

TC CERTIFICATES

Allgemeine Geschäftsbedingungen für digitale Zertifikate \ DE

A. Zertifizierungsdienste

1 Zertifizierung

1.1 Zertifizierung öffentlicher Schlüssel

1.1.1 Symantec nimmt die Zertifizierung von öffentlichen Schlüsseln gemäß den jeweils gültigen Zertifizierungsrichtlinien der jeweils zuständigen Zertifizierungsinstanz vor, die im Internet unter

<http://www.trustcenter.de/richtlinien> abrufbar sind.

1.1.2 Mit der Beantragung eines Zertifikates erklärt sich der Kunde damit einverstanden, dass ihm ein Zertifikat ausgestellt wird, das gemäß der Produktbeschreibung für dieses Zertifikat in das Zertifikatsverzeichnis der jeweiligen Zertifizierungsinstanz eingetragen und damit öffentlich zugänglich gemacht werden kann.

1.1.3 Eine Entscheidung über den Antrag auf Zertifizierung kann erst dann vorgenommen werden, wenn alle erforderlichen Daten vorliegen. Symantec behält sich vor, einen Antrag auf Zertifizierung abzulehnen, ohne dass der Vertrag an sich davon berührt wird.

1.1.4 Soweit Symantec bei der Beantragung des Zertifikates den Kunden darauf hingewiesen hat, kann Symantec in das Zertifikat Aussagen über die Beschränkung der Verwendung des Zertifikats aufnehmen.

1.2 Umfang der Zertifizierung

Es werden nur die Angaben, die der Zertifikatsinhaber bei der Antragsstellung auf ein Zertifikat macht, von Symantec bei der Zertifikatsausstellung überprüft. Der Umfang der Zertifizierung wird durch Symantec bestimmt.

1.3 Verwendung von Zertifikaten

1.3.1 Zertifikate mit inhaltlich falschen Zertifikatsangaben dürfen nicht verwendet werden. Private Schlüssel, auf die sich ein solches oder ein abgelaufenes oder ein gesperrtes Zertifikat bezieht, dürfen nicht verwendet werden.

1.3.2 Die Verwendung eines Zertifikates für missbräuchliche oder gesetzeswidrige Zwecke ist nicht zulässig.

2 Verzeichnisdienst

2.1 Zertifikatsabfrage

2.1.1 Wurde ein Zertifikat in ein Zertifikatsverzeichnis aufgenommen, kann jeder im Zertifikatsverzeichnis nach einzelnen Zertifikaten suchen.

2.1.2 Gesperrte Zertifikate werden von der jeweiligen Zertifizierungsinstanz über Zertifikatssperrelisten und gegebenenfalls über das Zertifikatsverzeichnis öffentlich zur Verfügung gestellt.

2.2 Weitergabe von Daten

2.2.1 Das Zertifikatsverzeichnis übermittelt die im Zertifikat enthaltenen Daten automatisiert allen, die das Zertifikat

oder nach bestimmten, in dem Zertifikat enthaltenen Daten anfragen. Diese Übermittlung erfolgt in alle Staaten der Welt. Es werden nur die im Zertifikat enthaltenen Angaben zur zertifizierten Person oder Organisation sowie der Status eines Zertifikats übermittelt.

2.2.2 Symantec wird nur die personen- und organisationsbezogenen Daten erheben, verarbeiten und nutzen, die für das Ausstellen eines Zertifikates und das Führen im Verzeichnisdienst erforderlich sind.

2.2.3 Symantec wird die in den Zertifikaten angegebenen Daten nicht zu Werbezwecken an Dritte weitergeben. Symantec wird die Verarbeitung von Daten nur an solche Unternehmen beauftragen, die konform zu den geltenden Datenschutzvorschriften arbeiten.

2.2.4 Symantec verpflichtet sich, alle personen- und organisationsbezogenen Daten, die nicht im Zertifikat enthalten sind, vor unbefugtem Zugriff sicher zu verwahren. Eine Nennung einer Organisation als Kunde bleibt unbenommen.

3 Sperren von Zertifikaten

3.1 Sperrwege

Eine Sperrung ist möglich

3.1.1 auf der Web-Site von Symantec für bestimmte Produkte unter <http://www.trustcenter.de/sperrn>,

3.1.2 per signierter E-Mail an certificate@trustcenter.de,

3.1.3 per Telefonanruf mit Sperrpasswort unter

+49 (0) 40 / 80 80 26-1 13 oder

3.1.4 schriftlich an Symantec c/o TC TrustCenter GmbH,

Kennwort: Sperrung,

Sonninstraße 24-28, 20097 Hamburg.

