Leistungsbeschreibung & zusätzliche Bedingungen Magenta Security OneTimePass.ID

Stand: 01.07.2022

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

Magenta Security OneTimePass ID – im Folgenden OneTimePass - bietet eine starke 2-Faktor-Authentifizierung auf Basis eines dynamischen Einmalpasswortsystems.

Der Service generiert mit Hilfe verschiedener Token (Authentifikationsmedien) Einmalpasswörter zur Anmeldung bei Online-Diensten und geschützten Systemen des Kunden (OneTimePass-Provider). Es steht eine eigene Benutzerverwaltung über Service-Portale im Internet zur Verfügung, zur Verwaltung und Zuweisung der Authentifikationsmedien zu den Benutzern des Kunden.

Die Administration ist in insgesamt vier Berechtigungsstufen (General Supervisor, Supervisor, Administrator und User) gestaffelt, um diese flexibel an Kundenwünsche / auf Kundenstrukturen (Niederlassungen, Abteilungen etc.) anpassen zu können.

Der OneTimePass-Dienst wird im hochsicheren und zertifizierten Telekom Trust Center betrieben.

Anbieter der Trust Center-Dienste und -Produkte ist die Deutsche Telekom Security GmbH, nachfolgend Telekom genannt.

2 FUNKTIONEN - AUTHENTIFIKATIONSMEDIEN

Die Telekom verkauft dem Kunden (im Folgenden: OTP-Provider) OneTimePass-Authentifikationsmedien (Hard- und/oder Software) zur wiederkehrenden Erzeugung von Einmalpasswörtern durch den Nutzer. Die verschiedenen Authentifikationsmedien sind in den folgenden Abschnitten beschrieben:

2.1 Kartenleser OTP-Reader III

Der Offline-Kartenleser OTP-Reader III mit Display und Tastatur wird zur Generierung von Einmalpassworten für OneTimePass genutzt. Unterstützt werden Smartcards bis TCOS 3.0. Die Batterien (Knopfzellen 2x CR-2025) können problemlos erneuert werden.

2.2 Chipkarte NetKey 3.0

Die TCOS Chipkarte NetKey 3.0 ist eine anonymisierte Krypto-Chipkarte, d.h. sie enthält keine Personendaten. Die Chipkarte wird in der sicheren Umgebung des Telekom Trust Centers produziert und dient zur Berechnung des dynamischen Einmalpasswortes.

Bei Nutzung der NetKey 3.0 mit dem OTP-Reader III wird beim Initialisieren der Karte (Brechen der NullPIN) sowohl die PIN als auch die PUK vom Nutzer festgelegt.

2.3 OneTimePass Token III

Der OneTimePass Token ist ein kompaktes Gerät, welches auf Knopfdruck Einmalpasswörter anzeigt. In diesen Token kommt keine Chipkarte zum Einsatz (keine Migration zu Zertifikats-Dienstleistungen möglich!). Die Token werden in einer sicheren Umgebung des Herstellers personalisiert. Die Übertragung der Geheimnisse vom Hersteller zur Telekom erfolgt grundsätzlich verschlüsselt.

Zur Erhöhung der Sicherheit wird bei Authentifikationen immer eine 4-stellige Server-PIN benötigt, die der Benutzer sich auf der Service Website für User (onetimepass.telesec.de) vergeben muss. Alternativ kann vom OneTimePass-Administrator die PIN-Generierung (Zufallszahl) und die PIN-Verteilung (per Email) angestoßen werden.

Der OneTimePass Token kann von OneTimePass-Nutzern verwendet werden. Für die Administration von OneTimePass kann der OneTimePass Token nach Freigabe des Providers auch eingesetzt werden.

2.4 OneTimePass SMS

Mit „OneTimePass SMS“ erhält der OneTimePass-Nutzer seine Einmalpasswörter vom OneTimePass-Server direkt per SMS. Der OneTimePass-Nutzer verwendet dabei sein aktuelles Mobiltelefon und seinen vorhandenen Mobilfunkvertrag bei einem beliebigen Mobilfunk-Provider. OneTimePass SMS ist nahezu weltweit nutzbar. Die Telekom ist nicht verantwortlich für den Empfang von SMS. Hierzu steht der Kunde in Verbindung mit dem Mobilfunk-Provider auf Benutzerseite in der Pflicht.

