PKI-OFFENLEGUNGSPFLICHTEN

BUSINESS.ID

DEUTSCHE TELEKOM SECURITY GMBH

VERSION:	04.00
GÜLTIG AB:	18.02.2022
STATUS:	FREIGABE
KLASSIFIZIERUNG:	ÖFFENTLICH
LETZTE ÜBERPRÜFUNG:	17.02.2022

ERLEBEN, WAS VERBINDET.

IMPRESSUM

HERAUSGEBER

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

Telefon: 0228 181-0
E-Mail: info@telekom.de
Internet: www.telekom.de/security
Pflichtangaben: www.telekom.com/pflichtangaben-dtsec

Aufsichtsrat: N.N (Vorsitzender)
Geschäftsführung: Thomas Fetten (Sprecher), Dr. Klaus Schmitz, Thomas Tschersich

Handelsregister: Amtsgericht Bonn HRB 15241
Sitz der Gesellschaft Bonn
Umsatzsteuer-Identifikationsnummer. DE 254595345
WEEE-Register-Nummer DE 56768674

Kurzinformation:	Dieses Dokument beschreibt die PKI-Offenlegungspflichten des PKI-Service Business.ID.
Dateiname:	BusinessId_PKI-Offenlegungspflichten_04.00_DE.docx
Dokumentennummer:	n.n.
Dokumentenbezeichnung:	PKI-Offenlegungspflichten des PKI-Service Business.ID.
Version:	04.00
Gültig ab:	18.02.2022
Status:	Freigabe
Klassifizierung:	Öffentlich
Letzte Überprüfung:	17.02.2022
Autor:	Uwe Völkel, Netphen, 01.10.2020
Inhaltlich geprüft:	Andreas Jud, Netphen, 17.02.2022
Freigegeben von:	Hubertus Halb, Netphen, 18.02.2022
Ansprechpartner:	tc-solutions.lastlevel@t-systems.com

ÄNDERUNGSHISTORIE

VERSION:	STAND:	BEARBEITER:	ÄNDERUNGEN / KOMMENTAR:
00.10	11.06.2018	Uwe Völkel	Initiale Fassung
00.20	27.07.2018	Lothar Eickhold	Qualitätssicherung der Vers. 00.10
01.00	27.07.2018	Uwe Völkel	Freigabe dieser Version
01.10	06.06.2019	Uwe Völkel	Ergänzung Kapitel 3, 5, 7, 8, 10.1, 10.2 ff, 12.1, 12.2
01.20	04.02.2020	UV	Abstimmungsversion
01.30	05.02.2020	LE, UV	Ergänzung
01.40	02.03.2020	LE, UV	Ergänzung
01.50	24.03.2020	AJ	QS
02.00	25.03.2020	UV	Freigabe dieser Version
02.10	01.10.2020	UV	Neues Word-Template, Überarbeitung des Firmennamens
02.20	08.10.2020	AJ	QS
02.30	09.10.2020	GK	QS formal
03.00	09.10.2020	HH	Freigabe dieser Version
03.90	17.02.2022	Telekom Security	QS und neuer Name „Business.ID“
04.00	18.02.2022	Telekom Security	Freigabe dieser Version

INHALTSVERZEICHNIS

1 EINLEITUNG

Der PKI-Service „Business.ID“ stellt Zertifikate für unterschiedliches Verwendungszwecke (Mail, VPN, Server, usw.) aus, basierend auf dem Standard X.509v3. Abhängig von der Nutzung verwendet die „Business.ID“ unterschiedliche Zwischenzertifizierungsstellen (Intermediat CA), die hierarchisch einer öffentlichen oder internen Stammzertifizierungsstelle (Root-CA) untersteht.

Die Prozesse der Deutsche Telekom Security GmbH (im Folgenden „DT Security“ genannt) werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319 411-1, policy OVCP und policy NCP) unterzogen. Zertifizierungsgegenstand sind alle Prozesse, die zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (TeleSec Business CA 1) dienen. Die Deutsche Telekom Security GmbH führt zusätzlich in regelmäßigen Abständen Selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) durch.

Dieses Dokument fasst die jeweiligen Kernpunkte der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) (siehe Kapitel 8) zusammen und dient als Übersicht für Antragsteller und vertrauende Dritte. Zur Gewährleistung der Vergleichbarkeit ist es gemäß ETSI EN 319 411-1 aufgebaut.