Die angegebenen Adressen und Rufnummern sind ausschließlich für Sperrungen reserviert. Es wird keinerlei Hilfe oder Beratung geleistet. Symantec bestätigt die erfolgte Sperrung eines Zertifikates durch eine signierte E-Mail.

3.2 Sperrgründe und -rechte

3.2.1 Zertifikatsinhaber

3.2.1.1 Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls

3.2.1.1.1 Angaben im Zertifikat ungültig sind (z. B. nach Wechsel der E-Mail-Adresse) oder Daten, die in seinem Zertifikat enthalten sind, nicht mehr den Tatsachen entsprechen beziehungsweise nicht mehr mit den Daten zum Zeitpunkt der Zertifizierung übereinstimmen,

3.2.1.1.2 der entsprechende Datenträger mit dem privaten Schlüssel nicht mehr benötigt wird,

3.2.1.1.3 der zum Zertifikat gehörige private Schlüssel verloren wurde,

3.2.1.1.4 der Verdacht besteht, dass unberechtigte Personen

TC CERTIFICATES

Allgemeine Geschäftsbedingungen für digitale Zertifikate \ DE

Zugriff auf den privaten Schlüssel haben oder ihn manipulieren können,

- 3.2.1.1.5** Identifikationsdaten preisgegeben wurden oder ein solcher Verdacht besteht und die Identifikationsdaten nicht geändert wurden.
- 3.2.1.2** Ein Zertifikatsinhaber ist jederzeit ohne Angabe von Gründen berechtigt, sein Zertifikat zu sperren.
- 3.2.2** Symantec
 - 3.2.2.1** Symantec ist verpflichtet, ein Zertifikat zu sperren, falls
 - 3.2.2.1.1** ein berechtigter Sperrantrag eines Zertifikatsinhabers oder eines Dritten vorliegt
 - 3.2.2.1.2** Symantec Kenntnis über einen verpflichtenden Sperrgrund des Zertifikatsinhabers erlangt,
 - 3.2.2.1.3** dem Zertifikatsinhaber nachgewiesen werden kann, dass er gegen Bestimmungen aus dem zugrundeliegenden Vertrags oder Bestimmungen der CPS verstoßen hat,
 - 3.2.2.1.4** die im Zertifikat genannte Person verstorben bzw. die im Zertifikat genannte Organisation umbenannt oder aufgelöst wurde,
 - 3.2.2.1.5** der Kunde den Vertrag beendet,
 - 3.2.2.1.6** Symantec davon überzeugt ist, dass dies notwendig ist, um die Vertrauenswürdigkeit der Zertifizierungsstelle zu schützen oder
 - 3.2.2.1.7** Symantec den Betrieb einstellt und es keine Übergabe an einen Nachfolger gibt oder der Betrieb sonst wie fortgeführt wird.
 - 3.2.2.2** Symantec ist berechtigt, ein Zertifikat zu sperren, falls
 - 3.2.2.2.1** kryptographische Algorithmen oder zugehörige Parameter durch technologische Fortschritte oder neue Entwicklungen in der Kryptologie unsicher werden, wenn das Zertifikat, mit diesen Algorithmen und Parametern erzeugt wurde,
 - 3.2.2.2.2** der Zertifikatsinhaber seinen vertraglichen Verpflichtungen nicht nachkommt, insbesondere das Zertifikat nicht bezahlt,
 - 3.2.2.2.3** Angaben im Zertifikat enthalten sind, die nicht diesen Zertifizierungsrichtlinien entsprechen oder
 - 3.2.2.2.4** es Hinweise auf eine Verletzung der Vertrauenswürdigkeit oder der Sicherheitsfunktionen des Zertifikats gibt, wie sie sich aus einer Missachtung der Sorgfalts- und Mitwirkungspflichten gemäß Ziffer 4 dieser Allgemeinen Geschäftsbedingungen ergeben.
- 3.2.3** Dritte
 - 3.2.3.1** Dritte sind verpflichtet, ein Zertifikat zu sperren, falls
 - 3.2.3.1.1** sie Kenntnis darüber erlangen, dass ein verpflichtender Sperrgrund für den Zertifikatsinhaber oder Symantec vorliegt oder
 - 3.2.3.1.2** bei Zertifikaten, die für die Organisation des Dritten ausgestellt wurden, die Person, auf die das Zertifikat ausgestellt wurde, aus der Organisation ausgeschieden ist.