Die Einmalpassworte werden sofort nach Prüfung der Mobilfunknummer auf Berechtigung von dem OneTimePass-SMS-Gateway versendet. Da es für SMS keine Priorisierung in den

Mobilfunknetzen gibt, kann die Telekom nicht garantieren, wie lange es von der Anfrage bis zur Zustellung des Einmalpasswortes per SMS dauert.

Hinweise zur Benutzung des SMS-Token entnehmen Sie bitte dem dazugehörigen Benutzerhandbuch.

2.5 OneTimePass Software-Token

Zur Vervollständigung des Portfolios werden Software-Token für verschiedene Betriebssysteme angeboten (weitere Token für mobile Endgeräte in Vorbereitung).

2.5.1 OneTimePass SoftToken für Microsoft Windows (in Verbindung mit Smartcard)

Der OneTimePass SoftToken ist eine spezielle Windows Applikation, welche die Generierung der Einmalpasswörter übernimmt. Der OneTimePass-SoftToken nutzt eine vorhandene Chipkarte in einem installierten Kartenleser zur Generierung der Einmalpasswörter.

Diese Software ist für sogenannte Online-Chipkartenleser (mit direkter PC-Anbindung) erforderlich (z.B. vorhandener Kartenleser am Arbeitsplatz oder integrierter Kartenleser im Notebook). Des Weiteren beinhaltet der OneTimePass SoftToken alle Funktionen für effizientes PIN-/PUK-Handling.

Der OneTimePass SoftToken gehört zum Lieferumfang der OneTimePass-Dienstleistung und kann im Downloadbereich der jeweiligen Service Webseiten heruntergeladen werden.

Der OneTimePass SoftToken ist mehrsprachig in Deutsch und Englisch verfügbar.

Zur Nutzung des OneTimePass SoftToken wird eine Microsoft Windows-Plattform (Windows 10/11) benötigt.

Voraussetzung zum Betrieb ist ein beliebiges Chipkartenterminal (Voraussetzung: Online-Leser, also mit Anbindung an einen PC), welches unter Windows nutzbar ist.

2.5.2 OneTimePass SmartToken (SMT)

Zur Generierung von Einmalpassworten bietet die Telekom den OneTimePass SmartToken als reine Softwarelösung an.

Die Applikation ist über die AppStores der Betriebssystemhersteller verfügbar.

Der Nutzer erhält nach der Einrichtung durch den OneTimePass Administrator einen Aktivierungscode via Email. Beim ersten Start der App wird diese für die Nutzung mit der OneTimePass-Plattform parametrisiert / initialisiert. Hierzu wird eine Onlineverbindung benötigt. Zur Nutzung des SmartTokens ist nach erfolgreicher Initialisierung keine Onlineverbindung erforderlich.

Zur Verwendung des SmartToken definiert der Nutzer eine PIN und eine PUK. Weitere Hinweise zur Benutzung des SmartToken entnehmen Sie bitte dem dazugehörigen Benutzerhandbuch.

2.5.3 SmartToken für Apple iOS

Der OneTimePass SmartToken für iOS kann in Verbindung mit einem Apple iPhone und iPad ab iOS-Version 11.0 oder höher (SmartToken 1.21) , sowie in Verbindung mit der Apple-Watch genutzt werden.

Die App wird über den Apple AppStore distribuiert:

- http://itunes.apple.com/de/app/telesec-onetimepass/id452199072

2.5.4 SmartToken für Google Android

Der OneTimePass SmartToken steht zur Verfügung für Smartphones und Tablets mit Android Betriebssystem ab Version 5.0 sowie für Wearables/Smartwatches mit Wear OS

Die App wird über den Google Playstore distribuiert:

- https://play.google.com/store/apps/details?id=de.otp.main

2.6 Statische OneTimePass-Nutzer

Ein statischer OneTimePass-Nutzer kann für das automatisierte Überwachen der OneTimePass-System-Verfügbarkeit verwendet werden.

Hilfreich sind statische Nutzer auch für einen Service Desk, um Nutzer, die ihr Authentifikationsmedien verloren haben, kurzfristig und temporär wieder arbeitsfähig zu machen. Die Freigabe, statische Nutzer anlegen zu können, erfolgt nur nach formloser schriftlicher Beauftragung durch den OTP-Provider.

