AlphaSSL
Zertifizierungspraxiserklärung (CPS)

Datum: 12. Mai 2010

Version: v1.3

Inhaltsverzeichnis

Dokumentenhistorie

Steuerung der Belegsänderung

Version	Freigabedatum	Verfasser	Status + Beschreibung
V1.0 V1.1 V1.2 V1.3	01. Mai 2007 09. Mai 2007 16. Dezember 2008 12. Mai 2010	Johan Sys Johan Sys Steve Roylance Johan Sys	Erste Version Verwaltungsupdate Verwaltungsupdate Verwaltungsupdate/Klarstellungen

Bestätigungen

Dieses AlphaSSL CA CPS bekräftigt folgende Industriestandards ganz oder teilweise:

- RFC 3647: Internet X.509 Public-Key-Infrastruktur Zertifikatsregeln und Rahmenvorschriften für Zertifikatsregeln (veraltete RFC 2527)
- RFC 5280: Internet X.509 Public-Key-Infrastruktur-Zertifikat und CRI-Profil.
- RFC 3279: Algorithmen und Identifikatoren für Internet X.509 Public-Key-Infrastruktur-Zertifikat und CRI-Profil
- Den ISO 1-7799 Sicherheits- und Infrastrukturstandard

1.0 Einleitung

Dieses Certification Practice Statement (CPS) der AlphaSSL Zertifizierungsbehörde (hiernach AlphaSSL CA genannt) gilt für die Dienste der AlphaSSL CA, die mit der Ausstellung und Verwaltung digitaler Zertifikate verbunden sind. Dieses CPS finden Sie am Aufbewahrungsort von AlphaSSL CA unter: http://www.alphassl.com/repository.html. Dieses CPS kann gelegentlich aktualisiert werden.

Dieses CPS befasst sich mit den technischen, verfahrensorientierten Personalrichtlinien und –Praktiken der CA in allen Diensten und während des gesamten Lebenszyklus der Zertifikate nach Ausstellung durch die AlphaSSL CA.

Ein Auskunftsersuchen über die Übereinstimmung der AlphaSSL CA mit Akkreditierungssystemen als auch jeder anderen Anfrage im Zusammenhang mit diesem CPS können Sie richten an:

AlphaSSL US
295 Greenwich St #516
New York, NY
10007
USA

AlphaSSL EU
78 York Street
London,
W1H 1DP
United Kingdom

1.1 Überblick

Dieses CPS gilt für die spezielle Domain der AlphaSSL CA. Dieses CPS zielt darauf ab, die Praktiken und Vorgehensweisen der AlphaSSL bei der Verwaltung von Zertifikaten vorzustellen und die Einhaltung der Anforderungen im Zusammenhang mit der Ausstellung digitaler Zertifikate gemäß den eigenen Anforderungen von AlphaSSL und den Anforderungen der Branche gemäß den oben festgelegten Standards zu demonstrieren. Folgende Zertifikatstypen werden in diesem CPS angesprochen:

AlphaSSL-Zertifikat	Ein Zertifikat zur Authentifizierung von Webservern

Dieses CPS legt die Rollen, Zuständigkeiten und Praktiken aller Unternehmen fest, die am Lebenszyklus, an der Nutzung, am Vertrauen auf und an der Verwaltung von AlphaSSL-Zertifikaten beteiligt sind. Die Bestimmungen dieser CPS hinsichtlich der Praktiken, Dienstleistungsebene, Zuständigkeiten und Haftung sind für alle beteiligten Parteien, einschließlich der AlphaSSL CA, der AlphaSSL RA, den Abonnenten und Relying Parties bindend. Einige Bestimmungen gelten möglicherweise auch für andere Einheiten, wie z. B. den Anbieter von Zertifizierungsdiensten, Anwendungsanbieter, usw.).

In diesem CPS werden die Anforderungen für die Ausstellung, Verwaltung und Nutzung von Zertifikaten beschrieben, die von der AlphaSSL CA unter einer verwalteten Brand Root.

Ein Abonnent oder eine Relying Party eines AlphaSSL CA-Zertifikats muss sich auf die AlphaSSL CPS beziehen, um einen Trust aufzubauen. Es ist auch wesentlich, die Vertrauenswürdigkeit der gesamten Zertifikatskette der AlphaSSL-Zertifikatshierarchie, einschließlich der Brand Root, aufzubauen.

Eine umfassende Liste mit Akkreditierungen und Anerkennung der Dienste steht auf Anfrage zur Verfügung.

Diese CPS steht online im Repository der AlphaSSL CA unter http://www.alphassl.com/repository.html zur Verfügung.

Die AlphaSSL CA akzeptiert Kommentare hinsichtlich dieser CPS, die an die oben in der Einleitung dieses Dokuments genannte Adresse gerichtet werden können.

1.2 AlphaSSL-Zertifikatstypen

In diesem Abschnitt werden die öffentlichen AlphaSSL-Produkte beschrieben.

1.2.1 Server-Zertifikate

AlphaSSL bietet Zertifikate für Server/Hardware, die für webbasierte Transaktionen verwendet werden können. In allen Fällen gewährt AlphaSSL dem Abonnenten eine Lizenz, um ein Backup sowohl des Zertifikats als auch des verbundenen privaten Schlüsselpaares zu Zwecken der Geschäftskontinuität zu erstellen. Es wird keine Lizenz für die Übertragung oder Vervielfältigung des Zertifikates und des verbundenen Schlüsselpaares zu einem anderen Zweck zur Verfügung gestellt, sofern dies nicht gesondert während des Verkaufsprozesses durch ein geeignetes Angebot oder eine Werbeaktion angegeben wird, die auf der entsprechenden AlphaSSL-Websiite angezeigt werden kann oder aber nicht muss.

AlphaSSL ist für Einheiten bestimmt, die an einer sicheren Kommunikation und Transaktionen auf Webserver-Ebene teilnehmen möchten. Durch die Verwendung der Secure Socket Layer-Technologie (SSL) sind diese Zertifikate für webbasierte Geschäfte wichtig, die sich mit gesicherten Transaktionen befassen. Von AlphaSSL wird nicht die Identität des Zertifikatsinhabers, sondern nur das Eigentum an der Domain oder die Möglichkeit zur Nutzung der Domain laut Darstellung des Domainnamensystems authentifiziert.

1.2.2 Zulässige Abonnentennamen

Zur Veröffentlichung in seinen Zertifikaten akzeptiert AlphaSSL Abonnentennamen, die eine Bedeutung haben und bei Bedarf authentifiziert werden können.

1.2.2.1 Pseudonyme

AlphaSSL kann die Verwendung von Pseudonymen erlauben, sich aber das Recht vorbehalten, die Identität des Abonnenten offenzulegen, falls dies gesetzliche oder infolge einer vernünftigen und berechtigten Anfrage erforderlich sein sollte.

1.2.3 Registrierungsverfahren

AlphaSSL behält sich das Recht vor, Registrierungsverfahren und die von Abonnenten eingereichten Daten zu aktualisieren, um den Identifizierungs- und Registrierungsprozess zu verbessern.

1.3 AlphaSSL-Zertifikate

1.3.1 Allgemeines

AlphaSSL-Zertifikate sind für eine sichere Kommunikation z. B. mit einer Website über einen SSL- oder TLS-Link bestimmt.

Der Anwender ist eine Einzelperson oder eine Organisation, die einen Internetserver, wie z. B. eine Website besitzt. AlphaSSL-Zertifikate werden verwendet, um eine vertrauliche Kommunikation mit dem Internetserver zu gewährleisten.

Die Gültigkeitsdauer von AlphaSSL-Zertifikaten liegt zwischen einem und fünf Jahren.
AlphaSSL-Zertifikate werden an Einheiten und Einzelpersonen ausgestellt, die einen Domainnamen besitzen oder das Recht haben, ein AlphaSSL-Zertifikat für eine bestimmte Domain anzufordern.

1.3.2 Zertifikatsanfrage

Eine Zertifikatsanfrage kann online über das Internet erfolgen (https). Der Antragsteller für das Zertifikat reicht gemäß einem von AlphaSSL CA bereitgestellten Verfahren einen Antrag über einen sicheren Online-Link ein. Eine zusätzliche Dokumentation zur Begründung des Antrages kann angefragt werden, damit AlphaSSL CA überprüft, dass der Domainname zum Antragsteller gehört oder dass der Antragsteller befugt ist, ein Zertifikat für diesen Domainnamen anzufordern. Der Antragsteller reicht bei AlphaSSL CA die zusätzliche Dokumentation ein. Nach der Überprüfung des Eigentums oder des Rechts auf Nutzung des Domainnamens stellt AlphaSSL CA das Zertifikat aus und sendet dem Antragsteller eine Mitteilung. Der Antragsteller lädt das Zertifikat herunter und installiert es auf dem Server. Der Antragsteller muss AlphaSSL CA nach Erhalt des Zertifikates umgehend über jegliche Ungenauigkeit oder jeden Fehler in einem Zertifikat benachrichtigen.

1.3.3 Inhalt

Typische Informationen, die auf einem AlphaSSL-Zertifikat veröffentlicht werden, beinhalten folgende Elemente:

- Domainname des Antragstellers
- Öffentlichen Schlüssel des Antragstellers
- Ländercode des Antragstellers (nicht verifiziert)
- Ausstellende Zertifizierungsstelle (AlphaSSL CA)
- Elektronische Signatur von AlphaSSL
- Algorithmusart
- Gültigkeitszeitraum des digitalen Zertifikates
- Seriennummer des digitalen Zertifikates

1.3.4 Eingereichte Informationen zur Überprüfung des Eigentums oder Rechts auf Nutzung des Domainnamens

Der Antragsteller muss AlphaSSL CA Kontaktdetails zur Verfügung stellen und diese über einen Click-Through-Prozess unterschreiben. AlphaSSL CA hat das Recht, ein unterzeichnetes Anmeldeformular oder einen unterzeichneten Bezugsvertrag anzufordern. AlphaSSL CA hat das Recht, einen Nachweis über das Eigentum des Domainnamens am Zertifikat anzufordern oder kann den Eigentümer des Domainnamens auffordern, den Antrag des Antragstellers zu bestätigen. AlphaSSL CA überprüft nicht den Ländercode innerhalb der Zertifikatsanfrage.

1.3.5 Zeit zum Bestätigen der eingereichten Daten

AlphaSSL unternimmt angemessene Bemühungen, um Zertifikatsantragsinformationen zu bestätigen und innerhalb eines vernünftigen Zeitrahmens ein digitales Zertifikat auszustellen. Für AlphaSSL werden Zertifikate normalerweise innerhalb von Minuten ausgestellt, aber die Überprüfung kann zwischen 1 und 3 Werktagen in Anspruch nehmen.

1.3.6 Ausstellungsverfahren

Das Ausstellungsverfahren für ein AlphaSSL-Zertifikat läuft wie folgt ab:

1. Der Antragsteller erstellt eine Certificate Signing Request (CSR) und ein Schlüsselpaar mithilfe einer entsprechenden Server-Software
2. Der Antragsteller folgt dem Online-Anmeldeverfahren
3. Der Antragsteller reicht die erforderlichen Informationen, einschließlich dem technischen Ansprechpartner, Serverinformationen und, gegebenenfalls, Zahlungsinformationen ein
4. Der Antragsteller stimmt zu, indem er sich durch das Online-Subscriber Agreement klickt

5. Die Daten werden automatisch mit der Zertifikatsanfrage an AlphaSSL CA gesendet
6. AlphaSSL CA überprüft die eingereichten Informationen durch Überprüfen des Domaineigentums oder des Rechts auf Nutzung der Domain und anderer Informationen, die als relevant erachtet werden. Dies kann auch Vergleiche von Drittdatenbanken oder Ressourcen mit Normungsinstituten, wie z.B. der Internet Engineering Task Force (IETF) oder der Internet Corporation for Assigned Names and Numbers (ICANN) oder eine unabhängige telefonische Überprüfung beinhalten
7. AlphaSSL CA kann den Antragsteller positiv überprüfen
8. AlphaSSL CA kann dem Antragsteller das Zertifikat ausstellen
9. Verlängerung: erlaubt
10. Widerruf: erlaubt

AlphaSSL kann Abweichungen dieses Verfahren anwenden, um Service-, Normungs- oder gesetzliche Anforderungen zu erfüllen.

1.3.7 Beschränkte Garantie

AlphaSSL CA haftet gemäß dieses CPS für bis zu 100 USD pro Schaden aufgrund eines falschen Domainnamens (fehlendes Eigentum oder Recht auf Nutzung der Domain) in einem Zertifikat.

1.3.8 Relevante AlphaSSL-Dokumente

Der Antragsteller muss folgende Dokumente, die unter http://www.alphassl.com/repository.html zur Verfügung stehen, zur Kenntnis nehmen und ist an diese gebunden:

1 AlphaSSL CPS
2 Subscriber Agreement

1.4 Zertifikatsnutzungen

Bestimmte Einschränkungen gelten für die Nutzung von AlphaSSL-Zertifikaten. Ein AlphaSSL-Zertifikat kann nur zur Authentifizierung eines Remote-Domainnamens und Webdienstes und die Verschlüsselung (Vertraulichkeit) des Kommunikationskanals verwendet werden.

Andere Nutzungen von AlphaSSL-Zertifikaten werden mit diesem CPS nicht unterstützt.

1.5 Dokumentname und Identifizierung

AlphaSSL CA gewährleistet für seine Zertifikate die Einhaltung der Anforderungen und Behauptungen dieses CPS.

1.6 PKI-Teilnehmer

Die AlphaSSL CA stellt ihre Dienste an AlphaSSL-Abonnenten zur Verfügung. Zu diesen Abonnenten zählen uneingeschränkt Einheiten, die Zertifikate zu folgenden Zwecken verwenden:

- Authentifizierung (digitale Signatur)
- Verschlüsselung

1.6.1 AlphaSSL Zertifizierungsbehörde

Eine Zertifizierungsbehörde, wie die AlphaSSL CA, ist eine Organisation, die digitale Zertifikate ausstellt, die in öffentlichen oder privaten Domains, innerhalb von Rahmenbedingungen, eines Transaktionskontextes, usw. verwendet werden. Eine Zertifizierungsbehörde wird auch als Ausstellungsbehörde bezeichnet, um den Zweck der Ausstellung von Zertifikaten auf Anfrage einer RA zu kennzeichnen.

Die AlphaSSL CA entwirft und implementiert die Richtlinie, die sich bei der Ausstellung eines bestimmten Typs oder einer Klasse von digitalen Zertifikaten durchsetzt.

Die AlphaSSL CA garantiert die Verfügbarkeit aller Dienste, die zur Verwaltung von AlphaSSL-Zertifikaten gehören, einschließlich, aber nicht beschränkt auf Ausstellung, Widerruf, Statusüberprüfung eines Zertifikates, sofern diese in bestimmten Anfragen verfügbar oder erforderlich werden. Die AlphaSSL CA verwaltet auch ein wesentliches Online-Registrierungssystem für die AlphaSSL-Zertifikate.

