DIGICERT E-MAIL PKI

ZERTIFIKATS-NUTZUNGSBEDINGUNGEN

ÖFFENTLICH VERTRAUENSWÜRDIGE S/MIME-ZERTIFIKATE

1. Geltungsbereich und Zweck

Kurzfassung: *Diese Bedingungen gelten ausschließlich für DigiCerts öffentlich vertrauenswürdige S/MIME-Zertifikate. Sie nehmen Bezug auf die DigiCert Certificate Policy und das Certification Practice Statement (CP/CPS) und spiegeln Branchenstandards wider (wie die S/MIME Baseline Requirements des CA/Browser Forums und Richtlinien von Root-Stores, z. B. Mozilla), die für öffentlich vertrauenswürdige S/MIME-Zertifikate gelten.*

Diese Bedingungen („Bedingungen“) gelten für öffentlich vertrauenswürdige S/MIME-Zertifikate, die von DigiCert oder seinen verbundenen Unternehmen ausgestellt werden. Sie gelten nicht für TLS/SSL-(browser-vertrauenswürdige) Zertifikate, private/interne S/MIME, Code-Signing, Dokumentensignierung oder EU-qualifizierte Zertifikate. Die Bedingungen beziehen das DigiCert Public Trust CP/CPS (das „CP/CPS“) ein, das unter https://www.digicert.com/legal-repository/ abrufbar ist und zusammen mit diesen Bedingungen regelt, wie S/MIME-Zertifikate ausgestellt, verwaltet und widerrufen werden. Diese Bedingungen spiegeln die vom CA/Browser Forum in den S/MIME Baseline Requirements (abrufbar unter www.cabforum.org/working-groups/smime/documents/) sowie in anwendbaren Root-Store-Policies (z. B. Mozilla, Microsoft, Apple) festgelegten Richtlinien und Anforderungen wider. **Als Zertifizierungsstelle („CA“) ist DigiCert verpflichtet, diese Branchenstandards ohne Ausnahme einzuhalten, einschließlich der unverzüglichen Sperrung (Widerruf) von Zertifikaten, wenn dies vorgeschrieben ist.**

2. Verwendung von S/MIME-Zertifikaten

Sie dürfen DigiCert S/MIME-Zertifikate nur zur Absicherung von E-Mail im Zusammenhang mit Signatur, Verschlüsselung und zugehöriger Kunde-Authentifizierung verwenden. Sie dürfen sie nicht für TLS/SSL-Webserver, Code-Signing, Dokumentensignierung oder andere, nicht damit zusammenhängende Zwecke verwenden.

Zulässige Nutzungen:

- Signieren von E-Mails zur Authentifizierung des Absenders und zur Sicherstellung der Nachrichtenintegrität
- Verschlüsseln von E-Mails zur Wahrung der Vertraulichkeit
- Kunde-Authentifizierung, sofern sie mit den Erweiterungen und Richtlinien des Zertifikats übereinstimmt

Unzulässige Nutzungen:

- TLS/SSL (Webserver-Authentifizierung)
- Code-Signing oder Dokumentensignierung (sofern nicht ausdrücklich vorgesehen)
- Jegliche Nutzung außerhalb des vorgesehenen Umfangs

Die Verwendung eines DigiCert S/MIME-Zertifikats für einen unzulässigen Zweck stellt einen Grund für den Widerruf dar (siehe Abschnitt „**Widerruf**“).

3. Beantragung eines Zertifikats

Kurzfassung: *Wenn Sie ein S/MIME-Zertifikat beantragen, sichern Sie zu, dass Ihre Angaben richtig sind und dass Sie berechtigt sind, ein Zertifikat für die E-Mail-Adresse/Domain und (sofern zutreffend) für die Organisation zu beantragen.*

Bei der Beantragung eines Zertifikats müssen Sie korrekte, vollständige und wahrheitsgemäße Informationen angeben. Dazu gehören die E-Mail-Adresse, Organisationsdaten und alle weiteren für die Ausstellung erforderlichen Angaben.