2.7 Systemvoraussetzungen

2.7.1 Standard Authentifikationsmedien

Zum Betrieb der OneTimePass-Authentifikationsmedien durch den OneTimePass-Nutzer sind prinzipiell keine besonderen Systemvoraussetzungen erforderlich. Es ist keine zusätzliche Client-Software erforderlich.

2.7.2 OneTimePass SMS

Zur Nutzung von OneTimePass SMS benötigt der OneTimePass-Nutzer ein aktuelles Mobiltelefon und einen beliebigen Mobilfunkvertrag.

Für den Empfang der Einmalpasswörter via SMS ist Mobilfunk-Netzabdeckung erforderlich. OneTimePass kann nahezu weltweit mit einer Vielzahl an Mobilfunkprovidern genutzt werden. Ein uneingeschränkter SMS-Empfang hängt von den jeweiligen Netzbetreibern und nationalen Regelungen ab und kann nicht garantiert werden.

2.7.3 OneTimePass SmartToken

Die Voraussetzungen für den Einsatz der SmartToken entnehmen Sie bitte dem Kapitel 2.5

3 LEISTUNGEN DER TELEKOM

3.1 Bereitstellung - Tarifmodelle

Mit der OneTimePass Dienstleistung stehen dem Kunden verschiedene Tarifmodelle zur Verfügung:

3.1.1 OneTimePass-Preismodell

Die OneTimePass-Nutzer werden monatlich pauschal verrechnet (abhängig von der verwendeten User-Staffel) und sind unabhängig von der Anzahl der Authentifikationen. Die Bereitstellung der Dienstleistung beinhaltet die Auslieferung von zwei OTP-Reader III und zwei SmartCard NetKey 3.0 für Administratoren. Dieses Modell eignet sich für beliebig viele Nutzer. Im Tarifmodell OneTimePass werden folgende Staffeln bzw. Pakete unterschieden:

OneTimePass Überlassung 10, ...

Mit OneTimePass Überlassung (10, 25, 50, 100, 250, 500, 1.000, 2.500, 5.000, 7.500, 10.000 und 10.000+) wird für den Kunden die Nutzeranzahl entsprechend der Pakete begrenzt, unabhängig davon, in wie vielen OneTimePass-Nutzergruppen der OneTimePass-Nutzer verwaltet wird. Durch Up- bzw. Downgrades können die Preisstaffeln verändert werden.

OneTimePass-Extension 25, ...

Mit OneTimePass Extension (25, 50, 100, 500 und 1.000) können auch kleinere Stufensprünge erreicht werden. Somit kann z.B. OneTimePass 1.000 (= 1.000 Nutzer) um eine OneTimePass-Extension 500 (= 500 Nutzer) auf insgesamt 1.500 Nutzer erweitert werden. Die OneTimePass-Extension Pakete bleiben bis zur Kündigung im Bestand und rechnen sich nicht mit einem Up-

bzw. Downgrade von OneTimePass auf. Wird also im o.g. Beispiel OneTimePass 1.000 auf OneTimePass 2.500 erhöht, bleibt die Extension 500, sofern diese nicht gekündigt wurde, bestehen. Es stehen somit 3.000 Nutzer zur Verfügung.

Das Volumen einer Extension darf nicht größer sein, als das Volumen des beauftragen OneTimePass-Paketes. Die Extensions 500 und 1.000 dürfen somit nicht für OneTimePass 100 und 250 genutzt werden.

3.1.2 OneTimePass-Teststellung

Die Teststellung ist eine vom Leistungsumfang nicht eingeschränkte Dienstleistung, monatliche Kosten entstehen nicht. Für die Teststellung wird lediglich ein einmaliges Bereitstellungsentgelt berechnet und beinhaltet zwei OTP-Reader III, zwei SmartCard NetKey 3.0 und fünf OneTimePass Token III. Die Laufzeit einer Teststellung beträgt max. 3 Monate (oder nach Vereinbarung). Erfolgt nach der Teststellung eine Beauftragung, wird der Bereitstellungspreis verrechnet.

3.1.3 OneTimePass-Reseller

Bei Interesse am Reselling von OneTimePass kontaktieren Sie bitte Ihre Telekom-Ansprechpartner.

