LEISTUNGSBESCHREIBUNG

Public Certificate Service Platform (PCSP)

Deutsche Telekom Security GmbH

Version	6.0
Gültig ab	10.01.2023
Vermerk:	Öffentlich
Status:	Freigegeben

ERLEBEN, WAS VERBINDET.

Impressum

HERAUSGEBER

DEUTSCHE TELEKOM SECURITY GMBH
Trust Center & ID Security

Untere Industriestraße 20
57250 Netphen, Deutschland

WWW: https://www.telesec.de

Bei Fragen zur PCSP, Server.ID-DV oder unseren anderen Produkten nutzen Sie gerne unser Kontaktformular unter:
https://www.telesec.de/de/service/kontakt/anfragemitteilung/

Wählen Sie dort die passende Kategorie, z.B. *ServerPass (ServerID; SSL / TSL Zertifikate)* aus. Wir melden uns dann bei ihnen!

Pflichtangaben:

https://www.telekom.com/de/telekom/pflichtangaben-dtsec-602264

Dokumentenhistorie

VERSION	DATUM	ÄNDERUNG
1.0	05.10.2021	Initiale Version
2.0	01.05.2022	Anpassung an DV-Beschreibung
3.0	07.09.2022	Korrektur CAs und Impressum Anpassung DV-Beschreibungen Auslagerung Nutzungsbedingungen in separates Dokument
3.1-Audit	07.09.2022	Auditversion als Entwurfsversion mit Scope DV via ACME und REST.
4.0	15.09.2022	Korrektur fehlerhafter Angabe in 2.3.1
4.1	22.09.2022	Zusammenführung Versionen 3.1-Audit und 4.0
5.0	17.11.2022	Anpassung in Kapitel 3.3.4
6.0	10.01.2023	Anpassung Verweis auf vereinheitlichte Nutzungsbedingungen für öffentliche Zertifikate (Kapitel 5 und 8)

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 Kundinnen und Kunden verschiedene öffentliche Zertifikate für unterschiedlichste Anwendungsfälle beantragen und ausstellen lassen können. 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.

In der aktuellen Version bietet die PCSP folgenden Leistungsumfang an:

- Beantragung, Validierung und Ausstellung von domainvalidierten Zertifikaten (DV)
- Bereitstellung einer ACME-Schnittstelle konform zu RFC-8555, welcher durch frei auf dem Markt verfügbare ACME[1]-Clients angesteuert werden kann, um ein DV-Zertifikat zu beantragen
- Bereitstellung einer REST-Schnittstelle zur Nutzung durch eine Web-Applikation über welche DV-Zertifikate über eine Maschine-zu-Maschine Kommunikation beantragt werden können.
- OCSP-Service zur Abfrage von Status- oder Sperrinformationen
- CRL-Sperrliste

Die Leistungen werden in den nächsten Kapiteln detaillierter ausgeführt.

Dabei ist der Internet-Kommunikationsweg zur PCSP bzw. PKI-Service nicht Gegenstand dieses Leistungsangebotes. Gleiches gilt für die Bereitstellung eines ACME-Clients oder einer Web-Applikation.

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.

[1] Automatic Certificate Management Environment

2 Funktionen

2.1 Allgemeine Ausführungen zur PCSP

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

2.1.1 Registrierungsinstanz RA (Registration Authority)

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

Die RA-Tätigkeit wird, wenn nicht nur automatische Prüfprozesse ausgeführt werden, durch Mitarbeiter*innen 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.

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, falls dies notwendig ist.

2.1.3 Archivierung

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

2.1.4 Beendigung

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

2.2 Übersicht der unterstützten Schnittstellen

Für die Kommunikation mit den im Trust Center der Telekom Security befindlichen Services werden gesicherte und mit anderen Kund*innen gemeinsam genutzte Netzübergänge über das Internet 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 Protokoll auf:

- ACME nach RFC 8555 (Automatic Certificate Management Environment (ACME)) über https
- REST-API über das https Protokoll
- 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.

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.

2.2.1 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.

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) genutzt wird.

