LEISTUNGSBESCHREIBUNG

Public Certificate Service Platform (PCSP)

Deutsche Telekom Security GmbH
Version 1.0
Stand 05.10.2021

ERLEBEN, WAS VERBINDET.

Impressum

HERAUSGEBER

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

Telefon: 0228 181-0 | E-Mail: info@telekom.de | Internet: www.telekom.de/security
Aufsichtsrat: Adel Al-Saleh (Vorsitzender) | Geschäftsführung: Thomas Fetten (Sprecher), Dr. Klaus Schmitz, Thomas Tschersich
Handelsregister: Amtsgericht Bonn HRB 15241, Sitz der Gesellschaft Bonn | USt-IdNr. DE 254595345 | WEEE-Reg.-Nr. DE 56768674

Inhaltsverzeichnis

1 Einleitung

Mit der Public Certificate Service Platform (PCSP) bietet die Deutsche Telekom Security GmbH (im Weiteren Telekom Security) einen Public-Key-Infrastructure (PKI) Service, mit welchem der Auftraggeber verschiedene Zertifikate für unterschiedlichste Anwendungsfälle beantragen und ausstellen lassen kann. In der aktuellen Version wird eine Bereitstellung von domainvalidierten TLS-Serverzertifikaten unterstützt. Die Plattform wird sukzessive um weitere Zertifikatsangebote ausgebaut. Die vorliegende Leistungsbeschreibung erweitert sich dabei ebenfalls über die Zeit.

Betrieben wird der Service in zwei, geografisch voneinander getrennten Rechenzentrumsstandorten (TwinCore), wobei innerhalb der jeweiligen Standorte die Trust Center Umgebung, als besonders gesicherte System-Insel, gegenüber der übrigen Rechenzentrumsinfrastruktur abgeschottet ist.

Wesentliches Merkmal dieses PKI-Service ist der hohe Automatisierungsgrad in den für die Zertifikatserstellung erforderlichen Prozessen. Kunden werden damit in die Lage versetzt, nach einem vorherigen Onboarding Prozess Zertifikate aus dem Trust Center der Telekom automatisiert über Standardschnittstellen zu beziehen.

In der ersten Ausbaustufe handelt es sich um eine ACME-Schnittstelle ((Automatic Certificate Management Environment (ACME)) nach RFC-8555.

Dabei ist der Internet-Kommunikationsweg zum PKI-Service nicht Gegenstand dieses Leistungsangebotes.

Die über die Public Certificate Service Platform ausgestellten, öffentlichen Zertifikate unterliegen Anforderungen des CA/Browser Forums und verschiedener ETSI-Regularien. Die Plattform hat daher eine entsprechende Auditierung und Zertifizierung durchlaufen.

2 Lösungsbeschreibung Public Certificate Service Platform

2.1 Allgemeine Ausführungen zur PCSP

Im Folgenden werden allgemeine Bestimmungen zur PCSP bekannt gegeben. Die weiterführenden Details zu den unterstützen Zertifikatsprodukten werden in separaten Kapiteln beschrieben.

2.1.1 Registrierungsinstanz RA (Registration Authority)

Jeder Zertifikatsantrag bedingt, unabhängig von der Art des verwendeten Verfahrens (manuell oder automatisiert), einer Genehmigung durch einen RA-Prozess. Daher kommt dieser RA eine besondere Bedeutung zu, da die CA das gewünschte End Entity Zertifikat erst nach Prüfung des Zertifikatsantrages mit anschließender Genehmigung durch die RA ausstellt.

Die RA-Tätigkeit wird durch Mitarbeiter des Telekom Security Trust Centers ausgeführt. Des Weiteren unterstützen automatisierte Prozessabläufe technisch bei der Prüfung der notwendigen Validierungsschritte vor der Ausstellung eines beantragten Zertifikates. Details zu den Vorgängen werden bei den jeweils angebotenen Zertifikatsprodukten beschrieben, siehe Kapitel 2.2.

2.1.2 Zertifizierung

Die Telekom Security bzw. die Public Certificate Service Platform wird einer jährlichen Zertifizierung durch ein unabhängiges Prüf- und Zertifizierungsunternehmen unterzogen.

Sollten neue Zertifikatsprodukte oder Schnittstellen etabliert werden, so finden Nachzertifizierungen der neu erstellten Anteile statt.

2.1.3 Übersicht der unterstützten Service Schnittstellen

Für die Kommunikation mit den im Trust Center der Telekom Security befindlichen Services werden gesicherte und mit anderen Kunden gemeinsam genutzte Netzübergänge verwendet. Zu den einzelnen Services erfolgt die Kommunikation immer mittelbar über eine zwischengeschaltete Sicherheitsinfrastruktur. Die Kommunikationsprotokolle setzen auf dem IPv4- und IPv6-Stack auf.

Nachstehende Übersicht listet das zum Service entsprechende Transportprotokoll auf:

- ACME-Schnittstelle nach RFC 8555 (Automatic Certificate Management Environment (ACME)) über https
- Abruf von Sperrinformationen mit OCSP über das http Protokoll
- Abruf von Sperrinformationen durch CRL-Dateidownload (Sperrliste) über das http Protokoll.

Der Sperr-Informationsservice stellt Informationen zu Verfügung, indem Statusinformationen zu gesperrten Zertifikaten online über das Internet abgerufen werden können.

Sperrinformationen zu gesperrten, aber bereits abgelaufenen Zertifikaten werden durch den Sperrservice nicht publiziert.

Telekom Security ermöglicht die Prüfung der Gültigkeit von ausgestellten Zertifikaten über das Internet per OCSP-Standard (Online Certificate Status Protocol). Zusätzlich wird eine Liste der gesperrten Zertifikate (CRL – Certificate Revocation List) im Internet zum Herunterladen bereitgehalten. Details hierzu können der Webseite www.telesec.de entnommen werden.

2.1.3.1 ACME-Schnittstelle nach RFC 8555

ACME ist ein standardisiertes Protokoll der IETF (RFC 8555) zum automatischen Bezug von Public Key Zertifikaten. Obwohl das Protokoll generell für verschiedene Zertifikatstypen entwickelt worden ist, wird es in RFC 8555 für die Verwaltung von TLS-Zertifikaten definiert, die über eine Domainvalidierung geprüft werden. Details hierzu siehe Kapitel 2.2.