2 KONTAKTE DES TRUST SERVICE PROVIDER (TSP)

Der Trust Service Provider (Anbieter von Vertrauensdienstleistungen, Zertifizierungsdienstleister), Deutsche Telekom Security GmbH ist über folgende Kontakte zu erreichen:

Anschrift: Deutsche Telekom Security GmbH
Trust Center & ID Solutions, Chapter Trust Center Products
Untere Industriestraße 20
57250 Netphen
Deutschland

Telefon: +49 (0) 1805-268204
Festnetz: 0,14 €/Minute, Mobilfunknetz: max. 0,42 €/Minute
E-Mail: telesec_support@t-systems.com
Internet: https://www.telesec.de

Zertifikats-Missbrauchsfälle können gemeldet werden über:
Telefon: +49 (0) 1805-268204
Festnetz: 0,14 €/Minute, Mobilfunknetz: max. 0,42 €/Minute
E-Mail: telesec_support@t-systems.com
Internet: https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

3 ZERTIFIKATSTYPEN, VALIDIERUNGSPROZESSE UND SCHLÜSSELVERWENDUNG

Mit der PKI-Dienstleistung Business.ID bietet die Deutsche Telekom Security GmbH eine mandantenfähige Company Public-Key-Infrastruture (PKI) an, mit der der Kunde selbst digitale Zertifikate gemäß des Standards X.509v3 für unterschiedlichste Anwendungen (z.B. E-Mail-Security (S/MIME), VPN, Client-Server-Authentifikation, Microsoft-Domänen-Anmeldung) ausstellen und verwalten (sperren, erneuern) kann.

Folgende Zertifikatstypen werden standardisiert bereitgestellt:

- Benutzer (Schlüsseltrennung Single-, Dual-, Triple-Key)
- Server
- Domain-Controller
- Router/Gateway
- Mail-Gateway

Abhängig von den jeweiligen Zertifikatstypen bietet die Business.ID folgende Zertifizierungsstellen zur Verfügung:

Öffentliche Zertifizierungsstelle

- T-TeleSec GlobalRoot Class 2 (RSA, SHA-256, 01.10.2008 – 01.10.2033)
  - TeleSec Business CA 1 (RSA, SHA-256, 29.11.2012 – 29.11.2024)

Interne Zertifizierungsstelle

- Deutsche Telekom Internal Root CA 1(RSA, SHA-1, 15.11.2007 – 15.11.2027)
  - Internal Business CA 2 (RSA, SHA-256, 11.02.2014 – 15.11.2027)
  - Business CA (RSA, SHA-1, 08.11.2011 – 09.11.2023)

- Deutsche Telekom Internal Root CA 2 (RSA, SHA-256, 03.08.2017 – 03.08.2039)
  - Internal Business CA 3 (RSA, SHA-256, 03.08.2017 – 03.08.2029
  - Internal Business CA 5 (RSA, SHA-256, 10.09.2019 – 10.09.2031

Alle o.g. Zertifikatstypen können unter einer internen Zertifizierungsstelle der Deutsche Telekom Security GmbH ausgestellt werden.

Unter einer öffentlichen Zertifizierungsstelle, die jährlich einer ETSI-Zertifizierung unterliegt (siehe Kapitel 13), können folgende Zertifikatstypen ausgestellt werden:

- Benutzer (Schlüsseltrennung Single-, Dual-, Triple-Key (außer SmartCard-LogOn)
- Server
- Mail-Gateway

Die Zertifikatserweiterungen „Schlüsselverwendung“ und „Erweiterte Schlüsselverwendung“ als auch „Gültigkeitszeitraum“ der Zertifikate ist abhängig vom Zertifikatstyp und den Vorgaben/Regelungen (z.B. Root-Programme der Betriebssystem- und Browserhersteller, Baseline Requirements des CA/Browser-Forums) für den Betrieb öffentlicher Zertifizierungsstellen.

Alle o.g. Zertifikate unterstützen die Schlüsselverwendung, die zur Erstellung einer digitalen Signatur und Verschlüsselung notwendig sind. Als „Erweiterte Schlüsselverwendung“ stehen, abhängig vom Zertifikatstyp, Secure E-Mail, Client-Authentifikation, Server-Authentifikation und Smartcard-LogOn zur Verfügung.

Die Gültigkeit von Zertifikaten, die von einer öffentlichen Zertifizierungsstelle ausgestellt werden, beträgt maximal sechsunddreißig (36) Monate. Eine Ausnahme gilt für Server-Zertifikate mit einer maximalen Gültigkeit von dreizehn (13) Monaten.

Der Gültigkeitszeitraum von Zertifikaten, die von einer internen Zertifizierungsstelle ausgestellt werden, beträgt maximal sechzig (60) Monate.

Der Zertifikatsverwaltungsprozess (Ausstellung, Erneuerung und Sperrung) aller Zertifikatstypen, der Validierungsprozess als auch Schlüsselverwendungen sind ausführlich in der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) dargestellt.