Eine entsprechende Veröffentlichung ist erforderlich, um sicherzustellen, dass Relying Parties über die mit den widerrufenen Zertifikaten verbundenen Funktionen informiert oder in Kenntnis gesetzt werden. Die Veröffentlichung wird durch Einbeziehung eines widerrufenen Zertifikates einer Zertifikatswiderrufsliste bekundet, die in einem Online-Verzeichnis veröffentlicht ist. Ausgestellte Zertifikate erscheinen auch in Verzeichnissen ausgestellter Zertifikate. Die AlphaSSL CA betreibt solche Verzeichnisse.

Der Verantwortungsbereich der AlphaSSL CA umfasst die gesamte Verwaltung des Zertifikats-Lebenszyklus einschließlich der folgenden Aktionen:

- Ausstellung
- Widerruf
- Verlängerung
- Statusüberprüfung

1.6.1.1 AlphaSSL CA Auslagerungsagent

Über einen Auslagerungsagent agiert AlphaSSL CA als Sicherheitseinrichtung, um CA-Dienste einschließlich der Ausstellung, Verlängerung, Statusüberprüfung und des Widerrufs von AlphaSSL CA-Zertifikaten bereitzustellen. Der AlphaSSL CA Auslagerungsagent betreibt einen Dienst für die AlphaSSL CA auf der Grundlage eines Dienstleistungsvertrages. Der Umfang des Dienstes entspricht dem Support in der Zertifikatsverwaltung. Der AlphaSSL CA Auslagerungsagent gewährleistet Dienste und Dienstebenen, die den von AlphaSSL CA vorgeschriebenen entsprechen. Der AlphaSSL CA Auslagerungsagent übernimmt Aufgaben im Zusammenhang mit der Verwaltung von Diensten und Zertifikaten im Auftrag von AlphaSSL CA.

1.6.1.2 Rollen von AlphaSSL CA

AlphaSSL CA agiert als Anbieter von Treuhandleistungen, um Treuhandleistungen direkt oder über einen Agenten einer Benutzergemeinschaft bereitzustellen. In diesem Fall beinhaltet ein Agent Dritteinheiten, die vertragsgemäß mit und innerhalb der von AlphaSSL CA festgelegten Bedingungen agieren.

1.6.2 Abonnenten

Abonnenten von AlphaSSL-Diensten sind natürliche Personen, die erfolgreich ein Zertifikat beantragen. Abonnenten sind Parteien, die die höchste Autorität über den privaten Schlüssel haben, der dem in einem abhängigen Zertifikat aufgelisteten öffentlichen Schlüssel entspricht.

- Natürliche Personen, die Abonnenten sind, besitzen normalerweise ein gültiges Ausweisdokument, wie z. B. einen Ausweis, Reisepass oder ähnliches, die als Referenz bei der Ausstellung von AlphaSSL-Zertifikaten verwendet werden können.

Für die Beantragung eines Zertifikats können zusätzliche Referenzen gemäß Erklärung im Online-Prozess erforderlich sein.

1.6.3 Relying Parties

Relying Parties sind natürliche oder rechtliche Personen, die sich auf ein Zertifikat und/oder eine digitale Signatur verlassen, die bezugnehmend auf einen im Zertifikat des Abonnenten aufgelisteten öffentlichen Schlüssel verifizierbar sind.

Um die Gültigkeit eines digitalen Zertifikats zu überprüfen, müssen Relying Parties immer auf die Widerrufsinformationen von AlphaSSL CA, derzeit eine Liste der widerrufenen Zertifikate (CRL) verweisen. Die Zertifikatsüberprüfung findet statt, bevor man sich auf die in einem Zertifikat aufgeführten Informationen verlassen. Relying Parties erfüllen die in dieser CPS beschriebenen Verpflichtungen.

1.7 Zertifikatsnutzung

Bestimmte Einschränkungen gelten für die Nutzung von AlphaSSL CA-Zertifikaten.

1.7.1 Angemessene Zertifikatsnutzung

AlphaSSL-Zertifikate können für öffentliche Domaintransaktionen verwendet werden, die Folgendes erfordern:

- Authentifizierung der Domain und
- Vertraulichkeit

Zusätzliche Verwendungszwecke werden speziell angegeben, sobald sie für die Endeinheiten zur Verfügung stehen. Die unbefugte Nutzung von AlphaSSL-Zertifikaten kann zur Aufhebung von Gewährleistungen führen, die von AlphaSSL CA für Abonnenten und Relying Parties von AlphaSSL-Zertifikaten angeboten werden.

1.7.2 Untersagte Zertifikatsnutzung

Die Zertifikatsnutzung durch eine Endeinheit ist durch die Nutzung von Zertifikatserweiterungen bei der Schlüsselnutzung und erweiterte Schlüsselnutzung beschränkt. Jede Nutzung des Zertifikates, die nicht dieser Erweiterung entspricht, ist unzulässig.

1.7.3 Zertifikatserweiterungen

AlphaSSL CA erstellt Zertifikate, die Erweiterungen enthalten können, die vom X.509 v.3 Standard oder anderen Standards als auch allen anderen Formaten, einschließlich den von Microsoft und Netscape verwendeten, verwendet werden. AlphaSSL verwendet bestimmte Einschränkungen und Erweiterungen für seine öffentlichen PKI-Dienste gemäß der Definition der International Standards Organization (ISO). Solche Einschränkungen und Erweiterungen können die Rolle und Positionen eines CA- oder Abonnenten-Zertifikates begrenzen, so dass solche Abonnenten unter wechselnden Rollen identifiziert werden können.

1.7.4 Kritische Erweiterungen

AlphaSSL CA verwendet bestimmte kritische Erweiterungen in den ausgestellten Zertifikaten, darunter:

- Eine Basiseinschränkung im Zertifikat, um zu zeigen, ob ein Zertifikat für eine CA bestimmt ist oder nicht
- Um die beabsichtigte Nutzung des Schlüssels zu zeigen
- Um die Anzahl der Ebenen in der Hierarchie gemäß einem CA-Zertifikat zu zeigen

1.8 Bestandsverwaltung

Die Bestandsverwaltungsbehörde von AlphaSSL CA verwaltet dieses AlphaSSL CPS. Die AlphaSSL CA registriert, beobachtet die Verwaltung und interpretiert dieses CPS. Die AlphaSSL CA stellt die Betriebsbedingungen zur Verfügung, die in der Lebenszyklusverwaltung von AlphaSSL-Zertifikaten gelten.

1.8.1 Umfang

AlphaSSL kann Änderungen und Aktualisierungen an seinen Richtlinien vornehmen, wenn dies für angebracht oder durch die Umstände als notwendig erachtet wird. Solche Aktualisierungen werden für alle Zertifikate, die ausgestellt wurden oder innerhalb von 30 Tagen nach dem Datum der Veröffentlichung der aktualisierten Version des CPS ausgestellt werden, bindend.

1.8.2 AlphaSSL Bestandsverwaltungsbehörde

Neue Versionen und veröffentlichte Aktualisierungen von AlphaSSL CA-Richtlinien werden von der Bestandsverwaltungsbehörde von AlphaSSL CA genehmigt. Zur Bestandsverwaltungsbehörde ihrer gegenwärtigen Organisationsstruktur der AlphaSSL CA gehören folgende Mitglieder:

- Mindestens ein Mitglied der Geschäftsleitung von AlphaSSL
- Mindestens zwei autorisierte Vertreter, die direkt am Entwurf und an der Entwicklung von AlphaSSL-Praktiken und -Richtlinien beteiligt sind

1.8.3 Akzeptanz aktualisierter Versionen des CPS

Nach der Genehmigung einer CPS-Aktualisierung durch die Bestandsverwaltungsbehörde wird dieses CPS im Repository von AlphaSSL unter http://www.alphassl.com/repository veröffentlicht.

AlphaSSL CA veröffentlicht eine Mitteilung über solche Aktualisierungen auf seiner öffentlichen Website unter http://www.alphassl.com. Die aktualisierte Version ist für alle bestehenden und künftigen Abonnenten bindend, sofern nicht innerhalb von 30 Tagen nach der Übermittlung der Benachrichtigung eine andere Mitteilung eingeht. Nach einem solchen Zeitraum ist die aktualisierte Version des CPS für alle Parteien bindend, einschließlich die Abonnenten und Parteien, die sich auf Zertifikate verlassen, die gemäß einer vorhergehenden Version des AlphaSSL CPS ausgestellt wurden.

AlphaSSL CA veröffentlicht auf seiner Website mindestens die zwei letzten Versionen seines CPS.

1.8.4 Versionsverwaltung und Kennzeichnung von Änderungen

Änderungen werden über eine neue Versionsnummer für das CPS gekennzeichnet. Neue Versionen werden mit einer ganzen Zahl gefolgt von einer Dezimale, die null beträgt, angezeigt. Kleinere Änderungen werden über eine Dezimale angezeigt, die größer als null ist. Kleinere Änderungen beinhalten:

- Kleinere redaktionelle Änderungen
- Änderungen der Kontaktdetails

1.9 Definitionen und Abkürzungen

Eine Liste der Definitionen finden Sie am Ende dieses CPS.

2.0 Zuständigkeiten für Veröffentlichung und Aufbewahrungsort

AlphaSSL CA behält sich das Recht vor, Informationen über die ausgestellten digitalen Zertifikate an einem öffentlich zugänglichen Online-Aufbewahrungsort zu veröffentlichen. AlphaSSL CA behält sich das Recht vor, Statusinformationen zum Zertifikat an Aufbewahrungsorten Dritter zu veröffentlichen.

AlphaSSL CA besitzt einen Online-Aufbewahrungsort für Dokumente, wo bestimmte Praktiken, Verfahren und der Inhalt bestimmter Richtlinien, einschließlich dieses CPS, offengelegt werden. AlphaSSL CA behält sich das Recht vor, mit geeigneten Mitteln innerhalb des AlphaSSL CA-Aufbewahrungsortes Informationen über seine Richtlinien zur Verfügung zu stellen und zu veröffentlichen.

Alle Parteien, die mit Ausstellung, Nutzung oder Verwaltung von AlphaSSL CA-Zertifikaten verbunden sind, werden hiermit benachrichtigt, dass AlphaSSL eingereichte Informationen auf öffentlich zugänglichen Verzeichnissen im Zusammenhang mit der Bereitstellung elektronischer Statusinformationen zum Zertifikat veröffentlichen kann.

AlphaSSL CA sieht davon ab, bestimmte Elemente von Dokumenten, einschließlich Sicherheitskontrollen, Verfahren, internen Sicherheitsrichtlinien usw. öffentlich verfügbar zu machen. Allerdings werden diese Elemente in Prüfungen im Zusammenhang mit formellen Akkreditierungsprogrammen offengelegt, an die sich AlphaSSL CA hält, wie z. B. Web Trust für CAs.

3.0 Identifikation und Authentifizierung

AlphaSSL CA pflegt entsprechende Verfahren zum Umgang mit Kennzeichnungspraktiken, einschließlich der Anerkennung von Markenrechten in bestimmten Namen.

AlphaSSL CA authentifiziert die Anfragen von Parteien, die Zertifikate gemäß dieser Richtlinie widerrufen möchten.

3.1 Erste Identitätsprüfung

Die Identifizierung des Antragstellers für ein Zertifikat wird gemäß einem dokumentierten Verfahren durchgeführt.

Für die Identifikations- und Authentifizierungsverfahren der Erstabonnentenregistrierung kann AlphaSSL CA sich auf solche Ressourcen als Drittdatenbanken verlassen.

3.2 Abonnentenregistrierungsprozess

AlphaSSL garantiert, dass:

- Abonnenten von Zertifikaten ordnungsgemäß identifiziert und authentifiziert werden
- Zertifikatsanfragen von Abonnenten vollständig, genau und ordnungsgemäß autorisiert sind

Insbesondere gilt Folgendes:

- AlphaSSL übermittelt dem Antragsteller eine Mitteilung über seine Webseite unter www.alphassl.com und die entsprechenden Rahmenbedingungen, die im Repository unter www.alphassl.com/repository veröffentlicht sind
- Bevor Sie eine Vertragsbeziehung mit dem Abonnenten eingehen, stellt AlphaSSL ein Subscriber Agreement zur Verfügung, welches der Abonnent vor der Antragsstellung an AlphaSSL genehmigen muss. Dieser Vertrag kann auch im Voraus im Repository von AlphaSSL unter www.alphassl.com/repository eingesehen werden
- AlphaSSL pflegt dokumentierte Vertragsbeziehungen mit allen von Dritten ausgegliederten Agenten, die zum Verteilen von Zertifikaten eingesetzt werden

3.2.1 Dokumente, die für die Abonnentenregistrierung verwendet werden

AlphaSSL oder eine autorisierte AlphaSSL RA überprüft normalerweise Zertifikatsanträge mit den entsprechenden Mitteln und auf der Grundlage eines dokumentierten Verfahrens.

3.2.1.1 AlphaSSL

Der Antragsteller muss bei AlphaSSL CA einen unterzeichneten Bezugsvertrag mit der Satzung der antragstellenden Organisation einreichen oder sich über ein unterzeichnetes Registrierungsformular oder über ein webbasiertes Registrierungs- und Bewerbungsverfahren, gegebenenfalls umfassend Click-Through-Vereinbarungen, bewerben.

AlphaSSL kann einen zusätzlichen Identifizierungsnachweis als Unterstützung der Überprüfung des Eigentums oder Rechts auf Nutzung der Domain des Antragstellers verordnen.

3.2.2 Datensätze für die Abonnentenregistrierung

AlphaSSL CA bewahrt Datensätze des ausgeführten Subscriber Agreements und alle Materialien oder Dokumente auf, die den Antrag unterstützen, der auch Folgendes beinhaltet, aber nicht beschränkt ist auf:

- Den AlphaSSL CA Subscriber Agreement, der vom Antragsteller genehmigt und ausgeführt wurde
- Die Zustimmung für die Aufbewahrung eines Datensatzes mit Informationen, die bei der Registrierung und jeder nachfolgenden Zertifikatsstatusänderung durch AlphaSSL und der Weitergabe dieser Informationen an Dritte gemäß denselben Bedingungen, die von diesem CPS im Falle der Kündigung der Dienste durch die CA erforderlich ist
- Die Tatsache, dass die im Zertifikat enthaltenen Informationen korrekt und genau sind
- Ein speziell entwickeltes Attribut, dass den Antragsteller innerhalb des Kontextes der AlphaSSL CA eindeutig identifiziert

Die oben angegebenen Attribute müssen für einen Zeitraum von mindestens 2 Jahren nach dem Ablauf des Zertifikates aufbewahrt werden.

3.3 Identifikation und Authentifizierung für Widerrufszwecke

Für die Identifikations- und Authentifizierungsverfahren von Widerrufsanträgen schreibt AlphaSSL CA die Verwendung eines Online-Authentifizierungsmechanismus und/oder eines Antrags vor, der an AlphaSSL CA gerichtet wird.

