Deutsche Telekom Security GmbH

Terms of Use for public certificates

Version: 1.0

Valid from: 10.01.2023

Status: Release

Last Review: 15.12.2022

Erleben,
was verbindet.

Version History

Version	Date	Changes / Comments
1.0	10.01.2023	Initial version of the common Terms of Use for all public certificates

Table of Content

1 Introduction

This document describes the Terms of Use of Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security) for all certificates below the public Root CAs of Telekom Security, including the Root CAs of T-Systems operated by Telekom Security.
Acceptance of this Terms of Use is a prerequisite for the issuance of any certificate. Acceptance refers only to the requirements relevant to the certificate type requested:

- Requirements that are not marked apply to all certificate types.
- Requirements with annotations in square brackets (e.g., [TLS]) apply only to the certificate types specified in the square brackets.

In addition to the obligations of the subscribers, this document contains further information and the obligations of the relying parties.
The structure of this document is based on the structure of a "PKI Disclosure Statement" (PDS) specified in ETSI EN 319 411-1, but non-applicable sections have been omitted. Also, provisions already made in the relevant General Terms and Conditions (GTC) are not listed again in this document.

2 TSP Contact Info

These Terms of Use are issued by Telekom Security:

- Address: Deutsche Telekom Security GmbH
  Trust Center & ID Security
  Untere Industriestraße 20
  57250 Netphen, Germany
- Email: trustcenter-roots@telekom.de
- Internet: https://www.telesec.de/de/service/kontakt/anfragemitteilung

Misuse reports and key compromises can be submitted via the following contact form:

- Internet: https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

3 Certificate type, validation procedures and usage

3.1 Certificate types

Telekom Security issues certificates of the types [TLS] and [SMIME] below the public Root CAs in the following variants:

- [TLS]:
  - [DV]: Domain validated TLS certificates in accordance with Domain Validation Certificate Policy as per ETSI EN 319 411-1 (DVCP, OID 0.4.0.2042.1.6) as well as the Baseline Requirements of the CA/Browser Forum (OID 2.23.140.1.2.1)
  - [OV]: Organization validated TLS certificates according to the Organizational Validation Certificate Policy as per ETSI EN 319 411-1 (OVCP, OID 0.4.0.2042.1.7) as well as the Baseline Requirements of the CA/Browser Forum (OID 2.23.140.1.2.2)
  - [EV]: Organization validated TLS certificates according to Extended Validation Certificate Policy as per ETSI EN 319 411-1 (EVCP, OID 0.4.0.2042.1.4) as well as the Extended Validation Guidelines of the CA/Browser Forum (OID 2.23.140.1.1)
  - [QEVCP-w] Organization validated qualified TLS certificates according to the Certificate Policy for EU qualified website authentication certificates based on EVCP according to ETSI EN 319 411-2 (QEVCP-w, OID 0.4.0.194112.1.4) as well as the Extended Validation Guidelines of the CA/Browser Forum (OID 2.23.140.1.1)
- [SMIME]:
  - [LCP]: Certificates in accordance with the Lightweight Certificate Policy as per ETSI EN 319 411-1 (LCP, OID 0.4.0.2042.1.3)
  - [NCP]: Certificates according to the Normalized Certificate Policy according to ETSI EN 319 411-1 (NCP, OID 0.4.0.2042.1.1)

3.2 Validation procedures

All information to be included in the certificates is validated by the relevant Registration Authorities.

3.3 Usage

The certificates may only be used for the following applications:

- [DV], [OV]: TLS server and client authentication of TLS-Servers
- [EV], [QEVCP-w]: TLS server authentication of Webservers
- [SMIME]: Certificates for encrypting and/or signing e-mails, files, or other data, as well as client authentication, if applicable

The application must adhere to the key usages specified in the certificates in the attributes keyUsage and extendedKeyUsage.