3.1.4 Lieferbedingungen

Die OneTimePass-Authentifikationsmedien werden in der Regel nur an OneTimePass-Provider ausgeliefert (Ausnahmen gegen Aufpreis).

Die Verteilung der OneTimePass-Authentifikationsmedien (inkl. Bedienungsanleitung) an die OneTimePass -Nutzer übernimmt der OneTimePass-Provider.

Die TCOS Chipkarte NetKey 3.0 ist in der Dual-Use-Liste aufgeführt und unterliegt somit den besonderen Export- und Importbestimmungen (ggf. sind Nutzungsbeschränkungen im Ausland zu beachten).

3.2 Betrieb

Die zentrale Authentifikationsdienstleistung wird von der Telekom im Telekom Trust Center betrieben und dem Provider für die vereinbarte Vertragszeit überlassen.

Der mittels OneTimePass geschützte Server stellt via Internet eine elektronische Gültigkeitsanfrage (Standard **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice (RADIUS) gemäß Protokoll RFC 2865 und RFC 2868) an die OneTimePass-Plattform im Telekom Trust Center. Dieser prüft die Gültigkeit des Einmalpasswortes und sendet die für das entsprechende Nutzer- bzw. Gruppenprofil eingestellten Attribute zurück. Die Anbindung kann auch alternativ mittels SOAP oder Federation Services erfolgen.

Das Telekom Trust Center stellt keine Beziehung der Abfrage zu einer natürlichen Person her; lediglich die Identifikationsnummer der Karte bzw. der Alias-Name ist bekannt.

3.2.1 OneTimePass-Dienste-Plattform

Die Telekom betreibt im Telekom Trust Center eine zentrale OneTimePass-Dienste Plattform, welche die eingereichten Einmalpasswörter des OneTimePass-Providers auf Gültigkeit prüft. In der Dienste-Plattform werden alle Provider verwaltet. Jeder Provider kann seinerseits individuelle

Gruppen und Profile verwalten. Durch diese zentrale Verwaltung können die OneTimePass-Authentifikationsmedien (s. Punkt 2) für unterschiedliche Anwendungen bei unterschiedlichen Providern eingesetzt werden, sofern sie vom jeweiligen Provider freigeschaltet wurden.

3.2.2 OneTimePass-Group

Der OneTimePass-Provider erhält die Möglichkeit, Nutzer in sogenannte Usergroups einzuteilen, um diese nach Anwendungen und Kundengruppen / Abteilungen (Controlling, Sales, ...) zu unterscheiden bzw. zu identifizieren. Allen Nutzern einer Group können auf Wunsch die gleichen RADIUS-Attribute zugeordnet werden. Somit vereinfacht sich die Administration der einzelnen Nutzer. Dem OneTimePass-Provider steht die Möglichkeit zur Verfügung, für die OneTimePass-Group eine Begrenzung der OneTimePass-Nutzer einzurichten. Je nach Preismodell bzw. Angebotspaket kann die Anzahl der OneTimePass-Groups durch die Telekom eingeschränkt werden.

3.2.3 OneTimePass Administration auf Kundenseite

Zur Administration der OneTimePass Dienstleistung erhält jeder Provider 2 der maximal 10 möglichen General Supervisor-Berechtigungen mit dem OneTimePass-Authentifikationsmedium SmartCard mit OTP Reader III zur Identifikation auf den Internet-Service-Seiten des Trust Centers.

Alle weiteren Funktionen und Berechtigungen der insgesamt vierstufigen Service Portale (General Supervisor, Supervisor, Administrator, User) werden vom Provider verwaltet und in den entsprechenden Handbüchern beschrieben.

3.2.4 OneTimePass Nutzer

Der OneTimePass-Nutzer wird durch den OneTimePass-Provider identifiziert und erhält ein ihm zugeordnetes Authentifikationsmedium. Die Administration der Nutzer erfolgt über die Internet-Service-Seiten des Trust Centers. Die Berechtigungen bzw. Leistungen sind im entsprechenden Benutzerhandbuch beschrieben.

3.2.5 Prüfung der Einmalpasswörter

Bei OneTimePass handelt es sich um eine sogenannte Zwei-Faktor-Authentifikation, die auf den beiden Faktoren „Besitz“ und „Wissen“ basiert.
Abhängig von der Art des verwendeten Authentifikationsmediums wird eine 4-stellige Server-PIN benötigt.

