Terms of Use and PDS for public certificates | Nutzungsbedingungen und PDS für öffentliche Zertifikate

Version 3, valid from 05.07.2025 | Version 3, gültig ab 05.07.2025

1 Introduction | Einleitung

This document describes the Terms of Use of Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security)[1] for all certificates under the public Root CAs of Telekom Security and also represents the "PKI Disclosure Statements" (PDS) for the Trust Services for issuing qualified certificates under the public Root CAs of Telekom Security:

- Trust service "Server.ID OV qualified" for issuing certificates of type [QNCP-w],
- Trust service "Server.ID EV qualified" for issuing certificates of type [QEVCP-w],
- Trust service "Client.ID QCP-n" for issuing certificates of type [QCP-n],
- Trust service "Client.ID QCP-l" for issuing certificates of type [QCP-l].

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 these Terms of Use is a prerequisite for the issuance of any certificate. Acceptance refers only to the requirements and specifications relevant to the certificate type requested:

- Requirements and specifications that are not marked apply to all certificate types.
- Requirements and specifications with annotations in square brackets (e.g., [TLS]) apply only to the certificate types specified in the square brackets, [QCP] is used globally to identify EU-qualified certificate types.

Dieses Dokument beschreibt die Nutzungsbedingungen der Deutschen Telekom Security GmbH (nachfolgend Telekom Security genannt)[2] für alle Zertifikate unterhalb der öffentlichen Root-CAs der Telekom Security und stellt zugleich die „PKI Disclosure Statements" (PDS) für die Vertrauensdienste zur Ausstellung der qualifizierten Zertifikate unterhalb der öffentlichen Root-CAs der Telekom Security dar:

- Vertrauensdienst „Server.ID OV qualified" zur Ausstellung von Zertifikaten des Typs [QNCP-w],
- Vertrauensdienst „Server.ID EV qualified" zur Ausstellung von Zertifikaten des Typs [QEVCP-w],
- Vertrauensdienst „Client.ID QCP-n" zur Ausstellung von Zertifikaten des Typs [QCP-n],
- Vertrauensdienst „Client.ID QCP-l" zur Ausstellung von Zertifikaten des Typs [QCP-l].

Diese Nutzungsbedingungen resultieren aus den anwendbaren Spezifikationen des European Telecommunications Standards Institute (ETSI, siehe https://www.etsi.org/) und des CA/Browser-Forums (siehe 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]

Die Akzeptanz dieser Nutzungsbedingungen ist Voraussetzung für die Ausstellung eines jeden Zertifikats und bezieht sich auf alle für den beantragten Zertifikatstyp relevanten Anforderungen und Festlegungen:

- Anforderungen und Festlegungen, die nicht markiert sind, gelten übergreifend für alle Zertifikatstypen.
- Anforderungen und Festlegungen in eckigen Klammern (z.B. [TLS]) gelten nur für die in den eckigen Klammern angegebenen Zertifikatstypen, [QCP] wird dabei übergreifend zur Kennzeichnung von EU-qualifizierten Zertifikatstypen verwendet.

[1] Telekom Security is itself a Trust Service Provider for all Trust Services considered in this document for the issuance of non-qualified certificates and qualified certificates of types [QNCP-w] and [QEVCP-w]. In addition, Telekom Security operates the Trust Services of Deutsche Telekom AG (hereinafter referred to as DTAG) considered in this document for the issuance of qualified certificates of types [QCP-n] and [QCP-l].

[2] Telekom Security ist selbst Vertrauensdiensteanbieter aller in diesem Dokumente betrachteten Vertrauensdienste zur Ausgabe von nicht qualifizierten Zertifikaten sowie von qualifizierten Zertifikaten der Typen [QNCP-w] und [QEVCP-w]. Darüber hinaus betreibt die Telekom Security die in diesem Dokument betrachteten Vertrauensdienste der Deutschen Telekom AG (nachfolgend DTAG) zur Ausgabe von qualifizierten Zertifikaten der Typen [QCP-n] und [QCP-l].

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 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.

Neben den Verpflichtungen der Antragsteller enthält das Dokument weitere Informationen sowie die Anforderungen an die Überprüfung von Zertifikaten durch vertrauende Dritte.

Die Struktur dieses Dokuments ist angelehnt an die in ETSI EN 319 411-1 vorgegebene Struktur eines PDS, nicht anwendbare Kapitel sind jedoch entfallen. Ebenso sind bereits in den relevanten Allgemeinen Geschäftsbedingungen (AGB) getroffene Regelungen in diesem Dokument nicht erneut aufgeführt.

