Leistungsbeschreibung Teleworker Secure Access

Professioneller und hochsicherer Unternehmenszugang

Stand Juni 2009

1. Standard-Leistungsumfang

1.1 Einführung

Teleworker Secure Access bietet Kunden die Möglichkeit ihre Mitarbeiter ortsunabhängig und sicher in ihr Firmen-Intranet einzubinden. Die Teleworker Zugänge werden mittels IPSec (Internet Protocol Security) im Tunnelmodus realisiert und über einen beliebigen Internetzugang aufgebaut. Über Teleworker Secure Access können externe Mitarbeiter unterschiedliche Applikationen ansprechen wie beispielsweise Intranet Portale, Exchange Server, Lotus Domino Server, SAP-Systeme oder auch Fileshare-Server und virtualisierte Desktops. Teleworker Secure Access nutzt zur Verschlüsselung und sicheren 2-Faktoren-Authentisierung eine zentrale Public-Key-Infrastruktur. Jeder Anwender des Kunden erhält einen USB-Token zur sicheren Anmeldung und zum Schutz des Firmennetzes vor unerlaubten Zugriffen. Das Service kann über einen Webbrowser durch den Kunden selbst administriert werden.

1.2 Technische Realisierung

1.2.1 Anforderungen für den Netzzugang

Voraussetzung für den Betrieb von Teleworker Secure Access ist ein direkter Tele2 Anschluss mittels TopNet (MPLS-VPN) oder TopInternet (mit Tele2 Endgerät) am Unternehmensstandort.
Der Internetzugang für die mobilen Anwender bzw. Teleworker ist nicht Bestandteil von Teleworker Secure Access aber Voraussetzung für seine Nutzung. Als Teleworker Internetzugänge können beliebige Zugangsarten (zum Beispiel xDSL, GPRS, UMTS oder WLAN) genutzt werden. Der Internetzugang liegt im Verantwortungsbereich des Kunden.

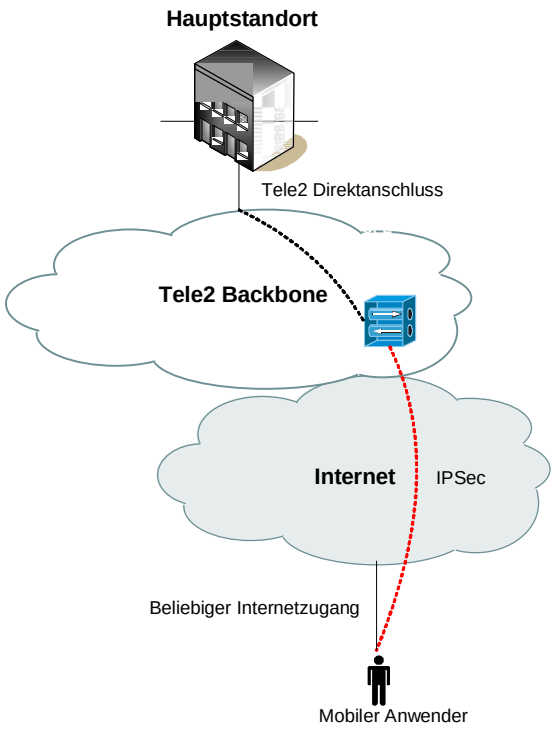

Abbildung 1: Funktionsweise Teleworker Secure Access

Abhängig von der Anzahl der mobilen Anwender und sonstiger Nutzung der Datenanbindung am Hauptstandort (beziehungsweise Serverstandort) ist eine Mindestbandbreite empfehlenswert. Richtwerte von Tele2:

Mobile Anwender [Anzahl]	5-10	11-50	51-100	100-200
Mindestbandbreite in kbit/s	1.024/1.024	2.048/2.048	4.096/4.096	8.192/8.192

