Nutzungsbedingungen für öffentliche Zertifikate

Version 2, gültig ab 01.11.2024

1 Einleitung

Dieses Dokument beschreibt die Nutzungsbedingungen der Deutschen Telekom Security GmbH (nachfolgend Telekom Security genannt) für alle Zertifikate unterhalb der öffentlichen Root-CAs der Telekom Security.

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:

- Anforderungen, die nicht markiert sind, gelten übergreifend für alle Zertifikatstypen.
- Anforderungen in eckigen Klammern (z.B. [TLS]) gelten nur für die in den eckigen Klammern angegebenen Zertifikatstypen.

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 „PKI Disclosure Statements“ (PDS), nicht anwendbare Kapitel sind jedoch entfallen. Ebenso sind bereits in den relevanten AGB getroffenen Regelungen in diesem Dokument nicht erneut aufgeführt.

2 Kontaktinformationen

Diese Nutzungsbedingungen werden 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

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

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 Zertifikatstypen, Validierungsverfahren und Verwendung

3.1 Zertifikatstypen

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

Typ	Ausprägung	Policy ETSI	Policy CA/Browser Forum
TLS	[DV] Domain-validiert	0.4.0.2042.1.6	2.23.140.1.2.1
	[OV] Organisations-validiert	0.4.0.2042.1.7	2.23.140.1.2.2
	[EV] Organisations-validiert gemäß [EV-GL]	0.4.0.2042.1.4	2.23.140.1.1
	[QEVCP-w] EU-qualifiziert auf Basis [EV]	0.4.0.194112.1.4	2.23.140.1.1
S/MIME Multipurpose	[MV] Mail-validiert	0.4.0.2042.1.3	2.23.140.1.5.1.2
	[OV] Organisations-validiert	0.4.0.2042.1.1	2.23.140.1.5.2.2
	[SV] Sponsor-validiert	0.4.0.2042.1.3 oder 0.4.0.2042.1.1	2.23.140.1.5.3.2
	[IV] Individual-validiert	0.4.0.2042.1.1	2.23.140.1.5.4.2

3.2 Validierungsverfahren

Alle in die Zertifikate aufzunehmenden Informationen werden durch die zuständigen Registrierungsstellen gemäß den Vorgaben validiert.

3.3 Verwendungszwecke

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

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

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

4 Vertrauensgrenzen

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.

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.

[QEVCP-w] Für die Bereitstellung der Statusinformationen gilt darüber hinaus:

- Die Statusdienste werden auch über die Gültigkeit der Zertifikate hinaus angeboten, Details dazu sind in den Leistungsbeschreibungen der jeweiligen Services aufgeführt.
- 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 Verpflichtungen der Antragsteller

5.1 Schlüsselgenerierung und Schutz der Schlüssel

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.

5.2 Antragstellung

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 Prüfung und Akzeptanz des Zertifikats

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 vor Verwendung des Zertifikats erfolgt, gilt das Zertifikat als akzeptiert.

5.4 Verwendung des Zertifikats und der Schlüssel

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 Änderung von Daten

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 Sperrung des Zertifikats durch den Antragsteller

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

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.

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

5.7 Sperrung des Zertifikats durch Telekom Security

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.

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 Anforderungen an die Überprüfung des Zertifikatsstatus durch vertrauende Dritte

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.

7 Anwendbare Vereinbarungen

Die Ausstellung und Nutzung der Zertifikate basiert auf

- der Telekom Security Certificate Policy sowie
- dem Telekom Security Certification Practice Statement Public (CPS Public).

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

8 Zulassungen, Vertrauenszeichen und Auditierung

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.

[QEVCP-w]: Informationen über den Qualifizierungsstatus der Telekom Security 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.

9 Glossar/Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
CA	Certification Authority
CP	Certification Policy
CPS	Certification Practice Statement
CRL	Cerificate Revocation List
ETSI	European Telecommunications Standards Institute
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 Impressum

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

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