Nutzungsbedingungen (Terms of Use)

der

Corporate PKI (cPKI) der Deutschen Telekom AG

Inhaltsverzeichnis

Änderungshistorie / Release Notes

Version	Stand	Autor/Bearbeiter	Änderungen/Kommentar
1.0	20.08.2018	Deutsche Telekom Security	Erste Version
1.0	20.05.2019	Deutsche Telekom Security	Jährliches Review
2.0	14.07.2020	Deutsche Telekom Security	Änderung des Firmennamens und jährliches Review
3.0	05.10.2020	Deutsche Telekom Security	Umformulierungen in Kapitel 3, Behebung eines Aufzählungsfehlers.
4.0	10.11.2021	Deutsche Telekom Security	Jährliches Review und Korrektur von Schreibfehlern

1. ALLGEMEINE HINWEISE

Es gelten die Konzernrichtlinien zur Sicherheit (Konzernrichtlinien IT-/NT-Sicherheit).

Darüber hinaus gilt weiterhin die KBV IT APS 4.0 Anlage 11 „MyCard/cPKI" Version 2.1 (KBV IT APS 4.0 - LINK) und alle weiteren Regeln und Gesetze.
Besondere Beachtung gilt der Einhaltung der eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste, deren Gesetz zur Durchführung dieser Verordnung und von Urheberrechten und Datenschutz.

Durch die Deutsche Telekom AG werden jedem Mitarbeiter der Deutschen Telekom AG, deren Töchter und Beteiligungen, die durch Workplace Services betreut werden, Zertifikate als Arbeitsmittel zur Verfügung gestellt.
Da die Ausstellung und Nutzung der Zertifikate aus einer öffentlichen Zertifizierungsstelle (CA) erfolgt, ist die Einhaltung der hier genannten Nutzungsbedingungen erforderlich und eine Zustimmung erforderlich.

Bitte lesen Sie deshalb diese Nutzungsbedingungen aufmerksam durch! 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 Nutzungsbedingungen beziehen sich auf die Zertifikate, die vom PKI-Service „cPKI" ausgestellt werden.
Die Verantwortung für den Betrieb dieser Public Key Infrastructure (PKI) trägt die

Deutsche Telekom Security GmbH
Trust Center Operations
Untere Industriestraße 20
57250 Netphen, Deutschland
Telefon: +49 (0) 1805-268204
E-Mail: telesec_support@t-systems.com
Intranet und Internet: https://corporate-pki.telekom.de

Auftraggeber für die dieser Public Key Infrastructure (PKI) ist die Deutsche Telekom AG, vertreten durch die
Deutsche Telekom IT GmbH
Landgrabenweg 151
53227 Bonn, Deutschland

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

Die Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319 411-1, policy LCP) unterzogen. Zertifizierungsgegenstand sind alle Prozesse, die zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (Deutsche Telekom secure email CA E03) dienen. T-Systems führt zusätzlich in regelmäßigen Abständen selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durch.

2. BEGRIFFSDEFINITIONEN

Was ist ein Zertifikat?

Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Die Ausstellung der Zertifikate innerhalb der Deutschen Telekom AG erfolgt durch eine offizielle Zertifizierungsstelle, die Certification Authority (CA).
Die Verwendung einer digitale Signatur, bindet unter Nutzung des öffentlichen Schlüssels die Identität (z.B. Person, Gerät) an ein elektronisches Dokument, bzw. Email.

Welche Zertifkatstypen gibt es?

Im Kontext der cPKI werden unter „Endteilnehmer“ alle Zertifikatsnutzer verstanden, für die ein Zertifikat ausgestellt werden kann und selbst keine Rolle einer Zertifizierungsstelle repräsentieren. Diese sind im Einzelnen:

- natürliche Personen (Benutzer, Registratoren, Rolleninhaber, Pseudonym),
- Personen- und Funktionsgruppen,
- juristische Personen (z.B. Stiftungen bürgerlichen Rechts, Körperschaften des Privatrechts wie Aktien Gesellschaften, eingetragene Vereine, Gesellschaften mit beschränkter Haftung, eingetragene Genossenschaften),
- Geräte (z.B. Server, Router, Gateways, Mail-Gateways, Domain-Controller, Firewalls, Roboter oder andere Geräte. Roboter können ggf. wie natürliche Personen agieren).

