Deutsche Telekom Security GmbH

Nutzungsbedingungen V-PKI-CAs

Version: 02.00

Gültig ab: 26.10.2023

Status: Final

Letztes Review: 26.10.2023

Öffentlich

Erleben,
was verbindet.

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen/Kommentar
0.9	04.11.2022	Deutsche Telekom Security GmbH	Initialversion der Nutzungsbedingungen nach Umsetzung TR-03145
1.0	05.12.2023	Deutsche Telekom Security GmbH	Finale Version
02.00	26.10.2023	Deutsche Telekom Security GmbH	Review - Update: Anpassungen in Kap. 5 (Empfehlungen Passwörter)

Inhaltsverzeichnis

1 Einleitung

Die Deutsche Telekom Security GmbH (nachfolgend Telekom Security genannt) betreibt im Auftrag der „Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben“ (BDBOS) in ihrem Trust Center als Trust Service Provider (TSP) die in die „Verwaltungs-PKI“ (V-PKI) des Bundes integrierten Zertifizierungsstellen „Deutschland Online Infrastruktur-Certification Authority“ (DOI-CA) und „Informationsverbund Berlin Bonn-Certification Authority“ (IVBB-CA), (nachfolgend V-PKI-CAs genannt).
Dieses Dokument beschreibt die Nutzungsbedingungen, deren Akzeptanz Voraussetzung für die Ausstellung eines jeden Zertifikats der V-PKI-CAs ist. Neben den Verpflichtungen der Zertifikatsnehmer enthält das Dokument weitere Informationen zu den V-PKI-CAs 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 nicht aufgeführt.

2 TSP Kontaktinformationen

Das Trust Center der Telekom Security ist wie folgt zu erreichen:

- Adresse: Deutsche Telekom Security GmbH
  Trust Center & ID Security
  Untere Industriestraße 20
  57250 Netphen, Deutschland
- E-Mail: trust_center_notary@telekom.de
- Internet: https://www.telesec.de/de/service/kontakt/anfragemitteilung

Die Kontakte zur Beantragung von Zertifikaten (URLs der Webseiten sowie ggf. die Anschriften zum Versand der Papieranträge) sowie die Kontakte der Service-Desks sind in den jeweiligen Benutzer-Handbüchern oder weiteren Anleitungen aufgeführt.

Die Kontakte zur Sperrung von Zertifikaten (URLs der Webseiten, Telefonnummern der jeweiligen Sperr-Hotline sowie ggf. Anschriften zum Versand schriftlicher Sperranträge) sind auf jedem Antragsformular (Kopie für den Antragsteller) aufgeführt.

3 Zertifikatstypen, Validierungsverfahren und Verwendung

3.1 Zertifikatstypen

Telekom Security stellt mit den V-PKI-CAs Zertifikate

- zur Signatur von Daten,
- zur Verschlüsselung von Daten sowie
- zur Authentisierung von Personen oder Geräten

für

- natürliche Personen (auch pseudonymisiert),
- Organisationen,
- Gruppen bzw. Funktionen sowie
- IT-Prozesse

aus.

Als Schlüsselmedien kommen sowohl Software-Zertifikate als auch Smartcards zum Einsatz. Die Schlüssel werden, sofern nicht vom Zertifikatsnehmer selbst erzeugt, wie folgt übergeben:

- Software-Zertifikate werden in Form von PKCS#12-Dateien, welche mit einem hinreichend langen und komplexen Passwort geschützt sind, über eine HTTPS-gesicherte Verbindung nach Authentifizierung des Zertifikatsnehmers oder der zuständigen RA zum Download angeboten.
- Smartcards werden an die im Rahmen der Registrierung erfasste Anschrift des Zertifikatsnehmers gesendet oder persönlich dem Zertifikatsnehmer übergeben.

Die erforderlichen Aktivierungsdaten werden bereits bei Antragstellung über eine HTTPS-gesicherte Verbindung übergeben und somit über einen separaten Weg zugestellt.

3.2 Validierungsverfahren

Alle in die Zertifikate aufzunehmenden Informationen werden durch die zuständigen Registrierungsstellen validiert. Jeder Antragsteller wird anhand eines gültigen amtlichen Ausweises nach festgelegten Verfahren persönlich identifiziert. Antragsteller sind entweder die natürlichen Personen, welche Zertifikate für sich selbst oder im Auftrag einer Organisation beantragen oder die „Schlüsselverantwortlichen“, welche Zertifikate für Gruppen, Funktionen und IT-Prozesse beantragen.