1.2.2 Anforderungen an Notebook bzw. PC

Auf dem Notebook/PC des mobilen Anwenders wird ein IPSec Client (Cisco® VPN Client) installiert, der bei Internetanbindung nach Eingabe eines PINs (Persönliche Identifikationsnummer) durch den Benutzer über Internet eine sichere Verbindung zum Tele2 IPSec Gateway aufbaut. Der mitgelieferte USB-Token dient zur Identifizierung und Authentifizierung des mobilen Anwenders auf der Tele2 PKI (Public-Key-Infrastruktur). Am Notebook/PC des mobilen Anwenders und Administrator des Kunden ist desweiteren ein Client (ActivClient™) für den USB Token erforderlich. Der ActivClient ist ein Desktop Client der Funktionalitäten ergänzt wie zum Beispiel Änderung des PIN durch den mobilen Anwender.

Mindestens erforderliche Installationen am Client des mobilen Anwenders:

- IPSec Client (Cisco® VPN Client)
- Smartcard / USB-Token Client (ActivClient™)

Der Administrator des Kunden, der Benutzer oder die zuständige Abteilung des Kunden installiert die Clients auf den Rechnern. Tele2 stellt dazu all diese notwendigen Installationsdateien und Handbücher (siehe 1.4) zur Verfügung.

Die folgenden Betriebssysteme sind für Teleworker Secure Access freigegeben:

- Microsoft Windows Vista SP1 x86
- Microsoft Windows XP SP2
- Microsoft Windows 2000 SP4
- Microsoft Windows Server 2003 SP1/R2/SP2 x86

Einer des folgenden Browser wird für das Operator Portal benötigt:

- Microsoft Internet Explorer 6
- Microsoft Internet Explorer 7
- Firefox 1.5
- Firefox 2.0
- Mozilla 1.7

Sonstige Anforderungen:

- USB 2.0
- Administratorenrechte für die Installation erforderlich
- Mindestens 256 MB Arbeitsspeicher
- Mindestens 200 MB Festplattenspeicherplatz lokal am Gerät
- Betriebsbereite Netzwerk- und Internetverbindung

Andere VPN Clients die erfolgreich mit Teleworker Secure Access getestet wurden (sind nicht im Leistungsumfang enthalten):

- TheGreenBow IPSec VPN Client 4.5

Tele2 übernimmt für nicht von Tele2 zur Verfügung gestellte Clients keine Funktionsgarantie.

1.2.3 Authentifizierung

Die Authentifizierung (auch Authentifikation) bezeichnet den Vorgang, die Identität einer Person an Hand eines bestimmten Merkmals zu überprüfen. Für die Identitätsüberprüfung nutzt Teleworker Secure Access den USB-Token (siehe 1.7), die PKI und den persönlichen Benutzer PIN. Es wird überprüft ob die zu authentifizierende Person im Besitz des privaten Schlüssels ist. Dieser befindet sich bei Teleworker Secure Access ausschließlich auf einer Smartcard im USB-Token des Teleworkers. Für den Authentizitätsnachweis wird eine vertrauenswürdige Instanz benötigt. Diese Aufgabe übernimmt eine Zertifizierungsstelle (Certification Authority - CA), bei Teleworker Secure Access liegt diese Aufgabe bei Tele2. Zur Anerkennung der Tele2 Zertifizierungsstelle ist die Installation des zugehörigen Root Zertifikats erforderlich. Teleworker Secure Access verwendet zur Authentifizierung eine Mutual RSA Methode.
Der persönliche Benutzer PIN wird benötigt um im Falle eines Verlusts des USB-Token einen Missbrauch durch Dritte zu verhindern und wird direkt auf der USB-Token Hardware sicher gespeichert. Der PIN kann von 6 bis 25 Zeichen Länge besitzen und darf nicht zu trivial sein (Beispiel „123456“). Nach 6 Fehlversuchen wird der USB-Token automatisch gesperrt und kann nur mithilfe des Kundenadministrators oder Tele2 Supports wieder reaktiviert werden.

