Leistungsbeschreibung & zusätzliche Bedingungen Business.ID

Stand: 12.09.2022

Impressum

Herausgeber

Deutsche Telekom Security GmbH

Bonner Talweg 100

53113 Bonn

Deutschland

nachfolgend – Telekom – genannt

WEEE-Reg.-Nr. DE 56768674

Die gesetzlichen Pflichtangaben finden Sie unter: http://www.telekom.com/pflichtangaben-dtsec

INHALT

1 EINLEITUNG

Mit der PKI-Dienstleistung Business.ID bietet die Deutsche Telekom Security GmbH eine Company Public-Key-Infrastructure (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. Business.ID bietet die Möglichkeit, innerhalb von wenigen Tagen eine PKI für ein 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 Deutsche Telekom Security GmbH zugreifen zu können.

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

2 FUNKTIONEN

Die Dienstleistung Business.ID 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 Business.ID ist in der Zertifizierungsrichtlinie (Telekom Security Certificate Policy (CP)) und der Erklärung zum Zertifizierungsbetrieb (Business. ID CPS) dokumentiert.

2.1 Zertifikatsverwaltung

2.1.1 Webseite

Für die Verwaltung der Business.ID benennt der Kunde (z.B. Firma, Behörde, Institution) mindestens eine verantwortliche Person, auf die ein Master-Registrator-Zertifikat ausgestellt wird, und damit die Funktion des Master-Registrators wahrnehmen soll.

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. Der Sub-Registrator hat die Aufgabe, innerhalb seines Zuständigkeitsbereiches die Ausstellung der Teilnehmer-Zertifikate zu initiieren (siehe Ziffer 2.1, Zentrale Registrierung) oder aber Zertifikatsanträge zu bearbeiten (genehmigen, ablehnen, Widervorlage, Ziffer 2.1, 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.

Im Falle, dass Benutzer selbst Zertifikate beantragen sollen, steht eine gesonderte Webseite zur Verfügung.

Der Kunde greift über eine SSL-gesicherte Internetverbindung (Protokoll HTTPS) auf die Webseiten der Business.ID zu. Erst nach erfolgreicher Authentisierung (Zugriffskontrolle) kann der Rolleninhaber des Kunden seine spezifischen Funktionen der Business.ID nutzen.

Je nach zugeordneter Funktionsrolle (Master Registator, Sub-Registrator oder Benutzer) steht dem Kunden folgender Funktionsumfang zur Verfügung.

a) Webseite für die Rolle „Master-Registrator“

- 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 Business.ID-Dokumenten,
- Erneuerung des Master-Registrator-Zertifikats,
- Erstellung von Statistiken innerhalb der Master-Domäne.

b) Webseite für die Rolle „Sub-Registrator“

- 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 Personalisierungsprozess 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 Business.ID-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“

- 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 Business.ID-Dokumenten

2.1.2 SCEP (Simple Certificate Enrollment Protocol

Die Business.ID unterstützt die Beantragung und Verwaltung von Zertifikaten für Netzwerkkomponenten (Router, Gateways) über das SCEP-Protokoll.

2.1.3 E-Mail

Die Business.ID 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.

2.1.4 CMP (Certificate Management Protocol)

Die Business.ID 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.

2.2 Verzeichnisdienst

Die Deutsche Telekom Security GmbH stellt einen zentralen Verzeichnisdienst für die Business.ID 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, je nach Vereinbarung bzw. Notwendigkeit.

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

2.3 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 2.1). Bei Bedarf kann nach einer Sperrung manuell die Erstellung einer neuen Sperrliste angestoßen werden.

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

2.4 Online-Zertifikatsvalidierung

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

2.5 Vorbelegung von Datenfeldern

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

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

2.6 Informationen und Meldungen

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

3 LEISTUNGEN DER TELEKOM

3.1 Bereitstellung

3.1.1 Allgemeines

3.1.1.1 Domänenkonzept

Der Kunde wird als eigenständiger Mandant innerhalb der Business.ID 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 Business.ID auch als Masterdomäne, und die Untergliederung in Zuständigkeitsbereiche als Subdomäne(n) bezeichnet. Der Name des PKI-Mandanten als auch der Zuständigkeitsbereich sind Bestandteil des Antragstellers im Zertifikat.

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

3.1.1.2 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 der 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 der entsprechenden Zertifikate in den jeweiligen Zertifikatsspeichern bzw. Anwendungen.

