Deutsche Telekom Corporate PKI (DTAG cPKI)

PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS))

Deutsche Telekom Security GmbH

im Folgenden „**Telekom Security**“ genannt

Version:	4.0		
Revision:	04	**Status:**	Freigegeben
Gültig ab:	01.07.2020	**Klassifizierung:**	Öffentlich
Autor:	Deutsche Telekom Security GmbH, Trust Center Operations		

DEUTSCHE TELEKOM SECURITY GMBH
Hausanschrift: Bonner Talweg 100, 53113 Bonn
Postanschrift: Bonner Talweg 100, 53113 Bonn
Telefon: 0228 181-0 | E-Mail: info@telekom.de | Internet: www.telekom.de/security
Geschäftsführung: Dr. Klaus Schmitz, Thomas Tschersich
Handelsregister: Amtsgericht Bonn HRB 15241, Sitz der Gesellschaft Bonn | USt-IdNr. DE 254595345
WEEE-Reg.-Nr. DE 56768674

Impressum

Herausgeber

Deutsche Telekom Security GmbH
Trust Center Operations
Untere Industriestraße 20
57250 Netphen
Deutschland

Dateiname	Dokumentennummer	Dokumentenbezeichnung
cPKI-Offenlegungspflichten_DE.pdf	4.0	PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS)) der DTAG cPKI

Version	Stand	Status
4.0	30.06.2020	Freigegeben

Ansprechpartner	Telefon / Fax	E-Mail
Deutsche Telekom Security GmbH Trust Center Operations	+49 (0) 1805-268204 1	telesec_support@t-systems.com

Kurzinfo

Dieses Dokument beschreibt die PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS)) der der Corporate PKI Next Generation (cPKI) der Deutschen Telekom AG (DTAG).

DEUTSCHE TELEKOM SECURITY GMBH
Hausanschrift: Bonner Talweg 100, 53113 Bonn
Postanschrift: Bonner Talweg 100, 53113 Bonn
Telefon: 0228 181-0 | E-Mail: info@telekom.de | Internet: www.telekom.de/security
Geschäftsführung: Dr. Klaus Schmitz, Thomas Tschersich
Handelsregister: Amtsgericht Bonn HRB 15241, Sitz der Gesellschaft Bonn | USt-IdNr. DE 254595345
WEEE-Reg.-Nr. DE 56768674

Änderungshistorie / Release Notes

Version	Stand	Autor/Bearbeiter	Änderungen/Kommentar
0.10	03.08.2018	Karl-Heinz Rödel	Initiale Fassung
0.20	03.08.2018	Oliver Stegemann	Qualitätssicherung der Vers. 00.10
1.0	03.08.2018	Karl-Heinz Rödel	Finale Version und Freigabe
1.1	17.04.2019	Karl-Heinz Rödel	Aufnahme zusätzlicher CAs
1.2	17.04.2019	Oliver Stegemann	Qualitätssicherung der Vers. 1.1
2.0	17.04.2019	Karl-Heinz Rödel	Finale Version und Freigabe
2.1	17.10.2019	Karl-Heinz Rödel	Aufnahme zusätzlicher CAs
2.2	18.10.2019	Oliver Stegemann	Qualitätssicherung der Vers. 2.1
3.0	18.04.2019	Karl-Heinz Rödel	Finale Version und Freigabe
3.1	30.06.2020	Karl-Heinz Rödel	Änderung der Firmenbezeichnung und der Adresse der Legaleinheit aufgrund des Betriebsübergangs von der T-Systems International GmbH zur Deutsche Telekom Security GmbH zum 01.07.2020
3.2	30.06.2020	Oliver Stegemann	Qualitätssicherung der Vers. 3.1
4.0	30.06.2020	Karl-Heinz Rödel	Finale Version und Freigabe

Inhaltsverzeichnis

1 EINLEITUNG

Der PKI-Service „cPKI der DTAG“ stellt Zertifikate für unterschiedliches Verwendungszwecke (Mail, VPN, Server, usw.) aus, basierend auf dem Standard X.509v3.

Abhängig von der Nutzung verwendet die „cPKI der DTAG“ unterschiedliche Zwischenzertifizierungsstellen (Intermediat CA), die hierarchisch einer öffentlichen oder internen Stammzertifizierungsstelle (Root-CA) untersteht.

Die Telekom Security-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 AG Issuing CA 01, Deutsche Telekom AG secure email Issuing CA) dienen. T- Systems führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durch.

Dieses Dokument fasst die jeweiligen Kernpunkte der CP/CPS (siehe Kapitel 8) zusammen und dient als Übersicht für Antragsteller und vertrauende Dritte. Zur Gewährleistung der Vergleichbarkeit ist es gemäß ETSI EN 319 411-1 aufgebaut.