2 Contact Info | Kontaktinformationen

This document is 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

Dieses Dokument wird herausgegeben von:
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/de/service/kontakt/anfragemitteilung

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

Missbrauchsmeldungen und Schlüssel-Kompromittierungen können über folgendes Kontaktformular eingereicht werden:
https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden

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.

Die Kontaktinformationen und Schnittstellen zur Sperrung von Zertifikaten sind in den Leistungsbeschreibungen des jeweiligen Services aufgeführt, siehe https://www.telesec.de/de/service/downloads/produkte-und-loesungen.

3 Certificate Types, Validation Procederes and Usage | Zertifikatstypen, Validierungsverfahren und Verwendung

3.1 Certificate Types | Zertifikatstypen

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

Telekom Security stellt unterhalb der öffentlichen Root-CAs folgende TLS- und S/MIME-Zertifikatstypen aus:

Type | Typ	Form | Ausprägung[3]	Policy ETSI	Policy CA/Browser Forum
TLS	[DV] Domain validated	0.4.0.2042.1.6	2.23.140.1.2.1
	[OV] Organisation validated	0.4.0.2042.1.7	2.23.140.1.2.2
	[EV] Extended 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
	[QNCP-w] EU qualified based on [OV]	0.4.0.194112.1.5	2.23.140.1.2.2
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
	[QCP-n] EU qualified based on [IV]	0.4.0.194112.1.0	2.23.140.1.5.4.2
	[QCP-l] EU qualified based on [OV]	0.4.0.194112.1.1	2.23.140.1.5.2.2

[3] Der Übersichtlichkeit halber wird in dieser Tabelle auf die deutsche Übersetzung verzichtet.

3.2 Validation Procedures | Validierungsverfahren

All information to be included in the certificates are validated by the responsible Registration Authorities and/or automated technical verifications in accordance with the specifications applicable to the respective certificate types.

Alle in die Zertifikate aufzunehmenden Informationen werden durch die zuständigen Registrierungsstellen und/oder automatisierte technische Prüfungen gemäß den für die jeweiligen Zertifikatstypen geltenden Vorgaben validiert.

Applicants and, where applicable, other persons to be identified in the application process are identified in accordance with the specifications applicable to the respective certificate types.

Antragsteller und ggf. weitere im Antragsprozess zu identifizierende Personen werden, sofern anwendbar, gemäß den für die jeweiligen Zertifikatstypen geltenden Vorgaben identifiziert.

Further details on the validation procedures are described in Chapter 4.2.1 of the [CPS][4].

Weitere Details zu den Validierungsverfahren sind in Kapitel 4.2.1 des [CPS][4] beschrieben.

3.3 Usage | Verwendungszwecke

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)
- [QCP-n] Generation of electronic signatures
- [QCP-l] Generation of electronic seals

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

Die Zertifikate dürfen nur für folgende Anwendungen genutzt werden:

- [TLS]: Authentifizierung von TLS-Servern
- [SMIME]: Verschlüsselung und/oder Signatur von E-Mails, Dateien oder sonstigen Daten, sowie ggf. Client-Authentifizierung
- [QCP-n] Erzeugung elektronischer Signaturen
- [QCP-l] Erzeugung elektronischer Siegel

Die Anwendung muss den in den Zertifikaten eingetragenen Schlüsselverwendungen in den Attributen „keyUsage“ (Schlüsselverwendung) und „extendedKeyUsage“ (erweiterte Schlüsselverwendung) genügen.

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

Aufgrund der unbedingt einzuhaltenden Sperrfristen (siehe Kap. 5) dürfen die unter diese Bedingungen fallenden Zertifikate nur dann in kritischen Umgebungen verwendet werden, wenn ein rechtzeitiger Austausch von Zertifikaten innerhalb der Sperrfrist gewährleistet ist!

4 Reliance Limits | Vertrauensgrenzen

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 stellt für alle Zertifikate, mindestens über den gesamten Zeitraum ihrer Gültigkeit, rund um die Uhr Statusdienste in Form von Sperrlisten und OCSP-Auskünften bereit. Die URLs der Statusdienste sind in den Zertifikaten aufgeführt. Sperrlisten werden mindestens einmal täglich aktualisiert und veröffentlicht. OCSP-Auskünfte werden ad hoc auf jede Anfrage generiert und für maximal 2 Stunden zur Wiederverwendung vorgehalten.

