DIGICERT X9 PKI

ZERTIFIKATS-NUTZUNGSBEDINGUNGEN

1. Geltungsbereich und Zweck

Kurzfassung: *Diese Bedingungen gelten ausschließlich für DigiCerts X9-PKI-Zertifikate. Sie nehmen Bezug auf die X9 CP sowie das DigiCert CPS und spiegeln Branchenstandards wider, die auf die hohen Sicherheitsanforderungen der Finanzbranche und vergleichbarer regulierter Umgebungen zugeschnitten sind. (Sie gelten* ***nicht*** *für DigiCerts Web-PKI-Zertifikate oder sonstige nicht-X9-Zertifikatsdienste.)*

Diese Bedingungen gelten für X9-PKI-Zertifikate, die von DigiCert oder seinen Affiliates unter der Aufsicht des „Accredited Standards Committee X9, Inc." (X9 ASC) ausgestellt werden. Sie gelten nicht für Zertifikate außerhalb der X9 PKI, etwa für DigiCerts öffentlich vertrauenswürdige Web-PKI-Zertifikate oder andere Zertifikatstypen und Dienste, die nicht der X9-Governance unterliegen.

Diese Bedingungen beziehen die „DigiCert X9 Financial PKI Certificate Policy" und einschlägige Richtliniendokumente (zusammen die „X9 CP") sowie das „DigiCert Certification Practices Statement for Private PKI" (das „DigiCert CPS") ein. Zusammen mit diesen Bedingungen regeln sie die Ausstellung, Verwaltung und Widerruf von X9-Zertifikaten. Die X9 CP ist auf Anfrage unter https://x9.org/x9-financial-pki-qa/ in der jeweils gültigen Fassung erhältlich; eine Kopie zu reinen Referenzzwecken ist im DigiCert Legal Repository verfügbar. Das DigiCert CPS ist unter https://www.digicert.com/legal-repository/ in der jeweils gültigen Fassung verfügbar (das „DigiCert Legal Repository").

Diese Bedingungen spiegeln die für die X9 PKI festgelegten Richtlinien und Anforderungen wider, die auf die Erfordernisse der Finanzbranche bzw. anderer hoch-sicherheitskritischer PKI zugeschnitten sind. (Sie unterscheiden sich von den „CA/Browser Forum Baseline Requirements" und anderen Leitlinien, die für öffentlich vertrauenswürdige TLS-Zertifikate gelten.)

2. Verwendung von X9-Zertifikaten

Kurzfassung: *Ein X9-PKI-Zertifikat darf nur für die in der X9 CP definierten und innerhalb Ihrer autorisierten Systeme oder Domains zulässigen Anwendungsfälle verwendet werden. Diese Anwendungsfälle umfassen unter anderem solche, die für den Finanzsektor relevant sind.*

X9-Zertifikate dürfen ausschließlich für die in der X9 CP autorisierten und im Zertifikat selbst abgebildeten Anwendungsfälle genutzt werden. Beispiele:

- mTLS und Kunde-Authentifizierung
- Geräte-Authentifizierung in geschlossenen Netzwerken
- Sichere API-Kommunikation
- Digital signierte Nachrichten im Finanzumfeld

X9-Zertifikate sind nicht für die öffentliche TLS/SSL-Web-PKI, für öffentliche S/MIME-E-Mails oder für sonstige allgemeine Zwecke außerhalb des X9-Vertrauensrahmens bestimmt.

Zertifikate dürfen nur auf Systemen oder Diensten installiert werden, die Ihrer administrativen Kontrolle unterliegen, und sie dürfen nur entsprechend den vorgesehenen „Key Usage"- und „Extended Key Usage"-Erweiterungen verwendet werden.

Auch wenn die technischen Felder eines Zertifikats theoretisch weitergehende Nutzungen zulassen, sind ausschließlich autorisierte PKI-Zwecke gestattet. Eine Nutzung außerhalb dieser Grenzen kann zum Widerruf führen und wird nicht unterstützt.

X9-Zertifikate werden für festgelegte Zwecke entsprechend Zertifikatstyp und -profil gemäß der X9 CP ausgestellt. DigiCert kann jedoch, in Abstimmung mit der X9 Policy Authority, erweiterte oder angrenzende Anwendungsfälle zulassen, sofern die entsprechenden Schlüsselverwendungen konsistent bleiben (z. B. Kunde-Authentifizierung). Solche Genehmigungen müssen innerhalb der technischen und sicherheitsrelevanten Grenzen der X9 CP bleiben und können einer ergänzenden Vereinbarung, Verifizierung oder Richtlinienprüfung unterliegen.