Bei einem Authentifikations-Request eines Nutzers wird somit der verwendete Aliasname des Users und sein Einmalpasswort (8-stellig) und ggf. die Server-PIN (4-stellig) übertragen.

Dem OneTimePass-System sind die nächsten 15 Passwörter bekannt. Sofern dieser Rahmen überschritten wird (z.B.: Generierung von Passwörtern ohne diese zur Authentifikation zu nutzen), besteht die Möglichkeit einer Synchronisation.

3.2.5.1 RADIUS

Um die OneTimePass Standard Dienstleistung nutzen zu können, benötigt der Provider in der Regel nur seine vorhandene Infrastruktur wie z.B. einen Router, VPN-Gateway oder Vergleichbares sowie das RADIUS-Protokoll (RFC 2865 und RFC 2868) zur Anbindung ans Trust Center. Die OneTimePass-Dienstleistung umfasst lediglich die Authentifizierung des Nutzers.

3.2.5.1.1 RADIUS – Nutzer Profil

Die Telekom stellt dem OneTimePass-Provider die RADIUS-Attribute nach RFC 2865 und RFC 2886 zur Verfügung. Diese Attribute können einer OneTimePass-Group oder einem OneTimePass-Nutzer zugeordnet werden. Die Administration erfolgt über die Internet Service-Seiten des Telekom Trust Centers.

3.2.5.1.2 RADIUS – Regeln

Die OneTimePass-Plattform unterstützt die Erstellung von Regelwerken, die es ermöglichen, für eine Gruppe festzulegen, unter welchen Bedingungen (Eingangs-Attribute) welche Aktionen (Ausgangs-Attribute) durchgeführt werden. Die Summe der Bedingungen und Aktionen werden als Events bezeichnet. Die Regelverwaltung wird über die Internet Service Seite für Administratoren durchgeführt.

3.2.5.2 Federation Services

Die vorhandenen Schnittstellen wurden um Federation Services ergänzt, die es Kunden ermöglicht, via SAML 2.0 und OpenID-Connect OneTimePass-Authentifizierungen durchzuführen.

Hierüber kann auf OTP Gruppenebene ein SingleSignOn zwischen mehreren SAML Service-Providern bzw. OpenID-Connect Clients realisiert werden.

Die Federation Services dienen einzig der Authentifikation; erweiterte Autorisierungs-Funktionalitäten werden in der derzeitigen Konfiguration nicht unterstützt!

Die zur Nutzung der Federation Services benötigten Einstellungen werden über die General-Supervisor Service-Webseiten vorgenommen.

Zu den Federation Services zählen:

- SAML 2.0
- OpenID Connect
- REST API

Bei Interesse an den Federation Services steht auf Anfrage eine ausführliche Dokumentation zur Verfügung. Weitere Hinweise zur Benutzung der Federation Services entnehmen Sie bitte dem dazugehörigen Benutzerhandbuch.

3.2.6 OneTimePass Administration

3.2.6.1 Internet Service Portal – Provider

Die Telekom stellt vier Service-Portale für den Kunden zur Verfügung. Die Kernfunktionen umfassen:

OneTimePass General Supervisor

Der General Supervisor ist die höchste Instanz zur Verwaltung des OneTimePass Dienstes. Zur Nutzung sind die mitgelieferten (oder bei Bedarf zusätzlich bestellten) Smartcards samt OTP Reader III vorgesehen. Es können maximal 10 General Supervisor eingerichtet werden. Mit dieser Berechtigung werden die grundlegenden Funktionalitäten und Leistungsmerkmale eingerichtet, sowie Benutzergruppen und die zugehörigen Supervisor eingerichtet.

OneTimePass Supervisor

Der Supervisor kann (je nach Konfiguration des General Supervisor) Berechtigung für eine oder mehrere Benutzergruppen besitzen und verwaltet dazu die Administratoren seiner Benutzergruppen.

OneTimePass Administrator

Der Administrator kann (je nach Konfiguration des Supervisor) Berechtigung für eine oder mehrere Benutzergruppen besitzen und verwaltet in seinem Portal die Zuordnung der Benutzer zu den verwendeten Authentifikationsmedien.