Mit der Beantragung eines Zertifikats erklären und gewährleisten Sie, dass: **(a)** Sie die gesetzlichen Rechte oder die Befugnis besitzen, die im Zertifikatsantrag aufgeführten Domain-Namen (sowie ggf. Organisations- oder Personennamen) zu nutzen und zu kontrollieren, und **(b)** Ihr Zertifikatsantrag und die beabsichtigte Nutzung **keine Rechte an geistigem Eigentum oder sonstige Rechte Dritter verletzen**. Ein Missbrauch des Registrierungsprozesses oder die Angabe falscher, irreführender oder unautorisierter Informationen stellt einen wesentlichen Verstoß gegen diese Bedingungen dar. DigiCert wird jeden Zertifikatsantrag ablehnen, der gegen diese Regeln verstößt; **jedes Zertifikat, das auf Grundlage falscher oder irreführender Angaben ausgestellt wurde, kann umgehend widerrufen werden.**

4. Überprüfung vor der Ausstellung

Kurzfassung: *DigiCert überprüft die Kontrolle über die E-Mail-Adresse (oder Domain) und — für bestimmte Zertifikatstypen — zusätzlich die Identität der Person oder Organisation.*

Vor der Ausstellung eines öffentlich vertrauenswürdigen S/MIME-Zertifikats führt DigiCert die erforderlichen Validierungsschritte gemäß CP/CPS und den S/MIME Baseline Requirements durch. Dazu gehören:

- **Mailbox-validiert (MV):** DigiCert verifiziert die Kontrolle über die im Zertifikat aufzunehmende E-Mail-Adresse. Dies kann eine Verifizierungs-E-Mail-Challenge, einen erforderlichen DNS-Eintrag für die Domain oder andere zugelassene Methoden zur Postfach-Kontrolle umfassen. DigiCert prüft außerdem DNS-CAA-Einträge auf etwaige „issuemail"-Eigenschaften, die die Ausstellung erlauben oder untersagen.
- **Organisations-validiert (OV):** Zusätzlich zur E-Mail-Kontrolle verifiziert DigiCert die rechtliche Existenz, den operativen Status und die Berechtigung Ihrer Organisation zur Nutzung der E-Mail-Domain. Dies kann die Prüfung amtlicher Register, Adress- und Telefonverifizierung sowie Abgleiche mit Drittquellen umfassen.
- **Sponsor-validiert (SV):** DigiCert validiert die E-Mail-Adresse und bestätigt, dass die Organisation den individuellen Zertifikatsinhaber sponsert. Die Sponsor-Organisation muss verifiziert sein und den Antragsteller benennen.
- **Individuell-validiert (IV):** DigiCert verifiziert die Identität der natürlichen Person, in der Regel anhand eines amtlichen Lichtbildausweises, einer notariellen Beglaubigung oder einer gleichwertigen Methode, und verifiziert die Kontrolle über die E-Mail-Adresse.

Kann DigiCert die Validierung nicht zu seiner Zufriedenheit abschließen, wird kein Zertifikat ausgestellt. DigiCert kann die Ausstellung auch ablehnen, wenn ein Risiko von Betrug oder Nicht-Einhaltung von Branchenstandards oder internen Prozessen besteht.

5. Erklärungen, Gewährleistungen und Freistellung der Registrierungsstelle („RA")

Wenn Ihre Organisation als RA agiert, erklären und gewährleisten Sie:

a. Sie führen sämtliche Identitätsprüfungen und Zertifikatsantragsfunktionen in vollständiger Übereinstimmung mit dem CP/CPS, den S/MIME Baseline Requirements und diesen Bedingungen durch;

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, wie sie im CP/CPS und den S/MIME Baseline Requirements verlangt werden.

