LEISTUNGSBESCHREIBUNG

TeleSec OneTimePass

Deutsche Telekom Security GmbH
Version 5.3
Stand 11.11.2020

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
Aufsichtsrat: Adel Al-Saleh (Vorsitzender) | Geschäftsführung: Thomas Fetten (Sprecher), Dr. Klaus Schmitz, Thomas Tschersich
Handelsregister: Amtsgericht Bonn HRB 15241, Sitz der Gesellschaft Bonn | USt-IdNr. DE 254595345 | WEEE-Reg.-Nr. DE 56768674

Inhaltsverzeichnis

1 Einleitung

TeleSec OneTimePass bietet eine starke 2-Faktor-Authentifizierung auf Basis eines dynamischen Einmalpasswortsystems.
Der Service generiert Einmalpasswörter zur Anmeldung bei Online-Diensten und geschützten Systemen und bietet eine eigene Benutzerverwaltung.
Dem Endkunden stehen verschiedene Token zur Auswahl.
Der TeleSec OneTimePass-Dienst wird im hochsicheren und zertifizierten Trust Center der Deutschen Telekom betrieben.

2 Leistungen der Telekom Security

Die Leistungen der Telekom Security teilt sich auf in die verschiedenen Preismodelle, den Betrieb und die Ausprägungen der Dienstleistung, sowie die Funktionen und Arten der verschiedenen Authentifikationsmedien („Token“).

2.1 Bereitstellung - Tarifmodelle

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

2.1.1 OneTimePass-Teststellung

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. Die Laufzeit einer Teststellung beträgt max. 8 Wochen (oder nach Vereinbarung). Erfolgt nach der Teststellung eine Beauftragung einer Dienstleistung, wird der Bereitstellungspreis mit dem entsprechenden Bereitstellungspreis des Tarifes verrechnet.

2.1.2 OneTimePass-Compact

Eine vom Leistungsumfang eingeschränkte Dienstleistung. Es steht nur eine OneTimePass-Group (siehe Punkt 0) zur Verfügung und es kann nur eine begrenzte Anzahl von Nutzern eingerichtet werden. Die Administrationsrechte und Serviceleistungen über die Service-Web-Seiten sind ebenfalls eingeschränkt. Es steht lediglich die Administrator Funktionalität zur Verfügung. Das Tarifmodell wird monatlich pauschal verrechnet, ist unabhängig von der Anzahl der Nutzer und 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 bis zu 100 Nutzer. Im Tarifmodell Compact werden folgende Staffeln bzw. Pakete unterschieden:

<u>Compact 10, 25, 50 oder 75:</u>
Mit OneTimePass Compact 10/25/50/75 wird für den Kunden eine OneTimePass Group mit maximal 10/25/50/75 Nutzern eingerichtet.

<u>Upgrade</u>
Die Telekom Security führt ein Upgrade von einer niedrigeren OneTimePass-Stufe (Compact 25 bzw. Compact 50) in eine höhere OneTimePass-Stufe (Compact 50 bzw. Compact 75) durch.

<u>Erhöhung der Nutzerzahl bei OneTimePass (Compact 75)</u>
Bei OneTimePass (Compact 75) erhöht die Telekom Security die Anzahl der Nutzer in weiteren Schritten um jeweils 50 bzw. 100 weitere Nutzer.

2.1.3 OneTimePass-Advanced

Dieses Tarifmodell ist vom Leistungsumfang nicht eingeschränkt. Es wird eine monatliche Pauschale für die Überlassung der Dienstleistung verrechnet. Die OneTimePass-Nutzer werden

ebenfalls monatlich pauschal verrechnet 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 Advanced werden folgende Staffeln bzw. Pakete unterschieden:

Überlassung Advanced 100, ...
Mit OneTimePass (Advanced 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.

Überlassung Advanced-Extension 50, ...
Mit OneTimePass (Advanced-Extension 50, 100, 500 und 1.000) können auch kleinere Stufensprünge erreicht werden. Somit kann z.B. OneTimePass-Advanced 1.000 (= 1.000 Nutzer) um eine OneTimePass-Advanced-Extension 500 (= 500 Nutzer) auf insgesamt 1.500 Nutzer erweitert werden. Die Advanced-Extension Pakete bleiben bis zur Kündigung im Bestand und rechnen sich nicht mit einem Up- bzw. Downgrade von OneTimePass-Advanced auf. Wird also im o.g. Beispiel OneTimePass-Advanced 1.000 auf OneTimePass-Advanced 2.500 erhöht, bleibt die Extension 500, sofern diese nicht gekündigt wurde, bestehen. Es stehen somit 3.000 Nutzer zur Verfügung.

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

2.1.4 OneTimePass-Reseller

Dieses Tarifmodell ist vom Leistungsumfang nicht eingeschränkt und steht nur definierten Partnern des Konzerns Deutsche Telekom zur Verfügung.