4.0 Systemanforderungen des Zertifikatslebenszykluses

Die folgenden Systemanforderungen gelten für den Zertifikatslebenszyklus.

Alle Einheiten innerhalb der AlphaSSL-Domain, einschließlich Abonnenten oder anderen Teilnehmern sich kontinuierlich verpflichtet, die AlphaSSL CA über alle Änderungen der in einem Zertifikat enthaltenen Informationen während der Betriebszeit eines solchen Zertifikats und bis zu seinem Ablauf oder Widerruf zu informieren.

Um seine Aufgaben auszuführen, kann AlphaSSL Drittagenten einsetzen, für die AlphaSSL die volle Verantwortung übernimmt.

Abonnenten durchlaufen ein Einschreibungsverfahren, das Folgendes erfordert:

- Ausfüllen eines Anmeldeformulares
- Erstellen eines Schlüsselpaares direkt oder indirekt über einen Agenten, der AlphaSSL selbst sein könnte, mit einer Mindestschlüssellänge von 1024 Byte. 2048 Byte sind seit dem 31. Dezember 2010 verpflichtend
- Lieferung des generierten öffentlichen Schlüssels entsprechend einem privaten Schlüssel für AlphaSSL CA
- Annahme des Bezugsvertrags

Der Abonnent ist verpflichtet, die Ausstellungsbedingungen durch einen Bezugsvertrag zu akzeptieren, der mit der AlphaSSL CA ausgeführt wird. Der Bezugsvertrag umfasst als Referenz dieses CPS.

Im Allgemeinen ist ein Online-Einschreibungsverfahren ausreichend, wenn dies von AlphaSSL CA ausdrücklich erlaubt wird.

4.1 Verarbeitung und Ausstellung eines Zertifikatsantrages

Für die Überprüfung der eingereichten Domain verfährt AlphaSSL CA nach einem AlphaSSL CA-Zertifikatsantrag. Folglich wird der Antrag entweder genehmigt oder abgelehnt. Eine solche Genehmigung oder Ablehnung muss nicht unbedingt vor dem Antragsteller oder einer anderen Partei gerechtfertigt werden.

Bei abgelehnten Anträgen von Zertifikatsanfragen notiert AlphaSSL CA den Grund für die Ablehnung des Antrages.

Nach der Ausstellung des genehmigten Zertifikats liefert AlphaSSL CA das ausgestellte Zertifikat direkt oder über einen Vertreter an den Abonnenten.

4.2 Zertifikatserstellung

Bezugnehmend auf die Ausstellung und Verlängerung von Zertifikaten stellt AlphaSSL gegenüber allen Parteien dar, dass Zertifikate sicher gemäß den folgenden Bedingungen ausgestellt werden:

- Das Verfahren zur Ausstellung eines Zertifikates ist sicher mit der verbundenen Registrierung, einschließlich der Bereitstellung eines vom Abonnenten generierten öffentlichen Schlüssels verknüpft
- Die Vertraulichkeit und Integrität der Registrierungsdaten wird jederzeit über entsprechende SSL (Secure Socket Layer)-Links gewährleistet
- Zertifikatsanträge und die Erstellung werden auch durch widerstandsfähige und getestete Verfahren unterstützt, die für die Einhaltung geltender Standards überprüft wurden

4.3 Annahme eines Zertifikates

Ein ausgestellten AlphaSSL CA-Zertifikat gilt vom Abonnenten als angenommen, wenn innerhalb eines Werktages nach Eingang kein Widerspruch gegen das ausgestellte Zertifikat vom Abonnenten an AlphaSSL eingeht.

Jeder Einwand für die Annahme eines ausgestellten Zertifikats muss ausdrücklich der AlphaSSL CA mitgeteilt werden. Die Argumentation für die Ablehnung einschließlich aller Felder im Zertifikat, die fehlerhafte Informationen enthalten, muss auch eingereicht werden.

Die AlphaSSL CA kann das ausgestellte Zertifikat an einem Aufbewahrungsort (X.500 oder LDAP) ablegen. Die AlphaSSL CA behält sich auch das Recht vor, die Zertifikatsausstellung durch AlphaSSL CA an andere Einheiten mitzuteilen.

4.4 Schlüsselpaar und Zertifikatsnutzung

Die Zuständigkeiten im Zusammenhang mit der Verwendung von Schlüsseln und Zertifikaten umfassen die unten aufgeführten:

4.4.1 Abonnent

Die Verpflichtungen des Abonnenten umfassenden Folgendes:

4.4.1.1 Pflichten des Abonnenten

Sofern in dieser CPS nicht anders angegeben beinhalten die Pflichten des Abonnenten Folgendes:

1. Annahme aller am AlphaSSL-Aufbewahrungsort veröffentlichten geltenden Konditionen und Bedingungen in der CPS
2. Benachrichtigung der AlphaSSL CA über Änderungen der eingereichten Informationen, die sich wesentlich auf die Vertrauenswürdigkeit dieses Zertifikats auswirken können
3. Einstellen der Nutzung eines AlphaSSL-Zertifikates, sobald es ungültig wird
4. Verwendung eines AlphaSSL-Zertifikates, wenn dies unter den gegebenen Umständen sinnvoll ist
5. Vermeiden des Kompromisses, Verlustes, der Offenlegung, Modifizierung oder anderweitigen ungefugten Nutzung eines privaten Schlüsseles oder des starken Passwortes, der zum Schutz des privaten Schlüssels in einem Szenario verwendet wird, wo AlphaSSL zur Generierung des Schlüssels verpflichtet ist
6. Verwendung sicherer Geräte und Produkte, die einen entsprechenden Schutz für die Schlüssel bieten. AlphaSSL CA stellt keine Verschlüsselungsmodule an Abonnenten aus.
7. Absehen von der Einreichung jeglicher Materialien an AlphaSSL CA oder ein anderes AlphaSSL CA-Verzeichnis, die Äußerungen enthalten, die gegen ein Gesetz oder die Rechte einer Partei verstoßen
8. Antrag auf Widerruf eines Zertifikates im Falle eines Vorfalls stellen, der die Integrität eines AlphaSSL CA-Zertifikats wesentlich beeinträchtigt
9. Absehen von einer Verfälschung mit einem Zertifikat
10. Ausschließlich Verwendung von Zertifikaten für rechtliche und zulässige Zwecke gemäß des CPS
11. Absehen von der Verwendung eines Zertifikats außerhalb möglicher Lizenzbeschränkungen, die von AlphaSSL CA auferlegt werden

Der Abonnent hat jederzeit alle oben genannten Pflichten gegenüber der CA.

4.4.1.2 Pflicht des Abonnenten gegenüber der Relying Parties

Ohne die Einschränkung anderer Verpflichtungen des Abonnenten, die anderer Stelle in diesem CPS genannt sind, sind Abonnenten verpflichtet, von Falschdarstellungen, die Sie in Zertifikaten gegenüber Dritten machen, die sich auf die hierin enthaltenen Informationen verlassen, abzusehen.

4.4.1.3 Vertrauen auf eigene Gefahr

Es liegt im eigenen Ermessen der Parteien, auf Informationen, die in den Speicherorten und Webseiten der AlphaSSL CA abgelegt sind, zuzugreifen, um auf die hierin enthaltenen Informationen zuzugreifen und sich darauf zu verlassen. Die Parteien bestätigen, dass sie entsprechende Informationen erhalten haben, um zu entscheiden, ob sie sich auf die in einem Zertifikat enthaltenen Informationen verlassen können. Die AlphaSSL CA ergreift die notwendigen Schritte für die Aktualisierung seiner Datensätze und Verzeichnisse betreffen den Status der Zertifikate und stellt dahingehend Warnungen aus. Die Nichteinhaltung der Nutzungsbedingungen der AlphaSSL CA Aufbewahrungsorte und der Webseite kann zur Kündigung der Beziehung zwischen der AlphaSSL CA und der Partei führen.

4.4.2 Relying Party

Eine Relying Party hat folgende Pflichten:

4.4.2.1 Pflichten einer Relying Party

Eine Partei, die sich auf ein AlphaSSL-Zertifikat verlässt:

- Überprüft ein AlphaSSL-Zertifikat durch die Verwendung von Zertifikatsstatusinformationen (z. B. eine CRL), die von AlphaSSL veröffentlicht wird
- Vertraut einem AlphaSSL CA-Zertifikat nur, wenn all auf einem solchen Zertifikat angegebenen Informationen über ein solches Prüfungsverfahren auf Richtigkeit und Aktualität überprüft werden können
- Verlässt sich auf ein AlphaSSL-Zertifikat, nur wenn dies unter den gegebenen Umständen sinnvoll ist.
- Vertraut einem Zertifikat nur dann, wenn es nicht widerrufen wurde

4.4.2.2 AlphaSSL CA-Bedingungen für Aufbewahrungsort und Website

Parteien, einschließlich Abonnenten und Relying Parties, die auf den AlphaSSL Ca-Aufbewahrungsort und die Website zugreifen, stimmen den Bestimmungen dieses CPS und allen anderen Nutzungsbedingungen zu, die die AlphaSSL CA zur Verfügung stellt. Parteien zeigen ihre Akzeptanz der Nutzungsbedingungen des CPS, indem sie eine Anfrage hinsichtlich des Status eines digitalen Zertifikates stellen oder auf irgendeine Weise solche bereitgestellten Informationen oder Dienste nutzen oder sich darauf verlassen:

- Erhalten von Informationen infolge der Suche nach einem digitalen Zertifikat
- Überprüfen des Statuses eines digitalen Zertifikates vor dem Verschlüsseln von Daten mithilfe des öffentlichen Schlüssels, der in einem Zertifikat enthalten ist
- Erhalten von Informationen, die auf der AlphaSSL CA Website veröffentlicht werden

4.5 Verlängerung des Zertifikats

Abonnenten können die Verlängerung von AlphaSSL-Zertifikaten beantragen. Um die Verlängerung eines AlphaSSL-Zertifikates zu beantragen, hinterlegt ein Endbenutzer eine Online-Anfrage.

Anforderungen für die eventuelle Verlängerung von Zertifikaten können von denen abweichen, die ursprünglich für das Abonnieren des Dienstes erforderlich sind.

4.6 Widerruf des Zertifikats

AlphaSSL CA muss angemessene Bemühungen unternehmen, um klare Richtlinien für den Widerruf von Zertifikaten zu veröffentlichen und eine Verfügbarkeit rund um die Uhr aufrechterhalten, um Widerrufsanträge zu akzeptieren und zu beantworten.

Die Identifikation des Abonnenten, der einen Widerruf eines Zertifikats beantragt, erfolgt gemäß einem internen dokumentierten Verfahren. Dieses Verfahren unterliegt der Prüfung durch autorisierte Parteien gemäß den Anforderungen, die von Akkreditierungsprogrammen festgelegt werden.

4.6.1 Umstände für den Widerruf

AlphaSSL CA widerruft ein digitales Zertifikat, wenn:

- Ein Verlust, Diebstahl, eine Veränderung, unautorisierte Offenlegung oder eine andere Gefährdung des privaten Schlüssels seitens des Zertifikatssubjekts vorliegt.
- Der Abonnent des Zertifikats gegen eine wesentliche Verpflichtung gemäß dieser CPS verstoßen hat
- Die Erfüllung der Verpflichtungen einer Person gemäß dieser CPS verzögert oder von einer natürlichen Katastrophe, einem Computer- oder Fernmeldeausfall oder einer anderen Ursache, die die Person nicht zu verantworten hat, verhindert wird, und infolge dessen die Informationen einer anderen Person wesentlich bedroht oder gefährdet werden.
- Eine Veränderung der im Zertifikat des Zertifikatssubjekts enthaltenen Information erfolgte.
- Die kontinuierliche Nutzung des Zertifikats für das AlphaSSL CA Trust-Modell nachteilig ist.

Sollte sich herausstellen, dass die Zertifikatsnutzung für AlphaSSL CA nachteilig ist, berücksichtigt AlphaSSL CA u.a. Folgendes:

- Die Art und Anzahl der eingegangenen Beschwerden
- Die Identität des/der Beschwerdeführer(s)
- Sachdienliche, gültige Rechtsvorschriften
- Antworten des Abonnenten auf die angebliche nachteilige Verwendung

Die AlphaSSL CA beantragt den Widerruf eines Zertifikates umgehend nach Überprüfung der Identität der antragstellenden Partei. Die Überprüfung der Identität kann über Informationselemente erfolgen, die in den Identifikationsdaten enthalten sind, die der Abonnent an AlphaSSL CA eingereicht hat. Auf Anfrage durch eine AlphaSSL CA ergreift AlphaSSL CA umgehend eine Maßnahme, um das Zertifikat zu widerrufen.

Zusätzlich den oben genannten Bedingungen für einen Widerruf, widerruft AlphaSSL ein Zertifikat, das beim Eintritt eines der folgenden Ereignisse ausgestellt wurde:

- Der Abonnent beantragt den Widerruf seines AlphaSSL-Zertifikates
- Der Abonnent zeigt an, dass die ursprüngliche Zertifikatsanfrage nicht autorisiert war und rückwirkend keine Autorisierung erteilt wird
- AlphaSSL CA erhält begründete Beweise, dass der private Schlüssel des Abonnenten (entsprechend dem öffentlichen Schlüssel im Zertifikat) beeinträchtigt oder dass das Zertifikat anderweitig missbraucht wurde
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Abonnent ein Zertifikat für kriminelle Aktivitäten, wie z.B. Phishing-Attacken, Betrug, etc. verwendet
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Abonnent gegen eine seiner wesentlichen Verpflichtungen gemäß dem Bezugsvertrag verstößt
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Gericht oder Vermittler das Recht eines Abonnenten zur Verwendung des im Zertifikat aufgelisteten Domainnamens widerrufen hat oder dass der Abonnent versäumt hat, seinen Domainnamen zu verlängern
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis über eine wesentliche Änderung der im Zertifikat enthaltenen Informationen
- Eine Festlegung im eigenen Ermessen von AlphaSSL CA, dass das Zertifikat nicht gemäß den AlphaSSL-Richtlinien ausgestellt wurde
- Falls AlphaSSL CA beschließt, dass eine der im Zertifikat angezeigten Informationen nicht richtig ist.

- AlphaSSL CA wurde auf illegalem Wege durch den Abonnenten oder Dritte zur Ausstellung des Zertifikats gezwungen.
- AlphaSSL CA stellt aus irgendeinem Grund den Betrieb ein und hat nicht dafür gesorgt, dass eine andere CA einen Widerrufungs-Support für das Zertifikat bereitstellt;
- Der private Schlüssel von AlphaSSL CA für die Ausstellung seiner Zertifikate wurde beeinträchtigt;
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Abonnent als abgewiesene Partei oder unerlaubte Person auf eine schwarze Liste gesetzt wurde oder von einem untersagten Bestimmungsort gemäß dem Gerichtsstand von AlphaSSL CA am Betriebsort agiert.

