Terms of Use

of the

Corporate PKI (cPKI) of Deutsche Telekom AG

Contents

Contents 1
1. GENERAL INFORMATION 2
2. DEFINITION OF TERMS 3
3. OBLIGATION OF REQUESTER/SUBSCRIBER/AUTHORIZED PERSON 4
4. HANDLING PERSONAL DATA IN THE CPKI, DATA PRIVACY CLASSIFICATION 6
4.1 Notification and consent for the use of confidential data 6
4.2 Disclosure in accordance with legal or administrative processes 6
5. CONSENT TO THE TERMS OF USE 7

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 Fetten (spokesperson), Dr. Klaus Schmitz, Thomas Tschersich
Commercial register: Bonn, local court, HRB 15241, registered office, Bonn | VAT identification no. DE 254595345
WEEE-Reg.-Nr. DE 56768674

1. GENERAL INFORMATION

The Group Security Policy *(Konzernrichtlinien IT/NT-Sicherheit)* applies.

In addition, the Group Works Agreement OS Appendix 11 "MyCard/cPKI" version 2.1 (GWA IT APS 4.0 Appendix 11 – LINK) and all other regulations and laws apply. Particular attention is paid to compliance with the eIDAS Regulation on Electronic Identification and Trust Services, the Act implementing this Regulation and the legislation on copyright and data protection.

Deutsche Telekom AG provides every employee of Deutsche Telekom AG, its subsidiaries and holdings supported by Workplace Services, with certificates as tools of their trade.
Since a public certification authority (CA) issues and uses the certificates, compliance with the Terms of Use stated here is required and consent must be given.

Therefore, please read these Terms of Use carefully. Only request a certificate if you agree to these Terms of Use.
If you do not agree to these Terms of Use you may not request, accept, or use a certificate.

These Terms of Use refer to certificates that are issued by the "cPKI" PKI service.
The party responsible for the operation of this Public Key Infrastructure (PKI) is

Deutsche Telekom Security GmbH
Trust Center Operations,
Untere Industriestrasse 20
57250 Netphen, Germany
Phone: +49 1805-268204
Email: telesec_support@t-systems.com
Intranet and internet: https://corporate-pki.telekom.de

The customer for this Public Key Infrastructure (PKI) is Deutsche Telekom AG, represented by
Deutsche Telekom IT GmbH
Landgrabenweg 151
53227 Bonn, Germany

The PKI service "cPKI" issues certificates for various purposes (email, VPN, server, etc.), based on the X.509v3 standard. Depending on usage, the "cPKI" uses different intermediate certification authorities (intermediate CAs), which are hierarchically subordinated to a public or internal root CA.

T-Systems processes are subject to a regular annual check (ETSI EN 319 411-1, policy LCP) by independent third parties. All processes that are used for the request, issue, revocation, and renewal of end user certificates in conjunction with a public certification authority (Deutsche Telekom secure email CA E03) are subject to certification T-Systems also performs quality assessment self-audits at regular intervals.

2. DEFINITION OF TERMS

What is a certificate?

A digital certificate is a set of digital data that confirms certain qualities of persons or objects. Its authenticity and integrity can be checked using cryptographic procedures. In particular, the digital certificate contains the data required for this check. The certificates are issued within Deutsche Telekom AG by an official certification office, the Certification Authority (CA).
A digital signature uses the public key to tie the identity (e.g., person, device) to an electronic document or email.

What types of certificate exist?

In the context of the cPKI, end entities are understood to be all certificate users to whom a certificate can be issued that do not themselves represent a role of a certification authority. Specifically, these are:

- Natural persons (users, registrars, role owners, pseudonyms)
- Groups of people and functions
- Legal persons (e.g., foundations under civil law, corporations under private law such as stock corporations, registered associations, limited liability companies, registered cooperatives)
- Devices (e.g., servers, routers, gateways, mail gateways, domain controllers, firewalls, robots, or other devices). If necessary, robots can act like natural persons).

Requester/subscriber/authorized person

The natural or legal person who requests a certificate (or its renewal). Once the certificate has been issued, the requester is called "certificate holder" and is legally bound by the terms of use and the Group Works Agreement (GWA).

In the case of certificates issued for devices, the requester is the organization (unit within Deutsche Telekom AG) that controls or operates the device listed on the certificate, even if the device sends the actual certification request. Usually, device certificates are requested via an authorized person (e.g., administrator) and installed on the component.

Key owner

A natural person authorized by the customer who is responsible for the proper use (distribution, use, and, if necessary, revocation) of the key pair and certificates that were issued for a group of persons or functions, legal person, robot, or device.

3. OBLIGATION OF REQUESTER/SUBSCRIBER/AUTHORIZED PERSON

The requester or subscriber, the authorized person, or the key owner who requests and administrates one or more certificates for an end entity or a device undertake