2 KONTAKTE DES TSP

Der TSP Telekom Security ist über folgende Kontakte zu erreichen:

Anschrift: Deutsche Telekom Security GmbH
Trust Center Operations
Untere Industriestraße 20
57250 Netphen
Deutschland

Telefon: +49 (0) 1805-268204[1]

E-Mail: telesec_support@t-systems.com

Intranet: https://corporate-pki.telekom.de

Internet: https://corporate-pki.telekom.de

Zertifikats-Missbrauchsfälle können gemeldet werden über:

Telefon: +49 (0) 1805-268204[2]

Mail: telesec_support@t-systems.com

Mitarbeiter des DTAG Konzerns können sich auch an die Ihnen bekannten Eingangskanälen der jeweils zuständigen Service Desks sowie an 24h Stunden dem Konzernlagezentrum der DTAG wenden.

[1] Festnetz: 0,14 €/Minute, Mobilfunknetz: max. 0,42 €/Minute

[2] Festnetz: 0,14 €/Minute, Mobilfunknetz: max. 0,42 €/Minute

3 ZERTIFIKATSTYPEN, VALIDIERUNGSPROZESSE UND SCHLÜSSELVERWENDUNG

Mit der PKI-Dienstleistung „cPKI der DTAG“ stellt Telekom Security im Auftrag der DTAG eine Company Public-Key-Infrastructure (cPKI) für digitale Zertifikate gemäß des Standards X.509v3 für unterschiedlichste Anwendungen (z.B. E-Mail- Security (S/MIME), VPN, Client-Server-Authentifikation, Microsoft-Domänen-Anmeldung) bereit. Benutzer-, Gruppen-, und Funktionszertifikate kann dabei die Benutzer oder Autorisierte Personen über das Web-Portal der cPKI und dem Service Desk der DTAG enrollen und verwalten (sperren, erneuern)

Folgende Zertifikatstypen werden standardisiert bereitgestellt:

- Benutzer (Single-Key, z.B. für SmartCard-LogOn)
- Computer
- Mobile Devices
- Server
- Domain-Controller
- Router/Gateway
- Mail-Gateway

Abhängig von den jeweiligen Zertifikatstypen stellt die cPKI folgende Zertifizierungsstellen zur Verfügung:

Öffentliche Zertifizierungsstelle

- T-TeleSec GlobalRoot Class 2 (RSA, SHA-256, 01.10.2008 – 01.10.2033 23:59:59 (GMT))
  - Deutsche Telekom AG secure email CA E02 (RSA, SHA-256, 25.02.2020 – 25.02.2030 23:59:59 (GMT))
  - Deutsche Telekom AG secure email CA (RSA, SHA-256, 09.04.2019 – 09.04.2029 23:59:59 (GMT))
  - Deutsche Telekom AG secure email CA (RSA, SHA-256, 18.01.2018 – 18.01.2028 23:59:59 (GMT))
  - Deutsche Telekom AG Issuing CA 01 (RSA, SHA-256, 13.07.2016 – 13.07.2026 23:59:59 (GMT))

Interne Zertifizierungsstelle

- Deutsche Telekom Internal Root CA 1(RSA, SHA-1, 15.11.2007 – 15.11.2027 23:59:59 (GMT))
  - Deutsche Telekom AG Issuing CA 02 (RSA, SHA-256, 29.11.2016 – 29.11.2026 23:59:59 (GMT))
  - Deutsche Telekom AG Issuing CA 02 (RSA, SHA-256, 13.07.2016 – 13.07.2026 23:59:59 (GMT))
  - Deutsche Telekom AG Issuing CA 03 (RSA, SHA-256, 13.07.2016 – 13.07.2026 23:59:59 (GMT))
  - Deutsche Telekom AG Issuing CA 03 (RSA, SHA-256, 14.01.2010 – 14.01.2026 23:59:59 (GMT))
- Deutsche Telekom Internal Root CA 2 (RSA, SHA-256, 03.08.2017 – 03.08.2037 23:59:59 (GMT))
  - Deutsche Telekom AG mobile device CA (RSA, SHA-256, 09.04.2019 – 09.04.2029 23:59:59 (GMT))
  - Deutsche Telekom AG mobile device CA (RSA, SHA-256, 18.01.2018 – 18.01.2028 23:59:59 (GMT))

- Deutsche Telekom AG authentication CA (RSA, SHA-256, 08.06.2019 – 08.06.2029 23:59:59 (GMT))
- Deutsche Telekom AG infrastructure CA (RSA, SHA-256, 08.06.2019 – 08.06.2029 23:59:59 (GMT))

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

Unter einer öffentlichen Zertifizierungsstelle, die jährlich einer ETSI-Zertifizierung unterliegt (siehe Kapitel 13), können folgende Zertifikatstypen ausgestellt werden:

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

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://corporate-pki.telekom.de/cps/cps.htm

Eine Zertifikatssperrung der og. Typen unter den öffentlichen CAs erfolgt über den für Ihren Organisationsbereich zuständigen Service Desk der DTAG.

