LEISTUNGSBESCHREIBUNG

TELESEC SHARED-BUSINESS-CA

DEUTSCHE TELEKOM SECURITY GMBH

VERSION:	01.00
GÜLTIG AB:	15.10.2020
STATUS:	FREIGABE
KLASSIFIZIERUNG:	ÖFFENTLICH
LETZTE ÜBERPRÜFUNG:	12.10.2020

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 Leistungsbeschreibung des PKI-Service TeleSec Shared-Business-CA.
Dateiname:	Shared-Business-CA_LB_01.00_DE_Freigabe.docx
Dokumentennummer:	n.n.
Dokumentenbezeichnung:	Leistungsbeschreibung des PKI-Service TeleSec Shared-Business-CA.
Version:	01.00
Gültig ab:	15.10.2020
Status:	Freigabe
Klassifizierung:	Öffentlich
Letzte Überprüfung:	12.10.2020
Autor:	Uwe Völkel, Netphen, 08.10.2020
Inhaltlich geprüft:	Andreas Jud, Netphen, 12.10.2020
Freigegeben von:	Hubertus Halbe, Leiter TC Produkte, Netphen, 12.10.2020
Ansprechpartner:	tc-solutions.lastlevel@t-systems.com

ÄNDERUNGSHISTORIE

VERSION:	STAND:	BEARBEITER:	ÄNDERUNGEN / KOMMENTAR:
00.10	08.10.2020	UV	Neues Word-Template, Überarbeitung des Firmennamens
00.20	12.10.2020	AJ	QS
01.00	12.10.2020	HH	Freigabe der Version

INHALTSVERZEICHNIS

1 ALLGEMEINES

Mit der PKI-Dienstleistung TeleSec Shared-Business-CA bietet die Deutsche Telekom Security GmbH (im Folgenden „DT Security“ genannt) eine 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. TeleSec Shared-Business-CA bietet die Möglichkeit, innerhalb von wenigen Tagen eine PKI für ein firmeninternes Identitätsmanagement aufzubauen und zu nutzen.

Die Deutsche Telekom Security GmbH stellt dem Kunden dazu die notwendige Infrastruktur und Zugänge bereit, um aus der Kundenlokation, via Internet auf die PKI-Komponenten im sicheren Trust Center der DT Security zugreifen zu können.

Hinweis: Die im Dokument genannten Produkt- und Firmennamen sind Marken der jeweiligen Eigentümer.

2 STANDARDLEISTUNGEN DER TELEKOM SECURITY

2.1 TeleSec Shared-Business-CA

2.1.1 Domänenkonzept

Der Kunde wird als eigenständiger Mandant innerhalb der TeleSec Shared-Business-CA eingerichtet. Innerhalb seines Mandanten kann der Kunde, abhängig von seinen ihm zugeteilten Berechtigungen (Befugnissen), selbstständig und unabhängig Zertifikate ausstellen und verwalten. Der Mandant wird im Rahmen der TeleSec Shared-Business-CA auch als Masterdomäne, und die Untergliederung in je Zuständigkeitsbereich als Subdomäne bezeichnet. Der Name des PKI-Mandanten als auch des Zuständigkeitsbereichs ist Bestandteil des Antragstellers im Zertifikat.

Damit bietet dieses zweistufige Domänenkonzept die Möglichkeit, Organisationsstrukturen des Kunden abzubilden.

2.1.2 Zertifizierungsstelle

Zertifikate werden im Allgemeinen von einer Zwischenzertifizierungsstelle (Intermediate Certification Authority oder auch Sub-CA) ausgestellt, die wiederum hierarchisch einer Stammzertifizierungsstelle (Root CA) untersteht.

Dabei kann, abhängig vom Typ oder Vorlage, das Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt werden, die entweder einer öffentlichen oder internen Stammzertifizierungsstelle untersteht. Das Zertifikat der Stammzertifizierungsstelle „T-TeleSec GlobalRoot Class 2“ ist bereits in vielen Zertifikatsspeichern und Anwendungen als vertrauenswürdige Zertifizierungsstelle (Vertrauensanker) vorinstalliert. Für die Stammzertifizierungsstelle „Deutsche Telekom Internal Root CA 2“ und „Deutsche Telekom Internal Root CA 1“ bedarf es dagegen einer Nachinstallation.