2.2 Betrieb – OneTimePass Dienstleistung

Die zentrale Identifikationsdienstleistung wird von der Deutschen Telekom Security GmbH in ihrem Trust Center betrieben und dem Provider für die vereinbarte Vertragszeit überlassen.

Mit Hilfe der OneTimePass-Authentifikationsmedien kann einem Nutzer der Zugang zu einem Server im Internet oder ein lokaler Netzzugang (z.B. zu seinem Internet-Service-Provider) mittels Einmalpasswort ermöglicht werden. Die Authentifikationsmedien können weiterhin zur Transaktionsauthentifikation (PIN/TAN-Ersatz) und als Authentifikation von Kunden einer Service-Hotline genutzt werden.

Der Nutzer gibt in das Abfragefeld des DFÜ-Netzwerks/Internetbrowsers die auf der Chipkarte aufgedruckte Identifikationsnummer bzw. den Alias-Namen und das vom Authentifikationsmedium errechnete und angezeigte Einmalpasswort ein. Das Passwort ist nur einmal gültig.

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 (Quelle: Internet)) an den OneTimePass-Server im Trust Center der Telekom Security. Dieser prüft die Gültigkeit des Einmalpasswortes und sendet die für das entsprechende Nutzer- bzw. Gruppenprofil eingestellten Attribute zurück.

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

2.2.1 OneTimePass-Server

Die Deutsche Telekom Security GmbH betreibt in ihrem Trust Center einen zentralen OneTimePass-Server, der die eingereichten Einmalpasswörter des OneTimePass-Providers auf Gültigkeit prüft. Der OneTimePass-Server ist über einen RADIUS-Server (RFC 2865 und RFC 2868) an das Internet angebunden. Im zentralen Server werden alle Provider verwaltet. Jeder Provider kann seinerseits individuelle Gruppen und Profile verwalten. Durch diese zentrale Verwaltung können die OneTimePass-Token (s. Punkt 1.1) für unterschiedliche Anwendungen bei unterschiedlichen Providern, sofern sie vom jeweiligen Provider freigeschaltet wurden, eingesetzt werden.

2.2.2 OneTimePass-Group

Der OneTimePass-Provider erhält die Möglichkeit, Nutzer in sogenannte Usergroups einzuteilen, um diese nach Anwendungen und Kundengruppen / Abteilungen (Buchhaltung, Streetworker, ...) 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 Security eingeschränkt werden.

2.2.3 OneTimePass Administration auf Kundenseite

Zur Administration der OneTimePass Dienstleistung erhält jeder Provider maximal 10 General Supervisor-Berechtigungen. Jeder General Supervisor erhält ein OneTimePass-Authentifikationsmedium 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 Kapitel 1.2.7 ff beschrieben..

2.2.4 OneTimePass Nutzer

Der OneTimePass-Nutzer wird durch den OneTimePass-Provider identifiziert und erhält ein ihm zugeordnetes OneTimePass-Authentifikationsmedium. Die Administration der Nutzer erfolgt über die Internet-Service-Seiten des Trust Centers. Die Berechtigungen bzw. Leistungen sind im Kapitel 1.2.9.1 beschrieben. Je nach Preismodell bzw. Angebotspaket wird die Anzahl der OneTimePass-Nutzer durch die Telekom Security eingeschränkt.

2.2.5 RADIUS – Nutzer Profil

Die Telekom Security 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 Trust Centers der Telekom Security.

2.2.6 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.

2.2.7 RADIUS – IP Pool (dynamische IP-Adresszuweisung)

Mit Hilfe von IP-Pools können IP-Adress-Bereiche definiert werden, die dem Gruppen- bzw. Benutzer-Attribut „Framed-IP-Address“ zugewiesen werden können. Aus diesem Pool wird dem Benutzer bei einer RADIUS-Anfrage eine freie IP-Adresse zugewiesen. Durch RADIUS-Accounting-Funktionalitäten ist der OneTimePass-RADIUS-Server in der Lage, diese dynamischen IP-Adress-Pools eigenständig zu verwalten. IP-Pools werden durch eine Netzmaske, eine Start- und eine End-Adresse bestimmt und werden über einen in der Gruppe eindeutigen Namen identifiziert. Die Verwaltung erreicht man über die Internet Service Seite für Administratoren.

Für deren Definition gelten folgende Regeln:

- Pro Gruppe können maximal 5 IP-Pools angelegt werden.
- Da der Name des Pools als Wert eines Attributs verwendet wird, gelten für Sonderzeichen die gleichen Einschränkungen wie für Attributwerte.
- Die Angabe der Netzwerkmaske erfolgt in der CIDR-Notation (z.Bsp. 111.222.1.0/24)
- Ein Pool darf maximal ein Adress-Intervall von 4096 Werten umfassen. D.h. der Wert für das Netzwerk-Suffix darf nicht kleiner als 20 sein.