- 3.2.3.2** Dritte sind berechtigt, ein Zertifikat zu sperren, falls
 - 3.2.3.2.1** sie Angaben zu einem Zertifikat bestätigt haben und diese Angaben nicht mehr den Tatsachen entsprechen oder
 - 3.2.3.2.2** sie im Zertifikat genannt werden und die gemeinsame Nennung von Zertifikatsinhaber und Dritten im Zertifikat nicht länger erwünscht ist.

B **Pflichten des Kunden** **4** **Sorgfalts- und Mitwirkungspflichten des Zertifikatsinhabers**

Diese folgenden Mitwirkungspflichten sind wesentliche Vertragspflichten des Zertifikatsinhabers.

- 4.1** Es dürfen nur inhaltlich richtige Zertifikatsangaben an Symantec übermittelt werden.
- 4.2** Der Datenträger mit dem privaten Schlüssel ist in persönlichem Gewahrsam zu halten. Die Beachtung der Sperrpflichten ist wesentlich für die Erfüllung des Vertrages. Wird der Datenträger mit dem privaten Schlüssel nicht mehr benötigt, ist er unbrauchbar zu machen und die Sperrung des Zertifikats zu veranlassen, falls es nicht abgelaufen ist.
- 4.3** Persönliche Identifikationsnummern oder Passwörter zur Identifikation gegenüber dem Datenträger mit dem privaten Schlüssel sind geheim zu halten. Sie dürfen insbesondere nicht auf dem zugehörigen Datenträger vermerkt oder auf andere Weise zusammen mit diesem aufbewahrt werden. Bei Preisgabe oder Verdacht der Preisgabe dieser Identifikationsdaten ist unverzüglich eine Änderung der Identifikationsdaten vorzunehmen oder eine Sperrung zu veranlassen.
- 4.4** Es ist sicherzustellen, dass sich auf den verwendeten Geräten kein Virus oder schädigende Software befindet, der/die zu einer Preisgabe der Identifikationsdaten oder der geheimen Schlüssel führen können, oder den Signier- oder Signaturprüfvorgang verfälschen können.
- 4.5** Für eine optimale Sicherheit ist es bei der Überprüfung digitaler Signaturen unerlässlich, in dem Zertifikatsverzeichnis von Symantec oder anderen Zertifizierungsstellen festzustellen, ob die Signaturschlüssel-Zertifikate dieser Stellen gültig und nicht gesperrt sind.
- 4.6** Jeder Inhaber eines Zertifikates wählt ein Sperrpasswort für die Sperrung dieses Zertifikats. Dieses Sperrpasswort soll im Notfall schnell verfügbar und vor Missbrauch durch Dritte geschützt sein. Symantec weist darauf hin, dass die missbräuchliche Nutzung des Sperrpasswortes im Einzelfall zu erheblichen Schäden führen kann.
- 4.7** Der Kunde lässt nur seine eigenen Namen von Symantec zertifizieren. Eigene Namen sind solche, an denen keine Dritten, insbesondere eigene Kunden oder andere Organisationen, Rechte haben.

TC CERTIFICATES

Allgemeine Geschäftsbedingungen für digitale Zertifikate \ DE

C Risikoverteilung

5 Haftung

5.1 Symantec haftet für Vorsatz und grobe Fahrlässigkeit. Bei Schäden aus der zurechenbaren Verletzung des Lebens, des Körpers oder der Gesundheit haftet Symantec für leichte Fahrlässigkeit unbegrenzt.

5.2 Für die Verletzung von wesentlichen Vertragspflichten haftet Symantec bei leicht fahrlässiger Verursachung beschränkt auf den von Symantec vorhersehbaren, vertragstypischen, unmittelbaren Durchschnittsschaden. Dies gilt auch bei leicht fahrlässigen Pflichtverletzungen der gesetzlichen Vertreter oder Erfüllungsgehilfen von Symantec. Wesentliche Vertragspflichten sind solche, deren Erfüllung zur Erreichung des Ziels des Vertrags notwendig ist.

