtlinien der Verkäufer von Anwendungssoftware und im CPS finden, ungeachtet davon, wie die Zertifikate genutzt werden. Jegliche Nutzung, die nicht nach den geltenden Branchenstandards oder dem CPS erlaubt ist, ist verboten. DigiCert rät stark davon ab, Zertifikate oder Schlüssel zu pinnen, Zertifikate, die im Web als vertrauenswürdig gelten, mit PKI zu verwenden, die nicht für das Web erstellt wurden, oder Zertifikate anderweitig zu nutzen, wenn diese Nutzung es Kunden erschweren würde, die Revozierungsfristen oder sonstige Anforderungen des CPS einzuhalten, denn eine solche Nutzung würde nicht als ausreichender Grund für eine Verlängerung der Revozierungsfrist betrachtet werden.

„**Schlüsselsatz**“ bedeutet einen Satz von zwei oder mehr Schlüsseln mit mathematischem Bezug, die als Private Keys bezeichnet werden oder als geteilte Schlüssel im Zusammenhang mit einem Public Key, wobei (i) der Public Key eine Nachricht verschlüsseln kann, die nur der Private Key entschlüsseln kann, und (ii) auch wenn der Public Key bekannt ist, es rechnerisch nicht machbar ist, den Private Key zu entdecken. Der Kunde wird DigiCert unverzüglich informieren, wenn er Kenntnis von einem Missbrauch eines Zertifikats, eines Private Key oder des Portals erlangt. Der Kunde ist dafür verantwortlich, die Genehmigung oder Erlaubnis einzuholen und aufrechtzuerhalten, die für die Bestellung, Nutzung und Verteilung eines Zertifikats an Endnutzer oder Systeme notwendig ist, einschließlich der Erlaubnis, die gemäß den US-Exportgesetzen erforderlich ist. SSL-Zertifikate können auf einem oder mehreren physischen Servern oder Geräten gleichzeitig genutzt werden; DigiCert kann jedoch eine Gebühr für die Nutzung der Zertifikate auf zusätzlichen Servern oder Geräten berechnen.

7. Schlüsselsätze.

„**Private Key**“ bedeutet der Schlüssel, der vom Kunden geheim gehalten wird und der zur Erstellung von digitalen Signaturen und/oder zum Entschlüsseln elektronischer Datensätze oder Dateien verwendet wird, die mit dem entsprechenden Public Key verschlüsselt wurden. „**Public Key**“ bedeutet ein öffentlich zugänglicher Schlüssel des Kunden, der im Zertifikat des Kunden enthalten ist und dem Private Key entspricht, den der Kunde geheim hält und nutzt. Der Kunde muss (i) Schlüsselsätze mithilfe von vertrauenswürdigen Systemen generieren, (ii) Schlüsselsätze nutzen, die mindestens 2048-Bit-Schlüsseln nach dem RSA-Standard entsprechen, und (iii) alle Private Keys vertraulich behandeln. Der Kunde ist alleine für ein Versäumnis, seinen Private Key zu schützen, verantwortlich. Der Kunde versichert, dass er Schlüsselsätze für Adobe Signing Certificates und Code Signing Certificates mit EV nur auf Geräten mit FIPS 140-2 Level 2 generiert und speichert. All sonstigen Zertifikatstypen können auf sicheren Software- oder Hardwaresystemen gespeichert werden. Der Kunde ist dafür verantwortlich sicherzustellen, dass der Erwerb, die Nutzung und Annahme der Schlüsselsätze, die DigiCert gemäß dem Agreement generiert werden, den geltenden lokalen Gesetzen, Vorschriften und Regelungen – unter anderem den Export- und Importgesetzen, -regelungen und -vorschriften – in den Rechtsräumen entsprechen, in denen der Kunde diese Schlüsselsätze erwirbt, nutzt, annimmt oder anderweitig empfängt. Wenn es dem Kunden erlaubt ist, Private Keys (einschließlich Kopien) im Zusammenhang mit der Nutzung von bestimmten DigiCert-Services zu importieren oder exportieren, haftet DigiCert dem Kunden gegenüber nicht für die Nutzung oder Speicherung der Private Keys (einschließlich Kopien) durch den Kunden, wenn diese nicht im entsprechenden Portal oder Service erstellt worden sind oder außerhalb des Portals oder eines solchen Service genutzt werden, auch nicht, wenn sie aus dem entsprechenden Portal oder Service exportiert wurden.

8. Veröffentlichung von Zertifikatsinformationen.

Vorbehaltlich gegenteiliger Bestimmungen in diesen Certificate Terms of Use oder einer sonstigen Vereinbarung zwischen dem Kunden und DigiCert stimmt der Kunde Folgendem zu: (i) öffentliche Bekanntgabe von Informationen durch DigiCert (z. B. Domainname des Kunden, Unternehmenssitz, Kontaktdaten), die in ein ausgegebenes Zertifikat eingebettet sind; (ii) Protokollierung von Kundenzertifikaten und darin eingebetteten Informationen durch oder im Namen von DigiCert in öffentlich verfügbaren Datenbanken für Zertifikatstransparenz für die Zwecke der Erkennung und Verhinderung von Phishing-Angriffen und anderen Formen des Betrugs, wobei der Kunde zustimmt, dass diese Informationen, wenn sie protokolliert sind, nicht vom Protokollserver entfernt werden dürfen. Eine solche Veröffentlichung von Zertifikatsinformationen entspricht dem geltenden CPS.

9. Client Certificate.

„**Client Certificate**“ bedeutet ein Zertifikat, das eine beliebige extendedKeyUsage-Erweiterung (EKU) enthält, bei der es sich nicht um codeSigning, timestamping oder serverAuthentication handelt. Die Nutzung eines Client Certificate ist vielfältig und wird durch das Profil des Client Certificate definiert. Die Nutzungsmöglichkeiten, die in einem Client-Certificate-Profil definiert sind, können unter anderem digitale Signaturen, E-Mail-Verschlüsselung oder die kryptografische Authentifizierung umfassen. Wenn der Kunde ein Client Certificate anfordern möchte, dann muss der Kunde (i) die Identität und Zugehörigkeit des Anforderers mithilfe angemessener interner Dokumentation gemäß dem CPS bestätigen und (ii) bestätigen, dass die bereitgestellten Informationen und verbindlichen Zusicherungen im Zusammenhang mit oder als Bestandteil eines Client Certificate in jeder wesentlichen Hinsicht wahr, vollständig und richtig sind.

10. Qualifizierte Zertifikate.

„**Qualifiziertes Zertifikat**“ bedeutet ein Zertifikat, (i) das von einem qualifizierten Vertrauensdienstanbieter gemäß den Anforderungen der geltenden Zertifizierungs- und elektronischen Signaturgesetze der EU oder der Schweiz ausgestellt wurde und (ii) das gemäß diesen Anforderungen die höchste Sicherheitsstufe, nämlich „qualifiziert“, hat.