Sperraufträge von Zertifikaten aus einer internen CA nimmt der Kontakt des TSP (siehe Kapitel 2) entgegen.

4 ABGRENZUNG DES VERTRAUENSBEREICHS

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

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.

Die Papierdokumente und elektronisch erfassten Antrags- und Zertifikatsdaten sowie die Daten der Zertifikatshistorie werden über die Zertifikatsgültigkeit hinaus weitere zehn Jahre zzgl. einer Karenzzeit archiviert. Bei einer Zertifikatserneuerung verlängert sich die Aufbewahrungsfrist der ursprünglichen Dokumente und Daten entsprechend.

Gleiche Vorgaben gelten für die externe Registrierungsstelle, die beim Kunden etabliert sind.

5 VERPFLICHTUNG DES ZERTIFIKATTEILNEHMERS

Die Verpflichtungen der Endteilnehmer sind im Dokument „Nutzungsbedingungen der cPKI“ aufgeführt.

Das aktuell gültige Dokument als auch alle bisherigen Versionen sind im Intranet und Internet unter https://corporate-pki.telekom.de/downloads.html abrufbar

6 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. Telekom Security 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.

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 in der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) oder einzelvertraglich geregelt.

8 ANWENDBARE UND VERTRAGLICHE VEREINBARUNGEN

Im Internet sind unter dem Link https://corporate-pki.telekom.de/downloads.html folgende Dokumente abrufbar:

- PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS)),
- Nutzungsbedingungen (Terms of Use),
- Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) (Repository, aktuelle Fassung und Vorläuferversionen)

9 VERFÜGBARKEIT DES DIENSTES

Die im Trust Center installierte Infrastruktur des PKI-Dienstes cPKI besteht aus den Komponenten

- Zertifizierungsinstanz (CA), die über ein Web-Portal im Intranet erreichbar ist,
- Zertifikats LifeCycle Management System, das über ein Web-Portal im Intranet erreichbar ist,
- LDAP-Verzeichnisdienst im Intranet und Internet, zum Abruf von Sperrlisten (CRL, ARL) sowie der öffentlichen CA- und Root-CA- Zertifikaten
- LDAP-Verzeichnisdienst im Intranet, zum Abruf von Sperrlisten (CRL, ARL), Endteilnehmer- Zertifikaten, 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.

10 DATENSCHUTZRICHTLINIE

Innerhalb der cPKI muss Telekom Security zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten.

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.

Die Telekom Security stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß Art. 32 DSGVO sowie nach nationales Recht § 64 BDSG sicher.

Entsprechend den Konzernvorgaben der Deutschen Telekom AG wurde für die cPKI ein Datenschutzkonzept im Rahmen eines obligatorisch durchzuführenden Verfahrens (sogenanntes PSA-Verfahren) erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte für die cPKI zusammen.

Nähere Informationen zum Datenschutz kann den Datenschutzhinweisen der cPKI entnommen werden. Die Datenschutzhinweise finden Sie im Downloadbereich der cPKI unter https://corporate-pki.telekom.de/de/de/downloads.htmll

11 KOSTENERSTATTUNG

Nicht anwendbar.

12 ANWENDBARES RECHT, BESCHWERDEN UND STREITBEILEGUNG

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 Deutsche Telekom Security GmbH in Bonn.

13 AUDITIERUNG

Zur Prüfung der Konformität wird die Zertifizierungsstelle sowohl durch interne Auditoren als auch durch eine anerkannte Prüfstelle (gemäß [ETSI EN 319 403]) auditiert. Im Rahmen der Audits wird neben der Dokumentation (Sicherheitskonzept, Betriebskonzept sowie weitere interne Dokumente) die Umsetzung der Prozesse und Einhaltung der Vorgaben überprüft.

Zur Gewährleistung der Konformität erfüllt die öffentlichen Zertifizierungsstellen die Anforderungen aus

[ETSI LCP]	ETSI EN 319 411-1 V1.1.1 (2016-02), European Telecommunications Standards Institute, „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, policy LCP
[ETSI EN TSP]	ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

A Weitere Dokumente

- Nutzungsbedingungen (Terms of Use),
- Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) (Repository, aktuelle Fassung und Vorläuferversionen)
- Datenschutzhinweis
- Benutzer-Handbuch für Zertifikatsnehmer der cPKI

B Akronyme und Begriffsdefinitionen

CA	Certification Authority
CP	Certificate Policy
cPKI	Corporate Public Key Infrastructure der DTAG
CPS	Certification Practice Statement
CRL	Certification Revocation List
DTAG	Deutsche Telekom AG
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PDS	PKI Disclosure Statement
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSE	Personal Security Environment
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSP	Trust Service Provider