1.2.4 Verschlüsselung

Die sensiblen Firmendaten dürfen nicht für Dritte lesbar sein – deshalb werden sie verschlüsselt. Verfahren die den gleichen Schlüssel zum Ver- und Entschlüsseln verwenden haben einen gemeinsamen Nachteil: Wie bringt man einen Schlüssel über den unsicheren Kanal (Internet) zum Empfänger. Teleworker Secure Access nutzt daher die Tele2 PKI. Hier wird ein sich ergänzendes Schlüsselpaar eingesetzt – einer zum Verschlüsseln und ein dazugehöriger zum Entschlüsseln. Einen der beiden kann man veröffentlichen (Public Key), den anderen hält man geheim (Private Key). Was mit dem öffentlichen Schlüssel verschlüsselt wird soll nur mit dem dazugehörigen privaten Schlüssel wieder entschlüsselt werden können. Es ist dabei praktisch unmöglich aus dem öffentlichen Schlüssel den privaten Schlüssel zu berechnen oder verschlüsselte Daten ohne den dazugehörigen privaten Schlüssel wieder zu entschlüsseln. Um das zu gewährleisten kommen mathematische aufwendige Verfahren zum Einsatz. Der private Schlüssel ist bei Teleworker Secure Access auf dem USB-Token des Benutzers gespeichert und aus Sicherheitsgründen nicht einsehbar oder exportierbar. Die Schlüssellänge beträgt 1024-bit.

1.2.5 NAT und Firewalls

Firewalls können am Unternehmensstandort und Notebook/PC des mobilen Anwenders eingesetzt werden.
Grundsätzlich werden private IP Adressen (nach RFC 1918) im Kunden LAN und mit Firewall geschützte Internetzugänge unterstützt. Die NAT (Network Adress Translation) Geräte und Firewalls müssen dabei folgende Verbindungen vom privaten Netz zum Internet bzw. externen Netz unterstützen.

Ausgehende Verbindungen für die Protokolle:

- UDP Port 500 (IPSec)
- UDP Port 4500 (NAT-Traversal)
- ESP

1.2.6 IP-Adressen

Den mobilen Anwendern des Kunden werden von Tele2 öffentliche IP Adressen zugewiesen um Adresskonflikte zu vermeiden. Auf Anfrage können auch interne IP Adressen des Kunden vergeben werden. Private IP-Adressen werden entweder dynamisch oder auch statisch aus einem durch den Kunden definierten Pool zugewiesen.

1.3 Realisierungsvarianten

Tele2 stellen ihren Kunden österreichweit verschiedene Realisierungsvarianten für Teleworker Secure Access zur Verfügung, sofern die Anbindung für Tele2 technisch und betrieblich möglich und ökonomisch sinnvoll ist.

1.3.1 TopNet

TopNet (MPLS-VPN) ermöglicht nahtlose Kommunikation zwischen Zentrale, Filialen, Außendienstmitarbeitern und Teleworkern durch den Einsatz von MPLS-Technologie im Netz von Tele2. Tele2 empfiehlt bei der Vernetzung von mehreren Standort TopNet als Anschlussvariante. Weitere Informationen sind bei Bedarf der Leistungsbeschreibung „TopNet“ zu entnehmen.

Teleworker Secure Access ermöglicht die sichere Einbindung von Teleworkern in das kundeneigene MPLS-VPN wie in Abbildung 2 dargestellt.
Mithilfe des VPN Client wird über Internet eine sichere Verbindung zum Tele2 IP-Sec Gateway aufgebaut. Nach erfolgreicher Authentifizierung des Benutzers wird dieser in das kundeneigene MPLS VPN eingebunden. Tele2 vergibt VPN IP Adressen, das Forwarding und Routing geschieht im Tele2 Core-Netz.