5.3 Symantec haftet nicht für die Handlungen der Zertifikatsinhaber oder Dritter, die unbefugt über ein Zertifikat verfügen, für ihre Geschäftsfähigkeit, ihre Zahlungsfähigkeit oder für die Gültigkeit der unter Verwendung dieser Schlüssel abgeschlossenen Geschäfte.

5.4 Symantec haftet nicht für Ausfälle, die außerhalb des Einflussbereichs von Symantec liegen, insbesondere nicht für technische Ausfälle oder die Unerreichbarkeit des Zertifikatsverzeichnisses oder einzelner Zertifikate.

5.5 Symantec übernimmt keinerlei Haftung für die Sicherheit der von den Kunden verwendeten Public-Key-Sicherheitssysteme, soweit sie nicht von Symantec erworben wurden.

5.6 Für den Verlust von Daten und/oder Programmen haftet Symantec insoweit nicht, als der Schaden darauf beruht, dass es der Kunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

5.7 Der Kunde hat etwaige Schäden oder Verluste, die ihn zu Schadensersatzforderungen berechtigen, unverzüglich schriftlich mitzuteilen.

6 Mängelhaftung

6.1 Der Kunde ist verpflichtet, nach Erhalt die Angaben im Zertifikat zu prüfen. Unvollständige und unrichtige Angaben sind Symantec sofort nach Leistungserbringung schriftlich anzuzeigen.

6.2 Symantec wird ein fehlerhaftes Zertifikat durch ein neues Zertifikat ersetzen, wenn der Fehler von Symantec verursacht wurde. Es ist zu beachten, dass ein fehlerhaftes Zertifikat gesperrt wird und damit nicht weiter verwendet werden kann.

6.3 Ist der Kunde Unternehmer, muss er Symantec offensichtliche Mängel des Zertifikats oder der gelieferten

Sache innerhalb einer Frist von zwei Wochen ab Leistungserbringung schriftlich anzeigen; andernfalls ist die Geltendmachung des Mängelhaftungsanspruchs ausgeschlossen. Versteckte Mängel sind unverzüglich nach ihrer Entdeckung schriftlich anzuzeigen. Zur Fristwahrung genügt die rechtzeitige Absendung. Den Kunden trifft die volle Beweislast für sämtliche Anspruchsvoraussetzungen, insbesondere für den Mangel selbst, für den Zeitpunkt der Feststellung des Mangels und für die Rechtzeitigkeit der Mängelrüge

6.4 Symantec leistet für Sachmängel zunächst nach Wahl von des Kunden Gewähr durch Nachbesserung oder Ersatzlieferung. Symantec ist jedoch berechtigt, die vom Kunden gewählte Art der Nacherfüllung zu verweigern, wenn sie nur mit unverhältnismäßigen Kosten möglich ist und die andere Art der Nacherfüllung ohne erhebliche Nachteile für den Kunden bleibt.

6.5 Schlägt die Nachbesserung fehl, kann der Kunde grundsätzlich nach seiner Wahl die Herabsetzung der Vergütung oder die Rückgängigmachung des Vertrags verlangen. Bei einer nur geringfügigen Vertragswidrigkeit, insbesondere bei nur geringfügigen Mängeln, steht dem Kunden jedoch kein Recht zur Rückgängigmachung des Vertrages zu.

6.6 Wählt der Kunde wegen eines Rechts- oder Sachmangels nach gescheiterter Nacherfüllung den Rücktritt vom Vertrag, steht ihm daneben kein Schadensersatz zu.

Wählt der Kunde nach gescheiterter Nacherfüllung Schadensersatz, verbleibt die Sache beim Kunden. Der Schadensersatz beschränkt sich auf die Differenz zwischen dem Kaufpreis und dem Wert der mangelhaften Sache. Dies gilt nicht, wenn Symantec die Vertragsverletzung arglistig verursacht hat.

6.7 Die Mängelhaftungsfrist beträgt ein Jahr ab Ablieferung der Sache. Dies gilt nicht, wenn der Kunde den Mangel Symantec nicht rechtzeitig angezeigt hat.

6.8 Erhält der Kunde eine mangelhafte Dokumentation, ist Symantec lediglich zur Lieferung einer mangelfreien Dokumentation verpflichtet und dies auch nur dann, wenn der Mangel der Dokumentation dem ordnungsgemäßen Gebrauch entgegensteht.