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.

Die Telekom Security bewahrt zum Nachweis der durchgeführten Validierungen zu jedem Zertifikat die im Rahmen der Identifizierung und Registrierung erfassten Informationen und Dokumente sowie die zum Zeitpunkt der Beantragung jeweils gültigen Versionen der „Telekom Security Certificate Policy“ (CP), des „Certification Practise Statements Public“ (CPS) sowie dieser Nutzungsbedingungen für 7 Jahre nach Ablauf des Zertifikats auf.

[4] Certification Practice Statement Public, see Sec. 7 | Certification Practice Statement Public, siehe Kap. 7

[QCP] The following also applies to the provision of status information:

- The status services are also offered beyond the validity of the certificates as follows:
  - [QNCP-w] [QEVCP-w] Availability for at least 2 years after the certificates expire,
  - [QCP-n] [QCP-l] Availability for the entire operational period of the Trust 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.

[QCP] Für die Bereitstellung der Statusinformationen gilt darüber hinaus:

- Die Statusdienste werden auch über die Gültigkeit der Zertifikate hinaus wie folgt angeboten:
  - [QNCP-w] [QEVCP-w] Bereitstellung bis mindestens 2 Jahre nach Ablauf der Zertifikate,
  - [QCP-n] [QCP-l] Bereitstellung über die gesamte Zeit des Betriebs der Vertrauensdienste.
- Gesperrte Zertifikate verbleiben auch nach ihrem Gültigkeitsende in der relevanten Sperrliste, in den Sperrlisten ist dementsprechend die Erweiterung expiredCertsOnCRL gesetzt.
- In den OCSP-Antworten ist die Erweiterung archiveCutOff mit dem Gültigkeitsbeginn des ausstellenden CA-Zertifikats gesetzt.

5 Obligations of Subscribers | Verpflichtungen der Antragsteller

5.1 Key Generation and Protection | Schlüsselgenerierung und Schutz der Schlüssel

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.
- [QCP-n] to keep the key under its sole control,
- [QCP-l] to keep the key under the control of the organization.

Der Antragsteller verpflichtet sich,

- sofern die Schlüssel durch den Antragsteller selbst generiert werden, diese gemäß den zum Zeitpunkt der Antragstellung gültigen Anforderungen an kryptografische Algorithmen und Schlüssellängen (siehe dazu die Vorgaben des jeweiligen Services) zu generieren,
- den privaten Schlüssel und dessen Aktivierungsdaten (z.B. PIN, Passwort) angemessen vor Manipulation und unberechtigtem Zugriff durch Dritte zu schützen,
- [QCP-n] den Schlüssel unter seiner alleinigen Kontrolle zu halten,
- [QCP-l] den Schlüssel unter der Kontrolle der Organisation zu halten.

5.2 Application | Antragstellung

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.

Der Antragsteller verpflichtet sich,

- die Angaben im Zertifikatsantrag vollständig und korrekt anzugeben,
- ggf. erhaltene Zugangsdaten zu Portalen oder Schnittstellen zur Beantragung oder Sperrung von Zertifikaten angemessen vor Manipulation und unberechtigtem Zugriff durch Dritte zu schützen und diese bei Verdacht auf Kompromittierung zu ändern bzw. ändern zu lassen.

5.3 Validation and Acceptance of the Certificate | Prüfung und Akzeptanz des Zertifikats

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 within 14 days after the issuance of the certificate, the certificate is deemed to be accepted.

Der Antragsteller verpflichtet sich das Zertifikat nach Erhalt zu prüfen und im Falle falscher Angaben im Zertifikat dieses unverzüglich der Telekom Security zu melden. Wenn keine entsprechende Meldung innerhalb von 14 Tagen nach Ausstellung des Zertifikats erfolgt, gilt das Zertifikat als akzeptiert.

5.4 Certificate and Key Usage | Verwendung des Zertifikats und der Schlüssel

The applicant agrees,

- to use the keys and the certificate only for the permitted purposes in accordance with Sec. 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.