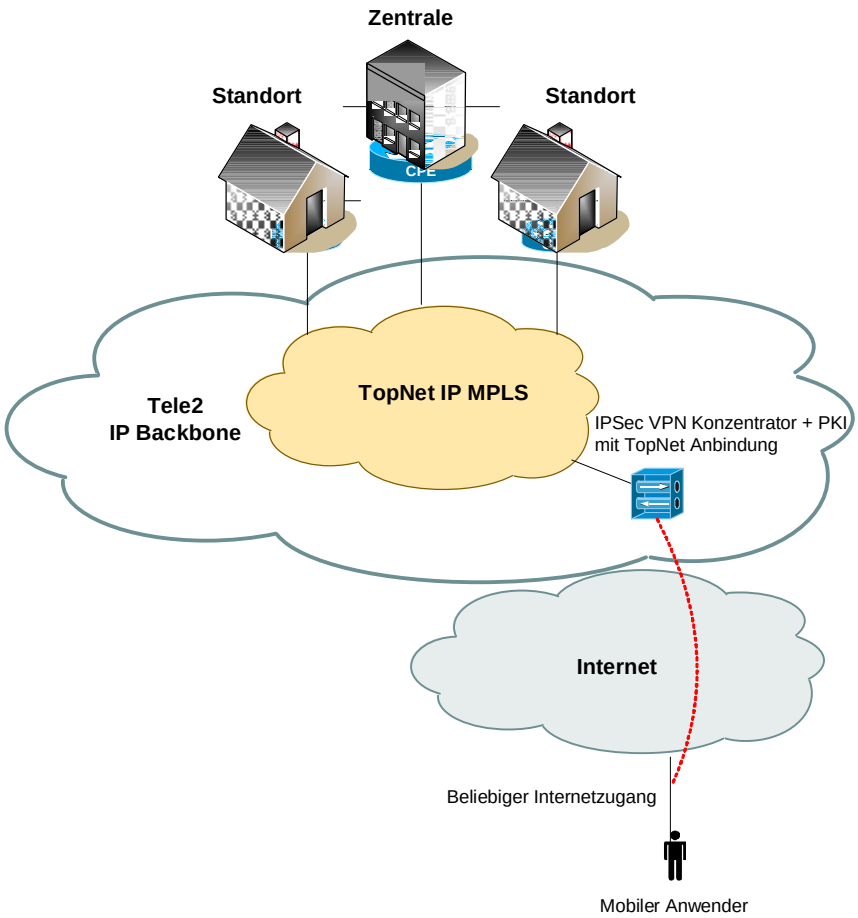

Abbildung 2: Realisierungsvariante TopNet

1.3.2 TopInternet

TopInternet steht für das Premium Internet Service von Tele2 und zeichnet sich durch höchste Flexibilität, Performance, Sicherheit und Qualität aus. Weitere Informationen sind bei Bedarf der Leistungsbeschreibung „TopInternet“ zu entnehmen.

TopInternet eignet sich insbesonders als Realisierungsvariante von Teleworker Secure Access für alle Unternehmensformen mit nur einem Standort.
Mithilfe des VPN Client wird über Internet eine sichere Verbindung zum Tele2 IP-Sec Gateway aufgebaut. Nach erfolgreicher Authentifizierung des Benutzers wird dieser über einen sogenannten „Permanent Virtual Circuit“ auf den Unternehmensstandort verbunden.