3.1.1.3 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 Business.ID, im Wesentlichen der Zertifizierungsrichtlinie (Certificate Policy (CP)) der Telekom Security (Telekom Security Certificate Policy (CP)) und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)). Die Business.ID bietet dazu zwei Möglichkeiten an.

- **Zentrale Registrierung**
  Die Ausstellung des Zertifikats für Personen und Geräte (siehe Ziffer 2.1) 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 2.1) eintreffen.
- **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.

3.1.2 Bereitstellung Business.ID

Damit die Business.ID 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 (Smartcards, Master-Registrator Zertifikat, Tools) enthalten, welche die Basis für den Zugriff auf das Trust Center bilden. Die Grundausstattung unterstützt dabei den Kunden sowohl bei der Ausstellung von Soft-PSE (Datei bestehend aus Zertifikat und privatem Schlüssel) als auch beim 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 Business.ID
- Überlassung eines oder mehrerer Sub-Registrator-Zertifikat(e) zur Verwaltung der vom Kunden angelegten Zuständigkeitsbereiche (Sub-Domänen) innerhalb der Business.ID
- SmartBridge: Hilfstool zur Erzeugung von Schlüsselpaaren und zur Kommunikation mit der CA
- Dokumentation, bestehend aus der Zertifizierungsrichtlinie (CPS), dem Service Level Agreement (SLA), der Installationsanleitung Registrator-PC und den rollenspezifischen Handbüchern
- Im Rahmen der Standard Leistung erfolgt die Validierung von Organisationsdaten und den zugehörigen Domänen bis zu einer Anzahl von maximal 5 Organisationen und maximal 15 Internet-Domänen. Eine größere Anzahl ist im Einzelfall separat zu vereinbaren und als optionale Leistung kostenpflichtig zu beauftragen.

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

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

Hinweis: ein notwendiger Smartcard Leser gehört nicht zum Lieferumfang der Business.ID. Hier kann ein handelsüblicher Kartenleser oder der onboard Kartenleser des jeweiligen Standard-PCs des Kunden verwendet werden.

3.1.3 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 3.1.1.1). Weitere Zertifikatsinformationen sind in der Zertifizierungsrichtlinie (Certificate Policy (CP)) der Telekom Security und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement (CPS)) dokumentiert.

Die Zertifikatsgültigkeit kann in x Tagen eingestellt werden und ist für die jeweils eingerichteten PKI-Mandanten gültig. Somit lassen sich z. B. ein, oder zwei oder drei Jahre Laufzeit einfach abbilden. Optional sind andere Gültigkeitszeiträume konfigurierbar, die aber nicht gegen Anforderungen der Normungsgremien usw. verstoßen dürfen.

3.1.3.1 Zertifikate für natürliche Personen und Personen- und Funktionsgruppen

Entsprechend der Konfiguration können nur bestimmte Zertifikatstypen 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.

3.1.3.2 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.

Bei Server-Zertifikaten können neben dem „Common Name“ noch bis zu vier (4) weitere Server-Namen (SAN) eingetragen werden. Darüber hinaus sind keine weiteren Einträge möglich.

3.1.3.3 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.

3.2 Betrieb

3.2.1 Trust Center Betrieb

Mit der Business.ID steht eine PKI-Infrastruktur 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. Das „Lifecyclemanagement“ der Zertifikate, die Schlüsselverwaltung und auch die Registrierung obliegen somit dem Kunden selbst.

3.2.2 Vor Ort Betrieb (PITR)

Der Betrieb beim Kunden setzt die Einhaltung bestimmter Rahmenbedingungen hinsichtlich Personen, Infrastruktur und Technik voraus.

Alle Rahmenbedingungen und Verhaltensregeln werden im Dokument „Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)“ beschrieben.

Insbesondere sind hier die Regelungen zum Registrator Arbeitsplatz enthalten.

3.3 Optionale Leistungen

Die Deutsche Telekom Security GmbH 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:

3.3.1 Workshop

Business.ID bietet dem Kunden einen Workshop zur Planung und Integration der Business.ID an. Ziel ist die Erarbeitung eines Konfigurationskonzeptes, die als Grundlage für die Integration der Business.ID dient. Der Workshop wird auf individuelle Kundenwünsche abgestimmt und findet in der Regel online oder in Abstimmung auch in der Lokation des Kunden statt.

3.3.2 Schulung

Business.ID bietet dem Kunden eine Schulung zur Konfiguration, Nutzung und Bedienung der Business.ID 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.