Anlage ACME Account
Bevor ein Client ein Zertifikat beziehen kann, muss er zunächst einen Account am ACME-Server der PCSP erstellen. Hierfür erzeugt sich der Client ein asymmetrisches Schlüsselpaar, welches im späteren Protokollverlauf für den Integritätsschutz (digitale Signatur) der übertragenen Nachrichten und zur Authentifizierung (z.B. bei Sperraufträgen, siehe Kapitel 2.2.9) genutzt wird.

Um die Beziehung zwischen dem ACME-Clientaccount zu einem Kundenaccount auf der Public Certficiate Service Platform herzustellen, wird das ACME-Accountfeld „externalAccountBinding“ (EAB) verwendet. Die notwendigen Credentials (externalAccountBinding MACkey) werden dem Kunden über die PCSP bereitgestellt und müssen vom Kunden bei der ACME Registrierung verwendet werden.

Zertifikatsrequst oder -erneuerung via ACME-Client
Kunden können OpenSource ACME-Clientimplementierungen verwenden, um Zertifikate zu bestellen oder zu erneuern. Dabei muss dem ACME-Client die Server-URL des ACME-Servers mitgeteilt werden. Darüber hinaus benötigt der Client den EAB-Schlüssel für die Registrierung. Mit der Client-Anfrage gibt der Kunde an, für welche Domains er ein Zertifikat bestellen möchte.

Wenn der ACME-Server diese Anfrage annimmt, sendet er dem Client die notwendigen Anforderungen, die der Client erfüllen muss, damit das Zertifikat ausgestellt oder erneuert wird.

Im Falle von TLS-Serverzertifikaten muss der Client den Besitz aller angegebenen Domains nachweisen. Für die Domainkontrollvalidierung sind zwei Challenge-Typen möglich: http Challenge und DNS Challenge. Der Client meldet sich zurück, wenn er alle Challenges abgearbeitet hat. Daraufhin prüft der Server die Challenges und verarbeitet bei positiver Prüfung den vom Client eingereichten Certificate Signing Request, was zur Signatur durch die CA führt.

Die PCSP stellt nach Ausführung aller Validierungsschritte das Zertifikat über den ACME-Server an den Kunden bereit.

Sperrung via ACME-Client
Die Beantragung von Sperranträgen kann grundsätzlich über die vom ACME-Protokoll bereitgestellten Funktionen erfolgen. Dazu ist die Signatur eines Sperrantrags mit dem zum Zertifikat gehörenden privaten Schlüssel oder dem privaten Schlüssel des mit dem Zertifikat assoziierten Account notwendig. Alternativ kann ein Sperrantrag durch Nachweis der Kontrolle über die im Zertifikat angegebene Domain autorisiert werden.

Darüber hinaus bietet das Trust Center eine weitere Schnittstelle über die eigene Webseite an, über die Missbrauch- sowie Problemmeldungen zu Zertifikaten gemeldet werden können. Telekom Security bearbeitet diese Meldungen und leitet bei Vorliegen eines entsprechenden Sperrgrunds die Sperrung von betroffenen Zertifikaten ein. Der Meldende des Problems wird über den Erhalt der Meldung sowie ggf. dadurch resultierende Sperrungen der betroffenen Zertifikate informiert. Details zur Kontaktaufnahme siehe Kapitel 3.3.5.

2.1.3.2 OCSP-Service

Die Onlineabfrage von Sperrinformationen erfolgt auf Basis des OCSP (Online Certificate Status Protocol) Protokolls, das die PCSP, anteilig nach RFC 6960, über das HTTP Internetprotokoll bereitstellt.

Damit ist ein Ressourcenschonender Online-Abruf von Sperrinformationen zu einem End Entity Zertifikat in direkter Weise möglich, ohne dass größere CRL-Dateien (siehe Kapitel 2.1.4.2) verarbeitet werden müssen.

Erreichbar und technischen Änderungen vorbehalten, ist die Web-Ressource unter:

http://ocsp.pcsp.telesec.de/ocspr

2.1.3.3 CRL-Service (Certificate Revocation List)

Diese Datei wird zyklisch durch die PCSP erzeugt und beinhaltet die Seriennummern der gesperrten EndEntity Zertifikate, das Sperrdatum und optional den Sperrgrund, soweit dieser durch den Auftraggeber angegeben wurde.

Unterschrieben wird diese Datei durch die EndEntity Zertifikate ausstellende CA.

Für die CA wird eine eigene Sperrliste für CA-Zertifikate (ARL- Authority Revocation List) erzeugt und mit dem ROOT Signaturschlüssel unterschrieben. Sollten CA-Zertifikate gesperrt werden, werden diese in der ARL im gleichen Format wie in der vorbezeichneten CRL Datei abgelegt.

Zum HTTP Download der CRL-Datei werden ein DNS-Eintrag und eine Web-Ressource im Trust Center der Telekom Security eingerichtet und betrieben. Erreichbar und technischen Änderungen vorbehalten, ist die Web-Ressource unter:

http://crl.pcsp.telesec.de/rl/Telekom_Security_DV_RSA_CA_21.crl

2.1.4 Reporting Service

Aktuell stellt die PCSP keinen eigenen Reporting Service zur Verfügung. Der Kunde erhält nur im Zuge seiner Arbeitsschritte, z.B. Anlage Account, Beauftragung Zertifikat, Sperrung Zertifikat, entsprechende Benachrichtigungen über die involvierten Clients oder per Mail. Details werden bei den jeweiligen Zertifikatsprodukten gegeben.

2.1.5 Archivierung

Die Telekom Security bewahrt die gesamte Dokumentation im Zusammenhang mit der Zertifikatsbeauftragung, der Zertifikatsverifizierung und deren Widerruf über die PCSP entsprechend der Vorgaben im Certificate Practice Statement auf.

2.1.6 Beendigung

Eine Beendigung der PCSP und der hierüber angebotenen Zertifikatsprodukte würde nach den Vorgaben des Certificate Practice Statement und eines Telekom Security Beendigungsplans erfolgen. Die Zertifikatsnehmer würden in diesem Falle frühzeitig über diesen Sachverhalt informiert.

2.2 Zertifikatsprodukt: Domainvalidiertes TLS-Serverzertifikat via ACME-Schnittstelle

2.2.1 Überblick

Mit den domainvalidierten TLS-Serverzertifikaten (kurz DV-Zertifikate) ermöglicht die Telekom Security, jedem Web-Server im Internet eine domainvalidierte Identität zuzuordnen.

Bei dieser Identität handelt es sich um ein vom Telekom Security Trust Center nach der ITU-T-Empfehlung X.509v3 erzeugtes Public-Key-Zertifikat. Dies wird auf Basis des vom Kunden zugelieferten öffentlichen kryptografischen Schlüsselteils (Public Key) erzeugt. Das Public-Key-Zertifikat wird nach Überprüfung der Domainkontrolle durch eine Zertifizierungsstelle der Telekom Security digital signiert.