Um die Beziehung zwischen dem ACME-Clientaccount zu einem Kund*innen-Account auf der Public Certficiate Service Platform herzustellen, wird das ACME-Accountfeld „externalAccountBinding“ (EAB) verwendet. Die notwendigen Credentials (externalAccountBinding MACkey) werden dem Kunden oder der Kundin nach der Bestellung eines entsprechenden Produkts über die PCSP bereitgestellt und müssen von diesen bei der ACME Registrierung verwendet werden.

Zertifikatsrequst oder -erneuerung via ACME-Client
Kund*innen 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 oder die Kundin 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:

- Agreed-Upon Change to Website - ACME
- DNS Change

Der Client meldet sich zurück, wenn er die Challenges für alle angefragten Domains 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 oder die Kundin 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 oder die 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.

2.2.2 REST-Schnittstelle

Die nach REST-Prinzipien erstellte Schnittstelle erlaubt eine Anbindung eines Web-Portals, Frontends, Resellers oder einer anders gearteten Web-Applikation zur Ansteuerung der Schnittstelle an die PCSP. Über dieses im Folgenden allgemein als Web-Applikation bezeichnete Interface, können Kunden und Kundinnen konkrete Zertifikatsprodukte der PCSP bestellen. Die Web-Applikation selbst ist nicht direkter Bestandteil der PCSP. Aufgrund der Architektur besteht somit auch die Möglichkeit mehrere Web-Applikationen über die Schnittstelle der PCSP zu adressieren und so unterschiedliche Kundenkanäle zu etablieren.

Anlage Account
Sollte es sich um einen Neukunden oder Neukundin handeln, so wird über eine Web-Applikation im Zuge einer initialen Bestellung eines Zertifikatsproduktes geprüft, inwiefern dieser Kunde oder Kundin bereits in der PCSP existiert. Sollte dies nicht der Fall sein, wird über die Schnittstelle der Auftrag gegeben einen Account anzulegen. Dadurch wird ein konkreter API-Key für diesen Account generiert und an die Web-Applikation zurückgegeben.

Zertifikatsrequest oder -erneuerung
Der Kunde oder Kundin wählt das oder die betreffenden Zertifikatsprodukte über die Web-Applikation aus und führt dort den kommerziellen Anteil der Bestellung durch. Im Zuge der Beauftragung in Richtung PCSP sind die abhängig vom gewählten Zertifikatsprodukt notwendigen Datenfelder und Nachweise zu befüllen. Erst nachdem die erforderlichen Daten, Zertifikatsrequest und Anlagen vollständig vorliegen, kann der Auftrag des Kunden oder der Kundin an die PCSP gegeben und dort geprüft und verarbeitet werden.

Zur Prüfung der Domainkontrolle werden die folgenden Methoden angeboten:
- Agreed-Upon Change to Website
- DNS Change

Nach erfolgreicher Prüfung der Daten und Untererlagen entsprechend offizieller Prüfvorschriften, erzeugt die PCSP das gewünschte Zertifikat und stellt dieses als Ergebnis der Web-Applikation über die Schnittstelle zur Verfügung.
Der Ablauf bei der Erneuerung eines Zertifikats gestaltet sich wie eine Neubeauftragung.

Sperrung
Die Sperrung eines Zertifikats ist über die Web-Applikation durch den Kunden oder die Kundin initiierbar. Die Schnittstelle übermittelt den Sperrrequest und dessen Grund und die PCSP führt die Sperrung des Zertifikats nach Authentifizierung der Anfrage durch.

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.

2.2.3 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 2.2.4) verarbeitet werden müssen.

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

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

2.2.4 CRL-Service (Certificate Revocation List)

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

Unterschrieben wird diese Datei durch die 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, sind die Web-Ressourcen der aktuell eingebundenen CAs unter:

- DV_CA: Telekom Security DV RSA CA 21,
  http://crl.pcsp.telesec.de/rl/Telekom_Security_DV_RSA_CA_21.crl
- DV-CA: Telekom Security DV RSA CA 22,
  http://crl.pcsp.telesec.de/rl/Telekom_Security_DV_RSA_CA_22.crl

2.2.5 Reporting Service

Aktuell stellt die PCSP bedingt einen eigenen Reporting Service zur Verfügung. Nutzt der Kunde oder die Kundin eine Web-Applikation und damit indirekt die REST-Schnittstelle, so werden Rückmeldungen über diese an die Applikation gegeben bzw. sind durch die Applikation abrufbar.

