Deutsche Telekom Security GmbH

Nutzungsbedingungen für öffentliche Zertifikate

Version: 1.0

Gültig ab: 10.01.2023

Status: Freigegeben

Letztes Review: 15.12.2022

Öffentlich

Erleben,
was verbindet.

Änderungshistorie

Version	Stand	Änderungen/Kommentar
1.0	10.01.2023	Initialversion der übergreifenden Nutzungsbedingungen für alle öffentlichen Zertifikate

Inhaltsverzeichnis

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, incl. der von der Telekom Security betriebenen Root-CAs der T-Systems.
Die Akzeptanz dieser Nutzungsbedingungen ist Voraussetzung für die Ausstellung eines jeden Zertifikats. Die Akzeptanz bezieht sich dabei nur auf die 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 Zertifikatsnehmer enthält das Dokument weitere Informationen sowie die Verpflichtungen der Zertifikatsnutzer (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 jeweils relevanten AGB getroffene Regelungen in diesem Dokument nicht erneut aufgeführt.

2 TSP Kontaktinformationen

Diese Nutzungsbedingungen werden herausgegeben von der Telekom Security:

- Adresse: Deutsche Telekom Security GmbH
  Trust Center & ID Security
  Untere Industriestraße 20
  57250 Netphen, Deutschland
- 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:

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

3 Zertifikatstypen, Validierungsverfahren und Verwendung

3.1 Zertifikatstypen

Telekom Security stellt unterhalb der öffentlichen Root-CAs Zertifikate der Typen [TLS] und [SMIME] in folgenden Ausprägungen aus:

- [TLS]:
  - [DV]: Domain-validierte TLS-Zertifikate gemäß Domain Validation Certificate Policy nach ETSI EN 319 411-1 (DVCP, OID 0.4.0.2042.1.6) sowie den Baseline Requirements des CA/Browser-Forums (OID 2.23.140.1.2.1)
  - [OV]: Organisations-validierte TLS-Zertifikate gemäß Organizational Validation Certificate Policy nach ETSI EN 319 411-1 (OVCP, OID 0.4.0.2042.1.7) sowie den Baseline Requirements des CA/Browser-Forums (OID 2.23.140.1.2.2)
  - [EV]: Organisations-validierte TLS-Zertifikate gemäß Extended Validation Certificate Policy nach ETSI EN 319 411-1 (EVCP, OID 0.4.0.2042.1.4) sowie den Extended Validation Guidelines des CA/Browser-Forums (OID 2.23.140.1.1)
  - [QEVCP-w] Organisations-validierte qualifizierte TLS-Zertifikate gemäß der Certificate Policy für EU-qualifizierte Website-Authentifizierungszertifikate auf Basis EVCP nach ETSI EN 319 411-2 (QEVCP-w, OID 0.4.0.194112.1.4) sowie den Extended Validation Guidelines des CA/Browser-Forums (OID 2.23.140.1.1)
- [SMIME]:
  - [LCP]: Zertifikate gemäß der Lightweight Certificate Policy nach ETSI EN 319 411-1 (LCP, OID 0.4.0.2042.1.3)
  - [NCP]: Zertifikate gemäß der Normalized Certificate Policy nach ETSI EN 319 411-1 (LCP, OID 0.4.0.2042.1.1)

3.2 Validierungsverfahren

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

3.3 Verwendungszwecke

Die Zertifikate dürfen nur für folgende Anwendungen genutzt werden:

- [DV], [OV]: TLS-Server- und Client-Authentifizierung von TLS-Servern
- [EV], [QEVCP-w]: TLS-Serverauthentifizierung von Web-Servern
- [SMIME]: Zertifikate zur 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.

4 Vertrauensgrenzen

Soweit gesetzlich zulässig, bewahrt die Telekom Security 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 „Trustcenter Certificate Policy“ (CP), des „Certification Practise Statement Public“ (CPS) sowie dieser Nutzungsbedingungen für 7 Jahre auf.