6.9 Garantien im Rechtsinne erhält der Kunde von Symantec nicht. Insbesondere kann Symantec aufgrund der Vielzahl von verfügbaren Anwendungsprogrammen (z. B. Browser) keine Zusicherung über die Kompatibilität der Zertifikate mit diesen Programmen geben.

6.10 Soweit Symantec vertragliche Leistungen infolge Arbeitskampf, höherer Gewalt, Krieg, Aufruhr oder

TC CERTIFICATES

Allgemeine Geschäftsbedingungen für digitale Zertifikate \ DE

anderer für Symantec unabwendbarer Umstände nicht oder nicht fristgerecht erbringen kann, treten für Symantec keine nachteiligen Rechtsfolgen ein.

7 Gefahrübergang

Die Gefahr des zufälligen Untergangs und der zufälligen Verschlechterung geht mit der Auslieferung der Ware an die zur Ausführung der Versendung bestimmte Person auf den Kunden über. Wird der Versand auf Wunsch des Kunden verzögert, geht die Gefahr mit der Meldung der Versandbereitschaft auf ihn über.

8 Eigentumsvorbehalt

8.1 Symantec behält sich das Eigentum an der gelieferten Ware bis zur vollständigen Begleichung aller Forderungen aus einer laufenden Geschäftsbeziehung vor. Der Kunde ist verpflichtet, die gelieferte Ware pfleglich zu behandeln.

8.2 Der Kunde ist verpflichtet, den Zugriff auf die unter Eigentumsvorbehalt gelieferte Ware, etwa im Falle einer Pfändung, sowie etwaige Beschädigungen oder die Vernichtung der gelieferten Ware unverzüglich mitzuteilen. Ein Besitzerwechsel der gelieferten Ware sowie den eigenen Geschäftssitzwechsel hat der Kunde Symantec mitzuteilen.

8.3 Symantec ist berechtigt, bei vertragswidrigem Verhalten des Kunden, insbesondere bei Zahlungsverzug oder bei Verletzung einer Pflicht nach Ziffer 8.2 dieser Allgemeinen Geschäftsbedingungen vom Vertrag zurückzutreten und die gelieferte Ware herauszuverlangen.

9 Ausfuhr

Die Ausfuhr von Soft- und Hardware mit Verschlüsselungseigenschaften durch Symantec erfolgt unter der Bedingung der Genehmigung der zuständigen Behörde am Tag der Ausfuhr. Wird eine Ausfuhr genehmigung versagt, ist Symantec zum Rücktritt vom Vertrag berechtigt. Ein Anspruch auf Schadensersatz wegen Verzögerung der Ausfuhr auf Grund der Dauer des Genehmigungsverfahrens kann nicht geltend gemacht werden.

Sie erkennen an, dass die Software sowie die zugehörigen technischen Daten und Services (zusammenfassend als "Kontrollgesetzen unterliegende Technologie" bezeichnet) den Import- und Exportgesetzen der Vereinigten Staaten von Amerika, insbesondere den Export Administration Regulations (US-Bestimmungen zur Verwaltung des Exports, EAR), sowie jedes Landes unterliegen können, in dem Kontrollgesetzen unterliegende Technologie importiert oder wiederausgeführt ("re-exportiert") wird. Sie erklären sich des Weiteren damit einverstanden, alle relevanten Gesetze

einzuhalten und keine Kontrollgesetzen unterliegende Technologie im Verstoß gegen US-Gesetze an Länder, Organisationen oder Personen zu exportieren, für die eine Exportlizenz oder andere behördliche Genehmigung erforderlich ist. Alle Symantec-Produkte dürfen nicht in die Länder Kuba, Nordkorea, Iran, Syrien und Sudan oder in ein anderes Land, das Handelssanktionen unterliegt, exportiert bzw. aus diesen wiedereingeführt ("re-exportiert") werden. DIE VERWENDUNG ODER BEREITSTELLUNG VON SYMANTEC-PRODUKTEN IM ZUSAMMENHANG MIT AKTIVITÄTEN EINSCHLIESSLICH, ABER NICHT DARAUF BESCHRÄNKT, WIE KONSTRUKTION, ENTWICKLUNG, HERSTELLUNG, SCHULUNG ODER TEST VON CHEMISCHEN, BIOLOGISCHEN ODER NUKLEAREN WAFFEN BZW. RAKETEN, DRONEN ODER WELTRAUMTRÄGERRAKETEN, DIE ALS TRÄGER VON MASSENVERNICHTUNGSWAFFEN DIENEN KÖNNEN, IST GEMÄSS US-GESETZGEBUNG UNTERSAGT.