Sie erklären sich bereit, DigiCert und dessen verbundene Unternehmen sowie deren jeweilige Direktoren, leitende Angestellte, Beauftragte, Mitarbeiter, Rechtsnachfolger und Abtretungsempfänger von allen Ansprüchen, Schäden, Verlusten, Haftungen oder Kosten (einschließlich angemessener Anwaltsgebühren) freizustellen, zu verteidigen und schadlos zu halten, die aus oder im Zusammenhang mit Ihren Handlungen oder Unterlassungen als RA entstehen, einschließlich unter anderem: (i) der unterlassenen Durchführung von Identitätsprüfungen gemäß CP/CPS, S/MIME Baseline Requirements und diesen Bedingungen, (ii) der fehlerhaften Ausstellung oder falschen Darstellung von Zertifikatsinformationen oder (iii) der unbefugten Nutzung oder Offenlegung privater Schlüssel oder Antragsdaten.

6. Gültigkeitsdauer von Zertifikaten

Kurzfassung: *Zertifikate haben begrenzte Lebensdauern. Die maximal zulässige Laufzeit beträgt 825 Tage (etwa 27 Monate). Sie müssen Zertifikate vor Ablauf ersetzen.*

Öffentlich vertrauenswürdige S/MIME-Zertifikate laufen nach begrenzter Zeit ab. Nach aktuellem Stand beträgt die nach den S/MIME Baseline Requirements maximal zulässige Gültigkeit 825 Tage. Branchenpraktiken können sich zukünftig zugunsten kürzerer Lebenszyklen entwickeln. DigiCert kann aus Komfortgründen Abonnement-Laufzeiten anbieten, die Zertifikate werden jedoch dennoch in den von der Branche vorgegebenen Intervallen neu ausgestellt.

Sie sind dafür verantwortlich, das Ablaufdatum jedes Zertifikats zu überwachen und rechtzeitig ein Ersatz-Zertifikat zu erhalten und zu installieren. Wenn ein Zertifikat abläuft, zeigen abhängige Systeme Fehler an oder können keine sichere Verbindung herstellen. Abgelaufene Zertifikate dürfen nicht verwendet werden. Die weitere Nutzung eines abgelaufenen Zertifikats ist unsicher und verstößt gegen diese Bedingungen. Planen Sie, Zertifikate bei Ablauf unverzüglich zu entfernen oder zu ersetzen.

DigiCert empfiehlt nachdrücklich, Automatisierung (z. B. CertCentral® APIs, Trust Lifecycle Manager oder andere Automatisierungs-Tools) für Erneuerungen und Ersatz einzusetzen.

7. Ihre Pflichten als Subscriber

Kurzfassung: *Durch die Beantragung oder Nutzung eines DigiCert S/MIME-Zertifikats verpflichten Sie sich zu bestimmten Pflichten. Zusammengefasst:* ***(a)*** *korrekte Angaben,* ***(b)*** *Schutz Ihres privaten Schlüssels,* ***(c)*** *Prüfung und Annahme der Zertifikatsinhalte,* ***(d)*** *Nutzung nur im zulässigen Umfang (für die validierte E-Mail-Adresse und im Einklang mit Recht und Richtlinien),* ***(e)*** *unverzüglicher Widerrufsantrag und Nutzungsstopp bei Schlüsselkompromittierung oder Unrichtigkeit von Angaben,* ***(f)*** *Nutzungsende des Zertifikats (und des Schlüssels) bei Ablauf oder Widerruf (mit der Ausnahme, dass Sie den Schlüssel ausschließlich zur Entschlüsselung zuvor empfangener E-Mails behalten dürfen, wo dies zulässig ist),* ***(g)*** *zeitnahe Reaktion auf*

*Sicherheitsanfragen von DigiCert und **(h)** Anerkennung des Widerrufsrechts von DigiCert bei Bedarf. Diese Pflichten ergeben sich aus branchenweiten Standards.*

Als Subscriber (Zertifikatsinhaber) haben Sie wichtige Pflichten, um Ihr S/MIME-Zertifikat sicher und im Einklang mit diesen Bedingungen, dem CP/CPS und den anwendbaren Standards zu verwenden. Sie erklären und gewährleisten gegenüber DigiCert und den Zertifikatsbegünstigten, 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 bereit, die Ihre S/MIME-Zertifikate betreffen. Sie aktualisieren Informationen unverzüglich, wenn sie sich während der Validierung ändern. Werden von Ihnen bereitgestellte Informationen veraltet oder unrichtig (z. B. Änderung Ihres rechtlichen Namens, des Organisationsnamens oder der Adresse oder wenn Sie eine im Zertifikat enthaltene E-Mail-Adresse nicht mehr kontrollieren oder rechtmäßig nutzen), aktualisieren Sie die Information bei DigiCert oder informieren DigiCert über die Änderung.