5 Verpflichtungen der Antragsteller

Der Zertifikatsnehmer verpflichtet sich

- die Angaben im Zertifikatsantrag vollständig und korrekt anzugeben,
- nachträgliche Änderungen an den bei Antragstellung gemachten Angaben der Telekom Security mitzuteilen, woraus ggf. eine Sperrung des Zertifikats und eine Beantragung eines neuen Zertifikats resultieren kann,
- sofern die Schlüssel durch den Zertifikatsnehmer 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,
- das Zertifikat nach Erhalt zu prüfen und im Falle falscher Angaben im Zertifikat dieses unverzüglich der Telekom Security zu melden. Wenn keine diesbezügliche Meldung vor Verwendung des Zertifikats erfolgt, gilt das Zertifikat als akzeptiert,
- die Schlüssel und Zertifikate nur für die zulässigen Verwendungszwecke gemäß Kap. 3.3 und nur in Übereinstimmung mit geltenden Gesetzen zu nutzen,

- den privaten Schlüssel nach Ablauf der Gültigkeit oder der Sperrung des Zertifikates sowie bei Bekanntwerden einer Kompromittierung der Zertifizierungsstelle nicht mehr zu nutzen, außer zur Entschlüsselung,
- den privaten Schlüssel und dessen Aktivierungsdaten (z.B. PIN, Passwort) angemessen vor Manipulation und unberechtigtem Zugriff durch Dritte zu schützen,
- 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,
- das Zertifikat unverzüglich zu sperren bzw. sperren zu lassen, wenn
    - der private Schlüssel verloren ist oder der Verdacht auf Kompromittierung besteht,
    - die Kontrolle über den privaten Schlüssel nicht mehr sichergestellt ist, z.B. durch Kompromittierung von Passwort oder PIN,
    - sich wesentliche Daten im Zertifikat (z.B. Name, Organisationseinheit, Domain) geändert haben,
    - keine Autorisierung des Zertifikats (mehr) vorliegt,
    - eine Schlüsselschwäche nachgewiesen wird oder der private Schlüssel nicht mehr den kryptografischen Anforderungen genügt,
    - ein Verstoß gegen diese Nutzungsbedingungen vorliegt,
- bei der Sperrung eines Zertifikats den korrekten Sperrgrund gemäß folgender Auflistung anzugeben:
    - „keyCompromise“ (Schlüsselkompromittierung):
      Der private Schlüssel des Zertifikatsnehmers ist kompromittiert.
    - „cessationOfOperation“ (Beendigung der Zertifikatsnutzung):
      Der Zertifikatsnehmer hat keine Kontrolle mehr über die im Zertifikat angegebenen Domain Namen, IP-Adressen oder E-Mail-Adressen oder ist nicht mehr autorisiert diese zu verwenden oder beendet aus anderen Gründen die Nutzung des Zertifikats bzw. des privaten Schlüssels.
    - „affiliationChanged“ (Zugehörigkeit geändert):
      Der Name des Zertifikatsnehmers oder andere Daten im Zertifikat haben sich geändert.
    - „Superseded“ (abgelöst): Das Zertifikat wird durch ein Folgezertifikat ersetzt und nicht länger benötigt.

  In allen anderen Fällen ist „unspecified“ (unspezifiziert) als Sperrgrund anzugeben.
- zu akzeptieren, dass Telekom Security ein Zertifikat sofort sperren darf, wenn einer der o.g. Sperrgründe vorliegt,
- [TLS] das Zertifikat nur auf Servern zu installieren, auf die unter den im Zertifikatsattribut subjectAltName aufgeführten Namen zugegriffen werden kann.

6 Verpflichtungen zur Überprüfung des Zertifikats-status durch vertrauende Dritte (Zertifikatsnutzer)

Telekom Security stellt für alle Zertifikate 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. Jeder Zertifikatsnutzer sollte

- die Gültigkeit des Zertifikats durch Prüfung
  - der Zertifikatskette bis zum Wurzelzertifikat,
  - der Gültigkeitsdauer des Zertifikats sowie
  - der Status- bzw. Sperrinformationen (CRLs oder OCSP) des Zertifikats

  validieren,
- die im Zertifikat in den Attributen „keyUsage“ und „extendedKeyUsage“ angegebenen Verwendungszwecke prüfen.

7 Anwendbare Vereinbarungen

Die Ausstellung und Nutzung der Zertifikate basiert auf

- der Telekom Security Certificate Policy,
- 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 Policies gemäß ETSI EN 319 411-1 bzw. ETSI EN 319 411-2 (siehe Kap. 3.1) wird die Telekom Security sowohl durch interne Auditoren als auch durch unabhängige externe Auditoren auditiert.
Im Rahmen der Audits werden neben der Dokumentation (CP, CPS, Nutzungsbedingungen und weitere interne Dokumente) auch die Umsetzung der Prozesse und die Einhaltung der Anforderungen geprüft, es wird dabei auch stichprobenartig eine zufällige Auswahl von Registrierungsstellen geprüft.
Die Audits durch externe Auditoren erfolgen jährlich sowie zusätzlich bei Bedarf. Die Audits durch interne Auditoren erfolgen in kürzeren Intervallen nach einem festgelegten Auditplan.