Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA

Bitte lesen Sie dieses Leistungs- und Nutzungsbedingungen aufmerksam! Beantragen Sie nur dann ein Zertifikat, wenn Sie diesen Nutzungsbedingungen zustimmen.

Im Falle, dass Sie mit diesen Bedingungen nicht einverstanden sind, dürfen Sie ein Zertifikat weder beantragen, noch akzeptieren oder nutzen.

Diese Leistungs- und Nutzungsbedingungen beziehen sich auf den Antragsteller / Zertifikatsnehmer / autorisierte Person, der/die Zertifikate vom PKI-Service „TeleSec Shared-Business-CA“ innerhalb eines PKI-Mandanten bezieht (beantragt, ausstellt, sperrt, erneuert).

Die Verantwortung für den Betrieb dieser Public Key Infrastructure (PKI) trägt der in Kapitel 2.1 genannte Provider (TSP).

1 Einleitung

1.1 Allgemeines

Der PKI-Service „TeleSec Shared-Business-CA“ stellt Zertifikate für unterschiedliches Verwendungszwecke (Mail, VPN, Server, usw.) aus, basierend auf dem Standard X.509v3. Abhängig von der Nutzung verwendet die „TeleSec Shared-Business-CA“ unterschiedliche Zwischenzertifizierungsstellen (Sub-CA, Intermediate-CA), die hierarchisch einer öffentlichen oder internen Stammzertifizierungsstelle (Root-CA) untersteht.

Dieses Dokument stellt die „Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA“ dar, die im Produktportfolio der Deutschen Telekom Security GmbH enthalten ist.

In der einschlägigen Literatur finden sich für dieses Dokument auch die Begriffe „Nutzungsbedingungen“, „Terms and Conditions“ oder „Terms of Use“.

1.2 Begriffsdefinitionen

Was ist ein Zertifikat?

Ein elektronisches Dokument, das eine digitale Signatur verwendet, um einen für Kryptografische Zwecke erzeugten öffentlichen Schlüssel an eine Identität (z.B. Person, Gerät) zu binden.

Antragsteller / Zertifikatsnehmer / autorisierte Person

Die natürliche oder juristische Person, die ein Zertifikat (oder dessen Erneuerung) beantragt. Ist das Zertifikat einmal ausgestellt, wird der Antragsteller als Zertifikatsnehmer bezeichnet und ist rechtlich durch die Leistungs- und Nutzungsbedingungen gebunden.

Für Geräte ausgestellten Zertifikate ist der Antragsteller die Organisation, die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt, auch wenn das Gerät den eigentlichen Antrag auf das Zertifikat sendet. Häufig werden Geräte-Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.

Schlüsselverantwortlicher

Eine durch den Kunden autorisiert natürliche Person, die verantwortlich ist für die ordnungsgemäße Verwendung (Verteilung, Nutzung und ggf. Sperrung) des Schlüsselpaars und Zertifikat, dass für eine Personen- und Funktionsgruppe oder Gerät ausgestellt wurde.

2 Leistungsbestandteil TeleSec Shared-Business CA

2.1 Kontakte des Trust Service Provider

Der Trust Service Provider (TSP) Deutschen Telekom Security GmbH ist über folgende Kontakte zu erreichen:

Anschrift: Deutschen Telekom Security GmbH
Trust Center & ID Solutions
Untere Industriestraße 20
57250 Netphen
Deutschland
Telefon: +49 (0) 1805-268204 [1]
E-Mail: telesec_support@t-systems.com
Internet: https://www.telesec.de

Zertifikats-Missbrauchsfälle können gemeldet werden über:

Telefon: +49 (0) 1805-268204 [2]
Mail: telesec_support@t-systems.com
Internet: https://www.telesec.de „Kontakt | Zertifikatsmissbrauch melden“

[1] Festnetz: 0,14 EUR/Minute, Mobilfunknetze: max. 0,42 EUR/Minute

[2] Festnetz: 0,14 EUR/Minute, Mobilfunknetze: max. 0,42 EUR/Minute

2.2 Zertifikatstypen, Validierungsprozesse und Schlüsselverwendung

Mit der PKI-Dienstleistung TeleSec Shared-Business-CA bietet Deutschen Telekom Security GmbH eine mandantenfähige Company Public-Key-Infrastruture (PKI) an, mit der der Kunde selbst digitale Zertifikate gemäß des Standards X.509v3 für unterschiedlichste Anwendungen (z.B. E-Mail-Security (S/MIME), VPN, Client-Server-Authentifikation, Microsoft-Domänen-Anmeldung) ausstellen und verwalten (sperren, erneuern) kann.

