# Deutsche Telekom Corporate PKI (DTAG cPKI)

## PKI Disclosure Statement (PDS)

Deutsche Telekom Security GmbH

hereinafter referred to as "**Telekom Security**"

|  |  |  |  |
|---|---|---|---|
| **Version:** | 7.0 |  |  |
| **Revision:** | 7.0 | **Status:** | Approved |
| **Valid from:** | 01.02.2023 | **Classification:** | Public |
| **Author:** | Deutsche Telekom Security GmbH, Trust Center Operations |  |  |

**DEUTSCHE TELEKOM SECURITY GMBH**
Address: Bonner Talweg 100, 53113 Bonn | Postal address: Bonner Talweg 100, 53113 Bonn
Phone: +49 228 181-0 | E-mail: info@telekom.de | Internet: www.telekom.de/security
Board of Management: Thomas Tschersich (spokesperson), Dr. Klaus Schmitz
Commercial register: Bonn, local court, HRB 15241, registered office, Bonn | VAT identification no. DE 254595345
WEEE-Reg.-Nr. DE 56768674

# Publication details

**Published by**

Deutsche Telekom Security GmbH
Trust Center & ID Security
Trust Center & ID Operations
Untere Industriestrasse 20
57250 Netphen
Germany

| File name | Document number | Document name |
|---|---|---|
| cPKI Disclosure Statement_7.0_EN.pdf | 7.0 | PKI Disclosure Statement (PDS) of the DTAG cPKI |

| Version | Last revised | Status |
|---|---|---|
| 7.0 | 31.01.2023 | final |

| Contact | Phone/fax | Email |
|---|---|---|
| Deutsche Telekom Security GmbH<br>Trust Center & ID Security<br>Trust Center & ID Operations | +49 1805-268204 1 | telesec_support@t-systems.com |

**Brief summary**

This document describes the PKI Disclosure Statement (PDS) of the Corporate PKI Next Generation (cPKI) of Deutsche Telekom AG (DTAG).

**DEUTSCHE TELEKOM SECURITY GMBH**
Address: Bonner Talweg 100, 53113 Bonn | Postal address: Bonner Talweg 100, 53113 Bonn
Phone: +49 228 181-0 | E-mail: info@telekom.de | Internet: www.telekom.de/security
Board of Management: Thomas Tschersich (spokesperson), Dr. Klaus Schmitz
Commercial register: Bonn, local court, HRB 15241, registered office, Bonn | VAT identification no. DE 254595345
WEEE-Reg.-Nr. DE 56768674

Change history/release notes

| Version | Last revised | Author/editor | Changes/comments |
|---|---|---|---|
| 0.10 | Aug. 3, 2018 | T-Systems International | Initial version |
| 0.20 | Aug. 3, 2018 | T-Systems International | Quality assurance for version 00.10 |
| 1.0 | Aug. 3, 2018 | T-Systems International | Final version and release |
| 1.1 | 17.04.2019 | T-Systems International | Inclusion of additional CAs |
| 1.2 | 17.04.2019 | T-Systems International | Quality assurance for version 1.1 |
| 2.0 | 17.04.2019 | T-Systems International | Final version and release |
| 2.1 | 17.10.2019 | T-Systems International | Inclusion of additional CAs |
| 2.2 | 18.10.2019 | T-Systems International | Quality assurance for version 2.1 |
| 3.0 | 18.04.2019 | T-Systems International | Final version and release |
| 3.1 | 30.06.2020 | T-Systems International | Adjustment of tables 11, 12, 13, 14 due to the change in the CA for pseudonyms, robot accounts, group and function accounts |
| 3.2 | 30.06.2020 | T-Systems International | Quality assurance for version 3.1 |
| 3.3 | 14.07.2020 | Telekom Security | Inclusion of additional CA |
| 3.4 | 14.07.2020 | Telekom Security | Quality assurance for version 3.3 |
| 4.0 | 14.07.2020 | Telekom Security | Released |
| 4.1 | 09.03.2021 | Telekom Security | Delete old revoked CAs |
| 4.2 | 10.03.2021 | Telekom Security | Review and Quality assurance Vers.4.2 |
| 5.0 | 10.03.2021 | Telekom Security | Released |
| 5.1 | 16.02.2022 | Telekom Security | Annual review of Vers.5.0, adjustment CA Name in Chapter 1. |
| 6.0 | 17.02.2022 | Telekom Security | Released |
| 6.1 | 11.01.2023 | Telekom Security | Annual review of Vers.6.0, change Board of Management, adjustment of contact in chapter 2, adjustment of internal CAs in chapter 3, update of audits in chapter 13 |
| 6.2 | 31.01.2023 | Telekom Security | Review and Quality assurance |
| 7.0 | 01.02.2023 | Telekom Security | Released |

# Contents

**Change history/release notes .... 3**

1 Introduction .... 5

2 Contacts of the TSP .... 5

3 Types of certificates, validation processes, and key uses .... 6

4 Delimitation of the confidence area .... 7

5 Obligation of the certificate holder .... 7

6 Obligations of the relying parties and certificate validation .... 7

7 Liability exclusion and limitations .... 8

8 Applicable and contractual agreements .... 8

9 Availability of the service .... 8

10 Data protection policy .... 9

11 Reimbursement of costs .... 9

12 Applicable law, complaints, and settlement of disputes .... 9

13 Auditing .... 10

# 1 INTRODUCTION

The PKI service "cPKI of DTAG" issues certificates for various purposes (email, VPN, server, etc.), based on the X.509v3 standard.