2.2.8 Prüfung der Einmalpasswörter

Bei TeleSec OneTimePass handelt es sich um eine sogenannte Zwei-Faktor-Authentifikation, die auf den beiden Faktoren „Besitz“ und „Wissen“ basiert. Bei Nutzung von Chipkarten besteht die Komponente Besitz aus der Chipkarte und die Komponente Wissen aus der zugehörigen Karten-PIN. Bei allen anderen Authentifikationsmedien, die keine PIN zur Legitimation nutzen, wird eine 4-stellige Server-PIN genutzt, die bei der Authentifikation an das 8-stellige Einmalpasswort angehängt wird.

Bei einem Authentifikationsrequest eines Nutzers wird somit der verwendete Aliasname des Users und sein Einmalpasswort und ggf. die Server-PIN (8-stellig / 12-stellig) übertragen.

Die Anfrage des OneTimePass-Nutzers wird zunächst auf einen Standard-RADIUS-Server des Providers geroutet. Das RADIUS-Protokoll ermöglicht die Nutzer-Identifikation mittels gespeicherter Daten auf einer lokalen oder externen Datenbank. Um die OneTimePass-Dienstleistung nutzen zu können, erhält der RADIUS-Server ein spezielles Profil. Dieses unterdrückt die Authentifikationsanfrage zur internen Datenbank und veranlasst automatisch einen Verbindungsaufbau zum Telekom Security Trust Center. Anstelle eines RADIUS-Servers sind auch andere RADIUS-Protokoll-unterstützende Komponenten denkbar.

Um die OneTimePass Standard Dienstleistung nutzen zu können, benötigt der Provider in der Regel nur die vorhandene Infrastruktur wie z.B. einen Router, das RADIUS-Protokoll, eine Nutzerdatenbank mit dem Benutzerprofil und einen Zugang zum Trust Center via Internet.

Der OneTimePass-Provider reicht zur Passwortprüfung lediglich die Kartennummer oder der jeweilige Alias und das aktuelle Einmalpasswort über das RADIUS-Protokoll an das Telekom

Security Trust-Center weiter. Bereits mit der Chipkartenproduktion wird das Leistungsmerkmal OneTimePass, bestehend aus einem individuellen DES-3-Schlüssel und einem Initialisierungsvektor (Startwert für das erste gültige Passwort) zur Erzeugung von Einmalpasswörtern, auf der Karte gespeichert. Dem zentralen OneTimePass-Server im Telekom-Trust-Center ist dieser Startwert und der mathematische Algorithmus für die weitere Passworterzeugung ebenfalls bekannt. Mit Hilfe dieser Vorgabe erzeugt das Trust Center automatisch weitere 15 (fünfzehn) Passwörter im Voraus. Generiert der Nutzer nun mehrere Passwörter die er nicht zur Prüfung an das Trust Center einreicht, so kann eine Synchronisation nur innerhalb dieser Grenzen garantiert werden. Jedes Passwort ist nur einmal gültig.

Sobald ein Einmalpasswort genutzt wird, werden alle vorher erzeugten Einmalpasswörter ungültig.

Weiterhin ist dem zentralen Server bekannt, ob die Chipkarte gültig oder gesperrt ist. Bei der Anfrage zur Passwortprüfung durch den OneTimePass-Provider wird in der Datenbank Datum, Uhrzeit und Kartennummer oder Alias gespeichert. Nach Prüfung des Einmalpasswortes im Telekom Security Trust-Center erhält der Nutzer eine Bestätigung (Gutaussage) oder eine Abweisung.

Dem Telekom Security Trust-Center sind keine Personen- oder Nutzerdaten bekannt.

Mit der Bestätigung (Gutaussage) des Telekom Security Trust-Centers werden dem OneTimePass-Nutzer die Benutzerrechte der Anwendung durch den OneTimePass-Provider mittels RADIUS-Protokoll zugeordnet. Der OneTimePass-Nutzer wird vom OneTimePass-Provider für die Anwendung freigeschaltet.

Die OneTimePass-Dienstleistung umfasst lediglich die Identifikation des Nutzers. Eine verschlüsselte Verbindung wird nicht realisiert.

Eine verschlüsselte Verbindung zwischen einem Web Server und einem OneTimePass-Nutzer kann z.B. mittels SSL- oder IPSEC-Verbindungen realisiert werden. Eine gesicherte SSL-Verbindung stellt das TeleSec-Produkt ServerPass her.

2.2.9 OneTimePass Administration

2.2.9.1 Internet Service Portal – Provider

Die Deutsche Telekom Security GmbH betreibt einen Internet-Server, auf dem der OneTimePass-Provider alle administrativen Tätigkeiten selbst ausführen kann. Mittels eines SSL-Server-Zertifikates (TeleSec ServerPass) erfolgt jeder Zugriff ausschließlich in verschlüsselter Form. Die Authentifikation erfolgt mittels UserID / Einmalpasswort. Das notwendige Einmalpasswort wird mittels der OneTimePass-Authentifikationsmedien erzeugt. Als Standard Authentifikationsmedium wird der Card Reader OTP-Reader III (siehe Kapitel 0) in Verbindung mit Chipkarte (siehe Kapitel 1.1.2) vorausgesetzt. Abhängig von der Security-Policy ihres Unternehmens kann der Administrator- / Supervisor-Login auch mittels OneTimePass-Token ermöglicht werden. Die Anmeldung mit diesen Authentifikationsmedien muss aber zunächst durch den General Supervisor freigegeben werden.

