Terms of Use for public certificates

Version 2, valid from 01.11.2024

1 Introduction

This document describes the Terms of Use of Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security) for all certificates issued under the public Root CAs of Telekom Security.

These Terms of Use result from the applicable specifications of the European Telecommunications Standards Institute (ETSI, see https://www.etsi.org/) and the CA/Browser Forum (see https://cabforum.org/):

- ETSI EN 319 401
- ETSI EN 319 411-1
- ETSI EN 319 411-2
- ETSI EN 319 411-6
- Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates [TLS-BR]
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [SMIME-BR]
- Guidelines for the Issuance and Management of Extended Validation Certificates [EV-GL]

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 Contact Info

These Terms of Use are issued by:
Deutsche Telekom Security GmbH
Trust Center & ID Security
Friedrich-Ebert-Allee 71-77
53113 Bonn
E-Mail: trustcenter-roots@telekom.de
Internet: https://www.telesec.de/en/service/contact/anfragemitteilung

Misuse reports and key compromises can be submitted via the following contact form:
https://www.telesec.de/en/service/contact/report-certificate-abuse.

The contact information and interfaces for revoking certificates are listed in the service descriptions of the respective service, see https://www.telesec.de/en/service/downloads/products-and-solutions.

3 Certificate type, validation procedures and usage

3.1 Certificate types

Telekom Security issues TLS and S/MIME certificates issued under the public Root CAs in the following variants:

Type	Form	Policy ETSI	Policy CA/Browser Forum
TLS	[DV] Domain Validated	0.4.0.2042.1.6	2.23.140.1.2.1
	[OV] Organization Validated	0.4.0.2042.1.7	2.23.140.1.2.2
	[EV] Organization Validated according to [EV-GL]	0.4.0.2042.1.4	2.23.140.1.1
	[QEVCP-w] EU-qualified based on [EV]	0.4.0.194112.1.4	2.23.140.1.1
S/MIME Multipurpose	[MV] Mail Validated	0.4.0.2042.1.3	2.23.140.1.5.1.2
	[OV] Organization Validated	0.4.0.2042.1.1	2.23.140.1.5.2.2
	[SV] Sponsor Validated	0.4.0.2042.1.3 or 0.4.0.2042.1.1	2.23.140.1.5.3.2
	[IV] Individual Validated	0.4.0.2042.1.1	2.23.140.1.5.4.2

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:

- [TLS]: Authentication of TLS servers
- [SMIME]: Encrypting and/or signing of 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.

Due to the strict revocation periods that must be complied with (see section 5), certificates may only be used in critical environments if a timely replacement of certificates within the revocation period is guaranteed!

4 Reliance limits

For all certificates, Telekom Security provides status services in the form of revocation lists and OCSP information, at least for the entire certificate validity period. The URLs of the status services are listed in the certificates. Revocation lists are updated and published at least once a day. OCSP information is generated ad hoc for each request and kept for reuse for a maximum of 2 hours.

Telekom Security retains the information and documents recorded during identification and registration as well as the versions of the “Telekom Security Certificate Policy” (CP), the “Certification Practice Statement Public” (CPS) and these Terms of Use valid at the time of application for 7 years after expiry of the certificate as proof of the validations carried out for each certificate.

[QEVCP-w] The following also applies to the provision of status information:

- The status services are also offered beyond the validity of the certificates; details are listed in the service descriptions of the respective services.
- Revoked certificates remain in the relevant revocation list even after they expire; the extension expiredCertsOnCRL is set accordingly in the revocation lists.
- In the OCSP responses, the archiveCutOff extension is set to the “valid from”-date of the issuing CA’s certificate.

5 Obligations of subscribers

5.1 Key generation and protection

The applicant agrees,

- if the keys are generated by the applicant himself, to generate them in accordance with the requirements for cryptographic algorithms and key lengths valid at the time of application (see the specifications of the respective service),
- to adequately protect the private key and its activation data (e.g. PIN, password) against manipulation and unauthorized access by third parties.

5.2 Application

The applicant agrees,

- to provide the information in the certificate application completely and correctly,
- to adequately protect any access data received for portals or interfaces for requesting or revoking certificates against manipulation and unauthorized access by third parties and to change them or have them changed if there is any suspicion of compromise.

