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“) Ruhsu158.7 (-5-1024e)-7 77 (h)-3 (ol)-7.1 .9 (r)3.3 (l)-7.1 (.)-0.t di.1 19710.7Es.7 -1.xte(e)-7 (mä)-7(r)

-

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

„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

”

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

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. D

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

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

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

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 Beq Bin

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.