„**Qualifizierter Vertrauensdienstanbieter**“ oder „**qVDA**“ bedeutet ein Affiliate von DigiCert, der von staatlicher Stelle für die Ausstellung von qualifizierten Zertifikaten zugelassen ist. Die Folgenden sind qVDA von DigiCert:

qVDA-Körperschaft	**Vertrauensliste**	**Zuständigkeitsbereich der Aufsichtsbehörde**
QuoVadis Trustlink B.V.	Vertrauensliste der Niederlande	Niederlande
DigiCert Europe Belgium B.V.	Vertrauensliste Belgiens	Belgien
QuoVadis Trustlink Schweiz AG	Vertrauensliste der Schweiz	Schweiz

„**qVDA-Services**“ bedeutet die Services, die durch die qVDA von DigiCert (gemäß obenstehender Definition und unabhängig davon, ob diese in der Eigenschaft als qVDA handeln oder anderweitig) oder Affiliates ausgegeben werden.

Wenn ein Kunde qVDA-Services kauft, dann finden sich die für diese bestimmten qVDA-Services geltenden CPS unter https://www.quovadisglobal.com/repository/. In Bezug auf die qualifizierten Zertifikate (i) wird der Kunde in dem Fall, wo gemäß den Branchenstandards eine qualifizierte Signaturerstellungseinheit (QSEE) gefordert ist, seine qualifizierten Zertifikate nur für die elektronischen Signaturen verwenden, die mit der QSEE generiert werden, auf der sie gespeichert sind; (ii) falls der Kunde eine natürliche Person ist, wird er seine Private Keys ausschließlich selbst verwalten und nutzen; und (iii) falls der Kunde eine juristische Person oder Organisation ist, wird sie ihre Private Keys nur in eigener Kontrolle und unter eigener Weisung verwalten und nutzen.

11. Verwaltung.

DigiCert wird generell jedes Zertifikat gemäß einer Anweisung durch den Kunden über das Portal ausstellen, verwalten, verlängern oder revozieren und kann darauf vertrauen, dass eine solche Anweisung richtig ist. Der Kunde stellt richtige und vollständige Informationen zur Verfügung, wenn er mit DigiCert kommuniziert, und benachrichtigt DigiCert innerhalb von 5 Arbeitstagen, wenn sich eine Information in Bezug auf sein Konto im Portal ändert. Der Kunde reagiert auf jegliche Anfragen von DigiCert bezüglich der Gültigkeit von Informationen, die vom Kunden bereitgestellt wurden, innerhalb von 5 Arbeitstagen ab Eingang der Anfrage. Der Kunde wird die Zertifikatsdaten vor Nutzung des Zertifikats auf ihre Richtigkeit prüfen und verifizieren. Zertifikate gelten ab dreißig (30) Tage nach Ausstellung des Zertifikats als vom Kunden angenommen oder früher ab Nutzung des Zertifikats, wenn nachgewiesen ist, dass der Kunde das Zertifikat genutzt hat. Auch wenn DigiCert Erinnerungen über ablaufende Zertifikate versendet, ist DigiCert keinesfalls verpflichtet, dies zu tun, und es liegt in der alleinigen Verantwortung des Kunden, die Verlängerung eines Zertifikats vor Ablauf sicherzustellen. „**Arbeitstag**“ bedeutet jeder Tag von Montag bis Freitag, ausschließlich von US-Feiertagen des Bundes, die in 5 U.S.C. § 6103 festgelegt sind.

12. Registration Authority.

Ausnahme von öffentlich vertrauenswürdigen TLS/SSL-Zertifikaten und qualifizierten Zertifikaten wird der Kunde gemäß den Bedingungen des geltenden CPS als Registration Authority (RA) benannt (und der Kunde nimmt diese Ernennung hiermit an). In Verbindung mit öffentlich vertrauenswürdigen TLS/SSL-Zertifikaten wird der Kunde gemäß den Bedingungen des geltenden CPS als Enterprise RA benannt (und der Kunde nimmt diese Ernennung hiermit an). Insoweit als der Kunde die Funktion einer Registration Authority oder Enterprise RA erfüllt, so tut er dies in Erfüllung des geltenden CPS und DigiCert kann auf die Handlungen des Kunden in der Eigenschaft als Registration Authority oder Enterprise RA vertrauen. Insoweit als ein Anspruch Dritter, eine Klage, ein Verfahren oder ein Urteil aus dem Versäumnis des Kunden hervorgeht, sich strikt an die Pflichten einer Registration Authority oder Enterprise RA zu halten, muss der Kunde DigiCert und auch die Direktoren, Bevollmächtigten, Vertreter, Mitarbeiter, Rechtsnachfolger und Zessionare von DigiCert gegen einen solchen Anspruch verteidigen, schadlos halten und entschädigen. Wenn der Kunde als Registration Authority oder Enterprise RA auftritt, dann wird der Kunde seine Abonnenten, die Zertifikate gemäß diesen Bedingungen erhalten, dazu veranlassen, sich an die Bedingungen des DigiCert-Abonnentenvertrags zu halten, der unter https://www.digicert.com/subscriber-agreement zu finden ist. Die Abonnenten des Kunden müssen den Abonnentenvertrag annehmen, bevor sie Zertifikate erhalten. „**Enterprise RA**“ hat die in der aktuellen, unter https://cabforum.org/baseline-requirements-documents/ (in der jeweils geltenden Fassung) verfügbaren Version der CAB Forum Baseline Requirements definierte Bedeutung.