OneTimePass User

Für den User gibt es ein Portal zur Selbstverwaltung (FAQ, Download von Handbüchern, PIN-Verwaltung, Sperren bei Verlust).

Alle weiteren Funktionen sind ausführlich in den jeweiligen Benutzerhandbüchern beschrieben, die im Downloadbereich der jeweiligen Hierarchie oder bei der Telekom auf Anfrage verfügbar sind.

3.2.6.2 SOAP-Administration

Alternativ zur Nutzung der Service-Webseiten kann die OneTimePass-Administration auch SOAP-basiert erfolgen. Die administrativen Tätigkeiten wurden in Form spezifizierter SOAP-Aufrufe nachgebildet und als Application Programming Interface (**API**) bereitgestellt. Somit kann ein bereits existierendes Administrationsportal leicht an OneTimePass angebunden werden. Die Authentifikation erfolgt hier durch ein Client-Zertifikat der Server.ID. Das optional erhältliche Dokument „OneTimePass SOAP-Spezifikation Vn.pdf“ beinhaltet den kompletten Befehlssatz inkl. WSDL-Beschreibung.

3.2.6.3 Bulk-Verwaltung

Für das effiziente gleichzeitige Verwalten / Administrieren vieler Benutzer werden mit der Bulk-Verwaltung (im Service Portal für Administratoren oder via SOAP) die Funktionen für Massen-Administration, Snapshots und User-Exports angeboten.

Die Massenadministration ermöglicht das Anlegen, Ändern oder Löschen von bis zu 5000 Datensätzen. Die Datensätze werden im CSV-Format übergeben, wobei als Trennsymbol das Semikolon Verwendung findet.

Mit den Funktionen Snapshots (Backup vor Massenimport) und User-Export stehen zwei weitere leistungsfähige Werkzeuge zur Verfügung. Eine ausführliche Anleitungen findet man im Benutzerhandbuch für Administratoren.

3.2.6.4 Internet Service Portal – Nutzer

Die Telekom betreibt für die OneTimePass-Nutzer ein Portal zu Selbstverwaltung mit folgenden Funktionen:

- Vergabe von Sperrpasswörtern
- Synchronisation von Token oder Chipkarte
- Darstellung des Nutzerprofils
- Sperrservice
- Fragen und Antworten (FAQ)
- Statistiken und Übersichten
- Downloadbereich (Handbücher etc.).

3.2.7 Sperrservice

Da es sich bei OneTimePass um eine zentrale Dienstleistung handelt, besteht für den OneTimePass-Nutzer die Möglichkeit, sich mit dem OneTimePass-Authentifikationsmedium bei mehreren OneTimePass-Providern anzumelden ohne ihre Anwendung zu beeinträchtigen bzw. ihren sicheren Zugang zu gefährden. Aus diesem Grund unterscheidet OneTimePass nach unterschiedlichen Sperrmöglichkeiten für Nutzer und Administratoren.

Weitere Hinweise zu Sperrmöglichkeiten entnehmen Sie bitte den dazugehörigen Handbüchern.

3.2.8 Systemvoraussetzungen

Um OneTimePass zu nutzen, sind folgenden Systemvoraussetzungen beim OneTimePass-Provider notwendig:

3.2.8.1 RADIUS

- Internetzugang zur Administration und zur Prüfung der Einmalpasswörter
- RADIUS-Client, der RADIUS-Requests nach dem Standard RFC 2865 und RFC 2868 erzeugen / senden kann (z.B. Router, Webserver, RAS-Server etc. ...).

3.2.8.2 SOAP

- Internetzugang zur Administration und ggf. Prüfung der Einmalpasswörter
- SOAP-Client, welcher ein gültiges Client-Zertifikat zur Benutzung der bereitgestellten API-Funktionen präsentieren kann (Kundeneigenleistung).

3.2.8.3 Federation Services

- Internetzugang zur Administration als General Supervisor, zur Aktivierung der Federation Services und Konfiguration der notwendigen Parameter.

3.2.9 Verfügbarkeit

Die über das Internet bereitgestellte Dienstleistung OneTimePass steht dem Kunden 7*24 h die Woche zur Verfügung. Details zu den genauen Verfügbarkeiten und Service Level können dem Service Level Agreement (SLA) in der aktuellsten Form entnommen werden.