OneTimePass bietet für Service und Administration folgende Benutzerberechtigungen an:

<u>OneTimePass-General-Supervisor (max. 10):</u>

- FAQ, Kontakt, aktuelle Meldungen, Download.
- Einrichten und Pflegen (ändern, sperren, löschen) der Supervisor.
- Einrichten und Pflegen von OneTimePass-Groups.
- Definition von Nutzerbegrenzungen pro OneTimePass-Group
- Sperrservice der General-Supervisor und Supervisor.
- Einrichten und Pflegen von RADIUS-Client-Groups.

- Beauftragen von neuen RADIUS-Clients.
- Zugriff auf monatliche OTP-Provider-Statistiken (Reporting- und Statistikdaten)

OneTimePass-Supervisor (Anzahl unbegrenzt):
- FAQ, Kontakt, aktuelle Meldungen, Download.
- Einrichten und Pflegen (ändern, sperren, löschen) der Administratoren zu den berechtigten OneTimePass-Groups.
- Sperrservice für Administratoren.
- Zuordnung von Standard-RADIUS-Attributen für alle Administratoren.
- Zuordnung von speziellen RADIUS-Attributen für einzelne Administratoren.

Der Supervisor hat die o.g. Berechtigungen für die ihm zugeordneten OneTimePass-Provider und deren OneTimePass-Groups. Ein Supervisor kann z.B. für mehrere OneTimePass-Provider und alle daraus resultierenden OneTimePass-Groups zuständig sein.

OneTimePass-Administrator (Anzahl unbegrenzt):
- FAQ, Kontakt, aktuelle Meldungen, Download.
- Service - Statusinformationen zu Token oder Chipkarten.
- Einrichten und Pflegen (ändern, sperren, löschen, synchronisieren) der Nutzer zu den berechtigten OneTimePass-Groups.
- Pflegen von RADIUS-Gruppenattributen, entsprechend der Vorgabe des Supervisors.
- Pflegen von speziellen RADIUS-Nutzerattributen, entsprechend der Vorgabe des Supervisors.

Der Administrator hat die o.g. Berechtigungen für die ihm zugeordneten OneTimePass-Provider und deren OneTimePass-Groups. Ein Administrator kann z.B. für mehrere OneTimePass-Provider und alle daraus resultierenden OneTimePass-Groups zuständig sein.

2.2.9.2 SOAP-Administration

Alternativ zur Nutzung der Service-Webseiten kann die komplette OneTimePass-Administration auch SOAP-basiert erfolgen. Alle administrativen Tätigkeiten wurden in Form spezifizierter SOAP-Aufrufe nachgebildet. Somit kann ein bereits existierendes Administrationsportal leicht an OneTimePass angebunden werden. Die Authentifikation erfolgt hier durch ein Zertifikat der Shared Business CA. Das optional erhältliche Dokument „OneTimePass SOAP-Spezifikation Vn.pdf“ beinhaltet den kompletten Befehlssatz inkl. WSDL-Beschreibung.

2.2.9.3 Bulk-Verwaltung

Für das effiziente gleichzeitige Verwalten / Administrieren von vielen Benutzern werden mit der Bulk-Verwaltung die Funktionen für Massen-Administration, Snapshots und User-Exports angeboten.

Massenadministration:
Die Massenadministration ermöglicht das massenhafte Anlegen, Ändern oder Löschen von bis zu 5000 Datensätzen. Ähnlich wie beim manuellen Anlegen von Benutzern wird zunächst eine Übersicht der für die gesamte Gruppe vergebenen Attribute angezeigt. Diese werden jedem Benutzer, der neu angelegt werden soll, automatisch zugeordnet, können aber mit weiteren Definitionen individuell ergänzt werden.
Für die Übergabe der Datensätze stehen zwei Möglichkeiten zur Verfügung. Zum Einen können sie in Form eines Dateiuploads auf den Server übertragen und zum Anderen direkt in das

vorhandene Textfeld eingetragen, bzw. aus der Zwischenablage hineinkopiert werden. Die benutzte Methode wird über das jeweilige Auswahlfeld bestimmt.

Außer dem Anlegen von Benutzern können auch bereits bestehende Benutzer über die Import-Funktion geändert werden. Die Änderungen wirken sich je nach Token-Typ ggf. auf die Server-PIN, das Servicepasswort und die Benutzerattribute aus. Diese Funktion wird über die Auswahlbox unter dem Eingabefeld gesteuert. Ist diese bei der Übergabe der Daten aktiviert, werden alle bereits vorhandenen Benutzer ohne weitere Nachfrage geändert. Sind Attribute für einen zu ändernden Benutzer angegeben, werden alle zuvor gesetzten Attribute gelöscht und nur die im Datensatz angegebenen Werte angelegt.