Nach dem Widerruf sendet die AlphaSSL CA eine Bestätigungs-E-Mail an die antragstellende Partei.

4.7 Aussetzung des Zertifikates

Eine Aussetzung des Zertifikates (den Status des AlphaSSL-Zertifikates als widerrufen festlegen, aber eine Rücksetzung dieser Maßnahme ermöglichen) ist nicht zulässig. Der Widerruf ist endgültig.

4.8 Zertifikatsstatusdienste

Die AlphaSSL CA stellt Dienstleistungen zur Überprüfung des Zertifikatsstatus einschließlich CRLs und entsprechende Web-Schnittstellen zur Verfügung.

CRL
In einer CRL werden alle Widerrufenen Zertifikate während des Bewerbungszeitraums aufgelistet. CRLs für die verschiedenen Produkte stehen unter http://crl.alphassl.com zur Verfügung.

Eine CRL wird alle 3 Stunden ausgestellt.

4.9 Ende des Abonnements

Das Abonnement des Abonnenten endet, wenn ein Zertifikat widerrufen wird, abläuft oder der Dienst beendet wird.

4.10 Problemmeldung und Antwortkapazität bei Zertifikaten

Zusätzlich zur Widerrufung des Zertifikates erteilt AlphaSSL Abonnenten, Relying Parties und anderen Dritten klare Anweisungen für die Meldung von Beschwerden oder vermuteter Gefährdung des privaten Schlüssels, Zertifikatsmissbrauch oder anderen Arten von Betrug, Gefährdung, Missbrauch oder unsachgemäßem Verhalten im Zusammenhang mit Zertifikaten. AlphaSSL CA muss angemessene Bemühungen unternehmen, um eine Möglichkeit bereitstellen, um rund um die Uhr solche Berichte zu bestätigen und zu beantworten.

4.11 Ablauf eines Zertifikates

Abonnenten, die Zertifikate direkt von AlphaSSL erhalten, erhalten eine Vorwarnung bezüglich des schwebenden Ablaufdatums des Zertifikates per E-Mail. Im Allgemeinen werden zwei Zeiträume (30 Tage im Voraus und 7 Tage im Voraus) als am effektivsten erachtet, allerdings kann dies nach Produkttyp schwanken, je nachdem, ob vorhergehende Authentifizierungsinformationen in einem Verlängerungsvorgang verwendet werden können.

5.0 Verwaltung, Bedien- und physische Steuerungen

In diesem Abschnitt werden nichttechnische Sicherheitskontrollen beschrieben, die von AlphaSSL CA zur Durchführung der Funktionen der Schlüsselgenerierung, Subjektauthentifizierung, Zertifikatserstellung, des Zertifikatswiderrufs, der Prüfung und Archivierung verwendet werden.

5.1 Physische Sicherheitskontrollen

Die AlphaSSL CA implementiert physische Kontrollen in ihren eigenen, geleasten oder gemieteten Räumlichkeiten.

Die AlphaSSL CA Infrastruktur ist logisch von jeder anderen Zertifikatsverwaltungsstruktur getrennt, die für andere Zwecke verwendet wird.

Die sicheren Räumlichkeiten der AlphaSSL CA befinden sich in einem für Hochsicherheitsabläufe geeigneten Bereich.

Der physische Zugang wird durch die Implementierung von Mechanismen zur Kontrolle des Zugangs von einem Bereich der Einrichtung in einen anderen oder des Zugangs in Hochsicherheitszonen beschränkt. Dazu zählen CA-Abläufe in einem sicheren, physikalisch überwachten und durch Alarm gesicherten Computerraum, der von einer Zone in die andere verlegt werden soll, um mithilfe eines Tokens und Zugangskontrolllisten durchgeführt zu werden.

Die AlphaSSL CA implementiert Präventiv- und Schutzmaßnahmen, als auch Maßnahmen gegen Brandversuche.

Medien sind sicher gelagert. Backup-Medien werden auch an einem getrennten Standort gelagert, der physisch sicher und von Feuer- und Wasserschäden geschützt ist.

Die AlphaSSL CA implementiert ein partielles Off-Site-Backup.

Die Standorte der AlphaSSL CA umfassen die Infrastruktur, um die AlphaSSL CA-Dienste bereitzustellen. An den AlphaSSL Standorten werden entsprechende Sicherheitskontrollen, einschließlich Zugangskontrollen, Einbruchsmeldung und Überwachung. Der Zugang zu den Standorten ist auf befugtes Personal begrenzt, das auf einer Zugangsliste aufgelistet ist, die der Prüfung unterliegt.

5.2 Verfahrenskontrollen

Die AlphaSSL CA folgt Personal- und Verwaltungspraktiken, die eine angemessene Sicherstellung der Vertrauenswürdigkeit und Kompetenz der Mitarbeiter und der Zufriedenheitsleistung ihrer Pflichten in den Bereichen von Technologien mit elektronischer Signatur bereitstellen.

Die AlphaSSL CA erhält eine unterzeichnete Erklärung von jedem Mitarbeiter über die nicht vorhandenen Interessenskonflikte, Gewährleistung der Vertraulichkeit und den Schutz persönlicher Daten.

Alle Mitarbeiter, die für Hauptverwaltungsabläufe verantwortlich sind, Administratoren, Sicherheitsbeamte und Systemprüfer oder alle anderen Positionen, die solche Abläufe wesentlich beeinflussen, werden in einer vertrauenswürdigen Position als dienlich erachtet.

Die AlphaSSL CA führt eine Erstuntersuchung aller Mitarbeiter durch, die Kandidaten für den Einsatz in vertrauenswürdigen Positionen sind, um einen sinnvollen Versuch zu unternehmen, ihre Zuverlässigkeit und Kompetenz zu bestimmen.

Wenn eine doppelte Kontrolle erforderlich ist, müssen mindestens zwei zuverlässige Mitarbeiter von AlphaSSL CA ihr jeweiliges und getrenntes Wissen einbringen, um mit einem laufenden Vorgang fortfahren zu können.

Die AlphaSSL CA stellt sicher, dass alle Maßnahmen im Hinblick auf AlphaSSL CA auf das System und die Person der CA zurückgeführt werden können, die die Aktion durchgeführt hat.

Die AlphaSSL CA implementiert eine doppelte Kontrolle für kritische CA-Funktionen.

5.3 Persönliche Sicherheitskontrollen

5.3.1 Qualifikationen, Erfahrung, Genehmigungen

Die AlphaSSL CA-Partner führen Kontrollen durch, um den Hintergrund, Qualifikationen und die Erfahrung festzustellen, die für die Ausübung der speziellen Tätigkeit innerhalb des Kompetenzbereichs erforderlich sind. Solche Hintergrundprüfungen sind speziell ausgerichtet. Hintergrundprüfungen beinhalten:

- Durchsuchen der Strafakte
- Überprüfen beruflicher Referenzen
- Bestätigung der vorhergehenden Beschäftigung
- Bestätigung des relevantesten erlangten Bildungsgrades
- Fehldarstellungen des Kandidaten
- Alles Weitere, das als notwendig erachtet wird

5.3.2 Hintergrundprüfungen und Anschreibeverfahren

Die AlphaSSL CA führt die relevanten Prüfungen bei potenziellen Mitarbeitern mittels Statusberichten durch, die von einer zuständigen Behörde, Äußerungen Dritter oder Selbstdeklarationen ausgegeben werden.

5.3.3 Schulungsanforderungen und Verfahren

Die AlphaSSL CA stellt für ihr Personal Schulungen zur Verfügung, um CA- und RA-Funktionen durchzuführen.

5.3.4 Umschulungszeitraum und -verfahren

Regelmäßige Schulungsaktualisierungen können auch durchgeführt werden, um die Kontinuität und Aktualisierungen des Wissens des Personals und der Abläufe festzulegen.

5.3.5 Arbeitsplatzrotation

Nicht zutreffend.

5.3.6 Sanktionen gegen das Personal

AlphaSSL CA sanktioniert Personal für unbefugte Handlungen, unbefugte Nutzung von Kompetenzen und unbefugte Nutzung von Systemen zum Zwecke des Abverlangens von Verantwortung vom Personal eines Teilnehmers, sofern dies unter den Umständen angemessen sein könnte.

5.3.7 Kontrollen unabhängiger Auftragnehmer

Unabhängige Auftragnehmer und ihr Personal unterliegen demselben Datenschutz und denselben Vertraulichkeitsbedingungen wie das Personal von AlphaSSL CA.

5.3.8 Dokumentation für Erstschulung und Umschulung

Die AlphaSSL CA stellt dem Personal verfügbare Dokumentation während der Erstschulung, Umschulung oder anderweitig zur Verfügung.

5.4 Prüfungserfassungsverfahren

Prüfungserfassungsverfahren beinhalten Ereignisprotokollierung und Prüfsysteme, die zum Zwecke der Aufrechterhaltung einer sicheren Umgebung implementiert werden.

AlphaSSL CA implementiert die folgenden Kontrollen:

AlphaSSL CA-Prüfung erfasst Ereignisse, die Folgendes beinhalten, aber nicht beschränkt sind auf:

- Erstellen eines Zertifikats
- Widerruf eines Zertifikats
- Veröffentlichung einer CRL

Buchungskontrolldatensätze umfassen:

- Die Identifizierung des Vorgangs
- Die Daten und Uhrzeit des Vorgangs
- Die Identifizierung des Zertifikates, das im Vorgang enthalten ist
- Die Identifizierung der Person, die den Vorgang ausgeübt hat
- Einen Verweis auf die Anfrage des Vorgangs

Dokumente, die für Prüfungen erforderlich sind, beinhalten:

- Infrastrukturpläne und Beschreibungen
- Physikalische Standortpläne und Beschreibungen
- Konfiguration von Software und Hardware
- Personalzugangslisten

AlphaSSL CA stellt sicher, dass das zuständige Personal Logdateien in regelmäßigen Abständen überprüft und ungewöhnliche Ereignisse erkennt und meldet.

Logdateien und Protokolle werden zur Inspektion vom zuständigen Personal von AlphaSSL CA und ernannten Prüfern archiviert. Die Logdateien sollten durch einen Zugangskontrollmechanismus ordnungsgemäß geschützt sein. Logdateien und Protokolle werden gesichert und müssen auf Anfrage unabhängigen Prüfern zur Verfügung gestellt werden.

Prüfungsereignisse werden nicht protokolliert.

5.5 Datensatzarchivierung

AlphaSSL CA bewahrt Archive in einem abrufbaren Format auf.

AlphaSSL CA gewährleistet die Integrität der physischen Speichermedien und implementiert ordnungsgemäße Kopiermechanismen, um einen Datenverlust zu vermeiden.

Archive sind für autorisiertes Personal von AlphaSSL CA entsprechend zugänglich.

Die AlphaSSL CA bewahrt interne Datensätze der folgenden Positionen auf:

- Alle Zertifikate für einen Zeitraum von mindestens einem Jahr nach Ablauf des Zertifikats
- Protokolle über die Ausstellung von Zertifikaten für einen Zeitraum von mindestens einem Jahr nach Ausstellung eines Zertifikats
- Protokoll des Widerrufs eines Zertifikats für einen Zeitraum von mindestens einem Jahr nach dem Widerruf eines Zertifikats
- CRLs für mindestens ein Jahr nach dem Ablauf oder Widerruf eines Zertifikats
- Support-Dokumente über die Ausstellung von Zertifikaten für einen Zeitraum von einem Jahr nach Ablauf eines Zertifikates. Support-Dokumente können elektronisch gespeichert werden.

5.5.1 Datensatztypen

AlphaSSL CA bewahrt auf zuverlässige Art und Weise Datensätze von digitalen Zertifikaten, Prüfungsdaten, Zertifikatsanwendungsinformationen, Logdateien und Dokumentationen zur Unterstützung von Zertifikatsanwendungen von AlphaSSL CA auf.

5.5.2 Aufbewahrungszeitraum

AlphaSSL CA bewahrt auf zuverlässige Art und Weise Datensätze von Zertifikaten für mindestens ein Jahr auf.

5.5.3 Schutz des Archivs

Folgende Bedingungen gelten für den Schutz von Archiven:
Nur der Datensatzadministrator (Mitarbeiter, der mit der Datensatzaufbewahrung betraut ist) kann das Archiv einsehen:

- Schutz gegen die Modifizierung des Archivs, wie z. B. Speicherung der Daten auf einem einmalig beschreibbaren Medium
- Schutz gegen Löschung des Archivs
- Schutz gegen Verschlechterung des Mediums, auf dem das Archiv gespeichert ist, wie z. B. eine Anforderung, dass Daten regelmäßig auf frische Medien verschoben werden

5.5.4 Archivsammlung

Das Archivsammlungssystem von AlphaSSL CA ist intern.

5.5.5 Verfahren zum Einholen und Überprüfen von Archivinformationen

Um Archivinformationen einzuholen und zu überprüfen, bewahrt AlphaSSL CA Datensätze unter klarer hierarchischer Kontrolle auf.

Die AlphaSSL CA bewahrt Datensätze im elektronischen oder papiergestützten Format auf. Die AlphaSSL CA kann von Abonnenten oder ihren Agenten verlangen, Dokumente als Unterstützung dieser Anforderung entsprechend einzureichen.

Ablagefristen beginnen am Datum des Ablaufs oder Widerrufs. Solche Datensätze können in elektronischem oder papiergestütztem Format oder jedem anderen Format aufbewahrt werden, das AlphaSSL CA als geeignet erachtet.

Die AlphaSSL CA kann gegebenenfalls Datensatzaufbewahrungsbedingungen überprüfen, um die Akkreditierungsprogramme, einschließlich WebTrust für CAs zu erfüllen.

5.6 Vergleich und Disaster Recovery

In einem separaten internen Dokument dokumentiert AlphaSSL CA geltenden Vorfälle, Vergleichsmeldungen und Umschlagsverfahren. Die AlphaSSL CA dokumentiert die verwendeten Recovery-Verfahren, wenn Rechnerressourcen, Software und/oder Daten beschädigt oder vermutlich beschädigt sind.

Die AlphaSSL CA bestimmt die notwendigen Maßnahmen, um die vollständige Wiederherstellung des Dienstes innerhalb eines angemessenen Zeitraums, je nach Art der Störung, im Falle eines Unglücks, beschädigten Servers, Software oder Daten sicherzustellen.

Ein Business-Continuity-Plan wurde implementiert, um die Geschäftskontinuität nach einer natürlich oder sonstigen Katastrophe sicherzustellen. Der maximal zulässige Ausfall beträgt einen Monat.

Vor dem Abschluss ihrer CA-Aktivitäten unternimmt die AlphaSSL CA Schritte, um die folgenden Informationen auf eigene Kosten der AlphaSSL CA an die bezeichnete Organisation zu übertragen:

Alle Informationen, Daten, Dokumente, Aufbewahrungsorte, Archive und Protokolle, die der AlphaSSL CA gehören.