Das aktuell gültige Dokument als auch alle bisherigen Versionen sind im Internet abrufbar unter: https://www.telesec.de/de/service/downloads/pki-repository/

Der PKI-Mandant wird durch die Rolleninhaber Master- und Sub-Registrator des Kunden selbst verwaltet. Diese Rolleninhaber sind auch für das Ausstellen und Sperren von Zertifikaten verantwortlich. Eine Zertifikatssperrung der og. Typen erfolgt durch den zuständigen Sub-Registrator des Kunden. Bei Benutzer-Zertifikaten besteht optional die Sperrung über eine Webseite zur Verfügung, sofern der Kunde dies unterstützt. Die Sperrung eines Sub-Registrator-Zertifikats erfolgt durch den verantwortlichen Master-Registrator des Kunden. Ein Sperrauftrag des Master-Registrator-Zertifikats nimmt der Kontakt des TSP (siehe Kapitel 2) entgegen.

4 ABGRENZUNG DES VERTRAUENSBEREICHS

Deutsche Telekom Security GmbH setzt keine Vertrauensgrenzen für die von ihr ausgestellten Zertifikate.

In der Zertifikatshistorie werden alle relevanten Ereignisse von der Antragstellung über die Registrierung, die Prüfungen durch den TSP, die Produktion bis zur Freischaltung und ggf. der Sperrung erfasst und Integritätsgeschützt abgelegt.

Die Papierdokumente und elektronisch erfassten Antrags- und Zertifikatsdaten sowie die Daten der Zertifikatshistorie werden über die Zertifikatsgültigkeit hinaus weitere zehn Jahre zzgl. einer Karenzzeit archiviert. Bei einer Zertifikatserneuerung verlängert sich die Aufbewahrungsfrist der ursprünglichen Dokumente und Daten entsprechend.

Gleiche Vorgaben gelten für die externe Registrierungsstelle, die beim Kunden etabliert sind.

5 VERPFLICHTUNG DES ZERTIFIKATTEILNEHMERS

Die Verpflichtungen der Endteilnehmer sind im Dokument „Leistungs- und Nutzungsbedingungen der Business.ID“ aufgeführt.

Das aktuell gültige Dokument als auch alle bisherigen Versionen sind im Internet abrufbar unter: https://www.telesec.de/de/service/downloads/pki-repository/

6 VERPFLICHTUNGEN DER VERTRAUENDEN DRITTPARTEI (RELYING PARTIES) UND ZERTIFIKATSVALIDIERUNG

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der Vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

Jeder Vertrauende Dritte sollte daher

- vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen,
- die Gültigkeit des Zertifikats überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie) sowie den Gültigkeitszeitraum und die Sperrinformationen (CRLs oder OCSP) des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit der vorliegenden CP/CPS einsetzen. Deutsche Telekom Security GmbH ist nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich,
- die technischen Verwendungszwecke prüfen, die durch die im Zertifikat angegebenen Attribute „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt sind.

Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

7 HAFTUNGSAUSSCHLUSS, HAFTUNGSBESCHRÄNKUNGEN

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf eine vorsätzliche Pflichtverletzungen zurückzuführen sind, haftet die Zertifizierungsstelle unbegrenzt.

Im Übrigen wird die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen, sind in der aktuellen Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) in Kapitel 9.7 und 9.8, Allgemeine Geschäftsbedingungen (AGB) TeleSec-Produkte oder einzelvertraglich geregelt.

8 ANWENDBARE UND VERTRAGLICHE VEREINBARUNGEN

Im Internet sind unter dem Link https://www.telesec.de/de/service/downloads/pki-repository/ folgende Dokumente abrufbar:

- Leistungs- und Nutzungsbedingungen der Business.ID
- Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) (Repository, aktuelle Fassung und Vorläuferversionen)

- PKI-Offenlegungspflichten (PKI Disclosure Statement (PDS))
- Leistungsbeschreibung
- Allgemeine Geschäftsbedingungen (AGB) TeleSec-Produkte
- Alle Zertifikate der Stamm- und Zwischenzertifizierungsstelle (Root- und Sub-CAs)
- Alle aktuellen Zertifikatssperrlisten (CRLs) und Sperrlisten der Zertifizierungsstellen (CARLs)

9 VERFÜGBARKEIT DES DIENSTES

Die im Trust Center installierte Infrastruktur des PKI-Dienstes Business.ID besteht aus den Komponenten

- Zertifizierungsinstanz (CA), die über ein Web-Portal im Internet erreichbar ist,
- LDAP-Verzeichnisdienst, zum Abruf von Sperrlisten (CRLs, CARLs), Endteilnehmer-Zertifikaten (sofern diese veröffentlicht werden sollen) und CA- und Root-CA-Zertifikaten,
- Online-Valierungsdienst OCSP, und
- Mail-Server.