2.1.3 Registrierungsstelle

Vor der Ausstellung eines Zertifikates muss der Antragssteller (Person bzw. Gerät) registriert werden. Die Registrierung erfolgt durch den Kunden selbst unter Einhaltung der Vorgaben der TeleSec Shared-Business-CA, im Wesentlichen der Zertifizierungsrichtlinie (Certificate Policy (CP))

und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)). Die TeleSec Shared-Business-CA bietet dazu zwei Möglichkeiten an.

- **Zentrale Registrierung**
  Die Ausstellung des Zertifikats für Personen und Geräte (siehe Ziffer 2.3.1) erfolgt zentral durch den zuständigen Sub-Registrator nachdem eine erfolgreiche Registrierung stattfand. Ebenfalls kann der Sub-Registrator Zertifikatsanträge bearbeiten (genehmigen, ablehnen, Wiedervorlage), die per SCEP-, CMP- oder Mail-Schnittstellen (siehe Ziffer 2.3.2) eintreffen. Regelungen des Registrierungsprozesses sind in dem CP/CPS beschrieben.
- **Dezentrale Registrierung**
  Der Antragsteller (natürliche Person) kann über eine Benutzerwebseite selbst einen Zertifikatsantrag stellen. Der zuständige Sub-Registrator führt die Registrierung nach den Regelungen der Zertifizierungsrichtlinie durch und genehmigt den Antrag, sofern keine Einwände bestehen. Anschließend steht das Zertifikat dem Antragsteller zum Herunterladen bereit. Regelungen des Registrierungsprozesses sind in der Erklärung zum Zertifizierungsbetrieb (CPS) beschrieben.

2.2 Bereitstellung TeleSec Shared-Business-CA

Damit die TeleSec Shared-Business-CA schnell und unkompliziert genutzt werden kann, ist in der Bereitstellung die Einrichtung eines PKI-Mandanten (Master-Domain) und die Lieferung einer Grundausstattung von Hard- und Software-Komponenten (Smartcard-Leser, Treiber-Software) enthalten, die Basis für den Zugriff auf das Trust Center bilden. Die Grundausstattung unterstützt dabei den Kunden bei der Ausstellung von Soft-PSE (Datei bestehend aus Zertifikat und privatem Schlüssel) als auch das Aufbringen von Zertifikaten auf eine vorbeschlüsselte Smartcard (Smartcard-Personalisierung).

Die Bereitstellung enthält folgende Leistungen:

- Einrichtung eines kundenindividuellen Verwaltungsbereiches (Mandant bzw. Master-Domäne),
- Bereitstellung eines Master-Registrator-Zertifikats auf Smartcard zur Verwaltung des Mandanten innerhalb der Shared-Business-CA,
- Überlassung eines Sub-Registrator-Zertifikats zur Verwaltung der vom Kunden angelegten Zuständigkeitsbereichen (Sub-Domänen) innerhalb der TeleSec Shared-Business-CA,
- einem Smartcard-Leser der Klasse 2 (mit Tastatur),
- der zugehörigen CSP-Software bzw. PKCS#11-Moduls,
- Dokumentation, bestehend aus der Zertifizierungsrichtlinie (CPS), dem Service Level Agreement (SLA), der Installationsanleitung Registrator-PC und den rollenspezifischen Handbüchern.

Die Einrichtung des PKI-Mandanten erfolgt in Abstimmung mit dem Kunden.

Die Installation der Grundausstattung erfolgt auf einem internetfähigen Standard-PC des Kunden.

2.3 Überlassung des Dienstes TeleSec Shared-Business-CA

Mit der TeleSec Shared-Business-CA steht eine PKI-Infrastru-ktur zur Verfügung, die von fachkundigem Personal im hochsicheren Trust Center der Telekom Security nach den Regelungen des Service Level Agreements (SLA) und der Zertifizierungsrichtlinie (Certificate Policy (CP)) und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) betrieben wird.

Der Kunde kann innerhalb seines Verwaltungsbereiches (PKI-Mandant bzw. Master-Domäne) selbst Zertifikate ausstellen, sperren und erneuern. Die Schlüsselverwaltung als auch die Registrierung obliegt somit dem Kunden selbst.