D Vertragsbeziehung

10 Geltung

10.1 Die in diesen Allgemeinen Geschäftsbedingungen beschriebenen Leistungen unterliegen nicht den Regelungen des Signaturgesetzes. Nur mit Zertifikaten, die in der entsprechenden Produktbeschreibung als „qualifizierte Zertifikate“ bezeichnet werden, können qualifizierte elektronische Signaturen erstellt werden.

10.2 Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen werden, selbst bei Kenntnis von Symantec, nicht Vertragsbestandteil, es sei denn, ihre Geltung wird ausdrücklich durch Symantec schriftlich zugestimmt.

10.3 Auf diese Allgemeinen Geschäftsbedingungen ist deutsches Recht unter Ausschluss des Internationalen Privatrechts und des UN-Kaufrechts anwendbar.

10.4 Änderungen dieser Allgemeinen Geschäftsbedingungen werden dem Kunden in Textform bekannt gegeben. Sie gelten als genehmigt, wenn der Kunde nicht schriftlich Widerspruch erhebt. Auf diese Folge wird ihn Symantec bei der Bekanntgabe besonders hinweisen. Der Kunde muss den Widerspruch innerhalb von sechs Wochen nach Bekanntgabe der Änderung Symantec schriftlich erklären.

10.5 Sollten Teile dieser Allgemeinen Geschäftsbedingungen nicht wirksam sein, so wird die Wirksamkeit der übrigen Bedingungen davon nicht berührt.

10.6 Ein kostenfrei ausgestelltes Zertifikat darf nicht gewerblich genutzt werden. Für kostenfrei erbrachte Leistungen erfolgt keine Gewährleistung und keine Unterstützung oder Hilfeleistung.

TC CERTIFICATES

Allgemeine Geschäftsbedingungen für digitale Zertifikate \ DE

10.7 Falls unterhalb dieses Vertrages dem Kunden Lizenzen an Programmen von Symantec gewährt werden, gelten die dem Programm beigefügten Lizenzbedingungen.

11 Vertragsschluss

11.1 Die Leistungen und Angebote von Symantec erfolgen ausschließlich aufgrund dieser Allgemeinen Geschäftsbedingungen, die auch ohne ausdrückliche nochmalige Vereinbarung für alle zukünftigen Geschäfte gelten, soweit der Kunde Unternehmer ist oder als Unternehmer handelt.

11.2 In Prospekten, Anzeigen und Ähnlichen enthaltene Angaben über das Leistungsprogramm von Symantec sind – auch bezüglich der Preisangaben – freibleibend und unverbindlich. Technische Änderungen bleiben im Rahmen des Zumutbaren vorbehalten.

11.3 Mit der Beantragung eines Zertifikats macht der Kunde ein Vertragsangebot, dass Symantec innerhalb von zwei Wochen nach Eingang bei Symantec annehmen kann. Dies kann entweder schriftlich oder durch Erbringung der Leistung gegenüber dem Kunden erfolgen.

11.4 Soweit ein beauftragtes Zertifikat auf eine Signaturkarte aufzubringen ist, erfolgt der Vertragsschluss unter dem Vorbehalt der richtigen und rechtzeitigen Selbstbelieferung durch die Zulieferer von Symantec. Dies gilt nur für den Fall, dass die Nichtlieferung nicht von Symantec zu vertreten ist, insbesondere bei Abschluss eines kongruenten Deckungsgeschäfts.

Der Kunde wird über die Nichtverfügbarkeit der Leistung unverzüglich informiert. Die Gegenleistung wird unverzüglich zurückerstattet.

11.5 Wenn die Leistung über das Internet-Angebot von Symantec beauftragt wurde, wird der Vertragstext von uns gespeichert und dem Kunden auf Verlangen nebst den vorliegenden Bedingungen per E-Mail zugesandt.

12 Gerichtsstand und Schriftform

12.1 Der Gerichtsstand für alle Rechtsstreitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist München, wenn der Kunde Unternehmer, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Ein etwaiger ausschließlicher Gerichtsstand bleibt hiervon unberührt.