13. Sicherheit und Nutzung von Schlüsselsätzen.

Der Kunde wird seine mit dem Zertifikat verbundenen Schlüsselsätze sicher generieren und schützen und alle notwendigen Schritte unternehmen, um einer Gefährdung, einem Verlust oder der unbefugten Nutzung eines Private Key, der mit einem Zertifikat verbunden ist, vorzubeugen. Der Kunde wird Passwörter verwenden, die den Anforderungen an die Netzwerksicherheit des CA/B Forum und sonstigen maßgeblichen Anforderungen in Bezug auf Best Practices entsprechen. Der Kunde wird es nur Mitarbeitenden, Vertretern und Auftragnehmern des Kunden erlauben, Private Keys zu nutzen oder auf diese zuzugreifen, wenn der Mitarbeitende, Vertreter oder Auftragnehmer eine Hintergrundprüfung durch den Kunden durchlaufen hat (insoweit dies gesetzlich zulässig ist) und in puncto PKI und sonstigen Bereichen der Informationssicherheit geschult und erfahren ist. Der Kunde wird DigiCert benachrichtigen, die Revozierung eines Zertifikats und des zugehörigen Private Key anfordern, die Nutzung des Zertifikats und des zugehörigen Private Key einstellen und das Zertifikat von allen Geräten entfernen, auf denen es installiert ist, wenn: (i) eine Angabe im Zertifikat unrichtig oder falsch ist oder wird oder (ii) ein Missbrauch oder eine Gefährdung oder der Verdacht auf Missbrauch oder Gefährdung des mit dem im Zertifikat enthaltenen Public Key verbundenen Private Key vorliegt. Im Falle von Code Signing Certificates wird der Kunde die Nutzung des Zertifikats und des zugehörigen Private Key unverzüglich einstellen und unverzüglich die Revozierung des Zertifikats fordern, wenn der Kunde glaubt, dass: (a) eine Angabe im Zertifikat unrichtig oder falsch ist oder wird, (b) der Private Key, der mit dem im Zertifikat enthaltenen Public Key verknüpft ist, missbraucht oder gefährdet wurde oder (c) das Zertifikat nachweislich dazu verwendet wurde, verdächtigen Code zu signieren. „**Verdächtiger Code**“ bedeutet Code, der schädliche oder böswillige Funktionalitäten jeglicher Art enthält oder schwerwiegende Sicherheitslücken wie Spyware, Malware oder sonstigen Code enthält, der sich ohne Zustimmung des Nutzers installiert und/oder sich der eigenen Entfernung widersetzt, und Code, der auf Arten genutzt werden kann, die nicht von seinen Schreibern beabsichtigt sind und die Vertrauenswürdigkeit der Plattformen, auf denen der Code ausgeführt wird, gefährden. Der Kunde wird davon absehen, denselben Private Key für unterschiedliche Zertifikatstypen zu verwenden. Zum Beispiel wird der Kunde davon absehen, mit einem Private Key, der für Code Signing verwendet wird, Zertifikate anzufordern, die kein Code Signing Certificate sind. Wenn DigiCert erkennt, dass ein Private Key für einen bestimmten Zertifikatstyp oder eine bestimmte Handlung (z. B. Code Signing) dazu verwendet wird, einen anderen Zertifikatstyp anzufordern (z. B. TLS/SSL- oder Client Certificates), dann muss DigiCert alle mit diesem Private Key oder dem zugehörigen Schlüsselsatz verbundenen Zertifikate revozieren, die sich im damit verbundenen Portalkonto des Kunden befinden oder die anderweitig von DigiCert ausgegeben wurden. Der Kunde wird auf Anweisungen von DigiCert betreffend eines gefährdeten Schlüsselsatzes oder Zertifikatsmissbrauchs innerhalb von 24 Stunden reagieren. Der Kunde wird die Nutzung des Schlüsselsatzes für ein Zertifikat unverzüglich einstellen, wenn (I) das Zertifikat revoziert wird, spätestens jedoch (II) an dem Tag, an dem der erlaubte Nutzungszeitraum für den Schlüsselsatz abläuft. Nach einer Revozierung muss der Kunde die Nutzung des Zertifikats einstellen.

Wenn der Kunde einen Private Key speichert, der für ein Code Signing Certificate in einem HSM (gemäß Definition im geltenden CPS) generiert worden ist, stimmt der Kunde in Bezug auf jeden solchen Private Key zu, dass (w) der Kunde seinen Private Key sicher in einem HSM speichert, das die Entfernung des Private Key verhindert, (x) das HSM entweder der alleinigen Kontrolle des Kunden unterliegt oder über eine geprüfte Cloud genutzt wird (z. B. Azure oder AWS), (y) der Kunde keinen Grund zur Annahme hat, dass dieser Private Key jemals außerhalb des HSM genutzt wurde oder wird, und (z) der Private Key in einem Kryptomodul geschützt wird, das mindestens den Standard FIPS 140-2 Level 2 (oder gleichwertig) oder Common Criteria EAL4+ erfüllt.

14. Defekte Zertifikate.

Die einzige Abhilfe, die einem Kunden im Falle eines defekten Zertifikats (ein „**Defekt**“) zur Verfügung steht, ist die Aufforderung an DigiCert, sich nach besten und wirtschaftlich vertretbaren Kräften zu bemühen, den Defekt nach Eingang der kundenseitigen Benachrichtigung über einen solchen Defekt zu beseitigen. DigiCert ist nicht verpflichtet, einen Defekt zu beheben, wenn (i) der Kunde das Zertifikat missbraucht, beschädigt oder geändert hat, (ii) der Kunde DigiCert nicht unverzüglich über den Defekt in Kenntnis gesetzt hat oder (iii) der Kunde gegen eine Bestimmung des Agreements verstoßen hat.

15. Relying Party-Garantie.

Der Kunde bestätigt, dass die Relying Party-Garantie nur zugunsten der vertrauenden Beteiligten wirkt. „**Relying Party-Garantie**“ bedeutet eine Garantie, die einem vertrauenden Beteiligten angeboten wird und die die Bedingungen des Relying Party Agreements und der beschränkten Garantie erfüllt, die auf der DigiCert-Website unter https://www.digicert.com/legal-repository veröffentlicht sind. Die Relying Party-Garantie für Zertifikate, die von einer

qVDA oder einem Affiliate von DigiCert ausgestellt wurden, ist unter https://www.quovadisglobal.com/repository veröffentlicht. Der Kunde hat keine Rechte aus der Relying Party-Garantie, einschließlich eines Rechts auf Durchsetzung der Bedingungen der Relying Party-Garantie oder der Geltendmachung einer Forderung gemäß der Relying Party-Garantie. „**Vertrauende Beteiligte**“ hat die Bedeutung wie in der Relying Party-Garantie festgelegt. Ein Verkäufer von Anwendungssoftware ist kein vertrauender Beteiligter, wenn die vom Verkäufer von Anwendungssoftware vertriebene Software lediglich Informationen bezüglich eines Zertifikats anzeigt oder die Nutzung des Zertifikats oder einer digitalen Signatur erleichtert.

16. Zusicherungen.

Für jedes angeforderte Zertifikat versichert und garantiert der Kunde das Folgende:

a. Der Kunde hat das Nutzungsrecht für bzw. ist der rechtmäßige Eigentümer (i) der im Zertifikat benannten Domain und (ii) des Common Name oder des Organisationsnamens, der auf dem Zertifikat genannt ist;

b. Der Kunde nutzt das Zertifikat nur für genehmigte und rechtmäßige Zwecke, unter anderem nicht dazu, um verdächtigen Code zu signieren, und nutzt das Zertifikat und den Private Key nur unter Einhaltung der geltenden Gesetze und nur gemäß dem Zertifikatszweck, dem CPS, einer geltenden Zertifikatsrichtlinie und dem Agreement;

c. Der Kunde hat das CPS gelesen und verstanden und stimmt diesem zu;

d. Der Kunde zeigt jede Nichteinhaltung des CPS oder der Baseline Requirements sofort schriftlich DigiCert gegenüber an;

e. Die im Zertifikat genannte Organisation und der Inhaber des registrierten Domainnamens haben Kenntnis von und stimmen jeder Zertifikatsanforderung zu.