Folgende Zertifikatstypen werden standardisiert bereitgestellt:

- Benutzer (Schlüsseltrennung Single-, Dual-, Triple-Key)
  - natürliche Personen, Personen- und Funktionsgruppen
- Server
- Mail-Gateway
- Router/Gateway
- Domain-Controller

Abhängig von den jeweiligen Zertifikatstypen bietet die Shared-Business-CA folgende Zertifizierungsstellen zur Verfügung:

Öffentliche Zertifizierungsstelle

- T-TeleSec GlobalRoot Class 2 (RSA, SHA-256, 01.10.2008 – 01.10.2033)
  - TeleSec Business CA 1 (RSA, SHA-256, 29.11.2012 – 29.11.2014)

Unter einer öffentlichen Zertifizierungsstelle, die jährlich einer ETSI-Zertifizierung unterliegt (siehe Kapitel 2.6), können folgende Zertifikatstypen ausgestellt werden:

- Benutzer (Schlüsseltrennung Single-, Dual-, Triple-Key (außer SmartCard-LogOn)
- Server
- Mail-Gateway

Interne Zertifizierungsstelle

- Deutsche Telekom Internal Root CA 1(RSA, SHA-1, 15.11.2007 – 15.11.2027)
  - Internal Business CA 2 (RSA, SHA-256, 11.02.2014 – 15.11.2027)
  - Business CA (RSA, SHA-1, 08.11.2011 – 09.11.2023)

- Deutsche Telekom Internal Root CA 2 (RSA, SHA-256, 03.08.2017 – 03.08.2039)
  - Internal Business CA 3 (RSA, SHA-256, 03.08.2017 – 03.08.2029
  - Internal Business CA 5 (RSA, SHA-256, 10.09.2019 – 10.09.2031

Alle o.g. Zertifikatstypen können unter einer internen Zertifizierungsstelle der Deutschen Telekom Security GmbH ausgestellt werden.

Die Zertifikatserweiterungen „Schlüsselverwendung“ und „Erweiterte Schlüsselverwendung“ als auch „Gültigkeitszeitraum“ der Zertifikate ist abhängig vom Zertifikatstyp und den Vorgaben/Regelungen (z.B. Root-Programme der Betriebssystem- und Browserhersteller, Baseline Requirements des CA/Browser-Forums) für den Betrieb öffentlicher Zertifizierungsstellen.

Alle o.g. Zertifikate unterstützen die Schlüsselverwendung, die zur Erstellung einer digitalen Signatur und Verschlüsselung notwendig sind. Als „Erweiterte Schlüsselverwendung“ stehen, abhängig vom Zertifikatstyp, Secure E-Mail, Client-Authentifikation, Server-Authentifikation und Smartcard-LogOn zur Verfügung.

Die Gültigkeit von Zertifikaten, die von einer öffentlichen Zertifizierungsstelle ausgestellt werden, beträgt maximal 36 Monate. Eine Ausnahme gilt für Server-Zertifikate mit einer maximalen Gültigkeit von 13 Monaten ab dem Ausstellungsdatum 01.09.2020.

Der Gültigkeitszeitraum von Zertifikaten, die von einer internen Zertifizierungsstelle ausgestellt werden, beträgt maximal 60 Monate.

Der Zertifikatsverwaltungsprozess (Ausstellung, Erneuerung und Sperrung) aller Zertifikatstypen, der Validierungsprozess als auch Schlüsselverwendungen sind ausführlich in der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) dargestellt.