Die Dienstleistung TeleSec Shared-Business-CA stellt, abhängig von den Funktionsrollen, Zertifikate für folgende Teilnehmer aus:

- Registrierungsmitarbeiter des Domänen-Betreibers (Master-Registrator, Sub-Registratoren und deren Derivate (CMP)) als untergeordnete Registrierungsstellen,
- natürliche Personen (Endnutzer, Pseudonym) als Single-, Dual- und Triple-Key-Zertifikate,
- Personen- und Funktionsgruppen, als Single-, Dual- und Triple-Key-Zertifikate,
- Geräte (z.B. Maschinen wie Router, Gateways, Server, Domain-Controller, Mail-Gateways).

Die Zertifikatsverwaltung erfolgt nach erfolgreicher Authentifizierung, über SSL-geschützte Webseiten rollenbasiert (Master-, Sub-Registrator, Benutzer). Der Umgang mit der TeleSec Shared-Business-CA ist in der Zertifizierungsrichtlinie (Certificate Policy (CP)) und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) dokumentiert.

2.3.1 Zertifikatsverwaltung über rollenbezogene Webseiten

Der Kunde greift über eine SSL-gesicherte Internetverbindung (Protokoll HTTPS) auf die Webseiten der TeleSec Shared-Business-CA zu. Erst nach erfolgreicher Authentisierung (Zugriffskontrolle) kann der Rolleninhaber des Kunden seine spezifischen Funktionen der TeleSec Shared-Business-CA nutzen. Je nach zugeordneter Funktionsrolle steht dem Kunden folgender Funktionsumfang zur Verfügung.

a) Webseite für die Rolle „Master-Registrator“
   Für die Verwaltung des PKI-Mandanten (Master-Domäne) benennt der Kunde (z.B. Firma, Behörde, Institution) eine verantwortliche Person, auf die ein Master-Registrator-Zertifikat ausgestellt wird, und damit die Funktion des Master-Registrators wahrnehmen soll.

   Dem Master-Registrator stehen folgende Funktionen auf der Webseite zur Verfügung:

   - Zuständigkeitsbereiche (Sub-Domänen) anlegen, suchen und bearbeiten,
   - Sub-Registrator-Zertifikate ausstellen, suchen und sperren; optional: Rollenzuweisung von Sub-Registrator-Zertifikaten (Derivaten) für die CMP-Schnittstelle.
   - Teilnehmer-Zertifikate suchen und bearbeiten,
   - Zertifikatssperrlisten (Certificate Revokation List, CRL) initiieren und herunterladen,
   - Anzeigen und Herunterladen von CA- und Root-CA-Zertifikaten,
   - Verwaltung des Mandanten durch Einstellen von Hinweisen, Einstellen von Kundendokumenten und Änderung von LogIn-Daten,
   - Anzeigen von Informationen wie Hinweise und Herunterladen von DT Security-Dokumenten,
   - Erneuerung des Master-Registrator-Zertifikats,
   - Erstellung von Statistiken innerhalb der Master-Domäne.

   Entsprechend den Kundenvorgaben sind Zuständigkeitsbereiche (Sub-Domänen) zu definieren (mindestens jedoch eine), um z. B. die Organisationsstruktur entsprechend abbilden zu können. Der Master-Registrator legt den Zuständigkeitsbereich an und stellt für die berechtigte Person ein Sub-Registrator-Zertifikat aus. Ein Sub-Registrator kann auch die Rechte zur Verwaltung mehrerer Zuständigkeitsbereiche erhalten.

b) Webseite für die Rolle „Sub-Registrator“
   Der Sub-Registrator hat die Aufgabe, innerhalb seines Zuständigkeitsbereiches die Ausstellung der Teilnehmer-Zertifikate zu initiieren (siehe Ziffer 2.1.3, Zentrale Registrierung) oder aber Zertifikatsanträge zu bearbeiten (genehmigen, ablehnen, Widervorlage, Ziffer 2.1.3, Dezentrale Registrierung). Der Sub-Registrator führt entsprechend der Vorgaben der Erklärung zum Zertifizierungsbetrieb (CPS) die Registrierung der Teilnehmer durch. Ebenfalls obliegt ihm die Erneuerung und Sperrung von Zertifikaten.