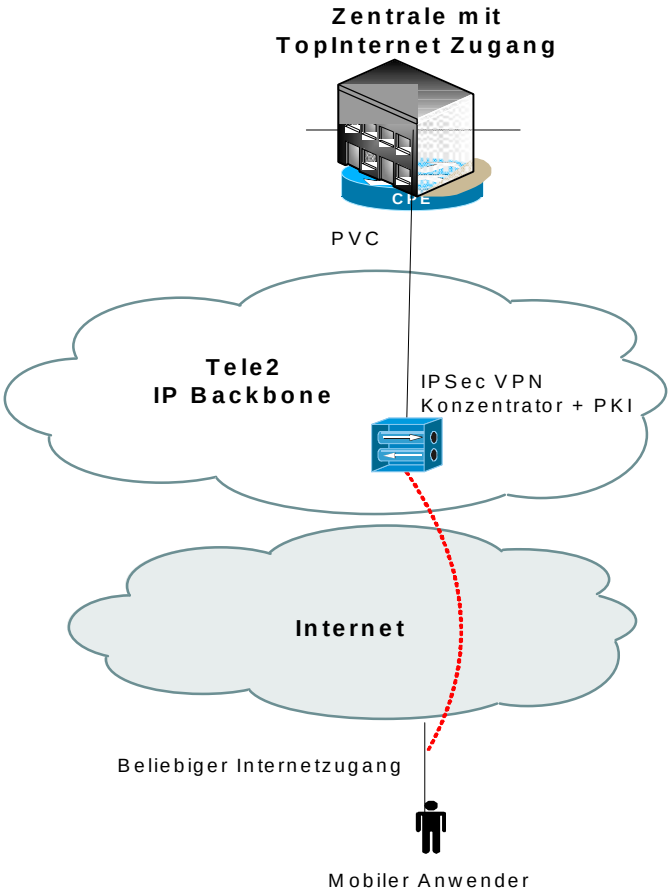

Abbildung 3: Realisierungsvariante TopInternet

1.4 Online Management und Dokumentation

Teleworker Secure Access wird über einen vorhandenen Webbrowser (z.B. Internet Explorer) administriert.

Es stehen folgende Möglichkeiten über den Online-Zugang unter http://tele2worker.at zur Verfügung:

- Operator Portal: Administration von Teleworker Secure Access
- User Portal: Update von Benutzerkonten durch den mobile Anwender
- Administratorenhandbuch: Anleitung für Kundenadministratoren
- Benutzerhandbuch: Anleitung für mobile Anwender

Die erforderlichen Zugangsdaten für den Kundenadministrator werden von Tele2 an die E-Mail Adresse laut Anmeldeformular geschickt. Die Zugangsdaten für die mobilen Anwender werden durch den Kundenadministrator verwaltet.

Folgende Aktionen können unter anderem über das Operator Portal veranlasst werden:

- Anlage und Verwaltung von Benutzern
- Definition und Änderung von Benutzerattributen: Vorname, Nachname, E-Mail Adresse,..
- Ausstellen von Benutzerzertifikaten
- Gesperrte Benutzer (z.B. aufgrund zu häufiger Falscheingabe des PINs) wieder reaktivieren
- Kurzfristiges oder dauerhaftes Sperren von Benutzern (z.B. da USB-Token gestohlen oder verloren wurde).
- Erneuerung von Benutzerzertifikaten

Das Sperren eines Benutzers bzw. eines Benutzerzertifikats kann nach Veranlassung bis zu einer Stunde verzögert wirksam werden.

1.5 Installation

Der Administrator des Kunden wird während der Ersteinrichtung von Tele2 kontaktiert und bekommt an die definierte E-Mail Adresse eine Bestätigungsmail mit Zugangsdaten. Nach Erhalt der USB-Token an die vorgegebene Kundenadresse kann der Administrator seinen persönlichen USB-Token über das User Portal selbst ausstellen. Mit Rückmeldung des Administrators an Tele2 wird die Serviceaktivierung vorgenommen und der Zugriff auf das Operator Portal ermöglicht.