5.3 Validation and acceptance of the certificate

The applicant agrees to check the certificate upon receipt and to report any incorrect information in the certificate to Telekom Security immediately. If no such report is made before the certificate is used, the certificate is deemed to be accepted.

5.4 Certificate and key usage

The applicant agrees,

- to use the keys and the certificate only for the permitted purposes in accordance with section 3.3 and only in compliance with applicable laws,
- [TLS] to use the certificate only for servers that can be accessed under the names listed in the subjectAltName certificate attribute,
- [TLS] not to use wildcard certificates for servers with fraudulently misleading sub-domain names,
- [SMIME] to use the certificate only for mailboxes whose addresses are listed in the subjectAltName certificate attribute,
- to immediately cease using the private key (except for decryption if necessary) after the revocation of the certificate or on becoming aware of a compromise of the certification authority.

5.5 Modification of data

The applicant agrees to notify Telekom Security of any subsequent changes to the information provided at the time of application. This may result in the certificate being revoked.

5.6 Revocation of the certificate by the applicant

The applicant agrees to immediately revoke the certificate or have it revoked, using the correct reason for revocation:

- “keyCompromise” if the confidentiality of the private key is no longer guaranteed because the private key has been lost or compromised or there is a suspicion of compromise or control over the private key is no longer ensured, e.g. due to compromise of the password or PIN
- “cessationOfOperation” if the certificate is no longer used
- “affiliationChanged” if the information provided in the certificate has changed
- “superseded” if the certificate is replaced by a subsequent certificate and is no longer needed
- [TLS] “cessationOfOperation” if the applicant no longer controls the domain names or IP addresses specified in the certificate or if the applicant is no longer authorized to use them
- [SMIME] “cessationOfOperation” if the applicant no longer controls the email addresses specified in the certificate or if the applicant is no longer authorized to use them

The applicant also agrees to notify Telekom Security immediately if he/she learns that one of the revocation reasons listed in section 5.7 applies. In this case, the applicant also agrees to revoke the certificate at Telekom Security's instruction, using the reason for revocation stated by Telekom Security.

The applicant may also revoke the certificate or have it revoked at any time without stating reasons, using the revocation reason “unspecified”.

5.7 Revocation of the certificate by Telekom Security

The applicant accepts that Telekom Security may revoke the certificate within one day if it turns out that

- the certificate request was not authorized or is no longer authorized,
- the private key has been compromised or a key weakness is detected,
- [TLS] the validation of the domain name(s) or IP address(es) cannot be trusted,
- [SMIME] the validation of the domain name(s) or mailbox address(es) cannot be trusted.

The applicant accepts that Telekom Security may revoke the certificate within one day or, in justified cases, within 5 days at the latest, if it turns out that

- the applicant has violated the Terms of Use or the CPS,
- the private key no longer meets the cryptographic requirements,
- the data included in the certificate is no longer applicable or may no longer be used,
- the certificate was issued incorrectly by Telekom Security,
- Telekom Security ceases operations,
- [TLS] Telekom Security loses the right to issue public TLS certificates,
- [SMIME] Telekom Security loses the right to issue public S /MIME certificates.

6 Certificate status checking obligations of relying parties

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

Telekom Security is audited annually and additionally as required by independent external auditors to confirm compliance with the applicable specifications (see section 1).

[QEVCP-w]: Information on Telekom Security's qualification status and details of the trusted CA certificates can be found in the “Trusted List Germany”, which can be accessed via the European Commission's eIDAS dashboard, see https://eidas.ec.europa.eu/efda/home.

9 Glossary / List of abbreviations

CA	Certification Authority
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Cerificate Revocation List
ETSI	European Telecommunications Standards Institute
GTC	General Terms and Conditions
OCSP	Online Certificate Status Protocol
PDS	PKI Disclosure Statement
S/MIME	Secure Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
URL	Uniform Resource Locator

10 Imprint

Deutsche Telekom Security GmbH
Friedrich-Ebert-Allee 71-77
53113 Bonn
WEEE-Reg.-Nr. DE 56768674

Compulsory Statement - http://www.telekom.com/compulsory-statement-dtsec