3. Beantragung eines Zertifikats

Kurzfassung: *Bei der Beantragung eines X9-Zertifikats müssen Sie wahrheitsgemäße und genaue Angaben machen und berechtigt sein, ein Zertifikat für die genannte Einheit, Domain und/oder das genannte Gerät zu beantragen.*

Bei der Beantragung eines DigiCert X9-PKI-Zertifikats müssen Sie vollständige, korrekte und wahrheitsgemäße Informationen einreichen. Sie müssen ordnungsgemäß dazu befugt sein, ein Zertifikat für die Organisation, die Person, das Gerät und/oder für sämtliche in Ihrem Antrag enthaltenen Domain-Namen oder sonstigen Identifikatoren zu beantragen. Reichen Sie keine Zertifikatsanträge für Domains oder Ressourcen ein, die Sie nicht besitzen oder kontrollieren, und fügen Sie keine Informationen (z. B. Unternehmensnamen, Marken oder andere Kennzeichen) ein, zu deren Nutzung Sie nicht berechtigt sind.

Mit Einreichung eines Zertifikatsantrags versichern und gewährleisten Sie: (a) dass Sie die gesetzlichen Rechte und Befugnisse besitzen, alle Namen, Identifikatoren und Informationen (einschließlich etwaiger Domain-Namen, IP-Adressen, Unternehmensangaben usw.), die Sie im Zertifikatsantrag angeben, zu nutzen und zu kontrollieren; und (b) dass Ihr Antrag sowie die Zertifikatsausstellung keine Rechte an geistigem Eigentum oder sonstige Rechte Dritter verletzen oder unrechtmäßig in Anspruch nehmen. Jeder Missbrauch des Registrierungsprozesses, jede wesentliche Falschdarstellung von Tatsachen oder die Bereitstellung falscher oder unautorisierter Informationen führt zur Ablehnung Ihres Antrags und kann zum Widerruf eines Zertifikats führen, das gegebenenfalls in Reliance auf solche Angaben ausgestellt wurde.

4. Überprüfung vor der Ausstellung

Kurzfassung: *Vor der Zertifikatsausstellung wird eine Identitäts- und Berechtigungsprüfung durchgeführt - entweder durch DigiCert oder (sofern Ihre Institution als RA agiert) durch Ihre Institution.*

X9-Zertifikate dürfen nur nach erfolgreicher Identitäts- und Berechtigungsverifizierung ausgegeben werden, im Einklang mit der X9 CP und dem anwendbaren CPS. In manchen Fällen handelt Ihre Institution als Registrierungsstelle (Registration Authority, „RA“) und führt die Verifizierung intern gemäß den X9-Standards durch; in anderen Fällen nimmt DigiCert diese Schritte direkt vor.

Die konkreten Verfahren hängen vom Zertifikatstyp und dem vorgesehenen Verwendungszweck ab und können Folgendes umfassen:

- Organisations- oder Domain-Validierung

- Prüfungen der Identität von Geräten oder Software
- Rollenbasierte Berechtigungsprüfungen
- Abgleiche mit behördlichen oder branchenspezifischen Datenquellen

Alle Zertifikate unterliegen der abschließenden Genehmigung durch DigiCert, selbst wenn Ihre Institution als RA fungiert. DigiCert kann die Ausstellung ablehnen, wenn der Antrag nach Einschätzung von DigiCert die Anforderungen der X9 CP nicht erfüllt oder wenn Sicherheits- oder Compliance-Bedenken bestehen.

5. Zusicherungen, Gewährleistungen und Freistellung der Registrierungsstelle

Wenn Ihre Organisation als RA fungiert, versichern und gewährleisten Sie:

(a) Sie werden sämtliche Identitätsprüfungen und Zertifikatsantragsfunktionen in voller Übereinstimmung mit der X9 CP, dem anwendbaren CPS und diesen Bedingungen durchführen;

(b) Sie verfügen über geschultes Personal, haben geeignete Background-Checks implementiert und unterhalten eine sichere Infrastruktur zur Erfüllung Ihrer RA-Pflichten; und

(c) Sie führen genaue Aufzeichnungen und unterstützen Prüfungs-/Audit-rechte gemäß den Anforderungen der X9 CP.