Für die Erstellung des Zertifikates steht mindestens ein Vertrauensanker (Root-CA) zur Verfügung. Dieser Vertrauensanker kann variieren.

Die aktuelle Zertifikatshierarchie bestehend aus Root- und Sub-CA gestaltet sich wie folgt:

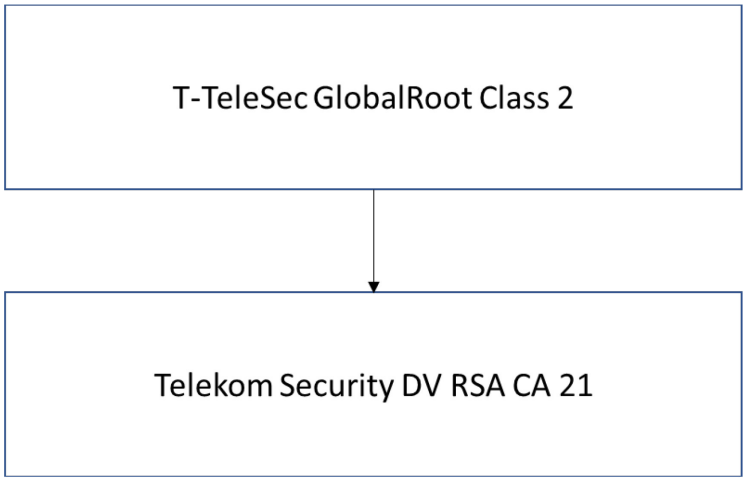

Abbildung 1 – Zertifikatshierarchie zur Ausstellung von domainvalidierten TLS-Serverzertifikaten

Zur Prüfung der Zertifikatskette werden die Zertifikate von ausstellenden Zertifizierungsstellen (Issuing CAs, in diesem Fall Telekom Security DV RSA CA 21) bereitgestellt. Hierfür wird die Authority-Information-Access-Erweiterung (AIA) genutzt. Diese Erweiterung wird in End-Entitätszertifikate aufgenommen und enthält die URL, unter der das Zertifikat der ausstellenden CA zu finden ist.

Zertifikatsschlüssellängen und -laufzeiten

Die folgende Tabelle detailliert die verwendeten Algorithmen, Schlüssellängen, Hashfunktionen sowie die Gültigkeitsdauer:

ZERTIFIKATLEVEL	ALGORIT.	SCHLÜSSELLÄNGE	HASHALGORITHMUS DER CA	MAX. GÜLTIG-KEITSDAUER
T-TeleSec GlobalRoot Class 2	sha256RSA	2048 Bit	SHA 256	25 Jahre (bis 02.10.2033)
Telekom Security DV RSA CA 21	sha256RSA	2048 Bit	SHA 256	10 Jahre (bis 22.04.2031)
DV-TLS-Serverzertifikat (RSA)	RSA	>= 2048 Bit[1]	SHA 256	12 Monate
DV-TLS-Serverzertifikat (EC-DSA)	EC-DSA	256 Bit oder 384 Bit[2]	SHA 256	12 Monate

Tabelle 1- Verwendete Schlüssellängen

Die Zertifikate auf den drei Ebenen haben unterschiedliche Laufzeiten bzw. Gültigkeitsdauern. Es wird dabei für jede Ebene ein Zeitpunkt definiert an welchem diese frühestens erneuert werden können. Dies setzt voraus, dass die verwendeten Algorithmen und Schlüssellängen in der Zwischenzeit nicht unsicher geworden sind und aufgrund dessen eine vorzeitige Erneuerung stattfinden muss.

2.2.2 DV-Zertifikatsauftrag via ACME-Schnittstelle

Die Zertifikatsbeauftragung erfolgt ausschließlich online durch den registrierten und damit autorisierten Kunden. Hierzu ist ein Onboarding-Prozess notwendig, über welchen Account-User angelegt werden.

Nach einem organisatorischen Onboarding-Prozess nutzt der Kunde zur Zertifikatsbeauftragung die standardisierte ACME-Schnittstelle (siehe Kapitel 2.1.3.1) nach RFC 8555 (Automatic Certificate Management Environment (ACME)) mit auf dem Markt befindlichen ACME-Client-Lösungen (siehe Kapitel 5). Der Kunde wählt dabei selbst den von ihm präferierten ACME-Client aus.
Telekom Security bietet keinen eigenen ACME-Client an. Da das Protokoll öffentlich ist, können öffentlich bekannte ACME Client-Implementierungen für die Beantragung verwendet werden. Voraussetzung hierbei ist, dass dieser ein sogenanntes External Account Binding-Verfahren unterstützt. Die im Zusammenhang mit der PCSP getesteten ACME Client-Implementierungen sind unter https://www.telesec.de/ aufgelistet.

Die domainvalidierten TLS-Serverzertifikatsaufträge durchlaufen den folgenden Ablauf:

1) Onboarding-Prozess und Auswahl einer gewünschten DV-Produktausprägung (siehe Kapitel 2.2.3)

[1] Min. Anforderung von RSA 2048 Bit muss durch den Auftraggeber bei Zertifikatsrequest erfüllt werden.
[2] Min. Anforderung von ECC-Schlüssel mit nist-p-256 bzw. nist-p-384 muss durch den Auftraggeber bei Zertifikatsrequest erfüllt werden.

2) Bestätigung des Auftrages
3) Verifikation der E-Mail-Adresse des technischen Ansprechpartners des Kunden.
4) Zuweisung von ACME Credentials zur Beantragung von Zertifikaten mittels auf dem Markt befindlicher ACME-Clients.
5) Validierung und Prüfung der Zertifikatsbeantragung durch die Telekom Security Registrierungsstelle.

2.2.3 Produktausprägungen

Die angebotenen domainvalidierten TLS-Serverzertifikaten stehen aktuell in folgenden Produktausprägungen zur Auswahl. Die Standardlaufzeit (Gültigkeit) der Zertifikate umfasst 1 Jahr:

1) **Standard:** Die Standardvariante des Produktes umfasst die Beantragung und Ausstellung eines domainvalidierten TLS-Serverzertifikats für 1 validierten Domainnamen.
2) **Multi-Domain:** Die Produktausprägung Multi-Domain umfasst die Beantragung und Ausstellung eines domainvalidierten TLS-Serverzertifikats mit mehreren validierten Domainnamen. Es dürfen hierbei max. 5 alternative Domainnamen angegeben werden.
3) **Wildcard:** Die Produktausprägung Wildcard umfasst die Beantragung und Ausstellung eines domainvalidierten TLS-Serverzertifikates mit einem validierten Domainnamen. Dieser Domainname darf jedoch im Gegensatz zur Standard-Variante ein führendes Platzhalterzeichen „*." beinhalten, welches mehr Flexibilität bietet.