6.0 Technische Sicherheitskontrollen

Die von AlphaSSL CA unternommenen Sicherheitsmaßnahmen zum Schutz ihrer kryptografischen Schlüssel und Aktivierungsdaten sind in den Zertifikatsregeln der AlphaSSL CA Managed Brand Root aufgeführt.

7.0 Zertifikat und CRL-Profile

In diesem Abschnitt werden das Zertifikat und CRL-Format festgelegt.

7.1 Zertifikatsprofil

AlphaSSL Zertifikate entsprechen im Allgemeinen einer (a) ITU-T Empfehlung X.509 (1997): Informationstechnologie - Open Systems Interconnection – Das Verzeichnis: Authentifizierungs-Framework, Juni 1997 und (b) RFC 5280: Internet X.509 Public-Key-Infrastruktur-Zertifikat und CRL-Profil, Mai 2008.

Feld	**Wert oder Wertbeschränkung**
Seriennummer	Einmaliger Wert pro Aussteller-DN
Signaturalgorithmus	Objektbezeichner des zur Unterzeichnung des Zertifikats verwendeten Algorithmus – sha1RSA – gemäß RFC 3279.
Aussteller-DN	AlphaSSL gemeinsam mit der entsprechenden dazwischenliegenden ausstellenden CA hängen von der Beschreibung ab.
Gültig vom	Koordinierte Weltzeit synchronisiert in Königlichen Observatorium von Belgien. Verschlüsselt gemäß RFC 5280.
Gültig bis	Koordinierte Weltzeit synchronisiert in Königlichen Observatorium von Belgien. Verschlüsselt gemäß RFC 5280.
Subjekt-DN	Gemäß 3.1
Subjekt Öffentlicher Schlüssel	Verschlüsselt gemäß RFC 5280
Unterschrift	Generiert und verschlüsselt gemäß RFC 5280

7.1.1 Ausstellerschlüssel-ID

AlphaSSL CA füllt im Allgemeinen die Ausstellerschlüssel-ID-Erweiterung von X.509 Version 3 der Endbenutzer-Bezugsverträge und der Intermediate CA-Zertifikate. Wenn der Zertifikatsaussteller die Inhaberschlüssel-ID-Erweiterung enthält, setzt sich die Ausstellerschlüssel-ID aus 160-bit SHA-1 Hash des öffentlichen Schlüssels der CA, die das Zertifikat ausstellt, zusammen. Andernfalls beinhaltet die Ausstellerschlüssel-ID-Erweiterung den Distinguished Name und die Seriennummer der zugrundeliegenden ausstellenden CA. Das kritische Feld dieser Erweiterung ist auf FALSCH eingestellt.

7.1.2 Authority Information Access

AlphaSSL füllt im Allgemeinen die Ausstellerschlüssel-ID-Erweiterung von X.509 Version 3 der Endbenutzer-Bezugsverträge und gegebenenfalls der Intermediate CA-Zertifikate mit der URL des Standortes, an dem eine Relying Party das Zertifikat der ausstellenden CA erhalten kann. Das kritische Feld dieser Erweiterung ist auf FALSCH eingestellt.

7.1.3 CRL-Verteilungspunkte

Die meisten AlphaSSL X.509 Version 3 Endbenutzer-Bezugsverträge und Intermediate CA-Zertifikate enthalten die CRL-Verteilungspunkte-Erweiterung einschließlich der URL des Standortes, an der eine Relying Party eine CRL erhalten kann, um den Status des CA-Zertifikats zu überprüfen. Das kritische Feld dieser Erweiterung ist auf FALSCH eingestellt.

7.1.4 Inhaberschlüssel-ID

Wenn AlphaSSL X.509 Version 3-Zertifikate mit einer Inhaberschlüssel-ID-Erweiterung füllt, wird die Schlüssel-ID basierend auf dem öffentlichen Schlüssel des Subjekts des Zertifikats gemäß einer der in RFC 5280 beschriebenen Methoden generiert. Wenn diese Erweiterung verwendet wird, wird das kritische Feld dieser Erweiterung auf FALSCH eingestellt.

7.2 CRL-Profil

Die meisten AlphaSSL X.509 Version 3 Endbenutzer-Bezugsverträge und Intermediate CA-Zertifikate enthalten die CRL-Verteilungspunkte-Erweiterung einschließlich der URL des Standortes, an der eine Relying Party eine CRL erhalten kann, um den Status des CA-Zertifikats zu überprüfen. Das kritische Feld dieser Erweiterung ist auf FALSCH eingestellt.

Feld	**Wert oder Wertbeschränkung**
Version	V2 gemäß RFC 5280.
Aussteller-DN	Die Einheit, die die CRL unterzeichnet und ausgestellt hat
Gültigkeitsdatum	Ausstellungsdatum der CRL CRLs sind nach Ausstellung gültig
Nächste Aktualisierung	Datum, an dem die nächste CRL ausgestellt wird
Signaturalgorithmus	Objektbezeichner des zur Unterzeichnung des Zertifikats verwendeten Algorithmus – sha1RSA – gemäß RFC 3279.
Ausstellerschlüssel-ID	160-bit SHA-1 Hash des öffentlichen Schlüssels der CA, die das Zertifikat ausstellt
CRL-Nummer	Eine monoton wachsende Sequenznummer gemäß RFC 5280

8.0 Konformitätsprüfung und andere Bewertung

Die AlphaSSL CA akzeptiert unter bestimmten Bedingungen die Prüfung von Praktiken und Verfahren, die nicht für die Öffentlichkeit zugänglich sind. Die AlphaSSL CA berücksichtigt und beurteilt des Weiteren die Ergebnisse solcher Prüfungen vor deren möglicher Implementierung.

Nach ihrer eigenen Einwilligung hinsichtlich des Umfangs und des Inhalts akzeptiert die AlphaSSL CA Konformitätsprüfungen, um sicherzustellen, dass sie Anforderungen, Standards, Verfahren und Dienstebenen gemäß dieser CPS und Akkreditierungsmodelle erfüllt, mit denen sie sich öffentlich als konform erklärt.

8.1 Konformitätsprüfung und andere Bewertung

AlphaSSL CA erfüllt gegenwärtig die Anforderungen des Akkreditierungsprogramms für CAs, das als WebTrust bekannt ist.

AlphaSSL muss außerdem jährlich die Akkreditierung durch qualifizierte Wirtschaftsprüfer gemäß dem WebTrust-Programm für CAs ersuchen.

Informationen über die Konformität von AlphaSSL mit den Anforderungen jedes anderen Akkreditierungsprogramms können direkt bei der Organisation eines solchen Akkreditierungsprogramms eingeholt werden.

8.1.1 Bedingungen des Prüfprozesses

Um die Prüfungen durchzuführen, gibt es einen unabhängigen Wirtschaftsprüfer, der in keiner Weise direkt oder indirekt mit AlphaSSL CA in Verbindung steht noch Interessenkonflikten diesbezüglich unterliegt.

Eine Prüfung erfolgt in Bereichen, die Folgendes beinhalten, aber nicht beschränkt sind auf:
Konformität der AlphaSSL CA Betriebsabläufe und Prinzipien mit den in der CPS definierten Verfahren und Dienstebenen.

- Verwaltung der Infrastruktur, die CA-Dienste implementiert
- Verwaltung der physikalischen Standort-Infrastruktur
- Einhaltung des CPS
- Einhaltung geltender Gesetze
- Durchsetzung vereinbarten Dienstebenen
- Überprüfung von Protokollen, Logs, relevanten Dokumenten, usw.
- Ursache für jedes Versäumnis, die obigen Bedingungen zu erfüllen

Im Hinblick auf Konformitätsprüfungen übernimmt AlphaSSL CA die Verantwortung für die Leistung aller Subunternehmer, die für die Durchführung von Zertifizierungsabläufen, einschließlich den im unteren Abschnitt beschriebenen, eingesetzt werden.

8.1.1.1 Geschäftspartnerschaften

Um besser auf die verschiedenen Zertifizierungsanforderungen der verteilten Grundgesamtheit von eCommerce-Dienstanbietern und Benutzern zu reagieren, kann AlphaSSL CA mit sorgfältig ausgewählten Geschäftspartnern kooperieren, um bestimmte Dienste im Zusammenhang mit PKI, einschließlich Zertifizierung und Registrierung, zu erbringen. AlphaSSL CA kann Teilbereiche seiner zu erbringenden Dienste ganz oder teilweise ausgliedern. Ungeachtet des Partners oder Agenten, der zur Verwaltung bestimmter Teile des Zertifikatslebenszyklus oder der Abläufe ausgewählt wurde, bleibt AlphaSSL CA letztendlich für den gesamten Prozess verantwortlich. AlphaSSL CA stellt sicher, dass Konformitätsprüfungen auch für solche ausgegliederten Dienste gelten. AlphaSSL CA begrenzt seine Verantwortung hierfür gemäß den Bedingungen in diesem CPS.

9.0 Andere geschäftliche und rechtliche Fragen

Bestimmte rechtliche Bedingungen gelten laut Beschreibung in diesem Abschnitt für die Ausstellung von AlphaSSL CA-Zertifikaten gemäß diesem CPS.

9.1 Gebühren

Die Ausstellung und Verwaltung von AlphaSSL CA-Zertifikaten unterliegt den Gebühren, die auf der Website von AlphaSSL CA unter www.alphassl.com oder über angefragte Angebote angegeben werden.

9.1.1 Rückerstattung

AlphaSSL CA akzeptiert schriftliche Rückerstattungsanfragen. Rückerstattungsanfragen müssen sorgfältig begründet und an die Rechtsabteilung von AlphaSSL CA gerichtet werden. AlphaSSL CA behält sich das Recht vor, Rückerstattungen zuzustimmen oder zu gewähren.

9.2 Finanzielle Verantwortung

AlphaSSL CA hat ausreichend Ressourcen, um die erkannten Verpflichtungen gemäß dieser CPS zu erfüllen. Die AlphaSSL CA stellt diesen Dienst „wie vorhanden“ zur Verfügung.

9.3 Vertraulichkeit von Geschäftsinformationen

Die AlphaSSL CA befolgt Datenschutzbestimmungen und Vertraulichkeitsregeln, die in der AlphaSSL CPS beschrieben sind. Vertrauliche Informationen beinhalten:

- Alle persönlich identifizierbaren, außer den in einem Zertifikat enthaltenen Informationen über Abonnenten
- Grund für den Widerruf eines Zertifikats, außer dem, der in veröffentlichten Zertifikatsstatusinformationen enthalten ist
- Protokolle
- Korrespondenz im Zusammenhang mit CA-Diensten
- CA private Schlüssel

Bei den folgenden Positionen handelt es sich nicht um vertrauliche Informationen:

- Zertifikat und dessen Inhalt
- Status eines Zertifikats

AlphaSSL CA gibt weder vertrauliche Informationen frei und ist auch nicht verpflichtet, vertrauliche Informationen ohne eine authentifizierte und berechtigte Anfrage vertrauliche Informationen freizugeben, in denen Folgendes festgelegt ist:

- Die Partei, der die AlphaSSL CA eine Pflicht schuldet, um Informationen vertraulich zu halten, ist die Partei, die solche Informationen anfragt.
- Ein Gerichtsbeschluss

Die AlphaSSL CA kann für die Bearbeitung solcher Offenlegungen eine Verwaltungsgebühr berechnen.

Parteien, die vertrauliche Informationen anfragen und erhalten, erhalten die Genehmigung, vorausgesetzt, dass sie diese für die erforderlichen Zwecke einsetzen, diese gegen Gefährdungen sichern und es unterlassen, sie zu verwenden oder an Dritte offenzulegen.

9.3.1 Offenlegungsbedingungen

Nicht vertrauliche Informationen können jedem Abonnenten und jeder Relying Party unter den folgenden Bedingungen offengelegt werden:
Nur ein einziges Zertifikat wird pro Anfrage durch den Abonnenten oder die Relying Party ausgestellt.
Der Status eines einzigen Zertifikats wird auf Anfrage durch einen Abonnenten oder eine Relying Party bereitgestellt.
Abonnenten können die Informationen konsultieren, die die CA über sie besitzt.

Vertrauliche Informationen dürfen weder an Abonnenten noch Relying Parties offengelegt werden. Die AlphaSSL CA steuert ordnungsgemäß die Offenlegung von Informationen an das CA-Personal.

Um Informationen unter Bezugnahme einzubeziehen, kann die AlphaSSL CA computer- und textgestützte Hinweise verwenden, die URLs, usw. enthalten.

9.4 Schutz persönlicher Daten

AlphaSSL CA verfügt über eine interne Richtlinie zum Schutz persönlicher Daten des Antragstellers, der ein AlphaSSL-Zertifikat beantragt.

9.5 Rechte am geistigen Eigentum

Die AlphaSSL CA besitzt und reserviert alle Rechte am geistigen Eigentum im Zusammenhang mit Ihren Datenbanken, Webseiten, AlphaSSL-Zertifikaten und jeder anderen Veröffentlichung, die von AlphaSSL CA stamm, einschließlich diesem CPS.

Die Distinguished Names, die in der AlphaSSL CA verwendet werden, bleiben ausschließliches Eigentum von AlphaSSL, die diese Rechte durchsetzt.

Zertifikate sind und bleiben Eigentum der AlphaSSL CA. Die AlphaSSL CA erlaubt die Vervielfältigung und Verteilung von Zertifikaten auf einer exklusiven, gebührenfreien Basis, vorausgesetzt, dass sie vollständig vervielfältigt und verteilt werden, außer dass Zertifikate nicht an einem öffentlich zugänglichen Aufbewahrungsort oder Verzeichnis ohne die ausdrückliche schriftliche Genehmigung von AlphaSSL CA veröffentlicht werden. Der Umfang dieser Beschränkung dient auch dazu, Abonnenten gegen eine unbefugte Wiederveröffentlichung ihrer persönlichen Daten, die in einem Zertifikat gespeichert sind, zu schützen.

Die AlphaSSL CA besitzt und reserviert alle Rechtem am geistigen Eigentum im Zusammenhang mit ihren eigenen Produkten und Diensten, die nicht ausdrücklich auf eine andere Partei übertragen oder an diese freigegeben wurden.

9.6 Darstellungen und Gewährleistungen

Die AlphaSSL CA verwendet diese CPS und einen Bezugsvertrag, um rechtliche Nutzungsbedingungen von AlphaSSL CA-Zertifikaten an Abonnenten und Relying Parties zu übertragen.

Teilnehmer, die Darstellungen und Gewährleistungen übernehmen können, umfassen je nach Bedarf AlphaSSL CA, Abonnenten, Relying Parties und alle anderen Teilnehmer.

Alle Parteien der AlphaSSL-Domain, einschließlich der AlphaSSL CA und Abonnenten, garantieren die Integrität ihrer jeweiligen privaten Schlüssel. Wenn eine solche Partei vermutet, dass ein privater Schlüssel beschädigt wurde, wird sie umgehend AlphaSSL CA benachrichtigen.