   Dem Sub-Registrator stehen folgende Funktionen auf der Webseite zur Verfügung:

- Ausstellen, genehmigen, suchen und bearbeiten von Endteilnehmer-Zertifikaten. Bei der Beantragung ist zu beachten, ob das Zertifikat auf Smartcard aufgebracht werden soll oder Schlüsselmaterial als Soft-PSE erzeugt wird. Um den Personalsierungsprozess von Smartcards zu vereinfachen, können Zertifikatsdaten hochgeladen und für die Beantragung übernommen werden,
- Beantragung von Soft-PSE im Bulk-Modus (Massengenerierung von Schlüsselmaterialien inkl. Zertifikat),
- Zertifikatssperrlisten (CRL) initiieren und herunterladen,
- Anzeigen und Herunterladen von CA- und Root-CA-Zertifikaten,
- Verwalten der kundenindividuellen Domäne durch Einstellen von Hinweisen, Einstellen von Kundendokumenten und Voreinstellung bei Benutzereingaben,
- Anzeigen von Informationen wie Hinweise und Herunterladen von DT Security-Dokumenten,
- Erneuerung des Sub-Registrator-Zertifikats,
- optional: Als Ergebnis des Registrierungsprozesses können Vorregistrierungsdaten (Pre-Authentication) hochgeladen werden. Zertifikatsanträge, die über die Benutzer-Webseite, Mail- oder SCEP-Schnittstelle eintreffen,werden gegen die Vorregistrierungsdaten geprüft und entsprechend bearbeitet. Im Gutfall wird das Zertifikat direkt ausgestellt. Anderseits muss der Sub-Registrator den Antrag manuell bearbeiten.

c) Webseite für die Rolle „Benutzer“
Im Falle, dass Benutzer selbst Zertifikate beantragen sollen, steht eine gesonderte Webseite mit folgenden Funktionen zur Verfügung:
- Beantragen, abholen, suchen, sperren, erneuern von Benutzer-Zertifikaten nach erfolgreicher Anmeldung an der Webseite,
- Zertifikatssperrlisten (CRL) herunterladen,
- Anzeigen und Herunterladen von CA- und Root-CA-Zertifikaten,
- Anzeigen von Informationen wie Hinweise und Herunterladen von DT Security-Dokumenten.

2.3.2 Weitere Schnittstellen

a) SCEP (Simple Certificate Enrollment Protocol)
Die TeleSec Shared-Business-CA unterstützt die Beantragung und Verwaltung von Zertifikaten für Netzwerkkomponenten (Router, Gateways) über das SCEP-Protokoll.

b) E-Mail
Die TeleSec Shared-Business-CA bietet die Möglichkeit Zertifikate für Benutzer (nur Single-Key) und Server per E-Mail zu beantragen. Unter Einhaltung der Formatvorgaben (PKCS#10-Request) wird der Antrag an eine definierte E-Mailadresse gesendet. Nach Genehmigung des Zertifikatsantrags durch den Sub-Registrator erfolgt die Zustellung des Zertifikats an die Mail-Adresse des Absenders.

c) CMP (Certificate Management Protocol)
Die TeleSec Shared-Business-CA unterstützt die Beantragung und Verwaltung von Zertifikaten (Benutzer, Server) über das CMP-Protokoll. Für die Nutzung dieser Schnittstelle bedarf es jedoch einer Individualentwicklung eines CMP-Clients durch den Kunden.

2.3.3 Verzeichnisdienst

DT Security stellt einen zentralen Verzeichnisdienst für die TeleSec Shared-Business-CA bereit, auf dem die aktuellen Sperrlisten (Certificate Revokation List (CRL), Authority Revokation List (CARL)) als auch Benutzer-Zertifikate abrufbar sind. Der Zugriff auf den Verzeichnisdienst ist öffentlich oder Benutzername/Passwort-geschützt.

Der Zugriff erfolgt mittels LDAP-Protokoll (Lightweight Directory Access Protocol).

2.3.4 Sperrlisten

Gesperrte Endteilnehmer- und Registrator-Zertifikate werden in einer Zertifikatssperrliste (CRL) veröffentlicht, die automatisch einmal pro Tag aktualisiert wird. Es besteht die Möglichkeit, anlassbezogen Sperrlisten zu initiieren (siehe Ziffer 2.3.1).

Gesperrte CA-Zertifikate werden in einer Sperrliste für Zertifizierungsstellen (CARL) veröffentlicht. Die Erzeugung erfolgt anlassbezogen, aber spätestens nach sechs Monaten durch DT Security.