17. Beschränkungen.

Der Kunde wird ein TLS/SSL-Zertifikat nur auf den Servern nutzen, die an den im ausgestellten Zertifikat aufgeführten Domainnamen verfügbar sind. Der Kunde wird zudem davon absehen:

a. TLS/SSL-Zertifikate oder Private Keys zu modifizieren, unterzulizenzieren oder abgeleitete Werke zu schaffen (mit Ausnahme von solchen, die für den Verwendungszweck des Zertifikats erforderlich sind);

b. Dateien oder Software, die Schaden für den Betrieb des Computers eines anderen verursachen können, hochzuladen oder zu verteilen;

c. Zusicherungen bezüglich eines TLS/SSL-Zertifikats zu machen oder ein solches zu nutzen, außer dies ist gemäß dem CPS zulässig;

d. die Verbindung eines Kunden mit einer juristischen Person vorzugeben oder falsch darzustellen;

e. ein Zertifikat oder eine damit verbundene Software oder Dienstleistung (z. B. das Portal) in einer Art und Weise zu nutzen, die begründetermaßen dazu führen könnte, dass eine zivil- oder strafrechtliche Klage gegen den Kunden oder DigiCert eingereicht wird;

f. ein Zertifikat oder eine damit verbundene Software dazu zu nutzen, das Vertrauen eines Dritten zu verletzen oder unaufgeforderte Massenanschreiben zu versenden oder zu empfangen;

g. Code Signing Certificates dazu zu verwenden, verdächtigen Code zu signieren;

h. ein Code Signing Certificate zu beantragen, wenn der Public Key im Zertifikat mit einem Nicht-Code Signing Certificate verwendet wird oder werden soll;

i. die ordnungsgemäße Funktion der DigiCert-Website oder etwaige Transaktionen zu stören, die über die DigiCert-Website abgewickelt werden;

j. mit einem Zertifikat zu versuchen, andere Zertifikate auszustellen;

k. die technische Implementierung der DigiCert-Systeme oder -Software zu überwachen, in diese einzugreifen oder sie zurückzuentwickeln oder anderweitig wissentlich die Sicherheit der DigiCert-Systeme oder -Software zu gefährden;

l. Zertifikatsinformationen an DigiCert zu übermitteln, die geistige Eigentumsrechte Dritter verletzen; oder

m. absichtlich einen Private Key zu erstellen, der im Wesentlichen dem Private Key von DigiCert oder eines Dritten gleicht.

n. Wenn nicht ausdrücklich die schriftliche Befugnis von DigiCert vorliegt, wird der Kunde kein Endzertifikat verwenden, um ein Zertifikat zu signieren.

18. Revozierung von Zertifikaten.

DigiCert kann ein Zertifikat ohne Ankündigung aus den im CPS genannten Gründen revozieren, unter anderem, wenn DigiCert begründetermaßen davon ausgeht, dass:

a. der Kunde die Revozierung des Zertifikats angefordert oder die Ausstellung des Zertifikats nicht genehmigt hat;

b. der Kunde die Services dazu verwendet, Inhalte zu posten oder verfügbar zu machen, die die Rechte DigiCerts oder eines Dritten verletzen;

c. der Kunde das Agreement verletzt oder eine Pflicht aus dem CPS nicht erfüllt hat;

d. eine Bestimmung des Agreements mit dem Kunden, die eine Zusicherung oder Verpflichtung in Bezug auf die Ausstellung, Nutzung, Verwaltung oder Revozierung des Zertifikats enthält, endet oder für ungültig befunden wird;

e. der Kunde auf eine staatliche Liste verbotener natürlicher oder juristischer Personen gesetzt wird oder aus einem Gebiet heraus operiert, das nach den Gesetzen der Vereinigten Staaten verboten ist;

f. das Zertifikat unrichtige oder irreführende Angaben enthält;

g. das Zertifikat ohne Berechtigung, außerhalb seines Verwendungszwecks oder zur Signierung von verdächtigem Code verwendet wurde;

h. der Private Key, der mit dem Zertifikat verbunden ist, offengelegt oder geknackt worden ist;

i. das Zertifikat (i) missbraucht wurde, (ii) gesetzeswidrig oder entgegen dem CPS oder den Branchenstandards verwendet oder ausgestellt wurde oder (iii) direkt oder indirekt für illegale oder betrügerische Zwecke verwendet wurde, z. B. für Phishing-Angriffe, Betrug, die Verteilung von Malware oder zu sonstigen illegalen oder betrügerischen Zwecken oder bei sonstigen Verletzungen gemäß der DigiCert-Richtlinie zur zulässigen Nutzung; oder

j. die Branchenstandards oder das CPS von DigiCert die Revozierung des Zertifikats erfordern oder die Revozierung notwendig ist, um die Rechte, die vertraulichen Informationen, den Betrieb oder den Ruf von DigiCert oder eines Dritten zu wahren.

19. Weitergabe von Informationen.

Der Kunde bestätigt und akzeptiert, dass wenn (i) das Zertifikat oder der Kunde als eine Quelle für verdächtigen Code erkannt wird, (ii) die Berechtigung zur Anforderung des Zertifikats nicht verifiziert werden kann oder (iii) das Zertifikat aus anderen Gründen als der Aufforderung durch den Kunden revoziert wird (z. B. als Folge der Gefährdung des Private Key, Entdeckung von Malware usw.), DigiCert berechtigt ist, Informationen über den Kunden, über eine Anwendung oder ein Objekt, das mit dem Zertifikat signiert worden ist, über das Zertifikat und über die Umstände in diesem Zusammenhang weiterzugeben, und zwar an andere Zertifizierungsstellen oder Branchengruppen, einschließlich dem CA/B Forum.

20. Branchenstandards.

Beide Parteien halten sich an alle Branchenstandards und Gesetze, die für die Zertifikate gelten; und wenn sich ein geltendes Gesetz oder Branchenstandard ändert und sich diese Änderung auf die Zertifikate oder sonstigen Services auswirkt, die

gemäß diesem Agreement geleistet werden, dann kann DigiCert die Services anpassen, ändern oder das Agreement kündigen, insoweit dies notwendig ist, um der Änderung zu entsprechen.

21. Geräte und Ausstattung.

Der Kunde ist auf Kosten des Kunden verantwortlich für (i) alle Computer, Telekommunikationsanlagen, Software, Internetzugang und Kommunikationsnetzwerke (gegebenenfalls), die für die Nutzung der Zertifikate und der damit verbundenen DigiCert-Software oder -Services erforderlich sind; und (ii) für das Verhalten des Kunden und für die Wartung, den Betrieb, die Entwicklung und Inhalte von dessen Website.

22. Leistungsberechtigte der Zertifikate.

Die vertrauenden Beteiligten und Verkäufer von Anwendungssoftware sind ausdrücklich die dritten Leistungsberechtigten der Pflichten und Zusicherungen des Kunden in Bezug auf die Nutzung oder Ausstellung eines Zertifikats. Die vertrauenden Beteiligten und Verkäufer von Anwendungssoftware sind keine ausdrücklichen dritten Leistungsberechtigten in Bezug auf die DigiCert-Software.