9.6.1 Verpflichtungen des Abonnenten

- Sofern in dieser CPS nicht anders angegeben, sind Abonnenten verantwortlich für die Kenntnis und gegebenenfalls die Inanspruchnahme einer Schulung zur Verwendung digitaler Zertifikate
- Sichere Erstellung ihres privaten-öffentlichen Schlüsselpaares, Nutzung eines zuverlässigen Systems
- Bereitstellung korrekter und genauer Informationen in ihren Kommunikationen mit AlphaSSL CA
- Sicherstellung, dass der an die AlphaSSL CA eingereichte öffentliche Schlüssel dem verwendeten privaten Schlüssel entspricht
- Annahme aller Konditionen und Bedingungen in dem AlphaSSL CA CPS und der verbundenen Richtlinien, die am AlphaSSL CA-Aufbewahrungsort veröffentlicht sind.
- Absehen von einer Verfälschung mit einem AlphaSSL-Zertifikat
- Verwendung von AlphaSSL-Zertifikaten für rechtliche und zulässige Zwecke gemäß diesem CPS
- Benachrichtigung von AlphaSSL CA über jegliche Änderungen der eingereichten Informationen
- Einstellen der Nutzung eines AlphaSSL-Zertifikats, wenn die enthaltenen Informationen ungültig werden
- Einstellen der Nutzung eines AlphaSSL-Zertifikats, sobald es ungültig wird
- Löschen eines ungültigen AlphaSSL-Zertifikats von jeglichen Anwendungen und/oder Geräten, auf denen es installiert wurde
- Verwendung eines AlphaSSL-Zertifikats, wenn dies unter den gegebenen Umständen sinnvoll ist
- Verhindern der Gefährdung, des Verlustes, der Offenlegung, Modifizierung oder anderweitig unbefugten Nutzung ihrer privaten Schlüssel
- Für alle Handlungen oder Unterlassungen von Partnern und Agenten, die Abonnenten zum Generieren, Erhalten, Hinterlegen oder Zerstören von privaten Schlüsseln verwenden
- Absehen von der Einreichung jeglicher Materialien an AlphaSSL CA oder ein anderes AlphaSSL CA-Verzeichnis, die Äußerungen enthalten, die gegen ein Gesetz oder die Rechte einer Partei verstoßen
- Beantragen des Widerruf eines Zertifikats im Falle eines Vorfalls stellen, der die Integrität eines AlphaSSL CA-Zertifikats wesentlich beeinträchtigt
- Umgehende Benachrichtigung der entsprechenden RA, wenn ein Abonnent die Gefährdung eines privaten Schlüssels bemerkt oder vermutet

AlphaSSL CA stellt einen Bezugsvertrag zur Verfügung, um sicherzustellen, dass der Abonnent sich an die folgenden Bedingungen hält:

- Einreichen genauer und vollständiger Informationen an AlphaSSL CA gemäß den Anforderungen dieses CPS, insbesondere im Hinblick auf die Registrierung
- Verwendung des Schlüsselpaares ausschließlich mit diesem CPS
- Mit angemessener Sorgfalt vorgehen, um die unbefugte Nutzung des privaten Schlüssels zu verhindern
- Laut dem AlphaSSL CA-Modells generiert der Abonnent immer seine eigenen Schlüssel. In diesem Fall gelten auch folgende Bedingungen:
    - Verwenden einer Schlüssellänge und eines Algorithmus, der für den Zweck elektronischer Signaturen als geeignet gilt
    - Unverzügliche Benachrichtigung von AlphaSSL CA, falls eines der folgenden Ereignisse bis zum Ende der im Zertifikat angezeigten Gültigkeitsdauer eintritt:
    - Der private Schlüssel des Abonnenten nicht verloren, gestohlen, möglicherweise gefährdet ist; oder
    - Kontrolle über den privaten Schlüssel der Abonnenten, der aufgrund einer Gefährdung der Aktivierungsdaten (z. B. PIN-Code) verloren gegangen ist
    - Ungenauigkeit oder Änderungen des Zertifikatsinhalts, über die der Abonnent benachrichtigt wird

9.6.2 Verpflichtungen der Relying Party

Eine Partei, die sich auf ein AlphaSSL-Zertifikat verlässt, muss:

- Technisch imstande sein, digitale Zertifikate zu nutzen
- Eine Mitteilung der AlphaSSL CA und die verbundenen Bedingungen für Relying Parties erhalten
- Ein AlphaSSL-Zertifikat durch die Verwendung von Zertifikatsstatusinformationen (z. B. eine CRL), die von AlphaSSL veröffentlicht werden, überprüfen
- Einem AlphaSSL CA-Zertifikat nur dann vertrauen, wenn alle auf einem solchen Zertifikat angegebenen Informationen auf Richtigkeit und Aktualität überprüft werden können
- Sich auf ein AlphaSSL-Zertifikat verlassen, nur wenn dies unter den gegebenen Umständen sinnvoll ist
- AlphaSSL CA ungehend benachrichtigen, wenn die Relying Party bemerkt oder vermutet, dass ein privater Schlüssel gefährdet ist

Wenn es darum geht, sich vernünftig auf ein Zertifikat zu verlassen, hat die Relying Party folgende Verpflichtungen:

- Überprüfen der Gültigkeit oder Widerruf des Zertifikats mithilfe aktueller Widerrufsstatusinformationen, die der Relying Party angegeben werden
- Berücksichtigen aller Einschränkungen bezüglich der Verwendung des Zertifikats, die der Relying Party entweder im Zertifikat oder in dieser CPS angegeben wird
- Ergreifen aller anderen Vorsichtsmaßnahmen, die im Bezugsvertrag, im AlphaSSL-Zertifikat als auch in anderen Richtlinien oder Bedingungen und Konditionen vorgeschrieben sind, die im Anwendungskontext, in dem ein Zertifikat verwendet werden kann, zur Verfügung gestellt werden

Relying Parties müssen jederzeit festlegen, dass es sinnvoll ist, sich gemäß den Umständen auf ein Zertifikat zu verlassen, unter Berücksichtigung der Umstände, wie z. B. den speziellen Anwendungskontext, in dem ein Zertifikat verwendet wird.

Relying Parties werden hiermit benachrichtigt, dass die in dieser CPS aufgeführten Bedingungen bindend sind, sobald sie eine AlphaSSL CA Ressource konsultieren, mit dem Ziel, Vertrauen aufzubauen und ein Zertifikat zu überprüfen.

9.6.3 Haftung des Abonnenten gegenüber der Relying Parties

Ohne die Einschränkung anderer Verpflichtungen des Abonnenten, die anderer Stelle in dieser CPS genannt sind, haften Abonnenten für alle Falschdarstellungen, die Sie in Zertifikaten gegenüber Dritten machen, die sich auf die hierin enthaltenen Informationen verlassen, abzusehen.

9.6.4 AlphaSSL CA-Bedingungen für Aufbewahrungsort und Webseite

Parteien, einschließlich Abonnenten und Relying Parties, die auf den AlphaSSL Ca-Aufbewahrungsort und die Webseite zugreifen, stimmen den Bestimmungen dieser CPS und allen anderen Nutzungsbedingungen zu, die die AlphaSSL zur Verfügung stellt. Parteien zeigen ihre Akzeptanz der Nutzungsbedingungen der CPS, indem sie eine Anfrage hinsichtlich des Status eines digitalen Zertifikats stellen oder auf irgendeine Weise solche bereitgestellten Informationen oder Dienste nutzen oder sich darauf verlassen. Die AlphaSSL CA-Aufbewahrungsorte beinhalten oder enthalten:

- Informationen, die infolge der Suche nach einem digitalen Zertifikat bereitgestellt werden
- Informationen, um den Status eines AlphaSSL-Zertifikats zu überprüfen
- Informationen, die auf der AlphaSSL CA Webseite veröffentlicht werden
- Alle anderen Dienste, die AlphaSSL CA über ihre Webseite bewerben oder bereitstellen kann

Wenn ein Aufbewahrungsort die Gefährdung eines privaten Schlüssels erkennt oder vermutet, wird er AlphaSSL CA umgehend benachrichtigen.

AlphaSSL CA behält während eines Anwendungszeitraums und für maximal fünf Jahre nach Ablauf oder Widerruf des Zertifikates einen Zertifikats-Aufbewahrungsort.

9.6.4.1 Vertrauen auf eigene Gefahr

Es liegt im eigenen Ermessen der Parteien, auf Informationen, die in den Aufbewahrungsorten und Webseiten der AlphaSSL CA abgelegt sind, zuzugreifen, um auf die hierin enthaltenen Informationen zuzugreifen und sich darauf zu verlassen. Die Parteien bestätigen, dass sie entsprechende Informationen erhalten haben, um zu entscheiden, ob sie sich auf die in einem Zertifikat enthaltenen Informationen verlassen können. Die AlphaSSL CA ergreift die notwendigen Schritte für die Aktualisierung ihrer Datensätze und Verzeichnisse betreffend den Status der Zertifikate und stellt dahingehend Warnungen aus. Die Nichteinhaltung der Nutzungsbedingungen der AlphaSSL Aufbewahrungsorte und der Webseite kann zur Kündigung der Beziehung zwischen der AlphaSSL CA und der Partei führen.

9.6.4.2 Genauigkeit von Informationen

AlphaSSL CA übernimmt jede Anstrengung, um sicherzustellen, dass Parteien, die auf Ihre Aufbewahrungsorte zugreifen, genaue, aktualisierte und korrekte Informationen erhalten. Die AlphaSSL CA kann allerdings keine Haftung akzeptieren, die über die in dieser CPS und der AlphaSSL CA Versicherungspolice festgelegten Grenzen hinausgehen.

9.6.5 Verpflichtungen der AlphaSSL CA

AlphaSSL CA verspricht:

- Dieses CPS und deren Änderungen laut Repository unter http://www.alphassl.com/repository einzuhalten
- Infrastruktur und Zertifizierungsdienste, einschließlich der Einrichtung und des Betriebs des AlphaSSL CA-Aufbewahrungsortes und der Webseite für den Betrieb öffentlicher Zertifikatsverwaltungsdienste bereitzustellen
- Trust-Mechanismen, einschließlich eines Schlüsselgenerierungsmechanismus, Schlüsselschutz und geheimer Verteilungsverfahren hinsichtlich der eigenen Infrastruktur bereitzustellen
- Umgehende Mitteilung im Falle einer Gefährdung des eigenen privaten Schlüssels bereitzustellen
- Anwendungsverfahren für die verschiedenen Arten von Zertifikaten, die öffentlich zur Verfügung gestellt werden, bereitzustellen und zu überprüfen
- Elektronische Zertifikate gemäß diesem CPS auszustellen und die hierin aufgeführten Verpflichtungen zu erfüllen
- Zertifikate, die gemäß diesem CPS ausgestellt wurden, zu widerrufen
- Akzeptierte Zertifikate gemäß dieser CPS zu veröffentlichen
- Unterstützung für Abonnenten und Relying Parties gemäß Beschreibung in dieser CPS zur Verfügung zu stellen
- Den Ablauf und die Verlängerung von Zertifikaten gemäß diesem CPS vorzusehen
- CRLs aller widerrufenen Zertifikate gemäß diesem CPS regelmäßig zu veröffentlichen
- Angemessene Dienstebenen gemäß einer Leistungsvereinbarung bereitzustellen
- Relying Parties über den Zertifikatswiderruf durch Veröffentlichen von CRLs am AlphaSSL CA-Aufbewahrungsort zu benachrichtigen

Die Haftung von AlphaSSL CA gemäß dem oben genannten Artikel für erwiesene Schäden, die direkt durch die oben aufgelisteten Ereignisse verursacht wurden, ist auf 1 Dollar für jedes einzelne Zertifikat beschränkt. Diese Grenze kann von AlphaSSL CA überprüft werden. AlphaSSL CA kann eine zusätzliche Versicherungsabdeckung gegen Gefahren ersuchen, die von der Richtigkeit der in einem Zertifikat enthaltenen Informationen hervorgehen.

Soweit dies gesetzliche erlaubt ist, kann die AlphaSSL CA für Folgendes nicht haftbar gemacht werden:

- Jede Verwendung von Zertifikaten, die nicht in diesem CPS festgelegt ist
- Falsifizierung von Transaktionen
- Unsachgemäße Nutzung oder Konfiguration von Anlagen, die nicht unter der Verantwortung der CA betrieben und in einer Transaktion, in der Zertifikate enthalten sind, verwendet werden
- Gefährdung von privaten Schlüsseln im Zusammenhang mit den Zertifikaten
- Verlust, Preisgabe oder Missbrauch von PIN-Code(s) usw., die dem Schutz privater Schlüssel im Zusammenhang mit den Zertifikaten dienen
- Die Einreichung fehlerhafter oder unvollständiger Daten, einschließlich Identifikationsdaten, Seriennummern und öffentlichen Schlüsselwerten
- Fehlerhafte oder unvollständige Anfragen für Abläufe auf Zertifikaten
- Höhere Gewalt
- Die Verwendung von Zertifikaten
- Die Verwendung von öffentlichen oder privaten Schlüsseln von quer-zertifizierten (nicht untergeordneten) CAs und ihren Relying Parties

AlphaSSL CA bestätigt, dass gemäß diesem CPS keine weiteren Verpflichtungen bestehen.

9.6.6 Informationen, die als Referenz in ein digitales Zertifikat eingebunden sind

AlphaSSL CA schließt folgende Informationen als Referenz in jedes ausgestellte digitale Zertifikat ein:

- Bedingungen und Konditionen der AlphaSSL CA CPS
- Jede andere geltende Zertifikatsrichtlinie, die auf einem ausgestellten AlphaSSL-Zertifikat angegeben ist
- Die verpflichtenden Elemente des Standards X.509.
- Alle nicht verpflichtenden aber individuellen Elemente des Standards X.509.
- Inhalt und Erweiterungen und verbesserte Kennzeichnung, die in einem Zertifikat nicht vollständig ausgedrückt werden
- Alle anderen Informationen, die in einem Feld eines Zertifikats als feststehend angegeben werden

9.6.7 Hinweise, die als Referenz einbezogen werden

Um Informationen als Referenz einzubeziehen, verwendet AlphaSSL computer- und textgestützte Hinweise. AlphaSSL kann URLs, OIDs, usw. verwenden.

9.7 Haftungsausschlüsse

In diesem Abschnitt sind Haftungshinweise ausdrücklicher Zusicherungen eingeschlossen.