2.3.5 Online-Zertifikatsvalidierung

Es wird die Online-Validierung von Endteilnehmer- und Registrator-Zertifikaten über das Standardprotokoll OCSP (Online Certificate Status Protokoll) unterstützt.

2.3.6 Vorbelegung von Datenfeldern

Bei der Nutzung einer öffentlichen Stamm- und Zwischenzertifizierungsstelle obliegt die Vorbelegung von Datenfeldern (Landeskennung, Organisation, Organisationseinheit, Ort und Gliedstaat) der DT Security.

Im Falle der Nutzung einer internen Stamm- und Zwischenzertifizierungsstelle kann der Sub-Registrator bestimmte Datenfelder für die Antragsstellung mit entsprechenden Werten vorbelegen.

2.3.7 Informationen und Meldungen

Die TeleSec Shared-Business-CA bietet die Möglichkeiten kundenindividuelle Informationen als auch Informationen der DT Security (Hinweise und Dokumente) innerhalb der rollenspezifischen Webseiten (Master- und Sub-Registrator, Benutzer) gezielt zu verteilen.

2.4 Überlassung von Zertifikaten

Die beantragten Zertifikatstypen enthalten neben den individuellen Angaben zum Zertifikatsinhaber immer Informationen des PKI-Mandanten (Master-Domäne) und Zuständigkeitsbereichs (Sub-Domäne) (siehe Ziffer 2.1.1). Weitere Zertifikatsinformationen sind in der Zertifizierungsrichtlinie (Certificate Policy (CP)) und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) dokumentiert.

Die Zertifikatsgültigkeit kann auf ein Jahr, zwei oder drei Jahre eingestellt werden und ist für die jeweils eingerichteten PKI-Mandanten gültig. Optional sind andere Gültigkeitszeiträume konfigurierbar, die aber nicht gegen Anforderungen der Normungsgremien usw. verstoßen dürfen.

2.4.1 Zertifikate für natürliche Personen und Personen- und Funktionsgruppen

Entsprechend der Konfiguration können nur bestimmte Zertifikatsbündel beantragt werden. Diese sind

a) Single-Key
   Besteht aus einem Zertifikat, das für die Verwendungszwecke Schlüsselverschlüsselung und Digitale Signatur geeignet ist. Es ist keine erweiterte Schlüsselverwendung gesetzt.
b) Dual-Key
   Bestehend aus zwei getrennten Zertifikaten, je eins für die Verwendungszwecke Schlüsselverschlüsselung und Digitale Signatur. Es ist keine erweiterte Schlüsselverwendung gesetzt.
c) Triple-Key
   Bestehend aus drei getrennten Zertifikaten, je eins für die Verwendungszwecke

Schlüsselverschlüsselung, Digitale Signatur und Smartcard-basierendes LogOn an Microsoft-Windows-Domänen. Als erweiterte Schlüsselverwendung ist Smartcard-Anmeldung und Client-Authentifizierung gesetzt.

2.4.2 Zertifikate für Geräte

a) Serverzertifikate
   Serverzertifikate zur Authentisierung von Webservern gemäß SSL/TLS-Standard.
b) Router/Gateway-Zertifikate
   Zertifikate zum Einsatz in Netzwerkkomponenten.
c) Mail-Gateway-Zertifikate
   Domänen-Zertifikat zum Einsatz in einem Mail-Gateway.
d) Domain-Controller-Zertifikate
   Ausstellung von Zertifikaten für Server, die als Domain-Controller in einer Microsoft-Serverdomäne betrieben werden.

2.4.3 Zertifikate für Registrierungsmitarbeiter inkl. Derivate des Mandanten

Registrierungsmitarbeiter erhalten ein Verwaltungs-Zertifikat, das ausschließlich nur für die jeweiligen Master- und Sub-Registratoren und die damit verbundenen Tätigkeiten zu verwenden ist.

Diese Regelung gilt ebenfalls für die Derivate der Registrator-Zertifikate, die für den Zugriff auf die CMP-Schnittstelle Verwendung finden.

3 PERSONELLE, INFRASTRUKTURELLE UND TECHNISCHE RAHMENBEDINGUNGEN

3.1 Personelle Rahmenbedingungen

Weitere Details sind im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.

3.2 Infrastrukturelle Rahmenbedingungen

Weitere Details sind im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.