Sie stellen DigiCert Inc., seine Affiliates und X9 ASC (sowie dessen Policy Authority) von sämtlichen Ansprüchen, Schäden, Verlusten, Haftungen oder Kosten (einschließlich angemessener Anwaltskosten) frei, die aus oder im Zusammenhang mit Ihren Handlungen oder Unterlassungen als RA entstehen, einschließlich unter anderem: (i) der unterlassenen Durchführung von Identitätsprüfungen im Einklang mit der X9 CP, (ii) der fehlerhaften Ausstellung oder falschen Darstellung von Zertifikatsinformationen oder (iii) der unbefugten Nutzung oder Offenlegung privater Schlüssel oder von Antragsdaten.

6. Gültigkeitsdauer von Zertifikaten

Kurzfassung: *X9-Zertifikate können für längere Zeiträume als Web-PKI-Zertifikate ausgestellt werden; sie laufen jedoch ab und dürfen nie länger gültig sein als der private Schlüssel der ausstellenden Stamm-CA. OCSP-Schlüssel haben eine maximale Nutzungsdauer von drei Jahren. Nutzen Sie Automatisierung, um Ablaufdaten proaktiv zu managen.*

X9-Zertifikate werden für Zeiträume ausgestellt, die sich nach Ihren Anforderungen richten, vorbehaltlich der X9 CP und des DigiCert CPS. Alle Zertifikate laufen jedoch ab und müssen vor dem Ablaufdatum ersetzt werden, um gültig zu bleiben. In keinem Fall darf die Gültigkeitsdauer eines Zertifikats die Lebensdauer des privaten Schlüssels der ausstellenden CA überschreiten. Darüber hinaus ist die maximale Nutzungsdauer privater Schlüssel für OCSP-Responder in der X9 CP begrenzt. DigiCert setzt diese und andere Lebenszyklusbeschränkungen gemäß den anwendbaren Zertifikatsprofilen und Richtlinien durch.

Um Dienstunterbrechungen zu vermeiden, sind Sie dafür verantwortlich, Ablaufdaten zu überwachen und die rechtzeitige Verlängerung oder Neuerstellung sämtlicher Zertifikate in Ihrer Umgebung sicherzustellen. DigiCert empfiehlt nachdrücklich, eine automatisierte Zertifikats-Lebenszyklusverwaltung einzusetzen, etwa mit DigiCert® Trust Lifecycle Manager oder kompatiblen Tools.

7. Ihre Pflichten als Subscriber

Kurzfassung: *Sie müssen Ihren privaten Schlüssel schützen, das Zertifikat nur im zulässigen Umfang (innerhalb des vorgesehenen Zwecks und der vorgesehenen Systeme) verwenden, die Nutzung einstellen, wenn Angaben unrichtig werden oder das Zertifikat kompromittiert ist, und mit DigiCert bei Zertifikatsanfragen kooperieren. Diese Pflichten sind durch die X9-Zertifikatsrichtlinie vorgeschrieben und für die Sicherheit wesentlich.*

Als Subscriber (wie in der X9 CP definiert) haben Sie wesentliche Verpflichtungen, die eine sichere Nutzung des Zertifikats ausschließlich gemäß diesen Bedingungen und der X9 CP gewährleisten. **Durch die Beantragung oder den Erhalt eines X9-Zertifikats erklären, versichern und gewährleisten Sie gegenüber DigiCert, dass Sie berechtigt sind, diese Bedingungen (einschließlich der einbezogenen X9 CP/CPS) anzunehmen und Ihre Organisation (sofern zutreffend) daran zu binden, und dass Sie Folgendes tun werden:**

(a) **Richtigkeit der Angaben**: Sie stellen jederzeit korrekte und vollständige Informationen in Ihrem Zertifikatsantrag und in sämtlicher Kommunikation mit DigiCert zur Verfügung, die die Ausstellung und Verwaltung des Zertifikats betreffen. Wenn sich während des Validierungsprozesses oder der Gültigkeitsdauer des Zertifikats Informationen ändern oder veralten, informieren Sie DigiCert unverzüglich oder aktualisieren die Informationen wie erforderlich.