3.3.3 Smartcards

Der Verkauf von folgenden Smartcard-Typen, die im Rahmen der Business.ID verwendbar sind, ist auf Anfrage separat möglich. 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.

4 MITWIRKUNGSLEISTUNGEN DES KUNDEN

Die PKI-Dienstleistung Business.ID ist ETSI zertifiziert und bietet dem Kunden ein Lifecycle-Management für elektronische Zertifikate. Aufgrund der umfangreichen Anforderungen sowohl der Normungsgremien (z.B. CAB oder Root-Programme) der Betriebssystem- und Browserhersteller als auch weiterer Nutzergremien, die es ermöglichen, dass die Zertifikate der Business.ID weltweit anerkannt werden, liegt der Funktionsumfang der Business.ID weitgehend fest und wird jährlich durch externe Audits geprüft.

Die Voraussetzungen (Hardware, Netzanbindung, Konfiguration, Schutzmaßnahmen usw.) für die Nutzung der Business.ID sind dokumentiert und müssen entsprechend umgesetzt werden. Eine Unterstützung im Rahmen der Dienstleistung Business.ID ist nicht vorgesehen. Die Unterstützung für Einsatzszenarien der Business.ID 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 Business.ID setzt beim Kunden ein umfangreiches Wissen im Aufbau und Betrieb einer PKI voraus. Installation, Konfiguration und Leistungsumfang der Business.ID und die durchzuführenden Registrierungstätigkeiten sind in den begleitenden Dokumenten der Business.ID ausführlich beschrieben. Die Dokumente werden in den jeweiligen Business.ID Frontends zum Download angeboten

4.1 Mitwirkungspflichten des Kunden

Der Kunde verpflichtet sich Mitwirkungsleistungen, die zur ordnungsgemäßen Leistungserbringung erforderlich sind, insbesondere jedoch nachfolgende, unentgeltlich, rechtzeitig und in erforderlichem Umfang zu erbringen:

Der Kunde verpflichtet sich und seine Mitarbeiter zur Einhaltung der Trust-Center Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS). Insbesondere ist er verpflichtet, sicherzustellen, dass alle Angaben zur Einrichtung der Masterdomäne sowie zum Ausstellen und Verwalten der Zertifikate den Tatsachen entsprechen. Für die Einrichtung der Masterdomäne sind Identifikationsnachweise vorzulegen. Organisationsänderungen hat der Kunde unverzüglich schriftlich bei der Telekom anzuzeigen.

Der Kunde ist verpflichtet, seine Nutzer rechtzeitig vor Beginn der Nutzung über die Einzelheiten dieses Vertrages, insbesondere über die Rechte und Pflichten nach Maßgabe der Allgemeinen Geschäftsbedingungen und der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) zu unterrichten. Der Kunde haftet für alle Pflichtverletzungen seiner Nutzer sowie sonstiger Dritter, die Pflichtverletzungen in der vom Kunden beherrschbaren Sphäre begehen, soweit er nicht den Nachweis führt, dass er die Pflichtverletzungen nicht zu vertreten hat.

Der Kunde verpflichtet sich im Rahmen dieser Leistung die gesetzlichen Bestimmungen und Anforderungen der Datenschutz-Grundverordnung (DSGVO) einzuhalten und die erforderliche Einwilligung des jeweils Betroffenen einzuholen.

Der Kunde wird mit technischen und personellen Mitteln alle Anstrengungen unternehmen, damit der PKI-Service Business.ID erfolgreich in die Kundenumgebung integriert und dauerhaft betrieben werden kann. Dazu gehört insbesondere:

- Beschaffung, Installation, Konfiguration und Betrieb des/der Registrator-PCs (PC-Arbeitsplatz/-plätze, Kartenleser) der Registrierungsstelle(n), die die zur Zertifikatsverwaltung (ausstellen, erneuern, sperren) innerhalb des/der PKI-Mandanten benötigt wird/ werden.
- Beschaffung des Smartcard-Leser, welcher kundenseitig bereitgestellt werden muss.
- 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.
- Validierung und Konfiguration von Massendaten (Organisationsdaten und Internetdomänen) durch die Sub-CA
- 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).
- Vollumfängliche Unterstützungen der Registrierungsstelle(n) im Incident-, Problem- und Change-Management als auch bei Sicherheitsvorfällen jeglicher Art in Zusammenhang mit der Business.ID.
- Eingereichte Dokumente müssen in deutscher oder englischer Sprache verfasst sein.
- Umsetzung von Weisungen der Zertifizierungsstelle (Business.ID).
- 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 Business.ID durch die Registrierungsstelle oder externe Auditoren im Rahmen der Zertifizierung der Business.ID.