Die Preisgestaltung der Produktausprägungen kann einer separaten Preisliste bzw. der Webseite https://www.telesec.de/ entnommen werden.

Für die beschriebenen Produkte gelten die Deutsche Telekom Security GmbH - Trust Center Certificate Policy in aktueller Version sowie das Deutsche Telekom Security GmbH – Trust Center Certificate Practice Statement Public. Beide Dokumente können über die Webseite https://www.telesec.de/ abgerufen werden.

2.2.4 Zertifizierung und Validierung

Für die Ausstellung eines domainvalidierten TLS-Serverzertifikats sind die angegebenen Domains zu prüfen und zu bestätigen. Folgende Aspekte werden in allen Vorgängen geprüft:

- Überprüfung der korrekten ACME Credentials
- Überprüfung eines korrekten Certificate Signing Request (CSR). Hierbei wird unter anderem auch geprüft, ob der für das Zertifikat bestimmte öffentliche Schlüssel die Anforderungen (siehe Tabelle 1) an kryptographische Algorithmen und Schlüssellängen erfüllt.
- Formale Überprüfung der angegebenen Domains auf Ausschlusskriterien (bspw. White-/ Blacklist).
- Überprüfung des Domainbesitzes durch offiziell zulässige Verfahren wie DNS-Check oder http-Check nach geltenden Vorgaben (Baseline Requirements des CA-Browser Forums).
- Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

2.2.5 Erneuerung

Die Erneuerung eines DV-Zertifikats wird wie eine Neustellung gehandhabt. Dieser Prozess läuft im ACME-Protokoll analog zur Bestellung eines Zertifikats ab. Mittels einer ACME-Client-

Implementierung besteht die Möglichkeit, Erneuerungen von Zertifikaten automatisiert zu vollziehen.

Abhängig von der eigenen Konfiguration des ACME-Clients und dem fortwährenden Vertragsverhältnis kann diese Erneuerung automatisiert angestoßen werden.

Die korrekte Nutzung der automatisierten Erneuerung liegt in der Verantwortung des Kunden. Bei der Zertifikatserneuerung kann eine Schlüsselerneuerung durchgeführt werden. Weitere Änderungen des Zertifikatsinhalts sind nicht erlaubt.

2.2.6 Wiederausstellung/Austausch (Re-Issue)

Eine Erneuerung (Re-Issue) im Sinne einer Wiederausstellung eines Zertifikats ist bei *domainvalidierten TLS-Serverzertifikaten* nicht vorgesehen. Jeder Zertifikatsantrag entspricht einer Neubeauftragung.

2.2.7 Sperrung

Beim Vorliegen eines Sperrgrundes muss das DV-Zertifikat gesperrt werden. Die Sperrung eines domainvalidierten TLS-Serverzertifikates kann durch die Telekom Security oder den Kunden durchgeführt werden. Eine Sperrung ist endgültig und kann nicht rückgängig gemacht werden.

Eine Sperrung seitens des Kunden kann über den ACME-Client ausgelöst werden oder durch Kontaktaufnahme mit dem Telekom Security Support. Siehe hierzu auch Kapitel 2.2.7.

Telekom Security führt eine Sperrung nur in begründeten Fällen durch. Sperrgründe sind in der Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb (CP/CPS) von domainvalidierten TLS-Zertifikaten aufgeführt. Der jeweilige Sperrgrund wird seitens Telekom Security gespeichert und nicht veröffentlicht.

Zertifikatsmissbräuche, Schlüsselkompromittierungen, fehlerhafte bzw. nicht-konforme Zertifikate, andere sicherheitsrelevante Zertifikatsprobleme oder der Verdacht auf solche Vorfälle können unter https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/ an Telekom Security gemeldet werden. Dabei sollten möglichst viele Informationen enthalten sein, die eine Verifizierung des Problems möglich machen. Im Falle einer Kompromittierung sollte dies bspw. einen mit dem privaten Schlüssel signierten CSR mit commonName „Compromised Key“ beinhalten.

3 Leistungen der Telekom Security

3.1 Leistungsbezug über die PCSP

Die *Public Certificate Service Platform* bietet grundlegende Leistungen zur Zertifikatsbeantragung- und des Managements von Zertifikaten. Hierbei werden verschiedene Zertifikatsprodukte unterstützt, zum aktuellen Zeitpunkt handelt es sich um das Zertifikatsprodukt „domainvalidierte TLS-Serverzertifikate“ (siehe Kapitel 2.2); es sind aber bereits weitere Produkte in Entwicklung.

Der Kunde beauftragt daher nicht die PCSP selbst, sondern konkrete Zertifikatsprodukte, welche in unterschiedlichen Produktausprägungen und Kontingentkombinationen angeboten werden. Die Produktausprägungen werden in diesem Dokument beschrieben, die möglichen Bestellkombinationen von Zertifikatspaketen in einer separaten Preisliste, welche über https://www.telesec.de/ für externe Kunden einsehbar ist.

Mit der Beauftragung eines Zertifikatsproduktes erhält der Kunde die Möglichkeit, eine bestimmte Anzahl von Zertifikaten zu einem vorgegebenen Preis flexibel nach seinem Bedarf zu beantragen und abzurufen.

Sollte die maximale Anzahl an aktiven Zertifikaten in dem beauftragten Paket erreicht worden sein, so kann entweder auf ein umfangreicheres Zertifikatspaket mit einer höheren Kontingentanzahl gewechselt oder die Menge gültiger Zertifikate reduziert werden, um eine erneute Ausstellmöglichkeit zu erhalten. Die Kontingentauslastung bezieht sich daher immer auf die gleichzeitig aktiven Zertifikate.

Je nach Konfiguration des verwendeten ACME-Clients kann eine automatisierte Erneuerung von Zertifikaten eingestellt werden, wodurch in einem definierten Zeitraum vor Ablauf des Zertifikats ein Erneuerungsantrag an die PCSP gestellt wird. Sollte zu diesem Zeitpunkt das Kontingent nicht ausgeschöpft sein, so wird der Auftrag automatisiert verarbeitet und ein neues Zertifikat ausgestellt.