Eine Erneuerung eines Zertifikats auf Basis der initial validierten Daten ist nur innerhalb der letzten 6 Wochen vor Ablauf der Gültigkeit möglich, sofern sich die Daten nicht geändert haben und das zu erneuernde Zertifikat nicht gesperrt ist.

Wenn sich die validierten Daten geändert haben, muss ein neues Zertifikat wie bei Erstbeantragung beantragt werden, eine Änderung von Zertifikatsdaten im Rahmen einer Erneuerung oder Ersatzausstellung wird nicht angeboten.

3.3 Verwendungszwecke

Die Zertifikate dürfen nur für folgende Anwendungen genutzt werden:

- Einfache und fortgeschrittene elektronische Signatur, unter Beachtung folgender Voraussetzungen:
  - Eine fortgeschrittene Signatur ist nur mit einem Zertifikat möglich, das als keyUsage ausschließlich „nonRepudiation“ verwendet.
  - Eine fortgeschrittene Signatur kann nur durch eine natürliche Person erzeugt werden, d.h. eine Erzeugung von fortgeschrittenen Signaturen ist nicht mit Gruppen- oder Funktionszertifikaten möglich.
  - Der Schlüssel zur Erzeugung der Signatur muss in der alleinigen Kontrolle des Zertifikatsnehmers sein.
- Authentisierung von Personen oder Geräten gegenüber Anwendungen.
- Verschlüsselung von Daten bis VS-NfD („Verschlusssache, Nur für den Dienstgebrauch“) und bestimmte personenbezogene Daten.

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

4 Vertrauensgrenzen

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 Certificate Policy (CP), des Certificate Practice Statement (CPS) sowie dieser Nutzungsbedingungen für 10 Jahre auf.

Für den Fall der Beendigung des Betriebs einer V-PKI-CAs durch die Telekom Security wird Telekom Security evaluieren, ob der Betrieb an einen anderen Trust Service Provider übertragen werden kann oder eingestellt werden muss. Die konkreten Schritte werden in einem Beendigungsplan festgelegt, alle Betroffenen werden rechtzeitig informiert.

5 Verpflichtungen der Antragsteller

Der Antragsteller 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 Benutzerhandbuch) mit zuverlässigen Schlüsselgeneratoren zu erzeugen und nur für das beantragte Zertifikat zu verwenden, d.h. bei Erneuerung oder Beantragung eines weiteren Zertifikats neue Schlüssel zu generieren,
- das Zertifikat inkl. des ausstellenden CA-Zertifikats 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,
- bei Nutzung von Smartcards deren unversehrten Empfang zu prüfen,
- die Schlüssel und Zertifikate nur für die zulässigen Verwendungszwecke gemäß Kap. 3.3 zu nutzen,
- für VS-NfD-Anwendungen nur für VS-NfD zugelassene Smartcards als Schlüsselmedium zu verwenden,
- 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. Private Schlüssel, die nicht mehr zur Entschlüsselung benötigt werden, sollten sicher gelöscht (Software-Zertifikate) bzw. zerstört (Smartcard-Zertifikate) werden,
- den privaten Schlüssel und dessen Aktivierungsdaten (z.B. Passwort, PIN) angemessen vor Manipulation und unberechtigtem Zugriff durch Dritte zu schützen. Insbesondere müssen Schlüssel, die nicht in Smartcards oder anderen kryptografischen Geräten gespeichert sind, durch hinreichend lange und komplexe Passwörter geschützt werden (Empfehlungen siehe www.bsi.bund.de - „BSI-Basisschutz: Sichere Passwörter“). Die Computer, auf denen diese Schlüssel verwendet werden, müssen dem Stand der Technik entsprechend gesichert sein (z.B. Virenschutz, Firewalls, regelmäßige Sicherheitsupdates),
- 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) 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 Zertifikaten für Gruppen, Funktionen oder IT-Prozesse verpflichten sich darüber hinaus die Schlüsselverantwortlichen,