Bei der Nutzung von ACME können dem Client hierüber keine Reportingdaten zur Verfügung gestellt werden. Eventuelle Benachrichtigen bei Erreichen eines Zertifikatskontingentes erfolgen hierzu per paralleler E-Mail an benannte Ansprechpartner*innen des Kunden oder der Kundin.

2.3 Domainvalidierte TLS-Serverzertifikate

2.3.1 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 oder Kundin 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:

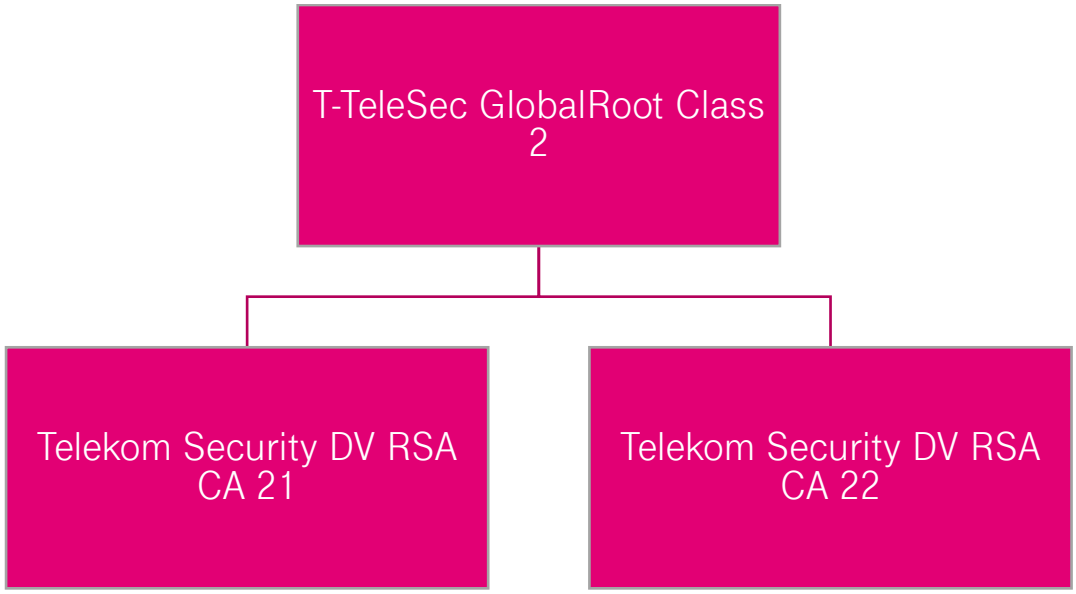

Abbildung 1 – Zertifikatshierarchie zur Ausstellung von domainvalidierten TLS-Serverzertifikaten

Zur Prüfung der Zertifikatskette werden die Zertifikate von ausstellenden Zertifizierungsstellen (Issuing CAs) 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
Telekom Security DV RSA CA 21	sha256RSA	2048 Bit	SHA 256	10 Jahre
Telekom Security DV RSA CA 22	sha256RSA	4096 Bit	SHA 256	10 Jahre
DV-TLS-Serverzertifikat (RSA)	RSA	>= 2048 Bit[2]	SHA 256	12 Monate
DV-TLS-Serverzertifikat (EC-DSA)	EC-DSA	256 Bit oder 384 Bit[3]	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.

2.3.2 Produktausprägungen

Domainvalidierte TLS-Serverzertifikate:
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:** Weitergehend besteht die Möglichkeit der Beantragung und Ausstellung eines **domainvalidierten** TLS-Serverzertifikats mit mehreren validierten Domainnamen. Es dürfen hierbei insgesamt max. 15 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. Es ist zudem auch möglich ein Zertifikat mit Wildcard und weiteren Domaineinträgen zu erhalten.

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

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

3 Leistungen der Telekom

3.1 Bereitstellung

3.1.1 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 Kunde oder die Kundin mit seinem/ihrem Account in der Lage, Zertifikate bei Telekom Security per ACME-Client anzufragen. Gleiches gilt für die Beantragung und Nutzung eines PCSP-Accounts über eine Web-Applikation.