Antragsteller / Zertifikatnehmer / autorisierte Person

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

Für Geräte ausgestellte Zertifikate ist der Antragsteller die Organisation (Stelle innerhalb der Deutschen Telekom AG), die über das in dem Zertifikat genannte Gerät Kontrolle ausübt bzw. es betreibt, auch wenn das Gerät den Antrag für das Zertifikat eigenständig sendet. In der Regel werden Geräte-Zertifikate über eine autorisierte Person (z.B. Administrator) beantragt und auf der Komponente installiert.

Schlüsselverantwortlicher

Eine durch den Kunden autorisierte natürliche Person, die verantwortlich ist für die ordnungsgemäße Verwendung (Verteilung, Nutzung und ggf. Sperrung) des Schlüsselpaars und der Zertifikate, die für eine Personen- und Funktionsgruppe, juristische Person, Roboter oder Gerät ausgestellt wurden.

3. VERPFLICHTUNG ANTRAGSTELLERS / ZERTIFIKATSNEHMERS / AUTORISIERTE PERSON

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 vor Ausstellung der Zertifikate sind auf Vollständigkeit und Korrektheit durch den Antragsteller zu prüfen. Name und Titel bei natürlichen Personen müssen hierbei einem gültigen amtlichen Identitätsnachweis, wie Personalausweis oder Reisepass, entsprechen und sind auf Verlangen vorzuweisen.
  Weicht der im Zertifikatsantrag angegeben Name vom amtlichen Identitätsnachweis ab, ist das Zertifikat als Pseudonym zu beantragen, d.h. der Vorname ist mit einem vorangestellten PN- kenntlich zu machen.
  Die im Zertifikatsantrag enthalten Daten für natürliche Personen, Pseudonyme, Roboter und Funktions- und Gruppen-Accounts basieren auf dem Corporate Identity und Account Management der DTAG. Diese Daten beruhen wiederum auf SAP HR, der Personalverwaltung der DTAG.
  Daher ist bei Nichtübereinstimmung der Daten im Zertifikatsantrag mit dem gültigen Identitätsnachweis ein Korrekturauftrag bei dem zuständigen Human Resources (HR) zu stellen und der aktuelle Zertifikatsausstellungsprozess abzubrechen.
  Dies gilt auch für Pseudonyme, wenn die Kenntlichmachung als Pseudonym fehlt oder falsch gesetzt ist.
- Im Falle von juristischen Personen, Personen- und Funktionsgruppen oder Geräten erfolgt die Zertifikatsbeantragung durch autorisierte Personen oder Schlüsselverantwortliche.
- Pseudonym, Roboter, Gruppen- oder Funktionsbezeichnungen sind so zu wählen, dass ausgeschlossen ist, dass Namen Berechtigungen suggerieren (wie z.B. Telekom CA), die der Zertifikatsinhaber nicht besitzt. Des Weiteren dürfen keine politischen Parolen, anstößige Namen verwendet werden oder Namen die Markenrechte verletzen.
  Das TrustCenter der DTAG behält sich vor, die Vergabe von Zertifikaten für ein Pseudonym, Roboter, Gruppen- oder Funktions-Accounts abzulehnen. Die Ablehnung bedarf keiner Begründung.
- Für die Namenswahl von Warenzeichen, Markenrechte usw. in Zertifikaten (z.B. Organization Name (O), Organizational Unit Name (OU)) ist eine besondere Sorgfaltspflicht walten zu lassen. Es liegt in der Verantwortung des Antragstellers, bzw. des Mandanten, dass die Namenswahl keine Warenzeichen, Markenrechte usw. oder die Rechte des geistigen Eigentums von Dritten verletzen. Die Zertifizierungsstelle der cPKI ist nicht verpflichtet, solche Rechte zu überprüfen.
- Nach Ausstellung der Zertifikate 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 cPKI entsprechen.
- Keinen Zertifikatsmissbrauch zu betreiben.
- Nutzer von Office und Business Applikationen (Endnutzer) dürfen die Schlüssel und Zertifikate nur in den von der Deutsche Telekom AG zur Verfügung gestellten Anwendungen einsetzen.
- Für nicht durch die Deutsche Telekom AG zur Verfügung gestellten Applikationen und für Administratoren von Anwendungen, Server und Maschinen und sonstigen Geräten gilt, dass Zertifikate nicht mit Anwendungen oder Maschinen genutzt werden dürfen, deren Funktionen unbekannt, verdächtig oder unzuverlässig erscheinen.