Das aktuell gültige Dokument als auch alle bisherigen Versionen sind im Internet abrufbar unter: https://www.telesec.de/de/service/downloads/pki-repository/

2.3 Verfügbarkeit des Dienstes

Die im Trust Center installierte Infrastruktur des PKI-Dienstes Shared-Business-CA besteht aus den Komponenten

- Zertifizierungsinstanz (CA), die über ein Web-Portal im Internet erreichbar ist,
- LDAP-Verzeichnisdienst, zum Abruf von Sperrlisten (CRL, ARL), Endteilnehmer-Zertifikaten (sofern diese veröffentlicht werden sollen) und CA- und Root-CA-Zertifikaten,
- Online-Valierungsdienst OCSP, und
- Mail-Server.

Verfügbarkeit der Zertifizierungsinstanz und Web-Server

- Die Zertifizierungsinstanz und Web-Server stehen im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Verzeichnisdienst steht im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Online-Validierungsdienst steht im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Mail-Server steht im monatlichen Mittel zu 98,0% zur Verfügung.

2.4 Datenschutzrichtlinie

Innerhalb der Shared-Business-CA muss Deutschen Telekom Security GmbH zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten.

Sollen von der Deutschen Telekom Security GmbH besondere Kategorien personenbezogener Daten im Sinne Artikel 9 Datenschutz-Grundverordnung (DSGVO) [EU-DSGVO] ver-

arbeitet werden, hat der Kunde die Deutschen Telekom Security GmbH hierüber unverzüglich schriftlich zu unterrichten.

2.4.1 Protokollereignisse

Es ist im Loggingkonzept festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden.

Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden und wie sie vor Verlust und unbefugtem Zugriff geschützt werden.

Es werden dabei die Anforderungen aus [ETSI EN TSP] Kapitel 2.4.2 umgesetzt.

In der Zertifikatshistorie werden alle relevanten Ereignisse von der Antragstellung über die Registrierung, die Prüfungen durch den TSP, die Produktion bis zur Freischaltung und ggf. der Sperrung erfasst und Integritätsgeschützt abgelegt.

2.4.2 Datenarchivierung

2.4.2.1 Art der archivierten Datensätze

Deutschen Telekom Security GmbH archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener oder elektronischer Form (z.B. Angebote, Aufträge) einer erstmaligen Zertifikatsbeantragung und ggf. bei Zertifikatserneuerungen,
- Informationen in Zertifikatsanträgen (Historie) und zum Zertifikatslebenszyklus (z.B. Sperr- und Erneuerungsanträge),
- Soft-PSE, die über Bulk beantragt wurden,
- Soft-PSE des Verschlüsselungs-Zertifikats, das bei Smartcard-Personalisierung (nur Triple-Key) generiert wurden,
- alle Audit-Daten/History-Daten/Logging-Dateien, die gemäß Kapitel 2.4.1 erfasst werden.

2.4.2.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommener Sperrungen, werden sieben (7) Jahre nach Ablauf der Zertifikatsgültigkeit vorgehalten, dies gilt auch für Zertifikatserneuerungen.
- Audit-, History- und Event-Logging Daten werden bis zu zweiundvierzig (42) Tage archiviert.

2.5 Abgrenzung des Vertrauensbereichs

Deutschen Telekom Security GmbH setzt keine Vertrauensgrenzen für die von ihr ausgestellten Zertifikate.

2.6 Auditierung

Die TeleSec Shared-Business-CA wird durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319 411-1, policy OVCP und policy NCP) unterzogen. Zertifizierungsgegenstand sind die PKI-Infrastruktur als auch alle Prozesse, die zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (TeleSec Business CA 1) dienen.

Deutschen Telekom Security GmbH führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durch.

2.7 Haftungsausschluss, Haftungsbeschränkungen

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf eine vorsätzliche Pflichtverletzung zurückzuführen sind, haftet die Zertifizierungsstelle unbegrenzt.

Im Übrigen wird die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen, sind in der aktuellen Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) in Kapitel 9.7 und 9.8, Allgemeine Geschäftsbedingungen (AGB) TeleSec-Produkte oder einzelvertraglich geregelt.