b. Schutz des privaten Schlüssels. Sie erzeugen den privaten Schlüssel Ihres Zertifikats sicher unter Verwendung vertrauenswürdiger Systeme und starker kryptografischer Standards (**mindestens ein 2048-Bit-RSA-Schlüssel oder eine äquivalente ECC-Stärke, die durch die S/MIME Baseline Requirements zugelassen ist**). Sie halten den privaten Schlüssel jederzeit vertraulich und unter Ihrer alleinigen Kontrolle und setzen Maßnahmen ein, die Verlust, Offenlegung oder unbefugte Nutzung verhindern (z. B. starke Passphrasen, sichere Keystores oder Tokens, geeignete Geräte- und Konto-Kontrollen). Sie sind dafür verantwortlich, den Zugriff auf private Schlüssel zu behalten, die zur **E-Mail-Entschlüsselung** verwendet werden, damit Sie zuvor empfangene verschlüsselte Nachrichten lesen können; soweit nach Richtlinie und Recht zulässig, wird die sichere Sicherung/Treuhand für Entschlüsselungs-Schlüssel empfohlen. (Geben Sie Ihren privaten Schlüssel nicht an Dritte weiter, außer wie im CPS erlaubt, z. B. über einen genehmigten unternehmensweiten Schlüsselverwaltungs-Mechanismus.)

c. Annahme des Zertifikats. Nach Ausstellung des Zertifikats durch DigiCert prüfen Sie die Details (z. B. Subject-Name, rfc822Name-E-Mail-Adresse(n) und etwaige Organisationsangaben), um die Richtigkeit zu bestätigen. Sie verwenden das Zertifikat nur, wenn Sie die Daten überprüft und das Zertifikat angenommen haben. Die Nutzung bedeutet Ihre Annahme. Stellen Sie Unrichtigkeiten fest, müssen Sie DigiCert kontaktieren, um das Zertifikat vor der Nutzung widerrufen oder neu ausstellen zu lassen.

d. Nutzung des Zertifikats. Sie installieren und verwenden das Zertifikat nur auf Ihren eigenen E-Mail-Clients, Geräten und Systemen (oder solchen, zu deren Betrieb Sie berechtigt sind), die E-Mails für die im Zertifikat enthaltene(n) validierte(n) E-Mail-Adresse(n) senden und/oder empfangen. Sie verpflichten sich, das Zertifikat ausschließlich in Übereinstimmung mit diesen Bedingungen (einschließlich CP/CPS) zu verwenden. Das Zertifikat darf **nicht** für andere Zwecke als den vorgesehenen Umfang verwendet werden (d. h. E**-Mail-Signatur und -Verschlüsselung** sowie zugehörige Kunde-Authentifizierung) und darf nicht für Server-TLS/SSL, Code-Signierung, Dokumentensignierung (sofern nicht ausdrücklich profiliert) oder sonstige außer-Umfang-Nutzung verwendet werden.

e. Meldung und Widerruf. Wenn Sie eine tatsächliche oder mögliche Kompromittierung des privaten Schlüssels oder eine missbräuchliche Nutzung des Zertifikats (einschließlich Phishing, Betrug oder anderer unrechtmäßiger Nutzung) vermuten oder feststellen, benachrichtigen Sie

DigiCert unverzüglich und beantragen umgehend den Widerruf des Zertifikats. Ebenso stellen Sie die Nutzung **sofort** ein und beantragen den Widerruf, wenn Angaben im Zertifikat zu irgendeinem Zeitpunkt falsch, ungenau oder irreführend sind (z. B. wenn eine E-Mail-Adresse neu zugewiesen/außer Betrieb genommen wird oder sich Organisationsangaben ändern).