4 Reliance limits

As far as legally permitted, Telekom Security retains the information and documents recorded during identification and registration as well as the versions of the "Trust Center Certificate Policy" (CP), the "Certification Practice Statement Public" (CPS) and these Terms of Use valid at the time of application for 7 years as evidence of the validations carried out for each certificate.

5 Obligations of subscribers

The subscriber assures

- to provide complete and correct information in the certificate application,
- to notify Telekom Security of any subsequent changes to the information provided at the time of application, which may result in the certificate being revoked and a new certificate being requested,
- in case the keys are generated by the subscriber himself, to generate them in accordance with the requirements for cryptographic algorithms and key lengths valid at the time of the application (see the specifications of the respective service),
- to check the certificate upon receipt and, in the event of incorrect information in the certificate, to report this immediately to Telekom Security. If no such report is made before the certificate is used, the certificate is deemed to be accepted,
- to use the keys and certificates only for the permitted purposes according to Section 3.3 and only in accordance with applicable laws,
- to not use the private key after the expiry of the validity or the revocation of the certificate, as well as upon becoming aware of a compromise of the Certificate Authority, except for the purpose of decryption,

- to protect the private key and its activation data (e.g., PIN, password) appropriately against manipulation and unauthorized access by third parties,
- to appropriately protect any access data received for portals or interfaces for requesting or revoking certificates from manipulation and unauthorized access by third parties, and to change this data or have it changed if compromise is suspected,
- to revoke the certificate or have it revoked immediately if
    - the private key is lost or there is a suspicion of compromise,
    - control over the private key is no longer ensured, e.g., by compromising the password or PIN,
    - significant data in the certificate (e.g., name, organizational unit, domain) has changed,
    - the certificate is not or no longer authorized,
    - a key weakness is proven or the private key no longer meets the cryptographic requirements,
    - there is a violation of these Terms of Use,
- to provide the correct reason when revoking a certificate according to the following list:
    - „keyCompromise“:
      The subscriber's private key is compromised.
    - „cessationOfOperation“:
      The subscriber no longer has control over or is no longer authorized to use the domain names, IP addresses or e-mail addresses specified in the certificate or terminates the use of the certificate or the private key for other reasons.
    - „affiliationChanged“:
      The name of the subscriber or other data in the certificate has changed.
    - „Superseded“ :
      The certificate is replaced by a follow-up certificate and is no longer required.

  In all other cases, "unspecified" must be provided as the revocation reason.
- to accept that Telekom Security may immediately revoke a certificate if one of the above reasons for revocation applies,
- [TLS] to install the certificate only on servers that can be accessed under the names listed in the certificate's subjectAltName attribute.

6 Certificate status checking obligations of relying parties

Telekom Security provides status information for all certificates around the clock in the form of revocation lists and OCSP information; the URLs of the status services are listed in the certificates. Revocation lists are updated and published at least once a day, OCSP responses are generated ad hoc to each request and kept for reuse for a maximum of 2 hours.

Relying parties shall

- verify the validity of the certificate by checking
  - the certificate chain to the Root Certificate,
  - the validity period of the certificate, and
  - the status resp. revocation information (CRLs or OCSP) of the certificate,
- validate the purposes specified in the certificate in the "keyUsage" and "extendedKeyUsage" attributes.

7 Applicable agreements

The issuance and use of certificates is based on

- the Telekom Security Certificate Policy,
- the Telekom Security Certification Practice Statement Public (CPS Public)

The above-mentioned Telekom Security documents as well as these Terms of Use, including their history, are available in the Telekom Security repository: https://www.telesec.de/en/service/downloads/pki-repository/

8 Certifications, trust marks and audit

As evidence of conformity with the applicable policies in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2 (see Section 3.1), Telekom Security is audited both by internal auditors and by independent external auditors.

As part of the audits, in addition to the documentation (CP, CPS, Terms of Use and other internal documents), the implementation of the processes and compliance with the requirements are also audited. A selection of Registration Authorities is also audited in the process.

Audits by external auditors are performed annually and additionally as required. Audits by internal auditors are performed at shorter intervals according to a defined audit plan.