9.7.1 Beschränkungen für andere Gewährleistungen

AlphaSSL CA übernimmt keine Gewährleistung für:

- Die Genauigkeit eines ungeprüften Teils von in Zertifikaten enthaltenen Informationen
- Die Genauigkeit, Authentizität, Vollständigkeit oder Eignung von Informationen, die in kostenlosen, Test- oder Demo-Zertifikaten enthalten sind

9.7.2 Ausschluss bestimmter Schadenselemente

In keinem Fall übernimmt die AlphaSSL CA die Haftung für:

- Jeglichen Gewinnausfall
- Jeglichen Datenverlust

- Alle indirekten, Folgeschäden oder Schadensersatzleistungen, die aus oder in Verbindung mit der Verwendung, Erbringung, Lizenz und Leistung oder Nicht-Leistung von Zertifikaten oder digitalen Signaturen entstehen
- Alle Transaktionen oder Dienste, die im Rahmen dieser CPS angeboten werden
- Alle anderen Schäden, außer denen durch Vertrauen auf die überprüften Informationen in einem Zertifikat, mit Ausnahme der Informationen, die in kostenlosen, Test- oder Demo-Zertifikaten enthalten sind
- Jede Verbindlichkeit, die in einem beliebigen Fall eingetreten ist, wenn der Fehler in solchen überprüften Informationen auf Betrug oder vorsätzliches Fehlverhalten des Antragstellers zurückzuführen ist

9.8 Haftungsbegrenzungen

Die gesamte Haftung von AlphaSSL ist gegenüber dem Abonnenten auf maximal 1000 USD begrenzt.

9.9 Entschädigungen

In diesem Abschnitt sind die geltenden Entschädigungen aufgeführt.

Soweit gesetzlich erlaubt stimmt der Abonnent zu, die AlphaSSL CA zu schützen und schadlos zu halten vor Handlungen und Unterlassungen, die zu einem Haftungsanspruch, Verlust oder Schaden und allen Verfahren und Ausgaben jeglicher Art, einschließlich angemessenen Anwaltskosten, führen, die für AlphaSSL infolge folgender Versäumnisse anfallen:

- Schutz des privaten Schlüssels des Abonnenten,
- Verwendung eines zuverlässigen Systems, wie vorgeschrieben
- Treffen der Vorsichtsmaßnahmen, die notwendig sind, um Gefährdung, Verlust, Offenlegung, Änderung oder unbefugte Nutzung des privaten Schlüssels des Abonnenten zu verhindern
- Beachten der Integrität der verwalteten Branded Root

9.10 Laufzeit und Kündigung

Dieses CPS bleibt gültig, solange nichts Gegenteiliges von AlphaSSL CA auf der Website oder am Aufbewahrungsort mitgeteilt wird.

Angekündigte Änderungen werden in jeder angezeigten Version entsprechend gekennzeichnet. Änderungen werden 30 Tage nach Veröffentlichungen gültig.

9.11 Individuelle Hinweise und Kommunikationen mit Teilnehmern

Die AlphaSSL CA akzeptiert Ankündigungen im Zusammenhang mit diesem CPS mittels digital unterzeichneter Nachrichten oder in Papierform. Nach Eingang einer gültigen, digital unterzeichneten Eingangsbestätigung von AlphaSSL CA erachtet der Absender seine Ankündigung als rechtskräftig. Der Absender muss eine solche Bestätigung innerhalb von zwanzig (20) Werktagen erhalten, jede andere schriftliche Ankündigung muss dann in Papierform per Kurierdienst, der die Lieferung bestätigt, oder per Einschreiben, mit im Voraus bezahltem Porto, Einschreiben mit Rückschein an folgende Adresse versendet werden. Einzelne Mitteilungen, die an AlphaSSL CA gemacht werden, müssen an legal@AlphaSSL.com oder per Post an die AlphaSSL CA an die in der Einleitung dieses Dokuments genannte Adresse gesendet werden.

9.12 Eigentum

AlphaSSL CA wird betrieben und ist Eigentum von GlobalSign NV/SA und sollte als eigene Marke von GlobalSign betrachtet werden. Die Brand Root ist die GlobalSign Brand Root CA (die gemäß den in der GlobalSign Zertifikatsrichtlinie beschriebenen und unter www.globalsign.com/repository veröffentlichten Praktiken verwaltet wird). Dieses CPS gilt nicht für die Brand Root Richtlinien, sondern beruht ausschließlich auf den in der GlobalSign Zertifikatsrichtlinie beschrieben Praktiken.

Dieses CPS ist endgültig und verbindlich zwischen GlobalSign NV/SA (Betreiber und Eigentümer der AlphaSSL CA), einem öffentlich-rechtlichen Unternehmen, mit eingetragenem Sitz in Ubicenter, Philipssite 5, B-3001 Leuven, Ust-ID-Nr. BE 0459.134.256 und registriert im Handelsregister unter der Nummer BE 0.459.134.256 RPR Leuven, (hiernach genannt „AlphaSSL“)

und

dem Abonnenten und/oder den Relying Parties, die die von AlphaSSL CA-Zertifizierungsdienste nutzen, sich darauf verlassen oder versuchen zu verlassen.

Für Abonnenten wird dieses CPS durch Annahme eines Subscriber Agreement wirksam und bindend. Für Relying Parties wird diese CPS bindend, indem eine zertifikatsbezogene Anfrage auf einem AlphaSSL-Zertifikat an ein AlphaSSL-Verzeichnis gesendet wird. Der Bezugsvertrag verwirkt die Zustimmung der Relying Party im Hinblick auf die Annahme der in diesem CPS dargelegten Bedingungen.

9.13 Änderungen

Änderungen dieses CPS werden durch eine entsprechende Nummerierung angezeigt.

9.14 Schlichtungsverfahren

Bevor auf jegliche Schlichtungsverfahren, einschließlich einer Beurteilung oder jeglicher Art von alternative Streitbeilegungsmechanismen (einschließlich Mini-Prozessen, Schiedsgerichtsbarkeit, verbindliche fachkundige Beratung, Kooperationsüberwachung und normale fachkundige Beratung) zurückgegriffen wird, stimmen die Parteien zu, AlphaSSL CA über die Streitigkeit zu informieren, in der Absicht, eine Lösung des Rechtsstreits herbeizuführen.

Nach Eingang einer Anfechtungsmitteilung beruft AlphaSSL CA einen Streitausschuss zusammen, der die Geschäftsleitung von AlphaSSL CA darüber berät, wie mit dem Rechtsstreit fortzufahren ist. Der Streitausschuss kommt innerhalb von zwanzig (20) Werktagen ab dem Eingang einer Anfechtungsmitteilung zusammen. Der Streitausschuss setzt sich zusammen aus einem Rechtsberater, einem Datenschutzbeauftragten, einem Mitglied der AlphaSSL CA Geschäftsführung und einem Sicherheitsbeamten. Der Rechtsberater oder Datenschutzbeauftragte leiten das Treffen. In seinen Beschlüssen schlägt der Streitausschuss der Geschäftsleitung von AlphaSSL CA eine Schlichtung vor. Die Geschäftsleitung von AlphaSSL CA kann im Nachhinein die vorgeschlagene Schlichtung der restlichen Partei mitteilen.

9.15 Anwendbares Recht

Dieses CPS wird gemäß dem belgischen Recht bestimmt, ausgelegt und interpretiert. Diese Rechtswahl erfolgte, um eine einheitliche Auslegung dieses CPS ungeachtet des Wohnsitzes oder Verwendungsortes von AlphaSSL-Zertifikaten oder anderen Produkten und Diensten, sicherzustellen. Das belgische Recht gilt für alle Geschäfts- oder Vertragsbeziehungen von AlphaSSL CA, in denen dieses CPS implizit oder explizit im Zusammenhang mit AlphaSSL CA Produkte und Diensten gilt oder angegeben wird, bei denen die AlphaSSL CA als Anbieter, Lieferant, Empfänger oder anderweitig agiert.

9.16 Konformität mit geltendem Recht

AlphaSSL CA entspricht dem geltenden belgischen Recht.

9.17 Erzwungene Angriffe

AlphaSSL unterliegt der belgischen Gerichtsbarkeit und Rahmenbedingungen. Die Infrastruktur von AlphaSSL CA befindet sich in Belgien und die RA-Infrastruktur befindet sich in Belgien und Japan. Verkaufsbüros und/oder strategische Partner von AlphaSSL haben keinen Zugriff auf die Infrastruktur von AlphaSSL CA. AlphaSSL CA wird jede angemessene Rechtsverteidigung gegen Nötigung von Dritten in Anspruch nehmen, um Zertifikate gegen das CPS auszustellen.

9.18 Sonstige Bestimmungen

9.18.1 Überleben

Die im Abschnitt „Rechtliche Bedingungen“ enthaltenen Verpflichtungen und Einschränkungen überdauern die Beendigung dieses CPS.

9.18.2 Trennbarkeit

Wenn eine Bestimmung dieser CPS, einschließlich der Beschränkung von Haftungsklauseln als ungültig oder nicht durchsetzbar befunden wird, sollte der Rest dieses CPS so ausgelegt werden, dass die ursprüngliche Absicht der Parteien herbeigeführt wird.

9.18.3 Andere Bestimmungen

Dieses CPS ist für ausdrückliche, implizite oder offensichtliche Nachfolger, Vollstrecker, Erben, Vertreter, Administratoren
und Rechtsnachfolger der Parteien verbindlich, für die diese CP/CPS gilt. Die in diesem CPS genau aufgeführten Rechte und Verpflichtungen sind von den Parteien durch Ausübung des Gesetzes übertragbar
(einschließlich infolge einer Zusammenlegung oder Übertragung einer Mehrheitsbeteiligung bei der Wahl der Sicherheiten) oder anderweitig, vorausgesetzt, dass eine solche Zuordnung im Einklang mit diesen CPS-Artikeln zur Kündigung oder Beendigung der Geschäftsabläufe erfolgt, und vorausgesetzt, dass eine solche Zuordnung keine Novation anderer Schulden oder Verpflichtungen beeinträchtigt, die die abtretende Partei den anderen Parteien zum Zeitpunkt einer solchen Zuordnung schuldet.

.

10.0 Liste der Definitionen

AKZEPTIEREN (EINES ZERTIFIKATES)
Genehmigen eines digitalen Zertifikats durch einen Zertifikats-Antragsteller innerhalb eines Transaktionsrahmens.

AKKREDITIERUNG
Eine formelle Erklärung durch eine Genehmigungsbehörde, dass eine bestimmte Funktion/Einheit bestimmte formelle Anforderungen erfüllt

ANTRAG AUF EIN ZERTIFIKAT
Eine Anfrage, die von einem Antragsteller auf ein Zertifikat an eine CA gestellt wird, um ein digitales Zertifikat auszustellen

ANBIETER EINER ANWENDUNGSSOFTWARE: Ein Entwickler von Internet-Browser-Software oder anderer Software, die Zertifikate anzeigt und verwendet und Root-Zertifikate verbreitet, wie z. B. KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA und Red Hat, Inc.

VERSICHERUNGEN
Eine Reihe von Äußerungen oder Verhalten, die auf die Übermittlung einer allgemeinen Ansicht abzielt.

PRÜFUNG
Verfahren, das zur Überprüfung der Konformität mit formellen Kriterien oder Kontrollen verwendet wird.

AUTHENTIFIKATION
Ein Prozess, der zur Bestätigung der Identität einer Person oder als Beweis der Integrität bestimmter Informationen verwendet wird, um sie in den richtigen Kontext zu setzen und eine solche Beziehung zu überprüfen.

AUTORISIERUNG
Gewährend von Rechten.

VERFÜGBARKEIT
Das Maß an Zugreifbarkeit auf Informationen oder Ressourcen.

HARDWARE-MODUL
Das gesamte System des Hardware-Moduls, das zur Aufbewahrung der Zertifikate und sicheren Generierung eines Schlüsselpaares verwendet wird

VERBINDLICH
Eine Aussage durch eine RA über die Beziehung zwischen einer genannten Einheit und ihrem öffentlichen Schlüssel.

ZERTIFIKAT
Der öffentliche Schlüssel eines Subjekts und die verbundene Information, die digital mit dem privaten Schlüssel des Zertifikatsausstellers unterzeichnet wurde. Sofern nicht anders angegeben handelt es sich bei den hierin beschriebenen Zertifikaten um die des Abonnenten.

LISTE DER WIDERRUFENEN ZERTIFIKATE ODER CRL
Eine von der CA verwaltete Liste mit Zertifikaten, die vor ihrer Ablaufzeit widerrufen werden.

ZERTIFIZIERUNGSBEHÖRDE ODER CA
Eine Einheit, die mit der Zuordnung eines öffentlichen Schlüssels zur Information über das Subjekt beauftragt wird, das im Zertifikat enthalten ist. Sofern nicht ausdrücklich angegeben handelt es sich bei der hierin beschriebenen CA und die AlphaSSL CA.

ZERTIFIZIERUNGSPRAXISERKLÄRUNG ODER **CPS**
Eine Erklärung der Praktiken in der Verwaltung von Zertifikaten während aller Lebensphasen.

ZERTIFIKATSSTATUSDIENSTE ODER **CSS**
Ein Dienst, der Relying Parties und anderen ermöglicht, den Status von Zertifikaten zu überprüfen.

ZERTIFIKATSKETTE
Eine hierarchische Liste mit Zertifikaten, die einen Bezugsvertrag und CA-Zertifikate enthält.
Ablauf des Zertifikats
Das Ende des Gültigkeitszeitraums eines digitalen Zertifikats.

ZERTIFIKATSERWEITERUNG
Ein Feld im digitalen Zertifikat, das zum Übertragen zusätzlicher Informationen zu folgenden Themen verwendet wird: den öffentlichen Schlüssel, den zertifizierten Abonnenten, den Zertifikatsaussteller und/oder den Zertifizierungsvorgang.