Wird ein Zertifikatsrequest gestellt und ein gültiges, inhaltlich und formal korrektes Zertifikat an den Kunden oder die Kundin ausgestellt, so gilt dieses als seinerseits/ihrerseits akzeptiert. Sollte eine Fehler identifiziert werden, so kann er/sie selbstständig eine direkte Sperrung vornehmen und ein neues Zertifikat beantragen.

3.1.2 Account Einrichtung

Zur Beantragung von Zertifikaten über die Schnittstellen der PCSP muss der Kunde oder die Kundin im Zuge des ersten Beantragungsvorgangs einen Account für die Organisation sowie einen technischen Nutzer oder Nutzerin einrichten lassen.

Mit der Einrichtung wird eine Bestätigung der Mail-Adresse des technischen Ansprechpartners bzw. der Ansprechpartnerin durchgeführt und anschließend abhängig von der gewählten Schnittstelle zusätzlich ACME-Credentials oder REST-API-Schlüssel ausgestellt.

- ACME-Credentials werden bei der Nutzung des ACME-Clients zur Kommunikation mit der ACME-Schnittstelle der PCSP benötigt. Der ACME-Client muss hierzu das sogenannte *External Account Binding*-Verfahren unterstützen.
- Der REST-API-Key wird für den Kund*innen-Account angelegt und die Web-Applikation kann in der Folge zertifikatsbezogene Bestellaktivitäten für diesen Kunden oder Kundin in Richtung PCSP initiieren. Dem Endkunden selbst wird der API-Key nicht sichtbar gemacht.

3.1.3 Bereitstellung Web-Applikations-Zugang für Großkund*innen oder Reseller

Im Rahmen von Großaufträgen oder bei Interesse von Resellern besteht die Möglichkeit über einen manuellen Vertragsabschluss einen individuellen REST API-Key anzulegen und diesen zur Ansteuerung der PCSP bereitzustellen. Großkund*innen oder Reseller würde dann eine eigene Web-Applikation zur Ansteuerung der PCSP über die REST-Schnittstelle umsetzen und einsetzen.

Die RA-Prüfschritte zur Ausstellung eines Zertifikats bleiben dabei identisch zu den im Folgenden beschriebenen Abläufen. Die Web-Applikation des Kunden oder der Kundin oder des Resellers ist nicht Teil der PCSP und kann von diesem individuell gestaltet werden. Voraussetzung ist ein Vertragsabschluss und die Implementierung der REST-API-Beschreibung zur korrekten Ansteuerung der PCSP.

3.2 Betrieb

3.2.1 Beantragung

Die Zertifikatsbeantragung erfolgt ausschließlich online durch registrierte und damit autorisierte Kund*innen. Hierzu ist ein einmaliger manueller Onboarding-Prozess notwendig, über welchen Account-User angelegt werden.

Nutzen Kund*innen danach die angebotene ACME-Schnittstelle so werden neue Zertifikatsanträge inkl. Zertifikatsrequest über den genutzten ACME-Client eingestellt.

Wählt ein Kunde oder Kundin eine Beantragung über eine Web-Applikation, welche die REST-Schnittstelle der PCSP anspricht, so können darüber die notwendigen Daten inkl. Zertifikatsrequest übermittelt werden.

3.2.2 Zertifizierung und Validierung via ACME-Client

Für die Ausstellung eines domainvalidierten Zertifikats mittels ACME-Client 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) (Zertifikatsrequest). Hierbei wird unter anderem auch geprüft, ob der für das Zertifikat bestimmte öffentliche Schlüssel die Anforderungen 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 Agreed upon Change to Website-Check nach geltenden Vorgaben (Baseline Requirements des CA-Browser Forums). Eine Dokumentation der verwendeten Verfahren findet im Certificate Practice Statement statt.
- Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

3.2.3 Zertifizierung und Validierung via Web-Applikation

Kunden und Kundinnen können über eine mögliche Web-Applikation domainvalidierte TLS-Serverzertifikate als Einzelzertifikate beantragen.

Im Falle eines domainvalidierten Zertifikats finden folgende Prüfschritte statt:

- Überprüfung eines korrekten Certificate Signing Request (CSR) (Zertifikatsrequest). Hierbei wird unter anderem auch geprüft, ob der für das Zertifikat bestimmte öffentliche Schlüssel die Anforderungen 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 Agreed upon Change to Website-Check nach geltenden Vorgaben (Baseline Requirements des CA-Browser Forums). Eine Dokumentation der verwendeten Verfahren findet im Certificate Practice Statement statt.
- Zusätzliche Prüfungen werden nach Bedarf durchgeführt.