Voraussetzung bei allen Zertifikatsausstellungen ist, dass die beantragte Domain nicht auf der Denied Liste für kritische Domains steht. Diese Liste wird in der PCSP regelmäßig aktualisiert und kann bei Zertifikatsbeantragung zu einer Ablehnung des Zertifikatsrequests führen.

3.2 Leistungsübergabepunkt

Die Leistungen der PCSP werden am Trust Center Zugangspunkt bereitgestellt.

Die notwendige Kommunikationsverbindung zum Trust Center Zugangspunkt ist nicht Vertragsbestandteil der Leistung.

Mit der Beantragung und Nutzung der bestätigten ACME-Credentials ist der Auftraggeber mit seinem Account in der Lage, Zertifikate bei Telekom Security per ACME-Client anzufragen.

Wird ein Zertifikatsrequest gestellt und ein gültiges, inhaltlich und formal korrektes Zertifikat an den Auftraggeber ausgestellt, so gilt dieses als seinerseits akzeptiert. Sollte der Auftraggeber einen Fehler identifizieren, so kann er selbstständig eine direkte Sperrung vornehmen und ein neues Zertifikat beantragen.

3.3 Betriebliche Serviceparameter

3.3.1 Betriebszeit

Die betreute Betriebszeit der in diesem Dokument beschriebenen betrieblichen Leistungen definieren sich auf einen täglichen Betrieb von 00:00 bis 24:00 Uhr.

3.3.2 Störungen

Eine Störung definiert sich als ein Ereignis, das nicht zum standardmäßigen Betrieb eines Services gehört und das tatsächlich oder potenziell eine Unterbrechung dieses Services oder eine erhebliche Minderung der zugesicherten Leistung verursacht.

Im Falle von auftretenden Störungen unterliegen diese der nach ITIL konformen, prozessual geführten Beseitigung, innerhalb der Betriebszeit.

Kundenseitig festgestellte Störungen, die im Zusammenhang mit dem beauftragten Service stehen, können an die Servicestelle gemeldet werden, siehe Kapitel 3.3.5.

3.3.3 Verfügbarkeit

In der nachfolgenden Übersicht sind die jeweiligen Services und Verfügbarkeiten, bezogen auf einen Betrieb täglich von **00:00 bis 24:00 Uhr**, im monatlichen Mittel, in Prozent angegeben.

- ACME-Schnittstelle 98 %
- Sperr-Information Service OCSP 98 %
- Sperr-Information Service CRL 98 %
- Trust Center Zugangspunkt 98 %

Höhere Verfügbarkeiten sind für zertifikatsausstellende Services erfahrungsbedingt nicht erforderlich.

Änderungen an der Plattform oder Infrastruktur, die im Rahmen von geplanten, sowie von adhoc Wartungsarbeiten (z. B. Release-, Security-, Patch-Management etc.) zur Aufrechterhaltung der zugesicherten Leistungen und betrieblichen Stabilität durchgeführt werden müssen, fallen nicht in die Verfügbarkeitsbetrachtung.

3.3.4 Wartung

Wartungsarbeiten, die die Verfügbarkeit der Dienste beeinflussen, werden, soweit möglich, in festen Wartungsfenstern durchgeführt. Sie dienen der Aufrechterhaltung der zugesicherten Eigenschaften der Services sowie der Aufrechterhaltung der besonderen Schutzbedürftigkeit der im Trust Center betriebenen Plattformen und Infrastruktur.

Die Wartungsfenster sind serviceabhängig wie folgt vorgesehen:

ACME-Schnittstelle, Sperr-Information Service, Trust Center Zugangspunkt und Trust Center PKI-Plattform

- täglich von **03:00 bis 06:30 Uhr** (MEZ/MESZ) und
- einmal täglich für den betroffenen Service in der Servicezeit gemäß Kapitel 3.3.5, wenn die anfallenden Wartungsarbeiten nicht länger als 30 Minuten dauern.

3.3.5 Servicezeit

Die Servicezeit wird an Werktagen (montags bis freitags) in der Zeit von **09:00 bis 15:00 Uhr** (MEZ/MESZ) erbracht. Innerhalb der Servicezeit werden auftraggeberseitige Aufträge bearbeitet.

Als Aufträge werden z. B.

- Onboarding neuer Kundenaccounts,
- Beratungsleistungen bei Störung des Service

verstanden.

Kontaktaufnahme:

Deutsche Telekom Security GmbH

Trust Center & ID Services

Untere Industriestraße 20

57250 Netphen, Deutschland

Telefon: +49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)

WWW: https://www.telesec.de

E-Mail: telesec_support@t-systems.com

Die Sperrschnittstelle via ACME-Client ist 24x7 für die Kunden verfügbar.

Ebenso kann 24x7 über Dritte eine Missbrauchsmeldung über die angegebene Webseite eingestellt werden.

Sollte der Auftraggeber etwaige Beschwerden an den Auftragnehmer richten wollen, so ist dies schriftlich an die genannte Anschrift, via E-Mail an die genannte Support-Adresse oder telefonisch während der genannten Servicezeiten möglich.

3.3.6 Systemzeit

Alle Zeiten, die im Telekom Security Trust Center zur Erzeugung und Signatur von Zertifikaten zur Anwendung kommen, leiten sich aus der UTC-0 Zeit (entspricht Greenwich Mean Time/GMT) ab.

3.3.7 Logging

Es findet ein Logging der technischen Komponenten der Public Certificate Service Platform anhand der Vorgaben des Certificate Practice Statement statt.

Etwaig seitens des Auftraggebers eingereichte schriftliche Unterlagen im Zuge der Bestellung oder des Zertifikatslebenszyklus werden gemäß der geforderten Aufbewahrungsfristen des Certificate Practice Statements archiviert.

3.3.8 Auditierung

Die Public Certificate Service Platform wird alle 12 Monate oder bei Bedarf einer Auditierung unterzogen. Hierbei liegen für die Bereitstellung von Zertifikatsprodukten notwendige Policies zugrunde, aktuell sind dies:

- ETSI EN 319 411-1
- ETSI EN 319 411-2

Weitere Details zur Auditierung werden im Certificate Practice Statement, Kapitel 8 gegeben.

4 Einseitige Leistungsänderungen

4.1 Leistungsänderungen

Die Telekom Security behält sich einseitige Leistungsänderungen oder Entgeltanpassungen vor. Der Auftraggeber erklärt sich mit diesen Anpassungen einverstanden solange ihm keine Nachteile entstehen. Im Falle eines geplanten Entgeltanstiegs wird der Auftraggeber vorab informiert.