4.2 Nicht enthaltene Leistungen, Nichtbestandteil des Service

Im Rahmen des Standard-Service Business.ID sind folgende Leistungen nicht enthalten. Die Erbringung bzw. die Beschaffung dieser Leistungen obliegen dem Kunden selbst.

- 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 Business.ID 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.

5 MINDESTLAUFZEIT/BEENDIGUNG

5.1 Tarifmodelle

5.1.1 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 16. Tag eines Kalendermonats) gültig und nicht gesperrt.

5.1.2 Classic

Innerhalb des Tarifs „Classic“ erfolgt die Abrechnung auf Basis generierter (ausgestellter) Zertifikate mit einer Gültigkeit von einem Jahr. Dieses Tarifmodell ist nur für Systemhäuser/Wiederverkäufer (Reseller) nutzbar.

5.1.3 Classic 2Y

Innerhalb des Tarifs „Classic 2Y“ erfolgt die Abrechnung auf Basis generierter (ausgestellter) Zertifikate mit einer Gültigkeit von zwei Jahren. Dieses Tarifmodell ist nur für Systemhäuser/Wiederverkäufer (Reseller) nutzbar.

5.1.4 Classic Pro

Innerhalb des Tarifs „Classic Pro“ erfolgt die Abrechnung auf Basis generierter (ausgestellter) Zertifikate mit einer Gültigkeit von drei Jahren. Dieses Tarifmodell ist nur für Systemhäuser/Wiederverkäufer (Reseller) nutzbar.

5.2 Abnahme der Leistung

Die Leistung gilt ab dem Tag der Zustellung der Verwaltungszertifikate als abgenommen. Damit startet die Vertragslaufzeit und die Entgeltpflicht.

5.3 Vertragsbeginn, -laufzeit und Kündigung

Die Mindestüberlassungszeit für Business.ID beträgt ab Vertragsabschluss 36 Monate und verlängert sich automatisch um 12 Monate, wenn sie nicht mit einer Frist von 3 Monaten zum Ende der Mindestüberlassungszeit bzw. des jeweiligen Verlängerungszeitraums gekündigt wird.

Die Gültigkeitsdauer der Zertifikate des Tarifmodells Classic und Classic Pro bleiben von der Kündigung unberührt. Die auf Basis des Tarifmodells Advanced ausgestellten Zertifikate werden nach dem Ende der Vertragslaufzeit gesperrt und verlieren die Gültigkeit.

5.4 Zahlungsbedingungen

5.4.1 Monatliche Preise

Monatliche Preise sind, beginnend mit dem Tag der Leistungserbringung, für den Rest des Monats anteilig zu zahlen. Danach sind diese Preise monatlich im Voraus zu zahlen. Ist der Preis für Teile eines Kalendermonats zu berechnen, so wird dieser für jeden Tag anteilig berechnet.

5.4.2 Einmalige Preise

Einmalige Preise sind nach Erbringung der Leistung zu zahlen.

5.5 Einseitige Leistungsänderungen

Die Deutsche Telekom Security GmbH behält sich einseitige Leistungsänderungen und Entgeltreduzierungen zu Gunsten des Kunden vor. Der Kunde erklärt sich mit diesen Anpassungen einverstanden.

In Abweichung zu dem vereinbarten Schriftformerfordernis wird die Deutsche Telekom Security GmbH den Kunden über etwaige Anpassungen durch Übersendung aktualisierter Versionen der bestehenden Vertragsunterlagen per E-Mail informieren, welche die bestehenden Unterlagen ersetzen.

6 MITGELTENDE DOKUMENTE

Ergänzend zu dieser Leistungsbeschreibung gelten die folgenden Dokumente:

- AGB DTSec IT Leistungen
- Trust Center Certificate Policy (CP)
- Erklärung zum Zertifikatsbetrieb, Business.ID (CPS Business.ID)
- Service Level Agreement Business.ID (SLA BUSINESS.ID)
- Rahmen-SLA für Trust Center Services (Rahmen-SLA)
- Leistungs- und Nutzungsbedingungen der Business.ID
- Personelle, Infrastrukturelle und Technische Rahmenbedingungen (PITR)

7 GLOSSAR/ ABKÜRZUNGSVERZEICHNIS

Begriff	Beschreibung
CA	Certification Authority
CAB	CA/Browser-Forum
CARL	Certification Authority Revocation 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 Infrastructure
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