Verfügbarkeit der Zertifizierungsinstanz und Web-Server

- Die Zertifizierungsinstanz und Web-Server stehen im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Verzeichnisdienst steht im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Online-Validierungsdienst steht im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Mail-Server steht im monatlichen Mittel zu 98,0% zur Verfügung.

10 DATENSCHUTZRICHTLINIE

Innerhalb der Business.ID muss Deutsche Telekom Security GmbH zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten.

Sollen von der Deutsche Telekom Security GmbH besondere Kategorien personenbezogener Daten im Sinne Artikel 9 Datenschutz-Grundverordnung (DSGVO) [EU-DSGVO] verarbeitet werden, hat der Kunde die Deutsche Telekom Security GmbH hierüber unverzüglich schriftlich zu unterrichten.

10.1 Protokollereignisse

Es ist im Loggingkonzept sowie im Installationshandbuch festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden und wie sie vor Verlust und unbefugtem Zugriff geschützt werden. Es werden dabei die Anforderungen aus [ETSI EN TSP] Kap. 10.2 umgesetzt.

10.2 Datenarchivierung

10.2.1 Art der archivierten Datensätze

Deutsche Telekom Security GmbH archiviert folgende Daten:

- Auftragsunterlagen in papiergebundener Form (z.B. Angebote, Aufträge),

- Informationen in Zertifikatsanträgen und zum Zertifikatslebenszyklus (z.B. Sperr- und Erneuerungsanträge),
- Soft-PSE, die über Bulk beantragt wurden,
- Soft-PSE des Verschlüsselungs-Zertifikats, das bei Smartcard-Personalisierung (nur Triple-Key) generiert wurden,
- alle Audit-Daten/History-Daten/Logging-Dateien, die gemäß Kapitel 10.1 erfasst werden.

10.2.2 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommener Sperrungen, werden sieben (7) Jahre nach Ablauf der Zertifikatsgültigkeit vorgehalten,
- Audit-, History- und Event-Logging Daten werden bis zu zweiundvierzig (42) Tage archiviert.

11 KOSTENERSTATTUNG

Die Erstattung von Entgelten durch Deutsche Telekom Security GmbH erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts. Darüber hinaus gelten die Regelungen der jeweils gültigen AGB oder sonstige mit dem Kunden vereinbarte vertraglichen Regelungen.

12 ANWENDBARES RECHT, BESCHWERDEN UND STREITBEILEGUNG

12.1 Allgemeines

Es gilt deutsches Recht. Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei. Gerichtsstand ist der Sitz der Deutsche Telekom Security GmbH in Bonn.

12.2 Außergerichtliche Streitbeilegung (Beilegung einer Streitigkeit)

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei.

13 AUDITIERUNG

Die Prozesse der Deutsche Telekom Security GmbH unterliegen regelmäßigen jährlichen Audits (ETSI EN 319 411-1, Policy OVCP und Policy NCP) durch unabhängige Dritte. Gegenstand der Zertifizierung sind alle Prozesse zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endnutzerzertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (derzeit TeleSec

Business CA 1). Die Deutsche Telekom Security GmbH führt außerdem in regelmäßigen Abständen Selbstaudits zur Qualitätsbewertung durch.

Zur Prüfung der Konformität wird die öffentliche Zertifizierungsstelle der Business.ID sowohl durch interne Auditoren als auch durch eine anerkannte Prüfstelle (gemäß [ETSI EN 319 403]) auditiert. Im Rahmen der Audits wird neben der Dokumentation (Sicherheitskonzept, Betriebskonzept sowie weitere interne Dokumente) die Umsetzung der Prozesse und Einhaltung der Vorgaben überprüft.

Zur Gewährleistung der Konformität erfüllt die öffentliche Zertifizierungsstelle der Business.ID die Anforderungen aus

[ETSI NCP OVCP]	ETSI EN 319 411-1 V1.1.1 (2016-02), European Telecommunications Standards Institute, „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, policy NCP and OVCP
[ETSI EN TSP]	ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

Anhang A: AKRONYME

AGB	Allgemeine Geschäftsbedingung
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
CARL	CA Revocation List
DSGVO	Datenschutz-Grundverordnung
ETSI	European Telecommunications Standards Institute
HTTPS	HyperText Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
NCP	Normalized Certificates Policy
OCSP	Online Certificate Status Protocol
OVCP	Organizational Validation Certificates Policy
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructur
PSE	Personal Security Environment
RA	Registration Authority
RSA	von Rivest, Shamir und Adleman entwickeltes asymmetrisches kryptographisches Verfahren
SHA	Secure Hash Algorithm
S/MIME	Secure / Multipurpose Internet Mail Extensions
TSP	Trust Service Provider
VPN	Virtual Private Network