(b) **Schutz des privaten Schlüssels**: Sie erzeugen den privaten Schlüssel Ihres Zertifikats sicher unter Verwendung vertrauenswürdiger Systeme und starker kryptografischer Standards (z. B. mindestens ein 2048-Bit-RSA-Schlüssel oder ein Elliptic-Curve-Schlüssel mit vergleichbarer Stärke, sofern nicht strengere Anforderungen durch X9 CP/CPS festgelegt sind). Sie treffen alle angemessenen Maßnahmen, um den privaten Schlüssel vertraulich zu halten und unter Ihrer alleinigen Kontrolle zu bewahren. Dies umfasst den Einsatz geeigneter Hardware- oder Software-Sicherheitsmodule, den Schutz zugehöriger Passwörter oder Token sowie die Verhinderung unbefugten Zugriffs. Der private Schlüssel darf nicht an unbefugte Personen weitergegeben oder offengelegt werden.

(c) **Annahme des Zertifikats**: Nach Ausstellung des Zertifikats durch DigiCert prüfen Sie umgehend die Zertifikatsdetails (z. B. Subject-Name, Unternehmensangaben, Domain-Namen oder andere Identifikatoren sowie sonstige Daten), um die Richtigkeit sicherzustellen. Entdecken Sie Unrichtigkeiten oder Probleme, benachrichtigen Sie DigiCert unverzüglich. Sie installieren oder verwenden das Zertifikat erst, nachdem Sie bestätigt haben, dass alle Angaben korrekt sind und Sie das Zertifikat annehmen.

(d) **Nutzung des Zertifikats**: Sie installieren und verwenden das Zertifikat nur auf den Servern, Geräten, in der Software oder Umgebung, für die es vorgesehen und autorisiert ist, wie sich aus dem Zertifikatsinhalt ergibt. Das bedeutet beispielsweise: Ein Server-TLS-Zertifikat wird nur auf den Servern installiert, die über die im Zertifikat genannten Domain-Namen oder Host-Kennungen erreichbar sind; ein E-Mail-Zertifikat wird nur für die angegebene E-Mail-Adresse oder den benannten Nutzer verwendet; ein Code-Signing-Zertifikat wird nur zur Signierung von Code im Namen der im Zertifikat genannten Organisation/Einheit eingesetzt. Sie verpflichten sich, das Zertifikat ausschließlich in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften und ausschließlich gemäß diesen Bedingungen (einschließlich der einbezogenen X9 CP/CPS) zu verwenden. Das Zertifikat darf nicht auf Systemen oder durch Einheiten

verwendet werden, für die es nicht ausgestellt wurde; es darf nur zur Absicherung derKommunikation oder Transaktionen eingesetzt werden, für die es bestimmt ist.

(e) **Meldung und Widerruf**: Wenn Sie vermuten, dass der private Schlüssel des Zertifikats kompromittiert wurde oder auf irgendeine Weise offengelegt wurde, oder wenn Sie von einer missbräuchlichen Nutzung des Zertifikats Kenntnis erlangen, benachrichtigen Sie DigiCert unverzüglich und beantragen Sie umgehend den Widerruf des Zertifikats. Ebenso gilt: Wenn Angaben im Zertifikat zu irgendeinem Zeitpunkt falsch, ungenau oder irreführend sind oder werden (z. B. wenn Sie einen im Zertifikat enthaltenen Domain-Namen nicht mehr besitzen oder kontrollieren, wenn sich Name oder Adresse Ihrer Organisation ändern oder wenn sonstige Angaben im Zertifikat nicht mehr gültig sind), stellen Sie die Nutzung des Zertifikats sofort ein und beantragen unverzüglich den Widerruf. Warten Sie nicht darauf, dass DigiCert oder eine andere Stelle solche Probleme feststellt —die Initiierung des Widerrufs in diesen Fällen liegt in Ihrer Verantwortung.