ZERTIFIKATSHIERARCHIE
Eine ebenenbasierte Folge von Zertifikaten einer (Root)-CA und untergeordneten Einheiten, die CAs und Abonnenten umfassen.
ZERTIFIKATSVERWALTUNG
Zu Aktionen im Zusammenhang mit Zertifikatsverwaltung zählen Speicherung, Verbreitung, Veröffentlichung und der Widerruf von Zertifikaten.
ZERTIFIKATSWIDERRUFSLISTE (CRL)
Eine Liste, die von einer CA ausgestellt und digital unterzeichnet ist und widerrufene Zertifikate beinhaltet. Eine solche Liste soll von Relying Parties jeder Zeit konsultiert werden können, bevor sie sich auf die in einem Zertifikat enthaltenen Informationen verlassen.
ZERTIFIKATSSERIENNUMMER
Eine fortlaufende Nummer, die ein Zertifikat innerhalb des Bereichs einer CA eindeutig identifiziert.
CERTIFICATE SIGNING REQUEST (CSR)
Eine maschinenlesbare Anwendungsform, um ein digitales Zertifikat zu beantragen.
ZERTIFIZIERUNG
Der Vorgang der Ausstellung eines digitalen Zertifikats.
ZERTIFIZIERUNGSBEHÖRDE (CA)
Eine Behörde, wie z. B. die AlphaSSL CA, die ein digitales Zertifikat ausstellt oder widerruft.
ZERTIFIZIERUNGSRICHTLINIE (CP)
Eine Aufstellung der Praktiken einer CA und der Bedingungen für Ausstellung, Widerruf, usw. eines Zertifikats. Eine CP wird als auch Leitfaden zum Aufbau der Vertrauenswürdigkeit der Infrastruktur eines Zertifizierungsdienstes verwendet.
ZERTIFIKATSAUSSTELLUNG
Lieferung von X.509 v3 digitalen Zertifikaten für die Authentifizierung und digitale Signatur basierend auf persönlichen Daten und öffentlichen Schlüsseln, die von der RA bereitgestellt werden und mit RFC 3647 und RFC 3039 kompatibel sind.
WIDERRUF DES ZERTIFIKATS
Online-Dienst, der verwendet wird, um ein digitales Zertifikat vor seinem Ablaufdatum dauerhaft zu deaktivieren.
ZERTIFIKATSWIDERRUFSLISTEN
Online-Veröffentlichung von vollständigen und schrittweisen digitalen Zertifikatswiderrufslisten, die mit RFC 5280 kompatibel sind
WIRTSCHAFTLICHE ANGEMESSENHEIT
Ein Rechtsbegriff aus dem bürgerlichen Recht. Im eCommerce ist die Verwendung der Technologie gemein, die eine angemessene Versicherung der Zuverlässigkeit bietet.
GEFÄHRDUNG
Ein Verstoß gegen eine Sicherheitsrichtlinie, die den Verlust der Kontrolle über sensitive Informationen zur Folge hat.
VERTRAULICHKEIT
Die Bedingung für die Offenlegung von Daten ausschließlich an ausgewählte und autorisierte Parteien.
BESTÄTIGEN EINER ZERTIFIKATSKETTE
Zum Überprüfen einer Zertifikatskette, um einen Endbenutzer-Bezugsvertrag zu überprüfen.
DIGITALES ZERTIFIKAT
Ein formatiertes Datenpaket, das sich auf ein identifiziertes Subjekt mit einem öffentlichen Schlüssel bezieht, den das Subjekt verwendet.
DIGITALE SIGNATUR
Um eine Nachricht mithilfe eines asymmetrischen Kryptosystems und einer Hash-Funktion so zu verschlüsseln, dass eine Person, die die ursprüngliche Nachricht und den öffentlichen Schlüssel des Unterzeichners besitzt genau feststellen kann, ob die Transformation mithilfe des privaten Schlüssels erstellt wurde, der dem öffentlichen Schlüssel des Unterzeichners entspricht, und ob die ursprüngliche Nachricht seit Durchführung der Transformation geändert wurde.
DISTINGUISHED NAME
Ein Datensatz, der eine reale Einheit, wie z. B. eine Person in einem computergestützten Zusammenhang, darstellt.
VERZEICHNISDIENST
Online-Veröffentlichung von Zertifikaten, die das Abrufen eines Zertifikats basierend auf ihrer Zertifikats-ID ermöglicht.

ENDBENUTZER-ABONNENT
Ein Abonnent außer der CA.
ERWEITERUNGEN
Erweiterungsfelder in X.509 v.3.0-Zertifikaten.
GENERIEREN EINES SCHLÜSSELPAARES
Ein zuverlässiger Prozess zur Erstellung privater Schlüssel während der Zertifikatsanwendung, deren entsprechende öffentliche Schlüssel während der Zertifikatsanwendung so der zuständigen CA eingereicht werden, dass die Fähigkeit des Antragstellers zur Verwendung des privaten Schlüssels aufgezeigt wird.

REGIERUNGSSTELLE

Eine von der Regierung betriebene Rechtsperson, Agentur, Abteilung, Ministerium oder ähnliche Einrichtung der Regierung eines Landes oder einer Gebietskörperschaft eines solchen Landes (wie z. B. Staat, Bundesland, Stadt, usw.)
HASH
Ein Algorithmus, der einen Satz von Bytes in einen anderen (allgemein kleineren) Satz abbildet oder übersetzt, sodass:
Eine Nachricht jedes Mal dasselbe Ergebnis erzielt, wenn der Algorithmus mithilfe derselben Nachricht als Input ausgeführt wird.
Es ist rechenbetont unmöglich, eine Nachricht von dem vom Algorithmus erzielten Ergebnis abzuleiten oder wiederherzustellen.
Es ist rechenbetont unmöglich, zwei verschiedene Nachrichten zu finden, die dasselbe Hash-Ergebnis mithilfe desselben Algorithmus zu erzielen.
IDENTIFIKATION
Der Vorgang der Bestätigung der Identität einer Einheit. Die Identifikation bei der Verschlüsselung eines öffentlichen Schlüssels wird mithilfe von Zertifikaten vereinfacht.
ALS REFERENZ EINBEZOGEN
Durch Identifikation des einzubindenden Dokuments ein Dokument in ein anderes eingliedern, mit Informationen, die dem Empfänger ermöglichen, die eingegliederte Nachricht als Ganzes aufzurufen und zu erhalten, und durch Ausdrücken der Absicht, dass sie Teil der einzubindenden Nachricht wird. Eine solche eingegliederte Nachricht muss dieselbe Wirkung haben, die sie als vollständig angegebene Nachricht in der Nachricht hat.

AUFNEHMENDE AGENTUR

Falls es sich um eine private Organisation handelt, die Regierungsbehörde im Gerichtsbereich der Gesellschaft, unter deren Amtsgewalt die legale Existenz der privaten Organisation begründet wurde (z. B. die Regierungsbehörde, die die Gründungsurkunde ausstellte). Falls es sich um eine Regierungsbehörde handelt, die Einheit, die das Recht, die Regulierung oder das Dekret erließ, die die legale Existenz der Regierungsbehörde begründete.

GERICHTSBEREICH DER GESELLSCHAFT

Falls es sich um eine private Organisation handelt, das Land und (gegebenenfalls) der Staat oder das Bundesland, in dem die legale Existenz der Organisation durch eine Ablage mit (oder einem Akt) einer entsprechenden Regierungsagentur oder -Stelle begründet wurde (z. B. wo sie eingetragen wurde). Falls es sich um eine Regierungsstelle handelt, das Land und (gegebenenfalls) der Staat oder das Bundesland, in dem die legale Existenz der Stelle gesetzlich begründet wurde.
SCHLÜSSELGENERIERUNGSPROZESS
Der zuverlässige Prozess des Erstellens eines privaten/öffentlichen Schlüsselpaares. Der öffentliche Schlüssel wird einer CA während des Zertifikatsanwendungsprozesses bereitgestellt.
SCHLÜSSELPAAR
Ein privater Schlüssel und sein entsprechender öffentlicher Schlüssel in asymmetrischer Verschlüsselung.
HINWEIS
Das Ergebnis der Benachrichtigung der Parteien, die in den Empfang von CA-Diensten gemäß dieser CPS involviert sind.
BENACHRICHTIGEN
Spezielle Informationen gemäß der Anforderung durch diese CPS und das geltende Recht einer anderen Person mitteilen.

OBJEKT-ID
Eine Folge ganzzahliger Komponenten, die einem registrierten Objekt zugeordnet werden können und die die Eigenschaft haben, einmalig unter allen Objekt-IDs innerhalb eines bestimmten Bereichs zu sein.
PKI-HIERARCHIE
Eine Gruppe von CAs, deren Funktionen gemäß des Prinzips der Vollmachtsübertragung organisiert sind und als übergeordnete und untergeordnete CA zusammenhängen.
GESCHÄFTSSITZ
Der Standort jeder Einrichtung (wie z. B. eine Fabrik, ein Einzelhandelsgeschäft, Lager, usw.), wo das Geschäft des Antragstellers geführt wird
PRIVATER SCHLÜSSEL
Ein mathematischer Schlüssel zum Erstellen privater Signaturen und manchmal (in Abhängigkeit des Algorithmus) zur Entschlüsselung von Nachrichten in Kombination mit dem entsprechenden öffentlichen Schlüssel.
ÖFFENTLICHER SCHLÜSSEL
Ein mathematischer Schlüssel, der öffentlich zugänglich gemacht wird, der zur Überprüfung von Signaturen verwendet wird, die mit dessen entsprechendem privaten Schlüssel erstellt wurden. In Abhängigkeit des Algorithmus können öffentliche Schlüssel auch zur Verschlüsselung von Nachrichten oder Dateien verwendet werden, die dann mit dem entsprechenden privaten Schlüssel entschlüsselt werden.
PUBLIC-KEY-KRYPTOGRAFIE
Kryptografie, die ein Schlüsselpaar mathematisch verbundener kryptografischer Schlüssel verwendet.
PUBLIC KEY INFRASTRUCTURE (PKI)
Die Architektur, Organisation, Techniken, Praktiken und Verfahren, die kollektiv die Implementierung und Bedienung eines zertifikatsbasierten kryptografischen Systems mit öffentlichem Schlüssel unterstützen.
REGISTRIERTER AGENT
Eine Einzelperson oder eine Einheit, für die Folgendes gilt:
Durch den Antragsteller autorisiert, Dienstleistungen von Prozess- und Geschäftskommunikationen im Auftrag des Antragstellers zu erhalten; und
Gelistet in den offiziellen Datensätzen des Gerichtsbereichs der Gesellschaft des Antragstellers in der in (a) festgelegten Rolle.

GESCHÄFTSSITZ

Die offizielle Adresse eines Unternehmens, die bei der Incorporating Agency erfasst ist, an die offizielle Dokumente gesendet und an der rechtliche Hinweise empfangen werden.

REGISTRIERUNGSNUMMER

Die einmalige Nummer, die der privaten Organisation, dem Antragsteller oder der Subjekteinheit von er Incorporating Agency im Rechtsbereich der Gesellschaft einer solchen Einheit zugewiesen wird.
REGISTRIERUNGSBEHÖRDE ODER **RA**
Eine Einheit, die dafür verantwortlich ist, Abonnenten zu identifizieren und zu authentifizieren. Die RA stellt keine Zertifikate aus. Sie beantragt hauptsächlich die Ausstellung eines Zertifikats im Auftrag von Antragstellern, deren Identität sie überprüfte.
RELATIVE DISTINGUISHED NAME (RDN)
Eine Reihe von Attributen, die die Einheit von anderen desselben Typs unterscheiden.
VERTRAUEN
Eine digitale Signatur akzeptieren und so agieren, dass sie Vertrauen weckt.
RELYING PARTY
Eine Einheit, die sich für die Durchführung einer Aktion auf ein Zertifikat verlässt.
AUFBEWAHRUNGSORT
Eine Datenbank und/oder ein Verzeichnis, in der/dem digitale Zertifikate und andere relevante, online abrufbare Informationen aufgelistet sind.
EIN ZERTIFIKAT WIDERRUFEN
Dauerhaft die Laufzeit eines Zertifikats ab einem bestimmten Zeitpunkt beenden.
GEHEIMER ANTEIL
Ein Teil eines kryptografischen Geheimnisses, das auf mehrere physikalische Token, wie z. B. Smartcards, usw. aufgeteilt wurde.

GEHEIMER GESELLSCHAFTER
Eine Person, die einen geheimen Anteil besitzt.
SHORT MESSAGE SERVICE (SMS)
Ein Dienst zum Senden von Nachrichten bis zu einer Länge von 160 Zeichen (224 Zeichen im 5-Bite-Modus) an Mobiltelefone, die Global System for Mobile (GSM)-Kommunikation nutzen.
SIGNATUR
Eine Methode, die vom Verfasser eines Dokuments verwendet oder übernommen wird, um sich selbst zu identifizieren, die entweder vom Empfänger akzeptiert wird oder deren Verwendung gemäß den Umständen allgemein üblich ist.
UNTERZEICHNER
Eine Person, die eine digitale Signatur für eine Nachricht oder eine Signatur für ein Dokument erstellt.
SMARTCARD
Ein Hardware-Token, das einen Chip enthält, der neben anderen kryptografischen Funktionen implementiert wird.
STATUSÜBERPRÜFUNG
Online-Dienst basierend auf dem Online Certificate Status Protocol (RFC 2560), das verwendet wird, um den aktuellen Status eines digitalen Zertifikats zu bestimmen, das CRLs erfordert
SUBJEKT EINES DIGITALEN ZERTIFIKATS
Die genannte Partei, der der öffentliche Schlüssel in einem Zertifikat als Benutzer des privaten Schlüssels entsprechend dem öffentlichen Schlüssel zugeordnet werden kann.
ABONNENT
Das Subjekt eines digitalen Zertifikats oder eine vom Subjekt ernannte Partei, die ein Zertifikat beantragt.
BEZUGSVERTRAG
Der Vertrag zwischen einem Abonnenten und einer CA für die Bereitstellung von öffentlichen Zertifizierungsdiensten.
VERTRAUENSWÜRDIGE POSITION
Eine Rolle innerhalb einer CA, die den Zugang zu oder die Kontrolle über kryptografischer Abläufe beinhaltet, die einen bevorzugten Zugang zur Ausstellung, Verwendung oder zum Widerruf von Zertifikaten, einschließlich der Vorgänge, die den Zugang zu einem Aufbewahrungsort beschränken, ermöglicht.
VERTRAUENSWÜRDIGES SYSTEM
Computer-Hardware, Software und Verfahren, die eine akzeptable Ebene gegen Sicherheitsrisiken bieten, ein angemessenes Maß an Verfügbarkeit, Zuverlässigkeit und einen korrekten Ablauf bereitstellen und eine sichere Richtlinie durchsetzen.
ALPHASSL CA REGISTRIERUNGSBEHÖRDE
Eine Einheit, die alle Abonnentendaten überprüft und der AlphaSSL CA zur Verfügung stellt.
ALPHASSL CA ÖFFENTLICHE ZERTIFIZIERUNGSDIENSTE
Ein digitales Zertifizierungssystem, das von AlphaSSL CA zur Verfügung gestellt wird, als auch die Einheiten, die gemäß Beschreibung in dieser CPS zur AlphaSSL CA Domain gehören.
ALPHASSL CA-VERFAHREN
Ein Dokument, das die internen Verfahren der AlphaSSL CA im Hinblick auf die Registrierung von Endbenutzern, Sicherheit, usw. beschreibt.

WEBTRUST-PROGRAMM FÜR CAS: Die geltende Version des AICPA/CICA WebTrust-Programms für Zertifizierungsbehörden, verfügbar unter http://www.webtrust.org/certauth fin.htm.
WEB -- WORLD WIDE WEB (WWW)
Ein grafikgestütztes Medium für die Dokumentveröffentlichung und das Abrufen von Informationen im Internet.
SCHRIFTLICH
Informationen, die als Referenz zugänglich und nutzbar sind.
X.509
Der Standard der ITU-T (International Telecommunications Union-T) für digitale Zertifikate.

11.0 Liste der Abkürzungen

CA: Certification Authority (Zertifizierungsbehörde)
RA: Registration Authority (Registrierungsbehörde)
LRA: Local Registration Authority
CEN/ISSS: European Standardization Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Zertifizierungspraxiserklärung
ETSI: European Telecommunications Standards Institute
GSCA: AlphaSSL Zertifizierungsbehörde
IETF: Internet Engineering Task Force
ISO: International Standards organization
ITU: International Telecommunications Union
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax