NUTZUNGSBEDINGUNGEN

Public Certificate Service Platform (PCSP)

Deutsche Telekom Security GmbH

Version	5.0
Gültig ab	17.11.2022
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. Wie melden uns dann bei ihnen!

Pflichtangaben:

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

Dokumentenhistorie

VERSION	DATUM	ÄNDERUNG
3.0	07.09.2022	Auslagerung Nutzungsbedingungen in separates Dokument. Zuvor waren diese direkter Inhalt der Leistungsbeschreibung 1.0 bzw. 2.0.
3.1	07.09.2022	Auditversion ist eine Entwurfsversion mit Scope DV via ACME und REST.
4.0	15.09.2022	Korrektur Verweise auf Leistungsbeschreibung
4.1	22.09.2022	Zusammenführung 3.1 und 4.0
5.0	17.11.2022	Anpassung in Mitgeltende Unterlagen

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 Kunde oder die Kundin verschiedene Zertifikate für unterschiedlichste Anwendungsfälle beantragen und ausstellen lassen kann. In der aktuellen Version wird eine Bereitstellung von domainvalidierten (DV) TLS-Serverzertifikaten unterstützt. Die Plattform wird sukzessive um weitere Zertifikatsangebote ausgebaut. Die vorliegenden Nutzungsbedingungen beziehen sich auf die zugehörige Leistungsbeschreibung-PCSP.

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 bzw. über Standardschnittstellen zu beziehen.

Aktuell unterstützt die Plattform zwei standardisierte Schnittstellen, es ist aber geplant weitere Schnittstelle zu ergänzen:

- ACME-Schnittstelle ((Automatic Certificate Management Environment (ACME)) nach RFC-8555, welche durch einen ACME-Client genutzt werden kann.
- REST-Schnittstelle, welche von einer generischen Web-Applikation angesteuert werden kann.

Dabei ist der Internet-Kommunikationsweg zum PKI-Service nicht Gegenstand dieser Nutzungsbedingungen.

Die über die Public Certificate Service Platform ausgestellten, öffentlichen Zertifikate unterliegen Anforderungen des CA/Browser Forums und verschiedener ETSI-Regularien. Die Plattform wird daher entsprechend auditiert und zertifiziert.

2 Mitwirkungsleistungen des Kunden oder der Kundin

Um die in der Leistungsbeschreibung der PCSP beschriebenen Leistungen erfolgreich umsetzen zu können, bedarf es einer engen Kooperation zwischen Kunde oder Kundin (alternativ als Auftraggeber oder Auftraggeberin bezeichnet) und Telekom Security. Der Kunde oder die Kundin ist verpflichtet, die in diesem Kapitel beschriebenen Mitwirkungsleistungen und Beistellungen auf eigene Kosten beizubringen.

Erbringt der Kunde oder die Kundin 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 Kunden oder der Kundin zu tragen.

Wir sprechen in den folgenden Ausführungen generell von Kunde oder Kundin, es kann aber auch sein das im Namen einer weiteren juristische Person auf Basis einer Bevollmächtigung bestellt und agiert wird.

2.1 Allgemeine Mitwirkungsleistungen und Nutzungsbedingungen

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

(b) Der Kunde oder die Kundin 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 durch den Kunden oder die Kundin selbst erzeugte kryptographische Schlüsselpaar ist ordnungsgemäß zu erzeugen. Hierzu hat sich der Kunde oder die Kundin an die vorgegebenen Schlüssellängen und Algorithmen gemäß dieser Leistungsbeschreibung bzw. dem Certificate Practice Statement zu halten.

(d) Der Kunde oder die Kundin hat erhaltene ACME-Zugangsdaten vor Missbrauch zu schützen und ausschließlich zweckbestimmt einzusetzen. Zugeordnete Nutzungs- und Zugangsberechtigungen sowie Identifikations- und Authentifikations-Sicherungen sind vor dem unbefugten Zugriff durch Dritte zu schützen.

(e) Der Kunde oder die Kundin hat den über eine ggf. genutzte Web-Applikation erhaltenen PCSP-Account ausschließlich bestimmungsgemäß zu verwenden und nicht an andere weiterzugeben.

(f) Der Kunde oder die Kundin 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.

(g) Der Kunde oder die Kundin 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.

(h) Der Kunde oder die Kundin 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.

(i) Der Kunde oder die Kundin hat tatsächlich als Endteilnehmer*in zu agieren und mit seinem/ihrem privaten Schlüssel keine CA-Funktionalitäten durchzuführen, wie z.B. Signatur von Zertifikaten oder Sperrlisten.

(j) 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 Kunde oder die Kundin, 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. Siehe auch Kapitel 2.2.

(k) Der Kunde oder die Kundin hat ein Zertifikat unverzüglich sperren zu lassen, wenn sich die den Angaben zu Grunde liegenden Tatsachen geändert haben (z.B. Verlust Domainbesitz). Der Kunde oder die Kundin hat ein Zertifikat ebenso unverzüglich zu sperren oder sperren zu lassen, wenn ein Sperrgrund gemäß Kapitel 2.2 vorliegt.

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

(m) Erfährt der Kunde oder die Kundin von einer Kompromittierung der ausstellenden Sub-CA der Telekom Security, so ist die Verwendung des privaten Endteilnehmer*innen-Schlüssels, mit Ausnahme der Schlüsselentschlüsselung, sofort und dauerhaft einzustellen.

(n) Ebenso hat der Kunde oder die Kundin innerhalb eines ihm oder ihr kommunizierten Zeitraums auf die Anweisungen der Telekom Security bei Kompromittierung eines Schlüssels oder Zertifikatsmissbrauchs zu reagieren.

(o) Sieht die Telekom Security für ein ausgestelltes Zertifikat einen eindeutigen Sperrgrund gemäß Certificate Practice Statement bzw. Kapitel 2.2, so muss der Kunde oder die Kundin die Sperrung seines Zertifikats akzeptieren.

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

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

(r) Der Kunde oder die Kundin stellt sicher, dass die durch das Telekom Security Trust Center, im Auftrag der Kund*in ausgestellten Zertifikate oder Zertifikatsketten keine Rechte von Dritten (z.B. Markenrecht), noch Zertifikate mit sittenwidrigem oder gegen geltende Gesetze verstoßenden Inhalte ausgestellt werden.

(s) Der Kunde oder die Kundin muss im Zuge des Beauftragungs- bzw. Onboarding-Vorgangs der Deutschen Telekom Security eine technische Ansprechpartnerin oder Ansprechpartner benennen. Änderungen sind der Deutschen Telekom Security unverzüglich mitzuteilen.

(t) Der Kunde oder die Kundin verpflichtet sich und seine Mitarbeiter*innen 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 Kunde oder die Kundin trägt die rechtlichen Konsequenzen, die durch die Nichteinhaltung der im o.g. CP/CPS beschriebenen Pflichten entstehen.

(u) Der Kunde oder die Kundin verpflichtet sich, das Zertifikat ausschließlich in Übereinstimmung mit allen geltenden Gesetzen und in Übereinstimmung mit der abgeschlossenen Vereinbarung und den Nutzungsbedingungen zu nutzen. Es gilt deutsches Recht.

(v) Der Kunde oder die Kundin 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 Kunde oder die Kundin die

nach geltendem Recht durchzuführenden Verfahren einzuhalten und z.B. die Genehmigung der jeweils betroffenen Personen einzuholen.

(w) Der Kunde oder die Kundin verpflichtet sich bei Serverzertifikaten, das Zertifikat nur auf Servern zu installieren, auf die unter dem im Zertifikatsattribut „subjectAltName“ aufgeführten Namen zugegriffen werden kann.

(x) Der Kunde oder die Kundin hat im Rahmen einer Supportanfrage die erforderlichen Informationen in ausreichender Tiefe bereitzustellen und Telekom Security Mitarbeiter*innen bei der Störungsbearbeitung zu unterstützen.

(y) Maßnahmen, die aufgrund von sicherheitsrelevanten Ereignissen oder der Gefahrenabwehr dienen, sind unverzüglich nach Mitteilung durch die Telekom Security auf Seite des Kunden oder der Kundin umzusetzen.

(z) Zertifikate besitzen einen Lebenszyklus, der durch Erreichen des Ablaufdatums endet. Der Kunde oder die Kundin ist für eine rechtzeitige Verlängerung seiner Zertifikate zuständig.

(aa) Der Kunde oder die Kundin 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.

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

(cc) Der Kunde oder die Kundin erklärt sich mit dem unverschlüsselten Schriftwechsel per E-Mail einverstanden und wird stets eine aktuelle E-Mail Adresse hinterlegen. Dem Kunden oder der Kundin ist bekannt, dass für die Leistungserbringung wesentliche Informationen, wie Zugangsdaten, Informationen zu Änderungen der Leistungen und der rechtlichen Bedingungen, sowie Rechnungen per E-Mail versendet werden.

2.2 Auswahl Sperrgründe durch Kunde oder Kundin

Für die durch die PCSP ausgegebenen Zertifikatsprodukte ergeben sich die folgenden Sperrgründe, welche Kunden oder Kundinnen im Falle einer gewünschten oder notwendigen Sperrung wählen können. Die Nummerierung und Bezeichnung erfolgen anhand RFC 5280:

Sperrgrund 0: Unspecified (Unspezifisch)
Sollten die unten dargestellten Sperrgründe nicht zutreffen, so muss der Sperrende oder die Sperrende keinen spezifischen Grund angeben außer „unspecified“.

Sperrgrund 1: keyCompromise (Schlüssel kompromittiert)
Der Grund „keyCompromise“ muss als Sperrgrund ausgewählt werden, falls ein Verdacht besteht das der private Schlüssel des Zertifikats kompromittiert wurde, d.h. eine unautorisierte Person Zugang zu diesem erhalten hat.