Depending on usage, the "cPKI of DTAG" uses different intermediate certification authorities (intermediate CAs), that are hierarchically subordinated to a public or internal root CA.

Telekom Security processes are subject to a regular annual check (ETSI EN 319 411-1, LCP policy) by independent third parties. All processes are subject to certification that are used for the application, issue, revocation, and renewal of end user certificates in conjunction with a public certification authority (Deutsche Telekom AG secure email Issuing CA03). Telekom Security also performs quality assessment self-audits at regular intervals.

This document summarizes the relevant main points of the CP/CPS (see Section 8) and provides an overview for proposers and relying third parties. It is structured in accordance with ETSI EN 319 411-1 to ensure comparability.

# 2 CONTACTS OF THE TSP

The Telekom Security TSP may be contacted as shown below:

Address: Deutsche Telekom Security GmbH
Trust Center & ID Security
Trust Center & ID Operations

Untere Industriestrasse 20

57250 Netphen

Germany

Phone: +49 1805-268204[1]

Email: telesec_support@telekom.de

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

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

Cases of misuse of certificates can be reported by:

Phone: +49 1805-268204[2]

Email: telesec_support@telekom.de

Employees of the DTAG Group may also apply to the familiar input channels of the relevant responsible service desks and the DTAG Group Situation Center 24 hours a day.

[1] Fixed network: EUR 0.14/minute, mobile network: max. EUR 0.42/minute

[2] Fixed network: EUR 0.14/minute, mobile network: max. EUR 0.42/minute

# 3 TYPES OF CERTIFICATES, VALIDATION PROCESSES, AND KEY USES

With the PKI service "cPKI of DTAG,", Telekom Security on behalf of DTAG provides a company Public Key Infrastructure (cPKI) for digital certificates in accordance with Standard X.509v3 for a wide range of applications (e.g., email security (S/MIME), VPN, client-server-authentication, Microsoft domain registration). The users or authorized persons may enroll and administrate (revoke, renew) user, group, and function certificates via the cPKI web portal and the DTAG service desk.

The following certificate types are provided as standard:

- User (single-key, e.g., for SmartCard LogOn)
- Computers
- Mobile devices
- Server
- Domain controller
- Router/gateway
- Mail gateway

Depending on the respective certificate types, cPKI provides the following certification authorities:

**Public certification authority**

- T-TeleSec GlobalRoot Class 2 (RSA, SHA-256, 01.10.2008 – 01.10.2033 23:59:59 (GMT))
    - Deutsche Telekom AG secure email CA E03 (RSA, SHA-256, 09.07.2020 – 09. 07.2030 23:59:59 (GMT))

**Internal certification authority**

- Deutsche Telekom Internal Root CA 1(RSA, SHA-1, 15.11.2007 – 15.11.2027 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 Internal Root CA 2 (RSA, SHA-256, 03.08.2017 – 03.08.2037 23:59:59 (GMT))
    - Deutsche Telekom AG internal secure email CA (RSA, SHA-256, 25.02.2020 – 25.02.2030 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, 01.12.2020 – 01.12.2030 23:59:59 (GMT))
    - Deutsche Telekom AG infrastructure CA (RSA, SHA-256, 08.06.2019 – 08.06.2029 23:59:59 (GMT))

All of the above certificate types can be issued by an internal Telekom Security certification authority.

The following types of certificate can be issued under a public certification authority, which is subject to ETSI certification every year (see Section 13):

- User (key separation: single key, triple key (except SmartCard LogOn)
- Mail gateway

The certificate management process (issuance, renewal, and revocation) of all certificate types, the validation process, and key uses are described in detail in the Certificate Policy (CP) and Certification Practice Statement (CPS).

The currently valid document and all previous versions are available on the internet at:
https://corporate-pki.telekom.de/cps/cps.htm

A certificate revocation of the above types of public CAs is performed using the DTAG service desk responsible for your organizational area.

The TSP contact (see Section 2) accepts revocation orders of certificates from an internal CA.

# 4 DELIMITATION OF THE CONFIDENCE AREA

Telekom Security sets no confidence limits for the certificates it issues.

The certificate history records and stores with integrity protection all relevant events from request through registration, tests by the TSP, production, activation, and revocation if required

The paper documents and electronically recorded request and certificate data as well as the certificate history data are archived for a further ten years, plus a grace period, beyond the certificate's period of validity. In the case of certificate renewal the storage period for the original documents and data is extended accordingly.

The same requirements apply to the external registration authority that is established at the customer.

# 5 OBLIGATION OF THE CERTIFICATE HOLDER

The obligations of the end users are listed in the document "Terms of Use of the cPKI."