23. Intermediate Certificate.

Dieser Abschnitt 23 gilt nur, wenn der Kunde ein ausgewiesenes Root und/oder Intermediate Certificate für die Ausstellung von privaten Zertifikaten oder öffentlich vertrauenswürdigen Zertifikaten gemäß den Angaben in einem Bestellformular kauft.

a. Erstellung. Innerhalb von 60 Tagen ab Eingang der entsprechenden Zahlung gemäß dem Agreement und den von DigiCert geforderten Angaben für die Erstellung eines Root und/oder Intermediate Certificate gemäß Unterpunkt (b) unten wird DigiCert ein Root und/oder Intermediate Certificate für die Ausstellung von (i) nicht öffentlich vertrauenswürdigen Zertifikaten über das Portal oder (ii) öffentlich vertrauenswürdigen Zertifikaten gemäß den Angaben in einem Bestellformular erstellen. Ein „**privates Zertifikat**“ bedeutet ein Zertifikat, das nicht in einen Trust Store eingebettet ist. Ein „**Root Certificate**“ bedeutet ein selbstsigniertes Zertifikat, das in einem sicheren Offlinezustand gespeichert ist und für die Ausstellung sonstiger Zertifikate genutzt wird. „**Intermediate Certificate**“ bedeutet ein Zertifikat, das mit einem Private Key, der dem Root Certificate entspricht, signiert wird und das für die Ausstellung von Zertifikaten zur Nutzung durch den Kunden verwendet wird.

b. Inhalte. DigiCert und der Kunde arbeiten gemäß dem Grundsatz von Treu und Glauben zusammen, um die entsprechenden Inhalte des Root bzw. Intermediate Certificate festzulegen. Der Kunde muss DigiCert alle Informationen bereitstellen, die DigiCert für die Erstellung des Root bzw. Intermediate Certificate benötigt, und zwar innerhalb von zwölf (12) Monaten ab Vertragsschluss über die Erstellung dieses Root bzw. Intermediate Certificate. Wenn der Kunde es versäumt, alle erforderlichen Informationen innerhalb dieses Zeitrahmens bereitzustellen, verwirkt der Kunde damit das Recht auf Anforderung des Root bzw. Intermediate Certificate und DigiCert wird alle Gebühren für die Erstellung des Root bzw. Intermediate Certificate einbehalten. Nachdem ein Intermediate Certificate erstellt wurde, kann der Kunde die Inhalte dieses Intermediate Certificate nicht abändern, kann aber so viele identische Kopien des Intermediate Certificate erstellen wie benötigt werden. Intermediate Certificates haben eine feste Lebensdauer von zehn Jahren. Danach laufen diese ab und können nicht verlängert werden. Der Kunde ist dafür verantwortlich sicherzustellen, dass alle Zertifikate, die von einem Intermediate Certificate ausgestellt werden, mindestens zwei Jahre vor Ablauf des Intermediate Certificate ablaufen. DigiCert ist berechtigt, Zertifikate zu revozieren, die vom Intermediate Certificate ausgestellt wurden und innerhalb des Zeitraums von zwei Jahren vor Ablauf des Intermediate Certificate noch gültig sind.

c. Eigentum. DigiCert behält, wenn in diesen Certificate Terms of Use nichts anderes angegeben ist, das alleinige Eigentum am Intermediate Certificate, aber nutzt das im Zusammenhang mit diesem Agreement ausgestellte Intermediate Certificate ausschließlich gemäß den Anweisungen, die der Kunde über das Portal gegeben hat. Der Kunde kann Kopien des Intermediate Certificate erzeugen und Kopien des Intermediate Certificate an seine eigenen Endnutzer und Kunden verteilen.

d. Hosting. DigiCert wird den Private Key für das Intermediate Certificate in DigiCerts sicheren PKI-Systemen hosten. Der Kunde darf den Private Key des Intermediate Certificate keinesfalls aus DigiCerts PKI-Systemen entfernen oder von einem Dritten von dort entfernen lassen. DigiCert wird dem Kunden CRL/OCSP-Services bereitstellen und hosten. DigiCert wird die CRL/OCSP-Services auch nach Ende des Agreements weiterhin

bereitstellen, bis alle Zertifikate, die darunter ausgestellt wurden, abgelaufen oder revoziert worden sind. Intermediate Certificates, die öffentlich vertrauenswürdige Zertifikate ausstellen, werden in DigiCerts PKI gehostet und von DigiCert-Mitarbeitern verwaltet, weil sie öffentlich vertrauenswürdige Zertifikate ausstellen und deshalb vom Audit des DigiCert Web Trust abgedeckt sind. Wenn sich Branchenstandards oder die Richtlinien eines Verkäufers von Anwendungssoftware in einer Art und Weise ändern, die eine separate Überprüfung des Intermediate Certificate erfordern, dann werden DigiCert und der Kunde nach dem Grundsatz von Treu und Glauben zusammenarbeiten, um die erforderliche Prüfung zu erhalten.

e. Revozierung. DigiCert ist berechtigt, das Intermediate Certificate zu revozieren, wenn: (i) der Kunde die Revozierung schriftlich von DigiCert fordert und dabei einen spezifischen Verstoß gegen die Branchenstandards nennt; (ii) DigiCert angemessen begründet, warum es der Meinung ist, dass das Intermediate Certificate gefährdet ist; (iii) der Kunde eine wesentliche Verletzung des Agreements begeht und den Verstoß nicht innerhalb von 30 Tagen nach Eingang der Meldung über den Verstoß behebt; (iv) der Kunde das Intermediate Certificate nach Ende der Berechtigung zur Nutzung des Intermediate Certificate weiterhin nutzt oder (v) DigiCert begründetermaßen der Meinung ist, dass die Revozierung nach Branchenstandards erforderlich ist.

f. Beschränkungen. Der Kunde wird davon absehen: (i) zusätzliche Intermediate Certificates vom Intermediate Certificate zu erstellen oder versuchen zu erstellen; (ii) das Intermediate Certificate an einen Dritten zu verkaufen, verteilen, vermieten, verpachten, lizenzieren, abtreten oder anderweitig zu übertragen; (iii) ein von DigiCert bereitgestelltes Intermediate Certificate nach seinem Ablauf, seiner Revozierung oder dem Ende dieses Agreements zu nutzen; (iv) ein von DigiCert bereitgestelltes Intermediate Certificate abzuändern, zu modifizieren oder zu überarbeiten; oder (v) das Intermediate Certificate zu nutzen, wenn der Kunde Grund zur Annahme hat zu glauben, dass der Private Key des Intermediate Certificate geknackt worden ist.