3.2.4 Ausstellung Zertifikat

Nach Durchführung der vorherigen Prüfschritte für ein domainvalidiertes TLS-Serverzertifikat, stellt die PCSP das beantragte Zertifikat aus und bestätigt so im ersten Fall die im Zertifikat genannte(n) Domains.
Nach der Ausstellung wird das Zertifikat auf dem Beantragungsweg entweder via ACME oder über die Web-Applikation zur Nutzung zur Verfügung gestellt.
Jedes Zertifikat besitzt dabei einen konkreten Zeitpunkt der Ausstellung durch die PCSP und somit eine fest vorgegebene Gültigkeitsdauer bis zu dessen Ablauf.

3.2.5 Erneuerung

Die Erneuerung eines 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 der Kund*innen. Bei der Zertifikatserneuerung kann eine Schlüsselerneuerung durchgeführt werden. Weitere Änderungen des Zertifikatsinhalts sind nicht erlaubt.

Wird statt des ACME-Clients die Web-Applikation genutzt, so können dort ein oder mehrere neue Zertifikate manuell und bedarfsbezogen beantragt werden.

3.2.6 Wiederausstellung/Austausch (Re-Issue)

Eine Erneuerung (Re-Issue) im Sinne einer Wiederausstellung eines Zertifikats ist aktuell nicht vorgesehen. Jeder Zertifikatsantrag entspricht einer Neubeauftragung.

3.2.7 Sperrung

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

Eine Sperrung eines Zertifikats kann bei Nutzung der ACME-Schnittstelle über den ACME-Client durch den Kunden oder die Kundin selbst erfolgen. Ebenso ist eine Sperrung über die Web-Applikation durch den Kunden oder die Kundin selbst möglich.

Alternativ kann eine Sperrung durch Kontaktaufnahme mit dem Telekom Security Support ausgelöst werden. Telekom Security führt eine Sperrung nur in begründeten Fällen durch.

Sperrgründe sind in der Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb (CP/CPS, Kapitel 4.9) 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 dem Root-Team des Trust Centers gemeldet werden. Hierzu ist die Mail-Adresse

TrustCenter-Roots@telekom.de zu verwenden. Bezüglich der Meldung von Schlüsselkompromittierungen sind die Instruktionen gemäß Kapitel 4.9.12 des Certificate Practice Statements zu berücksichtigen.

3.3 Supportleistungen

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.

Kund*innenseitig 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 %
- REST-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

Mit der PCSP steht eine PKI-Infrastruktur zur Verfügung, die von fachkundigem Personal im hochsicheren Trust Center der Telekom Security nach den Regelungen des Service Level Agreements (SLA) und der Zertifizierungsrichtlinie (Certificate Policy (CP)) und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) betrieben und gewartet wird.

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.

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 kund*innenseitige Aufträge bearbeitet.

Als Aufträge werden z. B.

- Onboarding neuer Kundenaccounts,
- Beratungsleistungen bei Störung des Service

verstanden.

Kontaktaufnahme:

Deutsche Telekom Security GmbH

Trust Center & ID Security

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

Bei Fragen zu unseren Produkten nutzen Sie gerne unser Kontaktformular unter:
https://www.telesec.de/de/service/kontakt/anfragemitteilung/

Die Sperrschnittstelle ist 24x7 für Kunden oder Kundinnen verfügbar.

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

Sollte der Kunde oder die Kundin etwaige Beschwerden an Telekom Security 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 Kund*innen 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 (DVCP)

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

4 Einseitige Leistungsänderungen

Für Leistungsänderungen beachten Sie bitte die gültigen AGB.
Aussagen zur Leistungsänderung finden sich in den anzuwendenden Allgemeinen Geschäftsbedingungen der Telekom Security (DT Sec) für IT-Leistungen.
Diese sind hier https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/ einsehbar.

5 Mitwirkungsleistungen des Kunden

Die Verpflichtungen der Antragsteller bzw. Kunden werden in den übergreifenden Nutzungsbedingungen für öffentliche Zertifikate detailliert.