The current valid document and all previous versions are available on the intranet and internet at:
https://corporate-pki.telekom.de/downloads.html.

# 6 OBLIGATIONS OF THE RELYING PARTIES AND CERTIFICATE VALIDATION

Relying parties must have sufficient information and knowledge to be able to evaluate the handling of certificates and their validation. The relying party is responsible for its own decisions regarding whether the information provided is reliable and trustworthy.

Every relying party should therefore

- Check that the information contained in the certificate is correct before using it

- Check that the certificate is valid by validating the entire certificate chain as far as the root certificate (certificate hierarchy) and checking the validity period and revocation information (CRLs or OCSP) of the certificate
- Use the certificate for authorized and legal purposes only in accordance with this CP/CPS. Telekom Security is not responsible for assessing the suitability of a certificate for a specific purpose
- Check the intended technical purposes, which are defined via the attributes "key usage" and "extended key usage" indicated in the certificate

Relying parties must use appropriate software and/or hardware to check certificates (validation) and the associated cryptographic procedures.

# 7 LIABILITY EXCLUSION AND LIMITATIONS

The certification authority will have unlimited liability for damage arising out of injury to life, limb, or health, and damage resulting from willful breaches of obligations.

Apart from that, liability for damage resulting from a breach of obligations due to negligence will be governed by the Certificate Policy (CP) and the Certification Practice Statement (CPS), or by individual agreement.

# 8 APPLICABLE AND CONTRACTUAL AGREEMENTS

The following documents are available on the internet via the link https://corporate-pki.telekom.de:

- PKI Disclosure Statement (PDS)
- Terms of use
- Certificate Policy (CP) and Certification Practice Statement (CPS) (repository, current version, and previous versions)

# 9 AVAILABILITY OF THE SERVICE

The infrastructure of the cPKI PKI service installed in the Trust Center comprises the following components:

- A certification authority (CA) that is accessible via an online web portal
- A certification LifeCycle Management System that is accessible via an intranet web portal
- LDAP directory service on the intranet and internet, for retrieving certificate revocation lists (CRLs, ARLs) and public CA and Root-CA certificates
- LDAP directory service on the intranet, for retrieving certificate revocation lists (CRLs, ARLs), end user certificates, CA and Root-CA certificates
- The OCSP online validation service
- The mail server

Availability of the certification authority and the web server

- As a monthly average, the certification authority and web server are available 98.0 percent of the time.
- As a monthly average the directory service is available 98.0 percent of the time.
- As a monthly average the online validation service is available 98.0 percent of the time.
- As a monthly average the mail server is available 98.0 percent of the time.

# 10 DATA PROTECTION POLICY

Within the cPKI, Telekom Security must store and process personal data electronically in order to provide its services.

The legal basis for the personal data processed within the cPKI for employees of Deutsche Telekom AG, its subsidiaries, and holdings, and for contractors who use the cPKI as part of their employment or contractual relationship is provided by Article 6 (letter 1b) of the GDPR and by national law pursuant to § 26 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz – BDSG*) "Data Processing for Employment Purposes." The use of the cPKI and the processing of personal data required for this are also regulated in a works agreement within Deutsche Telekom AG.

Telekom Security ensures the technical and organizational security and other measures in accordance with Article 32 GDPR and by national law pursuant to § 64 BDSG.

In accordance with the Group requirements of Deutsche Telekom AG, a data protection concept has been created for cPKI within a mandatory procedure to be executed (PSA procedure). This data privacy concept summarizes the aspects of the cPKI that are relevant to data privacy.

More information on data privacy is available in the cPKI Data Privacy information. The Data Privacy information can be found in the cPKI download area at https://corporate-pki.telekom.de/downloads.html.

# 11 REIMBURSEMENT OF COSTS

Not applicable.

# 12 APPLICABLE LAW, COMPLAINTS, AND SETTLEMENT OF DISPUTES

This agreement shall be subject to German law. In the event of disputes, the parties shall come to an agreement taking into account any applicable laws, regulations, and agreements made. The place of jurisdiction is the location of Deutsche Telekom Security GmbH in Bonn.

# 13 AUDITING

In order to check this compliance, the certification authority is audited by both internal auditors as well as by a recognized auditing body (in accordance with ETSI EN 319 403). Besides the documentation (security concept, operating concept, and other internal documents), the implementation of processes and compliance with provisions are reviewed during the course of the audits.

To ensure compliance, the public certification authorities meet the requirements of

[ETSI LCP] ETSI EN 319 411-1 V1.3.1 (2021-05), European Telecommunications Standards Institute, „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, policy LCP

[ETSI EN ESI] ETSI EN 319 403 V2.2.2 (2015-08), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

[ETSI EN TSP] ETSI EN 319 401 V2.3.1 (2021-05), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

# A Other documents

- Terms of use
- Certificate Policy (CP) and Certification Practice Statement (CPS) (Repository, current version and previous versions)
- Data privacy information
- User manual for cPKI certificate holders

# B Acronyms and definition of terms

| | |
|---|---|
| CA | Certification authority |
| CP | Certificate policy |
| cPKI | Corporate Public Key Infrastructure of 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 |