Die Datensätze werden im CSV-Format übergeben, wobei als Trennsymbol das Semikolon Verwendung findet.

Snapshots:
Die Funktion von Snapshots dient der Sicherung von Benutzerdaten, bevor Massen-Administrationen durchgeführt werden. Gesichert werden alle an den Benutzer geknüpften Informationen, wie die Tokennummer, den Alias oder den Lock-Status. Weiterhin werden alle für den Benutzer vergebenen Attribute gesichert.

Das Leistungsmerkmal „Snapshots“ kann bei Bedarf pro Kunde von den Trust Center Administratoren aktiviert werden.

User-Export:
Weiterhin im Bereich „Bulk-Verwaltung“ befindet sich die Funktion zum Export von Benutzerdaten. Über sie ist es möglich, alle Benutzerdaten der ausgewählten Gruppe im gleichen Format in eine Datei zu exportieren, wie sie von der Massen-Administration als Eingabedaten benötigt werden. Die erstellte Export-Datei wird Ihnen als Download in einem zweiten Browser-Fenster angeboten.

2.2.9.4 Internet Service Portal – Nutzer

Telekom Security betreibt für die OneTimePass-Nutzer einen Internet-Server auf dem alle nutzerbezogenen Tätigkeiten ausgeführt werden können. Alle Anfragen auf dem Server werden mit einem SSL-Server-Zertifikat verschlüsselt übertragen. Folgende Leistungen bietet die Telekom Security an:

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

2.2.10 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 auch nach unterschiedlichen Sperren.

Folgende Sperrgründe können vorliegen:

- defekte Chipkarte / defekter Token
- Fehlbedienungszähler ist nach mehrmaliger Falscheingabe der PIN abgelaufen, die Karte ist unbrauchbar
- OneTimePass-Nutzer hat die Chipkarte / den Token verloren
- Chipkarte / Token wurde gestohlen
- OneTimePass wird vom OneTimePass-Nutzer nicht mehr genutzt
- OneTimePass-Nutzer wird für bestimmte Nutzer Groups durch den Provider gesperrt.

Folgende Sperren können erfolgen:

- Globale Sperre (in allen Gruppen / bei allen Providern)
  - Temporär
  - Endgültig
- Lokale Sperre (nur innerhalb einer Gruppe)
  - Temporär
  - Endgültig

2.2.10.1 OneTimePass-Provider

Der OneTimePass-Provider ist berechtigt, alle OneTimePass-Nutzer in seinen OneTimePass-Groups zu sperren. Somit schließt der Provider aus, dass unberechtigte Nutzer auf seine Daten zugreifen können.

Ein Provider ist nicht berechtigt, einen Nutzer global zu sperren, da der OneTimePass-Nutzer das Authentifikationsmedium bei weiteren Providern zur Identifikation nutzen kann.

Eine globale Sperre der Chipkarte kann nur durch den OneTimePass-Nutzer selbst veranlasst werden. Die Sperrung wird unmittelbar nach dem Aktivieren im Web wirksam.

2.2.10.2 OneTimePass-Nutzer

Der OneTimePass-Nutzer darf alle Sperrungen der Karte / des Token veranlassen, die eine globale Auswirkung auf alle OneTimePass-Provider haben. Dies ermöglicht dem OneTimePass-Nutzer eine sehr kurze Reaktionszeit beim Verlust der Chipkarte / des Token. Es ist somit nicht notwendig, dass der OneTimePass-Nutzer eine Sperrung bei jedem Provider veranlassen muss.

Dem OneTimePass-Nutzer steht zur globalen Kartensperre die OneTimePass-Service Website zur Verfügung. Um eine Sperrung zu veranlassen, muss der OneTimePass-Nutzer sich mit seiner Chipkartennummer und einem gültigen Servicepasswort identifizieren.

Die Sperrung wird unmittelbar nach der Erteilung wirksam. Folgende Sperrvarianten stehen derzeit zur Verfügung:

- Globale Sperre ohne Widerruf, d. h. diese Sperre ist endgültig.
- Globale Sperre mit Widerruf

Um die Sperren zu aktivieren ist ein Servicepasswort notwendig, welches der OneTimePass-Nutzer wie folgt erhält:

- Alternative 1

  Die ersten fünf Einmalpasswörter, die nach dem Freischalten der Chipkarte generiert wurden, werden vom Trust Center der Deutschen Telekom als gültige Sperrpasswörter akzeptiert.

- Alternative 2

  Der OneTimePass-Nutzer ist berechtigt, sich über die OneTimePass-Service Website ein Servicepasswort zu vergeben. Das Servicepasswort kann nur mit einem gültigen Einmalpasswort aktiviert werden.

Sollte ein OneTimePass-Nutzer keinen Zugang zum Internet haben, kann dieser einen Provider seiner Wahl beauftragen, die Sperrung durchzuführen.