Der Antragsteller verpflichtet sich,

- die Schlüssel und das Zertifikat nur für die zulässigen Verwendungszwecke gemäß Kap. 3.3 und nur in Übereinstimmung mit geltenden Gesetzen zu nutzen,
- [TLS] das Zertifikat nur für Server zu verwenden, auf die unter den im Zertifikatsattribut subjectAltName aufgeführten Namen zugegriffen werden kann,
- [TLS] Wildcard-Zertifikate nicht für Server mit betrügerisch irreführenden Sub-Domain-Namen zu verwenden,
- [SMIME] das Zertifikat nur für Mailboxen zu verwenden, deren Adressen im Zertifikatsattribut subjectAltName aufgeführt sind,
- den privaten Schlüssel nach Sperrung des Zertifikates oder bei Bekanntwerden einer Kompromittierung der Zertifizierungsstelle nicht weiter zu nutzen, außer ggf. zur Entschlüsselung.

5.5 Modification of data | Änderung von Daten

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.

Der Antragsteller verpflichtet sich, nachträgliche Änderungen an den bei Antragstellung gemachten Angaben der Telekom Security mitzuteilen. Hieraus kann eine Sperrung des Zertifikats resultieren.

5.6 Revocation of the Certificate by the Applicant | Sperrung des Zertifikats durch den Antragsteller

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

Der Antragsteller verpflichtet sich, das Zertifikat unter Angabe des korrekten Sperrgrundes unverzüglich zu sperren oder sperren zu lassen, wenn einer der folgenden Gründe vorliegt:

- „keyCompromise“, wenn die Vertraulichkeit des privaten Schlüssels nicht mehr gewährleistet ist, weil der private Schlüssel verloren oder kompromittiert ist oder der Verdacht auf Kompromittierung besteht oder die Kontrolle über den privaten Schlüssel nicht mehr sichergestellt ist, z.B. durch Kompromittierung von Passwort oder PIN
- „cessationOfOperation“, wenn das Zertifikat nicht weiter genutzt wird
- „affiliationChanged“, wenn sich im Zertifikat gemachte Angaben geändert haben
- „superseded“, wenn das Zertifikat durch ein Folgezertifikat ersetzt und nicht länger benötigt wird
- [TLS] „cessationOfOperation“, wenn er keine Kontrolle mehr über die im Zertifikat angegebenen Domain Namen oder IP-Adressen hat oder nicht mehr autorisiert ist, diese zu verwenden
- [SMIME] „cessationOfOperation“, wenn er keine Kontrolle mehr über die im Zertifikat angegebenen E-Mail-Adressen hat oder nicht mehr autorisiert ist, diese zu verwenden

The applicant also agrees to notify Telekom Security immediately if he/she learns that one of the revocation reasons listed in Sec. 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.

Der Antragsteller verpflichtet sich darüber hinaus, dass er unverzüglich der Telekom Security meldet, wenn er erfährt, dass einer der in Kapitel 5.7 aufgeführten Sperrgründe vorliegt. In diesem Fall verpflichtet sich der Antragsteller darüber hinaus, auf Anweisung der Telekom Security das Zertifikat unter Angabe des von der Telekom Security genannten Sperrgrundes zu sperren.

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

Der Antragsteller darf darüber hinaus jederzeit ohne Angabe von Gründen das Zertifikat unter Angabe des Sperrgrundes „unspecified“ sperren oder sperren lassen.

5.7 Revocation of the Certificate by Telekom Security | Sperrung des Zertifikats durch 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.

Der Antragsteller akzeptiert, dass Telekom Security das Zertifikat innerhalb eines Tages sperren darf, wenn sich herausstellt, dass

- der Zertifikatsantrag nicht autorisiert war oder nicht mehr autorisiert ist,
- der private Schlüssel kompromittiert wurde oder eine Schlüsselschwäche nachgewiesen wird,
- [TLS] der Validierung des/der Domain-Namen oder IP-Adresse(n) nicht vertraut werden kann,
- [SMIME] der Validierung des/der Domain-Namen oder Mailbox-Adresse(n) nicht vertraut werden kann.

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.

Der Antragsteller akzeptiert, dass Telekom Security das Zertifikat innerhalb eines Tages bzw. in begründeten Fällen spätestens innerhalb von 5 Tagen sperren darf, wenn sich herausstellt, dass

- der Antragsteller gegen die Nutzungsbedingungen oder die CPS verstoßen hat,
- der private Schlüssel nicht mehr den kryptografischen Anforderungen genügt,
- die in das Zertifikat aufgenommenen Daten nicht mehr zutreffen oder nicht mehr verwendet werden dürfen,
- das Zertifikat von der Telekom Security fehlerhaft ausgestellt wurde,
- die Telekom Security den Betrieb einstellt,
- [TLS] die Telekom Security die Berechtigung verliert, öffentliche TLS-Zertifikate auszustellen,
- [SMIME] die Telekom Security die Berechtigung verliert, öffentliche S /MIME-Zertifikate auszustellen.