3.2.10 Wartung und Service

Diese Leistungen sind im jeweils gültigen OneTimePass Service Level Agreement (SLA) beschrieben, die dem Kunden auf Anforderung gerne zur Verfügung gestellt werden.

Über eine Newsletter-Funktionalität können die im OneTimePass-System gelisteten General-Supervisor über wichtige Änderungen oder Wartungsarbeiten per Email informiert werden.

3.3 Optionale Leistungen

Die Telekom erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt folgende zusätzliche Leistungen):

3.3.1 Serviceleistungen Hardware

3.3.1.1 Versandkosten

Versandkosten Ausland:

Alle Leistungen werden innerhalb von Deutschland erbracht. Lieferungen ins Ausland werden separat verrechnet.

Versandkosten für Endnutzer:

Alle Leistungen werden direkt an den Provider geliefert. Die Verteilung der Nutzer-Komponenten an den Endnutzer erfolgt durch den Provider. Wird eine Auslieferung direkt an den Endnutzer gewünscht, wird diese separat je Lieferadresse verrechnet.

3.3.2 Gültigkeitsdauer der Einmalpassworte (VPN-Einwahl)

Zur Nutzung der Einmalpassworte für zwei zeitlich aufeinanderfolgende Authentifikationen (z.B. bei VPN zum Aufbau der Internetverbindung gefolgt von der Authentifikation des VPN-Tunnels) hat der General Supervisor die Möglichkeit, die Gültigkeitsdauer für eine Benutzergruppe explizit einige Sekunden zu verlängern.

3.3.3 Schnittstelle zur Anbindung an das Telekom Trust Center

Standard-Anbindung an das Trust Center ist eine unverschlüsselte Internetverbindung. Darüber hinausgehend werden spezielle Anbindungen optional angeboten.

3.3.3.1 Schnittstelle zum Trust Center / MPLS

Zusätzlich zur Standard-Anbindung via Internet bietet die Telekom eine Anbindung an das Trust Center über einen zentralen MPLS-/IPLS-Anschluss. Auf Kundenwunsch kann eine direkte Anbindung eingerichtet werden. Sofern kein MPLS-Anschluss auf Kundenseite vorhanden ist, muss die Beantragung des Anschlusses in Eigenverantwortung durch den Kunden erfolgen.

3.3.3.2 Schnittstelle zum Trust Center / IPSEC-VPN

Zusätzlich zur Standard-Anbindung via Internet bietet die Telekom eine Anbindung an das Trust Center über IPSEC-VPN-Tunnel an. Auf Kundenwunsch kann eine direkte Terminierung eingerichtet werden.

3.3.3.3 Schnittstelle zum Trust Center / individuell

Auf Kundenwunsch besteht die Möglichkeit einer individuellen Anbindung zwischen OneTimePass-Provider und Telekom Trust Center. Diese Leistung wird separat projektiert und verrechnet.

3.3.3.4 Protokolle

3.3.3.4.1 RADIUS

Authentifizierungs-Anfragen werden üblicherweise über das hochperformante und etablierte RADIUS-Protokoll (RFC 2865 / 2868) gesendet.

3.3.3.4.2 SOAP

Alle administrativen Vorgänge, die über die Service Webseiten erledigt werden, können auch automatisiert über das SOAP-Protokoll übertragen werden. Hierzu stellt das Telekom Trust Center entsprechende Zertifikate zur Verfügung. Auch Authentifikationen können über SOAP übertragen werden (diese Schnittstelle eignet sich auf Grund der niedrigeren Performance nicht für massenhafte Anfragen).

3.3.3.4.3 Federation-Schnittstelle

Anbindung kann über SAML 2.0, OpenID-Connect oder REST-API erfolgen.

3.3.4 Administrations-Workshop

Die Telekom führt einen eintägigen OneTimePass- Workshop in den Räumen des Kunden durch. Er dient zur Schulung von OneTimePass General Supervisor, Supervisor und Administratoren. Innerhalb des Workshops werden die Service Portale und die vorhandenen Funktionen anhand praktischer Beispiele erklärt.

3.3.5 Kundenindividuelles Layout der Service Website

Ein kundenindividuelles Layout der Service Website wird grundsätzlich separat projektiert und mittels Festpreis verrechnet. Der technische Rahmen der Website wird von Telekom vorgegeben.