- 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, spätestens mit der Erneuerung des Zertifikats.
- 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 der 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.

Weitere wichtige Details zu folgenden Themen

- Zertifikatstypen, Validierungsprozesse und Schlüsselverwendung
- Verpflichtungen der vertrauenden Drittpartei (Relying Parties) und Zertifikatsvalidierung
- Abgrenzung des Vertrauensbereichs
- Haftungsausschluss, Haftungsbeschränkungen
- Verfügbarkeit des Dienstes
- Datenschutzrichtlinie

finden Sie im CP-CPS der Corporate PKI Deutsche Telekom AG
Die aktuelle Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der cPKI als auch Vorgängerversionen dieses Dokuments sind öffentlich im Internet sowie im Intranet abgelegt unter:
https://corporate-pki.telekom.de/cps/cps.htm

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. UMGANG MIT PERSONENBEZOGENEN DATEN IN DER CPKI, DATENSCHUTZKLASSIFIKATION

Innerhalb der cPKI müssen zur Leistungserbringung personenbezogene Daten elektronisch gespeichert und verarbeitet werden.
Die T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß Art. 32 DSGVO sicher.
Entsprechend den Konzernvorgaben der Deutschen Telekom AG wurde für die cPKI ein kombiniertes Sicherheits- und Datenschutzkonzept (SDSK) im Rahmen eines nach Konzernvorgabe obligatorisch durchzuführenden Verfahrens (sogenanntes PSA-Verfahren) erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte für die cPKI zusammen.
Nähere Details finden Sie in den Datenschutzhinweisen der cPKI im Download Bereich der cPKI https://corporate-pki.telekom.de

4.1 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Zertifikatsantragsteller stimmt der Nutzung von personenbezogenen Daten durch die cPKI zu, soweit dies zur Leistungserbringung erforderlich ist.
Für Mitarbeiter der Deutschen Telekom AG, ihrer Töchter und Beteiligungen, sowie für Auftragnehmer, die im Rahmen ihres Beschäftigungs- oder Auftragsverhältnisses die cPKI nutzen, ist die Rechtsgrundlage der innerhalb der cPKI verarbeiteten personenbezogener Daten durch die DSGVO Art. 6 Abs. 1 lit. b sowie durch nationales Recht nach § 26 BDSG „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“ gegeben. Die Nutzung der cPKI und die hierfür erforderliche Verarbeitung von personenbezogenen Daten ist des Weiteren in einer Betriebsvereinbarung innerhalb der Deutschen Telekom AG geregelt.
Ferner dürfen alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden und deren Veröffentlichung durch den Auftraggeber nicht widersprochen wurde.

4.2 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die cPKI wird in der Bundesrepublik Deutschland nach dem Deutschen Bundesdatenschutzgesetz und der DSVGO betrieben und unterliegt auf deren Basis festgelegten gerichtlichen oder verwaltungsmäßigen Prozessen. Die Verpflichtung zur Geheimhaltung vertraulicher Informationen oder personenbezogener Daten entfällt, soweit die Offenlegung kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens bestehen, die zur Offenlegung vertraulicher oder privater Informationen führen könnten, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei hierüber unter Beachtung der gesetzlichen Bestimmungen informieren.

5. ZUSTIMMUNG DER NUTZNUNGSBEDINGUNGEN

Der Zertifikatsnutzer hier „Zertifikatnehmer“ genannt, stimmt den in diesem Dokument aufgeführten Pflichten mit dem Betätigen des Weiter Buttons zu und erklärt die oben aufgeführten Anforderungen und Regelungen einzuhalten.
Werden die Regularien und Pflichten, die sich aus den Nutzungsbedingungen ergeben nicht eingehalten und es ergeben sich hieraus Haftungs- oder Schadensansprüche, greifen im Rahmen der Haftung die in den Arbeitsverträgen enthaltenen Bestimmungen. Für externe Mitarbeiter und Firmen gelten die in den jeweiligen Verträgen enthaltenen Haftungsbestimmungen.

Wichtiger Hinweis:
Das Trust Center der Deutsche Telekom Security GmbH behält sich vor, Zertifikate, bei Vorliegen von mindestens einem der in Kapitel 4.9.1 ff der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) der cPKI aufgeführten Sperrgründe, innerhalb von 24 (vierundzwanzig) Stunden zu sperren.