(f) **Einstellung der Nutzung**: Wenn ein Zertifikat aus irgendeinem Grund widerrufen wird oder das Ablaufdatum erreicht, entfernen Sie das Zertifikat unverzüglich von allen Geräten und Systemen, auf denen es installiert war, und stellen jede Nutzung des Zertifikats sowie des zugehörigen privaten Schlüssels ein. Die Nutzung eines abgelaufenen oder widerrufenen Zertifikats ist strikt untersagt. Nach Widerruf oder Ablauf verwenden Sie den zugehörigen privaten Schlüssel nicht zur Erstellung neuer Signaturen oder auf sonstige Weise, die auf dem Vertrauen in das widerrufene/abgelaufene Zertifikat beruht. Sobald ein Zertifikat nicht mehr gültig ist (wegen Widerrufs oder Ablaufs), gelten sowohl Zertifikat als auch Schlüssel als außer Betrieb.

(g) **Reaktionspflicht**: Sie reagieren zügig auf Anfragen oder Anweisungen von DigiCert in Bezug auf das Zertifikat oder dessen Nutzung. Wenn DigiCert Sie beispielsweise kontaktiert, um einen möglichen Kompromittierungsfall, Missbrauch oder eine Beschwerde im Zusammenhang mit Ihrem Zertifikat zu untersuchen, sagen Sie eine fristgerechte Antwort und Mitwirkung innerhalb des von DigiCert vorgegebenen Zeitrahmens zu. Eine zeitnahe Mitwirkung kann erforderlich sein, um Sicherheitsvorfälle oder Compliance-Themen zu adressieren und ist Voraussetzung für die fortgesetzte Nutzung des Zertifikats.

(h) **Anerkennung der Widerrufsrechte**: Sie erkennen an und stimmen zu, dass DigiCert als eine von X9 autorisierte Zertifizierungsstelle das Recht hat, Ihr Zertifikat gemäß der X9 CP zu widerrufen. Insbesondere kann Ihr Zertifikat bei einer Kompromittierung des privaten Schlüssels, bei wesentlichen Änderungen der im Zertifikat enthaltenen Informationen oder unter sonstigen Umständen widerrufen werden, die das Zertifikat unzuverlässig machen oder die Nicht-Einhaltung der X9 CP begründen. DigiCert ist berechtigt, einen solchen Widerruf mit sofortiger Wirkung und ohne vorherige Benachrichtigung vorzunehmen, wenn dies zum Schutz der Sicherheit der PKI oder zur Einhaltung geltender Anforderungen erforderlich ist. Im Falle eines Widerrufs informiert DigiCert Sie so bald wie zumutbar über den Widerruf und die Gründe, im Einklang mit den Verfahren der X9 CP.

8. Widerruf (Wann und Warum)

Kurzfassung: *X9-Zertifikate können auf Antrag des Subscriber oder widerrufen werden, wenn ein Sicherheitsrisiko besteht. Das Widerrufsverfahren folgt der X9 CP und kann sich von den Praktiken der öffentlichen Web-PKI von DigiCert unterscheiden (z. B. hinsichtlich Zeitablauf und Kriterien).*

Gemäß der X9 CP kann DigiCert ein X9-Zertifikat aus verschiedenen Gründen widerrufen, u. a.:

(a) **Kompromittierung oder vermutete Kompromittierung des privaten Schlüssels**: Ist der private Schlüssel eines Zertifikats bekanntlich oder mutmaßlich kompromittiert, widerruft DigiCert das Zertifikat zum Schutz der Integrität der PKI.
(b) **Wesentliche Änderungen oder unzutreffende Informationen**: Wenn Angaben im Zertifikat wesentlich falsch oder irreführend werden. Beispielsweise ist ein Widerruf erforderlich, wenn sich Name oder Kontrolle der Organisation des Subscribers so geändert haben, dass die zertifizierten Angaben nicht mehr zutreffen.
(c) **Missbrauch oder Richtlinienverstoß**: Wird ein Zertifikat missbräuchlich verwendet (außerhalb der zulässigen X9-Anwendungsfälle oder entgegen diesen Bedingungen und der X9 CP) oder verletzt der Subscriber seine Pflichten, kann DigiCert das Zertifikat widerrufen. Jede Situation, die das Zertifikat nicht konform zur X9 CP oder anderweitig unzuverlässig macht, führt zum Widerruf.
(d) **Auf Antrag des Subscribers oder eines Bevollmächtigten**: DigiCert widerruft ein X9-Zertifikat auf Antrag des Subscriber (oder eines bevollmächtigten Vertreters der Organisation bzw. der RA) nach Verifizierung der Authentizität des Antrags.
(e) **Sicherheits- oder Compliance-Erfordernis**: DigiCert kann ein Zertifikat widerrufen, wenn dies gesetzlich oder regulatorisch erforderlich ist, auf Anweisung der X9 Policy Authority oder wenn die fortgesetzte Vertrauensstellung das Sicherheitsniveau der X9-PKI beeinträchtigen könnte.