6 Anpassung/Mindestlaufzeit/Beendigung

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

Bei Bestellung eines Zertifikatsproduktes wird Kundinnen und Kunden 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 (innerhalb eines Kontingentsvertrages oder als Einzelbestellung) hat eine vorgegebene Gültigkeitszeit (in der Regel 12 Monate). 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 Kund*innen diese nicht vor Ablauf der Mindestvertragslaufzeit kündigen.	**Kontingentvertrag** (beinhaltet mehrere Zertifikate): Monatliche Änderung möglich. Details siehe Preisliste. **Einzelvertrag** (Bestellung eines einzelnen Zertifikats): Keine Änderung vorgesehen, es kann lediglich gesperrt oder ein Folgezertifikat beauftragt werden. Das Einzelzertifikat läuft gemäß seiner Gültigkeit ab.

Tabelle 2 - Mindestüberlassung

Ein Kontingentvertrag 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 verlängert sich die Mindestvertragslaufzeit und es verändert sich das Entgelt und die Anzahl der ausstellbaren Zertifikate für den Kunden oder die Kundin. Bestehende Zertifikate laufen gemäß ihrer Gültigkeit bis zum Ablauf weiter. Je nach Einstellung des ACME-Clients auf Seiten der Kunden oder Kundinnen kann eine automatische Verlängerung eines kurz vor Ablauf stehenden Zertifikats eingestellt werden. Dies hat entsprechende Auswirkungen auf die weitere Vertragslaufzeit.

Sollten Kund*innen einen Vertrag kündigen wollen, so ist das Entgelt bis zum Ende der Mindestvertragslaufzeit zu entrichten. Kündigt ein Kunde oder Kundin 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 Kund*innen verlängert werden. Kund*innen steht frei, diese mit Kündigung direkt selbst zu sperren.

Telekom Security entzieht nach Verarbeitung des Kündigungsauftrags durch Kund*innen 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 Kund*innen weiterhin den privaten Schlüssel des ausgestellten Zertifikats besitzen oder die Domain kontrollieren, für die das Zertifikat ausgestellt wurde.

Sollte ein Kunde oder Kundin mehrere Zertifikate bzw. Produkte auf der Public Certificate Service Platform gebucht haben, so werden nur die Anteile gesperrt, die er/sie gekündigt hat. Alle weiteren Leistungen der Public Certificate Service Platform können Kund*innen über seinen/ihren Account weiterhin nutzen.

7 Preise, kommerzielle Bedingungen

Die *Public Certificate Service Platform (kurz PCSP)* bietet grundlegende Leistungen zur Zertifikatsbeantragung- und des Managements von Zertifikaten. Hierbei werden zukunftsgerichtet verschiedene Zertifikatsprodukte unterstützt. **Die Preise zu den Leistungen werden dann in separaten Preislisten für die Produkte beschrieben.**
Der Kunde oder die Kundin beauftragt daher nicht die PCSP selbst, sondern konkrete Zertifikatsprodukte, welche in unterschiedlichen Produktausprägungen und Kontingentkombinationen angeboten werden. Die aktuell unterstützte Produktausprägung (Server.ID-DV als domainvalidierte TLS-Serverzertifikate) wird in diesem Dokument beschrieben, die möglichen Bestellkombinationen von Zertifikatspaketen in einer separaten Preisliste, welche über https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/ für externe Kund*innen einsehbar ist.

Mit der Beauftragung eines Zertifikatsproduktes erhält der Kunde oder die Kundin 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 einem 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.

Alternativ sind zu einem späteren Zeitpunkt je nach Produkt auch Einzelbestellungen von Zertifikaten möglich.

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 erforderlichen Prüfschritte zur Ausstellung des Zertifikatstyps erfolgreich durchlaufen werden, andernfalls kann dies zu einer Ablehnung des Zertifikatsrequests führen.

8 Mitgeltende Unterlagen

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

Die Nutzungsbedingungen der Zertifikatsprodukte werden in einem separaten Dokument **Nutzungsbedingungen für öffentliche Zertifikate** zusammengefasst.

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)**.

Für den Betrieb ist das Deutsche Telekom Security GmbH Trust Center Rahmen-**Service Level Agreement (SLA)** zu beachten.

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