24. Kennzeichenlizenz und Bedingungen Dritter.

a. DigiCert kann dem Kunden bestimmte Marken und Logos (jeweils ein „**Kennzeichen**“) zur Verfügung stellen, um es dem Kunden zu erlauben anzuzeigen, dass ein bestimmtes Zertifikat für ein bestimmtes Eigentum des Kunden von DigiCert ausgestellt wurde. Nach Ausstellung des jeweiligen Zertifikats und nur solange, wie dieses Zertifikat gültig ist und der Kunde sich vollständig an alle dafür geltenden Bedingungen hält, gewährt DigiCert dem Kunden eine beschränkte, widerrufliche Genehmigung über den Gültigkeitszeitraum des jeweiligen Zertifikats, das jeweilige Kennzeichen (in der Form, wie dem Kunden von DigiCert zur Verfügung gestellt) zu zeigen, um das gültige Zertifikat auf den Produkten, Domainnamen oder Dienstleistungen des Kunden korrekt und nicht irreführend anzuzeigen. Der Kunde verpflichtet sich, die Kennzeichen in keiner Weise zu modifizieren (und auch keine Markenhinweise zu entfernen oder zu modifizieren, die DigiCert an solchen Kennzeichen angebracht hat) oder zu unangemessenen Zwecken zu nutzen oder anzuzeigen oder unter Nutzung der Kennzeichen die Beziehung der Parteien in irgendeiner Weise fehlerhaft darzustellen oder den Ruf von DigiCert zu mindern oder schädigen oder den mit einem Kennzeichen oder einer sonstigen Marke oder Dienstleistungsmarke von DigiCert verbundenen Goodwill zu mindern oder schädigen, einschließlich der Nutzung eines Kennzeichens oder Zertifikats zusammen mit einer Website, die als kriminell, betrügerisch, täuschend, diffamierend, beleidigend, obszön, unangebracht oder Rechte verletzend bezeichnet werden könnte oder die anderweitig vernünftigerweise von DigiCert abgelehnt werden könnte. Aller Goodwill, der in Verbindung mit der Nutzung von Kennzeichen entsteht, dient dem Wohle von DigiCert und falls der Kunde ein Recht, einen Titel oder Rechtsanspruch auf oder an einem solchen Kennzeichen erhält, und zwar infolge der Nutzung eines solchen Kennzeichens, so tritt der Kunde dieses/diesen hiermit unwiderruflich an DigiCert ab.
b. Der Kunde bestätigt und vereinbart, dass wenn ein Kundenzertifikat einen Legal Entity Identifier („**LEI**“) enthält, der von Ubisecure Oy bereitgestellt wird, für die Kunden-LEI sowie auch für die Nutzung des Managementsystems des RapidLEI Legal Entity Identifier oder den Nachfolgerdienst die Ubisecure Oy RapidLEI-Nutzungsbedingungen gelten, die unter https://rapidlei.com/documents/global-lei-system-terms/ zur Verfügung stehen.
c. Der Kunde bestätigt und vereinbart, dass die Nutzung des Kunden von DigiCerts Post-Quanten-Kryptografie-Toolkit (das „**PQC-Toolkit**“) folgenden Bedingungen unterliegt, und zwar zusätzlich zu den Bedingungen einer sonstigen geltenden Lizenzvereinbarung: (i) die dem Kunden in Bezug auf das PQC-Toolkit gewährte Lizenz ist eine nicht exklusive, kündbare Lizenz, die nur in Verbindung mit einem DigiCert-Zertifikat genutzt werden kann, das eine Signatur und einen Public Key enthält, die durch oder mit dem PQC-Toolkit generiert worden sind oder im Rahmen von damit verbundenen Tests und Konfigurationsaktivitäten; (ii) der Kunde erwirbt kein

geistiges Eigentum oder sonstige gewerblichen Schutzrechte am PQC-Toolkit oder dem damit verbundenen geistigen Eigentum; (iii) der Kunde wird das PQC-Toolkit weder rückentwickeln noch übersetzen, disassemblieren, dekompilieren, entschlüsseln oder auseinanderbauen; (iv) der Kunde wird die Nutzung des PQC-Toolkits einstellen, nachdem die damit verbundenen Services von DigiCert gekündigt wurden; (v) die ISARA Corporation haftet dem Kunden gegenüber nicht für etwaige Schäden, gleich welcher Art; (vi) der Kunde wird das PQC-Toolkit nur gemäß den geltenden Gesetzen der Länder oder Gebiete importieren, exportieren oder wiederverwenden, in denen das PQC-Toolkit genutzt oder importiert oder aus denen es exportiert oder reexportiert wird; (vii) der Kunde wird keine Copyrights, Marken oder Patenthinweise im oder am PQC-Toolkit oder in oder an damit verbundenen Materialien ändern.

25. Flow-Down-Anforderungen. Der Kunde darf die technische Implementierung der DigiCert-Systeme oder -Software nicht überwachen, in diese eingreifen oder sie zurückentwickeln oder anderweitig wissentlich die Sicherheit der DigiCert-Systeme oder -Software gefährden und muss gegebenenfalls den von ihm ernannten Herstellern dieselben Einschränkungen auferlegen.

26. Von Microsoft geforderte Zusatzverpflichtungen.

a. Wenn der Kunde die Komponente der automatischen Registrierung von Microsoft nutzt, dann gelten die folgenden VON MICROSOFT GEFORDERTEN ZUSATZVERPFLICHTUNGEN:

b. Ausschluss der Gewährleistung. MICROSOFT UND SEINE AFFILIATES ÜBERNEHMEN KEINE GARANTIE, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND ODER GESETZLICHER ART, BEZÜGLICH DER SERVERSOFTWARE, DIE GEMÄSS DIESEN BEDINGUNGEN BEREITGESTELLT WIRD (DIE „**SERVERSOFTWARE**“) UND ÜBERNIMMT KEINE VERANTWORTUNG FÜR IHRE LEISTUNGSFÄHIGKEIT ODER DEREN FUNKTIONSAUSFALL. IN BEZUG AUF MICROSOFT WIRD DIE SERVERSOFTWARE „WIE GESEHEN“ MIT ALLEN FEHLERN ZUR VERFÜGUNG GESTELLT UND MICROSOFT UND SEINE AFFILIATES SCHLIESSEN HIERMIT ALLE SONSTIGEN GARANTIEN, PFLICHTEN UND BEDINGUNGEN AUS, OB AUSDRÜCKLICHER, STILLSCHWEIGENDER ODER GESETZLICHER ART, INSBESONDERE JEGLICHE STILLSCHWEIGENDE GARANTIE, BEDINGUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK, VERLÄSSLICHKEIT ODER VERFÜGBARKEIT – JEWEILS IN BEZUG AUF DIE SERVERSOFTWARE. MICROSOFT UND SEINE AFFILIATES ÜBERNEHMEN EBENFALLS KEINE GARANTIE ODER BEDINGUNGEN IN BEZUG AUF EIGENTUMSRECHTE, UNGESTÖRTEN BESITZ, ÜBEREINSTIMMUNG MIT DER BESCHREIBUNG ODER NICHTVERLETZUNG VON RECHTEN DRITTER IN BEZUG AUF DIE SERVERSOFTWARE.