f. Beendigung der Nutzung. Wenn ein Zertifikat aus irgendeinem Grund widerrufen wird oder das Ablaufdatum erreicht, entfernen Sie das Zertifikat **unverzüglich** von allen Systemen und stellen jede Nutzung des Zertifikats und dieses privaten Schlüssels zum Signieren oder gegenüber Verlassenden Parteien ein. Die Nutzung eines **abgelaufenen oder widerrufenen** Zertifikats, die fortbestehendes Vertrauen suggeriert, ist strikt untersagt. Zur Klarstellung: Das Aufbewahren des privaten Schlüssels **ausschließlich zur Entschlüsselung zuvor empfangener E-Mails** (oder zur Erfüllung gesetzlicher Archiv-/Aufbewahrungspflichten) ist zulässig, sofern dies nach Richtlinie und Recht erlaubt ist; den Schlüssel zur Fortführung der Signatur oder zur Umgehung von Widerruf oder Ablauf zu nutzen, ist unzulässig.

g. Reaktionspflicht. Sie reagieren zeitnah auf Anfragen oder Anweisungen von DigiCert in Bezug auf Ihr Zertifikat oder den zugehörigen Schlüssel. Eine zügige Mitwirkung kann entscheidend sein, um Sicherheitsbedrohungen zu mindern oder branchenweite **Widerrufsvorgaben** einzuhalten. Eine verspätete Reaktion stellt einen Verstoß gegen diese Bedingungen dar und kann zur Zertifikatsperrung führen.

h. Anerkennung der Widerrufsrechte. Sie erkennen an und akzeptieren, dass DigiCert als Zertifizierungsstelle das Recht hat, Ihr Zertifikat jederzeit zu widerrufen — auch ohne vorherige Benachrichtigung —, wenn Sie gegen diese Bedingungen verstoßen oder wenn der Widerruf zur Einhaltung des DigiCert CP/CPS, geltenden Rechts oder der Branchenstandards erforderlich ist. Sie stimmen zu, einen solchen Widerruf nicht zu behindern oder anzufechten, und verzichten auf jegliche Ansprüche auf Schadensersatz oder Rechtsbehelfe gegen DigiCert aufgrund eines Widerrufs, der im Einklang mit diesen Bedingungen durchgeführt wird. ***Branchenstandards verlangen von CAs häufig Widerrufe mit kurzer Frist (z. B. innerhalb von 24 Stunden bei bestimmten kritischen Vorfällen und innerhalb von 5 Tagen bei anderen aufgeführten Ereignissen). Sie erkennen an, dass DigiCert diese nicht verhandelbaren Fristen einhalten muss, und erklären sich bereit, in solchen Fällen entsprechend zu handeln.***

8. Widerruf (Wann und Warum)

Kurzfassung: *In bestimmten Fällen muss ein Zertifikat vor dem regulären Ablauf widerrufen werden. DigiCert muss zum Schutz der Sicherheit und zur Einhaltung der Branchenstandards rasch handeln. Sie sind zur Mitwirkung verpflichtet und dürfen den Widerruf nicht behindern.*

In manchen Fällen müssen Sie den Widerruf beantragen (z. B. bei Kompromittierung Ihres privaten Schlüssels oder wenn Sie die Kontrolle über eine E-Mail-Adresse verlieren). In anderen Fällen muss DigiCert ein Zertifikat auch ohne Ihren Antrag widerrufen — oft innerhalb kurzer Fristen. Diese Widerrufspflichten sind nicht verhandelbar und werden durch Branchenstandards vorgeschrieben, einschließlich der S/MIME Baseline Requirements und anwendbarer Root-Store-Policies (z. B. Mozilla Policy). Es gelten die folgenden Fristen.