1.6 Servicemanagement

Um die Verfügbarkeit des Services einhalten zu können, ist Tele2 bemüht, eventuell auftretende Störungen ehest möglich zu beheben. Um die Verfügbarkeit des Services einhalten zu können, wird dieses von Tele2 oder von beauftragten Dritten gewartet. Die Serviceleistung umfasst die Behebung aller Störungen und Fehler die im Verantwortungsbereich von Tele2 oder von ihr beauftragten Dritten liegen. Die Behebung von Fehlern und Störungen die von Tele2 oder ihren Erfüllungsgehilfen vertreten werden ist für den Kunden entgeltfrei.
Wird Tele2 jedoch zu einer Störungsbehebung gerufen und wird festgestellt, dass entweder keine Störung bei der Bereitstellung des Service vorliegt oder die Störung vom Kunden zu vertreten ist, hat der Kunde Tele2 den entstandenen Aufwand gemäß dem jeweils anwendbaren Spezialistenstundensatz zu ersetzen (siehe Tele2 AGB).
Der Nutzer erkennt an, dass eine zu 100 % Verfügbarkeit technisch generell nicht zu gewährleisten ist. Tele2 behält sich vor, aus Wartungs-, Sicherheits- oder Kapazitätsgründen die Dienstleistungen kurzzeitig auszusetzen oder zu beschränken.

1.7 Hardware

Tele2 stellt jedem Benutzer des Kunden USB-Token in Form eines Schlüsselanhängers zur Verfügung. USB-Token bezeichnen eine Hardware, die Teil eines Systems zur Identifizierung und Authentifizierung von Benutzern ist. Als weiteres Authentifizierungsmerkmal wird ein PIN eingesetzt der durch den Benutzer selbst gewählt werden kann. Der Besitz des Tokens ist zwingend erforderlich, um sich als berechtigter Nutzer auszuweisen.

Die USB-Token von Tele2 enthalten Smartcards, die ausgelesen und beschrieben werden. USB-Token mit Smartcards weisen den Vorteil auf kein Kartenlesegerät am Notebook/PC zu benötigen.

Tele2 überlässt seinen Kunden die benötigte Hardware im Rahmen des Service Teleworker Secure Access zur ordnungsgemäßen Benutzung. Bei Beendigung des Vertragsverhältnisses muss die Hardware an Tele2 retourniert werden. Tele2 behält sich vor, Hardware, deren optischer und technischer Zustand nicht der normalen Abnutzung entspricht, zum jeweiligen Zeitwert in Rechnung zu stellen.

1.7.1 Defekt von Hardware

Tele2 bietet eine kostenfreie Austauschwartung für defekte USB-Token bei sachgemäßer Nutzung innerhalb der ersten 36 Monate. Kunden die defekte Hardware tauschen möchten kontaktieren die Service-Hotline.

1.7.2 Verlust von Hardware

Der Benutzer kann direkt über das User Portal den Verlust eines USB-Tokens an den Kundenadministrator melden. Über den Tele2 Vertrieb kann ein neuer Token erworben werden. Bei Verlust des USB-Token sind einmalig € 99,- zu bezahlen.

1.7.3 Stornierung von Hardware

Das Service Teleworker Secure Access und seine Komponenten (USB-Token) wird entsprechend dem jeweiligen Access Produkt (TopNet oder TopInternet) mit dem vereinbarten Kündigungsverzicht abgeschlossen. Sollte es die wirtschaftliche Situation des Kunden erfordern einzelne Token vor Ablauf dieser Frist zu stornieren, ist mit dem zuständigen Vertriebsmitarbeiter von Tele2 eine kommerzielle Vereinbarung zu treffen. Andernfalls können dem Kunden die ausstehenden monatlichen Entgelte bis zum vereinbarten Vertragsende bei der nächsten Rechnungslegung auf einmal in Rechnung gestellt werden. Stornierte USB-Token sind in ordnungsgemäßen Zustand und einer entsprechenden Schutzverpackung an folgende Adresse zu senden:

Tele2 Telecommunication GmbH
Donau-City-Straße 11
A 1220 Wien

1.8 Wartung und Support

Dem Kunden steht die kostenlose Service-Hotline unter (0)50 500 3333 zur Meldung von technischen Störungen und telefonischem Support (Installationshilfe, Hilfe bei Bedienungsfehlern) von Mo-So von 0-24:00 zur Verfügung.
Fehler in den zentralen Komponenten im Tele2-Netzwerk werden von Tele2 von Mo-So von 0-24:00 proaktiv überwacht und behoben.