In Abweichung zu dem vereinbarten Schriftformerfordernis wird die Telekom Security den Auftraggeber über etwaige Anpassungen durch Übersendung aktualisierter Versionen der bestehenden Vertragsunterlagen informieren, welche die bestehenden Unterlagen ersetzen.

4.2 Erneute Akzeptanz von Nutzungsbedingungen

Sollten sich Änderungen an den Mitwirkungsleistungen und Nutzungsbedingungen des Auftraggebers im Verlauf seiner Vertragslaufzeit ergeben, so wird dies seitens Telekom Security transparent kommuniziert und der Auftraggeber informiert.

5 Mitwirkungsleistungen des Auftraggebers (Kunde)

Um die beschriebenen Leistungen erfolgreich umsetzen zu können, bedarf es einer engen Kooperation zwischen Auftraggeber (Kunde) und Telekom Security. Der Auftraggeber ist verpflichtet, die in diesem Kapitel beschriebenen Mitwirkungen und Beistellungen auf eigene Kosten beizubringen.

Erbringt der Auftraggeber eine erforderliche Mitwirkungsleistung oder Beistellung nicht, nicht rechtzeitig oder nicht in der vereinbarten Weise, so sind die hieraus entstehenden Folgen (z.B. Verzögerungen bei Leistungserbringung, Mehraufwand) von dem Auftraggeber zu tragen.

5.1 Allgemeine Mitwirkungsleistungen und Nutzungsbedingungen

(a) Der Auftraggeber ist dazu verpflichtet, im Rahmen der Servicebeauftragung vollständige und korrekte Daten anzugeben. Der Auftraggeber trägt dabei Sorge für die Richtigkeit der Antragsdaten (z.B. des Domainnamens, für den ein DV-Zertifikat beantragt werden soll).

(b) Der Auftraggeber verpflichtet sich, alle privaten Schlüssel und Aktivierungsdaten geheim zu halten und vor unbefugter Nutzung und Zugriff geschützt aufzubewahren, wenn für die dazugehörigen öffentlichen Schlüssel ein Public-Key-Zertifikat beim PCSP beantragt werden soll/wurde.

(c) Das vom Auftraggeber selbst erzeugte kryptographische Schlüsselpaar ist ordnungsgemäß zu erzeugen. Hierzu hat sich der Auftraggeber an die vorgegebenen Schlüssellängen und Algorithmen gemäß dieser Leistungsbeschreibung bzw. dem Certificate Practice Statement zu halten.

(d) Der Auftraggeber hat erhaltene ACME-Zugangsdaten vor Missbrauch zu schützen und ausschließlich zweckbestimmt einzusetzen. Dem Auftraggeber zugeordnete Nutzungs- und Zugangsberechtigungen sowie Identifikations- und Authentifikations-Sicherungen sind vor dem unbefugten Zugriff durch Dritte zu schützen.

(e) Der Auftraggeber hat bei Beantragung eines Zertifikates den Nachweis über den Besitz der Domain zu erbringen, für die das Zertifikat beantragt wird. Dies wird über den ACME-Prüfprozess verifiziert.

(f) Der Auftraggeber muss sich umgehend nach Bereitstellung des Zertifikats von der Korrektheit der im Zertifikat hinterlegten Daten überzeugen. Ebenso ist umgehend nach der Ausstellung zu überprüfen, dass der Zertifikatsinhalt den zugrundeliegenden Auftragsdaten entspricht. Sollte dies nicht der Fall sein, ist die Telekom Security zu benachrichtigen.

(g) Der Auftraggeber hat das ausgestellte Zertifikat und den zugehörigen privaten Schlüssel ausschließlich bestimmungsgemäß und für autorisierte und legale Zwecke zu verwenden. Das Zertifikat sollte nicht mit Anwendungen oder Maschinen genutzt werden, deren Funktionen unbekannt, verdächtig oder unzuverlässig erscheinen.

(h) Der Auftraggeber hat tatsächlich als Endteilnehmer zu agieren und mit seinem privaten Schlüssel keine CA-Funktionalitäten durchzuführen, wie z.B. Signatur von Zertifikaten oder Sperrlisten.

(i) Bei Verlust oder Verdacht der Kompromittierung eines privaten Schlüssels, der zu einem öffentlichen Schlüssel gehört, für den ein Public-Key-Zertifikat über die PCSP beantragt wurde, verpflichtet sich der Auftraggeber, das entsprechende Public-Key-Zertifikat unverzüglich zu sperren bzw. die Sperrung durch die Telekom Security zu veranlassen. Bei Kompromittierung des privaten Schlüssels ist dessen Verwendung unmittelbar und dauerhaft einzustellen. Das Zertifikat ist nicht mehr zu nutzen, wenn bekannt wird, dass das Zertifikat der Zertifizierungsstelle kompromittiert wurde.

(j) Der Kunde hat sein Zertifikat unverzüglich sperren zu lassen, wenn sich die den Angaben zu Grunde liegenden Tatsachen geändert haben (z.B. Verlust Domainbesitz bei DV-Zertifikat). Der Auftraggeber hat sein Zertifikat ebenso unverzüglich zu sperren oder sperren zu lassen, wenn ein Sperrgrund gemäß Kapitel 4.9.1.2 des Certificate Practice Statement vorliegt.

(k) Der Auftraggeber ist dazu verpflichtet, nach einer Sperrung eines Zertifikates die Verwendung des korrespondierenden privaten Schlüssels, mit Ausnahme der Schlüsselentschlüsselung, sofort oder dauerhaft einzustellen.

(l) Erfährt der Auftraggeber von einer Kompromittierung der ausstellenden Sub-CA der Telekom Security, so ist die Verwendung des privaten Endteilnehmer-Schlüssels, mit Ausnahme der Schlüsselentschlüsselung, sofort und dauerhaft einzustellen.

(m) Ebenso hat der Auftraggeber innerhalb eines ihm kommunizierten Zeitraums auf die Anweisungen der Telekom Security bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauchs zu reagieren.

(n) Sieht die Telekom Security für ein ausgestelltes Zertifikat einen eindeutigen Sperrgrund gemäß Certificate Practice Statement, so muss der Auftraggeber die Sperrung seines Zertifikats akzeptieren.

(o) Ein ggf. später vorhandenes Service-Passwort ist geheim zu halten.

(p) Der Auftraggeber hat sich unverzüglich ein neues Service-Passwort ausstellen zu lassen, falls die Vermutung besteht, dass unberechtigte Dritte von dem Service-Passwort Kenntnis erlangt haben.