Widerruf innerhalb von 24 Stunden (verpflichtend)

DigiCert widerruft Zertifikate innerhalb von 24 Stunden, wenn eine der folgenden Situationen eintritt:

a. Sie fordern DigiCert schriftlich auf, das Zertifikat zu widerrufen.

b. Sie teilen DigiCert mit, dass der ursprüngliche Zertifikatsantrag unautorisiert war.
c. DigiCert erhält Hinweise darauf, dass Ihr privater Schlüssel kompromittiert wurde.
d. DigiCert wird über eine nachgewiesene Methode informiert, mit der Ihr privater Schlüssel anhand des öffentlichen Schlüssels im Zertifikat leicht berechnet werden kann.
e. DigiCert erhält Hinweise darauf, dass die Validierung der Domain-Autorisierung oder -Kontrolle für ein im Zertifikat enthaltenes Subjekt-Identitätsmerkmal nicht verlässlich ist.

Widerruf innerhalb von 5 Tagen (verpflichtend)

DigiCert widerruft Zertifikate innerhalb von 5 Tagen, wenn eine der folgenden Situationen eintritt:

a. Das Zertifikat entspricht nicht mehr den erforderlichen technischen Standards (z. B. sind Kryptografie oder Schlüssellänge nach den S/MIME Baseline Requirements oder einer Root-Store-Policy nicht mehr zulässig).
b. DigiCert erhält Hinweise darauf, dass das Zertifikat missbräuchlich verwendet wurde.
c. DigiCert wird darüber informiert, dass Sie eine wesentliche Verpflichtung aus diesen Bedingungen verletzt haben.
d. DigiCert erhält Hinweise darauf, dass die Validierung der Kontrolle über eine im Zertifikat enthaltene E-Mail-Adresse oder einen Domain-Bestandteil nicht verlässlich ist.
e. DigiCert wird auf eine wesentliche Änderung der ursprünglich im Zertifikat enthaltenen Informationen aufmerksam.
f. DigiCert wird darauf aufmerksam, dass das Zertifikat nicht in vollständiger Übereinstimmung mit den S/MIME Baseline Requirements oder dem CP/CPS ausgestellt wurde.
g. DigiCert stellt fest, dass die im Zertifikat enthaltenen Informationen unzutreffend sind.
h. Das Recht von DigiCert, Zertifikate gemäß den S/MIME Baseline Requirements auszustellen, erlischt, wird widerrufen oder beendet — es sei denn, DigiCert hat Vorkehrungen getroffen, um das CRL/OCSP-Repository weiter zu betreiben.
i. Ein Widerruf ist aus einem anderen, oben nicht genannten Grund gemäß dem DigiCert CP/CPS erforderlich.
j. DigiCert wird über eine nachgewiesene Methode informiert, die Ihren privaten Schlüssel der Kompromittierung aussetzt, oder es liegt klarer Nachweis vor, dass die konkrete Methode zur Schlüsselgenerierung fehlerhaft war.

Wenn DigiCert feststellt, dass aus einem der vorstehenden Gründe ein Widerruf erforderlich ist, erfolgt der Widerruf so schnell wie praktikabel. Schwerwiegende Bedrohungen erfordern häufig kurzfristige Widerrufe. DigiCert hält die Branchenregel ein, innerhalb von 24 Stunden bei kritischen Vorfällen und innerhalb von 5 Tagen bei anderen aufgezählten Ereignissen zu widerrufen. Im Einklang mit CP/CPS und Branchenanforderungen untersucht DigiCert Problemberichte zügig und **verzögert den Widerruf nicht** über die zulässige Frist hinaus. Wenn Ihr Zertifikat widerrufen wird oder widerrufen werden soll, sendet DigiCert in der Regel eine Benachrichtigung an die hinterlegte Kontakt-E-Mail mit einer kurzen Begründung, sobald dies zumutbar ist. Nach dem Widerruf wird der Status im Widerrufs-Repository (CRL und/oder OCSP) veröffentlicht; für die Fortsetzung des Dienstes ist ein neues Zertifikat erforderlich. Sie stimmen zu, dass DigiCert zum Widerruf berechtigt ist, und akzeptieren die Folgen eines solchen Widerrufs. DigiCert haftet nicht für Verluste oder Schäden, die Ihnen durch einen Widerruf

entstehen, der gemäß diesen Bedingungen, dem CP/CPS oder den Branchenstandards vorgeschrieben ist.