2.2.11 Systemvoraussetzungen

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

- 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. ...).

2.2.12 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.

2.2.13 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 werden die im OneTimePass-System gelisteten General-Supervisor über wichtige Änderungen, oder Wartungsarbeiten, per E-Mail informiert.

2.3 Funktionen - Authentifikationsmedien

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

2.3.1 CardReader OTP-Reader III

Der Offline-CardReader OTP-Reader III mit Display und Tastatur hat folgenden Funktionsumfang:

- Einmalpasswortgenerator mittels Display und Tastatur
- Unterstützung von OneTimePass
- Unterstützung der neuesten Kartengeneration TeleSec NetKey 3.0 (aus Basis von TCOS 3.0)

Technische Daten:

- Grafisches LCD-Display
- Nummern- und Funktionstasten
- auswechselbare Batterien (2x CR-2025)
- Protokolle T = 1 und T = 0 (ISO 7816-3).

2.3.2 Chipkarte NetKey 3.0

Die TeleSec 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.

Grundfunktionen:

- Intelligente Prozessorchipkarte
- Auslieferungsschutz (Null-PIN Verfahren)
- OneTimePass Applikation
- Globale Karten-PIN (Zugriffsschutz)
- Globale Karten-PUK / PIN2
- Fehlbedienungszähler
- Evaluiertes Smartcard Betriebssystem TCOS (TeleSec Chipcard Operating System)

Weitere nutzbare Leistungen:

- Digitale Signatur
- Ver- und Entschlüsselung von beliebigen Dateien.
- Vier Zertifikate nach der ITU-T-Empfehlung x.509v3 (s.u.)
- weitere persönliche Zertifikate sind nachladbar.
- Standard-Applikationen (ausgenommen OneTimePass):
  - NetKey V 3.0 (drei Zertifikate)
  - SigG mit Schlüsseln von E4-evaluiertem Schlüsselgenerator (ein Zertifikat)
  - Zutrittskontrolle
  - Zeiterfassung
  - Watermark

Für die Nutzung der weiteren Leistungsmerkmale ist zusätzliche Soft- und Hardware erforderlich, die nicht Bestandteil dieses Vertrages ist.

Technische Daten:

- Evaluiertes Sicherheits-Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System) nach ITSEC E4 hoch (Information Technologie Security Evaluation Criteria Evaluationsstufe "E4", Mechanismenstärke "hoch") auf der Chipkarte
- Kommandoaufbau und -inhalt nach ISO/IEC 7816-4, 7816-8
- Proprietäre Kommandos nur bei nicht genormten Funktionen
- Asymmetrisches kryptografisches Verfahren RSA (Rivest Shamir Adleman) mit einer Schlüssellänge von 2.048 bit
- Symmetrische kryptografische Verfahren DES (Data Encryption Standard, 56 bit), DES3 (112 bit, 168 bit), IDEA (International Data Encryption Algorithm, 128 bit) mit ECB-Mode (Electronic Code Book) oder CBC-Mode (Cipher Block Chaining)
- Secure Messaging zur Übertragungssicherung
- Implementierung von Applikationen im Feld möglich
- Je nach Kartentyp freier Speicher für anwenderspezifische Applikationen
- Abwehrmechanismen gegen alle derzeit bekannten Angriffsszenarien.

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.

2.3.3 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 Deutschen Telekom Security GmbH 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 müssen weiterhin Chipkarten-basierte Lösungen verwendet werden.

2.3.4 OneTimePass SMS

Mit „OneTimePass SMS“ erhält der OneTimePass-Nutzer seine Einmalpasswörter vom OneTimePass-Server direkt per SMS. Der OneTimePass-Nutzer nutzt dabei sein aktuelles Mobiltelefon und seinen vorhandenen Mobilfunkvertrag bei einem beliebigen Mobilfunk-Provider. OneTimePass SMS ist nahezu weltweit nutzbar (unterstützte Länder und ggf. Einschränkungen können im Vorfeld angefragt werden).

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 Telekom Security nicht garantieren, wie lange es von der Anfrage bis zur Zustellung des Einmalpasswortes per SMS dauert.

Die Anforderung eines neuen Einmalpasswort beim OneTimePass-Server kann über die nachfolgend beschriebenen Wege erfolgen:

Anforderung per SMS:

Als eingetragener „OneTimePass SMS“-Nutzer können Sie von Ihrem Handy ein neues Einmalpasswort via SMS vom OneTimePass-SMS-Gateway anfordern, welches Ihnen anschließend per SMS zugestellt wird. Hierdurch entstehen Kosten für den Versand der Anforderungs-SMS.

Anforderung via Webseite:

Als zweite Alternative kann der registrierte „OneTimePass-SMS“-Nutzer, über einen Aufruf, der in die jeweilige Website integriert werden kann, ein Einmalpasswort für einen angegebenen OneTimePass-Alias anfordern. Das Einmalpasswort wird anschließend an das registrierte Mobiltelefon per SMS übertragen.