3.3 Technische Rahmenbedingungen

3.3.1 Registrator-Arbeitsplatz

Das Ausstellen und Verwalten von Zertifikaten aus der TeleSec Shared-Business-CA erfolgt über Web-basierende Komponenten eines Arbeitsplatzrechners (PC), der definierte Voraussetzungen erfüllen muss.

Weitere Details sind im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.

3.3.2 Rahmenbedingungen für Anwendungen und Geräte

Weitere Details sind im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.

3.4 Verhaltensregeln für Registratoren

Weitere Details sind im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.

4 TARIFMODELLE

4.1 Advanced

Innerhalb des Tarifs „Advanced“ erfolgt die Abrechnung auf Basis einer definierten Obergrenze von aktiven Zertifikaten pro Identität, unabhängig ob der Zertifikatsinhaber ein, zwei oder drei Zertifikate erhält. Der Status „aktiv“ bedeutet, das Zertifikat ist zu einem Stichtag (hier der 15. Tag eines Kalendermonats) gültig und nicht gesperrt.

4.2 Classic

Innerhalb des Tarifs „Classic“ erfolgt die Abrechnung auf Basis generierter (ausgestellter) Zertifikate mit einer Gültigkeit von einem Jahr.

4.3 Classic 2Y

Innerhalb des Tarifs „Classic Pro“ erfolgt die Abrechnung auf Basis generierter (ausgestellter) Zertifikate mit einer Gültigkeit von zwei Jahren.

4.4 Classic Pro

Innerhalb des Tarifs „Classic Pro“ erfolgt die Abrechnung auf Basis generierter (ausgestellter) Zertifikate mit einer Gültigkeit von drei Jahren.

5 ZUSÄTZLICHE LEISTUNGEN DER DEUTSCHE TELEKOM SECURITY GMBH

Die DT Security erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt, das sich nach den zum Zeitpunkt der Auftragserteilung gültigen Listenpreisen richtet, insbesondere folgende zusätzliche Leistungen:

5.1 Workshop

DT Security bietet dem Kunden einen Workshop zur Planung und Integration der TeleSec Shared-Business-CA an. Ziel ist die Erarbeitung eines Konfigurationskonzeptes, die als Grundlage für die

Integration der TeleSec Shared-Business-CA dient. Der Workshop wird auf individuelle Kundenwünsche abgestimmt und findet im Allgemeinen in der Lokation des Kunden statt.

5.2 Schulung

DT Security bietet dem Kunden eine Schulung zur Konfiguration, Nutzung und Bedienung der TeleSec Shared-Business-CA an. Ziel ist es den Funktionsumfang der rollenspezifischen Webseiten, insbesondere der Webseiten für Benutzer, Master- und Sub-Registratoren, kennen zu lernen. Die Schulung findet im Allgemeinen in der Lokation des Kunden statt.

5.3 Kundenindividuelle Leistungen

Leistungen, die individuell für den Kunden im Rahmen der TeleSec Shared-Business-CA erbracht werden (z.B. Bereitstellung und Überlassung einer LDAP-Replikation oder die Erarbeitung eines Migrationskonzepts beim Betreiberwechsel).

5.4 Smartcardleser

Verkauf des Smartcardleser Cardreader Advanced (USB) mit PIN-PAD zur Eingabe der Karten-PIN (siehe Datenblatt).

5.5 Smartcards

Verkauf von folgenden Smartcard-Typen, die im Rahmen der TeleSec Shared-Business-CA verwendbar sind. Die Smartcards basieren auf dem Smartcard-Betriebssystem TCOS und erfüllen höchste Sicherheitsanforderungen.

a) Netkey IDkey
   Smartcard mit bis zu zehn Schlüsselpaaren mit einer Schlüssellänge von 2.048-Bit.
b) Netkey IDkey PlugIn
   Leistungen wie Netkey IDkey, jedoch in der Bauform SIM-PlugIn.
c) Netkey 3.0
   Smartcard mit vier Schlüsselpaaren mit einer Schlüssellänge von 2.048-Bit.
d) Netkey 3.0 PlugIn
   Leistungen wie Netkey 3.0, jedoch in der Bauform SIM-PlugIn.

5.6 Software Card-Module TCOS 3.0 für Base-CSP.

Verkauf eines Softwaretools, das dem Microsoft Base-Smartcard-CSP den Zugriff und Verwendung der TCOS 3.0-Karte ermöglicht.