12.2 Alle Änderungen und Ergänzungen vertraglicher Vereinbarungen müssen zu Nachweiszwecken schriftlich niedergelegt werden. Dies gilt auch für das Schriftform-erfordernis selbst. Der Schriftform wird auch durch Einhaltung der digital signierten Form genügt.

E Beendigung des Vertrages

13 Kündigung

13.1 Die Laufzeit des Vertrags ist gebunden an die Gültigkeit des Zertifikats. Da das Zertifikat auch nach einer Sperrung noch im Zertifikatsverzeichnis geführt werden muss, kann bei einer Kündigung oder bei einem Rücktritt auch keine Rückerstattung geleisteter Zahlungen erfolgen.

13.2 Sollte Symantec feststellen, dass der Kunde unrichtige Angaben über seine Kreditwürdigkeit gemacht hat, kann Symantec durch schriftliche Erklärung den Vertrag kündigen.

13.3 Eine Kündigung wird mit einer Frist von einem Monat wirksam. Symantec wird die Kündigung durch Sperrung des Zertifikats vollziehen.

13.4 Das Recht zur außerordentlichen Kündigung bleibt unberührt. Dies ist insbesondere dann gegeben, wenn der Kunde sein Zertifikat bei der mutmaßlichen Begehung von Straftaten nutzt. Eine außerordentliche Kündigung hat eine sofortige Sperrung des Zertifikates zur Folge.

F Zahlungsbedingungen

14 Preise

14.1 Die von Symantec genannten Preise gelten zuzüglich der jeweils gültigen Umsatzsteuer.

14.2 Wenn zwischen Vertragsabschluss und dem vereinbarten oder einem vom Kunden gewünschten und von Symantec akzeptierten anderen Leistungs- beziehungsweise Lieferdatum mehr als vier Monate liegen, gelten die zur Zeit der Leistungserbringung, Lieferung oder Bereitstellung gültigen Preise. Übersteigen diese die zunächst vereinbarten Preise um mehr als zehn Prozent, ist der Kunde berechtigt, vom Vertrag zurückzutreten.

15 Zahlung

15.1 Rechnungsbeträge sind innerhalb von 14 Tagen ab Rechnungsdatum fällig.

15.2 Die Vertragsparteien können nur mit Forderungen aufrechnen, die rechtskräftig festgestellt oder unbestritten sind.

15.3 Gerät der Kunde mit der Zahlung in Verzug, kann Symantec ab Verzugsbeginn Zinsen in Höhe von acht Prozentpunkten p.a. über dem Basiszinssatz verlangen. Außerdem behält Symantec sich vor, den darüber hinausgehenden Verzugsschaden geltend zu machen.

15.4 Negative Auskünfte über den Kunden, insbesondere Wechsel- oder Scheckprotest, Scheckrückgabe und ähnliches sowie nachhaltige Überschreitung eines mit Symantec vereinbarten Zahlungsziels berechtigen

TC CERTIFICATES

Allgemeine Geschäftsbedingungen für digitale Zertifikate \ DE

Symantec, in Zukunft nur noch gegen Sicherheitsleistung oder Vorauszahlung zu liefern. In einem solchen Fall gilt eine Stundung von bereits fällig gewordenen Forderungen als widerrufen, und noch nicht fällige Forderungen werden in diesem Fall sofort fällig. Dies gilt ebenso für die Verschlechterung der Kreditfähigkeit des Kunden seit Vertragsabschluss, insbesondere wenn ein Insolvenzantrag gestellt wurde.

- 15.5** Die Abtretung von Forderungen ist nur mit vorheriger schriftlicher Zustimmung der anderen Vertragspartei zulässig. Die Zustimmung darf nicht unbillig verweigert werden. Ein Zurückbehaltungsrecht kann nur wegen Gegenansprüchen aus dem jeweiligen Vertragsverhältnis geltend gemacht werden.

G Besondere Absatzvereinbarungen

16 Promotion Codes

- 16.1** Für die vollständige oder teilweise Bezahlung eines Zertifikates kann auch ein Promotion Code verwendet werden. Promotion Codes können von Symantec kostenfrei oder kostenpflichtig zur Verfügung gestellt werden.

- 16.2** Promotion Codes haben eine vereinbarte Laufzeit. Nach Ablauf der Laufzeit verfallen nicht genutzte Promotion Codes.