2.8 Anwendbare und vertragliche Vereinbarungen

Im Internet sind unter den Links

https://www.telesec.de/de/service/downloads/pki-repository/

https://www.telesec.de/de/service/downloads/produkte-und-loesungen/

folgende Dokumente und Dateien abrufbar:

- Dieses Dokument (Leistungs- und Nutzungsbedingungen der TeleSec Shared-Business-CA)

- Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) (Repository, aktuelle Fassung und Vorläuferversionen)
- PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS))
- Leistungsbeschreibung
- Allgemeine Geschäftsbedingungen (AGB) TeleSec-Produkte
- Alle Zertifikate der Stamm- und Zwischenzertifizierungsstelle (Root- und Sub-CAs)
- Alle aktuellen Zertifikatssperrlisten (CRLs) und Sperrlisten der Zertifizierungsstellen (CARLs)

2.9 Anwendbares Recht, Beschwerden und Streitbeilegung

2.9.1 Allgemeines

Es gilt deutsches Recht. Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei. Gerichtsstand ist der Sitz der Deutschen Telekom Security GmbH in Bonn.

2.9.2 Außergerichtliche Streitbeilegung (Beilegung einer Streitigkeit)

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei.

3 Verpflichtung des Zertifikatteilnehmers

Der Antragsteller oder Zertifikatsnehmer, die autorisierte Person oder der Schlüsselverantwortliche, der ein oder mehrere Zertifikate für einen Endteilnehmer oder ein Gerät beantragt und verwaltet, verpflichten sich:

- Die Angaben im Zertifikatsantrag einer natürlichen Person vollständig und korrekt anzugeben, Name und Titel sind entsprechend einem gültigen Identitätsnachweis oder einer sonstigen integren Datenquelle nachzuweisen. Im Falle von Personen- und Funktionsgruppen oder Geräten erfolgt die Zertifikatsbeantragung durch autorisierte Personen oder Schlüsselverantwortliche.
- Zu überprüfen, dass die im Endteilnehmer-Zertifikat aufgenommenen Zertifikatsinhalte der Wahrheit entsprechen.
- Das ausgestellte Zertifikat bzw. die ausgestellten Zertifikate ausschließlich bestimmungsgemäß und für autorisierte und legale Zwecke zu verwenden, die den Regelungen der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) des PKI-Service Shared-Business-CA entsprechen.

- Keinen Zertifikatsmissbrauch zu betreiben und nicht den Regelungen der o.g. CP/CPS zu widersprechen.
- Die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der o.g. CP/CPS beschriebenen Pflichten entstehen.
- Die Schlüssel und Zertifikate nur in den zulässigen Anwendungen einzusetzen, die Anwendung muss dabei den im Zertifikat eingetragenen Schlüsselverwendungen genügen.
- Das bzw. die Zertifikate nicht mit Anwendungen oder Maschinen zu nutzen, deren Funktionen unbekannt, verdächtig oder unzuverlässig erscheint.
- Den privaten Schlüssel angemessen und vor unberechtigtem Zugriff durch Dritte zu schützen und nicht weiterzugeben, insbesondere die Anforderungen an technische Schutzmaßnahmen des privaten Schlüssels umzusetzen. Im Falle von privaten Schlüsseln von juristischen Personen oder Geräten erfolgt der Schutz durch autorisierte Personen und Schlüsselverantwortliche.
- Das jede digitale Signatur mit dem privaten Schlüssel erstellt wird, die zum im Zertifikat zugehörigen öffentlichen Schlüssel passt und dem Endteilnehmer eindeutig zugeordnet werden kann.
- Dass jede digitale Signatur mit dem Schlüsselmaterial eines gültigen und nicht gesperrten Zertifikats erfolgt.
- Tatsächlich als Endteilnehmer zu agieren und mit seinem privaten Schlüssel, dem der im Zertifikat enthaltene öffentliche Schlüssel zugeordnet ist, keine CA-Funktionalitäten durchzuführen, wie z.B. Signatur von Zertifikaten oder Sperrlisten.
- In gewissen Zeitabständen die PINs der Smartcard oder bei der sicheren Nutzung des privaten Schlüssels eines Software-Zertifikats das Passwort zu ändern.
- Bei dem Verdacht, dass jemand Kenntnis über eine PIN oder Passwort erlangt hat, die PIN bzw. Passwort sofort zu ändern.
- Den privaten Schlüssel nach Ablauf der Gültigkeit oder der Sperrung des Zertifikates nicht mehr zu nutzen, außer zur Entschlüsselung.
- Bei Verlust, Verdacht der Kompromittierung oder Manipulation des privaten Schlüssels und/oder PINs, wesentliche Änderungen des Zertifikatsangaben, Einstellung der Zertifikatsnutzung (z.B. Vertragskündigung) oder Missbrauchsvermutung eine Sperrung des entsprechenden Endteilnehmer-Zertifikat zu veranlassen bzw. selbst durchzuführen.
- Bei Kompromittierung des privaten Schlüssels ist die Verwendung des privaten Schlüssels des Zertifikatsinhabers unmittelbar und dauerhaft einzustellen.
- Das Zertifikat nicht mehr zu nutzen, wenn bekannt wird, dass das Zertifikat der Zertifizierungsstelle kompromittiert wurde.