5.7 Software PKCS#11-SDK für TCOS 3.0

Verkauf der Software-PKCS#11-SDK für TCOS 3.0, dass den Zugriff mittels PKCS#11-Schnittstelle auf die TCOS 3.0-Karte ermöglicht.

6 MITWIRKUNGSPFLICHTEN DES KUNDEN UND NICHTBESTANDTEILE DER LEISTUNG

Die zertifizierte PKI-Dienstleistung TeleSec Shared-Business-CA bietet den Kunden ein Lifecycle-Management für elektronische Zertifikate. Aufgrund der umfangreichen Anforderungen der Normungsgremien (z.B. ETSI, CAB) der Betriebssystem- und Browserhersteller als auch weiterer Nutzergremien, die es ermöglichen, dass die Zertifikate der TeleSec Shared-Business-CA weltweit anerkannt werden, liegt der Funktionsumfang der TeleSec Shared-Business-CA weitgehend fest und wird jährlich durch externe Audits geprüft. Individuelle Anpassungen sind im Rahmen der Dienstleistungen daher nur eingeschränkt möglich.

Die Voraussetzungen (Hardware, Netzanbindung, Konfiguration, Schutzmaßnahmen usw.) für die Nutzung der TeleSec Shared-Business-CA sind dokumentiert und müssen entsprechend umgesetzt werden. Eine Unterstützung im Rahmen der Dienstleistung TeleSec Shared-Business-CA ist nicht vorgesehen. Die Unterstützung für Einsatzszenarien der TeleSec Shared-Business-CA inklusive der Support- und Validierungsdienste sind nicht Bestandteil dieser PKI-Dienstleistung. Beides wird in der Regel durch den Kunden selbst oder seinem IT-Dienstleister durchgeführt.

Die Nutzung der TeleSec Shared-Business-CA setzt beim Kunden ein umfangreiches Wissen im Aufbau und Betrieb einer PKI voraus. Installation, Konfiguration und Leistungsumfang der TeleSec Shared-Business-CA und die durchzuführenden Registrierungstätigkeiten sind in den begleitenden Dokumenten der TeleSec Shared-Business-CA ausführlich beschrieben.

6.1 Mitwirkungspflichten des Kunden

- Der Kunde wird mit technischen und personellen Mitteln alle Anstrengungen unternehmen, damit der PKI-Service TeleSec Shared-Business-CA erfolgreich in die Kundenumgebung integriert und dauerhaft betrieben werden kann.
- Vollumfängliche Unterstützungen der Registrierungsstelle im Incident-, Problem- und Change-Management als auch bei Sicherheitsvorfällen jeglicher Art in Zusammenhang mit der TeleSec Shared-Business-CA.
- Umsetzung von Weisungen der Zertifizierungsstelle (TeleSec Shared-Business-CA).
- Zeitnahe und umfängliche Umsetzung von Änderungen der Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) (Quelle: https://www.telesec.de/de/service/downloads/pki-repository/) oder von Maßnahmen, die durch Änderungen in den Anforderungen relevanter Anforderungsquellen entstanden sind.
- Vollumfängliche Unterstützung bei Audits der TeleSec Shared-Business-CA durch die Registrierungsstelle oder externe Auditoren im Rahmen der Zertifizierung der TeleSec Shared-Business-CA.

6.2 Nicht enthaltene Leistungen

- Im Rahmen des Standard-Service TeleSec Shared-Business-CA sind folgende Leistungen nicht enthalten. Die Erbringung bzw. die Beschaffung dieser Leistungen obliegen dem Kunden selbst.
- Beschaffung, Installation, Konfiguration und Betrieb des/der Registrator-PCs (PC-Arbeitsplatz/-plätze) der Registrierungsstelle(n), die die zur Zertifikatsverwaltung (ausstellen, erneuern, sperren) innerhalb des/der PKI-Mandanten benötigt wird/ werden.
- Beschaffung, Installation, Konfiguration und Betrieb aller Hard- und Softwarekomponenten, wie z. B. Internetzugang, Telefon, Speichermedien, Antiviren-Software, Zugriffsschutz, Software-Updates, die benötigt werden, um den Umgang mit Registrator-PCs und die Zertifikatsverwaltung zu ermöglichen.