9. Öffentliche Offenlegung

DigiCert kann eigene Repositorien und Statusdienste betreiben, in denen Zertifikatsinformationen und Widerrufsstatus verfügbar sind (z. B. OCSP-Responder, CRLs und Zertifikats-Statuswebseiten), wie im CPS und den S/MIME Baseline Requirements vorgesehen. Diese sind ihrer Natur nach öffentlich. Durch die Nutzung des Zertifikats erkennen Sie an, dass dessen Status (gültig/widerrufen/abgelaufen) über solche Mechanismen öffentlich offengelegt werden kann.

10. Nicht unterstützte Praktiken (Nutzung auf eigenes Risiko)

Kurzfassung: *Bestimmte Vorgehensweisen im Zusammenhang mit Zertifikatsnutzung werden* ***ausdrücklich nicht empfohlen und nicht von DigiCert unterstützt****. Wenn Sie solche Praktiken einsetzen, geschieht dies auf Ihr eigenes Risiko, und DigiCert kann Sie ggf. nicht unterstützen oder keine Sonderwünsche berücksichtigen. Vermeiden Sie insbesondere das Hard-Coden (Pinning) von Zertifikaten/Schlüsseln in Anwendungen und versuchen Sie nicht, ein einzelnes Zertifikat für mehrere inkompatible Zwecke zu verwenden. Solche Praktiken können zu Dienstunterbrechungen oder Non-Compliance führen.*

Bestimmte Vorgehensweisen bei der Nutzung von DigiCert-Zertifikaten sind nachdrücklich **nicht empfohlen bzw. werden nicht unterstützt**. Die Anwendung solcher Vorgehensweisen erfolgt auf **eigenes Risiko**; in diesem Fall können die Unterstützungs- und Mitwirkungspflichten von DigiCert eingeschränkt sein:

- **Zertifikats/Schlüssel-Pinning:** DigiCert unterstützt kein **Hard-Coden oder „Pinning“** von DigiCert-Zertifikaten oder öffentlichen Schlüsseln in Anwendungen, Firmware oder Geräten. Beim Pinning wird Ihr System so konfiguriert, dass es nur einem bestimmten Zertifikat vertraut. Pinning kann zu Starrheit führen und bei notwendigem, schnellem Ersatz zu Ausfällen oder Sicherheitsrisiken. Wenn Sie Pinning mit einem DigiCert-Zertifikat implementieren, tragen Sie die volle Verantwortung für daraus resultierende Störungen. DigiCert wird erforderliche Maßnahmen (einschließlich Widerruf) **nicht verzögern**, um einer gepinnten Umgebung Rechnung zu tragen.

- **Doppelnutzung / Fehlgebrauch von Zertifikaten:** Verlassen Sie sich nicht auf ein einziges DigiCert-Zertifikat für mehrere, nicht dafür vorgesehene Anwendungsfälle. Beispielsweise ist die Nutzung eines Zertifikats sowohl für S/MIME-E-Mail-Verschlüsselung als auch für *andere Zwecke wie* TLS/SSL (Web-Sicherheit), Code-Signierung oder Kunde-Authentifizierung **nicht unterstützt**. Jeder Zertifikatstyp ist für einen spezifischen Verwendungszweck vorgesehen, wie sich aus Typ und Erweiterungen ergibt. Eine Nutzung entgegen dieser Vorgaben (selbst wenn technisch möglich) ist nicht empfohlen und kann zu Sicherheitslücken oder Non-Compliance führen. Wenn Sie ein Zertifikat in **unzulässiger Weise** verwenden, geschieht dies auf eigenes Risiko; DigiCert ist nicht verantwortlich für die Folgen einer solchen Nutzung.

- **Irreversibles Einbetten:** Vermeiden Sie das Einbetten von Zertifikaten in Kontexte, in denen sie nicht ohne weiteres ersetzt oder widerrufen werden können (z. B. fest in Firmware gebrannte Zertifikate oder weit verbreitete Artefakte ohne Update-Pfad). Wenn

ein solches Zertifikat abläuft oder widerrufen werden muss, können betroffene Geräte ausfallen, ohne dass eine Korrektur im Feld möglich ist.