(q) Der Auftraggeber stellt sicher, dass die durch das Telekom Security Trust Center, im Auftraggeberauftrag ausgestellten Zertifikate oder Zertifikatsketten keine Rechte von Dritten (z.B. Markenrecht), noch Zertifikate mit sittenwidrigem oder gegen geltende Gesetze verstoßenden Inhalte ausgestellt werden.

(r) Der Auftraggeber muss im Zuge des Onboarding-Vorgangs der Deutschen Telekom Security einen technischen Ansprechpartner nennen. Änderungen sind der Deutschen Telekom Security unverzüglich mitzuteilen.

(s) Der Auftraggeber verpflichtet sich und seine Mitarbeiter zur Einhaltung der Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb (Deutsche Telekom Security GmbH - Trust Center Certificate Policy (CP) und Telekom Security Certification Practice Statement (CPS)). Der Auftraggeber trägt die rechtlichen Konsequenzen, die durch die Nichteinhaltung der im o.g. CP/CPS beschriebenen Pflichten entstehen.

(t) Der Auftraggeber verpflichtet sich, das Zertifikat ausschließlich in Übereinstimmung mit allen geltenden Gesetzen und in Übereinstimmung mit der abgeschlossenen Vereinbarung und den Nutzungsbedingungen zu nutzen.

(u) Der Auftraggeber verantwortet im Rahmen der geltenden Datenschutzgesetze der Europäischen Union sowie den länderspezifischen Gesetzgebungen, dass die beantragten Zertifikate keine personenbezogenen Daten enthalten. Sollten dennoch personenbezogene Daten in den auszustellenden Zertifikaten enthalten sein, hat der Auftraggeber die nach geltendem Recht durchzuführenden Verfahren einzuhalten und z.B. die Genehmigung der jeweils betroffenen Personen einzuholen.

(v) Der Auftraggeber verpflichtet sich bei Serverzertifikaten, das Zertifikat nur auf Servern zu installieren, auf die unter den im Zertifikatsattribut subjectAltName aufgeführten Namen zugegriffen werden kann.

(w) Der Auftraggeber hat im Rahmen einer Supportanfrage die erforderlichen Informationen in ausreichender Tiefe bereitzustellen und den Telekom Security Mitarbeiter bei der Störungsbearbeitung zu unterstützen.

(x) Maßnahmen, die aufgrund von sicherheitsrelevanten Ereignissen oder der Gefahrenabwehr dienen, sind unverzüglich nach Mitteilung durch die Telekom Security auf Auftraggeberseite umzusetzen.

(y) Zertifikate besitzen einen Lebenszyklus, der durch Erreichen des Ablaufdatums endet. Der Auftraggeber ist für eine rechtzeitige Verlängerung seiner Zertifikate zuständig.

(z) Der Auftraggeber stellt sicher, dass die über die PCSP abgerufenen Zertifikate nur für die im CPS genannten zulässigen Anwendungsfälle eingesetzt werden. Sämtliche Zertifikate sind nicht für die Verwendung in Steuerungs- und Kontrolleinrichtungen in gefährlichen Umgebungen oder Umgebungen, in denen ein ausfallsicherer Betrieb gewährleistet sein muss und ein Ausfall zu Schäden wie Personenschäden, Tod, mittleren und schweren Umweltschäden, sonstige Katastrophen führen kann, vorgesehen, ausgelegt oder zugelassen. Hierzu gehören: Nukleare Einrichtungen, Flugzeugnavigations- oder-kommunikationssysteme, Luftverkehr-Kontrollsysteme, Waffenkontrollsysteme.

(aa) Für jede nicht eingelöste bzw. zurückgereichte Lastschrift hat der Kunde der Deutschen Telekom Security die ihr entstandenen Kosten in dem Umfang zu erstatten, wie er das Kosten auslösende Ereignis zu vertreten hat.

5.2 Technische Voraussetzungen

(a) Der Auftraggeber ist verpflichtet, einen Übertragungsweg zum Trust Center Zugangspunkt (z.B. Internet) beizustellen. Dieser ist nicht Bestandteil dieser Leistung durch die Telekom Security.

(b) Die auftraggeberseitigen Geräte und Systeme, die in einem automatisierten Verfahren Zertifikate erhalten sollen, müssen über die von Telekom Security vorgegebenen Schnittstellen und Protokolle verfügen und den PKI-Service netztechnisch erreichen können und deren Vorgaben einhalten.

(c) Telekom Security bietet keinen eigenen ACME-Client an. Da das Protokoll öffentlich ist können öffentlich bekannte ACME Client-Implementierungen für die Beantragung verwendet werden. Voraussetzung hierbei ist das dieser ein sogenanntes External Account Binding-Verfahren unterstützt. Die im Zusammenhang mit der PCSP getesteten ACME Client-Implementierungen sind unter www.telesec.de aufgelistet.

(d) Im Falle eines automatisierten Genehmigungsprozesses zur Zertifikatsausstellung durch die PCSP, müssen vom Auftraggeber bereitgestellte Genehmigungsinformationen (wie die hinterlegten http Challenges oder DNS Challenges) über das Internet zugänglich gemacht werden. Ebenso müssen die von der Telekom Security vorgegebenen Protokolle und Datenformate zur Abfrage der Genehmigungsinformation eingehalten werden.

(e) Es obliegt dem Auftraggeber, ein unkontrolliertes Verhalten (z.B. Zertifikatsabruf eines Gerätes im Stundentakt) eigener Geräte und Applikationen zu vermeiden, welches durch den Einsatz vollautomatisierter, zertifikatsausstellender Prozesse zu einer überdurchschnittlichen Belastung der Automatisierungsschnittstellen führt. Andernfalls greifen vertragliche Anfragelimits der Public Certificate Service Platform.

(f) Der Auftraggeber darf nicht selbst oder durch nicht autorisierte Dritte in Programme, die von der Deutschen Telekom Security administriert werden, oder in Daten eingreifen oder eingreifen lassen.

(g) Bei Überlassung von Software hat der Kunde nach Beendigung oder der Kündigung einzelner Lizenzen die überlassene Software einschließlich sämtlicher Kopien auf den betroffenen Systemen zu löschen. Der Kunde hat der Deutschen Telekom Security schriftlich zu bestätigen, dass keine weiteren Kopien mehr existieren.

(h) Ggf. vorhandene Urhebervermerke, Seriennummern und sonstige der Programmidentifikation dienende Merkmale dürfen auf keinen Fall entfernt oder verändert werden. Gleiches gilt für eine Unterdrückung der Bildschirmanzeige entsprechender Merkmale.