c. Ausschluss bestimmter Schäden. SOWEIT DIES GESETZLICH ZULÄSSIG IST, HAFTET MICROSOFT KEINESFALLS FÜR ETWAIGE BESONDERE, BEILÄUFIG ENTSTANDENE, STRAFSCHÄDEN, INDIREKTE ODER FOLGESCHÄDEN, GLEICH WELCHER ART (INSBESONDERE NICHT FÜR SCHADENSERSATZ FÜR ENTGANGENEN GEWINN ODER VERLUST VON VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSSTÖRUNG, PERSONENSCHÄDEN, VERLETZUNG DER PRIVATSPHÄRE, PFLICHTVERSÄUMNIS, AUCH IM GUTEN GLAUBEN UND BEI ANGEMESSENER SORGFALT, FÜR FAHRLÄSSIGKEIT UND FÜR SONSTIGEN MONETÄREN ODER ANDERWEITIGEN VERLUST, GLEICH WELCHER ART), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SERVERSOFTWARE HERVORGEHEN ODER IN IRGENDEINER WEISE DAMIT IN VERBINDUNG STEHEN ODER MIT DER BEREITSTELLUNG ODER NICHTBEREITSTELLUNG VON SUPPORT ODER SONSTIGEN SERVICES, INFORMATIONEN, SOFTWARE UND DAMIT IN VERBINDUNG STEHENDEM CONTENT ÜBER DIE SERVERSOFTWARE ODER ANDERWEITIG AUFGRUND DER NUTZUNG DER SERVERSOFTWARE ODER ANDERWEITIG GEMÄSS ODER IM ZUSAMMENHANG MIT DIESEN NUTZUNGSBEDINGUNGEN, AUCH IM FALLE DES VERSCHULDENS, DELIKTISCHER (EINSCHLIESSLICH FAHRLÄSSIGKEIT), VERSCHULDENSUNABHÄNGIGER HAFTUNG, VERTRAGSVERLETZUNG ODER VERSTOSS GEGEN DIE GARANTIEBESTIMMUNGEN VON MICROSOFT UND AUCH DANN, WENN MICROSOFT AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

d. Serversoftware-Anforderungen. Kunden können nur eine (1) Ausfertigung (wenn in der jeweils geltenden Bestellung nichts anderes bestimmt ist) der Serversoftware nutzen, die gemäß diesen Certificate Terms of Use bereitgestellt wird, wie in der diese Software begleitenden Dokumentation angegeben, und zwar nur dazu, um mit den nativen Client-Betriebssystemen Microsoft Windows 2000 Professional, Windows XP Home oder Professional oder Vista (oder deren jeweilige Nachfolger) zusammenzuarbeiten oder zu kommunizieren. Der

Kunde darf die Serversoftware unter keinen Umständen auf einem Personalcomputer nutzen. Für die untenstehenden Zwecke bedeutet „**Personalcomputer**“ ein Computer, der so konfiguriert ist, dass sein primärer Zweck die Nutzung durch jeweils eine Person ist, und der über ein Anzeigedisplay und eine Tastatur verfügt.

e. Leistungsberechtigte Dritte. Ungeachtet etwaiger unstimmiger Bedingungen im Agreement stimmt der Kunde hiermit zu, dass die Microsoft Corporation als Lizenzgeber des in der Serversoftware enthaltenen geistigen Eigentums als dritter Leistungsberechtigter der Bedingungen und Bestimmungen dieses Punktes 26 gilt, und zwar mit dem Recht, die Bedingungen dieser Certificate Terms of Use durchzusetzen, die eingeschlossenes geistiges Eigentum von Microsoft oder sonstige Interessen von Microsoft in Bezug auf diese Certificate Terms of Use betreffen.

f. Serverklasse 2. Wenn der Kunde die Serverklasse 2 gewählt hat, kann der Kunde die Serversoftware auf einem Server nutzen, der (a) nicht mehr als vier (4) Prozessoren enthält, wobei jeder dieser Prozessoren maximal zweiunddreißig (32) Bit und vier (4) Gigabyte RAM haben kann, und (b) bei dem kein Speicher hinzugefügt, geändert oder entfernt werden kann, ohne dass der Server, auf dem sie läuft, neu gebootet werden muss („**Hot-Swapping-Fähigkeit**“). Der Kunde kann die Serversoftware nicht in Verbindung mit einer Software nutzen, die Hot-Swapping-Fähigkeiten oder Clustering-Fähigkeiten hat, wobei Clustering-Fähigkeiten bedeutet, dass eine Gruppe von Servern als eine einzelne hochverfügbare Plattform funktionieren kann, auf der Anwendungen ausgeführt werden, und zwar mithilfe einer Anwendungs-Ausfallsicherung zwischen den Server-Nodes in der Gruppe.

g. Audit-Rechte. DigiCert kann ein Audit beim Kunden durchführen und die Einrichtungen und Verfahren des Kunden in den Geschäftsräumen des Kunden im Rahmen der gewöhnlichen Geschäftszeiten prüfen, um die Einhaltung aller Bestimmungen dieser Certificate Terms of Use durch den Kunden zu überprüfen, nachdem dieser mit einem Vorlauf von mindestens vierzehn (14) Tagen benachrichtigt worden ist. Ungeachtet etwaiger Unstimmigkeiten zwischen diesem Dokument und dem Agreement (insbesondere bei den Bestimmungen zur Vertraulichkeit) gilt, dass wenn sich der Kunde weigert, sich einer solchen Prüfung zu unterziehen, und DigiCert Grund zur Annahme hat, dass der Kunde sich nicht an die Bedingungen der Servicebeschreibung hält, der Kunde zustimmt, dass DigiCert (i) die Identität des Kunden gegenüber vertrauenden Beteiligten und Verkäufern von Anwendungssoftware offenlegen kann sowie (ii) die Grundlage für DigiCerts Annahme, dass diese nicht eingehalten werden.

h. Multiplexing-Geräte. Hardware oder Software, die die Anzahl von Nutzern reduziert, die direkt auf die über die Serversoftware bereitgestellten Services zugreifen oder diese nutzen, reduziert nicht die Anzahl der Nutzer, die so betrachtet werden, als griffen sie auf die über die Serversoftware bereitgestellten Services zu oder nutzten diese. Die Anzahl der Nutzer, die auf die Serversoftware zugreifen oder diese nutzen, ist gleich der Anzahl der Nutzer, die die Services entweder direkt oder über ein Multiplexing-Gerät nutzen oder auf diese zugreifen, wenn diese Services über (a) die Serversoftware oder (b) eine andere Software oder ein System bereitgestellt werden, bei denen die Authentifizierung oder Autorisierung für diese Software oder Systeme über die Serversoftware erfolgt (ein „**sonstiges authentifiziertes System**“). So wie der Begriff hier verwendet wird, bedeutet ein „**Multiplexing-Gerät**“ eine Hardware oder Software, die direkt oder indirekt Zugriff auf Services erhält oder bereitstellt, die über die Serversoftware oder ein sonstiges authentifiziertes System bereitgestellt werden, und zwar für oder im Namen von mehreren sonstigen Nutzern über eine reduzierte Anzahl von Verbindungen.

i. Windows CAL-Anforderung. Der Kunde muss für jeden Nutzer eine separate Windows CAL erwerben und diesem zuweisen, der entweder direkt oder über ein oder von einem Multiplexing-Gerät aus auf die Services zugreift, die von der Serversoftware oder einem sonstigen authentifizierten System bereitgestellt werden. Eine „**Windows CAL**“ bedeutet (a) eine Windows Device Client Access License („**CAL**“) oder eine Windows User CAL, und zwar in jedem Fall für ein Betriebssystem des Typs Microsoft Windows Server 2003 (Standard Edition, Enterprise Edition oder Datacenter Edition) (oder einem Nachfolgeprodukt dafür) („**Windows Server**“); oder (b) eine Microsoft Core CAL, die einer natürlichen Person oder einem elektronischen Gerät Zugriffsrechte und Nutzungsrechte für Windows Server gewährt, jeweils entweder wie (a) oder (b) oben, die der Kunde für die Nutzung von einem oder mehreren solcher Produkte oder elektronischen Geräte mit dem Betriebssystem des Typs Microsoft Windows Server erworben hat, wobei die Nutzung auf Benutzer- oder Gerätebasis erfolgt.