6 Certificate Status Checking Obligations of Relying Parties | Anforderungen an die Überprüfung des Zertifikatsstatus durch vertrauende Dritte

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.

Vertrauende Dritte sollten

- die Gültigkeit des Zertifikats validieren durch die Prüfung
  - der Zertifikatskette bis zum Wurzelzertifikat,
  - der Gültigkeitsdauer des Zertifikats sowie
  - der Status- bzw. Sperrinformationen (CRLs oder OCSP) des Zertifikats,
- die im Zertifikat in „keyUsage“ und „extendedKeyUsage“ angegebenen Verwendungszwecke prüfen.

[QCP] When checking the certificate chain, it must be verified that the issuing CA is listed with a corresponding entry in the EU Trusted List (“Trusted List Germany”, see also Sec. 9).

[QCP] Bei der Prüfung der Zertifikatskette muss geprüft werden, dass die ausstellende CA mit einem entsprechenden Eintrag in der EU Vertrauensliste („Trusted List Germany“ siehe dazu auch Kap. 9) aufgeführt ist.

7 Applicable Agreements | Anwendbare Vereinbarungen

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/

In addition, the General Terms and Conditions (GTC) relevant to the respective Trust Services apply, which can be accessed via the Telekom Security website: https://www.telesec.de/en/service/downloads/terms-of-service

Die Ausstellung und Nutzung der Zertifikate basiert auf
- der Telekom Security Certificate Policy [CP] sowie
- dem Telekom Security Certification Practice Statement Public (CPS Public) [CPS].

Die o.g. Dokumente der Telekom Security sowie diese Nutzungsbedingungen und PDS sind inkl. ihrer Historie im Repository der Telekom Security abrufbar: https://www.telesec.de/de/service/downloads/pki-repository/

Darüber hinaus gelten die für die jeweiligen Vertrauensdienste relevanten Allgemeinen Geschäftsbedingungen (AGB), welche über die Web-Seiten der Telekom Security abrufbar sind: https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen.

8 Applicable Law, Complaints and Dispute Resolution | Anwendbares Recht, Beschwerden und Streitbeilegung

German law applies.

In the case of disputes, the parties shall reach an agreement, taking into account made agreements, regulations and applicable laws.

Place of jurisdiction is the seat of Deutsche Telekom Security GmbH in 53113 Bonn, Germany.

Es gilt deutsches Recht.

Im Falle von Streitigkeiten treffen die Parteien eine Vereinbarung unter Berücksichtigung der getroffenen Vereinbarungen, Vorschriften und geltenden Gesetze.

Gerichtsstand ist der Sitz der Deutschen Telekom Security GmbH in 53113 Bonn, Deutschland.

9 Certifications, Trust Marks and Audit | Zulassungen, Vertrauenszeichen und Auditierung

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

[QCP]: 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.

Zum Nachweis der Konformität zu den anwendbaren Spezifikationen (siehe Kap. 1) wird die Telekom Security jährlich sowie zusätzlich bei Bedarf durch unabhängige externe Auditoren auditiert.

[QCP]: Informationen über den Qualifizierungsstatus der Telekom Security und der DTAG sowie Details zu den vertrauenswürdigen CA-Zertifikaten sind in der „Trusted List Germany“ zu finden, die über das eIDAS-Dashboard der Europäischen Kommission abzurufen ist, siehe https://eidas.ec.europa.eu/efda/home.

10 Glossary / List of abbreviations | Glossar/Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
CA	Certification Authority
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Cerificate Revocation List
DV	Domain validated
ETSI	European Telecommunications Standards Institute
EV	Extended Organization validated
EV-GL	Guidelines for the Issuance and Management of Extended Validation Certificates
GTC	General Terms and Conditions
IV	Individual validated
OCSP	Online Certificate Status Protocol
OV	Organization validated
PDS	PKI Disclosure Statement
QCP	Qualified Certificate Policy
S/MIME	Secure Multipurpose Internet Mail Extensions
SV	Sponsor validated
TLS	Transport Layer Security
URL	Uniform Resource Locator

11 Imprint | Impressum

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

Pflichtangaben:
http://www.telekom.com/pflichtangaben-dtsec