(i) Der Auftraggeber ist für die Sicherung seiner privaten Schlüssel sowie Verwaltung seiner beantragten Zertifikate zuständig. Die Telekom Security und ihre Erfüllungsgehilfen sind von sämtlichen Ansprüchen Dritter freizustellen, die auf einer rechtswidrigen Verwendung von

Software und der hiermit verbundenen Leistungen durch den Kunden beruhen oder mit seiner Billigung erfolgen.

(j) Erkennt der Kunde oder muss er erkennen, dass ein solcher Verstoß droht, besteht die Pflicht zur unverzüglichen Unterrichtung der Deutschen Telekom Security.

5.3 Folgen eines Pflichtverstoßes

Verletzt der Kunde ihm obliegende Pflichten erheblich oder nachhaltig und macht er dieses vertragswidrige Verhalten nicht unverzüglich rückgängig, so kann die Telekom Security

(a) die Nutzung der Leistung auf Kosten des Kunden sperren. Der Kunde bleibt in diesem Fall verpflichtet, die monatlichen bzw. jährlichen Preise zu zahlen

oder

(b) einen sofort in einer Summe fälligen pauschalierten Schadensersatz verlangen. Der Schadensersatz beträgt ein Viertel der bis zum Ablauf der regulären Vertragslaufzeit zu zahlenden restlichen Entgelten. Der Schadensbetrag ist höher anzusetzen, wenn die Telekom Security einen höheren Schaden nachweist. Er ist niedriger anzusetzen bzw. entfällt, wenn der Kunde nachweist, dass ein wesentlich geringerer oder überhaupt kein Schaden eingetreten ist.

6 Mindestüberlassungszeit/Beendigung

Die Leistungen der Public Certificate Service Platform werden dem Auftraggeber mit einer Mindestvertragslaufzeit in Monaten, je nach Art des bestellten Zertifikatsproduktes überlassen. Die Vertragslaufzeit beginnt am Tag der Bestellung durch den Kunden, an dem die Telekom Security die vertragliche Leistung aufnimmt.

Bei Bestellung eines Zertifikatsproduktes wird dem Auftraggeber transparent dargestellt, inwiefern ein monatliches, jährliches oder einmaliges Entgelt für dieses anfällt und wie die Abrechnung erfolgt.

Aktuell verfügbare Zertifikatsprodukte:

Zertifikatsprodukt	Mindestlaufzeit	Vertragliche Anpassung
Domainvalidiertes TLS-Serverzertifikat (Server-ID.DV)	Jedes Zertifikat hat eine vorgegebene Gültigkeitszeit. Die Gültigkeit kann durch eine Sperrung verkürzt werden. Die Mindestvertragslaufzeit für einen DV-Kontingentvertrag ist der aktuell gültigen Preisliste zu entnehmen. Die Vertragslaufzeit verlängert sich automatisch, insofern der Auftraggeber diese nicht vor Ablauf der Mindestvertragslaufzeit kündigt.	Monatlich möglich. Dies betrifft eine Änderung des gebuchten Zertifikatskontingents.

Tabelle 2 - Mindestüberlassung

Der Vertrag kann von beiden Vertragspartnern jeweils mit einer Frist von einem Monat zum Ende der Mindestvertragslaufzeit gekündigt werden.

Während der Vertragslaufzeit ist ein Wechsel des gebuchten Zertifikatskontingents (z.B. Buchung nächst höhere Kontingentgröße) zum jeweils nächsten Monat möglich. Hierdurch verändert sich das Entgelt und die Anzahl der ausstellbaren Zertifikate für den Kunden. Bestehende Zertifikate laufen gemäß ihrer Gültigkeit bis zum Ablauf weiter. Je nach Einstellung des ACME-Clients auf Auftraggeberseite kann eine automatische Verlängerung eines kurz vor Ablauf stehenden Zertifikats eingestellt werden. Dies hat entsprechende Auswirkungen auf die weitere Vertragslaufzeit.

Sollte der Auftraggeber seinen Vertrag kündigen wollen, so ist das Entgelt bis zum Ende der Mindestvertragslaufzeit zu entrichten. Kündigt der Auftraggeber einen monatlich abgerechneten Vertrag, so erfolgt eine direkte Sperrung der zugehörigen Zertifikate und keine Abrechnung im Folgemonat.

Einmalig oder jährlich gezahlte Zertifikate, die zum Zeitpunkt der Kündigung noch gültig sind, behalten ihre Gültigkeit bis zu ihrem Ablaufdatum oder zum Ende der Vertragslaufzeit, können aber nicht mehr durch den Kunden verlängert werden. Dem Auftraggeber steht frei, diese mit Kündigung direkt selbst zu sperren.

Telekom Security entzieht nach Verarbeitung des Kündigungsauftrags durch den Auftraggeber die ausgegebenen Credentials zur Nutzung der ACME-Schnittstelle bzw. sperrt diese für den Account, so dass keine Neubeantragung eines Zertifikats mehr möglich ist. Eine Sperrung von noch gültigen Zertifikaten ist weiterhin möglich, insofern der Auftraggeber weiterhin den privaten Schlüssel des ausgestellten Zertifikats besitzt oder die Domain kontrolliert, für die das Zertifikat ausgestellt wurde.

Sollte der Auftraggeber mehrere Zertifikate auf der Public Certificate Service Platform gebucht haben, so werden nur die Anteile gesperrt, die er gekündigt hat. Alle weiteren Leistungen der Public Certificate Service Platform kann der Auftraggeber über seinen Account weiterhin nutzen.

Mitgeltende Unterlagen

Es gilt die zugehörige AGB (Allgemeinen Geschäftsbedingung) der Deutschen Telekom Security GmbH für IT-Leistungen, in der jeweils gültigen Fassung.

Weitergehend gilt die aktuelle Deutsche Telekom Security GmbH Trust Center Certificate Policy (CP) und das Deutsche Telekom Security GmbH Trust Center Certificate Practice Statement Public (CPS).

Alle Dokumente finden Sie unter https://www.telesec.de/.

Abkürzungsverzeichnis/Glossar

Abkürzung	Beschreibung
ARL	Authority Revocation List
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation Lists
DNS	Domain Name System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ITIL	Information Technology Infrastructure Library
OCSP	Online Certificate Status Protocol
PCSP	Public Certificate Service Platform
PKCS	Public-Key Cryptography Standards
PKI	Public-Key-Infrastructure
RA	Registration Authority
RFC	Request for Comments
Root-CA	Root-Certificate Authority
TLS / SSL	Transport Layer Security / Secure Sockets Layer

Tabelle 3 - Abkürzungsverzeichnis