27. Von Adobe geforderte Zusatzverpflichtungen.

Wenn einem Kunden Adobe Signing Certificates ausgestellt werden, dann verpflichtet sich der Kunde zu Folgendem:

a. Einhaltung der AATL Certificate Policy 2.0 der Adobe Systems Inc., die derzeit unter 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 zur Verfügung steht und unter anderem Folgendes beinhaltet: (1) Generierung und Speicherung von Schlüsselsätzen für Adobe Signing Certificates nur auf Geräten der Sicherheitsstufe FIPS 140-2 Level 2; und (2) nach Registrierung eines neuen Kontos oder nach Beantragung der Registrierung eines neuen AATL-Zertifikats für einen Abonnenten Bereitstellung von wahren und richtigen Angaben an DigiCert, was voraussetzt, dass (A) ein Kontoadministrator eine starke Identitätsprüfung auf Basis eines persönlichen Treffens mit DigiCert oder ein anderes Verfahren durchläuft, das eine vergleichbare Sicherheit bietet (z. B. mittels gesicherter Videokommunikation), (B) ein Kontoadministrator eine starke Identitätsprüfung auf Basis eines persönlichen Treffens mit seinen Abonnenten (d. h. Endnutzern) durchläuft und die Aufzeichnung lokal speichert, um eine Prüfung zu ermöglichen, bis DigiCert ein Onlineverfahren für Administratoren bereitstellt, mit dem Bestätigungen und Aufzeichnungen hochgeladen werden können, und (C) der Identitätsprüfungsprozess, unabhängig ob für einen Administrator oder einen Abonnenten, eine Aufzeichnung enthält, die den Abonnenten selbst und einen gültigen offiziellen Ausweis (z. B. Führerschein, Reisepass, Personalausweiskarte, usw.) zeigt, dessen Foto mit dem Abonnenten übereinstimmt; und

b. der Bedingungen des geltenden CPS.

28. Zusätzliche Beschränkungen für Code Signing Certificates. Der Kunde darf Code Signing Certificates nicht wie folgt nutzen: (i) für oder im Auftrag einer Organisation, die nicht die Organisation des Kunden ist; (ii) Ausführung von Operationen mit einem Private Key oder einem Public Key in Verbindung mit einem Domain- und/oder einem Organisationsnamen, der nicht der auf dem Zertifikatsantrag des Kunden genannte ist; (iii) um verdächtigen Code zu verteilen; oder (iv) auf eine Art und Weise, in der Kontrolle übertragen oder Zugriff auf den Private Key gewährt wird, der dem Public Key des Zertifikats entspricht, und zwar auf oder für jemanden anderen als einen Mitarbeitenden des Kunden, den dieser dazu bevollmächtigt hat (und jede solche Übertragung muss auf sichere Weise erfolgen, damit der Private Key geschützt ist).

Für alle Code Signing Certificates mit OV, die ab dem 1. Juni 2023 ausgestellt werden, einschließlich von Verlängerungen oder Neuausstellungen von Zertifikaten, müssen alle Private Keys auf Hardware gespeichert werden, die gemäß FIPS 140 Level 2, Common Criteria EAL 4+ oder gleichwertig zertifiziert ist. Für alle Code Signing Certificates mit OV, die vor dem 1. Juni 2023 ausgestellt wurden, einschließlich von Verlängerungen oder Neuausstellungen von Zertifikaten, müssen alle Private Keys auf Hardware-Tokens gespeichert werden.

29. Zusätzliche Beschränkungen für nicht öffentliche TLS/SSL-Zertifikate. TLS/SSL-Zertifikate, die an ein privates Root Certificate gekettet sind, dürfen nur mit Intranet-Domains verwendet werden und dürfen nicht Geräten zugewiesen werden, die aus dem Internet öffentlich zugänglich sind. DigiCert behält sich das Recht vor, öffentlich zugängliche Internetserver und/oder Geräte zu überwachen, um sicherzustellen, dass private TLS/SSL-Zertifikate den Bestimmungen dieses Punktes entsprechen. Wenn DigiCert feststellt, dass ein privates TLS/SSL-Zertifikat auf eine Art und Weise genutzt wird, die den Bestimmungen dieses Punktes nicht entspricht, dann wird DigiCert den Kunden sofort über die Nichteinhaltung der Bestimmung benachrichtigen. Der Kunde muss dann innerhalb von vierundzwanzig (24) Stunden entweder (i) das private TLS/SSL-Zertifikat in eine Intranet-Domain verschieben oder (ii) das private TLS/SSL-Zertifikat von den Servern des Kunden entfernen und es revozieren. Wenn der Kunde das nicht konforme Zertifikat nicht revoziert oder entfernt, dann kann DigiCert das Zertifikat revozieren.

30. Elektronische Kommunikations-/Benachrichtigungsmittel. Wenn Sie durch DigiCert bereitgestellte E-Mails oder sonstige elektronische Kommunikations- oder Benachrichtigungsmittel („**Benachrichtigungsmittel**“) nutzen, um Mitteilungen oder Benachrichtigungen zu senden („**Mitteilungen**“), dann vereinbaren Sie, dass (1) die Inhalte von solchen Mitteilungen strikt auf Mitteilungen oder Benachrichtigungen über DigiCert-Produkte oder -Services beschränkt sind; (2) Sie sich an die geltenden Gesetze halten (einschließlich der geltenden Gesetzen zu elektronischer Kommunikation und geltenden Datenschutzgesetze), und zwar in den Rechtsprechungen der Empfänger der Mitteilungen; (3) Sie alleine für die Inhalte sämtlicher Kommunikation verantwortlich sind, die Sie mithilfe der Benachrichtigungsmittel versenden; und (4) Sie DigiCert entschädigen, verteidigen und schadlos halten werden gegenüber Forderungen Dritter, staatlichen Regulierungsmaßnahmen oder Strafen und sämtlichen

Haftungen, Schadensersatzzahlungen und Kosten, einschließlich von angemessenen Anwaltskosten, die durch die Nutzung der Benachrichtigungsmittel oder die Inhalte von Mitteilungen entstehen, die Sie mithilfe der Benachrichtigungsmittel versenden.

31. **Weitergeltung und Beendigung des Agreements.** Die Certificate Terms of Use gelten nach Beendigung des Agreements weiter, bis alle ausgestellten Zertifikate abgelaufen oder revoziert sind.