- Schlüssel nur an autorisierte Schlüsselnutzer weiterzugeben, wobei eine maximale Anzahl von 30 Kopien nicht überschritten werden darf,
- die weiteren Schlüsselnutzer über die Nutzungsbedingungen zu informieren und sich deren Akzeptanz bestätigen zu lassen,
- die weiteren Schlüsselnutzer zum sorgsamen Umgang mit dem privaten Schlüssel zu verpflichten,
- sofern erforderlich, weiteren sperrberechtigten Personen das Sperrkennwort mitzuteilen und diese, sofern nicht bereits geschehen, ebenfalls über die Nutzungsbedingungen zu informieren und sich deren Akzeptanz bestätigen zu lassen,
- nach dem Ausscheiden einer Person aus dem Kreis der Schlüsselnutzer durch geeignete Maßnahmen sicherzustellen, dass ein Missbrauch des privaten Schlüssels durch den ausgeschiedenen Schlüsselnutzer hinreichend sicher verhindert wird. Falls dies nicht möglich ist, muss das Zertifikat gesperrt werden und ein neues Zertifikat mit neuem Schlüssel beantragt werden.

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

Telekom Security stellt für alle von den V-PKI-CAs ausgestellten Zertifikate Statusdienste in Form von Sperrlisten und OCSP-Auskünften bereit. Die URLs der Statusdienste sind in den Zertifikaten aufgeführt.

Sperrlisten werden mindestens einmal täglich sowie nach einer Sperrung aktualisiert und veröffentlicht, OCSP-Auskünfte werden ad hoc auf jede Anfrage generiert und für maximal 2 Stunden zur Wiederverwendung vorgehalten.

Die Zertifikatsstatusdienste stehen 7x24h zur Verfügung. Die maximal tolerierbaren Ausfallzeiten sind in den jeweiligen Verträgen geregelt.

Jeder Zertifikatsnutzer sollte

- die Gültigkeit des Zertifikats durch Prüfung
  - der Zertifikatskette bis zum Wurzelzertifikat,
  - der Authentizität des Wurzelzertifikats durch Abgleich des Fingerprints des Wurzelzertifikats, veröffentlicht auf den Webseiten des Bundesamtes für Sicherheit in der Informationstechnik, https://www.bsi.bund.de,
  - der Gültigkeitsdauer des Zertifikats sowie
  - der Status- bzw. Sperrinformationen (CRLs oder OCSP) des Zertifikats

  validieren,
- die im Zertifikat angegebenen Verwendungszwecke durch die Attribute „keyUsage“ (Schlüsselverwendung) und „extendedKeyUsage“ (erweiterte Schlüsselverwendung) prüfen.

7 Anwendbare Vereinbarungen

Die Ausstellung und Nutzung der Zertifikate der V-PKI-CAs basiert auf

- der Telekom Security Certificate Policy,
- dem Telekom Security Certification Practice Statement der V-PKI-CAs sowie
- der Certificate Policy der V-PKI des Bundesamt für die Sicherheit in der Informationstechnik (BSI).

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/

Die Certificate Policy der V-PKI ist auf den Webseiten des BSI abrufbar: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Verwaltungs-PKI/Wurzelzertifizierungsstelle/CertificatePolicy/certificatepolicy_node.html

Sofern sich neue Versionen dieser Nutzungsbedingungen auch auf die Akzeptanz des Dienstes für bestehende Zertifikate auswirken, werden alle Zertifikatsnehmer mit aktiven Zertifikaten über die Veröffentlichung der neuen Version informiert und es wird eine angemessene Frist zur Ablehnung der neuen Nutzungsbedingungen gesetzt. Sollte innerhalb dieser Frist keine Ablehnung eingereicht werden, so gelten die neuen Nutzungsbedingungen als akzeptiert. Eine Ablehnung der neuen Nutzungsbedingungen hat die Sperrung der betroffenen Zertifikate zur Folge.

8 Zulassungen, Vertrauenszeichen und Auditierung

Telekom Security bestätigt mit einer Selbsterklärung als Anlage zum Vertrag über die Teilnahme an der Verwaltungs-PKI den ordnungsgemäßen Betrieb der V-PKI-CAs. Diese Selbsterklärung wird im Repository der Telekom Security veröffentlicht: https://www.telesec.de/de/service/downloads/pki-repository/

Zum Nachweis der Konformität wird der Betrieb der V-PKI-CAs sowohl durch interne Auditoren als auch durch unabhängige und vom BSI zugelassene externe Auditoren nach TR-03145 (mit ISO27001 als Voraussetzung) auditiert.

Im Rahmen der Audits werden neben der Dokumentation (CP, CPS, Sicherheitskonzept, Betriebskonzept 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. Die Audits durch interne Auditoren erfolgen in kürzeren Intervallen nach einem festgelegten Auditplan.