Proaktiver Versand:

Bei dieser Variante wird das erste Einmalpasswort direkt bei der Administration des neuen Nutzers versendet. Nach jeder erfolgreichen Authentifikation wird automatisch das nächste Einmalpasswort an den Nutzer versendet. Die Option „Proaktiver Versand“ wird in den Gruppeneigenschaften durch den General Supervisor aktiviert.

Der Text der OTP-SMS kann durch den General Supervisor Gruppen-weit angepasst werden, um so z.B. sprachliche Anforderungen verschiedener Ländergruppen zu bedienen.

2.3.5 OneTimePass Software-Token

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

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

Der TeleSec 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.

Bei Nutzung von E4 NetKey- / NetKey 3.0-Karten kann komfortabel der PIN Unblocking Key (PUK) nach Eingabe der Karten-PIN ausgelesen werden. Diese PUK kann wahlweise gespeichert, als PUK-Brief (auf Normalpapier oder speziellen PUK-Brief-Vorlagen) ausgedruckt oder per Email an den Nutzer versendet werden.

Der TeleSec 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 (Win XP, Win Vista, Win 7 32/64bit) benötigt – die Installation nutzt etwa 10 MB Festplattenplatz.

Voraussetzung zum Betrieb ist ein beliebiges Chipkartenterminal (Voraussetzung: Online-Leser, also mit Anbindung an einen PC) mit Seriell-, USB- oder PCMCIA-Anbindung, inkl. installiertem ctapi- oder PC/SC-Treiber.

2.3.5.2 OneTimePass SmartToken (SMT)

Zur Generierung von Einmalpassworten (ohne Onlineverbindung) bietet Telekom Security den OneTimePass SmartToken als reine Softwarelösung an.

Die Applikation wird kostenfrei über die AppStores der Betriebssystemhersteller distributiert.

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 parameterisiert / initialisiert. Hierzu wird eine Onlineverbindung über Mobilfunk oder WLAN benötigt. Zur Nutzung des SmartTokens ist nach erfolgreicher Initialisierung keine Onlineverbindung erforderlich.

Zur Verwendung des SmartToken definiert der Nutzer eine PIN und eine PUK. Nach dreimaliger Falscheingabe der PIN kann die Applikation nur durch die PUK freigeschaltet werden. Wird diese wiederum zehnmal falsch eingegeben, so wird die App gesperrt und die Geheimnisse werden gelöscht, um einem Mißbrauch vorzubeugen. Die App kann anschließend nur nach erfolgreicher Reaktivierung weiter genutzt werden.

2.3.5.2.1 SmartToken für Apple iOS

Der OneTimePass SmartToken für iOS kann in Verbindung mit einem Apple iPhone, iPad und iPod Touch ab iOS-Version 3.2 (SmartToken 1.21) bzw. iOS-Version 6 (SmartToken 1.30) genutzt werden.

Die App wird kostenfrei über den Apple AppStore distributiert:

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

2.3.5.2.2 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. Nicht lauffähig auf Geräten mit Tizen Betriebssystem (Samsung Gear S2 / Gear S3 / Galaxy Watch)!

Die App wird kostenfrei über den Google Playstore distributiert:

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

2.3.6 Statische OneTimePass-Nutzer

Sofern lediglich die reinen RADIUS-Funktionalitäten (statische/dynamische IP-Adress-Vergabe, etc.) genutzt werden sollen, besteht die Möglichkeit statische OneTimePass-Nutzer anzulegen. Ein statischer Benutzer verwendet kein dynamisches Einmalpasswort, sondern lediglich ein statisches Passwort. Des Weiteren kann der statische OneTimePass-Nutzer 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 wieder arbeitsfähig zu machen. Die Freigabe, statische Nutzer anlegen zu können, erfolgt nur nach formloser schriftlicher Beauftragung durch den OTP-Provider.

2.3.7 Systemvoraussetzungen

2.3.7.1 Standard Authentifikationsmedien

Zum Betrieb der OneTimePass-Authentifikationsmedien durch den OneTimePass-Nutzer sind keine besonderen Systemvoraussetzungen erforderlich, da keinerlei Hardware für die Nutzung von OneTimePass mit dem PC verbunden werden muss. Es ist auch keine zusätzliche Client-Software erforderlich. Als Standardsoftware auf der Nutzerseite kann z. B. das Microsoft DFÜ-Netzwerk (bei Absicherung eines Netzzugangs) genutzt werden.

2.3.7.2 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. Wenn die Lösung in neue Länder außerhalb Europa ausgerollt werden soll, so muß die Nutzbarkeit zunächst von Telekom Security geprüft werden.

2.3.7.3 OneTimePass SmartToken

Die Voraussetzungen für den Einsatz der SmartToken entnehmen Sie bitte den Kapiteln 1.1.5.2.1 bis 1.1.5.2.2.

2.3.8 Lieferbedingungen

Die OneTimePass-Authentifikationsmedien werden grundsätzlich nur an die OneTimePass-Provider ausgeliefert.