- To check that the information provided by the requester in the certificate request is complete and correct before issuing the certificates. Here the name and title of natural persons must correspond to a valid proof of identity such as a personal identity card or passport and must be demonstrated on request.
  If the name specified in the certificate request differs from the valid proof of identity, the certificate must be requested as a pseudonym, i.e. the first name must be identified by a PN- prefix.
  The data regarding natural persons, pseudonyms, and robots contained in the certificate request is based on the corporate identity and account management of DTAG. This data is based on SAP HR from the HR management at DTAG.
  Therefore, if the data in the certificate request does not match with the valid proof of identity, a correction request must be submitted to your Human Resources (HR) and the current certificate issuing process must be canceled.
  This also applies to pseudonyms if they are not identified as pseudonyms or are set incorrectly.
- Where legal persons, groups of persons and functions, or devices are concerned, the certificate will be requested by authorized persons or key owners.
- Pseudonyms and names of groups or functions must be selected so as to exclude the possibility that names suggest authorizations (such as Telekom CA) that the certificate owner does not possess. In addition, no political slogans, offensive names, or names that might infringe trademark rights may be used.
  The DTAG Trust Center reserves the right to refuse the issue of a pseudonym. The rejection does not require a statement of reasons.
- There is a particular duty to take care when selecting the names of trademarks, trademark rights, etc. in certificates (e.g., Organization Name (O), Organizational Unit Name (OU). It is the responsibility of the requester or client to ensure that the choice of name does not infringe upon any trademarks, trademark rights, etc., or the intellectual property rights of third parties. The cPKI NG certification authority is not obliged to verify such rights. Any resulting claims for damages are at the expense of the requester or client.
- After the certificate has been issued, to check that the certificate contents included in the end entity certificate reflect the truth.
- The certificate(s) issued must be used solely as intended and for authorized and lawful purposes which are in line with the rules of the Certificate Policy (CP) and the Certification Practice Statement (CPS) of the cPKI PKI service.
- To neither misuse the certificate nor act contrary to the rules of the aforementioned CP/CPS.
- To bear the legal consequences arising from non-fulfillment of the obligations described in the aforementioned CP/CPS.
- To use the keys and certificates only in the approved applications; the application must conform to the kinds of key usage set out in the certificate.
- Not to use the certificate(s) with applications or machines whose functions seem to be unknown, suspicious, or unreliable.
- To protect the private key appropriately and against unauthorized access and not to disclose it, and, in particular, to implement the requirements for technical protection measures for the private key. In the case

of private keys of legal persons or devices, the protection is provided by authorized persons and key owners.

- That every digital signature is generated using the private key that corresponds to the public key belonging to the certificate and that can be clearly assigned to the end entity.
- That every digital signature is made with the key material of a valid certificate that has not been revoked.
- To genuinely act as the end entity and not to carry out any CA functions, such as signing certificates or revocation lists, with its private key assigned to the public key contained in the certificate.
- To change the PINs of the smartcard or, where the secure use of the private key of a software certificate is concerned, the password at certain time intervals.
- To change the PIN or password immediately if there is any suspicion that someone may have discovered the PIN or password.
- To stop using the private key upon expiry of the validity of the certificate or upon its revocation, except for decryption.
- If the private key and/or PIN is lost, or if it is presumed to have been compromised or manipulated, if significant changes have been made to the details of the certificate, if its use has been discontinued (e.g., termination of contract), or in the case of presumed misuse, to revoke the end entity certificate in question or to have it revoked.
- In the event that the private key is compromised, use of the certificate owner's private key must cease immediately and permanently.
- To stop using the certificate if it becomes known that the certificate of the certification authority has been compromised.

Other important details on the following topics

- Types of certificates, validation processes, and key uses
- Obligations of the relying parties and certificate validation
- Delimitation of the trust area
- Liability exclusion and limitations
- Availability of the service
- Data protection policy

can be found in the document, CP-CPS_CPKI NG_ DTAG_SecureEmail_DE_20180803_v.3.20.pdf and in the following sections.
The current Certificate Policy (CP) and Certification Practice Statement (CPS) of cPKI, along with previous versions of this document, are stored publicly in the internet and the intranet at:
http://cpki.telekom.de

In addition, the end entity is advised:

- To ensure that the computer's software is up-to-date at all times.
- To use up-to-date anti-virus and firewall software.
- To protect the computer against unauthorized access by using passwords for BIOS, screen savers, etc. or by using a chip card.
- To only ever sign information whose content has been checked beforehand.
- If in doubt about the creation of an electronic signature, to check it once more before sending it.

4. HANDLING PERSONAL DATA IN THE CPKI, DATA PRIVACY CLASSIFICATION

Within the cPKI, personal data must be stored and processed electronically in order to provide services.
T-Systems ensures the technical and organizational security and other measures in accordance with § 32 GDPR.
In accordance with the Group requirements of Deutsche Telekom AG, a security and data protection concept (SDSK) 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 details can be found in the Data Privacy Information of the cPKI in the download area of the cPKI http://cpki.telekom.de

4.1 Notification and consent for the use of confidential data

The certificate requester consents to the use of personal data by a cPKI insofar as this is necessary for service provision purposes.
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 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.
Furthermore, all information that is not to be treated as confidential and for which the customer has not declined publication may be published.

4.2 Disclosure in accordance with legal or administrative processes

In the Federal Republic of Germany, the cPKI is operated in accordance with the German Federal Data Protection Act and the GDPR and is subject to the legal and administrative processes specified on that basis. The obligation not to disclose confidential information or personal data does not apply if disclosure of such information/data has been ordered by force of law or by a court ruling or an administrative authority or serves to implement legal judgments. As soon as there is reason to institute legal or official proceedings, which could lead to confidential or private information being disclosed, the contracting party involved in the proceedings shall inform the other contracting party about this, taking into account the legal provisions.

5. CONSENT TO THE TERMS OF USE

The certificate user, referred to hereunder as the "subscriber," agrees to the obligations stated in this document by clicking on the Next button and confirms that he will comply with the requirements and regulations set out below.

Important note:
T-Systems Trust Center reserves the right to revoke certificates within 24 (twenty-four) hours if at least one of the grounds for revocation listed in Section 4.9.1 et seq. of the Certificate Policy (CP) and the Certification Practice Statement (CPS) applies.