Die Telekom stellt dem Provider ein Dokument zur Verfügung, aus dem hervorgeht, welche Änderungen möglich sind.

3.3.6 Kundenindividuelle Sprache

Die OneTimePass Website wird in Deutsch, Englisch und Französisch bereitgestellt. Eine Implementierung einer weiteren Sprache ist nur in Verbindung mit einem individuellen Layout der Website möglich und wird zusätzlich mit einem Festpreis verrechnet. Die Telekom stellt dem Provider ein MS-Excel-Dokument mit den existierenden Texten der verfügbaren Sprachen als Ausgangssprache für die neue Übersetzung zur Verfügung.

3.3.7 OneTimePass-Consulting

Komplexe Dienstleistungen und individuelle Anforderungen werden je Anforderung separat projektiert und nach Aufwand verrechnet.

4 MITWIRKUNGSLEISTUNGEN DES KUNDEN

Der OneTimePass Kunde unterstützt die Anbindung seiner aktiven Komponente (Router) an das Telekom Trust Center. Zur Anbindung wird das Standard Protokoll RADIUS (**R**emote **A**uthentication **Di**al In **Us**er (RFC 2865 und RFC 2868)) verwendet. Alternativ kann auch eine Anbindung via SOAP oder Federation Services erfolgen

Der Kunde stellt sicher, dass die aktiven Komponenten das jeweilig gültige Protokoll unterstützen.

Der OneTimePass Kunde (OneTimePass Provider) stellt Mitarbeiter bereit, um die Nutzer der Dienstleistung OneTimePass einzurichten und eigenverantwortlich zu verwalten.

Folgende Verwaltungsgruppen / -hierarchien werden hierzu benötigt:

- OneTimePass General Supervisor
- OneTimePass Supervisor
- OneTimePass Administrator

5 MINDESTLAUFZEIT / BEENDIGUNG

Die Mindestüberlassungszeit für OneTimePass beträgt ab Vertragsabschluss 12 Monate und verlängert sich automatisch um 6 Monate, wenn sie nicht mit einer Frist von 1 Monat zum Ende der Mindestüberlassungszeit bzw. des jeweiligen Verlängerungszeitraums gekündigt wird.

6 MITGELTENDE DOKUMENTE

Ergänzend zu dieser Leistungsbeschreibung gelten die folgenden Dokumente:

- AGB DTSec IT Leistungen
- AGB DTSec Kauf und Miete Hardware

7 GLOSSAR / ABKÜRZUNGSVERZEICHNIS

Begriff	Beschreibung
E4 "hoch"	Evaluierungsstufen nach ITSEC - E4 = Evaluationsstufe, "hoch" = Mechanismenstärke
ITSEC	Information Technology Security Evaluation Criteria: deutsch: Kriterien für die Bewertung der Sicherheit in der Informationstechnik.
RA	Registration Authority = Registrierungsstelle zur Registrierung und Identifizierung von Anwendern für bestimmte Dienstleistungen.
RADIUS	Remote Authentication Dial In User Service - ist ein Standard für die Authentifizierung und das Accounting von Remote Access Dial-In Nutzern. RADIUS sorgt für die Kommunikation zwischen einem Dial In Server und einem Authentifizierungsserver.
RFC	Request For Comments - Die Internet Engineering Task Force (IETF) umfasst zahlreiche Arbeitsgruppen, deren Arbeitsergebnisse als RFC´s herausgegeben werden. Die RFC Dokumente haben je nach Ausprägung die Bedeutung eines Standards. Beispiele: RFC 2138 - beschreibt die Authentifizierung/Autorisierung RFC 2139 - beschreibt das Accounting
SigG	Signaturgesetz
TLS	Transport Layer Security – Protokoll zur sicheren Online-Datenübertragung im Internet zwischen Client und Server. Der Datentransfer sensitiver Daten über das World Wide Web findet verschlüsselt und abhörsicher statt. Dieses Protokoll (X.509-Standard) wird von allen gängigen Browsern unterstützt.
TCOS	TeleSec Chipcard Operating System - Chipkartenbetriebssystem welches von TeleSec entwickelt wurde und heute eines der sichersten der Welt ist.
TTC	Telekom Trust Center