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

Die TeleSec Chipkarte NetKey 3.0 ist in der Dual-Use-Liste aufgeführt und unterliegt somit den besonderen Export- und Importbestimmungen, welche dem OneTimePass-Nutzer transparent gemacht werden müssen.

2.4 Einseitige Leistungsänderungen

Die DT Security 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 Telekom den Kunden über etwaige Anpassungen durch Übersendung aktualisierter Versionen der bestehenden Vertragsunterlagen informieren, welche die bestehenden Unterlagen ersetzen.

2.5 Optionale Leistungen

Die Telekom Security erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt insbesondere folgende zusätzliche Leistungen (Nicht für das Tarifmodell OneTimePass Compact):

2.5.1 Serviceleistungen Hardware

2.5.1.1 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.

2.5.2 Gültigkeitsdauer der Einmalpassworte (VPN-Einwahl)

Bestimmte Anwendungen benötigen bei Zugriff mehrere Kanäle bzw. mehrere Anmeldungen (z.B. VPN). In einem solchen Fall würde OneTimePass mehrere Authentifikationen anstoßen, die mehrere Eingaben von Einmalpasswörtern zur Folge hätte. Mit dem Feature der „Kanalbündelung“ bietet die Dienstleistung OneTimePass die Möglichkeit einer Zwischenspeicherung des Einmalpasswortes für einige Sekunden während des Verbindungsaufbaus. Damit kann mit einer Authentifikation der Anwendung die geforderte Bandbreite nutzbar gemacht werden.

Eine weitere Verwendungsmöglichkeit dieser Option ist zum Beispiel zur Nutzung eines einzigen Einmalpasswortes zur Herstellung einer Internetverbindung und Authentifikation eines VPN-Tunnels.

Die Gültigkeitsdauer kann nur vom General Supervisor und nur Gruppen-weit aktiviert werden.

2.5.3 Bereitstellung einer Schnittstelle zur Anbindung an das Trust Center

2.5.3.1 Schnittstelle zum Trust Center / MPLS

Zusätzlich zur Standard-Anbindung via Internet bietet die Telekom Security 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, erfolgt die Beantragung des Anschlusses in Eigenverantwortung seitens des OneTimePass-Provider.

2.5.3.2 Schnittstelle zum Trust Center / IPSEC-VPN

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

2.5.3.3 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.

2.5.4 Administrations-Workshop

Die Telekom Security führt einen eintägigen OneTimePass- Workshop (entspricht 5 Zeitstunden) in ihren Räumen durch. Er dient zur Schulung von OneTimePass General Supervisor, Supervisor und Administratoren. Innerhalb des Workshops werden alle Funktionen der Service Portale und die vorhandenen Funktionen erklärt.

2.5.5 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 vorgegeben.

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

2.5.6 Kundenindividuelle Sprache

Die OneTimePass Website wird in Deutsch, Englisch Französisch und Holländisch 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 Deutsche Telekom Security GmbH stellt dem Provider ein MS-Excel-Dokument, mit den existierenden Texten, als Ausgangssprache für die neue Übersetzung zur Verfügung.

2.5.7 OneTimePass-Consulting

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

3 Mitwirkungsleistungen des Kunden

Der OneTimePass Kunde unterstützt die Anbindung seiner aktiven Komponente (Router) an das TrustCenter der T-Systems. Zur Anbindung wird das Standard Protokoll RADIUS (**R**emote **A**uthentication **Di**al In **Us**er (RFC 2865 und RFC 2868)) verwendet. Der Kunde stellt sicher, dass die aktiven Komponenten das RADIUS 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 Compact

OneTimePass Administrator

OneTimePass Advanced

OneTimePass General Supervisor
OneTimePass Supervisor
OneTimePass Administrator

4 Mindestüberlassungszeit/Beendigung

Die Mindestvertragslaufzeit von TeleSec OneTimePass beträgt 12 Monate, kündbar spätestens 3 Monate vor Ende der Laufzeit in schriftlicher Form.
Erfolgt keine fristgerechte Kündigung, so verlängert sich die Vertragslaufzeit um weitere 6 Monate.

Mitgeltende Unterlagen

Allgemeine Geschäftsbedingungen (AGB)

Es gelten im Übrigen die zum Zeitpunkt des Vertragsschlusses Beauftragung gültigen Allgemeinen Geschäftsbedingungen TeleSec-Produkte.

Service-Level-Agreement (SLA)

Aussagen über die Verfügbarkeit, die Wartung und den Service finden im jeweils aktuellen Service-Level-Agreement (SLA).

Abkürzungsverzeichnis/Glossar

Abkürzung	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 RFC 2139 - beschreibt das Accounting
SSL	Secure Socket Layer – 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) wurde von Netscape entwickelt und wird von allen gängigen Browsern unterstützt.
TCOS	TeleSec Chipcard Operating System - Chipkartenbetriebssystem welches von TeleSec entwickelt wurde und heute das sicherste der Welt ist.
TTC	Telekom Trust Center