3.1 Unzulässige Verwendung von Zertifikaten

Zertifikate der SBCA dürfen nicht im Rahmen folgender Zwecke verwendet werden:

- Steuerungs- und Kontrolleinrichtungen in gefährlichen Umgebungen,
- Umgebungen, in denen ein ausfallsicherer Betrieb gefordert ist (z.B. der Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder -kommunikationssystemen,

Luftverkehrs-Kontrollsystemen oder Waffenkontrollsystemen), wobei ein Ausfall zu Schäden (z.B. Personenschäden, Tod, mittleren und schweren Umweltschäden, sonstige Katastrophen) führen kann.

Es ist verboten Endteilnehmer-Zertifikate als CA- oder Root-CA-Zertifikate zu verwenden.

3.2 Empfehlungen

Darüber hinaus wird dem Endteilnehmer empfohlen:

- Den Computer immer auf dem aktuellen Softwarestand zu halten.
- Aktuelle Antiviren- und Firewallsoftware zu nutzen.
- Den Computer durch Passwörter für BIOS, Bildschirmschoner usw. oder mittels Chipkarte vor unberechtigten Zugriff zu schützen.
- Grundsätzlich nur Informationen zu signieren, deren Inhalt vorher geprüft wurde.
- Bei Zweifel an der Erstellung einer elektronischen Signatur, diese vor dem Versand selbst noch einmal nachzuprüfen.

4 Verpflichtungen der vertrauenden Drittpartei (Relying Parties) und Zertifikatsvalidierung

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der Vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

Jeder Vertrauende Dritte sollte daher

- vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen,
- die Gültigkeit des Zertifikats überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie) sowie den Gültigkeitszeitraum und die Sperrinformationen (CRLs oder OCSP) des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit der vorliegenden CP/CPS einsetzen. Deutschen Telekom Security GmbH ist nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich,
- die technischen Verwendungszwecke prüfen, die durch die im Zertifikat angegebenen Attribute „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt sind.

Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

Der Zertifikatsnutzer hier „Zertifikatsnehmer“ genannt, stimmt den in diesem Dokument aufgeführten Pflichten zu und erklärt die oben aufgeführten Anforderungen und Regelungen einzuhalten.

Ort, Datum _____ Unterschrift _____

A Akronyme und Begriffsdefinitionen

AGB	Allgemeine Geschäftsbedingung
BGB	Bürgerliches Gesetzbuch
CA	Certification Authority
CARL	CA-Sperrliste
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
DSGVO	Datenschutz-Grundverordnung
ETSI	European Telecommunications Standards Institute
HTTPS	HyperText Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
NCP	Normalized Certificates Policy
OCSP	Online Certificate Status Protocol
OVCP	Organizational Validation Certificates Policy
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructur
PSE	Personal Security Environment
RA	Registration Authority
RSA	von Rivest, Shamir und Adleman entwickeltes asymmetrisches kryptographisches Verfahren
SHA	Secure Hash Algorithm
TSP	Trust Service Provider
VPN	Virtual Private Network
VSBG	Verbraucherstreitbeilegungsgesetz