Zusätzlich zum Widerruf behält sich DigiCert vor, Zertifikate (d. h. vorübergehend) zu suspendieren, vorbehaltlich und gemäß den Anforderungen der X9 CP, während ein Sachverhalt untersucht wird. Ein suspendiertes Zertifikat kann anschließend vollständig widerrufen oder, sofern angemessen, wieder in Kraft gesetzt werden.

9. Verschiedenes

Integration mit anderen Vereinbarungen: Diese Bedingungen regeln zusammen mit der DigiCert X9 PKI CP und dem DigiCert CPS Ihre Nutzung der von DigiCert bereitgestellten X9-Zertifikatsdienste. Sie sind Bestandteil des DigiCert Master Services Agreement (https://www.digicert.com/content/dam/digicert/pdfs/legal/master-services-agreement-de.pdf) oder anderer anwendbarer Servicevereinbarungen zwischen Ihnen und DigiCert und ergänzen diese. Bei Widersprüchen zwischen diesen Bedingungen und der X9 CP hat die CP Vorrang. Bei Widersprüchen zwischen diesen Bedingungen und anderen Vereinbarungen, Serviceverträgen oder Bedingungen, die für DigiCert-Angebote gelten, haben diese Bedingungen Vorrang in Bezug auf Angelegenheiten, die sich speziell auf Ihre Nutzung von X9-Zertifikaten beziehen.

Keine Drittbegünstigten: Diese Bedingungen begründen keine Rechte zugunsten Dritter.

Änderungen der Bedingungen: DigiCert kann diese Bedingungen von Zeit zu Zeit aktualisieren oder ändern, um Änderungen bei Leistungen und Technologie, rechtlichen oder regulatorischen Anforderungen oder Änderungen der X9-PKI-Richtlinien oder Branchenstandards Rechnung zu tragen. Aktualisierte Fassungen dieser Bedingungen werden auf der DigiCert-Website (und/oder über Produkt-Click-Throughs, Repositorys oder Kommunikationskanäle) veröffentlicht und durch

ein aktualisiertes „Zuletzt aktualisiert“-Datum kenntlich gemacht. DigiCert kann Abonnenten über wesentliche Änderungen auch per E-Mail-Benachrichtigung oder Kontohinweis informieren. Durch die fortgesetzte Nutzung von X9-Zertifikaten oder zugehörigen Diensten nach einer Aktualisierung erklären Sie Ihr Einverständnis mit den überarbeiteten Bedingungen. Wenn Sie den Änderungen nicht zustimmen, sollten Sie die Nutzung der X9-Zertifikate und zugehörigen Dienste einstellen (vorbehaltlich etwaiger Übergangsregelungen oder Schonfristen, die DigiCert bekannt geben kann). Es liegt in Ihrer Verantwortung, diese Bedingungen regelmäßig auf Aktualisierungen zu prüfen. Diese Bedingungen bleiben in Kraft, bis alle unter ihnen ausgestellten Zertifikate abgelaufen oder widerrufen und nicht mehr in Gebrauch sind oder bis die Bedingungen durch eine neuere Version ersetzt werden.

Hinweis zur vereinfachten Sprache: Zur Erleichterung des Verständnisses enthalten einige Abschnitte dieser Bedingungen „Kurzfassung“-Zusammenfassungen oder vereinfachte Erläuterungen, die den Inhalt des jeweiligen Abschnitts veranschaulichen sollen. Diese vereinfachten Zusammenfassungen sind ausschließlich als Verständnishilfe gedacht und stellen keine rechtlich maßgeblichen Bestimmungen dar. Bei Auslegungszweifeln oder Widersprüchen zwischen einer Kurzfassung und dem vollständigen Text dieser Bedingungen geht stets der ausführliche Text (sowie die einbezogene X9 CP) vor. Die Verwendung vereinfachter Sprache dient der leichteren Verständlichkeit, schmälert jedoch nicht die rechtliche Verbindlichkeit der Bestimmungen. Maßgeblich sind die im vollständigen Text genannten Verpflichtungen von Ihnen und DigiCert.