17 TC ID Store

- 17.1** Bestellt ein Kunde einen TC ID Store findet die vorgenannte Ziffer 16 über die Promotion Codes keine Anwendung.

- 17.2** Abweichend von Ziffer 11.3 kommt der Vertrag durch eine schriftliche Bestätigung der Bestellung durch Zusendung der Zugangsdaten zustande.

- 17.3** Ergänzend zu Ziffer 15 wird der Kunde zu Beginn der Vertragslaufzeit ein Startguthaben einzahlen. Der Zeitraum, in welchem aus dem Startguthaben Zertifikate bestellt werden können, ist der Abruflzeitraum. Der Abruflzeitraum endet nach 12 Monaten oder wenn das Guthaben vorher aufgebraucht ist. Abweichend von Ziffer 13.1 endet die Laufzeit des Vertrages mit Ablauf der Gültigkeit des letzten Zertifikates. Ist am Ende des Abruflzeitraums ein Restguthaben vorhanden, wird dieses nicht zurückgezahlt.

- 17.4** Ergänzend zu Ziffer 4 gelten die folgenden Mitwirkungspflichten. Der Kunde wird:
- a)** die in den Symantec Zertifizierungsrichtlinien nieder gelegten Verpflichtungen beachten;
 - b)** nur überprüfte, inhaltlich richtige Zertifikatsangaben an Symantec übermitteln und nach dessen Erhalt die Angaben im Zertifikat prüfen. Unvollständige und unrichtige Angaben sowie erkennbare Mängel sind sofort

nach Leistungserfüllung schriftlich anzuzeigen, versteckte Mängel sofort nach Entdeckung.

c) dafür Sorge tragen, dass während der Laufzeit des Vertrages wenigstens ein Administrator für die Verwaltung des TC ID Store eingesetzt ist,

d) nur Administratoren für die Verwaltung des TC ID Stores einsetzen, die von dem Kunden ausreichend bevollmächtigt wurden hinsichtlich der Registrierung und dem Hinzufügen von Nutzern, dem Ändern von Nutzerdaten, dem Entfernen von Nutzern, dem Sperren, Suspendieren und Desuspendieren von Zertifikaten, der Schlüsselrückgewinnung und Ähnlichem. Die eingesetzten Administratoren sind auf Vorgabe der vorgenannten Anforderung a) sowie auf die Geheimhaltung seiner Zugangsdaten zu verpflichten.

e) „TC Business ID für Adobe Zertifikate“, sofern diese Leistungsgegenstand sind, ausschließlich in Übereinstimmung mit den geltenden Gesetzen und Vorschriften nutzen, einschließlich und uneingeschränkt des US Export-Rechts.

- 17.5** Abweichend zu Ziffer 3.2.1 wird die Sperrung eines Zertifikates ausschließlich in dem TC ID Store entweder durch den Zertifikatsinhaber oder den Administrator für die Verwaltung des TC ID Store vorgenommen werden.

- 17.6** Die Parteien werden alle anwendbaren datenschutzrechtlichen Bestimmungen beachten und die technischen Einrichtungen dementsprechend gestalten sowie ihre Mitarbeiter entsprechend verpflichten.

Soweit bei der Erbringung von Leistungen personenbezogene Daten anfallen, hat der Kunde die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sicherzustellen. Soweit der Kunde personenbezogene Daten zur Verfügung stellt, sichert der Kunde zu, dass die Daten rechtmäßig erhoben wurden und für die vorgesehenen Zwecke verarbeitet, genutzt und an Symantec übermittelt werden dürfen. Symantec wird die personenbezogenen Daten nur in dem Umfang erheben, verarbeiten und nutzen, wie dies zur Durchführung des Vertrages notwendig ist. Symantec ist nicht verpflichtet, die Rechtmäßigkeit der Datenerhebung, -verarbeitung oder -nutzung zu überprüfen. Der Kunde stellt Symantec von Ansprüchen Dritter frei, die darauf beruhen, dass die auftragsgemäße Erhebung, Verarbeitung oder Nutzung personenbezogener Daten rechtswidrig war. Der vorstehende Freistellungsanspruch erfasst auch die Kosten der Rechtsverteidigung. Der Kunde wird Symantec auf erste Anfrage etwaige Einwilligungserklärungen von Zertifikatsinhabern vorlegen.