- Registrierungsprozess aller Endteilnehmer und Registratoren (außer Master-Registrator), der zur Ausstellung, Erneuerung und Sperrung jeglicher Zertifikate führt.
- Zertifikatsmanagement (Ausstellen, Erneuern und Sperren) inkl. Schlüsselsicherung, -wiederherstellung jeglicher Zertifikatstypen.
- Rollout/Deployment: Zertifikatsverteilung von Soft-PSE und/ oder Smartcards mit korrespondierenden PIN-Brief, insofern die Standardprozesse (Benutzer-Webseite, Mail, SCEP, CMP) dies nicht abbilden, an die Zertifikatsantragsteller bzw. Zertifikatsinhaber oder andere technische Komponenten (z. B. kundenindividueller LDAP-Verzeichnisdienst, Active Directory).
- Personalisierung von Smartcards über eine Personalisierungsanlage, Erstellung von kundenindividuellen PIN-Briefen über einen Drucker, Kuvertierung, Versand und Porto.
- Versand und Verteilung von Smartcard-Lesegeräten und/oder Smartcards an Zertifikatsantragsteller bzw. Zertifikatsinhaber.
- Verskriptung von Software jeglicher Art (z. B. Treiber, Middleware)
- Automatische und/oder manuelle Softwareverteilung und Softwareinstallation (z.B. CA-Zertifikate, Soft-PSE, Treiber, Middleware (CSP, PKCS#11-Modul)).
- Bereitstellung und Verteilung zusätzlicher Validierungsinformationen (z. B. Zertifikatssperrlisten, OCSP Zugriffe) der PKI-Infrastruktur des Trust Centers.
- Entwicklung, Test, Integration und Pflege eines kundenindividuellen CMP-Clients, der mit der CMP-Server-Schnittstelle der TeleSec Shared-Business-CA interagiert (siehe aktuelle CMP-Spezifikation).
- Entwicklung oder Bereitstellung, Pflege und Konfiguration von Anwendungs-Software (z. B. Mail- oder VPN-Software, Netzwerksanmeldung) jeglicher Art, die X.509v3-Zertifikate unterstützen.
- Unterstützung von technischen Zertifikatsanträgen (Request) bei Server, Gateway etc.
- 1st und 2nd Level Service und Support für Endteilnehmer - außer Master-Registratoren - (Details siehe Service Level Agreement).
- Erstellung und Pflege zusätzlicher kundenindividueller Dokumente, die eine technische und/oder prozessorientierte Zertifikatsintegration in die Kundenanwendungen zur Folge haben.
- Unterstützung jeglicher Art wie z. B. Analyse, Projektierung, Consulting, Support, Engineering, die eine Integration des PKI-Service in das Kundennetz zur Folge haben.
- Entwicklung oder Bereitstellung, Pflege von Software-Komponenten jeglicher Art, die eine Synchronisation und/oder Replikation eines LDAP-Verzeichnisdienstes für Zertifikate und Sperrlisten unterstützen.

6.3 Weitere Punkte

- Weiterführende Informationen sind im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.
- Im Falle, dass o.g. Leistungen ganz oder teilweise mit erbracht werden sollen, bedarf es einer individuellen Vereinbarung.

Anhang A: AKRONYME

CA	Certification Authority
CAB	CA/Browser-Forum
CARL	Certification Authority Revcation List
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
ETSI	European Telecommunications Standards Institute (deutsch: Europäisches Institut für Telekommunikationsnormen)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LB	Leistungsbeschreibung
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PIN	Personal Identification Number
PITR	Personelle, Infrastrukturelle und Technische Rahmenbedingungen
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastruktur
PSE	Personal Security Environment
RA	Registration Authority
SCEP	Simple Certificate Enrollment Protocol
SDK	Software Development Kit
SIM	subscriber identity module
SLA	Service Level Agreement
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Socket Layer
TCOS	TeleSec Chipcard Operating System
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network

Anhang B: ERGÄNZENDE LITERATUR

Basis-Dokumentation

- Leistungsbeschreibung (LB)
- Service Level Agreement (SLA)
- Rahmen-SLA für Trust Center Services
- Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)
- Installationsanleitung RA-Platz

Arbeitsanweisung, Schnittstellenbeschreibungen und rollenspezifische Handbücher

- Arbeitsanweisung für Kunden
- Master-Registrator-Handbuch
- Sub-Registrator-Handbuch
- Benutzer-Handbuch
- SCEP-Schnittstelle
- Mail-Schnittstelle