Verwenden Sie DigiCert-Zertifikate nur in Übereinstimmung mit den Richtlinien von DigiCert, dem CP/CPS und anerkannten Best Practices. Jegliche Verwendung, die den schnellen Widerruf oder Ersatz erschwert (z. B. tief eingebettete Zertifikate in Hardware oder weit verbreitetes Pinning ohne Fallback-Plan), erfolgt auf Ihr eigenes Risiko. Halten Sie stets einen Plan für den raschen Zertifikatsersatz bereit.

11. Verschiedenes

Integration mit anderen Vereinbarungen: Diese Bedingungen regeln zusammen mit dem CP/CPS Ihre Nutzung der von DigiCert bereitgestellten S/MIME-Zertifikate. 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 dem CP/CPS hat das CP/CPS Vorrang. Bei Widersprüchen zwischen diesen Bedingungen und anderen Vereinbarungen, Serviceverträgen oder Bedingungen, die für DigiCert-Angebote gelten, haben diese Bedingungen Vorrang hinsichtlich Angelegenheiten, die sich speziell auf Ihre Nutzung von DigiCert S/MIME-Zertifikaten beziehen.

Gewährleistung zugunsten Verlassender Parteien und Drittbegünstigte: Verlassende Parteien („Relying Parties“) und Application Software Vendors (jeweils wie im CP/CPS definiert und jeweils ein „**Certificate Beneficiary**“) sind ausdrückliche Drittbegünstigte Ihrer Zusicherungen und Pflichten hierin. DigiCert kann eine begrenzte Gewährleistung zugunsten Verlassender Parteien anbieten, die Personen zugutekommt, die gutgläubig auf ein DigiCert-Zertifikat vertrauen (z. B. E-Mail-Empfänger oder Nutzer, die Schäden durch eine fehlerhafte Ausstellung erleiden). Eine solche Gewährleistung stellt keine Gewährleistung gegenüber Ihnen als Zertifikatnehmer dar, sondern gegenüber Dritten, wie im CPS oder in Gewährleistungsdokumenten beschrieben. Abgesehen von den ausdrücklich genannten Regelungen begründen diese Bedingungen keine weiteren Drittbegünstigtenrechte.

Änderungen der Bedingungen: DigiCert kann diese Bedingungen von Zeit zu Zeit aktualisieren oder ändern, um Änderungen bei Leistungen, Technologie, rechtlichen/regulatorischen Anforderungen oder Branchenstandards Rechnung zu tragen. Aktualisierte Fassungen werden auf der DigiCert-Website (und/oder über In-Product-Hinweise, Repositorys oder Kommunikationskanäle) veröffentlicht und durch ein aktualisiertes „Zuletzt aktualisiert“-Datum gekennzeichnet. DigiCert kann Abonnenten über wesentliche Änderungen zusätzlich per E-Mail oder Konto-Benachrichtigung informieren. Durch die fortgesetzte Nutzung von S/MIME-Zertifikaten oder zugehörigen Diensten nach einer Aktualisierung erklären Sie Ihr Einverständnis mit den überarbeiteten Bedingungen. Wenn Sie den Änderungen nicht zustimmen, beenden Sie die Nutzung von S/MIME-Zertifikaten und zugehörigen Diensten (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 hierunter ausgestellten Zertifikate abgelaufen oder widerrufen und außer Betrieb 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. Diese vereinfachten Zusammenfassungen dienen ausschließlich der Verständnishilfe und stellen keine rechtlich maßgeblichen Bestimmungen dar. Bei Unklarheiten oder Widersprüchen zwischen einer Kurzfassung und dem vollständigen Text gelten stets der ausführliche Text sowie das einbezogene CP/CPS. Die Verwendung vereinfachter Sprache soll die Verständlichkeit erhöhen und schmälert nicht die rechtliche Verbindlichkeit der Bestimmungen. Maßgeblich sind die im vollständigen Text genannten Verpflichtungen von Ihnen und DigiCert.