Sperrgrund 3: affiliationChanged (Änderung in der Organisation)
Der Sperrgrund „affiliationChanged“ sollte dann gewählt werden, wenn sich der im Zertifikat enthaltene Organisationsname oder andere Angaben geändert haben. Diese Option ist nicht relevant, wenn ausschließlich DV Zertifikate genutzt werden.

Sperrgrund 4: superseded (ungültig oder veraltet)
Sollte ein bestehendes Zertifikat durch ein neues Zertifikat ersetzt werden, so kann das bestehende Zertifikat mit dem Grund „superseded“ als veraltet gesperrt werden.

Sperrgrund 5: cessationOfOperation (Einstellung des Betriebs)
Zertifikatsinhaber*innen sollten ein Zertifikat mit dem Grund „cessationOfOperation“ sperren, falls sie nicht mehr im Besitz der im Zertifikat genannten Domainnamen sind oder wenn das Zertifikat keinen Einsatz mehr findet, da z.B. die Webseite eingestellt wird.

2.3 Technische Voraussetzungen

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

(b) Die kund*innenseitigen 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 öffentlich unter www.telesec.de bzw. über Telekom-interne Informationsquellen aufgelistet.

(d) Im Falle eines automatisierten Genehmigungsprozesses zur Zertifikatsausstellung durch die PCSP, müssen vom Kunden oder Kundin bereitgestellte Genehmigungsinformationen (wie die hinterlegten Challenges zur Überprüfung eines Domainbesitzes) 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 Kunden oder der Kundin, 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 Kunde oder die Kundin 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 oder die Kundin nach Beendigung oder der Kündigung einzelner Lizenzen die überlassene Software einschließlich sämtlicher Kopien auf den betroffenen Systemen zu löschen. Der Kunde oder die Kundin 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 Kunde oder die Kundin ist für die Sicherung seiner oder ihrer privaten Schlüssel sowie Verwaltung der beantragten Zertifikate zuständig. Die Telekom Security und ihre Erfüllungsgehilf*innen sind von sämtlichen Ansprüchen Dritter freizustellen, die auf einer rechtswidrigen Verwendung von Software und der hiermit verbundenen Leistungen durch den Kunden oder der Kundin beruhen oder mit seiner/ihrer Billigung erfolgen.

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

2.4 Folgen eines Pflichtverstoßes

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

(a) die Nutzung der Leistung auf Kosten des Kunden oder der Kundin sperren. Der Kunde oder die Kundin 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 oder die Kundin nachweist, dass ein wesentlich geringerer oder überhaupt kein Schaden eingetreten ist.

2.5 Akzeptanz eines Zertifikats

Wird ein Zertifikatsrequest gestellt und ein gültiges, inhaltlich und formal korrektes Zertifikat an den Kunden oder die Kundin ausgestellt und über die durch die PCSP vorhandenen Schnittstellen bereitgestellt, so gilt dieses als seinerseits/ihrerseits akzeptiert.

Sollte eine Fehler identifiziert werden, so kann der Kunde oder die Kundin selbstständig eine direkte Sperrung anhand einer der in Kapitel 2.2 genannten Sperrgründe vornehmen und ein neues Zertifikat beantragen.

3 Weitere Bestimmungen und Regelungen

3.1 Anwendbare Policy und 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)

3.2 CP und CPS

Es gelten die Regelungen der zugehörigen Certificate Policy und des Certificate Practice Statement in der zum Zeitpunkt der Zertifikatsbeantragung aktuellen Version:

- Telekom Security CP
- Telekom Security CPS Public

Beide Dokumente sind unter https://www.telesec.de/de/service/downloads/pki-repository/ verfügbar.

3.3 Aufzeichnung

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.

3.4 Anforderungen an vertrauende Dritte

Vertrauende Dritte sollten

- die Gültigkeit der Zertifikate über die angebotenen Statusdienste gemäß Kap. 4.9.10 und 4.10 des Certificate Practice Statements prüfen,
- die in den Nutzungsbedingungen oder im Zertifikat aufgeführten Beschränkungen zur Nutzung der Zertifikate berücksichtigen,
- alle weiteren Vorsichtsmaßnahmen treffen, die sich für Dritte aus Vereinbarungen oder anderweitigen Vorschriften ergeben.

3.5 Haftungsbeschränkungen

Aussagen zur Haftung finden sich in anzuwendenden Allgemeinen Geschäftsbedingungen der Telekom Security (DT Sec) für IT-Leistungen.
Diese sind hier https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/ einsehbar.

3.6 Verfügbarkeit der bereitgestellten Dienste

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.

4 Kontaktinformation und Verfahren bei Beschwerden und zur Streitbeilegung

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.

Mitgeltende Unterlagen

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

Die Leistungen der Zertifikatsprodukte werden in einer **Leistungsbeschreibung-PCSP** 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 1 - Abkürzungsverzeichnis